Introduction to Mathematics

Lectures

Krasnoyarsk
2008
# Table of Contents

## Preface

| Lecture 1. | The subject of Mathematics and its historical roots | 6 |
| 1.1. | Historical roots of Mathematics. | 6 |
| 1.2. | Subjects of modern Mathematics. | 9 |
| 1.3. | A scheme of practical application of Mathematics. | 11 |

## I. Language of Mathematics.

### Elements of Mathematical Logic

| Lecture 2. | Sentences and operations with them | 20 |
| Lecture 3. | Propositions and their truth tables | 22 |
| Lecture 4. | Proposition Algebra, its principal laws and their application to electrical engineering | 25 |
| Lecture 5. | Indefinite propositions, and operations with them | 29 |
| Lecture 6. | Universal and existential quantifiers, the negation rule | 31 |
| Lecture 7. | Types of theorems, methods of proofs. The notions of necessary and sufficient condition | 34 |
| Lecture 8. | The Principle of Mathematical Induction | 37 |

## II. Basic Notions of the Theory of Sets

<p>| Lecture 9. | Basic operations with sets | 42 |
| Lecture 10. | The direct product of sets | 47 |
| Lecture 11. | Set’s mappings | 50 |</p>
<table>
<thead>
<tr>
<th>Lecture</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Binary relations, relations of equivalence and partitions of sets</td>
<td>55</td>
</tr>
<tr>
<td>III</td>
<td><strong>Cardinalities of sets</strong></td>
<td>60</td>
</tr>
<tr>
<td>13</td>
<td>The notion of equinumerousity</td>
<td>61</td>
</tr>
<tr>
<td>14</td>
<td>Countable sets</td>
<td>65</td>
</tr>
<tr>
<td>15</td>
<td>Continuum Cardinality</td>
<td>73</td>
</tr>
<tr>
<td>16</td>
<td>The notion of cardinality, comparison of the cardinalities</td>
<td>81</td>
</tr>
<tr>
<td>IV</td>
<td><strong>Enumerative Combinatorics</strong></td>
<td>89</td>
</tr>
<tr>
<td>17</td>
<td>Combinations and Newton’s binomial formula</td>
<td>91</td>
</tr>
<tr>
<td>18</td>
<td>Permutations and arrangements</td>
<td>96</td>
</tr>
<tr>
<td>19</td>
<td>Permutations with repetitions</td>
<td>100</td>
</tr>
<tr>
<td>20</td>
<td>The inclusion-exclusion principle</td>
<td>104</td>
</tr>
<tr>
<td>21</td>
<td>The hats problem</td>
<td>109</td>
</tr>
<tr>
<td>V</td>
<td><strong>Order Relations and Axiom of Choice</strong></td>
<td>112</td>
</tr>
<tr>
<td>22</td>
<td>Partially ordered and ordered sets</td>
<td>114</td>
</tr>
<tr>
<td>23</td>
<td>Ordinal types</td>
<td>117</td>
</tr>
<tr>
<td>24</td>
<td>Well-ordered sets</td>
<td>119</td>
</tr>
<tr>
<td>25</td>
<td>Zermelo Theorem and Axiom of Choice</td>
<td>124</td>
</tr>
<tr>
<td>26</td>
<td>The Banach-Tarski Paradox</td>
<td>128</td>
</tr>
</tbody>
</table>

