SULEYMAN DEMIREL UNIVERSITY

Suleyman Demirel
University

Karmak Bagisbayev

MATHEMATICS for COMPUTER SCIENCE

Kaskelen, 2015

УНИВЕРСИТЕТ ИМЕНИ СУЛЕЙМАНА ДЕМИРЕЛЯ

Karmak Bagisbayev

MATHEMATICS
for
COMPUTER SCIENCE

Kaskelen, 2015

The lost Sir arthur 2002	The norw jeremy pa	The three west2003	The turn lindop200

УДК 510.63, 519.101, 519.171
ББК 22.176 я73
B15

Рекомендовано к изданию Учебно-методическим советом Университета имени Сулеймана Демиреля, протокол № 1 от 25 августа 2015 г.

Рецензенты:

Кулпешов Б. Ш., член-корр. НАН РК, доктор физико-математических наук, профессор, Международный университет информационных технологий

Вербовский В. В., доктор физико-математических наук, доцент, Университет имени Сулеймана Демиреля

K. N. Bagisbayev

Mathematics for Computer Science: Tutorial. — Kaskelen, Suleyman Demirel University, 2015. — 153 p. — In English.

ISBN 978-601-7046-56-9

Tutorial «Introduction to Mathematics» is designed for bachelors of specialties 5B060100 — "Mathematics", 5B010900 — "Mathematics", 5B050703 — "Information systems", 5B050704 — "Computing technics and programming technologies" and contains the following topics: Mathematical Logic, Sets, Relations and Functions, Mathematical Induction and Combinatorics, Number systems.

УДК 510. 63, 519.101, 519.171
ББК 22.176 я73

ISBN 978-601-7046-56-9

Contents

PREFACE

There are two basic ways to formulate mathematical statements (problems, hypotheses, theorems ...): Russian and French. Russian way is to select the most simple and concrete case (so that no one could simplify the formulation, while maintaining the essence of the case). French way is to generalize the statement so that no one could generalize it further.

V. Arnold

The textbook is written as an introductory course in Discrete Mathematics for Computer Science and Engineering. It will be divided into 3 volumes:

1. Fundamental Concepts of Mathematics: Mathematical Logic, Set Theory, Relations and Functions, Induction and Combinatorics, Number Systems

2. Elements of Discrete Structures: Modular Arithmetic, Graphs, State Machines

3. Elements of Discrete Probability Theory

Why do we need another book on the basics of mathematics and for whom it is intended? — asks the reader opening this book. For 30 years the author has taught basic courses of algebra, analysis, and general mathematics for students of mathematical, technical, financial and economic departments of various universities of the former Soviet Union. Later, working as a professor of mathematics at the universities of the French speaking countries, I found that the teaching of mathematics in those countries methodologically was seriously different from the approach concretized (Soviet, American, British), namely, was much influenced by the world-famous school of Bourbaki, i.e. was based on the abstract axiomatic approach, while concretized approach is based on visuality and proceeds from interests of applications. Both approaches have their positive and negative sides. Positive aspects of the axiomatic approach are a unified presentation style, the most general wording of definitions and theorems, and as a consequence, students' understanding of mathematics as a whole object. Negative aspects are the complexity of the perception of abstract definitions by students, the lack of easy applications and practical computations. Positive aspects of the concretized approach are easier assimilation by students of the learning material because of its visuality, often in conditions of real variables, because of the use of graphs, charts and drawings. Negative aspects are, above all, a narrow perception of mathematics as a set of disconnected with each other computational methods and, as a consequence, the inability of students who know how to solve a certain range of tasks to transfer this skill to solve mathematically similar problems in other words and with other objects.

The question arises: Is it possible to combine these two approaches by retaining only their best parts? As shown by a long-term experiment: Yes, it is possible! And the main idea in this way is to illustrate each abstractly formulated concept by maximal large number of elementary examples of different nature familiar since high school. Of course, this requires a certain amount of time, but it is far outweighed by the later.

Anyone who undertakes to write a textbook of mathematics, is faced with the dilemma between completeness and rapidly growing volume, between rigor and understandability, and therefore must constantly seek a compromise between these contradictions. Since this textbook is designed for students – non mathematicians, author avoided too abstract concepts. Also were skipped the objects and theorems serving exclusively to justify the foundations of mathematics and not used in applications.

The textbook can also be used as an introduction to the university courses of algebra and calculus.

In conclusion, I would like to thank the Fulbright Scholarship Program of the United States Department of State, without the aid of which the writing and publishing of this book would have been impossible.

Chapter 1

MATHEMATICAL LOGIC

1.1. Basic notions of Mathematical Logic

1.1.1. Propositions.

Proposition is a primary and indefinable notion.

We call **proposition** any statement that is either ***true*** or ***false***.

The notions *true* and *false* are also primary and are not defined.

They are called "**logical constants**".

Example 1.

Proposition "Washington is the capital of the USA" is *true*.

Proposition "New York is the capital of the USA" is *false*.

We denote propositions by italic letters p, q, r etc., and we denote the words *true* and *false* by the letters t and f respectively. Truth or falsity of a proposition is called its *truth value* and we write briefly

$$p = t \text{ or } p = f.$$

Example 2.

Let $p = (6 \textit{ is divisible by } 3)$, $q = (2 + 2 = 4)$ and $r = (5 \textit{ is an even number})$.

Then $p = t, q = t$ and $q = f$.

<u>**Notice**</u>. <u>**Using of the equality sign**</u> **"="**.

In this textbook we use the equality sign $A = B$

for different purposes like follows:

1. to express the identity of two objects A and B: for example $1 = 1$
2. to assign to the object A his value B: for example $p = t$ (see ex. 2)
3. to define a new object A by a known object B:

for example $q = (2 + 2 = 4)$, (see ex.2)

Note 1.

Not each statement is a proposition. For example, the statement "Mathematics is more interesting than Physics" is not proposition. Why?

Note 2. There are propositions, which *truth value* is not easy to establish immediately. For example, the statement "there are still undiscovered elementary particles" is the proposition.

Note 3. There are statements which are not propositions, but can become it with additional information. For example, the statement "There was a rain" is not proposition, but with the precision "Yesterday there was a rain" it becomes proposition.

Exercises 1.1

Determine which of the following statements are propositions and find their truth values:

a) $2 \times 3 = 6$; b) $5 < 3$; c) "*New York is the biggest city of USA*", d) New York is the best city of USA; e) "*Do you like New York?*".

1.2. Operations on Propositions.

We can create *compound* propositions from two *elementary* ones by using propositional connectives "and", "or", "if...then", "if and only if".

Using the particle "not" we can create a new proposition from old one by negation.

1.2.1. Definition. Negation.

We call *negation* of the proposition p a new proposition denoted by $\bar{p}$ (or $\neg p$), read "***not*** p" and defined by its *truth table*:

p	$\bar{p}$
t	f
f	t

In other words

$\bar{p}$ **is** $false$ **if** p **is** $true$**, and is** $true$ **if** p **is** $false$.

Examples:

If $p = (6 \textit{ is a prime number}) = f$,

then $\bar{p} = (6 \textit{ is not a prime number}) = (6 \textit{ is a composite number}) = t$.

If $q = (4 \textit{ is an odd number}) = f$,

then $\bar{q} = (4 \textit{ is not an odd number}) = (4 \textit{ is an even number}) = t$.

If $r = (7 = 7) = t$,

then $\bar{r} = (7 \neq 7) = f$.

If $s = (3 \textit{ is less than } 5) = (3 < 5) = t$,

then $\bar{s} = (3 \textit{ is not less than } 5) = (3 \geq 5) = f$.

More generally, there exist special notations for the negations of comparison relations:

$\overline{(a = b)} = (a \neq b)$; $\overline{(a \neq b)} = (a = b)$,

$\overline{(a > b)} = (a \leq b)$; $\overline{(a \leq b)} = (a > b)$,

$\overline{(a \geq b)} = (a < b)$; $\overline{(a < b)} = (a \geq b)$.

Notation. Expression "Number n is divisible by number m" is denoted briefly $m|n$ and we read m *divide* n. For example, $3|6$. Negation "n is not divisible by m" is denoted by $m \nmid n$ and we read m *doesn't divide* n. For example, $3 \nmid 7$.

So, $\overline{m|n} = m \nmid n$.

1.2.2. Definition. Conjunction.

We call *conjunction* of two propositions p and q a new proposition denoted by $p \wedge q$ (or $p\&q$), read "p ***and*** q" and defined by its *truth table*:

p	q	$p \wedge q$
t	t	t
t	f	f
f	t	f
f	f	f

In other words

$p \wedge q$ **is** $true$ **if** p **and** q **are both** $true$**, and is** $false$ **otherwise.**

Or once more

$p \wedge q$ **is** $false$ **if at least one of the propositions** p, q **is** $false$.

Example 1.

$(1 < 3 < 5) = (1 < 3) \wedge (3 < 5) = t \wedge t = t,$

$(1 < 3) \wedge (3 > 5) = t \wedge f = f,$

$(1 > 3) \wedge (3 < 5) = f \wedge t = f,$

$(1 > 3) \wedge (3 > 5) = f \wedge f = f,$

Example 2.

Forecast "there will be fair weather and warm tomorrow" is conjunction of two propositions:

"there will be fair weather tomorrow" *and* "there will be warm tomorrow"

It's clear that forecast as proposition will be true if and only if both of last propositions will be true.

Example 3.

Proposition "($snow\ is\ black$) and ($Earth\ is\ bigger\ than\ Moon$)" is false

because $f \wedge t = f$

<u>Note</u>. *Conjunction "and"* corresponds to the union "and" in English.

1.2.3. Definition. Disjunction.

We call *disjunction* of two propositions p and q a new proposition denoted by $p \vee q$, read "p *or* q" and defined by its *truth table*:

p	q	$p \vee q$
t	t	t
t	f	t
f	t	t
f	f	f

In other words

$p \vee q$ is $false$ if p and q are both $false$, and is $true$ otherwise.

Or once more

$p \vee q$ is $true$ if at least one of the propositions p, q is $true$ (or both).

Example 1.

$(3 \leq 5) = (3 < 5) \vee (3 = 5) = t \vee f = t,$

$(5 \leq 5) = (5 < 5) \vee (5 = 5) = f \vee t = t,$

Example 2.

$(number\ 2\ is\ even) \vee (number\ 2\ is\ prime) = t \vee t = t,$

$(number\ 2\ is\ even) \vee (number\ 2\ is\ composite) = t \vee f = t,$

$(number\ 2\ is\ odd) \vee (number\ 2\ is\ prime) = f \vee t = t,$

$(number\ 2\ is\ odd) \vee (number\ 2\ is\ composite) = f \vee f = f,$

Example 3.

Proposition "($snow\ is\ black$) or ($Earth\ is\ bigger\ than\ Moon$)" is true because $f \vee t = t$.

Note. *Disjunction "or"* in the definition above corresponds to the union "or" in English and can mean also "both", that is can be *true* when the propositions p and q are both *true* according to the last line of the truth table. For example, the proposition

"*I will go to the cinema with my friend A or my friend B*" will be also *true* if we will go to the cinema all three.

The next definition gives us another example of the union "or", namely "*either ... or*".

1.2.4. Definition. Exclusive "or".

We call *exclusive or* of two propositions p and q a new proposition denoted by $p \veebar q$, read "*either p or q*" and defined by its *truth table*:

p	q	$p \veebar q$
t	t	f
t	f	t
f	t	t
f	f	f

In other words

$p \veebar q$ is $true$ when exactly one of p and q is true (not both).

Example 1.

a) The Expression "*I will go to the cinema or to the theatre tonight*" in reality means the proposition

"*I will go either to the cinema or to the theatre tonight*" with *exclusive or*, because it is impossible to go to the cinema and to the theatre at the same time.

b) Expression $x = \pm 1$ means $(x = -1) \veebar (x = +1)$

Example 2.

$(number\ 2\ is\ even)\ \underline{\vee}\ (number\ 2\ is\ prime) = t \vee t = f,$

$(number\ 2\ is\ even)\ \underline{\vee}\ (number\ 2\ is\ composite) = t \vee f = t,$

$(number\ 2\ is\ odd)\ \underline{\vee}\ (number\ 2\ is\ prime) = f \vee t = t,$

$(number\ 2\ is\ odd)\ \underline{\vee}\ (number\ 2\ is\ composite) = f \vee f = f,$

Example 3.

Proposition

"*snow is either white or Eath is bigger than Moon*" is false

because $t\ \underline{\vee}\ t = f$.

1.2.5. Definition. Conditional.

We call *conditional* of two propositions p and q (taken in definite order) a new proposition denoted by $p \to q$, read "***if p then q***"

(or "***p implies q***") and defined by its *truth table*:

p	q	$p \to q$
t	t	t
t	f	f
f	t	t
f	f	t

In other words

$p \to q$ is *false* in only case when p is *true* and q is *false*", and is *true* otherwise.

Example 1.

$((5 > 3) \to (4\ is\ even)) = (t \to t) = t,$

$((5 > 3) \to (4\ is\ odd)) = (t \to f) = f,$

$((5 < 3) \to (4\ is\ even)) = (f \to t) = t,$

$((5 < 3) \to (4\ is\ odd)) = (f \to f) = t.$

As we see from this example (lines 3 and 4) or from truth table, just introduced mathematical "*implies*" differs from "implies" used in the ordinary speech.

The next example likely can help understand this so "strange" definition.

Example 2.

As we know Boston is the capital of the Massachusetts state.

So, it is natural to recognize that the conditional

"*If Mary is from Boston then Mary is from Massachusetts*"

is **always** true, i.e.

if Mary is really from Boston then $(t \to t) = t$,

if Mary is from Lowell (city in Massachusetts) then $(f \to t) = t$,

if Mary is from Washington then $(f \to f) = t$.

Example 3.

Proposition "$(snow\ is\ black)\ implies\ (Earth\ is\ smaller\ than\ Moon)$" is true

because $(f \to f) = t$.

Note.

As follows from the 3rd and 4th lines of the truth table

$(f \to t) = t$ and $(f \to f) = t$, so we can make an "interesting" declaration: "falsehood implies anything you want".

As follows from the 1st and 3rd lines of the truth table

$(t \to t) = t$ and $(f \to t) = t$, so we can make another "interesting" declaration: "truth follows from anything you want".

1.2.6. Definition. Biconditional.

We call *biconditional* of two propositions p and q a new proposition denoted by $p \leftrightarrow q$, read "***p if and only if q***" (or "***p is equivalent to q***") and defined by its *truth table*:

p	q	$p \leftrightarrow q$
t	t	t
t	f	f
f	t	f
f	f	t

In other words

$p \leftrightarrow q$ is *true* if the truth values of p and q are the same, and is *false* otherwise.

Example 1.

$[(2 + 3 = 5) \leftrightarrow (7\ is\ prime\ number)] = (t \leftrightarrow t) = t,$

$[(2 + 3 = 5) \leftrightarrow (7 is\ composite\ number)] = (t \leftrightarrow f) = f,$

$[(2 + 3 = 4) \leftrightarrow (7 is\ prime\ number)] = (f \leftrightarrow t) = f,$

$[(2 + 3 = 4) \leftrightarrow (7 is\ composite\ number)] = (f \leftrightarrow f) = t.$

Note. In ordinary daily speech we use often "if" but mean in reality "if and only if".

Example 2.

Proposition "$I\ will\ go\ to\ the\ cinema\ if\ you\ go\ with\ me$" means in reality proposition-biconditional

"$I\ will\ go\ to\ the\ cinema\ if\ and\ only\ if\ you\ go\ with\ me$"

Example 3.

Proposition

"$(snow\ is\ black)\ is\ equivqlent\ to\ (Earth\ is\ smaller\ than\ Moon)$" $is\ true$ because $(f \leftrightarrow f) = t$.

Important notice. Reminder.

In contrast to the ordinary speech when we combine compound propositions with propositional connectives

"$and(\wedge),\ or\ (\vee),\ either \dots or\ (\underline{\vee}),\ if \dots then(\rightarrow),\ if and\ only\ if(\leftrightarrow)$"

we do not pay attention to the verbal meaning of the propositions p and q wich may be even unrelated as we saw in all three examples above. All we need to establish truth or falsity of a compound proposition is to know the truth values of its components p and q.

Note. Arity of operations.

The number of arguments (or operands) involved in operation is called **arity** of this operation. For example, negation is a **unary** operation; conjunction, disjunction, exclusive disjunction, conditional, biconditional are **binary** operations.

Constants t and f can be considered sometimes as **nullary** operations.

Note. Other notations. There exist other notations of logical constants and logical operations used by different authors. For example, instead of t and f they use "1" and "0". Instead of $\wedge$ and $\vee$ they use "·" and "+".

Exercises 1.2.

1. Formulate the negations of the following propositions and find their truth values:
a) "$January\ is\ summer\ month$"; b) "$8\ is\ not\ divisible\ by\ 4$"; c) $2 < 3$;
d) $2 \leq 3$; e) "$all\ prime\ numbers\ are\ odd$".
2. Prove or disprove the following propositions by forming their negations:
a) $2 \leq 2$; example of answer: $\overline{2 \leq 2} = 2 > 2$ is false, that is $2 \leq 2$ is true;
b) $2 \leq 3$; c) $2 \geq 3$.
3. Generalize conjunction on arbitrary number of propositions:

$(p_1 \wedge p_2 \wedge \dots \wedge p_n) = (\dots((p_1 \wedge p_2) \wedge p_3) \dots \wedge p_n)$.
Prove that $p_1 \wedge p_2 \wedge \dots \wedge p_n$ is true if and only if all propositions $p_1, p_2, \dots, p_n$ are true.
4. Generalize disjunction on arbitrary number of propositions:
$(p_1 \vee p_2 \vee \dots \vee p_n) = (\dots((p_1 \vee p_2) \vee p_3) \dots \vee p_n)$.
Prove that $p_1 \vee p_2 \vee \dots \vee p_n$ is true if at least one of the propositions $p_1, p_2, \dots, p_n$ is true.
5. Find the truth values of:
a) $2 \leq 3$; b) $2 \geq 3$; c) $2 \cdot 2 \leq 4$; d) $2 \cdot 2 \geq 4$; e) $(2 \cdot 3 \geq 6) \wedge (2 \cdot 3 \leq 7)$;
f) $(2 \cdot 2 = 4) \vee (elephants\ live\ in\ America)$.
6. Find the truth values of p, q, r, s if:
a) "$p \wedge (2 \cdot 2 = 4)$" $= t$; b) "$q \wedge (2 \cdot 2 = 4)$" $= f$;
c) "$r \vee (2 \cdot 2 = 5)$" $= t$; d) "$s \vee (2 \cdot 2 = 5)$" $= f$.
7. Find on the coordinate plane $x0y$ the sets of points (x, y) such that:
a) $(x > 0) \wedge (y > 0)$; b) $(x > 0) \wedge (y \leq 0)$; c) $(x = 0) \wedge (y = 0)$;
d) $(x > 0) \vee (y > 0)$; e) $(x > 0) \vee (y \leq 0)$; f) $(x = 0) \vee (y = 0)$.
8. Find on the R the sets of the points x such that:
a) $\begin{cases} x \geq 0 \\ x \leq 0 \end{cases}$; b) $\begin{cases} x > 1 \\ x < 0 \end{cases}$; remainder: $\begin{cases} p \\ q \end{cases}$ is true if and only if $p \wedge q$ is true.
6. Find the truth values of: ("$m|n$" $is\ by\ definition$ "n is divisible by m")
a) $6|12 \rightarrow 3|12$; b) $6|7 \rightarrow 3|7$; c) $6|9 \rightarrow 3|9$; d) $3|9 \rightarrow 6|9$.
9. Find the truth values of p, q, r, s if:
a) "$4\ is\ even \rightarrow p$" $= t$; b) "$q \rightarrow 4\ is\ odd$" $= t$;
c) "$4\ is\ even \rightarrow r$" $= f$; d) "$s \rightarrow 4\ is\ odd$" $= f$.
10. Find the truth values of:
a) $6|12 \leftrightarrow 3|12$; b) $6|7 \leftrightarrow 3|7$; c) $6|9 \leftrightarrow 3|9$; d) $3|9 \rightarrow 6|9$.
11. Find the truth values of p, q, r, s if:
a) "$p \leftrightarrow (1 < 2)$" $= t$; b) "$q \leftrightarrow (1 > 2)$" $= t$;
c) "$r \leftrightarrow (1 < 2)$" $= f$; d) "$s \leftrightarrow (1 > 2)$" $= f$.
12. Is there a day of the week when the proposition
a) "If Today is Monday, then tomorrow will be Friday" is true?
b) "If Today is Monday, then tomorrow will be Tuesday" is false?

Answers: a) any day, but not Monday; b) no.

1.3. Logical Laws.

Note. We can create *compound propositions* of varying complexity from *elementary propositions* (operands) p, q, r etc. by means of introduced above logical operations, logical constants t, f and brackets:

for example $(\overline{p \wedge q}) \rightarrow ((r \vee \overline{p}) \leftrightarrow q)$

There is no order of precedence of logical operations, so all propositions must be properly bracketed like in example above.

Further below saying "proposition" we mean elementary proposition or compound proposition or even logical constants t and f.

1.3.1. Definition. Tautology.

A proposition that is true no matter what are the truth values of its operands is called a *tautology*.

Example. $p \underline{\vee} \bar{p}$ is tautology.

Proof

p	$\bar{p}$	$p \underline{\vee} \bar{p}$
t	f	$t \underline{\vee} f = t$
f	t	$f \underline{\vee} t = t$

The last column consists only *true*, hence the proposition $p \underline{\vee} \bar{p}$ is a tautology.

Definition. Contradiction.

A proposition that is false no matter what are the truth values of its operands is called a *contradiction.*

Example. $p \wedge \bar{p}$ is contradiction.

Proof

p	$\bar{p}$	$p \wedge \bar{p}$
t	f	$t \wedge f = f$
f	t	$f \wedge t = f$

The last column consists only *false*, hence the proposition $p \wedge \bar{p}$ is contradiction.

Definition. Contingency.

A proposition that is neither a tautology nor a contradiction is a *contingency*.

1.3.2. Definition. Logical Implication.

We say that proposition p ***logically implies*** proposition q if the implication $p \to q$ is a tautology and we denote it by $p \Rightarrow q$.

Note. In fact, $p \Rightarrow q$ if q is true whenever p is true.

Really, according to the truth table (1.2.5.) conditional $p \to q$ can be false in only case when p is true and q is false, so to prove $p \Rightarrow q$ it is sufficient to check if there is no such set of values of the operands occurring in p and q so that p is *true* and q is *false.*

Example. Prove that $(p \to q) \wedge p \Rightarrow q$

1. Proof by truth table

p	q	$p \to q$	$(p \to q) \wedge p$	$((p \to q) \wedge p) \to q$
t	t	t	t	t
t	f	f	f	t
f	t	t	f	t
f	f	t	f	t

The last column consists only *true*, hence $(p \to q) \wedge p \Rightarrow q$.

2. Proof by reasoning.

Really, as we know the implication $((p \to q) \wedge p) \to q$ can be false in only case when $(p \to q) \wedge p$ is true and q is false. But it's impossible because $(p \to q) \wedge p$ is true if and only if p *and* $p \to q$ are both true, and this implies $q = t$ because if not then $t \to f = f$. So, once again that $(p \to q) \wedge p \Rightarrow q$.

Note. If p doesn't logically imply q (i.e. $p \to q$ is not a tautology) we denote this relation by $p \nRightarrow q$.

Exercise. Prove that $p \vee q \nRightarrow p$.

1.3.3. Definition. Logical Equivalence.

Two propositions p and q are called ***logically equivqlent*** if their equivalence $p \leftrightarrow q$ is a tautology and we denote it by $p \Leftrightarrow q$ (sometimes $p \equiv q$).

In other words, $p \Leftrightarrow q$ if p and q have the same truth values no matter what truth values their component operands have.

Example. Prove that $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.

1. Proof by truth table.

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$	$p \leftrightarrow q$	$(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$
t	t	t	t	t	t	t
t	f	f	t	f	f	t
f	t	t	f	f	f	t
f	f	t	t	t	t	t

The last column consists only *true*, hence $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.

2. Proof by reasoning.

Suppose that $p \leftrightarrow q$ is true, i.e. p and q have the same truth values. Then $p \to q$ and $q \to p$ are both true, hence $(p \to q) \wedge (q \to p)$ is true too.

Suppose now that $(p \to q) \wedge (q \to p)$ is true. Then $p \to q$ and $q \to p$ are both true that is p and q cannot have different truth values, otherwise one of $p \to q$ or $q \to p$ must be false. So, $p \leftrightarrow q$ is true and we proved once again that $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.

In other words we can say that $p \Leftrightarrow q$ is the same as $p \Rightarrow q$ and $q \Rightarrow p$.

So $p \Leftrightarrow q$ if and only if $p \Rightarrow q$ and $q \Rightarrow p$, what will be used often in theorem's proof.

Note. If p is not logically equivalent to q (i.e. $p \leftrightarrow q$ is not a tautology) we denote this relation by $p \not\Leftrightarrow q$.

Exercise. Prove that $p \to q \not\Leftrightarrow q \to p$.

Note. Attention! Logical Implication $p \Rightarrow q$ and Logical Equivalence $p \Leftrightarrow q$ are not operations on propositions. They represent respectively the fact that the propositions $p \to q$ and $p \leftrightarrow q$ are always true. Logical Implication and Logical Equivalence are the Relations between the propositions, like equality between the numbers, parallelism between the straight lines etc. (they are propositions of fact; they do not have a truth table).

1.3.4. Classical Logical Laws.

Definition. Logical implications and logical equivalences of compound propositions are often called *Logical Laws*.

Here are below the list of the most used logical laws:

I. Law of Negation of the Negation (or Double Negation Law).

$\boxed{\bar{\bar{p}} \Leftrightarrow p}$

Proof:

p	$\bar{\bar{p}}$
t	$\bar{\bar{t}} = \overline{(\bar{t})} = \bar{f} = t$
f	$\bar{\bar{f}} = \overline{(\bar{f})} = \bar{t} = f$

The Law says that the double negation of any proposition is logically equivalent to the proposition itself.

II. Law of Contradiction.

$\boxed{p \wedge \bar{p} \Leftrightarrow f}$

Proof: see example of contradiction above.

The Law of Contradiction says that any proposition and its negation cannot be true simultaneously.

Note. However, there exists a Biblical legend about the King Solomon who had a ring on opposite sides of which were carved two great wisdoms:

"All passes" and "Nothing passes". If, in real life we philosophically accept both of these mutually exclusive propositions as true, we cannot do the same in mathematical logic. This example illustrates that the mathematical logic as a model of the real complicated word of human reasoning is not perfect, as all models built by man to explain the ambient world.

III. Law of Excluded Middle.

$\boxed{p \veebar \bar{p} \Leftrightarrow t}$

Proof: see example of tautology above.

The Law says that any proposition is either true or false, no middle.

Note. As you know there are political and financial forecasters who abuse this law, "unmistakably" doing any prediction simultaneously with its negation and connecting them by disjunction "or" like an old fortune-teller who predicted a pregnant woman, "give birth to a boy or a girl"

Note. In the most of books on mathematical logic the law of excluded middle is given in the equivalent form $p \vee \bar{p} \Leftrightarrow t$.

IV. Commutative Laws

of conjunction $\boxed{p \wedge q \Leftrightarrow q \wedge p}$

of disjunction $\boxed{p \vee q \Leftrightarrow q \vee p}$

V. Associative Laws

of conjunction $\boxed{(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)}$

of disjunction $\boxed{(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)}$

VI. Distributive Laws

$\boxed{p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)}$

$\boxed{p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)}$

VII. Idempotent Laws

$\boxed{p \wedge p \Leftrightarrow p}$, $\boxed{p \vee p \Leftrightarrow p}$

VIII. Bound Laws

$\boxed{p \wedge t \Leftrightarrow p}$, $\boxed{p \wedge f \Leftrightarrow f}$,

$\boxed{p \vee t \Leftrightarrow t}$, $\boxed{p \vee f \Leftrightarrow p}$

IX. Absorption Laws

$\boxed{p \vee (p \wedge q) \Leftrightarrow p}$,

$\boxed{p \wedge (p \vee q) \Leftrightarrow p}$

X. De Morgan's Laws

$\boxed{\overline{p \wedge q} \Leftrightarrow \overline{p} \vee \overline{q}}$

$\boxed{\overline{p \vee q} \Leftrightarrow \overline{p} \wedge \overline{q}}$

XI. Contrapositive Laws

$\boxed{p \to q \Leftrightarrow \overline{q} \to \overline{p}}$

$\boxed{p \to q \Leftrightarrow \overline{p} \vee q}$

XII. Inference Laws:

a. Modus Ponens $\boxed{(p \to q) \wedge p \Rightarrow q}$,

b. Modus Tollens $\boxed{(p \to q) \wedge \overline{q} \Rightarrow \overline{p}}$,

c. Law of Syllogism $\boxed{(p \to q) \wedge (q \to r) \Rightarrow p \to r}$

Proof

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$
t	t	t	t	t	t	t	t
t	t	f	t	f	f	f	t
t	f	t	f	t	f	t	t
t	f	f	f	t	f	f	t
f	t	t	t	t	t	t	t
f	t	f	t	f	f	t	t
f	f	t	t	t	t	t	t
f	f	f	t	t	t	t	t

The last column consist only $true$, hence $(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$

Note. You see that the truth table of propositions with 1 operand has $2^1 = 2$ row (see ex-s for tautology and contradiction above), with 2 operands has $2^2 = 4$ rows (see ex-s for logical implication and logical equivalence above), with 3 operands has $2^3 = 8$ rows (see ex. for Law XI (c)).

More generally the truth table for proposition with n operands will have 2^n rows that you can be able to prove later during the study of combinatorics.

Note. <u>Equivalent Transformations</u>. If in a compound proposition we replace an operand by another logically equivalent one, we will receive a new proposition logically equivalent to the initial proposition. Such replacements are called $Equivalent\ Transformations$. They allow us to simplify the different logical expressions. In such simplifying we replace a tautology by the logical constant t and a contradiction by the logical constant f.

Example. $\left(\overline{p \vee \overline{q}} \vee (\overline{p} \wedge r)\right) \wedge (q \vee \overline{q}) \wedge (q \vee r) \Leftrightarrow \left(\overline{p \vee \overline{q}} \vee (\overline{p} \wedge r)\right) \wedge t \wedge (q \vee r) \Leftrightarrow \left(\overline{p \vee \overline{q}} \vee (\overline{p} \wedge r)\right) \wedge (q \vee r) \Leftrightarrow ((\overline{p} \wedge q) \vee (\overline{p} \wedge r)) \wedge (q \vee r) \Leftrightarrow \overline{p} \wedge (q \vee r) \wedge (q \vee r) \Leftrightarrow \overline{p} \wedge (q \vee r)$.

Explain each transformation in this chain of transformations by using logical laws.

Exercises 1.3.

1. Prove Logical Laws I – XII by creating appropriate truth tables or by another short way if possible.

2. Find the solution of the following well-known fun task:

The police detained four gangsters suspected in car theft: Henry, George, Lois and Tom. During the interrogation they gave the following testimonies: Henry: "It was Lois". Lois: "Tom made it". George: "It's not me". Tom: "Lois is lying, saying that it was me".

Further investigation showed that only one of them told the truth. Who stole the car?

Solution. If we denote the propositions $L =$ "*Lois stole the car*", $T =$ "*Tom stole the car*", $G =$ "*George stole the car*" then according to 4 testimonies above during interrogation the result is disjunction $L \vee T \vee \bar{G} \vee \bar{T}$ and according to the investigation is true because at least one of them is true (Bound Laws VIII). According to the Law of Excluded Third one of the propositions T or $\bar{T}$ is true and the all others are false because according to the investigation only one testimony is true. Suppose first T is true. Then $L, \bar{G}, \bar{T}$ are false. But if $\bar{G}$ and $\bar{T}$ are false then G and T are true, i.e., there are two true testimony that contradict to the investigation. If $\bar{T}$ is true then $L, \bar{G}, T$ are false or only G is true. So, answer is "George stole the car".

3. Defendants A, B and C gave the following testimonies.

A: "B is guilty and C is not guilty",

B: "A is not guilty or C is guilty",

C: "I am not re true guilty but at least one of A and B is guilty"

Assuming that all four testimonies are true at the same time, find which one of them is guilty.

Answer: B is guilty.

Hint: Prove first that $(B \wedge \bar{C}) \wedge (\bar{A} \wedge C) \wedge [\bar{C} \wedge (A \vee B)] \Leftrightarrow \bar{A} \wedge B \wedge \bar{C}$.

4. Using the definition of the Logical Implication, Logical Equivalence and Syllogism Law prove that

a) $(p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_n) \Rightarrow (p_1 \Rightarrow p_n)$,

b) $(p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n) \Rightarrow (p_1 \Leftrightarrow p_n)$,

c) If $p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_n \Rightarrow p_1$ then $p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n$.

5. Prove that $\overline{p \leftrightarrow q} \Leftrightarrow p \underline{\vee} q$.

1.4. Definitions and Theorems

1.4.1. Theorems of Logical Implication. Converse, Inverse and Contrapositive Propositions.

Any theorem is given as a proposition. To prove a theorem it is to prove that this proposition is a tautology.

Definition.

Theorems of the form $p \Rightarrow q$ are called

Theorems of the *Logical Implication*.

p is called ***hypothesis*** and q is called ***conclusion***.

Most often, theorems are given in the form of a *Logical Implication*.

To prove such theorems is to prove that the conditional proposition $p \rightarrow q$ is a tautology, in other words that it is a logical implication $p \Rightarrow q$.

Example. The theorem

"*Mary is from Boston*" $\Rightarrow$ "*Mary is from Massachusetts*"

was proved in fact in 1.2.5 (example 2). According to the note 2 (1.3.2) in order to prove this theorem it is sufficient to assume that hypothesis is true. Then conclusion is obviously true because Boston is a city in the State of Massachusetts.

Definition.

For each conditional proposition $p \rightarrow q$

we can construct three propositions: $\bar{q} \rightarrow \bar{p}$, $q \rightarrow p$, $\bar{p} \rightarrow \bar{q}$ called respectively

contrapositive, ***converse***, and ***inverse*** proposition of the ***direct*** proposition $p \rightarrow q$.

Let's build the tables of truth for these four propositions:

		direct	contrapositive	converse	inverse
p	q	$p \rightarrow q$	$\bar{q} \rightarrow \bar{p}$	$q \rightarrow p$	$\bar{p} \rightarrow \bar{q}$
t	t	t	t	t	t
t	f	f	f	t	t
f	t	t	t	f	f
f	f	t	t	t	t

Let consider a direct conditional proposition "If Mary is from Boston then Mary is from Massachusetts". This proposition is always true, i.e. is a theorem.

1. **Contrapositive proposition.**

The contrapositive proposition "If Mary is not from Massachusetts then Mary is not from Boston" is true, i.e. is a theorem.

As we see generally from the 3rd and 4th columns of the truth table above

$p \rightarrow q \Leftrightarrow \bar{q} \rightarrow \bar{p}$.

Conclusion: *Contrapositive proposition of a theorem is a theorem.*

This theorem is called *contrapositive theorem* and it is logically equivalent to the direct theorem.

2. **Converse proposition.**

But the converse proposition "If Mary is from Massachusetts then Mary is from Boston" is false, i.e. is not a theorem.

(Example when converse proposition is also a theorem will be given soon below).

As we see generally from the 3rd and 5th columns of truth table above

$p \to q \not\Leftrightarrow q \to p.$

Conclusion:

Not each converse proposition of a theorem is a theorem.

3. **Inverse proposition.**

The inverse proposition "If Mary is not from Boston then Mary is not from Massachusetts" is false, i.e. is not a theorem.

As we see generally from the 3rd and 6th columns of the truth table above

$p \to q \not\Leftrightarrow \overline{p} \to \overline{q}.$

Conclusion: *Not each inverse proposition of a theorem is a theorem.*

Note. As we see generally from the 5th and 6th columns of the truth table above

$q \to p \Leftrightarrow \overline{p} \to \overline{q}$, that is

converse and inverse propositions are logically equivalent

1.4.2. Proof of the theorems: by Contrapositive, by Contradiction, by Syllogism.

Proof by Contrapositive.

The last conclusion about contrapositive proposition allows us instead of proving the direct theorem to prove its contrapositive which may be sometimes easier.

Example. Instead of proving the direct theorem

"$If\ m^2\ is\ odd\ then\ m\ is\ odd$"

we will prove its contrapositive "$If\ m\ is\ even\ then\ m^2\ is\ even$".

Really, if m is even then $m = 2n, n \in N$, hence $m^2 = 4n^2 = 2 \cdot (2n^2) = 2p$,

i.e. m^2 is even. Contrapositive theorem is proved, consequently direct theorem is proved too.

Note. As we see also from the 4rd and 5th columns of the truth table above

$q \to p \Leftrightarrow \overline{p} \to \overline{q}$, i.e. the converse and inverse propositions are logically equivalent.

Proof by Contrapositive is the special case of more general

Proof by Contradiction (Reductio ad Absurdum).

In a proof by Contradiction we prove a proposition r (which is not necessary an implication) by assuming its negation $\overline{r}$ and deriving a contradiction $r \wedge \overline{r}$.

Example. Prove that $\sqrt{2}$ is not rational number, i.e., there are no natural numbers m and n such that $\sqrt{2} = m/n$.

Proof. Assume negation of the theorem: there are two naturals $m, n \in N$ such that

$\sqrt{2} = m/n$ and m/n is an uncancelled fraction, i.e. is written in least terms.

Then

$\left(\sqrt{2} = \frac{m}{n}\right) \Rightarrow \left(2 = \frac{m^2}{n^2}\right) \Leftrightarrow (2n^2 = m^2) \Rightarrow (m^2\ is\ even) \Leftrightarrow$

$(m\ is\ even) \Leftrightarrow (m = 2m', m' \in N)$. Then $\left(2n^2 = 4m'^2\right) \Leftrightarrow \left(n^2 = 2m'^2\right)$, i.e.

$(n^2\ is\ even) \Leftrightarrow (n\ is\ even) \Leftrightarrow (n = 2n', n' \in N\ )$. Consequently $\frac{m}{n} = \frac{2m'}{2n'} = \frac{m'}{n'}$

contradicting the hypothesis that m/n was uncancelled fraction. So, $\sqrt{2}$ is not rational number.

Proof by Syllogism: $(p \to q) \wedge (q \to r) \Rightarrow p \to r$

Example. Let

p = "Mary is from Boston", q ="Mary is from Massachusetts",

r = "Mary is from USA".

Then Syllogism $(p \to q) \wedge (q \to r) \Rightarrow p \to r$ for this example will be

"If Mary is from Boston then Mary is from Massachusetts.

If Mary is from Massachusetts then Mary is from USA.

Conclusion: If Mary is from Boston then Mary is from USA"

1.4.3. Necessary and sufficient conditions.

Definition. In any theorem of the form $p \Rightarrow q$ the proposition p is called *sufficient condition* for the proposition q and the proposition q is called *necessary condition* for the proposition p. So, the theorem $p \Rightarrow q$ instead of "$if\ p\ then\ q$" can be also read as "$p\ is\ sufficient\ for\ q$", or "$q\ is\ necessary\ for\ p$".

Example 1. Let's consider the same example from above. The theorem

"*If Mary is from Boston then Mary is from Massachusetts*" can be also read as

"$(Mary\ is\ from\ Boston)$ is $sufficient\ for$ $(Mary\ is\ from\ Massachusetts)$"
or
"$(Mary\ is\ from\ Massachusetts)$ is $necessary\ for$ $(Mary\ is\ from\ Boston)$".

You must clearly distinguish the difference between *necessity* and *sufficiency*.

Sufficiency of "*Mary is from Boston*" guarantees "*Mary is from Massachusetts*".

Necessity of "*Mary is from Massachusetts*" doesn't guarantee that "*Mary is from Boston*" (for example Mary can be from Lowell). It means only "*if Mary is not from Massachusetts then Mary is not from Boston*". Really as we know $p \to q \Leftrightarrow \overline{q} \to \overline{p}$, but $p \to q \not\Leftrightarrow q \to p$.

1.4.4. Theorems of Logical Equivalency.

Definition.

Theorems of the form $p \Leftrightarrow q$ are called
Theorems of the *Logical Equivalency*.

Theorems $p \Leftrightarrow q$ are read "*p if and only if q*" and are written sometimes shortly "*p iff q*".

To prove such theorems is to prove that the biconditional proposition $p \leftrightarrow q$ is a tautology.

As we know yet $p \Leftrightarrow q$ if and only if $p \Rightarrow q$ and $q \Rightarrow p$.

Therefore we can replace the proof of the theorem $p \Leftrightarrow q$ by the proofs of two theorems $p \Rightarrow q$ and $q \Rightarrow p$. It's clear that in this case
p is necessary and sufficient condition for q
and *q is necessary and sufficient condition for p*
and the theorem $p \Leftrightarrow q$ instead of "*p if and only if q*" can be read also "*p is necessary and sufficient for q*".

Example. The proposition "Two squares are congruent if and only if their areas are equal" is a theorem. To prove this theorem is equivalent to prove two theorems

"If two squares are congruent then their areas are equal" and
"If the areas of two squares are equal then they are congruent".

1.4.5. Definitions.

Consider the definition of the square:

"A rectangle is called a square if all its sides are equal". This definition means in addition that there is no any square with unequal sides, i.e. a complete definition of the square should be an equivalency as follows:

"A rectangle is called a square if and only if all its sides are equal".

In fact, all definitions contain hidden convention about logical equivalency; and instead of "if and only if" we use its symbol $\overset{def}{\Leftrightarrow}$ (or $\overset{def}{=}$).

For example: "A rectangle is a square $\overset{def}{\Leftrightarrow}$ all its sides are equal" (*)

But most of all we miss the mark "def" in the definitions and we write briefly $\Leftrightarrow$

(or $=$) without ambiguity.

With the definition given above for the square it is easy to prove the theorem:

"A rectangle is a square $\Leftrightarrow$ its diagonals are perpendicular to each other" (**)

We can interchange the signs $\overset{def}{\Leftrightarrow}$ and $\Leftrightarrow$ in (*) and (**) respectively, and then

(**) becomes a definition which should be given before and (*) becomes a theorem which should be proved after.

1.4.6. Valid and Invalid Arguments. True Conclusion. Modus Ponens. Modus Tollens.

We consider here below only the most used methods of proof: *direct*, *by conrapositive*, and *by contradiction*.

Definition. An ***argument*** is a conditional proposition $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$, where propositions $p_1, p_2, \ldots, p_n$ are hypotheses and proposition q is a conclusion. An argument is called *valid* if this conditional is a theorem (tautology),

i.e. if $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$, otherwise it is called *invalid*.

To show an argument is invalid, it is enough to give one example of truth values for the propositions such that $p_1 \wedge p_2 \wedge \ldots \wedge p_n = t$, and $q = f$.

This is called a *counterexample* to the argument. The simplest example is $p \to q$.

Here below we consider the most used valid arguments.

Note. From now and further instead of write proposition p *is true* or p *is false* we say and we write briefly p or $\overline{p}$.

Modus Ponens: $(p \to q) \wedge p \Rightarrow q$.

Most of the simple theorems are given in the form of

Modus Ponens: $(p \to q) \wedge p \Rightarrow q$.

Using the truth table we proved this tautology in the example of 1.3.2.

But it's easy to prove it directly by definition of conjunction and conditional.

In fact, $(p \to q) \wedge p$ is true if and only if $p \to q$ *and* p are both true. But if p is true in the true conditional $p \to q$ then q must be true.

QED (quod erat demonstrandum – which was to be shown).

Example. Consider once again an example from above:

$p =$"Mary is from Boston", $q =$"Mary is from Massachusetts".

Then Modus Ponens $(p \to q) \wedge p \Rightarrow q$ for this example will be

"If Mary is from Boston then Mary is from Massachusetts. Mary is from Boston.

Conclusion: Mary is from Massachusetts"

Note. However, even if an argument is valid it is not sufficient to expect its conclusion to be true.

Example. Argument

"*If* 5 *is divisible by* 3, *then* 10 *is divisible by* 3. 5 *is divisible by* 3.

So, 10 *is divisible by* 3".

This argument is valid because it has the same type $(p \to q) \wedge p \Rightarrow q$.

But its conclusion "10 *is divisible by* 3" is false, since its hypothesis "5 *is divisible by* 3" is false.

So to get a true conclusion q is to check that:

1. **argument $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$ is valid,**
2. **all hypotheses $p_1, p_2, \ldots, p_n$ of the argument are true.**

Modus Tollens: $(p \to q) \wedge \overline{q} \Rightarrow \overline{p}$.

If we replace in the Modus Ponens: $(p \to q) \wedge p \Rightarrow q$ everywhere p by $\overline{q}$ and q by $\overline{p}$ we obviously obtain a new tautology $(\overline{q} \to \overline{p}) \wedge \overline{q} \Rightarrow \overline{p}$. Now remembering Contrapositive Law $p \to q \Leftrightarrow \overline{q} \to \overline{p}$ and doing equivalent replacement we obtain definitive form of the proof by Modus Tollens: $(p \to q) \wedge \overline{q} \Rightarrow \overline{p}$.

So, if $p \to q$ is true, and we assume negation $\overline{q}$ (i.e. q is false) we obtain negation $\overline{p}$ (i.e. p is false). QED.

Example. Consider the same example from above:

$p =$"Mary is from Boston", $q =$"Mary is from Massachusetts".

Modus Tollens $(p \to q) \wedge \overline{q} \Rightarrow \overline{p}$ for this example will be

"If Mary is from Boston then Mary is from Massachusetts. Mary is not from Massachusetts. Conclusion: Mary is not from Boston".

Modus Syllogism $p \wedge (p \to q) \wedge (q \to r) \Rightarrow r$.

If proving a theorem by syllogism we want to guarantee a true conclusion r, we must modify the argument: $p \wedge (p \to q) \wedge (q \to r) \Rightarrow r$

Exercise. Prove it not by creating truth table but using Associative Law of conjunction and Modus Ponens!

Appropriate example in this case will be as follows: "Mary is from Boston.

If Mary is from Boston then Mary is from Massachusetts.

If Mary is from Massachusetts then Mary is from USA.

Conclusion: Mary is from USA".

Exercises 1.4.

1. Find the converse, inverse and contrapositive propositions of the following theorems and verify which of them a theorem is too:

a) "If a quadrangle is a rhombus, then its diagonals are mutually perpendicular",

b) "If a parallelogram is a rhombus, then its diagonals are mutually perpendicular".

c) "If each summand of a sum is even, then the sum is even",

c) "If a triangle is right, then the squared length of the hypotenuse is equal to the sum of the squared lengths of its legs.

2. Using contrapositive law prove the theorem:

a) "If mn is odd number, then m and n are odd",

b) "If $a^2 + b^2 \neq 0$ then $a \neq 0$ or $b \neq 0$.

3. Parents said to their children: "If we go to visit on weekends, then you go to the movies".

The children started to discuss it:

John: "If we go to the movies, then the parents go to visit",

Peter: "If the parents do not go to visit, then we do not go to the movies".

Mary: "If we do not go to the movies, then the parents do not go to visit".

a) Who of the children said the proposition logically equivalent to the parent's proposition?

b) Who of the children said the same proposition but in other words?

4. Find the necessary and sufficient conditions in the following theorems:

a) "If the two rectangles are congruent then their areas are equal",

b) "The two squares are congruent if and only if their areas are equal"

What is fundamental difference between the theorems a) and b) ?
Could you change the wording of the theorem a) that it has the form "if and only if"?

5. There are two expressions:
a) "A rectangle is a square iff all its sides are equal",
b) "A rectangle is a square iff its diagonals are mutually perpendicular".
Taking each of them alternately for the definition of a square prove the second as a theorem.

6. Prove that the following example is the argument of Modus Ponens and determine p and q.
"If a rectangle ABCD is a square then its diagonals are perpendicular to each other. A rectangle ABCD is a square. Conclusion: diagonals of ABCD are perpendicular to each other".

7. Prove that the argument $((p \to q) \wedge q) \to p$ is **invalid**.
Examples:
a) "*If* 4 *is even, then* 8 *is even.* 8 *is even*. Consequently, 4 is even".
Conclusion "4 is even" is true.
b) *If* $a = b$, *then* $|a| = |b|$. $|a| = |b|$. Consequently, $a = b$"
Conclusion "$a = b$" is false if, for example $a = -b$.
So, the conclusion in an invalid argument with true hypotheses may be true or false.

8. Prove that the argument $((p \to q) \wedge \overline{p}) \to \overline{q}$ is **invalid**.
Example: "If mathematics is interesting, then it is useful. Mathematics is not interesting".
Could you affirm that conclusion "Mathematics is not useful" is true? Answer: No!
Arguments of the exercises 7 and 8 are the most widespread logical errors.

1.5. Propositional Forms.

1.5.1. Operations on Propositional Forms. Logical Equivalence and Implications.

Definition.

There exist statements depending on variable and becoming propositions if we substitute instead of the variable its value from a domain given. We call them **Propositional Forms** and denote $p(x), x \in D$.

An *example* of $p(x)$ is the value of x for which $p(x)$ is true.
A *counterexample* is a value of x for which $p(x)$ is false.

Example 1. Let x an integer number, then
$p(x)$ = "*number x is odd*" is the propositional form.
For example $p(3) = t,\ p(4) = f$.
Value $x = 3$ is *an example*, value $x = 4$ is *a counterexample*.

Example 2. Let $p(x) =$"*x is American*", $x \in$ *all Humanity*.

There are propositional forms depending on two or more variables.
Example 3. Let x, y real numbers and $p(x,y) = (x < y)$.
Then for example $p(1,2) = t,\ p(2,1) = f$.

Example 4. Let $p(x,y) =$ "*x is the wife of y*", $x \in$ *Set of all wives*, $y \in$ *Set of all husbands*.

Note. Arity. Arity of propositional form is determined by the number of arguments involved in it, e.g. propositional forms in examples 1 and 2 are **unary**, and propositional forms in examples 3 and 4 are **binary**. This concept can be naturally extended till ***n*-ary** forms. The order of arguments does matter (ex. 3).

Nullary propositional form is an elementary proposition.

Definition. Two propositional forms $p(x)$ and $q(x)$, $x \in D$ are called ***logically equivqlent*** if for all $x \in D$ their truth values coincide and we denote it $p(x) \Leftrightarrow q(x)$.

Example 5. Let $x \in R$, $x - 1 = 0 \Leftrightarrow x = \sin\frac{\pi}{2}$;
Both sides are true when $x = 1$ and are false for all other values of x.

All operations on propositions are applied in natural way to propositional forms.

Examples. Let $x \in R$
1) Negation
a) If $p(x) = (2 + x = 5)$ then $\overline{p}(x) = (2 + x \neq 5)$.
$p(x)$ *is true for* $x = 3$ *and is false for all* $x \neq 3$,
$\overline{p}(x)$ *is true for all* $x \neq 3$ *and false for* $x = 3$.
b) $\overline{(x > 2)} \Leftrightarrow (x \leq 2)$.
2) Conjunction
a) $(|x| < 3) \Leftrightarrow (-3 < x < 3) \Leftrightarrow (x > -3) \wedge (x < 3)$,
b) $\begin{cases} x + y = 2 \\ x - y = 0 \end{cases} \Leftrightarrow ((x + y) = 2) \wedge ((x - y) = 0) \Leftrightarrow (x = 1) \wedge (y = 1)$
c) $(x^2 + y^2 = 0) \Leftrightarrow (x = 0) \wedge (y = 0)$
3) Disjunction

a) $(|x| > 3) \Leftrightarrow (x < -3) \vee (x > 3)$

b) $x(x-1) = 0 \Leftrightarrow (x = 0) \vee (x = 1)$

4) Implication

$(x < 1) \rightarrow (x^2 < 1)$ is false for $x \leq -1$ and is true for all other x (prove it!).

5) Equivalency

a) $(x = 1) \leftrightarrow (x^2 = 1)$ is false for $x = -1$ and is true for all other x (prove it!).

b) $(x = 1) \leftrightarrow (y = 2)$ is true for $x = 1$ and $y = 2$ or $x \neq 1$ and $y \neq 2$; and is false if $x = 1$ and $y \neq 2$ or $x \neq 1$ and $y = 2$.

Definition. We say that the propositional form $p(x),\ x \in D$ **logically implies** the propositional form $q(x),\ x \in D$ and we write $p(x) \Rightarrow q(x)$ if for all $x \in D$

the implication $p(x) \rightarrow q(x)$ is true.

Example. Let $x \in R$, $(x\ is\ divisible\ by\ 4) \Rightarrow (x\ is\ divisible\ by\ 2)$.

Example. Prove that

"$m\ is\ divisible\ by\ 6\ if\ and\ only\ if\ m\ is\ divisible\ by\ 2\ and\ m\ is\ divisible\ by\ 3$"

or briefly: $(6|m) \Leftrightarrow (2|m) \wedge (3|m)$.

Proof:

$\Rightarrow$. Really: $(6|m) \Rightarrow (m = 6n) \Rightarrow (m = 2(3n)) \Rightarrow (2|m)$.

By analogy $(6|m) \Rightarrow (m = 6n) \Rightarrow (m = 3(2n)) \Rightarrow (3|m)$.

So $(6|m) \Rightarrow (2|m) \wedge (3|m)$

$\Leftarrow$. $(2|m) \wedge (3|m) \Rightarrow (m = 2a) \wedge (m = 3(2a)) \Rightarrow (m = 6a) \Rightarrow (6|m)$

So, $(6|m) \Leftrightarrow (2|m) \wedge (3|m)$. QED.

Note 1. Identically true and identically false propositional forms.

If a propositional form $p(x), x \in D$ is true or false for all $x \in D$ it is called *identically true* or respectively *identically false* propositional form.

For example, the propositional forms $x^2 \geq 0$ and $x^2 < 0$ are respectively the identically true and identically false propositional forms on R.

Note 2. The rule of using of the chain of $\Leftrightarrow$ and $\Rightarrow$ in the equivalent transformations of compound propositions is also true for propositional forms:

a) $(p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_n) \Rightarrow (p_1 \Rightarrow p_n)$,

b) $(p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n) \Rightarrow (p_1 \Leftrightarrow p_n)$,

c) If $p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_n \Rightarrow p_1$ then $p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n$.

Obviously, if in a mixed chain of $\Rightarrow$ and $\Leftrightarrow$ there is at least one implication $\Rightarrow$ the total relation between the first and the last member of the chain will be implication $p_1 \Rightarrow p_n$. We use these rules to solve the equations.

Examples:

1) Solving an equation and using of chain of $\Rightarrow$ we can get by accident "extra roots", for example $(x = 1) \Rightarrow (x^2 = 1) \Leftrightarrow (\sqrt{x^2} = \pm 1) \Leftrightarrow (x = \pm 1)$,

so $(x = 1) \Rightarrow (x = \pm 1)$. The root $x = -1$ is the "extra root" and is not a solution of the initial equation $(x = 1)$.

2) When we divide the equation by an expression containing the unknown, we can lose a root of the equation. In this case $p_1 \not\Rightarrow p_n$, for example

$((x-1)(x-2) = 0) \not\Rightarrow (x - 1 = 0)$ (why?). So we lost here the root $x = 2$.

The correct solution is $(x-1)(x-2) = 0 \Leftrightarrow (x = 1) \veebar (x = 2)$

3) If a chain contain only $(\Leftrightarrow)$ then $p_1 \Leftrightarrow p_n$, for example

$(7x - 2 = 2x + 3) \Leftrightarrow (7x - 2x = 3 + 2) \Leftrightarrow (5x = 5) \Leftrightarrow (x = 1)$.

So, $(7x - 2 = 2x + 3) \Leftrightarrow (x = 1)$.

Note 3. ***Convention about extension** of propositional forms.*

Usually domain of definition D of a propositional form is clear from the context (see examples 1-4 above). But we can extend it without any problems by defining $p(x) = f$ for all x for which $p(x)$ makes no sense.

For example, $p(x) = (\frac{1}{x-1} = 1)$ is defined for all $x \in R$ excluding $x = 1$.

We define $p(1) = f$. So, now domain of definition is R and $p(x) = t$ for $x = 2$ and $p(x) = f$ for all other $x \in R$.

Example. Let $x \in R$; $x = x \not\Leftrightarrow \frac{x^2}{x} = x$ because for $x = 0$ the left side is true and the right side (according to the convention above) is false. But if we restrict the domain of definition $x \in R^* = R - \{0\}$ then $x = x \Leftrightarrow \frac{x^2}{x} = x$ on R^*.

Exercise. Let $x \in R$. Prove that $(xlogx = 0) \not\Leftrightarrow (x = 0) \vee (log(x) = 0)$.

1.5.2. Quantifications.

A propositional form can become a proposition not only by substitution of the variable its value from the domain of definition, but also by means of the word expressions such that "for all" and "there exists" putting before the propositional form.

Definition. ***Universal quantification.***

If $p(x), x \in D$ is a propositional form, the proposition "for all $x \in D$ $p(x)$ is true" called the *universal quantification* of $p(x)$ and denoted briefly $\forall x \in D, p(x)$. This is a proposition, and is either *true* or *false*.

The symbol $\forall$ is called an ***universal quantifier***.

Example.

a) $p(x) = "x + 2 = 5", x \in N$.

The proposition $\forall\, x \in N, x + 2 = 5$ is false.

b) $q(x) = "(x + 1)^2 = x^2 + 2x + 1", x \in R$

The proposition $\forall\, x \in R,\ (x + 1)^2 = x^2 + 2x + 1$ is true.

Definition. ***Existential quantification.***

If $p(x), x \in D$ is a propositional form, the proposition "there exists an $x \in D$ such that $p(x)$ is true" is called the ***existential quantification*** of $p(x)$, and denoted briefly $\exists x \in D,\ p(x)$. This is a proposition, and is either *true* or *false*. The symbol $\exists$ is called an ***existential quantifier***.

Example.

a) $p(x) = "x + 2 = 5", x \in N$.

The proposition $\exists x \in N,\ x + 2 = 5$ is true. It is $x = 3$.

b) $q(x) = "2x = 5", x \in N$

$\exists x \in N,\ 2x = 5$ is false (attention $x \in N$!).

But if we consider R as a domain for x then this proposition is true (why?).

Note 1. The letter x in the expressions $\forall x \in D, p(x)$ and $\exists x \in D, p(x)$ is not real variable, i.e. you cannot substitute instead of x its value from D. Variable x in these expressions is called "dummy variable" because you can replace it by any letter. That is $\forall x \in D, p(x) \Leftrightarrow \forall y \in D, p(y)$, also $\exists x \in D, p(x) \Leftrightarrow \exists y \in D, p(y)$.

Note 2. Defined above logical equivalence and implication for propositional forms can be written now in the form of quantifications:

$p(x) \Leftrightarrow q(x) \overset{def}{\Leftrightarrow} \forall x \in D, p(x) \leftrightarrow q(x)$ (is true),

$p(x) \Rightarrow q(x) \overset{def}{\Leftrightarrow} \forall x \in D, p(x) \rightarrow q(x)$ (is true).

Usually we omit the expression "is true" in brackets.

So, in the equivalent transformations of propositional forms the expression "for all x " always implicitly present even if we do not write it, like in the exercises below.

Note 3. The universal quantification $\forall$ can be read also as "for any", "for every", "for each" etc.

The existential quantification $\exists$ can be read also as "for some, "there exists at least one" etc.

Definition. ***Existential quantifier*** $\exists'$. If in the expression $\exists x$ we want to emphasize the uniqueness of the x, we use *existential quantifier* $\exists'$ which is read "**there exists only one**".

Example-exercise. What is the difference between two propositions: $\exists x \in Z,\ x^2 = 4$ and $\exists' x \in N,\ x^2 = 4$?

Quantification negation rule. It is obviously that the negation of the proposition "for all $x \in D$ $p(x)$ is true" is "there exists an $x \in D$ such that $p(x)$ is false",

i.e. $\overline{\forall x \in D, p(x)} \Leftrightarrow \exists x \in D,\ \bar{p}(x)$. By analogy: $\overline{\exists x \in D, p(x)} \Leftrightarrow \forall x \in D, \bar{p}(x)$.

So, we have got a rule:

In order to negate quantification one must change quantifier to other type ($\forall$ to $\exists$ and $\exists$ to $\forall$) and negate propositional form.

Examples.

a) Let L and L' two straight lines on same plane. Parallelism of L and L' is the proposition $\forall x \in L,\ x \notin L'$, where x is a point of the plane. In other words L and L' have no common points. Negation of the parallelism, i. e. intersection or coincidence is: $\exists x \in L,\ x \in L'$.

b) If an equation $f(x) = 0$ has a real root we write it $\exists x \in R,\ f(x) = 0$. Negation of this proposition is $\forall x \in R,\ f(x) \neq 0$.

Note 3. If in the expression $\exists x$ we want to emphasize the uniqueness of the x, we use *existential quantifier* $\exists'$ which is read "there exists only one" or "there exists a unique".

Example-exercise. What is the difference between two propositions:
$\exists x \in Z,\ x^2 = 4$ and $\exists' x \in N,\ x^2 = 4$?

Note 4.

Application of quantifiers to one of the two variables (for example to x) of the propositional form $p(x,y)$ keeps the second variable free and creates a new propositional form of one variable y: $\forall x \in D, p(x,y)$ or $\exists x \in D, p(x,y)$.

Application of a quantifier to the second variable creates an elementary proposition. The quantifiers of the same type you can swap:

$\forall y \in D, \forall x \in D, p(x,y) \Leftrightarrow \forall x \in D, \forall y \in D, p(x,y)$ or

$\exists y \in D, \exists x \in D, p(x,y) \Leftrightarrow \exists x \in D, \exists y \in D, p(x,y)$, but you cannot apply it generally for the quantifiers of the different type. For example,

$\forall x \in R, \exists y \in R, (x+y=0)$ is true, but $\exists y \in R, \forall x \in R, (x+y=0)$ is false.

However, for any form p we can write

$\exists y \in D, \forall x \in D, p(x,y) \Rightarrow \exists x \in D, \forall y \in D, p(x,y)$.

Note 5. The Rule of the Negation of quantifiers can be naturally extended to the propositional forms with any number of variables. For example,

$$\overline{\forall x \in D, \exists y \in D, p(x,y)} \Leftrightarrow \overline{\forall x \in D, \big(\exists y \in D, p(x,y)\big)} \Leftrightarrow$$
$$\Leftrightarrow \exists x \in D, \overline{\big(\exists y \in D, p(x,y)\big)} \Leftrightarrow \exists x \in D, \forall y \in D, \bar{p}(x,y).$$

Exercises 1.5.

1. Investigate whether the following propositional forms can have false value:
a) "If x is the brother of y, then x and y are the relatives";
b) "If x is the brother of y, then y is the brother of x";
c) "x is the son of y if and only if y is the father of x";
d) "x is older than y if and only if y is younger than x"

2. Let $x, y \in R$. Prove that
a) $(x=1) \Rightarrow (x^2=1)$, but $(x^2=1) \nRightarrow (x=1)$, so $(x=1) \not\Leftrightarrow (x^2=1)$,
b) $(x \neq 1) \nRightarrow (x^2 \neq 1)$, but $(x^2 \neq 1) \Rightarrow (x \neq 1)$, so $(x \neq 1) \not\Leftrightarrow (x^2 \neq 1)$,
c) $(x \geq 1) \Rightarrow (x^2 \geq 1)$, but $(x^2 \geq 1) \nRightarrow (x \geq 1)$, so $(x \geq 1) \not\Leftrightarrow (x^2 \geq 1)$,
e) $(x < 1) \nRightarrow (x^2 < 1)$, but $(x^2 < 1) \Rightarrow (x < 1)$, so $(x < 1) \not\Leftrightarrow (x^2 < 1)$,
f) $(|x| < 0) \Leftrightarrow (\sin x = 2)$; $(x^2 \geq 0) \Leftrightarrow (\sin^2 x + \cos^2 x = 1)$,
g) $(x=1) \Leftrightarrow (x^3=1)$; $(x \neq 1) \Leftrightarrow (x^3 \neq 1)$,
h) $(x \leq 1) \Leftrightarrow (x^3 \leq 1)$; $(x > 1) \Leftrightarrow (x^3 > 1)$,

i) $xy = 0 \Leftrightarrow (x=0) \vee (y=0)$; $xy \neq 0 \Leftrightarrow (x \neq 0) \wedge (y \neq 0)$,
j) $x^2 + y^2 = 0 \Leftrightarrow (x=0) \wedge (y=0)$,
k) $x/y = 0 \Leftrightarrow (x=0) \wedge (y \neq 0)$,
l) $|x| = 1 \Leftrightarrow (x=1) \vee (x=-1)$,
m) $|x| < 1 \Leftrightarrow (x > -1) \wedge (x < 1)$,
n) $|x| > 1 \Leftrightarrow (x < -1) \vee (x > 1)$,
o) $|x| > 2 \Leftrightarrow x^2 > 4$; $|x| \leq 2 \Leftrightarrow x^2 \leq 4$,
p) $x^2 - 3x + 2 = 0 \Leftrightarrow (x=1) \vee (x=2)$.

3. Let $x \in R$. Find the truth values of the following propositions:
a) $\forall x,\ (x^2-1) = (x-1)(x+1)$;
b) $\forall x,\ |x| > 0$;
c) $\forall x,\ x^2 + x + 1 > 0$;
d) $\exists x,\ |x| \leq 0$;
e) $\exists x,\ |x| + 2 = 3$;
d) $\exists x,\ x^2 + x + 1 = 0$;
e) $\exists x,\ x^2 > x$.

4. Let $x \in R$. Write the following propositions using quantifiers:
a) There exists a number x such that $x + 3 = 5$;
b) At least one number x is a root of the equation $x^2 + bx + c = 0$;
d) Whatever the number x, $x \cdot 0 = 0$;
e) Any number is positive or negative or is equal to zero.

5. Verify that the two following propositions are both true:
$a)\ \exists x,\ \cos x \neq 2$; $b)\ \forall x,\ \cos x \neq 2$.
Which of them gives us more information about x?

6. Let $x, y \in R$. Find the truth values of the following propositions:
a) $\forall x\ \forall y\ \ (x-y)^2 = x^2 - 2xy + y^2$,
b) $\forall x\ \exists y\ \ xy = 1$,
c) $\exists x\ \exists y\ \ xy = 1$,
d) $\exists x\ \forall y\ \ xy = 0$,

7. Change by negation the true proposition to the false one and the false proposition to the true one:
a) $\forall x \in R,\ x^2 \geq 0$; b) $\exists x \in R, |x| < 0$.

8. Determine whether the following propositional forms
$x^2 = 1$ and $(x+\sqrt{2})(x-0.5)(x-1)(x+1)$ are equivalent on:
$a)\ R,\ b)\ Q,\ c)\ Z,\ d)\ N$. Answers: a) no, b) no, c) yes, d) yes.

9. Find the sets of truth for the following propositional forms:
$a)\ \frac{x-2}{3} - \frac{x+5}{4} = -1,\ \ b)\ 5(4-x) < 3(x+12)$. Answers: $a)\ \{11\},\ b)\ ]-2,+\infty[$

10. Let $x \in R$. Determine which of the following two propositional forms implies the second:
$a)\ |x| < 5$ and $x^2 - 3x + 2 = 0,\ b)\ x^2 = -1$ and $x^4 = 16$.

11. Find the positive values of δ such that $|x-2| < \delta \Rightarrow |x^2 - 4| < 5$. Answer: $\delta \in]0,1[$

Chapter 2

SETS

2.1. Basic notions of Sets.

2.1.1. Set representation.

The notions of a set, of an element, of the relation "to be an element of a set" are basic and indefinable and we used it in fact in previous chapters.

Sometimes instead of "set" we can use as synonyms "collection", "domain", family, etc. and instead of "element" we use " member", " object", "point", etc.

Here below are some examples of the sets well-known from the school:

1. Set of natural numbers:
   $N = \{1, 2, \dots, n, \dots\}$
2. Set of integers:
   $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$,
3. Set of rational numbers:
   $Q = \{\frac{m}{n},\ m \in \mathbb{Z},\ n \in \mathbb{N}\}$,
4. Set of real numbers:
   $R = (-\infty, +\infty)$,
5. Set of prime numbers:
   $Pr = \{2, 3, 5, 7, \dots\}$,
6. Set of composite numbers:
   $Cmpst = \{4, 6, 8, 9, \dots\}$
7. Set of even numbers
   $Ev = \{2n | n \in Z\}$,
8. Set of odd numbers
   $Od = \{2n + 1 | n \in Z\}$.

We express that "a is element of the set A" or "a belong to A" by writing $a \in A$.

Negation of this relation is denoted by definition $a \notin A \overset{def}{\Leftrightarrow} \overline{a \in A}$,
e.g. $-5 \in \mathbb{Z},\ -5 \notin \mathbb{N}$.

Examples:

a) A **singleton** $\{a\}$ is the set containing only one element a.

Note that $a \in \{a\}$ is true, but $\{a\} \in a$ is false.
If $b = \{1,2\}$, (i.e. contain two elements 1 and 2), then the singleton $\{b\} = \{\{1,2\}\}$ still contain only element $\{1,2\} \in \{b\}$.

b) The set $S = \{a, \{a\}, \{a, b\}\}$ contains three elements: $a, \{a\}, \{a, b\}$.
The first element $a \in S$. The second element $\{a\} \in S$ is the singleton containing one element a, and the third element $\{a, b\} \in S$ is the set containing two elements a and b.

A set can be represented in one of the three ways:

1. **Explicit listing**: by listing (or enumeration) its elements between braces, e.g. $A = \{a, b, c, d, e\}$.
2. **Implicit listing**: by listing enough of its elements to find a pattern and by using three dots $(\dots)$, as we did e.g. for the sets $\mathbb{N}$ and $\mathbb{Z}$ above.
3. **By the Property of its elements.**
   Let $p(x)$ is a propositional form defined on a domain D.
   Then the collection of $x \in D$ such that $p(x)$ is true create a set denoted $A = \{x \in D \mid p(x)\ is\ true\}$, called the set of $x \in D$ with the **property $p(x)$**.
   Usually we omit the expression $is\ true$ in the braces. Vertical bar "|" (or sometimes colon ":") replaces the expression "such that".
   The set A is called also "set of truth" of the propositional form p in D.
   Another notation of the set A is $A = \{x \in D \mid p(x)\} = \{x | x \in D \wedge p(X)\}$,
4. **By the function.** Let $y = f(x)$ a function with $x \in A$ and $f(x) \in B$.
   Then $\{f(x) | x \in A\}$ is the set of all $f(x) \in B$ where x runs through all values

   in A, e.g. the set of even numbers $Ev = \{2n | n \in Z\}$.

Examples:

1) $\{x \in N | -2 < x < 2\} = \{1\}$,
2) $\{x \in Z | 1 \le x \le 5\} = \{1, 2, 3, 4, 5\}$,
3) $\{x \in R | x^2 - x = 0\} = \{0,1\}$.
4) $Pr = \{x \in N | x\ is\ a\ prime\ number\} =$
   $= \{x \in N \mid x > 1 \wedge "has\ no\ divisors\ other\ than\ 1\ and\ itself"\} =$
5) $Cmpst = \{x \in N | x\ has\ a\ divisor\ other\ than\ 1\ and\ itself\}$.
6) $Od = \{x \in Z | x\ is\ not\ divisible\ by\ 2\}$,
7) $Ev = \{x \in Z |\ x\ is\ divisible\ by\ 2\}$,
8) $N_0 = \{0, 1, 2, \dots\}$
9) $Z^* = \{x \in Z | x \ne 0\}$
10) $Q^* = \{x \in Q | x \ne 0\}$,

11) $R^{*} = \{x \in R | x \neq 0\}$,
12) $Z_{+} = \{x \in Z | x \geq 0\}$, $Z_{-} = \{x \in Z | x \leq 0\}$,
13) $Q_{+} = \{x \in Q | x \geq 0\}$, $Q_{-} = \{x \in Q | x \leq 0\}$,
14) $R_{+} = \{x \in R | x \geq 0\}$, $R_{-} = \{x \in R | x \leq 0\}$,
15) $Z_{+}^{*} = \{x \in Z | x > 0\}$, $Z_{-}^{*} = \{x \in Z | x < 0\}$,
16) $Q_{+}^{*} = \{x \in Q | x > 0\}$, $Q_{-}^{*} = \{x \in Q | x < 0\}$
17) $R_{+}^{*} = \{x \in R | x > 0\}$, $R_{-}^{*} = \{x \in R | x < 0\}$,
18) $[a, b] = \{x \in R | a \leq x \leq b\}$, $(a, b) = \{x \in R | a < x < b\}$,
$[a, b) = \{x \in R | a \leq x < b\}$, $(a, b] = \{x \in R | a < x \leq b\}$.

2.1.2. Equality (coincidence) of sets.

Definition. Two sets A and B are called *equal* if and only if they consist of the same elements:

$$(A = B) \overset{def}{\Leftrightarrow} (x \in A \Leftrightarrow x \in B)$$

Note 1. Order of elements in sets. According the definition of equality of sets the order of the listed elements does not matter, for example, $\{a, b\} = \{b, a\}$, i.e. the order of listed elements does not matter. But there exist "ordered sets" in which the order of the elements is important. They will be considered later in the Cartesian products and Combinatorics and they will be denoted in parentheses. For example, (a, b) and (b, a) are different 2-tuples.

Note 2. Repetitions of elements. Multisets. According the definition of equality of sets the repetition of the elements in sets does not matter, for example, $\{a, b, c\} = \{a, b, b, c\} = \{a, b, c, c\}$. So, in future we assume that the sets are considered in their simplest form, i.e. **without repletion.**

However, in mathematics there is a notion of "**multisets**" where repetition of elements more than once is allowed and does matter. The notion of multiset is a generalization of the notion of set and will be considered in Combinatorics.

In order to distinguish sets and multisets the square brackets are used for the last. The number of times an element belongs to the multiset is called its multiplicity. The total number of elements in a multiset, including the repeated is called cardinality of the multiset. For example, in the multiset $[a, a, a, b, b, c]$ the multiplicities of the elements a, b, c are respectively 3, 2, 1 and the cardinality of the multiset is 6. **In multisets, as in sets the order of elements does not matter.**

Examples. The collection of the dividers of the number 360 is the multiset $[2, 2, 2, 3, 3, 5]$, because $360 = 2^{3} \cdot 3^{2} \cdot 5$. The collection of the roots of the equation $x^{3} - 4x^{2} + 5x - 2 = 0$ is the multiset $[1, 1, 2]$.

Note 3. Obviously, $p(x) \Leftrightarrow q(x)$ if and only if $\{x | p(x)\} = \{x | q(x)\}$, i.e. equivalent "properties" defined the same set.

Example. Since "Triangle is equilateral" $\Leftrightarrow$ "Triangle has three equal angles".

So, the set of all equilateral triangles is equal to the set of all triangles with three equal angles.

2.1.3. Empty set.

Definition. A set containing no elements is called *empty set* and denoted by $\emptyset$.

Empty set can be defined by any contradiction.

Example. $\emptyset = \{x | x \neq x\}$;
or, once again, $\emptyset = \{x \in N | -1 < x < 1\}$.

2.1.4. Inclusion. Subset.

Definition. Inclusion. Subset. A set A is called subset of the set B if and only if each element of A is an element of B. It is denoted by $A \subseteq B$ and read A *is included in* B (*or* B *includes* A: $B \supseteq A$). So,

$$A \subseteq B \overset{def}{\Leftrightarrow} (x \in A \Rightarrow x \in B).$$

If $A \subseteq B$ and $A \neq B$ and $A \neq \emptyset$, then A is called a ***proper subset*** of B and we write $A \subset B$.

Note. By definition: $A \subseteq B \Leftrightarrow B \supseteq A$.

Examples.

a) $N \subset N_{0} \subset Z \subset Q \subset R$,
b) "The set of all equilateral triangles" $\subseteq$ "The set of all isosceles gles" $\subseteq$ "The set of all triangles",
c) "The set of all squares" $\subseteq$ "The set of all rectangles" $\subseteq$ "The set of all parallelograms",
d) "The set of all squares" $\subseteq$ "The set of all rhombuses" $\subseteq$ "The set of all parallelograms",

2.1.5. The Power Set.

Definition. *Power set* of a set S denoted $\mathcal{P}(S)$ is the set of all subsets of S. So,

$$\mathcal{P}(S) = \{A | A \subseteq S\}.$$

Obviously,

a) $A \subseteq S \Leftrightarrow A \in \mathcal{P}(S)$,

b) $a \in S \Leftrightarrow \{a\} \in \mathcal{P}(S)$,

c) $A \in \mathcal{P}(S), \emptyset \in \mathcal{P}(S)$.

Examples:

$S = \emptyset,\ \mathcal{P}(S) = \{\emptyset\}$,

$S = \{a\},\ \mathcal{P}(S) = \{\emptyset, \{a\}\}$,

$S = \{a, b\},\ \mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,

$S = \{a, b, c\},\ \mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

2. 1.6. Cardinality of finite sets. Finite and infinite sets.

Definition. The set S is called finite if it contains a finite number of elements, otherwise it is called infinite. The number of elements in finite set S is called *cardinality* of the set S and denoted by $Card\ S$ (or $|S|$).

Theorem. Cardinality of the Power Set of a finite set.
If S is a finite set, then

$$Card\ S = 2^{Card\ S}.$$

The **Proof** will be given in *Combinatorics*. It also can be done by using The Principle of Mathematical Induction as an exercise.

Example. Consider the examples just above:

0. $S = \emptyset,\ \mathcal{P}(S) = \{\emptyset\},\ Card\ \mathcal{P}(S) = 2^0 = 1$,

1. $S = \{a\},\ \mathcal{P}(S) = \{\emptyset, \{a\}\},\ Card\ \mathcal{P}(S) = 2^1 = 2$,

2. $S = \{a, b\},\ \mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\},\ Card\ \mathcal{P}(S) = 2^2 = 4$,

3. $S = \{a, b, c\}$,

$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\},\ Card\ \mathcal{P}(S) = 2^3 = 8$, etc.

Exercises 2.1.

1. List the elements of the following sets:

a) $\{x \in N | x^2 < 50\}$, b) $\{x \in Z | x^2 < 50\}$, c) $\{x \in Q | x^2 - 1 = 2\}$, d) $\{x \in R_+ | x^2 - 1 = 2\}$,
e) $\{x \in N | x^4 = 16\}$, f) $\{x \in Z | x^4 = 16\}$

2. Find all the subsets of the set $S = \{a, b, c, e\}$, i.e. create the power $\mathcal{P}(S)$.

3. Prove that *Inclusion* $\subseteq$ is
a) *reflexive*: $\forall A,\ A \subseteq A$;
b) *transitive*: $(A \subseteq B) \wedge (B \subseteq C) \Rightarrow (A \subseteq C)$,
c) *not symmetric*: $(A \subseteq B) \not\Rightarrow (B \subseteq A)$,
d) $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$,
e) $\forall A,\ \emptyset \subseteq A$, in particular $\emptyset \subseteq \emptyset$.