**Index of Names**

**Subject Index**

**Bibliography**
Preface

Dear first-year students! This book is addressed especially to you, to beginners of mathematical departments, to future mathematicians or to those who will use Mathematics as an important tool in their activities. One would like this book to help you to learn principal mathematical disciplines: Algebra, Analysis, and Programming. This is the main difference between these lectures and the book by B.V. Gnedenko with almost the same title: "Introduction to the speciality "Mathematics" (see number [4] in the bibliography), for the book [4] lays stress on the representation of Mathematics as a language of different sciences adopted to study natural phenomena. Our book is devoted to the language of Mathematics itself. First of all, I analyze (on the elementary level!) basic notions of the following branches of Mathematics: Mathematical Logic, Sets’ Theory, Combinatorics (see Chapters I.-V.). In the introductory chapter I briefly relate on the historic roots of Mathematics and describe a scheme of its practical application to other sciences. An index with the names of all mathematicians cited in the text (the index contains also brief notes about them), Greek and Gothic alphabets are placed at the end of the book. The chapters are divided on sections with double numeration: the first figure indicates the number of the chapter and the second – the number of the section in the chapter. Referring to the sections I write "s.3.2" (section 3.2). To avoid frequent use of words "theorem is proved" or "which was to be proved", sometimes the sign □ is used instead.

It is worth to note that not all the material of the book is used in lectures. The Theory of Ordinal Types is rather difficult for the first apprehension, however it is included into the book for completeness of the Theory of Powers and it is addressed to the students interested in the topic.
The book is written on the base of the cycle of lectures "Introduction to the speciality" given during the last years by me for students of Department of Mathematics and Computer Sciences of Krasnoyarsk State University.

I would like to note that I am very much obliged to Prof. A.P. Yuzhakov for the appearance of this book; he strictly recommended me to deliver this cycle of lectures and even worked out its coarse plan. At the beginning I accepted this suggestion without ardour but working on the lectures and contacting with students I have discovered it tastes nice and, it seems, I have found some methodical innovations giving the lectures. Profs. K.K. Dzhanseitov and V.A. Sapozhnikov also influenced somehow on the choice of the material for the book. Several helpful suggestions were made by Profs. S.V. Larin and B.V. Yakovlev. I thank all these colleagues of mine. Besides, I am deeply grateful to post-graduate students of Functions Theory Chair N.A. Buruchenko and I.A. Tsikh, and to K. Kozlova for the help in making TeX pictures and the text.

September, 1997

A.K. Tsikh
Lecture 1. The subject of Mathematics and its historical roots

1.1. Historical roots of Mathematics.

For a person reducing Mathematics to solving equations it might appear incredible that tens of thousands of mathematical articles are publishing every year and the number of branches in this science is so great that mathematicians from adjacent directions understand one another worse than physicists or natural scientists. However this is not surprising. One could observe the same phenomenon already at the first stages of Mathematics in ancient Egypt and Babylon. For example, different peoples used different systems of calculus and, of course, they understood one another with difficulties. Note that in that time the highest level in Mathematics was achieved in Babylon where the calculus on the base of sixty was used, i.e. they counted not by units, tens, hundreds etc., but by units (1-s), sixty’s (60-s), three thousand six hundreds (3600-s) etc.

If we follow in historical order the motives of development of Mathematics then we note that practical purposes (related to the necessity of the use of Mathematics in daily life, in other sciences, in military arts) alternated with motives, generated by Mathematics itself. For instance, ancient Egyptians and Babylonians needed to build houses and channels, to measure ares and volumes and so on. That is why the notions of line, surface, angle arose and that is why these ones together with the notion of number had leaded to the notion of value (quantity). As a result, on the base of daily needs, the first branches of Mathematics (Geometry and Algebra) we born. In the late ancient Greece, Ptolemei used some theorems in Astronomy, Papp studied properties of geometrical figures, Diofant found irrational numbers (the fact that diagonal and sides of quadrant are not commensurable) and uses them for solving some algebraic equations). Thus, in the Ancient Greece the first mathematical theories were formed, mathematicians begun to work with notions and established the deductive method of investigation (from simple facts and examples they transited to more complicated facts and propositions, they
proved theorems).

The decline of Greek Mathematics was related with the devastating wars, which caused the creation of the Roman Empire (I A.C.) and with the destruction of the famous Alexandrian Library by Christian fanatics (391 A.C.). The small survived part of the library have served as a base for development of Mathematics in Arabian Islamic States and then in Europe. Arabic mathematicians rewrote, commented and improved achievements of Greek Mathematics; besides, they adopted the notion of negative number from China and took over decimal calculus from India. Arabic mathematicians achieved a high level in the Art of Calculation and Operation with Symbols (which they incorporated into Algebra). In this way they introduced algorithms into Mathematics, i.e. methods consisting of finite number of rules, leading to entirely mechanical solution to any problem from a class of typical ones. Among achievements of Arabic mathematicians we also should mention works on trigonometry stimulated by astronomic observations.