4. Prove that
a) If $A \subseteq B$, then $A \cap B = A$, e.g. $R_+ \cap R = R_+$,
b) If $A \subseteq B$, then $A \cup B = B$, e.g. $R_+ \cup R = R$

5. Prove that $A - B = \emptyset \Leftrightarrow A \subseteq B$

6. Prove the Arguments:
a) $(a \in A) \wedge (A \subseteq B) \Rightarrow a \in B$
b) $(A \subseteq B) \wedge (a \notin B) \Rightarrow a \notin A$

2.2. Operations on Sets.

2.2.1. Intersection. Disjoint sets.

Definition. Intersection.
The intersection of two sets A and B is the set denoted by $A \cap B$ consisting of the elements belonging to A and to B simultaneously. So,

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

Examples:

a) $\{1, 2, 3, 4\} \cap \{3, 4, 5, 6\} = \{3, 4\}$,

b) $N \cap N_0 = \{0\}$,

c) $Z_+ \cap Z_- = \{0\},\ \ Q_+ \cap Q_- = \{0\},\ \ R_+ \cap R_- = \{0\}$,

d) $Z_+ \cap Z^* = Z_+^*,\ \ Z_- \cap Z^* = Z_-^*$ etc.,

e) "Set of all rectangles" $\cap$ "Set of all rhombuses"= "Set of all squares"

f) $[a,b] \cap [b,c] = \{b\}$,
g) if $a < b < c < d$ then $[a,c] \cap [b,d] = [b,c]$.

Definition. Disjoint Sets. Two sets A and B are called *disjoint* if $A \cap B = \emptyset$.

Examples:
a) R_+^* and R_-^* are disjoint,
b) $[a,b)$ and $(b,c]$ are disjoint,
c) "Set of all triangles" and "Set of all rectangles" are disjoint.
d) $P$and $Cmpst$ are disjoint.

2.2.2. Union.

Definition. Union.
Union of two sets A and B is the set denoted by $A \cup B$ consisting of the elements belonging to A or to B. So,

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

Examples:
a) $\{1,2,3,4\} \cup \{3,4,5,6\} = \{1,2,3,4,5,6\}$,
b) $\{0\} \cup N = N_0$
c) $\{0\} \cup R^* = R$,
d) $R_- \cup R_+ = R$,.
e) "Set of all even numbers" $\cup$ "Set of all odd numbers" $= Z$.

2.2.3. Symmetric difference.

Definition. Symmetric difference.
Symmetric difference of two sets A and B is the set denoted by $A \Delta B$ containing the elements which belong to either A or B. So,

$$A \Delta B = \{x | x \in A \veebar B\}.$$

Examples:
a) $\{1,2,3,4\} \Delta \{3,4,5,6\} = \{1,2,5,6\}$,
b) $A = [0,2),\ \ B = [1,+\infty),\ \ A\Delta B = [0,1) \cup [2,+\infty)$.
c) "Set of all rectangles" Δ "set of all rhombuses" =

= "Set of all rectangles with unequal adjacent sides" $\cup$ "Set of all rhombuses with angles other than right angles"

2.2.4. Difference. Compliment.

Definition. Difference.
The difference $A \setminus B$ of sets A and B is the set consist of the elements of A which do not belong to B. So,

$$A \setminus B = \{x \in A | x \notin B\}$$

Note. The difference of sets $A \setminus B$ is denoted sometimes as $A - B$.

Examples:
a) $\{1,2,3,4\} \setminus \{3,4,5,6\} = \{1,2\}$,
b) $[0,2] \setminus [1,\infty) = [0,1)$,
c) $N \setminus N_0 = \{0\}$,
d) $R \setminus \{0\} = R^*,\ \ R_+ \setminus \{0\} = R_+^*,\ \ R \setminus R_+ = R_-^*$,
e) $N \setminus \{1\} = P \cup Cmpst$
f) "Set of all rectangles"\"Set of all rhombuses"=
= "Set of all rectangles with unequal adjacent sides"

Definition. Compliment. In particular, if $A \supseteq B$ then the difference is denoted by

$$C_A B = A \setminus B$$

and called *compliment* of B in A.

Examples:
a) $C_{\{1,2,3,4\}}\{3,4\} = \{1,2\}$,
b) $C_Z N = Z_-$,
c) $C_R R_+ = R_-^*$,
d) "Compliment of the set of all squares in the set of rectangles"=
= "Set of all rectangles with unequal adjacent sides",

2.2.5. Universe.

We always assume that all sets of discourse are the subsets of some large (as large as we like, but fixed) set called the ***Universe*** (or universal set), and denoted by $\boldsymbol{U}$. For example, in plane geometry - it is the set of all points of the plane, which subsets are the points, lines, figures. In elementary arithmetic – it is the set of all rational numbers. When we talk about propositional forms $p(x)$ we can assume that their domains of definition are the Universe U, if not we can extend these domains till U assigning $p(x) = f$ for those x for which $p(x)$ does not make sense. Therefore, in the expressions $A = \{x \in U \mid p(x) \text{ is true}\}$ to determine subsets A by the property $p(x)$ we omit common U and we write briefly $A = \{x \mid p(x)\}$.

Definition. Compliments in the Universe.
For the compliment of set A in the universe U we use special symbol

$$\bar{A} = C_U A = U \setminus A$$

Exercise. Prove that $\bar{\emptyset} = U,\ \bar{U} = \emptyset$.

2.2.6. Laws of Set Operations.

The laws of the sets operations remind appropriate laws of the propositions

So, for any sets A, B, C:

I. Double Compliment Law (Analog of Double Negation Law).

$$\bar{\bar{A}} = A.$$

II. Compliments Law (Analog of the Law of Contradiction).

$$A \cap \bar{A} = \emptyset$$

III. Compliments Law (Analog of the Law of Excluded Third).

$$A \cup \bar{A} = U$$

IV. Commutative Laws

of intersection $A \cap B = B \cap A$

of union $A \cup B = B \cup A$

V. Associative Laws

of intersection $(A \cap B) \cap C = A \cap (B \cap C)$

of union $(A \cup B) \cup C = A \cup (B \cup C)$

VI. Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

VII. Idempotent Laws

$$A \cap A = A$$
$$A \cup A = A$$

VIII. Bound Laws: $A \cup U = U,\ A \cap \emptyset = \emptyset,$

Identity Laws: $A \cup \emptyset = A,\ A \cap U = A,$

IX. Absorption Laws

$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$

X. De Morgan's Laws

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

XI. Analog of Contrapositive Law

$$A \subseteq B \Leftrightarrow \bar{B} \subseteq \bar{A}$$

XII. Analog of Syllogistic Law

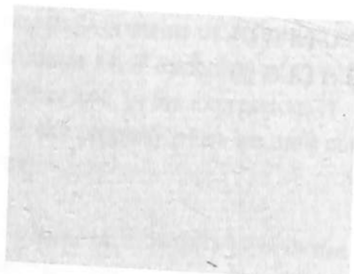
$$(A \subseteq B) \wedge (B \subseteq C) \Rightarrow (A \subseteq C)$$

XIII. The principle of extensionality (Analog of $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$).

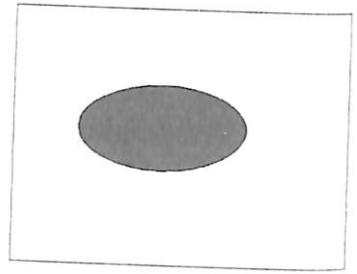
$$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

2.2.7. Venn Diagrams.

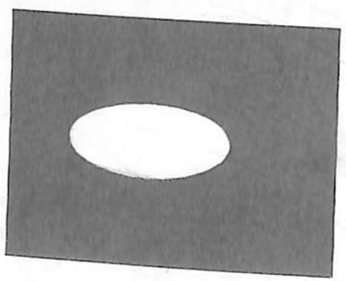
Venn diagrams are pictorial representations of sets as enclosed areas in the plane. The universal set U is represented as rectangle and colored regions represent sets A, B, C... as subsets of the Universe. Venn diagrams are very useful to get an idea when you prove equality of sets, but they do not replace certainly a serious mathematical proof.



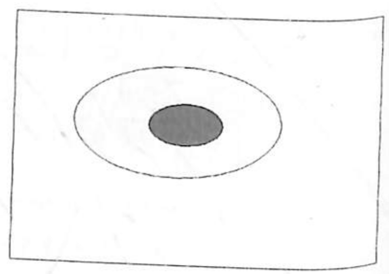
Universe U



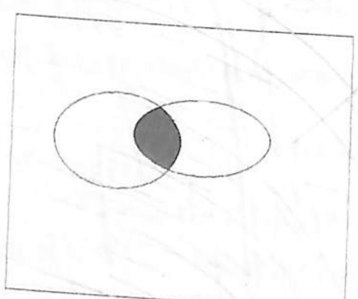
Set A



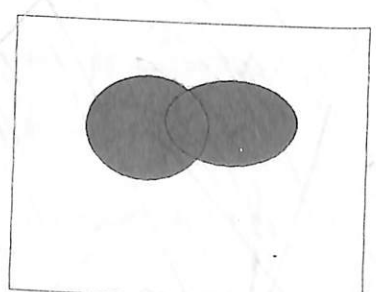
Complement $\overline{A} = U - A$



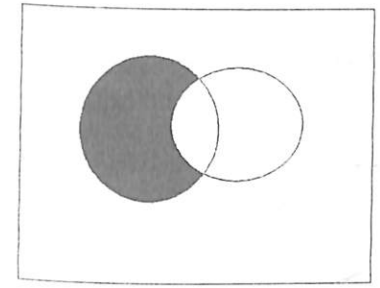
Inclusion $A \subseteq B$



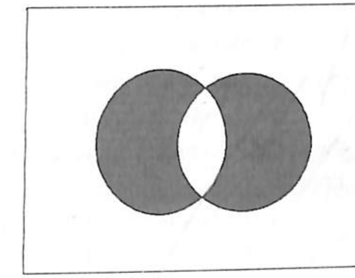
Intersection $A \cap B$



Union $A \cup B$



Difference $A \setminus B$



Symmetric difference $A \triangle B$

2.2.8. Inclusion-exclusion principle.

In this section for the cardinality of the set A, for brevity, we will use $|A| = Card\ A$.

Theorem. Let $A_1, A_2, \dots, A_n$ be finite sets. Then the cardinality of the union of all these sets is:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n| -$$
$$-|A_1 \cap A_2| - |A_1 \cap A_3| - \dots - |A_{n-1} \cap A_n| +$$
$$+|A_1 \cap A_2 \cap A_3| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n| + (-1)^{n-1}|A_1 \cap A_2 \cap \dots \cap A_n|$$

The **proof** in general case can be done by Mathematical Induction and you can make it after the study.

We verify the theorem for two sets A and B:

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

Really, the set $A \cup B$ consist of elements of A and of those elements of B that are not contained in A. Then adding $|A| + |B|$ we count **two** times the common elements of A and B, i.e. the elements of $A \cap B$.

Example. The total number of students in an American university is 1000. The number of students who speak Spanish as a foreign language is 600, who speak French as a foreign language is 500. The number of students who speak both foreign languages is 200. Find the number of students:

1. who speak a foreign language,
2. who speak only Spanish,

3. who speak only French,

4. who speak exactly one foreign language

5. who do not speak any foreign language.

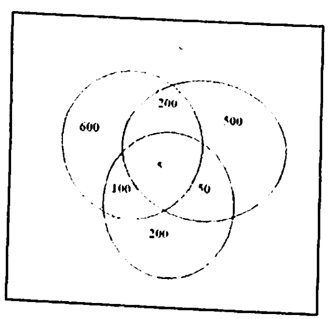
Solution. Denote the set of all university students as the *universe* U, A – the set of the students who speak Spanish, B – the set of the students who speak French.

1. The number of students who speak a foreign language is $600 + 500 - 200 = 900$,
2. The number of students who speak only Spanish is $600 - 200 = 400$,
3. The number of students who speak only French is $500 - 200 = 300$,
4. The number of students who speak only one foreign language is $400 + 300 = 700$,
5. The number of students who do not speak any foreign language is $1000 - 900 = 100$.

Exercise. Deduce a formula from the theorem for $n = 3$

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

and solve the problem above including Chinese as foreign language and taking into account additional information: $|U| = 1000$,
$|Sp| = 600, |Fr| = 500, |Ch| = 200,$
$|Sp \cap Fr| = 200, |Sp \cap Ch| = 100, |Fr \cap Ch| = 50, \ |Sp \cap Fr \cap Ch| = 5.$
Use the following drawing.



Solution.

1. Speaking a foreign language $600 + 500 + 200 - 200 - 100 - 50 + 5 = 955$,

2. Speaking only Spanish $600 - 200 - 100 + 5 = 305$,

3. who speak only French $500 - 200 - 50 + 5 = 255$,

3′. who speak only Chinese $200 - 100 - 50 + 5 = 55$,

4. who speak exactly one foreign language $305 + 255 + 55 = 615$,

5. who do not speak any foreign language $1000 - 955 = 5$.

6. Find the total number of students who speak exactly two foreign languages and then separately: Spanish and French, Spanish and Chinese, French and Chinese.

Exercises 2.2.

1. Prove that:

a) $A\Delta B = \emptyset \Leftrightarrow A = B$.

b) $A\Delta B = A \cup B \Leftrightarrow A \cap B = \emptyset$

c) $A\Delta B = \{x | (x \in A \cup B) \wedge (x \notin A \cap B)\}$

d) $A\Delta B = (A - B) \cup (B - A)$

2. Prove that the sets:
$A - B, B - A, A \cap B$ are pair wise disjoint
and $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$

3. Prove that:

a) $A\Delta B = (A \cup B) - (A \cap B)$,

b) $A\Delta B = (A - B) \cup (B - A)$.

4. Prove that: $C_A B = \emptyset \Leftrightarrow A = B$

5. Prove that: $A \cup B = (A \cap B) \cup (A\Delta B)$

6. Prove all the Sets operations laws.

7. Let $U_p = \{x \in U | p(x)\}$ the set of truth of the propositional form $p(x)$ defined on universe U. Prove that

a) $U_{\bar{p}} = \bar{U}_p$,

b) $U_{p\wedge q} = U_p \cap U_q$,

c) $U_{p\vee q} = U_p \cup U_q$,

d) $U_{p\underline{\vee} q} = U_p \Delta U_q$,

e) $p \Leftrightarrow q$ if and only if $U_p = U_q$,

f) $p \Rightarrow q$ if and only if $U_p \subseteq U_q$.

8) Let $U = \{a, b, c, d, e\}$, $A = \{a, b, c\}$, $B = \{c, d, e\}$. Find
$A \cap B$, $A \cup B$, $A\Delta B$, $A - B$, $B - A$, $\bar{A}$, $\bar{B}$,

2.3. Family of Sets. Partition of a Set into Classes.

2.3.1. Family of sets. Intersection and Union.

Definition. Family of sets.

Let I be a set and for every $i \in I$ we assign a set A_i. The set I is called *set of indexes*. and the set $\{A_i\}_{i\in I} = \{A_i | i \in I\}$ is called *family of sets*.

Definition. Intersection of the family of sets.

We define intersection of the family of all $\{A_i\}_{i\in I}$ as the set of elements belonging to all A_i simultaneously and denote it by

$$\bigcap_{i\in I} A_i = \{x | \forall i \in I \;\; x \in A_i\}.$$

In particular, if $I = N$ we denote intersection by

$$\bigcap_{i=1}^{\infty} A_i$$

Exercises:

1) Prove that:

a) if $i \in N$, $A_i = [0, \frac{1}{i}]$ then $\bigcap_{i=1}^{\infty} A_i = \{0\}$,

b) if $i \in N$, $A_i = (0, \frac{1}{i})$ then $\bigcap_{i=1}^{\infty} A_i = \emptyset$.

2) if $i \in N_0$, $A_i = \{x \in N | x \le i\}$ then find $\bigcap_{i=1}^{\infty} A_i$

Definition. Union of the family of sets.

We define union of the family of all $\{A_i\}_{i\in I}$ as the set of elements belonging to at least one of A_i and denote it by

$$\bigcup_{i\in I} A_i = \{x | \exists i \in I \;\; x \in A_i\}.$$

In particular, if $I = N$ we denote it by

$$\bigcup_{i=1}^{\infty} A_i$$

Exercise.

1) Prove that

if $i \in N$, $A_i = \left(0, \frac{i}{i+1}\right)$ then $\bigcup_{i\in N} A_i = (0, 1)$.

2) if $i \in N_0$, $A_i = \{x \in N | x \le i\}$ then find $\bigcup_{i=1}^{\infty} A_i$

2.3.2. Partition of a set into classes.

Definition. Partition of a set into classes.

Let A a set. The family of the nonempty sets $\{A_i\}_{i\in I}$ is a *partition* of the set A if:

1. sets A_i are pair wise disjoint: $\forall i, j \in I \;\; i \ne j \Rightarrow A_i \cap A_j = \emptyset$,
2. $\bigcup_{i\in I} A_i = A$.

The sets $A_i, i \in I$ are called *classes*. Obviously that each element of A belongs to one and only one class A_i.

Examples:

1. Trivial partitions of a set A are:
   a) family $\{A\}$ containing only one element – the set A itself,
   b) family consist of all singleton subsets $\{a\}$ of A,
2. Family of the half open intervals with integer ends $\{A_i = [i, i+1) | i \in Z\}$ form the partition of R.
3. The set of all elementary propositions is naturally partitioned into two classes: class of true and class of false propositions.
4. The set of all propositional forms defined on the same domain D is partitioned into the classes logically equivalent to each other propositional form.
5. Let A the set of all points of a plane. Then the family of all straight lines parallel to one straight line form a partition of A.
6. Let A and B the sets of even and odd numbers respectively. Then they form a partition of Z.
7. Three sets $R_-^{*}, \{0\}, R_+^{*}$ form a partition of R.
8. Three sets $Pr, \{1\}, Cmpst$ form a partition of N.
9. The set Ev and the set Od form a partition of N.
10. The group of boys and the group of girls form a partition of the class.

Counterexample. Power set $\mathcal{P}(S)$ is not partition of S. Why?

Exercises 2.3.

1. If $i \in R$, $A_i : y = ix$ is a straight line on a plane, find $\bigcup_{i\in R} A_i$, $\bigcap_{i\in R} A_i$.
2. If $i \in R$, $A_i : y = x + i$ is a straight line on a plane, prove that they form a partition of this plane.
3. Prove the partitions of all 10 examples above.
4. Prove that De Morgan's Laws are generalized to the intersection and union of any family of sets:

$$\overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \bar{A_i}, \quad \overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \bar{A_i}$$

2.4. Cartesian Product.

2.4.1. Cartesian Product.

Definition. Let A, B be two sets. Cartesian product of A and B is the set of all **ordered pairs** (x, y), where $x \in A, y \in B$, denoted by $A \times B$. So,

$$\boldsymbol{A \times B = \{(x, y) | x \in A \wedge y \in B\}}.$$

The elements of the set $A \times B$, i.e. the pairs $(x, y) \in A \times B$ are called sometimes **points** of the set $A \times B$, and the elements x and y are called **coordinates** of the point (x, y) or the first and the second **projections** of the point (x, y) and we write respectively $x = \mathbf{Pr}_1(x, y)$ and $y = \mathbf{Pr}_2(x, y)$.

By definition: $(x, y) = (x', y') \Leftrightarrow (x = x') \wedge (y = y')$.

When we say "ordered pair" (x, y) we mean that x is necessarily from the first set A and y is necessarily from the second set B. So, generally $A \times B \neq B \times A$. Obviously, $A \times B = B \times A \Leftrightarrow A = B$. In this case we denote Cartesian product by $A^2 = A \times A$ and we call it **Cartesian square** of A. Ordering of the pair (x, y) in this case means that generally $(x, y) \neq (y, x)$ and $(x, y) = (y, x) \Leftrightarrow (x = y)$!

In other words x and y are in the pair (x, y) are **naturally ordered by their index numbers** (i.e. by their place) in the pair but not compared with each other, i.e. x is the first and y is the second. In particular, in the ordered pair (x, x) the first and the second elements are equal each other, however we consider the pair (x, x) as the ordered pair, where there is the first element and there is the second element.

General notion of ordered sets will be given in the next chapter.

As you can see for the ordered sets the **parentheses** are used instead of **braces.**

Definition. Diagonal of the Cartesian Square.

Diagonal of A^2 is the subset

$$D = \{(x, y) \in A^2 | y = x\} = \{(x, x) | x \in A\}.$$

Examples:

1. **Chess board.** Let $A = \{a, b, c, d, e, f, g, h\}$ and $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Then Cartesian product $A \times B$ is a "chess board":

$$A \times B = \{(a, 1), (a, 2), \dots, (a, 8), (b, 1), (b, 2), \dots, (h, 8)\}$$

containing $8 \times 8 = 64$ points (elements).

2. **Rational numbers.** For the purpose of constructing complete theory of rational numbers based on the integers we will use the ordered pairs $(m, n) \in Z \times Z^*$ instead of the usual $\frac{m}{n}$. We call them rational numbers (fractions), m, n numerator and denominator respectively. We will build this theory step by step. Cartesian product $Z \times Z^* = \{(m, n) | m \in Z, n \in Z^*\}$ after the definition of "quotient set", addition and multiplication will be called set of rational numbers Q.

3. **Arithmetic plan R^2 and physical plan P.**

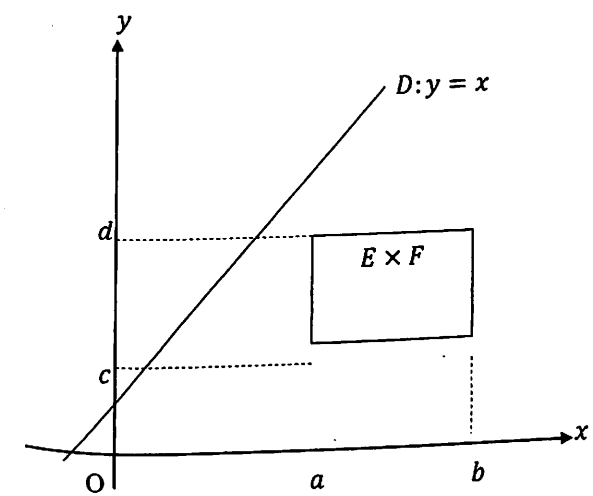
Consider Cartesian square $R^2 = \{(x, y) | x, y \in R\}$. This set R^2 is very convenient to describe the real **physical plan P** (see note below). If we build rectangular (Cartesian) coordinate system on the surface P, then we can establish one-to-one correspondence between each point of $M \in P$ with coordinates x, y and each element $(x, y) \in R^2$ also called point. For this reason R^2 is called **arithmetic plan R^2**. Diagonal of R^2 is the set

$D = \{(x, x) | x \in R\}$, i.e. is the straight line $y = x$.

Let $E = [a, b] \subset R$, $F = [c, d] \subset R$ two intervals in R.

Their Cartesian product is rectangle in R^2:

$E \times F = \{(x, y) \in R^2 | x \in [a, b] \wedge y \in [c, d]\} \subset R^2$



2.4.2. Cartesian Product of Several Sets.

Definition. Cartesian product of two sets is naturally generalized to an arbitrary number of factors: $A \times B \times C = \{(x, y, z) | x \in A \wedge y \in B \wedge z \in C\}$ which elements (x, y, z) are called **ordered triples or 3-tuples**, etc.

$S_1 \times S_2 \times ... \times S_n = \{(x_1, x_2, ..., x_n) | x_1 \in S_1, x_2 \in S_2, ..., x_n \in S_n\}$ which elements $(x_1, x_2, ..., x_n)$ are called ordered n-tuples.

In particular, Cartesian exponents are: $S^3 = \{(x, y, z) | x, y, z \in S\}$, ...,
$S^n = \{(x_1, x_2, ..., x_n) | x_i \in S \; \forall i = 1, 2, ..., n\}$.

Notes:

1. When the n-tuple $(x_1, x_2, ..., x_n)$ is called "ordered" that means that the coordinates $x_1, x_2, ..., x_n$ are ordered only by their indexes (or their places) in the n-tuple. The order or any other relation between $x_1, x_2, ..., x_n$ as the elements of the set S is not assumed.

2. Memorize that n-tuple $(x_1, x_2, ..., x_n) \in S^n$ is not a set $\{x_1, x_2, ..., x_n\}$ in general sense. So, the repetition of the elements (coordinates) in the writing of the n-tuple $(x_1, x_2, ..., x_n) \in S^n$ is allowed, e.g. $(a, a, ..., a) \in$ Diagonal of S^n.

2.4.3. Cardinality of the Cartesian product of finite sets.

Theorem. If $S_1, S_2, ..., S_m$ are finite sets and, then

$$\boldsymbol{card\,(S_1 \times S_2 \times ... \times S_m) = card\, S_1 \cdot card\, S_2 \cdot ... \cdot card\, S_m}$$

In particular,

$$\boldsymbol{card\, S^m = (card\, S)^m}$$

Proof. Let $card\, S_1 = n_1,\; card S_2 = n_2, ..., card S_k = n_m$. Then $card\,(S_1 \times S_2)$ is the number of all pairs (x_1, x_2), where x_1 can be replaced by any of n_1 elements of S_1 and x_2 can be replaced by any of n_2 elements of S_2. So, the number of all pairs (x_1, x_2) is $n_1 \cdot n_2$. The number of all 3-tuples (x_1, x_2, x_3) is equal to number of all pairs (x_1, x_2) equal to $n_1 \cdot n_2$ multiplied by n_3 because x_3 can be replaced by any of n_3 elements of S_3. So, $card\,(S_1 \times S_2 \times S_3) = n_1 \cdot n_2 \cdot n_3$.

A similar reasoning till k complete the proof.

In particular, if $S_1 = S_2 = \cdots = S_m = S$, and $card\, S = n$, then $card\, S^m = n^m$.

Examples:

1. The number of all cells on the chessboard is $8 \cdot 8 = 64$.

2. The number of all three-digit numbers is $9 \cdot 10 \cdot 10 = 900$, because 1st digit belongs to $\{1, 2, ..., 9\}$, 2nd and 3rd digits belong to $\{0, 1, 2, ..., 9\}$.

Digression. A set $\boldsymbol{R^n}$, where R is the set of real numbers, is called $\boldsymbol{n-}$ ***dimensional arithmetical spase.***

Arithmetic space $\boldsymbol{R^3}$ can be is associated with surrounding us real physical space $\boldsymbol{S}$ by building in it a single rectangular coordinate system with a fixed length scale and by establishing one-to-one correspondence between each point of $M \in S$ with coordinates x, y, z and each 3-tuples $(x, y, z) \in R^3$ also called point.

Analogously, arithmetic plan $\boldsymbol{R^2}$ can be is associated with a real **physical plan** $\boldsymbol{P}$ like a surface of paper, surface of blackboard, the earth's surface, sea surface etc. by building on them (x, y) coordinate system.

Spaces $\boldsymbol{R^n}$ with $n > 3$ do not have a simple geometric or physical interpretation, except the space-time R^4 (but with another metric).

A real opportunity to describe physical space $\boldsymbol{S}$ by means of $\boldsymbol{R^3}$ or physical plane $\boldsymbol{P}$ by means of $\boldsymbol{R^2}$ with so, that the Pythagorean theorem would be true on the whole space (or plane) is far from obvious and cannot be verified by logical inference. It is a problem not of mathematics but of physics and moreover, of experimental physics.

Consider an example of hypothetical universe which is a huge spherical surface.

2- dimensional intelligent creatures living in this universe and exploring at the first time of their development "small" areas of the surrounding world, they would not feel the curvature of the surface and would take it for flat. The theorems of the Euclidian plan geometry would be true with the high precision on these small areas and these creatures could apply Cartesian coordinate system. But exploring larger and larger areas they would find significant deviations from the theorems of the Euclidian plan geometry and would find the impossibility of a building of a single Cartesian coordinate system in such universe. Analogously surrounding us 3- dimensional physical space S can posses a "curvature" which does not allow us to identify it in its entirety with R^3. Such doubts may also arise when we use Euclidian geometry in the microcosm of atomic dimensions. However, modern experimental knowledge allows us to assert that the Euclidian geometry is applicable in large scales till 10^{28} cm, except the regions near massive stars, and in small scales till 10^{-13}cm.

We must also add, that the fact that the dimension of our space (not counting the time) is equal to 3 is also experimental fact, despite its obviousness. There are physical theories where the dimension of the physical space is greater than 3, but it manifests itself in scales smaller than 10^{-25} cm.

The reader can find a serious discussion of problems associated with the dimension, curvature of physical space in the special literature on cosmology, general relativity, gravitation and atomic physics.

Exercises 2.4.

Let A, B, C, D be sets. Then

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
3. $(A \times B) \cap C = (A \times C) \cap (B \times C)$
4. $(A \times B) \cup C = (A \times C) \cup (B \times C)$
5. $A \times \emptyset = \emptyset \times A = \emptyset$.

Chapter 3.
RELATIONS and FUNCTIONS

3.1. Relations. Graphs of Relations.

3.1.1. Binary Relations. Graphs.

Definitions. Binary Relations.

Let X and Y two sets. Any propositional form ρ defined on $X \times Y$ is called ***binary relation* from X to Y** (or sometimes on $X \times Y$).

If a pair $(x, y) \in X \times Y$ is such that $\rho(x, y)$ is true, i.e. belongs to the set of truth of ρ, then we say that x *is* related to y by ρ and we write $x\rho y$. Otherwise we say that x is not related to y by ρ and we write $\overline{x\rho y}$.

Expression "from X to Y" is often denoted by $X \to Y$.

Definition. Graph of Relation.

Let ρ be a relation from X to Y. Set of truth of the propositional form ρ in $X \times Y$ is called graph of ρ and denoted by $\boldsymbol{Gr(\rho)}$:

$$Gr(\rho) = \{(x, y) \in X \times Y \mid x\rho y\}.$$

Obviously, $Gr(\rho) \subseteq X \times Y$.

Definition. Relations "on".

If $X = Y$, then we say that the relation ρ is defined on X (instead of "on $X \times X$")

or between the elements of X. And we can say that the elements $x, y \in X$ are related (or not) by ρ instead of "x is related (or not) to y by ρ".

Examples:

1. Let X and Y be two sets. **Trivial** relations from X to Y:
   a) **full** relation $\boldsymbol{\rho_f}$: $\rho_f(x, y) = t \ \forall (x, y) \in X \times Y, Gr\,(\rho_f) = X \times Y$.
   b) **empty** relation $\boldsymbol{\rho_e}$: $\rho_e(x, y) = f \ \forall (x, y) \in X \times Y, Gr\,(\rho_e) = \emptyset$.
2. Let $X = \{2, 3\}, Y = \{4, 5, 6, 7, 8, 9\}, x\rho y \Leftrightarrow x|y \ \ (x \ devide \ y)$.
   Then $Gr\,(\rho) = \{(2, 4), (2, 6), (2, 8), (3, 6), (3, 9)\}$.
3. Let M be a set of all men and W be a set of all women, then the relation $m\rho w \Leftrightarrow$ "***m is the husband of w***" is the binary relation from M to W.

$Gr\ (\rho)$ is the set of all married pairs (where the first is husband and the second is wife), is the subset in $M \times W$.

4. If we consider the relation "$\boldsymbol{m\ is\ married\ to\ w}$" from M to W we will get the same graph (so, the same relation). But, if we consider this new relation on the more convenient set H $(H = M \cup W - Humanity)$ (in other words from H to H), then the graph of this new relation (in H^2) will be different. Why?

5. **Relation "to be friend of"** is the binary relation on the set of all people H.

The graph of this relation is the subset of all pairs of people in H^2 having at least one friend.

6. **Relation "to be parent of"** is the binary relation on the set of all people H.

The graph of this relation is the subset of pairs in H^2 which the first element is the parent (mother or father) and the second element is his (her) child (son or daughter).

7. **Relation of Identity I** (equality, coincidence). Let X be a set.
Relation $xIy \Leftrightarrow x = y$ is called relation of identity on X.
Graph of this relation is the diagonal of X^2: $\{(x, y) \in X^2 | y = x\}$.

8. Let L be the set of all straight lines on the same plan.
a) **Parallelism** $a \parallel b$ is a relation on L.
b) **Perpendicularity** $a \perp b$ is a relation on L.

9. Let Tr be the set of all triangles on the same plan.
Then the relation of the **similarity of triangles** $(\sim)$ is the binary relation on Tr.

10. **Logical implication and logical equivalency** are two binary relations on the set of all propositions.

11. **Logical implication and logical equivalency** are two binary relations on the set of all propositional forms defined on the same domain.

12. **Belonging.** Let S be any set and $\mathcal{P}(S)$ its power. Then the relation $a \in A$, (where a is an element of S, and A is a subset in S, i.e. is an element of $\mathcal{P}(S)$), is the binary relation on $S \times \mathcal{P}(S)$.

13. **Inclusion and equality.** Let S be any set and $\mathcal{P}(S)$ its power. Then the relations $A \subseteq B$ and $A = B$ between the subsets in S are the binary relations on the $\mathcal{P}(S)$.

14. Let $X = Y = R$ and $x\rho y \Leftrightarrow x^2 + y^2 \leq 1$.
Then $Gr(\rho)$ is the disk in R^2 of radius 1 centered at the origin O.

Note. As we see any relation ρ between the sets X and Y as a propositional form is completely determined by its set of truth on $X \times Y$, i.e. by its graph $Gr(\rho)$. So,

$$x\rho y \Leftrightarrow (x, y) \in Gr(\rho).$$

Example.
Let
$X = \{2, 3\},\ Y = \{4, 5, 6, 7, 8, 9,\},\ Gr\ (\rho) = \{(2, 4), (2, 6), (2, 8), (3, 6), (3, 9)\}$
Relation ρ is completely defined by its graph. But if we look at it attentively, we can find its propositional form's expression $x\rho y \Leftrightarrow x|y$ (x $devide$ y), example 2 considered above.

3.1.2. Domain. Range. Codomain. Equality of relations.

Definition. Let ρ be a binary relation from X to Y.
The ***domain*** of ρ is the set denoted and defined as follows
$$D(\rho) = \{x \in X | \exists y \in Y | x\rho y\} = \{x \in X | (x, y) \in Gr(\rho)\} \subseteq X,$$
The ***range*** of ρ is the set denoted and defined as follows
$$Ran(\rho) = \{y \in Y | \exists x \in X | x\rho y\} = \{y \in Y | (x, y) \in Gr(\rho)\} \subseteq Y.$$
The ***codomain*** of ρ is the set Y and denoted by $Cod(\rho) = Y$.

Examples: (see examples 1-13 above)
1. $D(\rho_f) = X,\ Ran(\rho_f) = Y,\ D(\rho_e) = Ran(\rho_e) = \emptyset.$
2. $D(\rho) = X,\ Ran(\rho) = \{4, 6, 8, 9\} \subset Y.$
3. $D(\rho) = \{set\ of\ all\ married\ men\} \subset M,$
$Ran(\rho) = \{set\ of\ all\ married\ women\} \subset W,$
4. $D(\rho) = Ran(\rho) = \{set\ of\ all\ married\ people\} \subset H,$
5. $D(\rho) = Ran(\rho) = \{set\ of\ all\ people\ having\ at\ least\ one\ friend\} \subset H,$
6. $D(\rho) = \{set\ of\ all\ men\ having\ at\ least\ one\ child\},$
$Ran(\rho) = \{set\ of\ all\ people\ having\ the\ father\},$
7. $D(I) = Ran(I) = X,$
8. $D(\parallel) = Ran(\parallel) = L,\ D(\perp) = Ran(\perp) = L,$
9. $D(\sim) = Ran(\sim) = Tr,$
11. $D(\in) = S,\ Ran(\in) = \mathcal{P}(S) - \emptyset,$
12. $D(\subseteq) = Ran(\subseteq) = \mathcal{P}(S),\ D(=) = Ran(=) = \mathcal{P}(S),$
13. $D(\rho) = Ran(\rho) = [-1, 1].$

Note. For any point $(x, y) \in X \times Y$ we defined yet its projections:

$x = \Pr_1(x,y)$ and $y = \Pr_2(x,y)$.

Then for any subset $A \subseteq X \times Y$ we define projections of A as follows:

$\Pr_1(A) = \{x | x = \Pr_1(x,y) \wedge (x,y) \in A\} \subseteq X$,

$\Pr_2(A) = \{y | y = \Pr_2(x,y) \wedge (x,y) \in A\} \subseteq Y$.

Exercise. Prove that $D(\rho) = \Pr_1(Gr(\rho))$, $Ran(\rho) = \Pr_2(Gr(\rho))$.

Notation: A set X with a binary relation ρ is often represented briefly by the pair (X, ρ). So, e.g. $(N, \leq)$ means the set of the natural numbers with the relation of non-strict inequality.

Definition. Equality of Relations.

Equality of two binary relations ρ *from* X *to* Y and ρ_1 *from* X_1 *to* Y_1 is defined as follows:

$\rho = \rho_1 \Leftrightarrow X = X_1 \wedge Y = Y_1 \wedge \forall(x,y) \in X \times Y \; x\rho y \Leftrightarrow x\rho_1 y$.

Obviously, $\rho = \rho_1 \Leftrightarrow Gr(\rho) = Gr(\rho_1)$.

Note. n-ary relations between the sets $X_1, X_2, \dots, X_n$ (order of indexes does matter!) are naturally defined. Any propositional form $\rho(x_1, x_2, \dots x_n)$, defined on $X_1 \times X_2 \times \dots \times X_n$ is called ***n − ary relation.***

Example. The sum of natural numbers $x + y = z$ generates a **ternary** $(n = 3)$ relation $\rho(x,y,z)$: $x + y = z$ defined on $N \times N \times N$.

For example, $\rho(1,2,3)$ is true, but $\rho(2,3,4)$ is false.

3.1.3. Composition of Relations. Inverse Relation.

Definitions. Composition. Let X, Y, Z be sets and ρ_1, ρ_2 be binary relations *from* X *to* Y and *from* Y *to* Z respectively. Composition of ρ_1 and ρ_2 is the binary relation *from* X *to* Z, denoted by $\rho_2 \circ \rho_1$ and defined as follows:

$$\boldsymbol{x(\rho_2 \circ \rho_1)z \Leftrightarrow \exists y \in Y | x\rho_1 y \wedge y\rho_2 z}$$

Then the graph of the composition is

$Gr(\rho_2 \circ \rho_1) = \{(x,z) \in X \times Z | \exists y \in Y | (x,y) \in Gr(\rho_1) \wedge (y,z) \in Gr(\rho_2)\}$.

Attention. The relation ρ_1 acting first in the composition is the second in the writing of $\rho_2 \circ \rho_1$.

Examples:

1. $X = \{1,2,3\}$, $Y = \{a,b\}$, $Z = \{A,B,C\}$,
$Gr(\rho_1) = \{(1,a), (2,a), (2,b), (3,b)\}$,
$Gr(\rho_2) = \{(a,A), (a,B), (b,B), (b,C)\}$.
Then $Gr(\rho_2 \circ \rho_1) = \{(1,A), (1,B), (2,A), (2,B), (2,C), (3,B), (3,C)\}$.
2. Let $X = Y = Z = R$, $x\rho_1 y \Leftrightarrow x^2 + y^2 \leq 1$, $y\rho_2 z \Leftrightarrow y \geq z$.
Then the composition $x(\rho_2 \circ \rho_1)z \Leftrightarrow (-1 \leq x \leq 1) \wedge (z \leq \sqrt{1 - x^2})\}$.
3. Let ρ_1, ρ_2 be binary relations on humanity H, $\rho_1 =$ "*to be husband of*", $\rho_2 =$ "*to be mother of*". Then $\rho_2 \circ \rho_1 =$ "*to be father of*",
$\rho_1 \circ \rho_2 =$ "*to be mother in law of*". So, $\rho_1 \circ \rho_2 \neq \rho_2 \circ \rho_1$,
4. If $\rho =$ "*to be parent of*", Then $\rho^2 = \rho \circ \rho =$ "*to be grandparent of*",
5. Let L be the set of all straight lines on the same plan.
Then $\perp \circ \parallel = \perp$, $\parallel \circ \perp = \perp$, $\parallel \circ \parallel = \parallel$, $\perp \circ \perp = \parallel$.
6. Let $\sim$ be the similarity of triangles on Tr. Then $\sim \circ \sim = \sim$.
7. Let $\mathcal{P}(S)$ be the power of the set S.
Then $= \circ \subseteq \Leftrightarrow \subseteq$, $\subseteq \circ = \Leftrightarrow \subseteq$, $\subseteq \circ \subseteq \Leftrightarrow \subseteq$, $= \circ = \Leftrightarrow =$.

Note. Let ρ_1, ρ_2 be binary relations on $X \times Y$ and $Y \times Z$ respectively. Generally, $\rho_2 \circ \rho_1 \neq \rho_1 \circ \rho_2$. First of all, $\rho_2 \circ \rho_1$ is defined on $X \times Z$. Whereas, $\rho_1 \circ \rho_2$ is not even defined if $X \neq Z$. But even if $X = Y = Z$ and $\rho_2 \circ \rho_1$ and $\rho_1 \circ \rho_2$ are defined both, they are not necessarily equal each other what we saw in example 3 above.

Definition. Inverse Relation.

Let ρ is binary relation from X to Y. The inverse of ρ is binary relation ρ^{-1} from Y to X defined as follows:

$$y\rho^{-1}x \Leftrightarrow x\rho y.$$

Obviously,

1. $Gr(\rho^{-1}) = \{(y,x) \in Y \times X | y\rho^{-1}x\} = \{(y,x) \in Y \times X | x\rho y\}$,
2. $D(\rho^{-1}) = Ran(\rho)$,
3. $Ran(\rho^{-1}) = D(\rho)$.
4. $(\rho^{-1})^{-1} = \rho$.

Examples:

1. **Trivial** relations ρ_f, ρ_e from X to Y. Inverse relations ρ_f^{-1}, ρ_e^{-1} are from Y to X.

$$\rho_f^{-1} = \rho_f,\ \rho_e^{-1} = \rho_e.$$

2. Consider once again example 2 from above:
Let $X = \{2,3\}, Y = \{4,5,6,7,8,9\}, x\rho y \Leftrightarrow x|y$ $(x\ devide\ y)$.
$Gr\ (\rho) = \{(2,4),(2,6),(2,8),(3,6),(3,9)\} \subseteq X \times Y$.
Inverse relation ρ^{-1} *from* Y *to* X will be $y\rho^{-1}x \Leftrightarrow$ "y *is divisible by* x"
with the $Gr(\rho^{-1}) = \{(4,2),(6,2),(6,3),(8,2),(9,3)\} \subseteq Y \times X$.
3. Inverse relation of the relation "to be husband of" from M to W is the relation "to be wife of" from W to M.
4. Inverse relation of the relation "to be married to" on H is the same relation "to be married to" on H.
5. Inverse relation of the relation "to be friend of" on H is the same relation "to be friend of" on H.
6. Inverse relation of the relation "to be parent of" defined on H is "to be child of".
7. Inverse relation of the **Identity** relation I on X is $I^{-1} = I$.
8. Let L be the set of all straight lines on plan P. Then:
a) $\|^{-1}=\|$, b) $\perp^{-1}=\perp$.
11. Inverse relation of the relation $a \in A$ on $S \times \mathcal{P}(S)$ is the relation $A \ni a$ on $\mathcal{P}(S) \times S$.
12. Inverse relations of the relations $\subseteq$ and $=$ on $\mathcal{P}(S)$ are respectively the relations $\supseteq$ and $=$.

Note. The graphs $Gr\ (\rho)$ and $Gr(\rho^{-1})$ are included in the different sets $X \times Y$ and $Y \times X$ respectively. When we use Cartesian coordinate system on the plan to represent them we find that these graphs coincide. And it is natural contrary to the widespread mistake in mathematical textbooks where these graphs must be symmetrical relatively the bisector of the 1st and 3rd quadrants. We will try here to understand this misconception. If we use the horizontal axis for the set X and the vertical axis for the set Y and draw both graphs, of course they coincide. However, if the sets X and Y are both of the "same nature" and if there exists a set S such that $X \subseteq S$ and $Y \subseteq S$ (in particular, if $X = Y = S$), then $X \times Y$, $Y \times X \subseteq S^2$; $Gr(\rho), Gr(\rho^{-1}) \subseteq S^2$. And only in this case we can draw both graphs in the same coordinate system differently. Namely, using for $Gr\ (\rho)$ horizontal axis for the set X and the vertical axis for the set Y, **but** for the $Gr\ (\rho^{-1})$ horizontal axis for the set

Y and the vertical axis for the set X, we receive two different graphs on the same plan:

$$Gr(\rho) = \{(x,y) \in S^2 | x \in X \wedge x\rho y\}$$
$$Gr(\rho^{-1}) = \{(y,x) \in S^2 | y \in Y \wedge x\rho y\}.$$

The points $(x,y) \in S^2$ and $(y,x) \in S^2$ are called symmetric with respect the diagonal $D = \{(x,y) \in S^2 | x = y\}$. Therefore, the graphs $Gr(\rho)$ and $Gr(\rho^{-1})$ are also called symmetric with respect to the diagonal $D: y = x$.

Note. If, in particular, the relation ρ defined on X is symmetric relatively x and y, i.e. if $x\rho y \Leftrightarrow y\rho x$, then the graphs of ρ and ρ^{-1} coincide and their common graph is symmetrical to itself with respect to the diagonal $D: y = x$.

Examples:

1. Let ρ be the binary relation $R \to R,\ x\rho y \Leftrightarrow y = x^2$.
The inverse relation ρ^{-1} is: $x\rho^{-1}y \Leftrightarrow x = y^2$ (or $y = \pm\sqrt{x}$.)
The graphs of ρ and ρ^{-1} are symmetrical with respect to the diagonal $y = x$:

$y = x^2$ $\quad$ $y = x$

$x = y^2$(or $y = \pm\sqrt{x}$.)

2. Let ρ be the binary relation $R \to R,\ x\rho y \Leftrightarrow x^2 + y^2 = 1$.
This relation is symmetrical with respect to x and y: $x^2 + y^2 = 1 \Leftrightarrow y^2 + x^2 = 1$.

Their common graph is the unit circle centered at the origin O and is symmetrical with respect to the diagonal $y = x$:

Definition. Set $\mathcal{R}(X,Y)$. The set of all binary relations from X to Y is denoted by $\mathcal{R}(X,Y)$.

Exercise. Number of all binary relations from X to Y.

Let X, Y be finite sets with $card\ X = n$ and $card\ Y = m$.

Prove that the set $\mathcal{R}(X,Y)$ is finite too and find its cardinality, i.e. find the number of all binary relations from X to Y.

Solution. As we know any binary relation is determined by its truth set in $X \times Y$ and vice versa. The cardinality of $X \times Y = nm$. Since any subset of $X \times Y$ can be the truth set of appropriate binary relation from X to Y, it follows that the number of all binary relations from X to Y is equal to the number of all subsets of $X \times Y$, i.e. to the cardinality of the power of $X \times Y$ i.e. to 2^{nm}. So,

$$card\ \mathcal{R}(X,Y) = 2^{card\ X \cdot card\ Y}$$

Inverse of a composition of relations.

Prove the following important theorem as an exercise:

If ρ_1, ρ_2 are binary relations respectively from X_1 to X_2, and from X_2 to X_3 respectively, then the composition relation $\rho_2 \circ \rho_1$ is from X_1 to X_3, its inverse is the binary relation from X_3 to X_1 and

$$(\rho_2 \circ \rho_1)^{-1} = \rho_1^{-1} \circ \rho_2^{-1}$$

Example. Let $\rho_1 =$ *"to be brother of"*, $\rho_2 =$ *" to be parent of"*.

Then

$\rho_2 \circ \rho_1 =$ *" to be parent of"* $\circ$ *"to be brother of"* $=$ *"to be uncle of"*,

$\rho_1^{-1} =$ *"to be brother of"*, $\rho_2^{-1} =$ *" to be child of"*,

Then, $(\rho_2 \circ \rho_1)^{-1} =$ *"to be nephew or niece of the uncle "*.

$\rho_1^{-1} \circ \rho_2^{-1} =$ *" to be broter of"* $\circ$ *" to be child of"* $==$

"to be nephew or niece of the uncle " $= (\rho_2 \circ \rho_1)^{-1}$.

More generally:

If $\rho_1, \rho_2, \dots, \rho_n$ are the binary relations respectively from X_1 to X_2, from X_2 to X_3, … , from X_n to X_{n+1}, then the binary relation $\rho_n \circ \dots \circ \rho_2 \circ \rho_1$ is from X_1 to X_{n+1} and its inverse

$$(\rho_n \circ \dots \circ \rho_2 \circ \rho_1)^{-1} = \rho_1^{-1} \circ \rho_2^{-1} \circ \dots \circ \rho_n^{-1}$$

is the binary relation from X_{n+1} to X_1.

Notes.

1. Inverse is defined only for binary relations.
2. Any binary relation has an inverse.

Compositional degrees of relations.

If $X_1 = X_2 = \dots = X_{n+1} = X$, $\rho_1 = \rho_2 = \dots = \rho_n = \rho$, then we can define compositional degrees of relations:

$\boldsymbol{\rho^n = \rho \circ \rho \circ \dots \circ \rho}$ (n times, $n \in N$) from X to X.

Because of $(\rho^n)^{-1} = (\rho \circ \rho \circ \dots \circ \rho)^{-1} = \rho^{-1} \circ \rho^{-1} \circ \dots \circ \rho^{-1} = (\rho^{-1})^n$, we define negative compositional degrees $\boldsymbol{\rho^{-n}} = (\rho^n)^{-1} = (\rho^{-1})^n$.

By definition $\boldsymbol{\rho^0 = I_X}$ - identity relation on X.

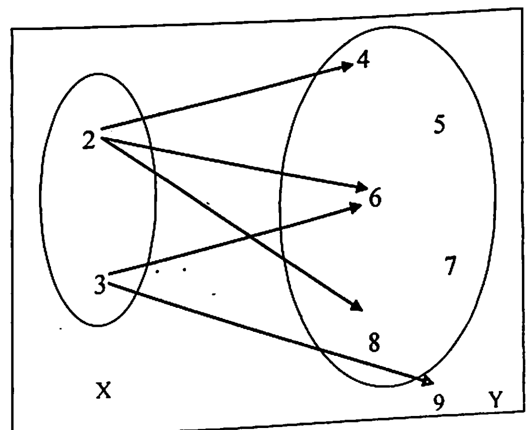
So, compositional degrees $\boldsymbol{\rho^n}$ are defined for all $n \in Z$.

3.1.4. Representation of Relations.

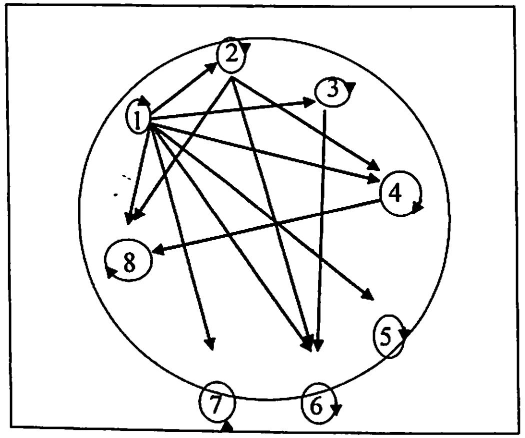
Arrow diagrams. Arrow diagrams can be easily explained by the following example from above:

a) Let $X = \{2,3\}, Y = \{4,5,6,7,8,9\}$, $x\rho y \Leftrightarrow x|y$ $(x\ devide\ y)$.

Then $Gr\ (\rho) = \{(2,4), (2,6), (2,8), (3,6), (3,9)\}$.



b) If in particular, the binary relation is defined from X to X, i.e. on X, then Arrow diagram for the relation, for example of divisibility on the set $X = \{1,2,3,4,5,6,7,8\}$ will be as follows:



Matrix of a Relation. We will demonstrate it on the example a):

$$\begin{array}{c|cccccc} & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 2 & 1 & 0 & 1 & 0 & 1 & 0 \\ 3 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}$$

Exercises 3.1.

1. Let ρ_1, ρ_2, ρ_3 be binary relations respectively $from\, X_1\, to\, X_2,\ from\, X_2\, to\, X_3, from\, X_3\, to\, X_4$.
Prove that the composition of relations is associative:
$(\rho_3 \circ \rho_2) \circ \rho_1 = \rho_3 \circ (\rho_2 \circ \rho_1)$.

2. Let ρ be binary relation from X to Y,
I_X, I_Y be relations of identity on X and on Y respectively.
Prove that,
a) $\rho \circ I_X = \rho,\ I_Y \circ \rho = \rho$,
In particular, if $X = Y$ then $\rho \circ I_X = I_X \circ \rho = \rho$,
b) $\rho^{-1} \circ \rho = I_X, \rho \circ \rho^{-1} = I_Y$
In particular, if $X = Y$ then $\rho^{-1} \circ \rho = \rho \circ \rho^{-1} = I_X$.

3. Let ρ be the binary relation $R \to R,\ x\rho y \Leftrightarrow y > x$. Find:
a) the inverse relation ρ^{-1},
b) on the plan R^2 the graphs of the relations ρ and ρ^{-1}.

4. Let ρ be the binary relation $R \to R,\ x\rho y \Leftrightarrow y > 0$. Find:
a) the inverse relation ρ^{-1},
b) on the plan R^2 the graphs of the relations ρ and ρ^{-1}.

5. Let ρ be the binary relation $X = \{2,3\} \to Y = \{4,5,6,7,8,9\},\ x\rho y \Leftrightarrow x\ devide\ y$.
Find:
a) the inverse relation ρ^{-1},
b) on the plan R^2 the graphs of the relations ρ and ρ^{-1}.

3.2. Equivalence Relations.

3.2.1. Reflexive, Symmetric and Transitive Relations.

Reflexive Relation.
Definition. Binary relation ρ on the set S is called **reflexive** if:

$$\forall x \in S\ x\rho x.$$

Examples:
1. Relation of equality (=) on the set of natural numbers N is reflexive:

$$\forall x \in N\quad x = x.$$

2. Relation (<) on N is not reflexive: $x < x$ is false.

Definition. Symmetric Relation.
Binary relation ρ on the set S is called **symmetric** if:

$$x\rho y \Rightarrow y\rho x$$

Examples:
1. Relation of equality (=) on the set of natural numbers N is symmetric:

$$x = y \Rightarrow y = x.$$

2. Relation (<) on N is not reflexive: $x < y \nRightarrow y < x$.

Transitive Relation.
Definition. Binary relation ρ on the set S is called **transitive** if:

$$x\rho y \wedge y\rho z \Rightarrow x\rho z$$

Examples:
1. Relation (<) on the set of natural numbers N is transitive:

$$x < y \wedge y < z \Rightarrow x < z.$$

2. Relation $\perp$ on the set L of all straight lines on the plan P is not transitive:

$$x \perp y \wedge y \perp z \nRightarrow x \perp z.$$

3.2.2. Equivalence Relations.

Definition. Equivalence Relation.

Binary relation ρ on the set S is called the **equivalence relation**, denoted by special symbol $(\sim)$ if:

1. $\sim$ is **reflexive**: $x \sim x$,
2. $\sim$ is **symmetric**: $x \sim y \Rightarrow y \sim x$,
3. $\sim$ is **transitive**: $x \sim y \wedge y \sim z \Rightarrow x \sim z$

Properties 1-3 are called axioms of equivalence relation.

A set S with equivalence relation $\sim$ on it, is denoted by $(S, \sim)$.

Examples:

1. Let S be any set. Then relation of equality (identity) $(=)$ is the equivalence relation on S:

$x = x, \quad x = y \Rightarrow y = x, \quad x = y \wedge y = z \Rightarrow x = z.$

2. Relation of the logical equivalency $\Leftrightarrow$ on the set of all propositions or on the set of all propositional forms with the same domain of definition is the equivalence relation: $p \Leftrightarrow p,\ (p \Leftrightarrow q) \Rightarrow (q \Leftrightarrow p),\ (p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \Rightarrow (p \Leftrightarrow r)$

3. Relation of the parallelism $\parallel$ on the set L of all straight lines on the plan P is the equivalence relation: $a \parallel a,\ a \parallel b \Rightarrow b \parallel a,\ a \parallel b \wedge b \parallel c \Rightarrow a \parallel c$.

4. Trivial full relation ρ_f on any set X is the equivalence relation: all elements of X are equivalent between themselves.

5. Relation of similarity of triangles on the set of all triangles Tr is the equivalence relation: $\Delta \sim \Delta,\ \Delta_1 \sim \Delta_2 \Rightarrow \Delta_2 \sim \Delta_1,\ \Delta_1 \sim \Delta_2 \wedge \Delta_2 \sim \Delta_3 \Rightarrow \Delta_1 \sim \Delta_3$.

6. In the shop we define a binary relation on the set of all goods: $a \sim b$ if cost $(a) = cost\ (b)$. Check that such defined relation is equivalence.

7. Congruence relation is the equivalence relation on the set of all geometric shapes.

8. Relation "has the same birthday as" is the equivalence relation on the set of all people H.

Counterexamples. The following relations are not equivalence:

1. Relation "to be friend of" is reflexive (everybody is supposed to be friend of himself/herself), is symmetric, but not transitive.

2. Relation "to love" is only reflexive, is not transitive and unfortunately is not symmetric.

2. Relation "to be brother of" is transitive, is not reflexive, is not symmetric on the set of all people, but can be symmetric on the set of all men.

3. Relation "to be parent of" is not reflexive, is not symmetric and is not transitive.

4. Divisibility $x|y$ is reflexive and is transitive, but is not symmetric.

6. Perpendicularity $a \perp b$ is symmetric, is not reflexive and is not transitive on L.

7. Inclusion $A \subseteq B$ is reflexive, transitive but not symmetric on $\mathcal{P}(S)$.

3.2.3. Congruent Relation Modulo m.

Definition. Let $m \in N,\ x, y \in Z$. We write

$$x \equiv y\ (mod\ m)$$

and we say "x *is congruent* y *modulo* m" if $m|(x - y)$.

In other words,

$$x \equiv y\ (mod\ m) \Leftrightarrow \exists n \in Z\ \ (x - y) = mn.$$

The number m is called *modulus*.

Examples:

1. $9 \equiv 12\ (mod\ 3),\ 8 \not\equiv 12\ (mod\ 3)$.

Congruent Relation Modulo m is an equivalency relation. Really:

1. Reflexivity: $x \equiv x\ (mod\ m)$ because $x - x = m \cdot 0$.
2. Symmetry: $x \equiv y\ (mod\ m) \Rightarrow \exists n \in Z | (x - y) = mn \Rightarrow$ $(y - x) = m(-n)\ and\ (-n) \in Z \Rightarrow y \equiv x (mod\ m)$.
3. Transitivity: $x \equiv y\ (mod\ m) \wedge y \equiv z\ (mod\ m) \Rightarrow$ $(x - y) = mn \wedge (y - z) = mk \Rightarrow (x - z) = (x - y) + (y - z) = m(n + k)$.

So, $(x - z) = m(n + k),\ (n + k) \in Z \Rightarrow x \equiv z\ (mod\ m)$.

Example. We use often in geometry and trigonometry the congruent relation modulo 2π: $\forall x, y \in R\ \ x \equiv y\ (mod\ 2\pi) \Leftrightarrow \exists n \in Z\ \ (x - y) = 2\pi n$.

If x and y are the radian measurements of the angles and $x \equiv y\ (mod\ 2\pi)$, then geometrically they represent the same angle. If these angles are represented on the unit circle, then they correspond to the same point on this point. Each angle can be represented by the "standard" value as a real number in the interval $[0, 2\pi)$.

3.2.4. Rational numbers.

On the set $Z \times Z^*$ we define the relation of "equality" as follows:

$$(m,n) = (m',n') \Leftrightarrow mn' = nm',$$

e.g. $(1,2) = (2,4) = (3,6)$ *etc.*

(remember equality of the rational numbers: $\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow mn' = nm'$).

It is easy to check that, such defined **"equality" is an equivalence relation.** Really:

1. reflexivity: $(m,n) = (m,n) \Leftrightarrow mn = nm$,
2. symmetry: $(m,n) = (m',n') \Leftrightarrow mn' = nm' \Leftrightarrow m'n = n'm \Leftrightarrow (m',n') = (m,n)$
3. transitivity: $(m,n) = (m',n') \wedge (m',n') = (m'',n'') \Leftrightarrow$

$$mn' = nm' \wedge m'n'' = n'm'' \Leftrightarrow mn' \cdot m'n'' = nm' \cdot n'm'' \Leftrightarrow mn'' = nm''$$
$$\Leftrightarrow (m,n) = (m'',n'').$$

So, this "equality" is equivalence.

3.2.5. Vectors-arrows.

Vector-arrow in the real space (or on the real plan) is defined as a straight segment $\overrightarrow{AB}$ with start point A and end point B. On the set of all such vectors we define the equality relation as follows:

We assume that the "parallel translation" of vectors in the space is determined by one way or another. We assume that the vector $\overrightarrow{A'B'} = \overrightarrow{AB}$ if $\overrightarrow{A'B'}$ if it can be by combined by mean of "parallel translation" with vector $\overrightarrow{AB}$. We assume also that the space has no "curvature" and the "parallel translation" satisfies the properties: $\overrightarrow{AB} = \overrightarrow{AB}$, $\overrightarrow{AB} = \overrightarrow{A'B'} \Rightarrow \overrightarrow{A'B'} = \overrightarrow{AB}$,

$$\overrightarrow{AB} = \overrightarrow{A'B'} \wedge \overrightarrow{A'B'} = \overrightarrow{A''B''} \Rightarrow \overrightarrow{AB} = \overrightarrow{A''B''}.$$

Equality defined in this manner is an equivalence relation. We note in passing that the notion of parallel translation in the real space is far from trivial and can depend on physical properties of the space, in particular on its curvature.

3.3. Equivalence Classes. Quotient Set.

3.3.1. Equivalence classes.

Definition. Let $\sim$ be an equivalence relation on S and $a \in S$ be an element. Equivalence class of the element a is the subset in S, denoted by $\bar{a}$ (or $cl(a)$, or $[x]$) and defined as follows:

$$\bar{a} = \{x \in S | x \sim a\},$$

i.e. $\bar{a}$ is the set of all $x \in S$ equivalent to a.

Example: Let L be a set of all straight lines, $D \in L$ be a line. Relation $\parallel$, as we know, is equivalence relation on L. Class $\bar{D}$ is the set of all lines parallel to D.

Prove the following theorem as an exercise.

Theorem. Fundamental Properties of the equivalence classes:

Equivalence class is completely determined by any of its elements called **representative of the class**, i.e.

$$a \sim b \Leftrightarrow \bar{a} \sim \bar{b}.$$

So, the equivalence classes are either coinciding or pair wise disjoint.

Examples:

1. Equivalence class of the element a for the equality relation is $\bar{a} = \{a\}$, i.e. is a singleton.
2. The set of all elementary propositions is divided into two equivalence classes: those who are true and those who are false.
3. Equivalence class of the relation "has the same birthday as" is the set of people born in the same day.
4. **Residue classes modulo m.**

For the equivalence relation $x \equiv y \ (mod\ m)$ defined on Z

$$\bar{a} = \{a, a \pm m, a \pm 2m, \dots\}.$$

Classes $\bar{a}$ are called residue classes modulo m, e.g.

$\bar{0} = \{0, \pm m, \pm 2m, \dots\}$, $\bar{1} = \{1, 1 \pm m, 1 \pm 2m, \dots\}$,

$\overline{-1} = \{-1, -1 \pm m, -1 \pm 2m, \dots\}$ *etc.*

5. For the relation $\alpha \sim \beta \Leftrightarrow \alpha \equiv \beta \ (mod\ 2\pi)$ defined on the set of the all angles with the common origin O and common adjacent OA equivalence class $\bar{\gamma}$ is the set of the angles represented by the same radius-vector OB:

$$\bar{\gamma} = \{\gamma, \gamma \pm 2\pi, \gamma \pm 4\pi, \dots\}.$$

6. **Rational numbers.**

Let $(m,n) \in Z \times Z^*$. Its equivalence class according to the definition given above is

$$\overline{(m,n)} = \{(m',n') \in Z \times Z^* | \, mn' = nm'\}$$

Note, that the elements (m,n) and (km', kn'), where $k \in Z^*$ is any, belong to the same class. So, we consider as the simplest representative of each class the pair (m,n), where m and n are mutually prime numbers, i.e. have no common factors other than 1 and -1. It is easy (using the Fundamental Arithmetic Theorem) to prove that this representative is unique up to simultaneous change of signs of the numerator and denominator. For example, for the class $\{(-1,2),(1,-2),(-2,4),(2,-4),(-3,6),(3,-6),...\}$ the simplest representatives are $(-1,2),(1,-2)$. In the case when m and n have the same sign, we choose the simplest representative of where numerator and denominator are positive.

We call from now rational number the whole equivalence class and we denote it $\frac{m}{n}$ instead of $\overline{(m,n)}$. For example, $\frac{1}{2}=\overline{(1,2)}=\{(1,2),(-1,-2),(2,4),...\}$.

Theorem.

An equivalence relation $\sim$ partitions a set S into classes, namely equivalence classes of $\sim$.

Inversely, any partition of S into classes define an equivalence relation on S whose equivalence classes coincide with these classes. This equivalence relation is defined as follows:

Let $\{A_i\}_{i\in I}$ be a partition of S. We define binary relation ρ:

$x\rho y \Leftrightarrow \exists i\in I | x\in A_i \wedge y\in A_i$ and we prove that ρ is an equivalence relation.

The proof of this theorem is not difficult, but we omit it here by referring to any textbook for mathematics students.

3.3.2. Quotient Set.

Definition.

Quotient set of a set S with respect to an equivalence relation $\sim$ is the set of equivalence classes and it is denoted by $S/\sim$.

Examples:

1. Quotient set of the set of all people with respect to the relation "has the same birthday as" consist of 366 elements. Each element (class) is the set of all people born in the same day.

2. **Residue classes modulo m**. Consider congruent relation modulo m on $\mathbb{Z}$: $x\equiv y\ (mod\ m)$. If $m=2$, then there are only two equivalence classes: e.g. $\bar{0}=\{0,2,-2,4,-4,...\}$, and $\bar{1}=\{1,3,-1,5,-3,...\}$. Note, that $\bar{0}=\bar{2}=\overline{-2}=\cdots$, $\bar{1}=\bar{3}=\overline{-1}=\cdots$. So, the quotient set is denoted by

$Z_2=Z/\sim$ and contains only two elements: $Z_2=\{\bar{0},\bar{1}\}$. By analogy, it is easy to find in general case $Z_m=\{\bar{0},\bar{1},\dots,\overline{m-1}\}$, where
$\bar{0}=\{0,m,-m,2m,-2m,...\}$,
$\bar{1}=\{1,m+1,-m+1,2m+1,-2m+1,...\},\dots,$
$\overline{m-1}=\{m-1,2m-1,-1,3m-1,-m-1,...\}$ and
$\bar{0}=\bar{m}=\overline{-m}=\overline{2m}=\cdots$, $\bar{1}=\overline{m+1}=\overline{1-m}=\cdots$ etc.

3. **Free vectors-arrows.**

Since equality of vectors-arrows is defined as equivalence relation the set of all vectors-arrows can be partitioned into the equivalent classes called **free vectors-arrows**. Usually we fix an arbitrary point in the space called origin O and from each class of equal (equivalent) vectors we choose the representative that starts at the origin O. The set of vectors starting at the same origin O is the "model" of the quotient space of all free vectors.

Note. In addition to free vectors in physics are also used fixed and sliding vectors, which should not be confused.

4. **Rational numbers.**

The set of equivalence classes, i.e. quotient set $Z\times Z^*/=$ is called set of rational numbers and denoted by Q. Operations of addition and multiplication on Q are defined as follows:

$\frac{m}{n}+\frac{p}{q}=\frac{mq+pn}{nq}$, that is $\overline{(m,n)}+\overline{(p,q)}=\overline{(mq+pn,nq)}$

$\frac{m}{n}\cdot\frac{p}{q}=\frac{mp}{nq}$, that is $\overline{(m,n)}\cdot\overline{(p,q)}=\overline{(mp,nq)}$

These operations are defined correctly, i.e. do not depend on the choice of representatives. Really, if

$(m,n)=(m',n')\Leftrightarrow mn'=m'n$ and $(p,q)=(p',q')\Leftrightarrow pq'=p'q$, then $(mn')(pq')=(m'n)(p'q)\Leftrightarrow mpn'q'=m'p'nq\Leftrightarrow(mp,nq)=(m'p',n'q')$

or $\frac{mp}{nq}=\frac{m'p'}{n'q'}$ for multiplication. Check analogously for addition.

Exercises 3.3.

Let "$\sim$" be a binary relation defined on $N\times N$, as follows:

$(m,n)\sim(m',n')\Leftrightarrow m+n'=m'+n$.

Prove that so defined relation is an equivalence relation:

a) $(m,n)\sim(m,n)$,

b) $(m,n)\sim(m',n')\Rightarrow(m',n')\sim(m,n)$,

c) $(m,n)\sim(m',n')\wedge(m',n')\sim(m'',n'')\Rightarrow(m,n)\sim(m'',n'')$

and describe its equivalence classes.

3.4. Order Relation. Partial and Total Order. Strict order.

3.4.1. Order.

Definition. Binary relation on a set S, denoted by $\preccurlyeq$ is called **order** (or ordering relation), if:

1. reflexive: $\forall x \in S \quad x \preccurlyeq x$,
2. anti-symmetric: $x \preccurlyeq y \wedge y \preccurlyeq x \Rightarrow x = y$,
3. transitive: $x \preccurlyeq y \wedge y \preccurlyeq z \Rightarrow x \preccurlyeq z$,

We say in this case, that the set S is **ordered** by relation $\preccurlyeq$ and we denote it $(S, \preccurlyeq)$.

Properties 1-3 are called axioms of order.

Relation $x \preccurlyeq y$ is called often inequality (or non-strict inequality).

Examples:

1. **Equality relation on any S set is an order**, called **trivial** order.
   In particular, a set S can be a singleton: $S = \{a\}$.
2. **Logical implication** $\Rightarrow$ on the set of all propositions (or propositional forms defined on the same domain) is order:
$p \Rightarrow p, \quad (p \Rightarrow q \wedge q \Rightarrow p) \Rightarrow (p \Leftrightarrow q), \quad (p \Rightarrow q \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
3. **$(\mathcal{P}(S), \subseteq)$ is an ordered set:**
   $A \subseteq A,\ (A \subseteq B \wedge B \subseteq A) \Rightarrow (A = B),\ (A \subseteq B \wedge B \subseteq C) \Rightarrow (A \subseteq C)$.
4. $(N, \leq)$, $(Z, \leq)$, are ordered sets.
5. **$(N, |)$ is ordered set:**
   $n|n,\ (n|m \wedge m|n) \Rightarrow (n = m),\ (n|m \wedge m|k) \Rightarrow (n|k)$.
6. **Order of rational numbers.** On the set $Q = Z \times Z^*$ we define order based on the order in Z as follows:
   $(m, n) \leq (m', n') \wedge (nn' > 0) \Leftrightarrow mn' \leq nm'$. Check all three axioms!
7. **Alphabetical order.**
   Let S be a finite set consist of n elements. There are $n!$ permutations of S (it will be shown later in combinatorics). So, we can establish $n!$ different order relations. Usually, one of them is taken as main, e.g. if the set $S = \{1, 2, \dots, n\}$, then the main permutation is $(1, 2, \dots, n)$. If S is alphabet, then the main permutation is $(a, b, c, d, \dots, z)$ etc.

Definition. Inverse Order.

On the ordered set $(S, \preccurlyeq)$ we define inverse order: $x \succcurlyeq y \Leftrightarrow y \preccurlyeq x$.

Exercise. Prove that $\succcurlyeq$ is an order relation.

Exercise. Why strict inequality $<$ is not order on Z?

Note. Let $(S, \preccurlyeq)$. We cannot assert that every two elements $x, y \in S$ are comparable, i.e. that $x \preccurlyeq y$ or $y \preccurlyeq x$. For example:

1. obviously, $\exists A, B \in (\mathcal{P}(S), \subseteq)$ that are non-comparable: $A \not\subseteq B$ and $B \not\subseteq A$.
2. the elements $2, 3 \in (N, |)$ are non-comparable: $3 \nmid 5$ and $5 \nmid 3$.

3.4.2. Total (or linear) Order.

Definition. Order relation $\preccurlyeq$ is called **total** (or **linear**) order if, in addition to the 3 axioms of order, it satisfies else 4th axiom, namely the dichotomy axiom:

4. $\forall x, y \in S \quad x \preccurlyeq y \ or\ y \preccurlyeq x$,

i.e. if any two elements of S are "comparable".

A set S with total order on it is called **totally** ordered set or **chain**.

3.4.3. Partial Order. Chains.

Definition. Partial Order.

Order which is not total order is called **partial** order.

So, set of all ordering relations is equal to the union of all partial order relations and of all total order relations.

Examples:

1. examples 2, 3, 5 are examples of partial order.
2. examples 1, 4, 6, 7 are examples of total order.

Definition. Chains in the partial ordered sets.

We can use the term **chain** also for a **totally ordered subset** in the partially ordered. For example, $(N, |)$ is a partially ordered, but the subset $A = \{1, 2, 4, 8, 16, \dots 2^n, \dots\}$ is totally ordered. i.e. is a chain in $(N, |)$.

Note. Obviously, if $(S, \preccurlyeq)$ is a chain, then $(S, \succcurlyeq)$ is also a chain.

The chains $(S, \preccurlyeq)$ and $(S, \succcurlyeq)$ are called respectively **increasing** and **decreasing** chains.

3.4.4. Definition. Strict Order.

Let $(S, \preccurlyeq)$ be ordered set with non-trivial order $\preccurlyeq$.

Binary relation on S denoted by $\prec$ and defined as follows

$$x \prec y \Leftrightarrow x \preccurlyeq y \wedge x \neq y$$

is called **strict order** relation corresponding to non-strict order relation $\preccurlyeq$.

Relation $x \prec y$ is called often strict inequality.

Examples of the strictly ordered sets:

1. $(Z,<)$, 2. $(\mathcal{P}(S),\subset)$. 3. Relation $a\rho b \Leftrightarrow (a|b \wedge a \neq b)$ is a strict order on N.

Example. Lexicographic order.

Let $(S,\preccurlyeq)$ be a totally ordered set. We define on the Cartesian square S^2 a new binary relation $\sqsubseteq$ as follows: $\forall (a_1,a_2),(b_1,b_2) \in S^2$

$$(a_1,a_2) \sqsubseteq (b_1,b_2) \Leftrightarrow (a_1 \prec b_1) \vee (a_1 = b_1 \wedge a_2 \preccurlyeq b_2).$$

Prove yourself that $\sqsubseteq$ is a total order on S^2.

This relation of total order is naturally extended on S^n:

$$(a_1,a_2,\dots,a_n) \sqsubseteq (b_1,b_2,\dots,b_n)$$
$$\Leftrightarrow (a_1 \prec b_1) \vee (a_1 = b_1 \wedge a_2 \prec b_2) \vee \dots$$
$$\vee (a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_{n-1} = b_{n-1} \wedge a_n \preccurlyeq b_n)$$

and called lexicographic order. It is used for example, in compiling dictionaries of list of students in the class. Set S in such cases is alphabet with natural order.

Exercises 3.4.

1. Prove that a strict order $\prec$ is **not** order relation:

$1'$. "antireflexive": $\forall x \in S \quad x \prec x$ is false.

$2'$. "antisymmetric": $\forall x,y \in S \quad x \prec y \wedge y \prec x$ is false

$3'$. transitive: $x \prec y \wedge y \prec z \Rightarrow x \prec z$

$4'$. if $\preccurlyeq$ is a total order, then the property of dichotomy become a trichotomy: *either* $x \prec y$ *or* $y \prec x$ *or* $x = y$, i.e. only one of 3 relations is true.

2. If $\prec$ is a relation satisfying $1',2',3'$ then the relation $\preccurlyeq$ on S defined by $x \preccurlyeq y \Leftrightarrow x \prec y \vee x = y$ is an order relation. And if $\prec$ satisfies also $4'$, then $\preccurlyeq$ is a total order.

3. Prove that in the definition of total order we can omit 1st axiom reflexivity, because of *dichotomy axiom* $\Rightarrow$ *reflexivity axiom*.

4. Let $(S,\preccurlyeq)$ be an ordered set. On S^2 we define relation $\sqsubseteq$ as follows: $(a_1,b_1) \sqsubseteq (a_2,b_2) \Leftrightarrow (a_1 \preccurlyeq a_2) \wedge (b_1 \preccurlyeq b_2)$.

Prove that $(S^2,\sqsubseteq)$ is partially ordered, even if $(S,\preccurlyeq)$ is totally ordered.

3.5. Intervals and their extreme points in ordered sets

3.5.1. Definition. Intervals.

Let $(S,\preccurlyeq)$ be an ordered set, $a,b \in S$ and $a \preccurlyeq b$. Then

$[a,b] = \{x \in S | a \preccurlyeq x \preccurlyeq b\}$ is called closed interval,

$(a,b] = \{x \in S | a \prec x \preccurlyeq b\}$ is called left half-open interval,

$[a,b) = \{x \in S | a \preccurlyeq x \prec b\}$ is called right half-open interval,

$(a,b) = \{x \in S | a \prec x \prec b\}$ is called open interval.

In all cases the elements a and b are called respectively left and right ends of the interval.

3.5.2. Definition. Majorants. Minorants. Bounded Set.

Let $(S,\preccurlyeq)$ be an ordered set and $A \subseteq S$ be a non empty subset.

1. Element $a \in S$ is called **minorant** (or **lower bound**) of A

$$\forall x \in A \quad a \preccurlyeq x.$$

2. Element $b \in S$ is called **majorant** (or **upper bound**) of A

$$\forall x \in A \quad x \preccurlyeq b.$$

3. A set $A \subseteq S$ is called bounded bellow if it has at least one minorant.
4. A set $A \subseteq S$ is called bounded above if it has at least one majorant.
5. A set $A \subseteq S$ is called bounded if it bounded bellow and above.

Examples:

1. In the set $(R,\leq)$ we consider the subset $A = [-1,2)$.

Majorants are e.g. $2, 5, 10^3$ *etc*. Minorants are e.g. $-1,-3,-10^3$ *etc*.

Set A is bounded. Set R is not bounded.

2. In the set $(N,|)$ we consider the subset $A = \{m,n\}$.

Any common multiple of the numbers m,n is a majorant of A and, inversely, any majorant of A is common multiple of m and n. For example, majorants of $A = \{6,9\}$ are $18,36,54$ *etc*. Analogously, the set of minorants of A is the set of common divisors of m and n. For example, minorants of $A = \{6,9\}$ are 1 and 3.

The set A is bounded. Note, that any subset in $(N,|)$ is bounded bellow by number 1.

3. In the set $(\mathcal{P}(S),\subseteq)$ for any subset $A \subseteq \mathcal{P}(S)$ there exits the majorant; it is S and the minorant; it is $\emptyset$. Any subset $A \subseteq \mathcal{P}(S)$ is bounded.

Note. A set $A \subseteq S$ bounded in $(S, \preccurlyeq)$ is not necessarily bounded if we consider it independently in $(A, \preccurlyeq)$. In fact, $[0,1)$ is obviously bounded above in $(R, \leq)$, but is not bounded above in $([0,1), \leq)$.

3.5.3. Definition. Maximum and Minimum.

Let $(S, \preccurlyeq)$, $A \subseteq S$, $A \neq \emptyset$.

Minorant a is called **minimum** (or **least element**) of A if $a \in A$ and we denote it $a = min\ A$.

Majorant b is called **maximum** (or **greatest element**) of A if $b \in A$ and we denote it $b = max\ A$.

In other words, $a = min\ A \Leftrightarrow (\forall x \in A\ \ a \preccurlyeq x) \wedge (a \in A)$,

$$b = max\ A \Leftrightarrow (\forall x \in A\ \ x \preccurlyeq b) \wedge (b \in A)$$

Theorem. Uniqueness of minimum and maximum.

If there exits min A ($max\ A$), then it is unique.

Proof. Suppose that there are two minimum $a = min\ A$ and $a' = min\ A$. Then $a \preccurlyeq a'$ because a is minorant of A and $a' \preccurlyeq a$ because a' is minorant too.

So, by virtue of the antisymmetry of the order relation $a' = a$.

Analogously we can prove that $max\ A$ is also unique.

Examples:

1. $(R, \leq)$, $min\ [-1,2) = -1$, $max\ [-1,2)$ does not exist. Note, that R itself has no max, has neither min nor max.
2. $(N, |)$, $A = \{m, n\}$ has max and min if and only if $m|n$. In this case $min\ A = m$, $max\ A = n$. E.g. $\{6, 9\}$ has no max, has no min. But $min\ \{3,9\} = 3$, $\max\{3,9\} = 9$.
3. $(N, \leq)$, $\forall A \subseteq N\ (A \neq \emptyset)$ there exist $min\ A$. If A is bounded above, then there is else $max\ A$.
4. Let $(S, \preccurlyeq)$, and $\{a\} \subseteq S$ be a singleton. Then $min\{a\} = max\{a\} = a$.
5. Let $(\mathcal{P}(S), \subseteq)$. Then $\forall A \in \mathcal{P}(S)\quad \emptyset \subseteq A \subseteq S$, corollary $\emptyset$ is min and S is max in $\mathcal{P}(S)$.

3.5.4. Definition. Infimum. Supremum.

Let $(S, \preccurlyeq)$, $A \subseteq S$, $A \neq \emptyset$.

1. If the set of minorants m of A is not empty and has the greatest element, then it is called **infimum** (or **greatest lower bound**) of A and denoted by $inf\ A$:

$$inf\ A = max\ m.$$

2. If the set of majorants M of A is not empty and has the least element, then it is called **supremum** (or **least upper bound**) of A and denoted by $\sup A$:

$$\sup A = min\ M.$$

Theorem. If $inf A$ ($sup\ A$) exists, then it is unique.

The **Proof** follows from the uniqueness of the greatest (least) element of any set if it exists.

Examples:

1. Let $(R, \leq)$, $A = [-1, 3)$.
$min[-1,3) = inf[-1,3) = -1$, $max\ [-1,3)$ does not ist, $sup\ [-1,3) = 3$.
2. Let $(N, |)$, $A = \{m, n\}$.
$inf\{m, n\} = GCD\ (the\ greatest\ common\ divisor)$,
$sup\{m, n\} = LCM\ (the\ least\ common\ multiple)$.
For example, $sup\{6{,}9\} = 18$, $inf\{6, 9\} = 3$.

4. Let $(\mathcal{P}(S), \subseteq)$, $A, B \in \mathcal{P}(S)$ $(i.e. A, B \subseteq S)$, then
$inf\{A, B\} = A \cap B$, $sup\{A, B\} = A \cup B$.

Note. We must remember that the existence (or nonexistence) of majorants and minorants of a set A, and thus of $\min A, \max A$, $inf A, sup\ A$, depend on A considered independently or as subset of another set.

For example, $A = ([0,1), \leq)$ considered independently is not bounded above and hence does not have neither max nor sup. But the set $A = [0,1)$ considered as the subset of $(R, \leq)$ is bounded above, $max\ A$ does not exist, $sup\ A = 1$.

Exercise 3.5. Duality of $\preccurlyeq$. Prove, that if a subset $(A, \preccurlyeq)$ in $(S, \preccurlyeq)$ has a majorant (minorant), maximum (minimum), then the subset $(A, \succcurlyeq)$ in $(S, \succcurlyeq)$ will have respectively the minorant (majorant), minimum (maximum). If $(A, \preccurlyeq)$ is increasing chain in $(S, \preccurlyeq)$, then $(A, \succcurlyeq)$ will be decreasing chain in $(S, \succcurlyeq)$.

3.6. Functions (Mappings). Graphs.

3.6.1. Function.

Definition. Let X and Y be sets. Binary relation f from X to Y is called functional relation or **function** (or **mapping**) **from X to Y** if for **every** element $x \in X$ there exists **one and only one** element $y \in Y$ such that xfy is true, or briefly if

$$\forall x \in X \quad \exists' y \in Y : xfy$$

So, function is a special case of binary relation with two special conditions:

1. for **every** $x \in X$ there exists $y \in Y$ such that xfy is true
2. this y is **unique**.

When a relation f from X to Y is a function we write it
$f: X \to Y$ and instead of xfy we will write $y = f(x)$
(or sometimes $X \xrightarrow{f} Y, x \overset{f}{\mapsto} y, or\ x \mapsto f(x)$).
In particular, the function $f: X \to X$ is called **transformation** of X.

As the function is a special case of binary relation the notions of the graph, domain, codomain and range remain valid for the function:

$$Gr(f) = \{(x, y) \in X \times Y \mid y = f(x)\} = \{(x, f(x)) \in X \times Y \mid x \in X\} \subseteq X \times Y,$$

Any function (like a relation) is completely determined by its graph.

$D(f) = X$, elements $x \in X$ are called **inputs.**

The definition of the domain of the function is simpler and shorter than the domain of the general relation because of the 1st condition of the definition 3.8.1.

$$Cod(f) = Y,$$

$Ran(f) = \{y \in Y \mid \exists x \in X \mid y = f(x)\} \subseteq Y$ (as well as for binary relations),

But for functions there is another notation of $Ran(f) = Im(f)$
(Im is from Image).

Note also that **not each** element $y \in Y$, i.e. generally $Im(f) \subseteq Y$.

Definition. Image. Preimage. Let $f: X \to Y$ be a function.

Element $f(x) \in Y$ is called **image** of $x \in X$ *under* f.

Element $x \in X$ is called **preimage** of $f(x) \in Y$ *under* f, note that it is not necessarily unique.

Sometimes element x is called **point, variable** or **argument**, element $f(x)$ is called **value** of the function f at x.

Definition. Let $f: X \to Y$ be a function and $A \subseteq X$ be a subset.
The image of A under f is defined as follows:
$f(A) = \{f(x) \in Y \mid x \in A\}$, i.e. as the set of all images $f(x)$ when $x \in A$.
In particular, $f(\emptyset) = \emptyset$, $f(X) = Ran(f) = Im(f)$.

The concept of function is so important in mathematics, that the definition of function independent on binary relation is desirable.

Definition. Let X and Y be sets.

A **function** (or mapping) f from X to Y, denoted by $f: X \to Y$, **assigns** (or corresponds) to each element $x \in X$ exactly one element $y \in Y$, denoted $y = f(x)$.

As a function is a special case of a binary relation all definitions and theorems in this chapter here bellow for functions can be deduced from the corresponding definitions and theorems for the relations. But for the independence of the presentation we will give independently the definitions of the equality of the functions, of the composition of the functions, of the inverse function. The consistency of these definitions with the corresponding definitions for the relations can be done by the reader himself as the exercise.

Examples:

1. Let M be the set of all men and W be the set of all women. Then the relation from M to W: "m *is the husband of* w" is not function. Really, not each man is married, so the 1st condition of the definition of a function is not fulfilled.

2. Let C be the set of all children having at least one parent and P be the set of all parents. Then the relation from C to P: "c *is the child of* p" is not function. Really, some children have two parents (father and mother), so the 2nd condition of the definition of a function is not fulfilled.

3. If in example 1 we consider the same relation "m *is the husband of* w" from Mr to W, where Mr is the set of all married men, then this relation is the function.

Really, for every married man there exits his exactly one wife.

4. **Constant function.** The function $f: X \to X$ such that

$\forall x \in X \;\; f(x) = c$, where c is fixed element from Y, is called **constant function**. $Im(f) = c$. $Gr(f) = X \times \{c\}$.

5. **Identity function.** The function $I: X \to x$ such that

$$\forall x \in X \;\; I(x) = x$$

is called **identity** function on X. $Im(I) = X$.

$Gr(I) = \{(x,x) | x \in X\}$ – Diagonal of X^2.

6. **Characteristic function of a set.** Let X be a set and $A \subseteq X$ be a subset. The function $\chi_A: X \to \{0,1\}$ such that

$$\chi_A(x) = \begin{cases} 1, if\ x \in A \\ 0, if\ x \notin A \end{cases}$$

is called characteristic function of a set A.

7. **Sequences.** Let X be a set and N be the set of natural numbers.

The function $x: N \to X, n \mapsto x(n)$ is called **sequence** in X. The values of $x(n), n \in N$ are usually denoted x_n, and sequence is denoted $(x_n)_{n\in N}$ $\{x_1, x_2, \dots, x_n, \dots\}$.

For example, the function $x(n) = x_n = \frac{1}{n}, n \in N$ defines in R the sequence $\left(\frac{1}{n}\right)_{n\in N}$ or $\{1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots\}$. A sequence is called **numerical sequence** if $X = R$- the set of real numbers.

8. **Function-compliment.** Let U be the universe and A be its subset. For every A there exits its compliment $\bar{A} = U - A$. Let $\mathcal{P}(U)$ be the power of U, i.e. the set of all subsets of U, so $A, \bar{A} \in \mathcal{P}(U)$. Then

$$f: \mathcal{P}(U) \to \mathcal{P}(U), \qquad f(A) = \bar{A}$$

is the function.

8. **Canonical function.** Let (X, ρ) be a set X with an equivalence relation ρ on it and $\bar{x}$ be the equivalence class of x, X/ρ be the quotient set. Then the function

$$g: X \to X/\rho, \qquad g(x) = \bar{x}$$

is called **canonical function**.

9. **Function of two variables.** Function $f: X \times Y \to Z$, is called function of two variables. In practice instead of $z = f((x,y)), (x,y) \in X \times Y$ we usually write $z = f(x,y),\ x \in X,\ y \in Y$ in order to underline expression "of two variables".

10. **Binary operations on $\mathcal{P}(U)$.** Let U be the universe and $\mathcal{P}(U)$ its power and $A, B \in \mathcal{P}(U)$ subsets in U. Then the binary operations $\cap$, $\cup$, $-$, Δ generate the functions of two variables $f, g, h, p: \mathcal{P}(U) \times \mathcal{P}(U) \to \mathcal{P}(U)$:

$f(A,B) = A \cap B,\ g(A,B) = A \cup B,\ h(A,B) = A - B,\ p(A,B) = A\Delta B.$

11. **Projectors-functions.** The projectors-functions are defined as follows:

$Pr_X: X \times Y \to X,\ Pr_X(x,y) = x$ and $Pr_Y: X \times Y \to Y,\ Pr_Y(x,y) = y$.

Functions of two variables are naturally generalized to the case of n variables.

12. **Predicates and Boolean functions.**

Every $n - ary$ propositional form $P(x_1, x_2, \dots, x_n)$, where $x_1 \in X_1, x_2 \in X_2 \dots, x_n \in X_n$ generate a function from the set $X = X_1 \times X_2 \times \dots \times X_n$ to the set $\{t, f\}$ which is called $\boldsymbol{n - ary}$ **Predicate-function** or just **Predicate.** So, all propositional forms can be considered and called as Predicates. Obviously, two equivalent propositional forma generate the same Predicate.

In particular, when all variables $x_1, x_2, \dots, x_n$ are elementary propositions Predicates are called **Boolean functions.** For example, all compound propositions discussed above in the 1st chapter can be considered as Boolean functions.

Any Boolean function of n variables can be defined by its truth table containing 2^n rows.

13. The "floor" function $\lfloor\cdot\rfloor: R \to R$, $\lfloor x \rfloor$ =greatest integer less than or equal to x, e.g.: $\lfloor 2 \rfloor = 2, \lfloor 2.1 \rfloor = 2, \lfloor e \rfloor = 2, \lfloor \pi \rfloor = 3, \lfloor -2.1 \rfloor = -3, \lfloor -e \rfloor = -3$.

$D(\lfloor\cdot\rfloor) = R,\ Im(\lfloor\cdot\rfloor) = Z$.

14. The ceiling function $\lceil\cdot\rceil: R \to R$, $\lceil x \rceil$ =least integer greater than or equal to x, e.g.: $\lceil 2 \rceil = 2, \lceil 2.1 \rceil = 3, \lceil e \rceil = 3, \lceil \pi \rceil = 4, \lceil -2.1 \rceil = -2, \lceil -e \rceil = -2$.

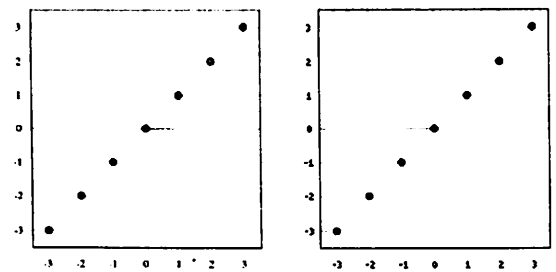
$D(\lceil\cdot\rceil) = R,\ Im(\lceil\cdot\rceil) = Z$.

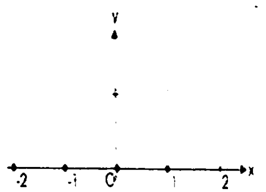
Obviously: $\forall x \in R\ \ \lfloor x \rfloor \le x \le \lceil x \rceil,\ \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 1, & x \notin Z \\ 0, & x \in Z \end{cases}$

15. The "fractional part" function $\{\cdot\}: R \to R$, $\{x\} = x - \lfloor x \rfloor$, e.g.: $\{2\} = 0, \{2.1\} = 0.1, \{e\} = 0.718\dots, \{\pi\} = 0.141\dots, \{-2.1\} = 0.9, \{-2.9\} = 0.1$

$D(\{\cdot\}) = R,\ Im(\{\cdot\}) = [0,1)$. Function $\{\cdot\}$ is periodic with period 1.

Here bellow there are the graphs of the floor, ceiling and fractional part functions respectively taken from Wikipedia.





16. The *modulus operator* (mod) is the function of two variables usually written in the form of a binary relation $mod: Z \times Z_+^* \to Z$,

$mod\ (x)$ =reminder when x is divided $by\ y$. For example

$20\ mod\ 6 = 2$ because $20 = 3 \cdot 6 + 2$,

$47\ mod\ 7 = 5$ because $47 = 6 \cdot 7 + 5$, etc.

3.6.2. Equality of functions.

Definition. Two functions $f: X \to Y$ and $f_1: X_1 \to Y_1$ are called **equal** if and only if $X = X_1,\ Imf = Img$ and $\forall x \in X\ f(x) = g(x)$.

This definition implies that

$f \neq g \Leftrightarrow (X \neq X_1) \vee (Imf \neq Img) \vee (\exists x \in X \mid f(x) \neq g(x))$

3.6.3. Restriction and Extension of Functions.

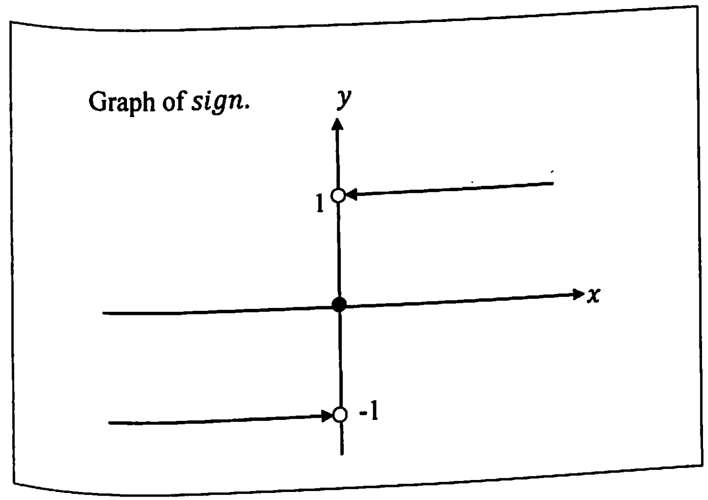
Definition. Let $f: X \to Y$ and $A \subset X$ be a subset. **Restriction** of f to the subset A is the function $g: A \to Y$ such that $\forall x \in A\ g(x) = f(x)$.

A restriction of f on A is often denoted instead of g by f_A.

Conversely, if there is a function $g: A \to Y$ then we call **extension** of g to the set $X \supset A$ any function $f: X \to Y$ such that $\forall x \in A\ f(x) = g(x)$.

Example. The function $\boldsymbol{sign}: \boldsymbol{R} \to \boldsymbol{R}$ is defined as follows:

$$sign\ (x) = \begin{cases} -1, & if\ x < 0 \\ 0, & if\ x = 0 \\ 1, & if\ x > 0 \end{cases}$$



Obviously, $Im\ (sign) = \{-1, 0, 1\}$ and $sign$ is an odd function.

The function $g: R \to R$, defined as $g(x) = \frac{x}{|x|}$ is the restriction of $sign$ to $R^* = R - \{0\}$, and the function f is an extension of g from R^* to R.

Note that a restriction g of given f is defined uniquely, but an extension f of given g is not defined uniquely.

Example. The function $\boldsymbol{abs}: \boldsymbol{R} \to \boldsymbol{R}$ is called absolute value (or modulus) and is

defined as follows:

$$abs\,(x) = |x| = \begin{cases} -x, & if\ x < 0 \\ 0, & if\ x = 0 \\ x, & if\ x > 0 \end{cases}$$

Obviously, $Im\,abs = R_+$, abs is an even function.

Notation. Set $\mathcal{F}(X,Y)$. The set of all functions from X to Y is denoted by $\mathcal{F}(X,Y)$ and instead of $f: X \to Y$ they write in practice $f \in \mathcal{F}(X,Y)$.

If, in particular, $X = Y$ they denote $\mathcal{F}(X,Y)$ by $\mathcal{F}(X)$.

Exercise. Let X, Y be finite sets with $card\,X = n$ and $card\,Y = m$.

Prove that the set $\mathcal{F}(X,Y)$ is finite too and find its cardinality, i.e. find the number of all functions from X to Y.

Solution. Denote the elements of $X = \{a_1, a_2, \dots, a_n\}$. There are m different possibilities of choosing a value for $f(1)$ from the elements of Y. There are the same m different possibilities of choosing a value for $f(2)$ etc, till $f(n)$. So, common number of possibilities of choosing $f(1), f(2), \dots, f(n)$ will be $\tilde{A}_m^n = \underbrace{m \cdot m \cdot \dots m}_{n\ times} = m^n$. So, $card\,\mathcal{F}(X,Y) = m^n$ or

$$\boxed{card\,\mathcal{F}(X,Y) = card\,Y^{card\,X}}.$$

If, in particular $Y = \{t, f\}$ i.e. $card\,Y = 2$, then **the number of all unary Predicate functions on X is equal to 2^n.**

The meaning of the symbol $\tilde{A}_m^n$ will be clear in the study of combinatorics.

Exercise 3.6. Let $X_1, X_2, \dots, X_n, Y$ be finite sets with $card\,X_1 = k_1$, $card\,X_2 = k_2, \dots, card\,X_n = k_n$ and $card\,Y = m$.

Prove that $X = X_1 \times X_2 \times \dots \times X_n$ and $\mathcal{F}(X,Y)$ are finite too and

$$\boxed{card\,\mathcal{F}(X,Y) = m^{k_1 k_2 \dots k_n} = card\,Y^{card\,X_1 \cdot card\,X_2 \cdot \dots \cdot card\,X_n}}.$$

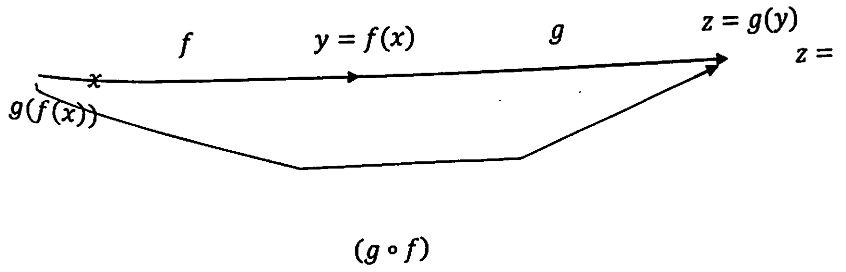
If, in particular $X_1, X_2, \dots X_n$ are the propositions, i.e. take their values in $\{t, f\}$, $Y = \{t, f\}$, then $k_1 = k_2 = \dots = k_n = card\,Y = 2$ then **the number of all Boolean functions of n variables is equal to 2^{2^n}.**

3.7. Composition of functions.

3.7.1. Composition of functions.

Definition. Composition of two functions $f: X \to Y$ and $g: Y \to Z$ is the function denoted by $g \circ f$ and defined as follows:

$$(g \circ f): X \to Z, \quad (g \circ f)(x) = g[f(x)].$$



Example.

Let $f: Z \to N$, $f(x) = x^2$; $g: N \to R$, $g(x) = x + \pi$.

Then $(g \circ f): Z \to R$, $(g \circ f)(x) = g[f(x)] = g(x^2) = x^2 + \pi$.

Note that when $f: X \to Y$, $g: Y \to Z$ the composition $g \circ f$ is defined above, but the composition $f \circ g$ is not necessarily defined. It is possible if and only if $Z = X$. But even in this case when $Z = X$ the two compositions $g \circ f$ and $f \circ g$ are defined from X to X but $g \circ f \neq f \circ g$ in general. So, the operation of composition of functions is not **commutative.** In the particular cases when $g \circ f = f \circ g$ we say that the functions f and g **commute.**

Examples.

1. Let $f: R \to R$, $f(x) = sinx$; $g: R \to R$, $g(x) = x^2$.
Then $(g \circ f): R \to R$, and $(f \circ g): R \to R$,
$(g \circ f)(x) = g[f(x)] = g(sinx) = \sin^2 x$,
$(f \circ g)(x) = f[g(x)] = f(x^2) = sinx^2$, so $g \circ f \neq f \circ g$.

2. Prove that the functions $abs, sign: R \to R$ commute, that is $abs \circ sign = sign \circ abs$ and draw their common graph.

Solution: Really,

$$(abs \circ sign)(x) = abs(sign(x)) = \begin{cases} 1, & if\ x < 0 \\ 0, & if\ x = 0 \\ 1, & if\ x > 0 \end{cases}$$

$$(sign \circ abs)(x) = sign(abs(x)) = \begin{cases} 1, & if\ x < 0 \\ 0, & if\ x = 0 \\ 1, & if\ x > 0 \end{cases}$$

Note. If $f: X \to Y$ is a function, I_X, I_Y are the **identity-functions** on X and Y respectively, then $f \circ I_X = I_Y \circ f = f$.

In particular, if $X = Y$, then $f \circ I_X = I_X \circ f = f$.

3.7.2. Associativity of a Composition of functions.

Theorem.

If $f: X \to Y,\ g: Y \to Z,\ h: Z \to V$, then

$$\boldsymbol{h \circ (g \circ f) = (h \circ g) \circ f}$$

as functions from X to V.

The proof is obvious. Do it!

Note. Associativity of the functions composition allows omitting the parenthesis and write $h \circ g \circ f$.

3.7.3. Compositional Powers of a function.

If $f: X \to X$, then we can define the "compositional powers" of the function: $f^n: X \to X,\ f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n}$ and $f^n(x) = f\{\ldots f[f(x)]\}$.

We also define $f^0 = I_X$.

Do not confuse this "compositional powers" with the "multiplicative" powers when on the set X is defined in some way a "multiplication" and "multiplicative powers" are denoted unfortunately by exactly the same notations: $f^n: X \to X$, $f^n = f \cdot f \cdot \ldots \cdot f,\ f^n(x) = f(x) \cdot f(x) \cdot \ldots \cdot f(x)$. For example, compositional and multiplicative squares of the function sin are respectively:

$\sin^2 x = \sin(\sin(x))$ and $\sin^2 x = sinx \cdot sinx = \sin^2 x$ are absolutely different things. But there is no real danger with confusing of these notations because it is always clear from the context what powers we are speaking about. In this chapter we speak only about compositional powers.

3.7.4. Involution-function.

Definition. The function $f: X \to X$ is called an **involution** if $f^2 = I_X$.

Examples:

1. **Identity-function** $I_X: X \to X,\ \forall x \in X\ I_X(x) = x$ is involution. Really:
$\forall x \in X\ \ I_X^2(x) = I_X(I_X(x)) = I_X(x) = x$. So, $I_X^2 = I_X$.

2. Function $f: R \to R,\ f(x) = -x$ is involution. Really:
$\forall x \in R\ \ f^2(x) = f(f(x)) = f(-x) = -(-x) = x$. So, $f^2 = I_X$.

3. Function $f: R^* \to R^*,\ f(x) = \frac{1}{x}$ is involution. Really:
$\forall x \in R^*\ \ f^2(x) = f(f(x)) = f\left(\frac{1}{x}\right) = \frac{1}{\frac{1}{x}} = x$. So, $f^2 = I_X$.

3.7.5. Idempotent -function.

Definition. The function $f: X \to X$ is called an **idempotent** if $f^2 = f$.

Examples:

1. **Constant-function** $f: X \to X,\ \forall x \in X\ f(x) = c$, where $c \in X$ is constant, is idempotent. Really:
$\forall x \in X\ f^2(x) = f[f(x)] = f(c) = c = f(x)$. So, $f^2 = f$.

2. **Identity-function** $I_X: X \to X,\ \forall x \in X\ I_X(x) = x$ is idempotent. Really:
$\forall x \in X\ \ I_X^2(x) = I_X(I_X(x)) = I_X(x) = x$. So, $I_X^2 = I_X$.

3. **Projectors.** Consider special case of the projectors on R^2.
Let R^2 be the arithmetic plan and $f, g: R^2 \to R^2$ be two functions:
$\forall (x,y) \in R^2\ f(x,y) = (x,0),\ g(x,y) = (0,y)$.
We prove that f, g are the idempotent. Really:
$\forall (x,y) \in R^2\ f^2(x,y) = f[(f(x,y)] = f(x,0) = (x,0) = f(x,y)$. So, $f^2 = f$.
$\forall (x,y) \in R^2\ g^2(x,y) = g[(g(x,y)] = g(0,y) = (0,y) = g(x,y)$. So, $g^2 = g$.

Note also that f and g commute. Really:
$\forall (x,y) \in R^2\ (g \circ f)(x,y) = g[f(x,y)] = g(x,0) = (0,0)$ and
$\forall (x,y) \in R^2\ (f \circ g)(x,y) = f[g(x,y)] = f(0,y) = (0,0)$.

So, $g \circ f = f \circ g$.

We call and we denote **axis X and Y** the sets

$X = \{(x,y) \in R^2 | y = 0\} \subset R^2, \ Y = \{(x,y) \in R^2 | x = 0\} \subset R^2$.

The point $(x, 0)$ is called **projection** of the point (x, y) on the axis X.

The point $(0, y)$ is called **projection** of the point (x, y) on the axis Y.

For functions f and g we use the special names **projectors** on the axis X and Y respectively and we denote them by $Pr_X = f, \ Pr_Y = g$.

Exercises 3.7.

1. Let $f: X \to X$ be an involution. Prove that for all $n \geq 2$ $f^n = I_X$ if n is even and $f^n = f$ if n is odd.
2. Let Mp be the set of all married people and $f: Mp \to Mp$ be the function (transformation) defined as follows: $f(x) = y \Leftrightarrow$ "x *is married to* y". Prove that f is involution.
3. Prove that abs and $sign$ are idempotent-functions: $abs^2 = abs, \ sign^2 = sign$. i.e. $\forall x \in R \ \ abs^2(x) = abs(x), \ \ sign^2(x) = sign(x)$
4. Let $f: X \to X$ be an idempotent. Prove that $\forall \, n \geq 2 \ \ f^n = f$.
5. The functions $f, g, h: R \to R$ are defined as follows:

$f(x) = x^3, \qquad g(x) = \sin x, \ \ h(x) = 2x - 1.$

Find the functions

$g \circ f, \ f \circ g, \ h \circ f, \ h \circ g, \ g \circ f \circ h, \ f \circ g \circ h, \ h \circ h, \ f \circ h \circ f \circ h,$

i.e. find the expressions

$(g \circ f)(x), \quad (f \circ g)(x), \quad (h \circ f)(x), \quad (h \circ g)(x), \quad (h \circ h)(x)$

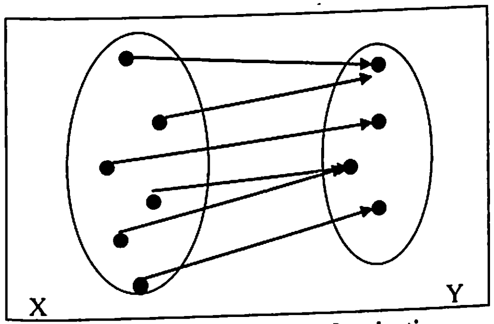
$(g \circ f \circ h)(x), \quad (f \circ g \circ h)(x), \quad (f \circ h \circ f \circ h)(x)$

3.8. Surjection, Injection and Bijection. Inverse function.

3.8.1. Surjection.

Definition. A function $f: X \to X$ is called **surjective** (or **onto** function) if $Imf = Y$, i.e. if for all $y \in Y$ there exists (at least one) $x \in X$ such that $y = f(x)$.

Note. In general $Imf \subseteq Y$. So, any function $f: X \to Imf$ is surjection.



Arrow diagram of surjection.

Examples:

1. The function **absolute value** (or **modulus**)

$$f: R \to R, \ f(x) = |x| = \begin{cases} -x, if \ x < 0 \\ 0, if \ x = 0 \\ x, if \ x > 0 \end{cases}$$

is not surjective, but the function $f: R \to R_+, \ f(x) = |x|$ is surjection.

Remember: $R_+ = \{x \in R | x \geq 0\}$.

2. **Projectors**

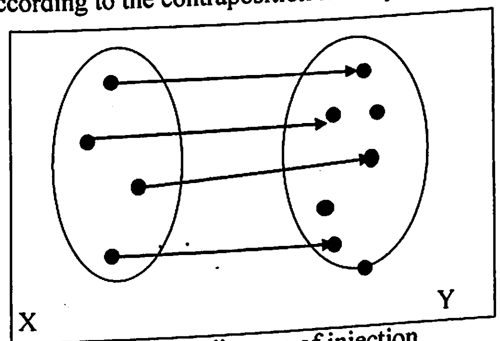
$Pr_X: X \times Y \to X, \ Pr_X(x,y) = x$ and $Pr_Y: X \times Y \to Y, \ Pr_Y(x,y) = y$ are surjective functions.

3.8.2. Injection.

Definition. A function $f: X \to X$ is called **injective** (or **one-to-one** function) if the different inputs in X have the different images in Y:

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Or according to the contraposition law if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.



Arrow diagram of injection.

Examples:

1. The function $f: R \to R,\ f(x) = x^n,\ n \in N$ is an injection if n is odd and is not an injection if n is even.

Really: if n is odd, then $x_1^n = x_2^n \Rightarrow x_1 = x_2$, and if n is even, then $x_1^n = x_2^n \nRightarrow x_1 = x_2$ because it is possible that $x_1 = -x_2$.

2. Projector-functions are not injective if X and Y contain more than one elements. Let, for example, $Pr_X: X \times Y \to X$ be the 1st projector and $y_1 \neq y_2$ be two different elements $\in Y$. Then $(x, y_1), (x, y_2) \in X \times Y$ and $(x, y_1) \neq (x, y_2)$,

but $Pr_X(x, y_1) = x$ and $Pr_X(x, y_2) = x$, so $Pr_X(x, y_1) = Pr_X(x, y_2)$.

Note. Any no injective function $f: X \to Y$ has an injective restriction $f_A: X \to Y$, where $A \subset X$.

Really, for each $y \in Imf$ we choose in some way exactly one of its preimage $x \in X$ and include it into A. Then thus constructed function will be injective. We used implicitly here axiom of choice.

Example. Let $f: R \to R,\ f(x) = x^2$. Here, $Imf = R_+$ and for every $y \in Imf$ there are no more than two x such that $x^2 = y$, namely $x \in R_+$ and $x \in R_-$.

Choosing as a set A the sets R_- or R_+ alternately we get two injective restrictions:

$$f_{R_-}: R_- \to R,\ f_{R_-}(x) = x^2 \text{ and } f_{R_+}: R_+ \to R,\ f_{R_+}(x) = x^2$$

or briefly (without of ambiguity)

$$f: R_- \to R,\ f(x) = x^2 \text{ and } f: R_+ \to R,\ f(x) = x^2.$$

Exercise. Consider example just above and choose as a set $A = \{x \in R_+ | x^2 \in N\} \cup \{x \in R_- | x^2 \notin N\}$

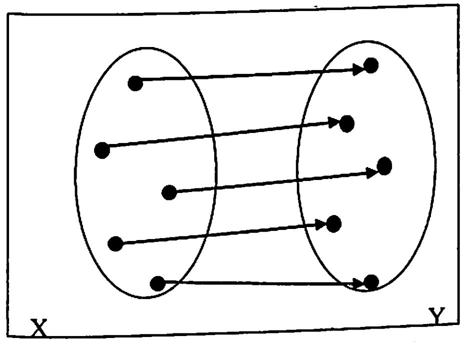
Then the restriction $f_A: A \to R$ is injective.

Also the restriction $f_B: B \to R$, where $B = R - A$, is injective too.

3.8.3. Bijection.

Definition. A function $f: X \to X$ is called **bijective** (or **on-to-one correspondence)** if it is surjective and injective.

In other words, f is bijective if and only if $\forall y \in Y\ \exists' x \in X |\ y = f(x)$.



Arrow diagram of bijection.

Examples.

1. Identity function $I: X \to X,\ I(x) = x$ is obviously bijective.
2.
a) The function $sin: R \to R,\ \ sin(x) = sin\, x$ is not surjective, not injective.
b) The function $sin: R \to [-1, 1]$ is surjective, but not injective.
c) The function $sin: [-\frac{\pi}{2}, \frac{\pi}{2}] \to R$ is not surjective, but injective.
d) The function $sin: [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ is bijective.

Verify 1) – d) and draw their graphs.

Note. Instead of surjective, injective, bijective we say also respectively surjection, injection, bijection.

Exercise. Prove (show graphically) that the following functions are bijective:

1. $cosin: [0, \pi] \to [-1, 1],\ cosin(x) = cos\, x$,
2. $tan: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to R, tan(x) = tan\, x = sin\, x / cos\, x$,
3. $cot: (0, \pi) \to R,\ cot(x) = cot\, x = cos\, x / sin\, x$,
4. $exp_a: R \to R_+^*,\ exp_a(x) = a^x, (exp_e(x) = e^x)$,
5. $log_a: R_+^* \to R,\ log_a(x) = log_a\, x, (log_e(x) = ln\, x,)$.
6. $degr_n: R \to R,\ degr_n(x) = x^n,\ n \in N \text{ and } n \text{ is odd}$.
6. a) $degr_n: R_+ \to R_+,\ degr_n(x) = x^n,\ n \in N \text{ and } n \text{ is even}$.
6. b) $degr_n: R_- \to R_+,\ degr_n(x) = x^n,\ n \in N \text{ and } n \text{ is even}$.
7. $degr_n: R^* \to R^*,\ degr_n(x) = x^n,\ n \in Z_-^* \text{ and } n \text{ is odd}$.
7. a) $degr_n: R_+^* \to R_+^*,\ degr_n(x) = x^n,\ n \in Z_-^* \text{ and } n \text{ is even}$.
7. b) $degr_n: R_-^* \to R_+^*,\ degr_n(x) = x^n,\ n \in Z_-^* \text{ and } n \text{ is even}$.

Remember: $Z_-^* = \{-1, -2, \dots\}$,
$R_- = \{x \in R | x \leq 0\}$, $R_+ = \{x \in R | x \geq 0\}$,
$R_-^* = \{x \in R | x < 0\}$, $R_+^* = \{x \in R | x > 0)\}$.

Exercise.
a) Let X, Y be finite sets with $card\ X = m, card\ Y = n$. Prove that: there exists a bijection $f: X \to Y \Leftrightarrow m = n$.

b) Let X, Y be finite sets with $card\ X = card\ Y = n$.
Prove that the set of all bijections $\mathcal{F}_{bij}(X, Y)$ is finite too and $card\ \mathcal{F}_{bij}(X, Y) = P_n = n!$

3.8.4. Inverse function.
Definition. Let $f: X \to Y$ be bijection. Then for each $y \in Y$ there exists (because f is surjection) exactly one (because f is injection) preimage $x \in X$ such that $f(x) = y$. This defines a function which we denote by $f^{-1}: Y \to X$ and call **inverse function** of f.

So, according to the definition:

$$\begin{cases} x \in X \\ y = f(x) \end{cases} \Leftrightarrow \begin{cases} y \in Y \\ x = f^{-1}(y) \end{cases}$$

Since any bijection has its inverse function, then it is called also **invertible** function.

Reminder. Do not confuse compositional degree f^{-1} with the multiplicative one $\frac{1}{f}$!

3.8.5. Properties of the inverse function:
1. Inverse function $f^{-1}: Y \to X$ is obviously bijective and is defined uniquely.
2. Inverse of inverse is the origin function f, i.e. $(f^{-1})^{-1} = f$.
3. $f^{-1} \circ f = I_X$, i.e. $\forall x \in X \;\; f^{-1}[f(x)] = x$ and
$f \circ f^{-1} = I_Y$, i.e. $\forall y \in Y \;\; f[f^{-1}(y)] = y$.
4. $D(f^{-1}) = Ran\ (f) = Y,\ Ran\ (f^{-1}) = D(f) = X$.

Exercise. Prove that the property 3 is the characteristic property of the inverse function in the following sense. If for a function $f: X \to Y$ there exists a function $g: Y \to X$ such that $g \circ f = I_X$ and $f \circ g = I_Y$, then f is bijective and $g = f^{-1}$.

Examples:
1. $I_X: X \to X$ is bijective and $I_X^{-1} = I_X$.
2. Since the function $sin: [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ is bijective then there exists its **principal inverse** function $sin^{-1}: [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, denoted by $arcsin$. So,

$$\begin{cases} x \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \\ y = sin\ x \end{cases} \Leftrightarrow \begin{cases} y \in [-1, 1] \\ x = arcsin\ y \end{cases}$$

3. By analogy, we define the other inverse functions

1) $cos^{-1} = arccos: [-1, 1] \to [0, \pi]$ - **principal** inverse

$$\begin{cases} x \in [0, \pi] \\ y = cos\ x \end{cases} \Leftrightarrow \begin{cases} y \in [-1, 1] \\ x = arccos\ y \end{cases}$$

2) $tan^{-1} = arctan: R \to (-\frac{\pi}{2}, \frac{\pi}{2})$ - **principal** inverse

$$\begin{cases} x \in (-\frac{\pi}{2}, \frac{\pi}{2}) \\ y = tan\ x \end{cases} \Leftrightarrow \begin{cases} y \in R \\ x = arctan\ y \end{cases}$$

3) $cot^{-1} = arccot: R \to (0, \pi)$ - **principal** inverse

$$\begin{cases} x \in (0, \pi) \\ y = cot\ x \end{cases} \Leftrightarrow \begin{cases} y \in R \\ x = arccot\ y \end{cases}$$

4) $exp_a^{-1} = log_a: R_+^* \to R$

$$\begin{cases} x \in R \\ y = a^x \end{cases} \Leftrightarrow \begin{cases} y \in R_+^* \\ x = log_a\ y \end{cases}$$

$(y = e^x \Leftrightarrow x = ln\ y)$

5) $log_a^{-1} = exp_a: R \to R_+^*$

$$\begin{cases} x \in R_+^* \\ y = log_a\ x \end{cases} \Leftrightarrow \begin{cases} y \in R \\ x = a^y \end{cases}$$

$(y = ln\ x \Leftrightarrow x = e^y)$

6) $degr_n^{-1} = \sqrt[n]{} : R \to R,$ *if* $n \in N$ *and* n *is odd*

$$\begin{cases} x \in R \\ y = x^n \end{cases} \Leftrightarrow \begin{cases} y \in R \\ x = \sqrt[n]{y} \end{cases}$$

6) a) $degr_n^{-1} = \sqrt[n]{} : R_+ \to R_+,$ *if* $n \in N$ *and* n *is even*

$$\begin{cases} x \in R_+ \\ y = x^n \end{cases} \Leftrightarrow \begin{cases} y \in R_+ \\ x = \sqrt[n]{y} \end{cases}$$

6) b) $degr_n^{-1} = \sqrt[n]{} : R_+ \to R_-,$ *if* $n \in N$ *and* n *is even*

$$\begin{cases} x \in R_- \\ y = x^n \end{cases} \Leftrightarrow \begin{cases} y \in R_+ \\ x = -\sqrt[n]{y} \end{cases}$$

7) $degr_n^{-1} = \sqrt[n]{} : R^* \to R^*,$ *if* $n \in Z_-$ *and* n *is odd*

$$\begin{cases} x \in R^* \\ y = x^n \end{cases} \Leftrightarrow \begin{cases} y \in R^* \\ x = \sqrt[n]{y} \end{cases}$$

7) a) $degr_n^{-1} = \sqrt[n]{} : R_+^* \to R_+^*,$ *if* $n \in Z_-$ *and* n *is even*

$$\begin{cases} x \in R_+^* \\ y = x^n \end{cases} \Leftrightarrow \begin{cases} y \in R_+^* \\ x = \sqrt[n]{y} \end{cases}$$

7) b) $degr_n^{-1} = \sqrt[n]{} : R_+^* \to R_-^*,$ *if* $n \in Z_-$ *and* n *is even*

$$\begin{cases} x \in R_-^* \\ y = x^n \end{cases} \Leftrightarrow \begin{cases} y \in R_+^* \\ x = -\sqrt[n]{y} \end{cases}$$

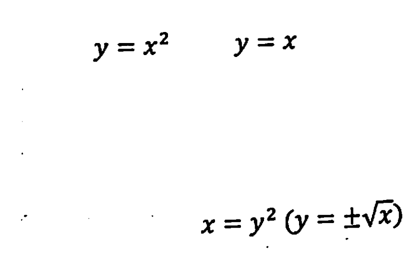
Note1. As we know any binary relation from X to Y is invertible, i.e. has an inverse relation. Then why a function from X to Y, being a special case of the relation is not always invertible? The answer is simple. If a function is not bijective, it is not invertible as a function, the inverse doesn't exist. But any function from X to Y considered as a binary relation has its inverse relation which is not a function if original function is not bijective.

Example 1. Let C be a set of all children, W be a set of all women and the function $f: C \to W$ assigns for **each** child from C his/her **unique** mother from W.

The inverse of this function doesn't exist for two possible reasons: either a women from W has no children or has several children. Nevertheless, if f considered as a relation from C to W "to be child of the mother" then the inverse relation f^{-1} (not a function!) from W to C "to be mother of" exists.

Example 2 (see inverse relations). Let $f: R \to R_+,\ f(x) = x^2$. Obviously this function is a surjection, but not an injection because $(-x)^2 = x^2$, so f is not bijection and has no inverse function f^{-1}. But as a binary relation f has an inverse relation

$f^{-1}: R_+ \to R,\ f^{-1}(x) = \pm\sqrt{x}$, which is shown on the graph below.



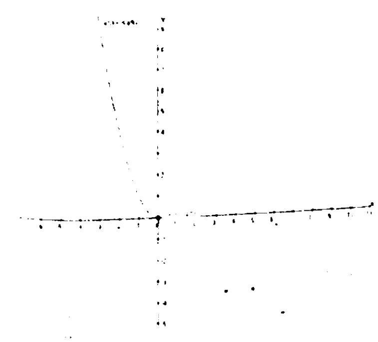
But if we consider the following two restrictions of this function:

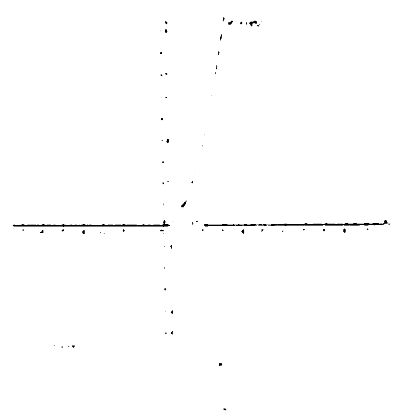
$f_l: R_- \to R_+,\ f_l(x) = x^2$ and $f_r: R_+ \to R_+,\ f_r(x) = x^2$,

then they are bijective and invertible:

$f_l^{-1}: R_+ \to R_-,\ f_l^{-1}(x) = -\sqrt{x};\quad f_r^{-1}: R_+ \to R_+,\ f_r^{-1}(x) = \sqrt{x}$.

Here below you can see the graphs of these functions (blue) with their inverses (green) symmetric with respect to the diagonal $y = x$ (red) respectively on the left and on the right.





3.8.6. Inverse of an involution.

Theorem. Any involution $f: X \to X$ is bijective and $f^{-1} = f$.
Proof. Really, according the definition of involution $f^2 = I_E$ or $f \circ f = I_E$. Consequently according to the 3rd property of the inverse function $f^{-1} = f$.

Corollary. This theorem allows us to define involution as an invertible function whose inverse coincide with the original: $f^{-1} = f$.

3.8.7. Graph of an inverse function.

Definition. Let $f: X \to Y$ and $f^{-1}: Y \to X$ mutually inverse functions. Their graphs, by definition, are:

$$Grf = \{(x, y) \in X \times Y | y = f(x)\} \subseteq X \times Y,$$

$$Grf^{-1} = \{(y, x) \in Y \times X | x = f^{-1}(y)\} = \{(y, x) \in Y \times X | y = f(x)\} \subseteq Y \times X.$$

We repeat here once again all that was said for the graphs of binary relations.

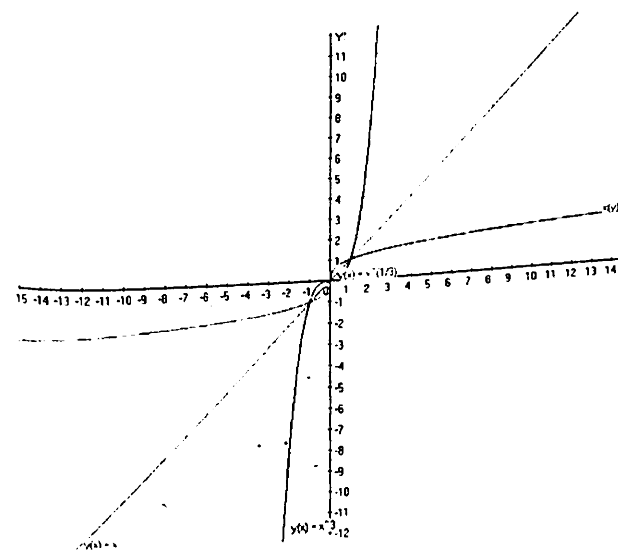
Note. For graphs of original functions and their inverses we can repeat literally the same as for the graphs of binary relations. The graphs $Gr\, f$ and Grf^{-1} are included in different sets $X \times Y$ and $Y \times X$ respectively. When we use Cartesian coordinate system on the plan to represent them we find that these graphs coincide. And it is natural contrary to the widespread mistake in mathematical textbooks where these graphs must be symmetric relatively the bisector of the 1st and 3rd quadrants. We will try here to understand this misconception. If we use the horizontal axis for the set X and the vertical axis for the set Y and draw both graphs, of course they coincide. However, if the sets X and Y are both of the "same nature" and if there exists a set S such that $X \subseteq S$ and $Y \subseteq S$ (in particular, if $X = Y = S$), then $X \times Y,\ Y \times X \subseteq S^2;\ Grf, Grf^{-1} \subseteq S^2$. And only in this case we can draw both graphs in the same coordinate system differently. Namely, using for $Gr\, f$ horizontal axis for the set X and the vertical axis for the set Y, **but** for the $Gr\, f^{-1}$ horizontal axis for the set Y and the vertical axis for the set X, we receive two different graphs on the same plan drawing:

$$Grf = \{(x, y) \in S^2 \,| x \in X \wedge y = f(x)\} = \{(x, f(x)) \in S^2 | x \in X\}$$
$$Grf^{-1} = \{(y, x) \in S^2 | y \in Y \wedge y = f(x)\} = \{(f(x), x) \in S^2 | x \in X\}.$$

The points $(x, y) \in S^2$ and $(y, x) \in S^2$ are called symmetric with respect the diagonal $D = \{(x, y) \in S^2 | x = y\}$. Therefore, the graphs $Gr(f)$ and $Gr(f^{-1})$ are also called symmetric with respect to the diagonal D as we see in examples above and bellow.

Example. Consider $f: R \to R,\ y = f(x) = x^3$.

Its inverse $f^{-1}: R \to R,\ x = f^{-1}(y) = \sqrt[3]{y} = y^{\frac{1}{3}}$. The graphs of f and f^{-1} on the plan in the coordinate system XOY are coincide of course. But if instead of the function $x = \sqrt[3]{y}$ we consider the function $y = \sqrt[3]{x}$ we will see that the graphs of $y = x^3$ (blue) and $y = \sqrt[3]{x}$ (green) are symmetric with respect to the diagonal $D = \{(x, y) \in R^2 | y = x\}$ or briefly with respect to the straight line $y = x$ (red).



3.8.8. Graphs of the involutions.

Since for the involutions $f = f^{-1}$, their graphs coincide. On the other hand, they must be symmetric with respect to the

line $y = x$. Therefore the graphs of the involutions themselves are symmetric with respect to the line $y = x$.

Exercise. Graphs of involutions.
Consider the followings involutions and draw their graphs
a) Involution $f: R^* \to R^*,\ f(x) = \frac{1}{x},\ f^{-1}: R^* \to R^*, f^{-1}(x) = \frac{1}{x}$.
b) Involution $f: R \to R,\ f(x) = -x,\ f^{-1}: R \to R,\ f^{-1}(x) = -x$.

3.8.9. Permutations.

Definitions. Bijection $f: X \to X$ is called permutation of X.
We denote the set of all permutations of X by $P(X)$.

It follows directly from the definition that:
1. $f, g \in P(X) \Rightarrow g \circ f \in P(X),\ f \circ g \in P(X)$
2. $f \in P(X) \Rightarrow f^{-1} \in P(X)$ and $f \circ f^{-1} = f^{-1} \circ f = I_X$

Examples: Draw the graphs.
1. Permutation of R:
   $f: R \to R,\ f(x) = x^n,\ n \in N \text{ and } n \text{ is odd.}$
2. Permutation of R^*:
   $f: R^* \to R^*,\ f(x) = x^n,\ n \in Z_-^* \text{ and } n \text{ is odd.}\ (Z_-^* = \{-1, -2, \dots\})$.
3. Permutation of: R_+:
   $f: R_+ \to R_+, f(x) = x^n, n \in N \text{ and } n \text{ is even.}$
4. Permutation of: R_+^*:
   $f: R_+^* \to R_+^*, f(x) = x^n, n \in Z_-^* \text{ and } n \text{ is even.}$

3.8.10. Negative compositional powers of a permutation.

Above for a function $f: X \to X$ we defined non-negative powers of f.

If f is a permutation, i.e. if f is bijective we can define negative compositional powers of f. Since $(f^n)^{-1} = (f \circ f \circ \dots \circ f)^{-1} = f^{-1} \circ \dots \circ f^{-1} \circ f^{-1} = (f^{-1})^n$, then $(f^n)^{-1} = (f^{-1})^n$. So, we can define negative compositional powers as follows: $f^{-n} = (f^n)^{-1} = (f^{-1})^n$. Thus, compositional powers f^n of permutation f are defined for all $n \in Z$.

3.8.11. Permutations of finite sets.

Let $X = (a_1, a_2, \dots, a_n)$ be a finite set with n elements ordered by the indexes of their elements. Since we are not interested in the nature of the elements of X, then without loss of generality we denote it by $X = (1, 2, \dots, n)$. Let $f: X \to X$ be a permutation of X. We will write this permutation as a table with two rows in which the first consist of inputs from X, and the second row consist of their corresponding images under f: $i_1 = f(1), i_2 = f(2), \dots, i_n = f(n)$:

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

These permutations functions one-to-one correspond to the permutations of sets without repetition considered in combinatorics. So, the number of all such permutation functions is equal to permutations of the set X and, as we know from combinatorics is equal to $P_n = n!$

Identity permutation of X has the form

$$I_X = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Composition of permutations and inverse permutation are defined naturally.
We'll show them by the next example.

Example. Let $X = (1, 2, 3)$,

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

Then,

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

Do not forget that in composition $g \circ f$ the function which maps permutation is f and the second is g. Therefore to find the composition it is convenient to use an intermediate step like follows:

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix}$, where the second line is from f and the third line is obtained by taking into account g. So, finally $1 \mapsto 3 \mapsto 3,\ 2 \mapsto 1 \mapsto 2,\ 3 \mapsto 2 \mapsto 1$.

By analogy,

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

It is easy to find inverse permutation for f. Really, if $f: 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$ then $f^{-1}: 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1$, hence

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Verify that

$$f \circ f^{-1} = f^{-1} \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I_X.$$

Exercises 3.8.

1. Prove that the **composition of two surjections is a surjection**.

2. Prove that the **composition of two injections is also an injection**.

3. **Composition of two bijections is also a bijection.**
Let $f: X \to Y,\ g: Y \to Z$ be bijections. Prove that :
a) $(g \circ f): X \to Z$ is bijection, i.e. is invertible $(g \circ f)^{-1}: Z \to X$
b) $\boxed{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$
c) Generalize the result: if
$f_1: X_1 \to X_2, f_2: X_2 \to X_3, \dots, f_n: X_n \to X_{n+1}$ are bijective functions, then the composition $f_n \circ \dots \circ f_2 \circ f_1$ is a bijection from X_1 to X_n
and $(f_n \circ \dots \circ f_2 \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1} \circ \dots \circ f_n^{-1}$ is a bijection from X_n to X_1.
d) Consider example
$tan: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to R,\ y = tan\, x;\ \ exp: R \to R_+^*,\ \ z = e^y$. Prove that
$(exp \circ tan): \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to R_+^*,\ z = (exp \circ tan)(x) = e^{tan x}$ is bijection and
$(exp \circ tan)^{-1} = (tan)^{-1} \circ (exp)^{-1} = (arctan \circ ln)$. i.e.
$x = (exp \circ tan)^{-1}(z) = (arctan \circ ln)(z) = arctan\, ln\, z.$

4. Let X, Y be finite sets with $card\, X = m, card\, Y = n$. Prove that:
there exists a surjection $f: X \to Y \Leftrightarrow m \geq n$.

5. Let X be finite set and $f: X \to X$. Prove that f is surjection $\Leftrightarrow$ f is injection.

5. Let X, Y be finite sets with $card\, X = m,\ card\, Y = n$.
Prove that there exists an injection $f: X \to Y \Leftrightarrow m \leq n$.

6. Let X, Y be finite sets with $card\, X = m, card\, Y = n$.
Prove that the set of all injections $\mathcal{F}_{inj}(X, Y)$ is finite too and

$$\boxed{card\, \mathcal{F}_{inj}(X, Y) = A_n^m = n(n-1)(n-2) \cdot \dots \cdot (n-m+1) = \frac{n!}{(n-m)!}}$$

7. Show that the following functions are injective (i.e. one-to-one):
a) $f: R \to R, f(x) = 2x + 1$
b) $f: R \to R, f(x) = ax + b, a \in R^*, b \in R$
c) $f: R^* \to R, f(x) = \frac{1}{x}$
d) $f: R - \{1\} \to R, f(x) = \frac{x+1}{x-1}$
e) $f: (-1, 1) \to R, f(x) = \frac{x}{1+x^2}$
f) $f: R \to R, f(x) = x^3$
g) $f: N \to N, f(x) = x^2$
h) $f: N \to N, f(x) = 2^x$

8. Show that the following functions are not injective
a) $f: R \to R, f(x) = x^2$
b) $f: R \to R, f(x) = |x|$
c) $f: R \to R, f(x) = x^3 - x$

9. For all the functions in ex. 7 above:
a) find the range of the function
b) decide in each case whether the function is surjective (i.e. is onto).

10. Let $f: X \to Y,\ \ g: Y \to Z$. Prove that:
a) $g \circ f$ is injective $\Rightarrow f$ is injective,
b) $g \circ f$ is surjective $\Rightarrow g$ is surjective.

11. Show that the following functions are bijective and in each case find their inverses:
a) $f: R \to R,\ f(x) = ax + b,\ a \in R^*, b \in R,$
b) $g: R \to R,\ g(x) = x^3 - 1,$
c) $h: R - \{1\} \to R - \{1\},\ h(x) = \frac{x+1}{x-1}.$
Prove that $h = h^{-1}, i.e.\ h$ is an involution.

3.9. Image and Preimage of Sets.

3.9.1. Function $f_*:\mathcal{P}(X) \to \mathcal{P}(Y)$.

Definition. Let $f: X \to Y$ be a function and $A \subseteq X$ be a subset.

The image of A under the function f is the set of the images $f(x)$ of all $x \in A$:

$$f(A) = \{f(x) \in Y | x \in A\} \subseteq Y.$$

Thus for each subset of $A \subseteq X$, i.e. for each element $A \in \mathcal{P}(X)$ the function f assigns an element $f(A) \in \mathcal{P}(Y)$ and thereby define a new function

$f_*: \mathcal{P}(X) \to \mathcal{P}(Y)$.

In particular, if $A = X$, then $f(X) = Im\, f = Ran f$.

The function $f_*: \mathcal{P}(X) \to \mathcal{P}(Y)$ is not generally bijective and therefore is not invertible. However, there exists **always** a function from $\mathcal{P}(Y)$ to $\mathcal{P}(X)$ which is conventionally called the "inverse function" of f_*, denoted by

$f_*^{-1}: \mathcal{P}(Y) \to \mathcal{P}(X)$ and defined as follows:

$$\forall \boldsymbol{B} \in \mathcal{P}(\boldsymbol{Y})\ (\boldsymbol{i.e.} \boldsymbol{B} \subseteq \boldsymbol{Y})\ \boldsymbol{f_*^{-1}(B)} = \{\boldsymbol{x} \in \boldsymbol{X} | \boldsymbol{f(x)} \in \boldsymbol{B}\} \in \mathcal{P}(\boldsymbol{X}).$$

Since $f_*^{-1}(B) \subseteq X$, then it is called **preimage** of the set $B \subseteq Y$.

Note that thus defined function f_* is always surjective, since $\forall B \in \mathcal{P}(Y)$ preimage $f_*^{-1}(B)$ is always exists as an element of $\mathcal{P}(X)$, even if $f_*^{-1}(B) = \emptyset \in \mathcal{P}(X)$.

In particular, for each $y \in Y$ (or for each $\{y\} \in \mathcal{P}(Y)$) the subset $f_*^{-1}(\{y\}) \subseteq X$(may be empty) is the set of all preimages of $y \in Y$.

It is obvious, that the original function $f: X \to Y$ is surjective iff $\forall y \in Y$ $f_*^{-1}(\{y\}) \neq \emptyset$, is injective iff $\forall y \in f(X)$ $f_*^{-1}(\{y\})$ consists of exactly one element $x \in X$, and is bijective iff $\forall y \in Y$ $f_*^{-1}(\{y\})$ consists of exactly one element $x \in X$.

Note. Often in practice the function f_* is denoted, without ambiguity, by the same letter f. So, henceforth, for simplicity, we often write $f^{-1}(B)$ meaning $f_*^{-1}(B)$. In particular, we write $f^{-1}(y)$ meaning $f_*^{-1}(\{y\})$.

Obviously, if f is not bijective then the real f^{-1} doesn't exist.

But even if f is bijective and f^{-1} exists, do not forget that f and f_* are the different functions.

Examples:

1. The function $f: R \to R,\ f(x) = x^2$
   is not surjective: $f(R) = R_+ \neq R$,
   is not injective: $\forall y \in R_+^*$ there are **two** preimages:
   $f^{-1}(y) = \{-\sqrt{y}, +\sqrt{y}\}$.
2. Consider again the example already studied.
   Let C be a set of all children, W be a set of all women and the function $f: C \to W$ assigns for each child from C his/her unique mother from W. As we know this function is neither surjective nor injective, so is not bijective and the set $f^{-1}(w)$ for some $w \in W$ is the set of all children of the same mother, which may be empty if w has no children or may contain several children of this mother.
3. The function $sin: R \to R,\ f(x) = sin\, x$
   is not surjective: $sin(R) = [-1, 1] \neq R$,
   is not injective: $\forall a \in [-1, 1]$ there are an **infinite** number of preimages:
   $sin^{-1}(a) = Arcsin\, a = (-1)^n arcsin\, a + n\pi,\ n \in Z$.
   Remember that $sin^{-1}(a) = Arcsin\, a$ is used here as a notation of the set of all preimages of $a \in [-1, 1]$, and $arcsin\, a$ is the *"principal value"* $\in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ of the principal inverse $arcsin$ at point a.

Exercises 3.9.

1. Verify other trigonometric formulas:
$\forall a \in [-1, 1]$ there are an **infinite** number of preimages:
$cos^{-1}(a) = Arccos\, a = \pm arccos\, a + 2n\pi,\ n \in Z,\ arccos\, a \in [0, \pi]$,
$\forall a \in R$ there are an **infinite** number of preimages:
$tan^{-1}(a) = Arctan\, a = arctan\, a + n\pi,\ n \in Z,\ arctan\, a \in (-\frac{\pi}{2}, \frac{\pi}{2})$,
$\forall a \in R$ there are an **infinite** number of preimages:
$cot^{-1}(a) = Arccot\, a = arccot\, a + n\pi,\ n \in Z,\ arccot\, a \in (0, \pi)$.
2. **Properties of images and preimages under a function (mapping)** f.
Prove the following properties:
I. Let $A \subseteq X,\ B \subseteq X$. Then:
1. $A = \emptyset \Leftrightarrow f(A) = \emptyset$,
2. $A \subseteq B \Rightarrow f(A) \subseteq f(B)$,
3. $f(A \cup B) = f(A) \cup f(B)$.
4. $f(A \cap B) \subseteq f(A) \cap f(B)$.
II. Let $A \subseteq Y,\ B \subseteq Y$. Then:

5. $A \subseteq B \Rightarrow f^{-1}(A) \subseteq f^{-1}(B)$,
6. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$,
7. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$,
8. $f^{-1}(C_Y B) = C_X f^{-1}(B)$.

Note that if $f: X \to Y$ is bijective, then the properties of f and f^{-1} relatively the subsets from X and Y are equivalent, e.g. $f(A \cap B) = f(A) \cap f(B)$.

3.10. Canonical decomposition of functions. Solution of the equation $f(x) = y$. General and particular solutions.

3.10.1. Canonical surjection.

Theorem. Let X be a set and $\sim$ be an equivalence relation on X and $X/\sim$ is the quotient set of the set X with respect to an equivalence relation $\sim$.

Then the function $g: X \to X/\sim,\ g(a) = \bar{a}$ is surjection.

Proof. Really, every $\bar{a} \in X/\sim$ is not empty because it contains at least the element $a \in X$ by the definition of the class $\bar{a}$. So, the function g is **surjective**, but in general, is not injective.

Definition. The function $g: X \to X/\sim,\ g(a) = \bar{a}$ is called a **canonical** (or **natural**) **surjection.**

3.10.2. Relation "the same image".

Definition. Let $f: X \to Y$. The binary relation ρ_f on X (from X to X) defined as follows:

$$a\rho_f b \Leftrightarrow f(a) = f(b)$$

is called relation **"the same image"**.

Sometimes this relation is called **"Kernel of a function f"** and denoted by $\boldsymbol{Ker\, f}$.

Theorem. The relation "the same image" is the equivalence relation.

Proof is obvious:

1. Reflexivity : $f(a) = f(a)$
2. Symmetry: $f(a) = f(b) \Rightarrow f(b) = f(a)$
3. Transitivity: $f(a) = f(b) \wedge f(b) = f(c) \Rightarrow f(a) = f(c)$■

As ρ_f is an equivalence relation, then X/ρ_f is a quotient set is a family of the equivalence classes, each of which consist of elements having the same image in Y under f.

Function $g: X \to X/\rho_f$ is of course a particular case of the canonical surjection.

Examples:

1. Let $f: R \to R,\ f(a) = a^2$. Each equivalence class $\bar{a}$ is the subset in R consisting of two elements $\bar{a} = \{-a, a\}$, if $a \neq 0$ and $\bar{0} = \{0\}$.

The quotient set $R/\rho_f = \{\bar{a} \mid a \in R\}$.

The function $g: R \to R/\rho_f,\ g(a) = \bar{a}$ is a canonical surjection.

2. Let $f: R \to R,\ f(a) = tan\ a$. Each equivalence class $\bar{a}$ is the subset in R consisting of an infinite number of elements $\bar{a} = \{a + n\pi \mid n \in Z\}$.

The quotient set $R/\rho_f = \{\bar{a} \mid a \in R\}$.

The function $g: R \to R/\rho_f,\ g(a) = \bar{a}$ is a canonical surjection.

3.10.3. Canonical injection.

Definition. Let $f: X \to Y$. The function $\tilde{f}: X/\rho_f \to Y,\ \tilde{f}(\bar{a}) = f(a)$ is called **canonical injection** corresponding to the function f.

By the definition of the equivalence class $\bar{a}$ the value of $\tilde{f}(\bar{a}) = f(a)$ doesn't depend on the choice of representative of a from the class $\bar{a}$, i.e. the function $\tilde{f}$ is correctly defined. Injectivity of the $\tilde{f}$ is obvious by its definition.

Examples:

In the examples above: 1. $\tilde{f}(\bar{a}) = a^2$, 2. $\tilde{f}(\bar{a}) = tan\ a$.

3.10.4. Canonical Decomposition (factorization) of functions.

Any function $f: X \to Y$ can be represented as a composition of a surjection and an injection:

$$f = \tilde{f} \circ g,$$

where $X \xrightarrow{g} X/\rho_f \xrightarrow{\tilde{f}} Y$.

If instead of Y we consider its subset $f(X) \subseteq Y$, then the function

$\tilde{f}: X/\rho_f \to f(X)$ will be bijective and invertible: $\tilde{f}: f(X) \to X/\rho_f$ and the equation $\tilde{f}(\bar{x}) = y$ will have one and only one solution for all $y \in f(X)$.

3.10.5. Solution of the equation $f(x) = y$. General and particular solutions.

Let $f: X \to Y$. To solve the equation

$$f(x) = y, \qquad (1)$$

where $y \in Y$ is fixed element, is to find the set of all its preimages $f^{-1}(\{y\}) \subseteq X$.

The set $f^{-1}(\{y\})$ is called a **set of all solutions** or **general solution** of (1).

An arbitrary element of $f^{-1}(\{y\})$ is called **particular solution** of (1).

If $y \notin Im\, f$ ($Im\, f = Ran\, f = f(X)$), then the set of all solutions $f^{-1}(\{y\})$ is obviously empty and we say that the **equation (1) has no solution in X.**

If $y \in Im\, f$, then the set $f^{-1}(\{y\})$ is not empty and the **equation (1) has a solution in X.** Obviously, **if $x \in f^{-1}(\{y\})$ is a particular solution, then the general solution is $f^{-1}(\{y\}) = \bar{x}$**, where $\bar{x}$ is the equivalence class of the element x when X is partitioned by the relation ρ_f.

If $f^{-1}(\{y\})$ is a singleton, i.e. $\bar{x} = x$, then we say that the **solution of the equation (1) is unique.**

Note. From what was said it follows that:

If f is surjective $Im\, f = Y$, then the **equation (1) has at least one solution for all $y \in Y$.**

If f is injective, then **equation (1) either has no solution** (if $y \notin Im\, f$) or **has exactly one solution** (if $y \in Im\, f$).

If f is bijective, then there exists inverse function $f^{-1}: Y \to X$ and the equation (1) has exactly one solution $x = f^{-1}(\{y\}) = f^{-1}(y)$ for all $y \in Y$.

Examples:

1. Let $f: R \to R,\ f(x) = x^2$.
Equivalence class of the element x is $\bar{x} = \{-x, x\}$. Here $Im\, f = R_+$.
The equation $x^2 = y$ has no solutions if $y \notin R_+$, (i.e. if $y \in R_-^*$).
If $y \in R_+$, then the equation $x^2 = y$ has the general solution
$\bar{x} = f^{-1}(\{y\}) = \{-\sqrt{y}, \sqrt{y}\}$ consisting of two particular solutions $-\sqrt{y}$ *and* $\sqrt{y}$. (which coincide if $y = 0$). If we consider the restriction of f, for example, on R_+ (R_-), then the equation $x^2 = y$ has the unique solution $\sqrt{y}$ ($-\sqrt{y}$) $\forall y \in R_+$.

2. Let $f: R \to R,\ f(x) = \sin x$.
Equivalence class of the element x is $\bar{x} = \{(-1)^n x + n\pi | n \in Z\}$.
Here $Im\, f = [-1, 1]$.
The equation $\sin x = y$ has no solutions if $y \notin [-1, 1]$.
If $y \in [-1, 1]$, then the equation $\sin x = y$ has the general solution
$\bar{x} = f^{-1}(\{y\}) = \{(-1)^n \arcsin y + n\pi | n \in Z\}$ consisting of the infinite number of particular solutions. If we consider the restriction of f, for example, on $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$,
then the equation $\sin x = y$ has the unique solution $x = \arcsin y$ $\forall y \in [-1, 1]$.

3.11. Morphisms and Isomorphisms.

Notation. A set X, with a binary relation ρ defined on it, is denoted as an ordered pair (X, ρ).

3.11.1. Morphism.

Definition. Let (X, ρ) and $(Y, \mathcal{R})$ be sets with binary relations on them. A function $f: X \to Y$ is called **morphism** from (X, ρ) to $(Y, \mathcal{R})$, if

$$\forall\, a, b \in X \quad a\, \rho\, b \Rightarrow f(a)\, \mathcal{R}\, f(b) \qquad (2)$$

We say that morphism f **preserves the relations** and we write $f: (X, \rho) \to (Y, \mathcal{R})$.

3.11.2. Isomorphism.

Definition. Let (X, ρ) and $(Y, \mathcal{R})$ be sets with binary relations on them. A function $f: X \to Y$ is called **isomorphism**, if f is bijective, f and f^{-1} are morphisms.

In other words if:

1. f is bijective,

2. f is a morphism from (X,ρ) to $(Y,\mathcal{R})$: $\forall a,b \in X \quad a\,\rho\, b \Rightarrow f(a)\,\mathcal{R}\, f(b)$,

3. f^{-1} is a morphism from $(Y,\mathcal{R})$ to (X,ρ): $\forall A,B \in Y \ A\mathcal{R}B \Rightarrow f^{-1}(A)\rho f^{-1}(B)$.

We say that the pairs (X,ρ) and $(Y,\mathcal{R})$ are **isomorphic** and we write $(X,\rho) \leftrightarrow (Y,\mathcal{R})$ if there exits an isomorphism $f:(X,\rho) \rightarrow (Y,\mathcal{R})$.

Exercise. Prove that the 2nd and 3rd conditions in the definition above can be replaceable by the next one:

$$\forall a,b \in X \quad a\,\rho\, b \Leftrightarrow f(a)\,\mathcal{R}\, f(b).$$

Exercises:

1. Prove that an isomorphism is an equivalence relation on the set of all pairs (X,ρ).

2. Let $f: X \rightarrow Y$ be a bijection and ρ be a binary relation on X. Define a binary relation $\mathcal{R}$ on Y **induced** by the relation ρ on X as follows:

$\forall A,B \in Y \ A\mathcal{R}B \Leftrightarrow f^{-1}(A)\rho f^{-1}(B)$.

Prove that (X,ρ) and $(Y,\mathcal{R})$ are isomorphic.

Prove that if ρ is an equivalence relation (or an order relation), then and $\mathcal{R}$ is an equivalence relation (or an order relation) too.

The definitions of a morphism and an isomorphism are naturally generalized on the n-ary relations.

Let $\rho,\mathcal{R}$ be n-ary relations defined on $X = X_1 \times X_2 \times \dots \times X_n$ and Y (Y can be Cartesian product too) respectively.

A function $f: X \rightarrow Y$ is called morphism if

$$\forall (a_1, \dots, a_n) \in X \quad \rho(a_1, \dots, a_n) \Rightarrow \mathcal{R}\,(f(a_1), \dots, f(a_n))$$

If in additional, f is bijective and

$$\forall (a_1, \dots, a_n) \in X \quad \rho(a_1, \dots, a_n) \Leftrightarrow \mathcal{R}\,(f(a_1), \dots, f(a_n)),$$

then f is called isomorphism.

3.11.3. Algebraic structure.

Definition. The most important case of the n-ary relations for the algebra is the ternary ($n = 3$) functional relation $(*): \ X \times X \rightarrow X$ which is called **binary operation** on X and $\forall (a,b) \in X \times X$ assigns a unique element $c \in X$ denoted by $c = a * b$.

The set X with the binary operation $*$ is called **algebraic structure** and denoted as an ordered pair $(X, \ *)$.

Algebraic structures from magmas to fields and linear spaces will be studied in the next volume devoted to algebra. Now, here bellow we give only few examples of algebraic structures. Instead of $(a,b) \in X \times X$ we write often $(a,b) \in X^2$ or $a,b \in X$.

Examples:

1. $(N,+)$, really $\forall a,b \in N \quad a+b = c \in N$,
2. $(Z, \ \cdot)$, really $\forall a,b \in Z \quad a \cdot b = c \in Z$.

3.11.4. Morphism and Isomorphism of Algebraic structures.

Definition. Let $(X, \ *), (Y, \ \odot)$ be two algebraic structures.

A function $f: X \rightarrow Y$ is called **morphism** if

$$\boldsymbol{\forall a,b \in X \ \ f(a * b) = f(a) \odot f(b).}$$

If in additional, f is bijective it is called **isomorphism** and the structures $(X, \ *), (Y, \ \odot)$ are called **isomorphic**.

Obviously, if f is an isomorphism from $(X, \ *)$ to $(Y, \ \odot)$, then inverse function f^{-1} is the isomorphism from $(Y, \ \odot)$ to $(X, \ *)$.

We say also that morphism (or isomorphism) f **preserves the operations.**

Examples:

1. Prove that the structures $(R,+)$ and $(R_+^*, \ \cdot)$ are isomorphic.

Solution. Consider the function $f: R \rightarrow R_+^*, \ f(x) = exp(x) = e^x$.

Then f is the isomorphism. Really:

$\forall a,b \in R \quad exp(a+b) = e^{a+b} = e^a \cdot e^b = exp(a) \cdot exp(b)$.

The inverse function $f^{-1}: R_+^* \rightarrow R, \ f^{-1}(x) = \ln(x)$ is the inverse isomorphism:

$$\forall a,b \in R_+^* \quad ln(a \cdot b) = ln(a) + ln(b)$$

2. Consider two structures $(R, \ \cdot)$ *and* $(R_+, \ \cdot)$.

Then the function $f: R \rightarrow R_+ \quad f(x) = |x|$ is morphism. Really,

$\forall a,b \in R \quad f(a \cdot b) = |a \cdot b| = |a| \cdot |b| = f(a) \cdot f(b)$.

But this morphism is not isomorphism, because f is not bijective: $a \neq -a$ but $|a| = |-a|$.

Note. The deep meaning of morphisms $f:(X,\rho) \rightarrow (Y,\mathcal{R})$ (for relations) or

$f:(X, *) \to (Y, \odot)$ (for algebraic structures) is that they carry many of the properties of relations or operations from X (in the terms of ρ or $*$) to Y (in the terms of $\mathcal{R}$ or $\odot$). While the isomorphisms do the structures (X,ρ) and $(Y,\mathcal{R})$ or $(X, *)$ and $(Y, \odot)$ in this sense mathematically identical or indistinguishable despite the possible difference in their "physical" nature. So, establishing an isomorphism between the two structures, we work in a more comfortable one, get the results and then transfer them to the second.

Example. Slide Rule.

The slide rule as a mechanical analog computer was invented in 17th century and was used for multiplication and division and also for functions such as roots, and logarithms and trigonometry. It was based on the isomorphism from the example 1 above:

$$\forall a,b \in R_+^* \quad ln(a\cdot b) = ln(a) + ln(b).$$

The slide rule in its simplest form consisted of two wooden bars sliding relatively to each other with logarithmic scales on them. In order to find the product $a\cdot b$ we find $ln(a)$ on the 1st bar and $ln(b)$ on the 2nd. Then sliding the bars relatively to each other find $ln(a) + ln(b)$ which is equal to $ln(a\cdot b)$ according to the formula above. Finally, using inversely the logarithmic scale on the slide rule find the product $a\cdot b$. As we see due to this formula the operation of multiplication has been replaced by a more simple operation of addition.

Numerous examples of morphisms and isomorphisms of sets with binary relations , in particular ordered sets, will be given later in algebra and calculus.

Chapter 4.

MATHEMATICAL INDUCTION and COMBINATORICS.

4.1. Mathematical Induction.

4.1.1. The Principle of Mathematical Induction.

Theorem. Let p be a propositional form defined on N and satisfying the following two conditions:

1. $p(1)$ is true
2. $p(n-1) \Rightarrow p(n)\quad n \in \{2,3,\dots,n,\dots\} = N - \{1\}$

Then $p(n)$ is true $\forall n \in N$.

Example:

1. **Bernoulli's inequality**

Let $x \in R$ and $x > -1$. Prove that

$$\forall n \in N \quad (1+x)^n \geq 1 + nx$$

Proof.

Step 1. Really, if $n = 1$, then $(1+x)^1 \geq 1 + 1\cdot x$, i.e. $p(1)$ is true.

Step 2. Assume that $p(n-1)$ is true, i.e. $(1+x)^{n-1} \geq 1 + (n-1)x$.

Then $(1+x)^n = (1+x)^{n-1}(1+x) \geq (1+(n-1)x)(1+x) =$

$= 1 + nx + (n-1)x^2 \geq 1 + nx$, i.e. $p(n)$ is true, or $p(n-1) \Rightarrow p(n)$.

So, inequality is proved $\forall n \in N$.

2. Prove equality

$$1 + 3 + 5 + \dots + (2n-1) = n^2$$

Proof.

Step 1. $1 = 1^2$, $p(1)$ is true.

Step 2. Assume $p(n-1)$ is true, i.e.

$1 + 3 + 5 + \dots + [2(n-1) - 1] = (n-1)^2$. Then

$1 + 3 + 5 + \dots + [2(n-1) - 1] + (2n-1) = (n-1)^2 + (2n-1) = n^2$,

i.e. $p(n)$ is true or $p(n-1) \Rightarrow p(n)$. So, equality is true $\forall n \in N$.

Exercises:

1. Try to prove the Principle of Mathematical Induction.
2. Prove the theorem into the "negative" part $Z_- = \{0,-1,-2,\dots\}$:

"if $p(0)$ is true and $p(n) \Rightarrow p(n-1)$, then $p(n)$ is true for $\forall n \in Z_-$

Exercises 4.1.

Using Principle of Mathematical Induction prove, that for $\forall n \in N$:

1. $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

2. $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

3. $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$

4. $5^{2n} - 6n + 8$ is divisible by 9

5. $\mathit{Card}\, A = n \Rightarrow \mathit{Card}\, \mathcal{P}(A) = 2^n$

6. **Inclusion-exclusion Principle**:
Let $A_1, A_2, \ldots, A_n$ be finite sets.
Then the cardinality of the union of all these sets is:
$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n| -$
$-|A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_{n-1} \cap A_n| +$
$+|A_1 \cap A_2 \cap A_3| + \cdots + |A_{n-2} \cap A_{n-1} \cap A_n| + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|$
If, in particular $A_1, A_2, \ldots, A_n$ are pairwise disjoint sets, then
$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.

4.2. Combinatorics.

4.2.1. Allocations (or sampling, or arrangement) without repetitions (or replacements).

Definition. Let $S = \{a_1, a_2, \ldots a_n\}$ be a finite set with n pairwise distinct elements.

Any naturally **ordered subset** $(a_1, a_2, \ldots a_m) \subseteq S$ consisting **of m** $(1 \le m \le n)$ elements **from n** elements of S is called ***$m-$ allocation* of n without repetitions.**

(Sometimes it is called allocation of n different elements taken m at time).

Notation. The number of all m- allocations of n without repetitions is denoted by A_n^m.

Example 1:
Let $n = 3$, $S = \{a, b, c\}$.
Then 1, 2, 3 –allocations of 3 without repetitions elements are:

1 *of* 3: $(a), (b), (c)$ – 3 in total, so $A_3^1 = 3$.

2 *of* 3: $(a,b), (a,c)$,
$(b,a), (b,c)$,
$(c,a), (c,b)$ – 6 in total, so $A_3^2 = 6$.

3 *of* 3: $(a,b,c), (a,c,b)$,
$(b,a,c), (b,c,a)$,
$(c,a,b), (c,b,a)$ – 6 in total, so $A_3^3 = 6$.

Theorem 1.

$$\boxed{A_n^m = n(n-1)(n-2) \cdot \ldots \cdot (n-m+1)}$$

Proof is by Mathematical Induction on m when n is fixed.
Step 1. $m = 1$, $A_n^1 = n$. Really, in this case $S = \{a_1, a_2, \ldots a_n\}$,
1- allocations of n are $(a_1), (a_2), \ldots, (a_n)$ – n in total.
Step 2. Assume, that $A_n^{m-1} = n(n-1) \cdot \ldots \cdot [n - (m-1) + 1] =$
$= n(n-1) \cdot \ldots \cdot (n-m+2)$, $(2 \le m \le n)$.
Each m- allocation without repetitions of n elements can be obtained from an $(m-1)$-allocation without repetitions of n elements by adding one element from $n - (m-1) = n - m + 1$ remaining elements of S. Consequently,
$A_n^m = A_n^{m-1} \cdot (m-n) = n(n-1) \cdot \ldots \cdot (n-m+2) \cdot (n-m+1) =$
$= n(n-1) \cdot \ldots \cdot (n-m+1)$. So, the theorem is proved.

In Example 1 above: $A_3^1 = 3$, $A_3^2 = 3 \cdot 2 = 6$, $A_3^3 = 3 \cdot 2 \cdot 1 = 6$.

Example. The number of all **three-digit** numbers **without repetition** of digits and composed from $\{1,2,3,4,5\}$ is $A_5^3 = 5 \cdot 4 \cdot 3 = 60$, starting with 123 and ending with 543.

Notation. By definition: $\boldsymbol{n! = 1 \cdot 2 \cdot \ldots \cdot n}$
For example, $1! = 1$, $2! = 1 \cdot 2 = 2$, $3! = 1 \cdot 2 \cdot 3 = 6$, etc.
By convention: $0! = 1$.

Theorem. There is another shorter formula for the number of $m-$ allocations of n without repetitions:

$$\boxed{A_n^m = \frac{n!}{(n-m)!}}$$

Proof: $A_n^m = n(n-1)\cdot\ldots\cdot(n-m+1) =$
$$= \frac{n(n-1)\cdot\ldots\cdot(n-m+1)\cdot(n-m)\cdot\ldots\cdot 2\cdot 1}{(n-m)\cdot\ldots\cdot 2\cdot 1} = \frac{n!}{(n-m)!}$$

For example: $A_3^1 = \frac{3!}{(3-1)!} = \frac{3!}{2!} = \frac{1\cdot2\cdot3}{1\cdot2} = 3.$

Note. Note that allocations can differ by the content or by the order of their elements.

4.2.2. Permutations without repetition.

Let $S = \{a_1, a_2, \ldots a_n\}$ be a set with n pairwise distinct elements.

Definition. Any n –arrangement without repetition of n elements of S is called **permutation without repetition** of S.

As we see a permutation is particular case of an m – arrangement of n when $m = n$.

Notation. The number of permutations without repetitions of n elements is denoted P_n.

Example 2:
Let $n = 3,\ S = \{a, b, c\}$.
Then permutations of 3 elements are:
$(a,b,c), (a,c,b), (b,a,c), (b,c,a), (c,a,b), (c,b,a)$, so $P_3 = 6$.

Theorem 2.
$$\boxed{P_n = n!}$$

Proof follows from the theorem 2 when $m = n$:
$P_n = A_n^n = n(n-1)\cdot\ldots\cdot 1 = n!$

In example 2 above: $P_3 = 3! = 1\cdot2\cdot3 = 6.$

Note. Note that permutations consist of the same elements and differ only by the order of these elements.

4.2.3. Combinations without repetition.

Let $S = \{a_1, a_2, \ldots a_n\}$.

Definition. Any subset (**order doesn't matter!**) consisting of m $(1 \le m \le n)$ elements from n elements of S is called **m –combination of n without repetitions.**

Notation.
The number of m-combinations of n without repetitions is denoted by C_n^m (or sometimes $\binom{n}{m}$).

Example 3.
Let $n = 3,\ S = \{a, b, c\}$.
1, 2, 3 –combinations of 3 elements without repetitions are:
1 *of* 3: $\{a\}, \{b\}, \{c\}$ – 3 in total, so $C_3^1 = 3$.
2 *of* 3: $\{a,b\}, \{a,c\}, \{b,c\}$ – 3 in total, so $C_3^2 = 3$.
3 *of* 3: $\{a,b,c\}$ – 1 in total, so $C_3^3 = 1$.

Theorem 3.
$$\boxed{C_n^m = \frac{n!}{m!\,(n-m)!}}$$

Proof. The number of m –arrangements of n without repetitions is A_n^m and each arrangement is repeated $m!$ times if order doesn't matter. So,
$$C_n^m = \frac{A_n^m}{P_m} = \frac{n!}{m!\,(n-m)!}$$
In example 3 above: $C_3^1 = \frac{3!}{1!2!} = 3,\ C_3^2 = \frac{3!}{2!1!} = 3,\ C_3^3 = \frac{3!}{3!0!} = 1.$

Note. Note that combinations differ by the content of their elements.

4.2.4. Allocations (samplings) from the different finite sets.

Definition. Let $S_1, S_2, \ldots, S_m$ be finite sets with cardinalities $n_1, n_2, \ldots, n_m$ respectively. Any point $(a_1, a_2, \ldots, a_m) \in S_1 \times S_2 \times \ldots \times S_m$ $(a_i \in S_i, i = 1,2,\ldots,m)$, considered as an **ordered** set is called **m –allocation** of $n_1, n_2, \ldots, n_m$ taken one-by-one from the sets $S_1, S_2, \ldots, S_m$

Notation. The number of all such allocations is denoted by $\tilde{A}^m_{n_1,n_2,\dots,n_m}$.

Theorem 4. The number n of all such allocations is obviously is the cardinality of $S_1 \times S_2 \times \dots \times S_m$, i.e. is given by formula (see 2.4.3)

$$\boxed{\tilde{A}^m_{n_1,n_2,\dots,n_m} = n_1 \cdot n_2 \cdot \dots \cdot n_m}$$

Example 4.

1. The number of all **three-digit even** numbers composed from the digits $\{0,1,2,3,4,5\}$ is equal to $5\cdot 6\cdot 3 = 90$, because 1st digit is one of the 5 elements from $S_1 = \{1,2,3,4,5\}$, 2nd digit is one of the six elements from $S_2 = \{0,1,2,3,4,5\}$ and 3rd digit is one of the 3 elements from $S_3 = \{0,2,4\}$.

The first three-digit even number is 100 and the last is 554.

4.2.5. Allocations with repetitions (or sampling with replacement).

Definition. If, in particular $S_1 = S_2 = \dots = S_m = S, n_1 = n_2 = \dots = n_m = n$, then a point $(a_1, a_2, \dots, a_m) \in S^m$ $(a_i \in S, i = 1,2,\dots,m)$ considered as an ordered set is called **m – allocation of n with repetition** (or sampling with replacement).

Repetition of the elements $a_1, a_2, \dots a_n$ in $(a_1, a_2, \dots, a_m)$ is possible and is necessary if $m > n$, because all $a_1, a_2, \dots, a_m \in S$.

Notation. The number of m –allocations of n with repetitions is denoted by $\tilde{A}^m_n$.

Example 5:

Let $n = 2$, $S = \{a, b\}$. Then $1,2,3$ – allocations of 2 with repetition elements are:

1 *of* 2: $(a),(b)$, –2 in total, so $\tilde{A}^1_2 = 2$, $\tilde{A}^2_2 = 2^2 = 4$.

2 *of* 2: $(a,a),(a,b),(b,a),(b,b)$ – 4 in total, so $\tilde{A}^2_2 = 4$.

3 *of* 2: $(a,a,a),(a,a,b),(a,b,a),(a,b,b)$,
$(b,a,a),(b,a,b),(b,b,a),(b,b,b)$ – 8 in total, so $\tilde{A}^3_2 = 8$, etc.

Theorem 5.

$$\boxed{\tilde{A}^m_n = n^m}$$

Proof. Proof of the theorem 5 is a particular case of the theorem 4.

In the Example5. above: $\tilde{A}^1_2 = 2^1 = 2$, $\tilde{A}^2_2 = 2^2 = 4$, $\tilde{A}^3_2 = 2^3 = 8$, etc.

Example. The number of all **three-digit** numbers composed from the digits $\{1,2,3,4,5\}$ is $\tilde{A}^3_5 = 5^3 = 125$, starting with 111 and ending with 555.

4.2.6. Permutations with repetition.

Let $S = \{a_1, a_2, \dots a_n\}$ be a set.

Definition. Allocations with repetition consisting of the same elements with their multiplicities and differing only by their order are called permutations with repetition.

Notation. The number of all **different** permutations containing m_1 times element a_1, m_2 times element $a_2,\dots$, m_n times element a_n and consisting of $m = m_1 + m_2 + \dots + m_n$ elements is denoted by $\tilde{P}^{m_1,m_2,\dots,m_n}_m$.

The number of all permutations $(a_1, a_2, \dots, a_m)$ consisting of m elements is equal, as we know, to $m!$. But due to the repetition of some elements the total number of the **different** permutations will be less than $m!$

Example 6. Consider first all permutations of 3 distinct elements:
$(a,b,c),(a,c,b),(b,a,c),(b,c,a),(c,a,b),(c,b,a)$.

Total number is $\tilde{P}^{1,1,1}_3 = P_3 = 6$.

If we suppose now that $a = b$, then the permutations containing two elements a and one element c are:
$(a,a,c),(a,c,a),(a,a,c),(a,c,a),(c,a,a),(c,a,a)$, where each permutation is repeated $2! = 2$ times (1st and 3rd, 2nd and 4th, 5th and 6th) due inside permutations of a and a. So, the number of the **different** (due to the order) permutations is $\tilde{P}^{2,1}_3 = 3$. They are: $(a,a,c),(a,c,a),(c,a,a)$.

Theorem 6. The number of the **different** (by the order!) permutations with repetitions is

$$\boxed{\tilde{P}^{m_1,m_2,\dots,m_n}_m = \frac{m!}{m_1!\,m_2!\dots m_n!} = \frac{(m_1+m_2+\dots+m_n)!}{m_1!\,m_2!\dots m_n!}}$$

Proof. The total number of permutations is $m = (m_1 + m_2 + \cdots + m_n)!$ and each permutation is repeated m_1 times due to a_1, m_2 times due to a_2, …,m_n times due to a_n. So, the number of the **different** permutations is

$$\tilde{P}_m^{m_1,m_2,\dots,m_n} = \frac{m!}{m_1!m_2!\dots m_n!} = \frac{(m_1+m_2+\cdots+m_n)!}{m_1!m_2!\dots m_n!}$$

In the example 6 above: $\tilde{P}_3^{1,1,1} = \frac{3!}{1!1!1!} = 6$, $\tilde{P}_3^{2,1} = \frac{3!}{2!1!} = 3$.

Example. Find the number of the different letter permutations can be formed using the letters $PEPPER$.

So, $S = \{P, E, R\}$, $m_1 = 3, m_2 = 2, m_3 = 1, m = 3 + 2 + 1 = 6$.

$\tilde{P}_6^{3,2,1} = \frac{6!}{3!2!1!} = 60$.

4.2.7. Combinations with repetition.

Let $S = \{a_1, a_2, \dots a_n\}$.

Definition. Any set (**order doesn't matter!**) consisting of $\boldsymbol{m}$ $(m \in N)$ elements from $\boldsymbol{n}$ elements of S is called $\boldsymbol{m}$ **–combination of $\boldsymbol{n}$ with repetitions.**

Notation.

The number of m – combinations of n with repetitions is denoted by $\tilde{C}_n^m$.

Example 7:

Let $n = 2$, $S = \{a, b\}$. Then $1, 2, 3$ – combinations with repetition of 2 elements are:

1 *of* 2: $(a), (b)$, –2 in total, so $\tilde{C}_2^1 = 2$.

2 *of* 2: $(a, a), (a, b), (b, b)$ – 3 in total, so $\tilde{C}_2^2 = 3$.

3 *of* 2: $(a, a, a), (a, a, b), (a, b, b), (b, b, b)$ – 4 in total, so $\tilde{C}_2^3 = 4$, etc.

Theorem 7.

$$\boxed{\tilde{C}_n^m = C_{n+m-1}^m = \frac{(m+n-1)!}{m!\,(n-1)!}}$$

Proof.

For any m – combination of n with repetition we assign a chain as follows:

$$\overbrace{a_1a_1 \dots a_1}^{m_1} @ \overbrace{a_2a_2 \dots a_2}^{m_2} @ \overbrace{a_3a_3 \dots a_3}^{m_3} @ \dots @ \overbrace{a_na_n \dots a_n}^{m_n}$$

where we put a separator @ (or any other symbol) between the groups of repeated elements in order to separate them, $m = m_1 + m_2 + \cdots + m_n$ is the number of all elements in the m – combination. If any group of repeated elements is absent in the chain there will be two or more successive separators @-s in this place. For example, if a_2 is absent, then the corresponding chain will be of the form

$$\overbrace{a_1a_1 \dots a_1}^{m_1} @@ \overbrace{a_3a_3 \dots a_3}^{m_3} @ \dots @ \overbrace{a_na_n \dots a_n}^{m_n}$$

So, all chains for m – combinations will have $n - 1$ number of separators @-s. The total number of all elements in the chain, including @-s, will be $m + n - 1$.

What is the difference between two m – combinations? They can be differ by the different collection of numbers $m_1, m_2, \dots, m_n$, i.e. by the different locations of the $n - 1$ separators @-s. Note that the numbers m and n are fixed. So, the total number of all m – combinations with repetition is the number of all permutations with repetition with m elements and $n - 1$ separators. Don't forget that the order of the elements in combination doesn't matter. So, the total number m – combinations of n with repetition is equal to the number of all permutations with repetition of m elements and $n - 1$ separators:

$$\boxed{\tilde{C}_n^m = \tilde{P}_{m+n-1}^{m,n-1} = \frac{(m+n-1)!}{m!\,(n-1)!} = C_{m+n-1}^m}$$

The theorem is proved.

In example 7 above: $\tilde{C}_2^1 = \frac{(2+1-1)!}{1!(2-1)!} = 2$, $\tilde{C}_2^2 = \frac{(2+2-1)!}{2!(2-1)!} = 3$, $\tilde{C}_2^3 = \frac{(2+3-1)!}{3!(2-1)!} = 4$.

Example. How many dominoes are in the normal domino game?

Solution. Dominoes can be considered as the 2 – combinations with repetition of the seven digits set $\{0, 1, 2, 3, 4, 5, 6\}$. The number of all such combinations is

$\tilde{C}_7^2 = \frac{(2+7-1)!}{2!(7-1)!} = \frac{8!}{2!6!} = \frac{7 \cdot 8}{2} = 28$ which corresponds to the well-known number to any domino player.

Note. How to list all allocations with/without repetitions and not to miss anything.

If we replace temporary the elements in $S = \{a_1, a_2, \dots a_n\}$ by their indexes, then it will be easier to control them in allocations by ordering them as numbers.

In example 1 without repetitions $S = \{1,2,3\}$ and the allocations are:

(1), (2), (3), (1,2), (1,3), (2,1), (2,3), (3,1), (3,2),
(1,2,3), (1,3,2), (2,1,3), (2,3,2), (3,1,2), (3,2,1).

In example 5 with repetitions $S = \{1,2\}$ and the allocations are:

(1), (2), (1,1), (1,2), (2,1), (2,2),
(1,1,1), (1,1,2), (1,2,1), (1,2,2), (2,1,1), (2,1,2), (2,2,1), (2,2,2).

The same we do for permutations and combinations.

Note. Since any set include empty set $\emptyset$ as its subset, then the number of elements in $0-$ allocations and $0-$ combinations of n elements are by the definition:

$$A_n^0 = \tilde{A}_n^0 = C_n^0 = \tilde{C}_n^0 = 1$$

4.2.8. The Sum and Product Rules.

Task 1. Let $S_1, S_2, \dots, S_m$ be finite **pairwise disjoint** sets with cardinalities $\boldsymbol{n_1, n_2, \dots, n_m}$ respectively.

Find the number $\boldsymbol{n}$ of ways to choose exactly one element from the collection $S_1, S_2, \dots, S_m$.

Solution of this task is given obviously by the formula of the **Sum Rule**:

$$\boxed{\boldsymbol{n = n_1 + n_2 + \dots + n_m}}$$

Example. You have 4 black, 3 brown and 2 white pairs of shoes. How many options do you have for your walking?

Answer: $n = 4 + 3 + 2 = 9$.

Let $S_1, S_2, \dots, S_m$ be finite **pairwise disjoint** sets with cardinalities $\boldsymbol{n_1, n_2, \dots, n_m}$ respectively.

Task 2. Let $S_1, S_2, \dots, S_m$ be finite sets with cardinalities $\boldsymbol{n_1, n_2, \dots, n_m}$ respectively.

Find the number $\boldsymbol{n}$ of ways to choose a sequence of elements $(a_1, a_2, \dots, a_m)$,

$(a_i \in S_i, i = 1,2, \dots, m)$.

Solution of this task is given obviously by the formula of the **Product Rule** (see formula 4.2.4. for allocations from the different sets):

$$\boxed{\boldsymbol{n = n_1 \cdot n_2 \cdot \dots \cdot n_m}}$$

Example. You have 4 shirts, 3 pants and 2 pairs of shoes. How many options do you have for your walking?

Answer: $n = 4 \cdot 3 \cdot 2 = 24$.

4.2.9. Pigeonhole Principle.

Theorem. If m pigeons are put into n pigeonholes, then at least one pigeonhole must contain more than one pigeon if $m > n$, and at least one pigeonhole must be empty if $m < n$.

Example.

Hair-counting. The population of Almaty city (Kazakhstan) is more than 1,500,000 people. It is known that the number of hairs of a human head is less than 1,000,000. So, at least two people of this city have the same number of hairs.

Exercise. The Birthday Problem.

Show that if the number of students of Faculty is 370 then there exist at least two students who share the same birthday, and if number of students is 360 then there exist the days when there is no birthday celebration on the Faculty.

Generalized Pigeonhole Principle.

If m pigeons are put into n pigeonholes, then there is at least one pigeonhole containing at least $\left\lceil \frac{m}{n} \right\rceil$ pigeons and there is at least one pigeonhole containing at most $\left\lfloor \frac{m}{n} \right\rfloor$ pigeons, where $\lceil \cdot \rceil$ and $\lfloor \cdot \rfloor$ are respectively "ceiling" and "floor" functions, i.e. $\lceil x \rceil$ and $\lfloor x \rfloor$ are the closest to x integers such that $\lfloor x \rfloor \le x \le \lceil x \rceil$, for example, $\lceil \pi \rceil = 4, \lfloor \pi \rfloor = 3, \lceil 2 \rceil = \lfloor 2 \rfloor = 2$.

Example. Among 1500 students of the university there are at least

$\left[\frac{1500}{366}\right] = 5$ students with the same birthday and there is at least one day of the year with the number of birthdays at most $\left[\frac{1500}{366}\right] = 4.$

Exercises 4.2.

1. How many striped three-color flags can be made using seven different colors if the colors mustn't be repeated and the order of the colors matter? (Hint: allocations without repetition).

2. How many striped colored flags can be made using all seven different colors if the colors mustn't be repeated and the order of the colors matter? (Hint: permutations without repetition).

3. How many striped three-color flags can be made using seven different colors if the colors mustn't be repeated and the order of the colors doesn't matter?
(Hint: combinations without repetition).

4. There are 4 roads from the village A to the village B
and 5 roads from the village B to the village C.

a) How many ways are to travel from A to C?
(Hint: allocations from the different sets).
b) How many ways are to travel from A to B and back to A, without going to C?
(Hint: allocations with repetition).

5. Find the number of the different letter permutations can be formed using the letters of the word *MATHEMATICS*. (Hint: permutations with repetition).

7. Ten different postage stamps are sold at the post office.
Find the number of ways to buy 12 stamps.
(Hint: combinations with repetition).

4.3. Binomial Coefficients. Binomial Theorem.

4. 3.1. Binomial Coefficients.

Definitions. The numbers C_n^m $(n \in N,\ m = 0, 1, \ldots, n)$ are called Binomial Coefficients.

Theorem.

1. $C_n^m = C_n^{n-m}$

2. $C_n^m = C_{n-1}^{m-1} + C_{n-1}^m,\ (n \geq 2)$

Proof.

1. $C_n^m = \frac{n!}{m!(n-m)!} = \frac{n!}{(n-m)!m!} = C_n^{n-m}.$

2. $C_{n-1}^{m-1} + C_{n-1}^m = \frac{(n-1)!}{(m-1)!(n-m)!} + \frac{(n-1)!}{m!(n-1-m)!} = \frac{(n-1)!(n-m+m)}{m!(n-m)!} = \frac{n!}{m!(n-m)!} = C_n^m$

Notations.

1. There exists another notation for $C_n^m = \binom{n}{m}$.

2. $\sum_{i=1}^n a_i = a_1 + a_2 + \cdots + a_n$

4.3.2. Binomial Theorem.

For all $a, b \in R,\ n \in N$ there is Binomial Theorem:

$$\boxed{(a+b)^n = \sum_{m=0}^{n} C_n^m a^{(n-m)} b^m = C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^m a^{(n-m)} b^m + \cdots + C_n^n b^n}$$

Proof is by induction on n.

Step 1. $n = 1$, the formula $(a+b)^1 = C_1^0 a + C_1^1 b$ is true since $C_1^0 = C_1^1 = 1.$

Step 2. Assume that $(a+b)^{n-1} = \sum_{m=0}^{n-1} C_{n-1}^m a^{(n-1-m)} b^m$ is true. Then

$(a+b)^n = (a+b)(a+b)^{n-1} = (a+b) \sum_{m=0}^{n-1} C_{n-1}^m a^{(n-1-m)} b^m =$

$= \sum_{m=0}^{n-1} C_{n-1}^m a^{(n-m)} b^m + \sum_{m=0}^{n-1} C_{n-1}^m a^{n-(m+1)} b^{m+1} =$

$= \sum_{m=0}^{n-1} C_{n-1}^m a^{(n-m)} b^m + \sum_{m=1}^{n} C_{n-1}^{m-1} a^{(n-m)} b^m =$

$= C_n^0 a^n + \sum_{m=1}^{n-1} C_{n-1}^m a^{(n-m)} b^m + \sum_{m=1}^{n-1} C_{n-1}^{m-1} a^{n-m} b^m + C_n^n b^n =$

$= C_n^0 a^n + \sum_{m=1}^{n-1} (C_{n-1}^m + C_{n-1}^{m-1}) a^{n-m} b^m + C_n^n b^n = \sum_{m=0}^{n} C_n^m a^{(n-m)} b^m,$

taking account here that $C_n^0 = C_{n+1}^0,\ C_n^n = C_{n+1}^n,\ C_{n-1}^m + C_{n-1}^{m-1} = C_n^m,$

So, $(a+b)^n = \sum_{m=0}^{n} C_n^m a^{(n-m)} b^m$. Theorem is proved.

Examples:

1. $n = 2,\ (a+b)^2 = C_2^0 a^2 b^0 + C_2^1 a^1 b^1 + C_2^2 a^0 b^2 = a^2 + 2ab + b^2.$
2. $n = 3,\ (a+b)^3 = C_3^0 a^3 b^0 + C_3^1 a^2 b^1 + C_3^2 a^1 b^2 + C_3^3 a^0 b^3 =$
$= a^3 + 3a^2 b + 3ab^2 + b^3$

4.3.3. Corollary 1.

$\forall n \in N$

$$\sum_{m=0}^{n} C_n^m = C_n^0 + C_n^1 + \dots + C_n^m + \dots + C_n^n = 2^n$$

Proof follows from **3.8.2.** where $a = 1,\ b = -1$.

Since C_n^m is the number of the subsets consisting of m elements from n elements of the set S, then the sum **3.8.2.** is the number of all subsets of the set S (including empty set $\emptyset$) and is equal to 2^n.

4.3.4. Pascal's Triangle.

Pascal's triangle is a triangular array of the binomial coefficients based on the formulas:

$C_n^m = \frac{n!}{m!(n-m)!},\ C_n^m = C_{n-1}^{m-1} + C_{n-1}^m, (n \geq 2),\quad C_n^m = C_n^{n-m},$

Row number n $(n = 0, 1, \dots)$ in this triangle consist of $n+1$ numbers C_n^m from

$m = 0$ to $m = n$.

So, $C_0^0 = 1\ (o! = 1),$

$C_1^0 = \frac{1!}{0!1!} = 1,\ C_1^1 = \frac{1!}{1!0!} = 1,$

$C_2^0 = \frac{2!}{0!2!} = 1,\ C_2^1 = C_1^0 + C_1^1 = 2,\ C_2^2 = \frac{2!}{2!0!} = 1,$

$C_3^0 = \frac{3!}{0!3!} = 1, C_3^1 = C_2^0 + C_2^1 = 3, C_3^2 = C_2^1 + C_2^2 = 3, C_3^3 = \frac{3!}{3!0!} = 1$ and so on,

The first six rows of Pascal's triangle

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & & & & \end{array}$$

Each number in the triangle is equal to the sum of the two directly above it. Pascal's triangle has many applications in various fields of mathematics.
You can use it to calculate binomial sums, for example:
$(a+b)^5 = a^5 + 5a^4 b + 10a^3 b^2 + 10a^2 b^3 + 5ab^4 + b^5.$

Exercises 4.3.

1. Find $(a+b)^n$ for $n = 4, 5, 6$.
2. Prove the following formula and rewrite it explicitly for $n = 1, 2, 3, 4$:

$$(a-b)^n = \sum_{m=0}^{n} (-1)^m C_n^m a^{(n-m)} b^m =$$

$$= C_n^0 a^n - C_n^1 a^{n-1} b + \dots + (-1)^m C_n^m a^{(n-m)} b^m + \dots (-1)^n C_n^n b^n$$

3. Prove that $\forall n \in N$

$$\sum_{m=0}^{n} (-1)^m C_n^m = C_n^0 - C_n^1 + \dots + (-1)^m C_n^m + \dots (-1)^n C_n^n = 0,$$

or $C_n^0 + C_n^2 + \dots + C_n^{2k} + \dots = C_n^1 + C_n^3 + \dots + C_n^{2k+1} + \dots$

Chapter 5.

NUMBER SYSTEMS.

5.1. Natural numbers, Integers and Rational numbers.

The set theory, elements of which were presented here above, is so called naïve set theory and goes back to Georg Cantor. A modern rigorous set theory is called axiomatic set theory. But for the purposes of our textbook we confine ourselves to the naïve set theory and also omit axioms of choice, of Zorn, of Zermelo underlying the basic of the next constructions of the theory. We also omit the notion of well ordered set which is necessary for the proof of the transfinite induction and we confine ourselves to the mathematical induction for the set of natural numbers. The modern construction of the set of natural numbers is also based on the axiomatic way, but we will base on the concept of natural numbers arising from a simple counting of objects. As for rational numbers, we continue and complete their rigorous construction on the basis of integers, which in turn are based on the natural numbers.

5.1.1. Natural numbers *N*.

Historical digression.

Leopold Kronecker (German mathematician1823 – 1891):

"God created the natural numbers, all the rest is the work of Man".

In my opinion even natural numbers were the work of Man. And not at once! God gave Man the ability to observe, analyze, abstract and conclude. And that was enough! Try to explain. Primitive Man from the very beginning of his activity was forced to count what surrounds him: people, animals, leathers, stones, and finally own fingers. And we believe that primitive Man counted them differently, i.e. one person, two people, etc., ten people, one animal, two animals, etc., ten animals, one finger, two fingers, etc., ten fingers, were different counting for him, though he may dimly suspect that between one person, one animal and one finger, between two people, two animals and two fingers etc., between ten people, ten animals and ten fingers there is some connection. But what? Something was missing! As time passed and life has gradually forced Man to learn how to add people: 1 person + 1 person = 2 people, 2 people + 1 person = 3 people, etc., for example, 7 people +3 people =10 people. He also began to make elementary subtractions. The same operations he learned to do with animals, with leathers, with stones and finally with his fingers. Primitive Man saw that the previously observed relation (one-to one correspondence) between the counting people, animals, stones and whatever **preserve** the operation of addition: the sum of 2 people + 3 people = 5 people corresponds to the sum of 2 animals + 3animals = 5 animals and also corresponds to the sum of 2 stones + 3 stones = 5 stones etc., i.e. he realized that in order to count the number of animals entered in the corral if the 2 first animals entered before and then 3 else, there is no need to go to the corral: just enough to add 2 stones + 3 stones or better yet to add 2 fingers+3 fingers (the first computer that was always with him) and be sure that the quantity of animals in the corral is 5! The same phenomenon he observed for the subtraction.

And in that moment something happened that should have happened!

The Primeval Genius finally tore the property of the object from the object itself and created an abstract concept of numbers 1, 2, 3, ...that do not exist in nature, but only in his mind and that can be safely applied to any new objects of any nature. We can say with certainty that it was the first great mathematical model of the real physical world.

Note. The mentioned above phenomenon of correspondence between the numbers of the objects of different nature **preserving** the operations (addition, subtraction) is called isomorphism that we touched in the end of the chapter 3. It will be clarified later in the study of algebra.

This isomorphism is not obvious and is a purely experimental fact. Tested on a limited number of objects, it gives us confidence in its validity for any number of them.

So, we take the set of natural numbers as the set $N = \{1, 2, \dots, n, \dots\}$ with the operations of addition and multiplications and their properties (laws):

$\forall a, b, c \in N$

1. $(a + b) + c = a + (b + c)$ - associative law of addition
2. $a + b = b + a$ - commutative law of addition
3. $(ab)c = a(bc)$ - associative law of multiplication
4. $ab + ba$ - commutative law of multiplication
5. distributive law of multiplication with respect to addition

$$\begin{cases} a(b+c) = ab + ac \\ (b+c)a = ba + ca \end{cases}$$

6. No zero divisors: if $a, b \in N$ are such that $a \cdot b = 0$ then $a = 0$ or $b = 0$.

Later, to denote the number of elements of the empty set people have added the number zero denoted by 0 and this new set is denoted by $N_0 = \{0, 1, 2, ...\}$ and called often also set of natural numbers.

Still later to indicate historical dates before the birth of Christ, the depth below sea level, the temperatures below the ice melting and many similar reasons, people had to invent negative integer, which were initially seen as mystical.

But the main reason for the consideration of negative integers for mathematicians is different.

In the set of natural numbers $\boldsymbol{N_0}$ the equation $\boldsymbol{a + x = c}$ is always solvable if and only if $\boldsymbol{a \leq c}$ and we denote this solution by $\boldsymbol{x = c - a}$. What can we do in order to solve the equation $a + x = c$ for all $a, c \in N_0$, including $a > c$?

The solution of this problem is to build a new wide set Z including the set N_0, such that the equation $a + x = c$ has a solution for all $a, c \in N_0$. And the most interesting part of this construction is that the newly constructed set Z is entirely based on N_0, i.e. does not use anything other than N_0. This method was invented by the great German mathematician Karl Weierstrass (1815-1897).

5.1.2. Integers Z.

Consider the Cartesian square $N_0^2 = N_0 \times N_0$ and define a binary operation $\oplus$ on it as follows:

1) $\forall (a, b), (a', b') \in N_0^2 \qquad (a, b) \oplus (a', b') = (a + b', b + a') \in N_0^2$.

2) Associativity and Commutativity of the operation of addition + on N_0 implies the same properties for $\oplus$ on N_0^2 (check it!).

3) Consider the binary relation $\sim$ on N_0^2 defined as follows:

$\forall (a, b), (a', b') \in N_0^2 \qquad (a, b) \sim (a', b') \Leftrightarrow a + b' = a' + b$.

Binary relation $\sim$ is the equivalence relation on N_0^2 (check it!).

So, the set N_0^2 can be partitioned into equivalence classes and generate a quotient set $N_0^2/\sim$.

4) The operation $\oplus$ and the equivalence relation $\sim$ are **compatible**, that is if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$ then $(a, b) \oplus (c, d) \sim (a', b') \oplus (c', d')$ (check it!). It allows us to define on the quotient set $N_0^2/\sim$ a new binary operation $\oplus$ (we use the same notation for simplicity) as follows:

$\forall \overline{(a, b)}, \overline{(a', b')} \in N_0^2 \qquad \overline{(a, b)} \oplus \overline{(a', b')} = \overline{(a, b) \oplus (a', b')}$,

where $\overline{(a, b)}$ means equivalence class of (a, b).

This operation is defined correctly due to the mentioned compatibility.

So, the quotient set $N_0^2/\sim$ with operation $\oplus$ defined on it becomes a new algebraic structure $(N_0^2/\sim, \oplus)$ with associative and commutative operation $\oplus$.

We denote $N_0^2/\sim$ by Z.

5) For any two pairs $(a, b), (a', b') \in \overline{(a, b)}$ we have by definition $a + b' = a' + b$ or $a - b = a' - b'$, i.e. the difference between the first and the second elements of the pair is the same.

For the classes $\overline{(a, b)}$ where $a \geq b$ we choose as the simplest representative the pair $(a, 0)$ with $a \geq 0$ and denote it by $\boldsymbol{a} = \overline{(a, 0)}$. For example, $\boldsymbol{0} = \overline{(0,0)} = \{(0,0), (1,1), (2,2), ...\}$, $\boldsymbol{1} = \overline{(1,0)} = \{(1,0), (2,1), (3,2), ...\}$, $\boldsymbol{2} = \overline{(2,0)} = \{(2,0), (3,1), (4,2), ...\}$, etc. Denote $\widetilde{N_0}$ the subset of Z of the classes $\overline{(a, b)}$ with $a \geq b$ or $\widetilde{N_0} = \{\boldsymbol{0, 1, 2, ...}\}$.

Then the function

$f: N_0 \to Z \quad f(a) = \boldsymbol{a} = \overline{(a, 0)}$ is isomorphism between N_0 and $\widetilde{N_0}$.

Really, f is bijective,

$f(a + c) = \overline{(a + c, 0)} = \boldsymbol{a + c} = \overline{(a, 0)} + \overline{(c, 0)} = f(a) + f(c)$.

So, we can say that N_0 is "immersed" in Z.

For the classes $\overline{(a, b)}$ where $a < b$ we choose as the simplest representative the pair $(0, b)$ with $b > 0$ and denote it by $-\boldsymbol{b} = \overline{(0, b)}$, $b \in N^*$. For example, $-\boldsymbol{1} = \overline{(0,1)} = \{(0,1), (1,2), (1,3), ...\}$, $-\boldsymbol{2} = \overline{(0,2)} = \{(0,2), (1,3), (2,4), ...\}$, etc. Denote this subset by $Z_-^* = \{-\boldsymbol{1}, -\boldsymbol{2}, ...\}$.

Finally, $Z = Z_-^* \cup \widetilde{N_0} = \{..., -\boldsymbol{2}, -\boldsymbol{1}, \boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, ...\} = \{\boldsymbol{0}, \pm\boldsymbol{1}, \pm\boldsymbol{2}, ...\}$.

The equation $\boldsymbol{a + x = c}$ is solvable in Z for all natural $a, c \in Z$.

If $a \leq c$ $(c - a \in N_0)$, then

$\boldsymbol{x = c - a} = \overline{(c, 0)} - \overline{(a, 0)} = \overline{(c - a, 0)} \in \widetilde{N_0}$, and the number $\boldsymbol{x} = \overline{(x, 0)} \in \widetilde{N_0}$, and it corresponds to $x = c - a \in N$.

If $a > c$, then $\boldsymbol{x = c - a} = \overline{(c, 0)} - \overline{(a, 0)} = \overline{(c - a, 0)} = \overline{(0, a - c)} = -\boldsymbol{(a - c)}$.

Relation of order on Z is given by definition:

$(a, b) < (a', b')$ if and only if $a + b' < a' + b$. So defined order gives

$... < -2 < -1 < 0 < 1 < 2 < \cdots$

The set Z has no divisors of zero.

The set of integers with two operations of addition and multiplication satisfying the same properties as for natural numbers is called often **Ring of Integers**.

5.1.3. Rational numbers Q.

Rational numbers were invented to indicate first of all fractions.

The main reason for mathematicians to construct the set of rational numbers was the need to solve the equation $ax = c$ for all $a, c \in Z, a \neq 0$ and c is not necessarily divisible by a. The set of rational numbers Q can be constructed in the same way on the base of the set Z as the set of integers was constructed above on the base of the set N_0. In fact we constructed the set Q earlier in the chapter about relations.

The set of rational numbers with two operations of addition and multiplication satisfying the same properties as for natural numbers and integers is called often **Field of Rational numbers.**

5.1.4. Real numbers R.

As we know there is no rational number a such that $a^2 = 2$. But we can find the rational numbers whose squares are as close to 2 as we like. There are other quantities, for example numbers e, π, etc, which cannot be represented by rational numbers, but can be approximated by rational numbers as close as we like.

It means that if you represent rational numbers as points of an infinitely long line, then this line has empty holes which we call irrational numbers. The completion of the set Q by these irrational numbers is called the **set (or field) of real numbers.**

This completed (without holes) line is cold **real line** and is denoted by R.

Of course this definition of real numbers is not rigorous definition for modern mathematics but it is enough for our current purposes.

Addition, multiplication, relation of order with their properties are transferred from the set of rational numbers on the set of real numbers.

The main reason for mathematicians to construct the real numbers is to be able to make "passage to limit" that will be studied in the course of calculus.

Note. We must note that for purposes of physical measurements in real life, which always are made only approximately, there is no need to have real numbers, we can manage only rational.

5.2. Complex numbers.

5.2.1. Complex number. Operations on complex numbers.

Definition. Let $R^2 = \{(a,b) | a \in R, b \in R\}$.

We call **complex number** any ordered pair $(a,b) \in R^2$ and we denote it by $z = (a,b)$.

The first a is called the **reel part** of z and is denoted by $a = Re\, z$.

The second b is called **imaginary part** of z and is denoted $b = Im\, z$

Don't forget that imaginary part b is reel number too.

Two complex numbers $z = (a,b)$ and $z' = (a',b')$ are equal by definition:

$$z = z' \Leftrightarrow (a = a') \wedge (b = b')$$

Definition. We define the **addition and multiplication** of two complex numbers

$z = (a,b)$ and $z' = (a',b')$ as follows:

(1) $z + z' = (a + a',\ b + b')$,

(2) $z \cdot z' = (aa' - bb',\ ab' + ba')$.

Exercise. Using the definition of the difference $z - z'$ as the complex number z'' such that $z = z' + z''$, prove that $z - z' = (a - a', b - b')$

The set of all complex numbers with these two operations is called a field of complex numbers and denoted by C.

Exercise. Using the properties of the addition and multiplication of real numbers as given prove the analogous properties for the complex numbers as the following theorem.

Theorem. Let $z, z', z'' \in C,\ z = (a,b),\ z' = (a',b'),\ z'' = (a'',b'')$.

Then

1) **addition is associative:** $(z + u) + v = z + (u + v)$,
2) **addition is commutative:** $z + u = u + z$,
3) element $\mathbf{0} = (0,0)$ is the element "zero" for the addition:
   $\forall z \in C\ \ z + \mathbf{0} = \mathbf{0} + z = z$, also $z \cdot \mathbf{0} = \mathbf{0} \cdot z = \mathbf{0}$,
4) element $-z = (-a, -b)$ is the "opposite" element to $z = (a,b)$:
   $z + (-z) = -z + z = \mathbf{0}$,
   so the **subtraction** " $-$ " can be defined on C as follows:
   $z' - z = z' + (-z) = (a' - a, b' - b)$,
5) **multiplication is associative:** $(zu)v = z(uv)$,

6) **multiplication is commutative**: $zu = uz$,

7) element $\mathbf{1} = (1, 0)$ is the element "unit" for the multiplication:

$\forall z \in C \quad z \cdot \mathbf{1} = \mathbf{1} \cdot z = z$,

8) $\forall\, z \neq \mathbf{0}\ \exists'$ "inverse" element z^{-1} such that $zz^{-1} = z^{-1}z = \mathbf{1}$

and if $z = (a, b)$, then $z^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$,

so the **division** "/" can be defined on C as follows:

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

(it is clear that the division by z is impossible in only case

$z = \mathbf{0}$, i. e. $a = b = 0$).

9) **multiplication is distributive over addition**:

$z(u + v) = zu + zv, \quad (u + v)z = uz + vz.$

5.2.2. Immersion of R in C.

Consider a subset $R' \subset C$ defined by $R' = \{(a, 0) \in C \mid a \in R\}$, i.e. the subset of all complex numbers which imaginary part is zero.

We note that $z, z' \in R'$, then $z + z' \in R'$ and $z \cdot z' \in R'$.

Really, let $z = (a, 0),\ \ z' = (a', 0)$. Then

1) $z + z' = (a + a', 0) \in R'$,

2) $zz' = (aa', 0) \in R'$,

3) $\mathbf{0} \in R'$,

4) $-z = (-a, 0) \in R'$,

5) $\mathbf{1} = (1, 0) \in R'$,

6) $z^{-1} = \left(\frac{a}{a^2+0^2}, \frac{0}{a^2+b^2}\right) = (a^{-1}, 0) \in R'$.

Let consider the function $f: R \to R' \subset C,\ \forall a \in R \quad f(a) = (a, 0) \in R'$.

Then,

1) f is obviously bijective,

2) $f(a + b) = (a + b, 0) = (a, 0) + (b, 0) = f(a) + f(b)$

3) $f(ab) = (ab, 0) = (a, 0)(b, 0) = f(a)f(b)$,

i.e. f is isomorphism between R and R'.

This isomorphism allows us to identify R and R' and say that R is immersed in C or C is extension of R.

Imaginary unit i.

Consider the special complex number $i = (0,1)$ called **imaginary unit**.

Then $i^2 = (0,1)(0,1) = (0^2 - 1^2,\ 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$.

Since the number $(-1, 0)$ corresponds to the reel number -1 we can write by convention $i^2 = -1$ or $i = \sqrt{-1}$.

Note. There are many books that introduce complex numbers after reel numbers starting by the equality $i^2 = -1$ or $i = \sqrt{-1}$ for a new symbol i. But there is no reel number whose square is -1 or there is no reel square root of -1. It should be well understood and remembered that conventional write $i^2 = -1$ or $i = \sqrt{-1}$ means in reality $i^2 = (-1, 0)$ or $i = \sqrt{(-1, 0)}$.

Note. Don't forget that there are two square roots of $\sqrt{-1} = \pm i$.

Exercise. Prove that i^n has exactly four possible values:

$i,\ i^2 = -1, i^3 = -i, i^4 = 1, \dots, i^{4n} = 1, i^{4n+1} = i, i^{4n+2} = -1, i^{4n+3} = -i$.

5.2.3. Cartesian form of complex numbers.

Complex number $z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$, where by convention $(a, 0) = a,\ (b, 0) = b$.

In particular, if $b = 0$, then complex number $z = a$ is called "reel" number, if $a = 0$, then complex number $z = bi$ is called "purely imaginary" number

Cartesian form of complex number $z = a + bi$ will be used more frequently than the initial form $z = (a, b)$, because the operations of addition and multiplication become more convenient and visible. Really, if $z = a + bi,\ u = c + di$, then

$z + u = (a + bi) + (c + di) = (a + c) + (b + d)i$,

$z - u = (a + bi) - (c + di) = (a - c) + (b - d)i$,

$zu = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$,

$$\frac{z}{u} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd)}{c^2 + d^2} + \frac{(bc - ad)}{c^2 + d^2}i,$$

in particular,

$$\frac{1}{u} = \frac{1}{c + di} = \frac{c}{c^2 + d^2} - \frac{d}{c^2 + d^2}i.$$

Examples. Let $z = 7 - 4i, u = 3 + 2i$. Then:

$zu = (21 + 8) + (14 - 12)i = 29 + 2i$,

$z + u = 10 - i, z - u = 4 - 6i,$

$\frac{z}{u} = 1 - 2i, \frac{1}{u} = \frac{3}{13} - \frac{2}{13}i$

5.2.4. Conjugate.

Definition. Conjugate of the complex number $z = a + bi = (a, b)$ is the complex number denoted by $\bar{z} = a - bi = (a, -b)$.

Exercise. Prove the following **properties of the conjugate:**

1. $\bar{\bar{z}} = z$,
2. $z + \bar{z} = 2Re\, z,\ \ Re\, z = (z + \bar{z})/2$
3. $z - \bar{z} = 2iIm\, z,\ \ Im\, z = (z - \bar{z})/2i$
4. $z\bar{z} = (Re\, z)^2 + (Im\, z)^2$,
5. $\overline{z + u} = \bar{z} + \bar{u}$,
6. $\overline{z \cdot u} = \bar{z} \cdot \bar{u}$.

Example. $(3 + 4i)(\overline{3 + 4i}) = (3 + 4i)(3 - 4i) = 3^2 + 4^2 = 25$

5.2.5. Modulus of a complex number. Distance between complex numbers.

Definition. The modulus of a complex number $z = a + bi$ is the non-negative reel number denoted by $|z| = \sqrt{a^2 + b^2} = \sqrt{(Re\, z)^2 + (Im\, z)^2}$.

The distance between two complex numbers $z = a + bi$ and $z' = a' + b'i$ is $|z - z'| = \sqrt{(a - a')^2 + (b - b')^2}$

Exercise. Prove the following **properties of modulus:**

1. $|z| \geq 0,\ \ |z| = 0 \Leftrightarrow z = \mathbf{0}\ (a = 0,\ b = 0)$,
2. $|z| = \sqrt{z\bar{z}}$,
3. $|zu| = |z||u|,\ \ \left|\frac{z}{u}\right| = \frac{|z|}{|u|}$, *in paricular* $\left|\frac{1}{z}\right| = \frac{1}{|z|}$ or $|z^{-1}| = |z|^{-1}$
4. $|Re\, z| \leq |z|,\ \ |Im\, z| \leq |z|$,
5. $|z + u| \leq |z| + |u|,\ \ ||z| - |u|| \leq |z - u|$ – ***the triangle inequalities.***

Square root of a complex number.

Problem. Let $c = a + bi$ be a complex number.

Find $z = \sqrt{c}$, i.e. find the complex number $z = x + yi$ such that $z^2 = c$.

Solution.

$z^2 = (x + yi)^2 = x^2 - y^2 + 2xyi$,

$$z^2 = c \Leftrightarrow \begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \Leftrightarrow \begin{cases} x^2 - \frac{b^2}{4x^2} = a \\ y = \frac{b}{2x} \end{cases} \Rightarrow x^4 - ax^2 - \frac{b^2}{4} = 0 \Leftrightarrow$$

$$x^2 = \frac{a+\sqrt{a^2+b^2}}{2} \Rightarrow x_{1,2} = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}},\ \ y_{1,2} = \frac{b}{\pm 2\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}} =$$

$$\pm sign\, b\sqrt{\frac{b^2}{2(a+\sqrt{a^2+b^2})}} = \pm sign\, b\sqrt{\frac{b^2(a-\sqrt{a^2+b^2})}{2(a^2-a^2-b^2)}} =$$

$$= \pm sign\, b\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} = \begin{cases} \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}, if\ b > 0 \\ \mp\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}, if\ b < 0 \end{cases}$$

So, $z_1 = x_1 + y_1 i,\ \ z_2 = x_2 + y_2 i = -x_1 - y_1 i$, i.e. z_1 and z_2 are opposite.

Finally we can write briefly

$$\sqrt{a + bi} = \pm\left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\frac{b}{|b|}\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\right) \text{ if } b \neq 0,$$

$\sqrt{a + bi} = \pm\sqrt{a},\ if\ b = 0.$

Example. $z^2 = -5 + 12i,\ b = 12 > 0$,

$x_{1,2} = \pm\sqrt{\frac{-5+\sqrt{25+144}}{2}} = \pm 2,\ \ y_{1,2} = \pm\sqrt{\frac{5+\sqrt{25+144}}{2}} = \pm 3.$

So, $z_{1,2} = \pm(2 + 3i)$ or $z_1 = 2 + 3i,\ \ z_2 = -2 - 3i$.

Equation of the second degree.

Exercise. Let $a, b, c \in C$. Solve the equation $\boldsymbol{az^2 + bz + c = 0}$.

Solution.

$$az^2 + bz + c \equiv a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a^2}\right],$$

$$az^2 + bz + c = 0 \Leftrightarrow \left(z + \frac{b}{2a}\right)^2 = \frac{b^2-4ac}{4a^2} = 0 \Leftrightarrow z_{1,2} + \frac{b}{2a} = \pm\frac{\sqrt{b^2-4ac}}{2a},$$

$$z_{1,2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

In the field of the complex numbers C an equation of the second degree is always solvable. In particular, an equation of the second degree $ax^2 + bx + c = 0$ with reel coefficients $a, b, c \in R$ heel has no reel roots if its discriminant

$d = b^2 - 4ac < 0$, but it has two conjugate complex roots

$$x_{1,2} = \frac{-b \pm \sqrt{d}}{2a} = \frac{-b \pm i\sqrt{-d}}{2a}, \qquad (-d > 0).$$

Later in course of the algebra we will learn that any polynomial equation of n-th degree is solvable in the field C and has n roots (complex in general) counting their multiplicities.

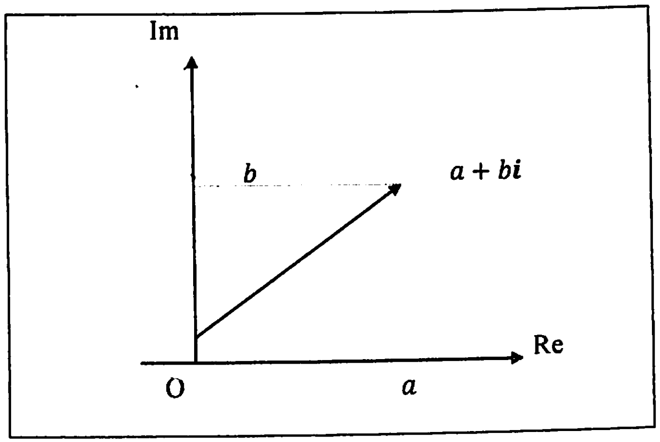
5.2.6. Complex plane.

Let R^2 be the arithmetic plane with Cartesian coordinate system.

Consider the function $f: R^2 \to C,\ \ f(x, y) = x + yi$.

This function is obviously bijective: to any point $(x, y) \in R^2$ it assigns a one and only one complex number $x + yi \in C$ and reciprocally.

The plane of all points $M(z), (z = x + yi)$ is called **complex plane**, the axis OX is called axis of reels and the axis OY is called axis of purely imaginaries.



Let $z = a + bi,\ z' = a' + b'i \in C,\ k \in R$.

Since $z + z' = (a + a') + (b + b')i,\ kz = ka + kbi$ we can see that the addition of two complex numbers and multiplication of the complex number by the reel number (scalar) are defined by the same rules as for the vectors $\overrightarrow{OM} = (a, b)$ and $\overrightarrow{OM'} = (a', b')$: $\overrightarrow{OM} + \overrightarrow{OM'} = (a + a', b + b'),\ \ k \cdot \overrightarrow{OM} = (ka, kb)$.

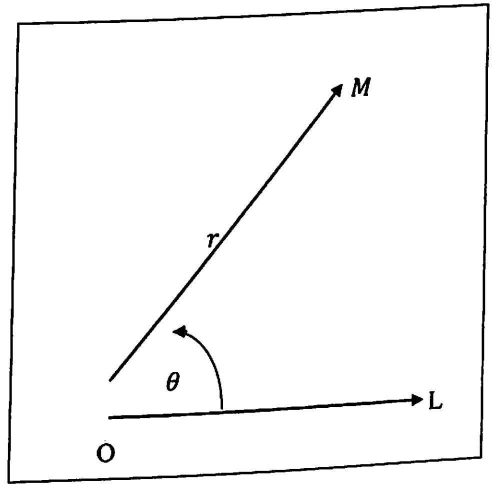
5.2.7. Polar coordinate system.

Polar coordinate system on the plane P is constructed as follows.

We fix a point $\boldsymbol{O}$ on the plane called ***pole*** and a ray $\boldsymbol{OL}$ called ***polar axis***.

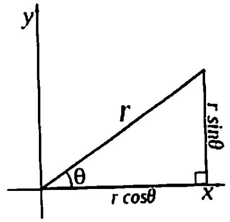
To each point $M \in P, (M \neq \mathbf{0})$ we assign a pair of real numbers (r, θ) called ***polar coordinates*** of the point M, where the ***polar radius***

$r = |\overrightarrow{OM}| \in [0, +\infty)$ is the length of the radius-vector $\overrightarrow{OM}$ (or the distance from the pole O to the point M) and the ***polar angle*** $\boldsymbol{\theta}$ is the value of the angle formed by the radius-vector $\overrightarrow{OM}$ with polar axis OL measured counterclockwise from the polar axis for positive values of θ and clockwise for negative values of θ. The angle θ is determined up to $2n\pi$ (or 360°n), $n \in Z$. When a unique representation is needed it is usual to take $\theta \in (-\pi, \pi]$ (or sometimes $\theta \in [0, 2\pi)$), respectively $(-180°, 180°]$ (or $[0, 360°)$). For the pole $\boldsymbol{O}$ obviously $r = 0$ and the angle θ is not determined and can be taken arbitrary from the interval $(-\pi, \pi]$, often $\theta = 0$.



5.2.8. Converting between Cartesian and Polar coordinates.

Consider the Cartesian system of coordinate on the same plane such that its origin $(0, 0)$ coincides with the pole O and the positive direction of the abscissa axis coincides with the polar axis. Then the Cartesian coordinates are expressed in terms of the polar coordinates as follows:



$$\begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases} \quad (*)$$

The formulas $(*)$ determine the function $f: E \to F,\ f(r,\theta) = (x,y)$, where $E = [0,+\infty) \times (-\pi,\pi],\quad F = R^2$. Restriction of this function $f: E^* \to F^*$,
where
$E^* = (0,\ +\infty) \times (-\pi,\pi],\ F^* = R^2 - \{(0,0)\}$ is bijective and its inverse $f^{-1}: F^* \to E^*,\ f^{-1}(x,y) = (r,\theta)$ gives the converting formulas from the Cartesian coordinates to the polar coordinates inverse of $(*)$:

$r = \sqrt{x^2+y^2}$, according to Pythagorean theorem,

$\theta \in (-\pi,\pi]$ can be found uniquely from the equations

$\cos\theta = \frac{x}{\sqrt{x^2+y^2}},\ \sin\theta = \frac{y}{\sqrt{x^2+y^2}}$, for example

$$\theta = \begin{cases} \arctan\left(\frac{y}{x}\right), & if\ x > 0 \\ \arctan\left(\frac{y}{x}\right) + \pi, & if\ x < 0\ and\ y \geq 0 \\ \arctan\left(\frac{y}{x}\right) - \pi, & if\ x < 0\ and\ y < 0 \\ \frac{\pi}{2}, & if\ x = 0\ and\ y > 0 \\ -\frac{\pi}{2}, & if\ x = 0\ and\ y < 0 \\ undefined, & if x = 0\ and\ y = 0 \end{cases}$$

The function f^{-1} can be extended as $f^{-1}: R^2 \to [0,+\infty) \times (-\pi,\pi]$, by defining at point $(0,0)$ $r = 0$ and θ equal to any fixed value from $(-\pi,\pi]$, for example $\theta = 0$.

In our days we often use another notation of this formula for the angle θ that came from computer sciences $\theta = atan2(y,x)$ and has the same meaning.

Example.

A point with Cartesian coordinates $(1,1)$ has Polar coordinates $\left(\sqrt{1^2+1^2}, \arctan\left(\frac{1}{1}\right)\ (mod\ 2\pi)\right) = (\sqrt{2}, \frac{\pi}{4} + 2n\pi, n \in Z)$.

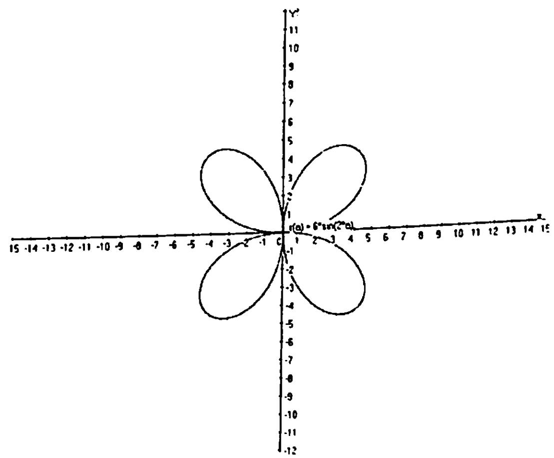
A point with Polar coordinates $(2, -\frac{\pi}{4})$ has Cartesian coordinates $\left(2\cos(-\frac{\pi}{4}), 2\sin(-\frac{\pi}{4})\right) = (\sqrt{2}, -\sqrt{2})$.

5.2.9. Polar equation of a curve.

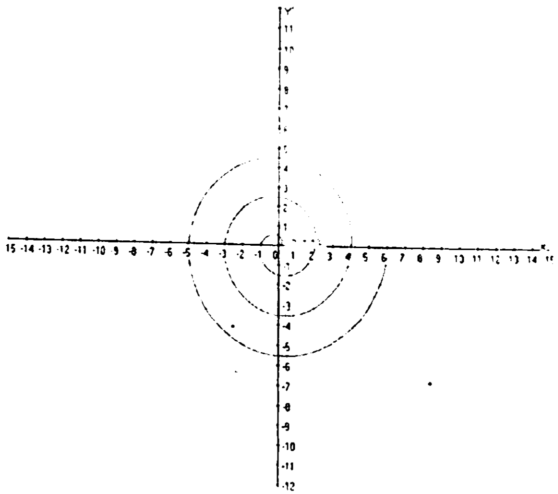
Analogous to the equations of curves in Cartesian coordinates $y = f(x)$ they can be given in polar coordinates $r = f(\theta)$.

Examples:

1. $r = r_0$, where $r_0 \geq 0$ is constant, represent a circle of radius r_0 centered at pole.
2. $\theta = \theta_0$, where θ_0 is constant, represent a ray from the pole.
3. $r = 2\sin 4\theta$ represent a "polar rose"



4. $r = \theta/\pi$ represent the Archimedean spiral (on the drawing below $\theta \in [0,6\pi]$).



5.2.10. Trigonometric form of complex numbers.

Definition. For any complex number $z = x + yi$ we can assign the point M (or vector $\overrightarrow{OM}$) with Cartesian coordinates (x, y) or polar coordinates (r, θ).

The polar radius r and polar angle θ of the vector $\overrightarrow{OM}$ are called respectively **modulus** (absolute value) and **argument** of the complex number z and are denoted by

$$|z| = r = |\overrightarrow{OM}|, \quad arg\, z = \theta = (OX, \overrightarrow{OM}) \ (mod\ 2\pi).$$

We repeat here the already known definition of the modulus in other words.

The expression $mod\ 2\pi$ means "up to $2n\pi,\ n \in Z$".

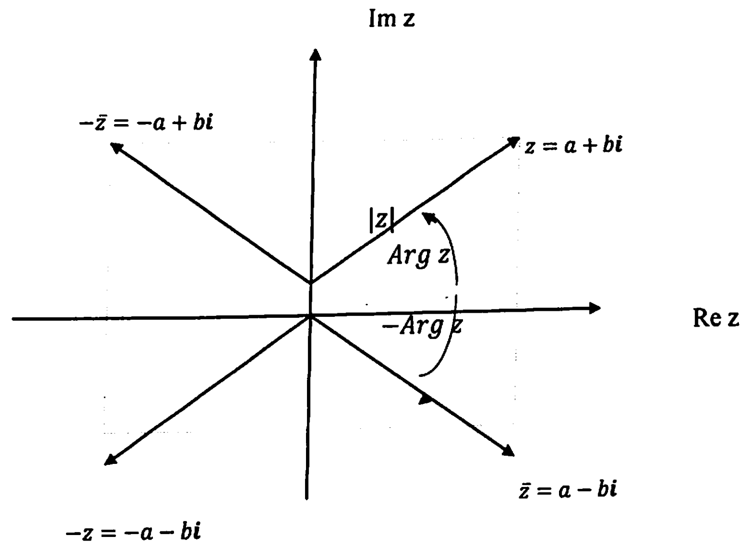
If $z = \mathbf{0}$, then $|z| = 0$ and arg z is not defined.

The value of an argument from $(-\pi, \pi]$ (sometimes $[0, 2\pi)$) is called **principal value of argument** of z and denoted by $\boldsymbol{Arg\ z}$.

So, **arg** $z = \{\boldsymbol{Arg\ z + 2n\pi,\ n \in Z}\}$.

Exercise:

Prove that $|\bar{z}| = |z|,\ Arg\ \bar{z} = -Arg\ z$



As we already know $x = r\cos\theta,\ y = r\sin\theta$.

So $z = x + yi = r\cos\theta + r\sin\theta\, i$.

And finally $\boldsymbol{z = r(\cos\theta + i\sin\theta)}$ – **trigonometric form of a complex number.** (1)

Exercise. Let $z = r(\cos\theta + i\sin\theta)$ and $z' = r'(\cos\theta' + i\sin\theta')$ be two complex numbers in trigonometric form.

Prove that $z = z' \Leftrightarrow (r = r') \wedge (\theta = \theta')\ (mod\ 2\pi)$.

Note. We can compare among themselves real or imaginary parts, modules or Arguments of two complex numbers (because they are real numbers), but we cannot compare complex numbers themselves. **Complex numbers are not comparable!**

Examples:

1. $z = 1 - i$.

$r = \sqrt{1^2 + (-1)^2} = \sqrt{2}, \cos\theta = \frac{1}{\sqrt{2}}, sin\theta = -\frac{1}{\sqrt{2}}$, hence $\theta = -\frac{\pi}{4}\ (mod\ 2\pi)$.

$z = \sqrt{2}(cos\frac{\pi}{4} - i\,sin\frac{\pi}{4})$

2. Modulus and Argument of a reel number x.

a) if $x > 0$, then $|x| = x, \quad Arg\ x = 0,\ x = x(\cos o + i\sin 0)$,

b) if $x < 0$, then $|x| = -x,\ Arg\ x = \pi,\ x = -x(\cos\pi + i\sin\pi)$.

3. Modulus and Argument of a purely imaginary number yi.

a) if $y > 0$, then $|yi| = y, \quad Arg\ x = \frac{\pi}{2},\ yi = y(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2})$,

b) if $y < 0$, then $|yi| = -y,\ Arg\ x = -\frac{\pi}{2},\ yi = -y(\cos\frac{\pi}{2} - i\sin\frac{\pi}{2})$.

Let z and z_1 be two complex numbers:

$z = r(cos\theta + i\,sin\theta),\ z_1 = r_1(cos\theta_1 + i\,sin\theta_1)$.

Argument of a product.

Then $zz_1 = rr_1(cos\theta + i\,sin\theta)(cos\theta_1 + i\,sin\theta_1) = rr_1[(cos\theta cos\theta_1 - sin\theta sin\theta_1) + i\,(cos\theta sin\theta_1 + sin\theta cos\theta_1)] = rr_1[\cos(\theta + \theta_1) + i\,sin(\theta + \theta_1)]$.

So, $\boxed{|zz_1| = |z||z_1|,\ arg(zz_1) = arg\ z + arg\ z_1\ (mod\ 2\pi)}$

Example. $z = \cos\frac{\pi}{3} + i\,sin\ \frac{\pi}{3},\ z_1 = 2\left(\cos\frac{\pi}{6} + i\,sin\ \frac{\pi}{6}\right)$,

$zz_1 = 2\left(\cos\frac{\pi}{2} + i\,sin\ \frac{\pi}{2}\right) = 2i$.

Argument of a quotient. Assume $z_1 \neq 0$.

$$\frac{z}{z_1} = \frac{r}{r_1}\frac{(cos\theta + i\,sin\theta)}{(cos\theta_1 + i\,sin\theta_1)} = \frac{r}{r_1}\frac{(cos\theta + i\,sin\theta)(cos\theta_1 - i\,sin\theta_1)}{(cos\theta_1 + i\,sin\theta_1)(cos\theta_1 - i\,sin\theta_1)} = \frac{r}{r_1}\frac{(cos\theta + i\,sin\theta)(cos\theta_1 - i\,sin\theta_1)}{(cos\theta_1 + i\,sin\theta_1)(cos\theta_1 - i\,sin\theta_1)} = \frac{r}{r_1}\,[\cos(\theta - \theta_1) + i\sin(\theta - \theta_1)].$$

So,

$$\boxed{\left|\frac{z}{z_1}\right| = \frac{|z|}{|z_1|},\ arg\left(\frac{z}{z_1}\right) = arg\ z - arg\ z_1\ (mod\ 2\pi)}$$

In particular, $\frac{1}{z} = \frac{1}{r}\ (cos\theta - i\ sin\theta)$, i.e.

$\left|\frac{1}{z}\right| = \frac{1}{|z|},\ Arg\left(\frac{1}{z}\right) = -Arg\ z$.

Examples. $z = 6(\cos\frac{\pi}{4} + i\,sin\ \frac{\pi}{4}),\ z_1 = 3\left(\cos\frac{\pi}{2} + i\,sin\ \frac{\pi}{2}\right)$,

$\frac{z}{z_1} = 2\left(\cos(-\frac{\pi}{4}) + i\,sin\ (-\frac{\pi}{4})\right) = \sqrt{2}(1 - i)$.

5.2.11. De Moivre's formula.

Let $z = r(cos\theta + isin\theta),\ z \in C^*$ (i.e. $z \neq 0$), $n \in N$.

Prove by Mathematical Induction

De Moivre's theorem:

$$\boxed{z^n = r^n(\cos n\theta + i\sin n\theta)}$$

i.e. $|z^n| = |z|^n,\ \ arg\ z^n = n\ arg\ z\ \ (mod\ 2\pi)$.

For $n = 0$ by definition $z^0 = \mathbf{1}$. Then $\mathbf{1} = r^0(cos0 + isin0)$, i.e. De Moivre's formula remains valid.

For negative integer n by definition $z^n = \frac{1}{z^{-n}}$, where $-n \in N$.

De Moivre's formula remains valid for negative integer n too.

Really, if $n < 0$, then $-n > 0$. So,

$$z^n = \frac{1}{z^{-n}} = \frac{1}{r^{-n}[\cos(-n\theta) + isin(-n\theta)]} = \frac{1}{r^{-n}}(\cos n\theta + i\sin n\theta) =$$

$= r^n(\cos n\theta + i\sin n\theta)$, where $n < 0$.

So, **De Moivre's formula is valid for** $\forall\ n \in Z$.

A special case of $|z| = 1$:

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

This formula allows us to express $\cos n\theta,\ \sin n\theta,\ \tan n\theta$ by $\cos\theta, \sin\theta, \tan\theta$:

$$\cos n\theta = Re\,(\cos\theta + i\sin\theta)^n,\quad \sin n\theta = Im\,(\cos\theta + i\sin\theta)^n.$$

Example $n = 3$.

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

$$\cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta = \cos 3\theta + i\sin 3\theta$$

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta = 4\cos^3\theta - 3\cos\theta,$$

$$\sin 3\theta = 3\cos^2\theta\sin\theta - 4\sin^3\theta = 3\sin\theta - 4\sin^3\theta.$$

5.2.12. n^{th} root of a complex number ($n \in Z$).

Definition. The n^{th} root of a complex number z is the complex number c such that $c^n = z$.

It is denoted by $c = \sqrt[n]{z}$ or $c = z^{\frac{1}{n}}$.

So, $c = \sqrt[n]{z} \Leftrightarrow c^n = z$.

Theorem. There are exactly n n^{th} roots of a complex number z given by the formulas

$$\sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + i\sin\frac{\theta + 2k\pi}{n}\right), k = 0, 1, \dots, n-1$$

Proof. We denote $z = r(\cos\theta + i\sin\theta),\ c = \rho(\cos\alpha + i\sin\alpha)$.

Then $z = c^n \Leftrightarrow r(\cos\theta + i\sin\theta) = \rho^n(\cos n\alpha + i\sin n\alpha) \Leftrightarrow$

$\Leftrightarrow \rho^n = r$ and $n\alpha = \theta + 2k\pi,\ k \in Z \Leftrightarrow \rho = \sqrt[n]{r}$ and $\alpha = \frac{\theta + 2k\pi}{n}, k \in Z$.

Despite the fact that n takes an infinite numbers of values in Z, the number of different roots due to the 2π periodicity of $\sin$ and $\cos$ is exactly n. They can be exhausted by taking $k = 0, 1, \dots, n-1$.

Really, the formula of the roots rewritten in the form

$\sqrt[n]{z} = \sqrt[n]{r}\left(\cos(\frac{\theta}{n} + \frac{2k\pi}{n}) + i\sin(\frac{\theta}{n} + \frac{2k\pi}{n})\right)$ gives the different values when $k = 0, 1, \dots, n-1$. For $k = n$ the formula gives the same value of root as for $k = 0$, for $k = n + 1$ the same value as for $k = 1$, etc. Similarly, for $k = -1$ the formula gives the same value of root as for $k = n - 1$. Really, without affecting the formula we can add to the argument 2π. Then $\theta + 2\pi - \frac{2\pi}{n} = \theta + \frac{2(n-1)\pi}{n}$, etc.

Example. Square roots of a complex number.

$$\sqrt{z} = \sqrt{r}\left(\cos\frac{\theta + 2k\pi}{2} + i\sin\frac{\theta + 2k\pi}{2}\right), \qquad k = 0, 1$$

$$(\sqrt{z})_0 = \sqrt{r}\left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\right),\ (\sqrt{z})_1 = -\sqrt{r}\left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\right).$$

As we see the square roots are opposite: $(\sqrt{z})_1 = -(\sqrt{z})_0$

5.2.13. n^{th} roots of unity.

Find z if $z^n = \mathbf{1}, n \in Z$, i.e. find $\sqrt[n]{\mathbf{1}}$.

Solution.

$1 = \cos 0 + i\sin 0,$

$$z = \sqrt[n]{\mathbf{1}} = \sqrt[n]{1}\left(\cos\frac{0 + 2k\pi}{n} + i\sin\frac{0 + 2k\pi}{n}\right) = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right),$$

$$k = 0, 1, \dots, n-1$$

$z_0 = 1,$

$z_1 = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right),$

............................,

$z_{n-1} = \left(\cos\frac{2(n-1)\pi}{n} + i\sin\frac{2(n-1)\pi}{n}\right).$

These roots are uniformly located on the unit circle centered at the origin with the angle $\frac{2\pi}{n}$ between the two neighbors.

Example. Find $\sqrt[3]{\mathbf{1}}$.

$z_0 = 1,$

$z_1 = \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2},$

$z_2 = \left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$

5.2.14. Euler's formula.

Let U be the unit circle centered at origin O of the complex plane C.

Consider the function $e: R \to U,\ e(\theta) = \cos\theta + i\sin\theta$

This function is obviously periodic with the period 2π:

$\forall\,\theta \in R\quad e(\theta + 2\pi) = e(\theta)$.

Moreover,

$e(a + b) = \cos(a + b) + i\sin(a + b) =$

$(\cos a + i \sin a)(\cos b + i \sin b) = e(a)e(b)$, ÷
that is the function e is the **morphism** $(R, +) \to (U, \cdot)$.
We let by definition the next notation:
$e^{i\theta} = \cos\theta + i\sin\theta$,
called **Euler's formula.**

So, the trigonometric form of a complex number $z = r(\cos\theta + i\sin\theta)$ can be written as follows: $z = re^{i\theta}$.

Examples:

1) $1 = 1 \cdot e^{i0}$, 2) $i = e^{i\frac{\pi}{2}}$, 3) $-1 = e^{i\pi}$, 4) $1 + i = \sqrt{2}e^{i\frac{\pi}{4}}$
5) $\sqrt[n]{z} = \sqrt[n]{r}e^{i\frac{\theta+2k\pi}{n}}, k = 0, 1, \ldots, n-1$

Note. The Euler's formula at the moment is only a convenient notation.
Later in course of complex analysis where complex variable function e^z is defined independently this formula will be proved.

Computing with the $e^{i\theta}$ instead of $\cos\theta + i\sin\theta$ becomes much easier.
For example,
1) $zz' = re^{i\theta} \cdot r'e^{i\theta'} = rr'e^{i(\theta+\theta')}$,
2) $\frac{z}{z'} = \frac{r}{r'}e^{i(\theta-\theta')}$,
3) $\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}$, $\sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2}$
4) $\cos^m\theta = \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^m = \frac{1}{2^m}(e^{i\theta} + e^{-i\theta})^m$

5.2.15. Rational Powers of complex numbers.

Finally, for any $z \neq 0$ and rational $r = \frac{m}{n} \in Q$, where $m \in Z, n \in N$ have no prime common factor (i.e. the form $\frac{m}{n}$ is unique), we can define the rational power z^r as follows:

$$\boxed{z^r = z^{\frac{m}{n}} = (z^{1/n})^m = (\sqrt[n]{z})^m}.$$

Since there are exactly n values of the roots $\sqrt[n]{z}$ then there are exactly n values of the rational power $\sqrt[n]{z}$.

Exercises 5.2.

1. Find the following numbers:

$(1+2i)^2$, $b)\ (1+3i)(2-i)$, $c)\ \frac{(1+3i)}{(2-i)}$, $d)\ 1 + i + i^2 + \cdots + i^{100}$

and their real and imaginary parts.

2. Solve the equations:

$a)\ (2-i)z + (-3+i) = 5 + 2i$, $b)\ \frac{z+1}{z-i} = \frac{1+i}{1-i}$, $c)\ \frac{1}{z+3} = \frac{i}{z-1+i}$,

$d)\ (2+i)z^2 - (5-i)z + 2 - 2i = 0$, $e)\ z^2 + \bar{z} = 0$, $f)\ |z| - iz = 1 - 2i$,

$g)\ z^3 - z^2 + z - 1 = 0$.

3. Express each of the following complex numbers in trigonometric form and:

$a)\ 1$, $b)\ -4$, $c)\ -i$, $d)\ 1 + \sqrt{3}i$, $e)\ \left(\frac{1}{i-1}\right)^{100}$

and then write down them in the form of Euler's formula.

4. Express each of the following complex numbers in Cartesian form:

$a)\ 5\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$, $b)\ 2\left(\cos\frac{\pi}{6} - i\sin\frac{\pi}{6}\right)$, $c)\ e^{-i\pi}$, $d)\ 3e^{29i\pi}$

5. Using a trigonometric form calculate the following complex numbers:

$a)\ \sqrt{2i}$, $b)\ \sqrt{8i}$, $c)\ \sqrt[3]{1}$, $d)\ \sqrt[4]{i}$.

6. Find the distance between the numbers $1 - i$ and $4 + 3i$.

7. On the complex plane C find the points z such that:
$a)\ Re\,z > 1$, $b)\ 1 < Im\,z \leq 3$, $c)\ |z| = 1$, $d)\ |z - (2+3i)| > 1$,
$e)\ 1 \leq |z| < 3$, $f)\ Arg\,z = \frac{\pi}{6}$, $g)\ \frac{\pi}{6} < Arg\,z \leq \frac{\pi}{3}$.

8. Suppose that $k \in R^*, c \in C$ are fixed numbers.
Prove that $kz + \overline{kz} + c = 0$ is the equation of a straight line on the plane C.

9. Show that the equation $z = z_0 + kt$, where $z_0, t \in C$ are fixed, parameter $k \in R$ is the equation of a straight line on the plane C. And vice versa: equation of any straight line on the plane C can be written in the form $z = z_0 + kt$.

10. Show that for any $z, u \in C$ the equality $|z+u| + |z-u| = 2(|z| + |u|)$ is an identity called "parallelogram law". Give geometric interpretation of this identity.

Учебное издание

Karmak Bagisbayev

MATHEMATICS FOR COMPUTER SCIENCE

Учебное пособие

Технический редактор В. В. Вербовский
Компьютерная верстка К. Н. Багисбаев
Подписано в печать 27.08.2015. Формат 60x90/16. Бумага офсетная.
Печать цифровая. Объем 9,56. Тираж 500 экз.

Отпечатано в типографии Университета имени Сулеймана Демиреля