The next turn of the mathematical development was in Middle Age Europe (VI-XVI A.C.). Appearance of the universities played an important role in this development; the oldest university in Europe (medical university) in Italian Salerno (XI A.C.), university of Paris (XII A.C.), Universities in Prague (1348), Krakow (1364), Leipzig (1409), Basel (1459) were among them. For instance, beginning from XV century every Kurf¨ urst or Bürgermeister in Germany aspired to open a university even in a small town. In spite of the fact that Mathematics was not principal discipline in the education of the Middle Age, the universities were important centers of spreading and development of mathematical knowledge.

During Renaissance (XV - XVI A.C.) the Mathematics go out from the knowledge of Ancient Greece and East from the first time. In that time the notions of irrational and imaginary numbers were introduced, the algebraic equations of third and forth orders were solved in radicals, the plane trigonometry was elaborated and the spherical one was introduced. Mathematics became a powerful tool for solving problems related not only with the commerce, the land survey etc., but with new technologies and new
investigations in Natural Sciences.

The development of the capitalism in Europe (since XVII A.C.) caused direct influence of practical needs on Mathematics. Since R. Decart introduced the notion of *coordinates*, Mathematics was considered as a Natural Science Method (in combination with the main method: experimentation). First of all, this was displayed in the investigations of Celestial Mechanics (J. Kepler, G. Galilei, I. Newton). At this time the foundations of Differential and Integral Calculus were formed (I. Newton, G. Leibniz). The speed of the development of Mathematics grew in XVIII century. The shipbuilding (Stability Theory for ships), War Technology (Theory of projectile flight), Hydrodynamics and Hydraulics, Physics of Heat Processes, Physics of Electromagnetic Phenomena became spheres of influence of Mathematics. Differential Equations, describing movements of bodies in Mechanics, and other natural phenomena, began to dominate in Mathematics. A great contribution in the development of Mathematics in XVIII century was made by L. Euler; he was born in Basel (Switzerland) but he lived mostly in Russia, being academician of S.-Petersburg Academy of Sciences. Among achievements of XVII ( century we note a new branch of Geometry, the Projective Geometry; its appearance influenced Fine Arts as well as practical needs. One of the founder of Projective Geometry was G. Desargues; he used Perspective’s Theory created in Fine Arts (L. da Vinci) and described in Arts Theory (A. Dürer). Projective Geometry became a base of the Descriptive Geometry; the last is still a foundation for the most complicated engineering drafts, i.e. it is a language of mechanical engineers.

At this point we stop the list of the principal achievements of Mathematics up to XVIII century; according to S.N. Markov [12], we divide History of Mathematics on the following periods:

- *the period of accumulation of elementary mathematical facts* (Mathematics of Ancient Egypt and Babylon);

- *the period of Mathematics of constant values* (Mathematics of Ancient Greece and Middle Age China, India, Islamic Caliphate and Europe);
• the period of Mathematics of variable values (European Mathematics in XVII-XVIII centuries).

During these three periods, the ground for the fourth one the period of modern Mathematics, including XIX, XX, and XXI centuries, was prepared. Now we briefly characterize it.

1.2. Subjects of modern Mathematics.

The four periods of development of Mathematics correspond to the four stages of its teaching. The period of accumulation of elementary mathematical facts corresponds to the teaching in modern Elementary School. Mathematics of constant values is taught now in the Secondary School. The last years of Secondary School and first years of Universities are devoted to Mathematics of variable values. Finally, the modern Mathematics is studied on the middle and the last courses of the universities. In order to give an idea of the corresponding disciplines we briefly summarize the main achievements of modern Mathematics, and describe the formation of its branches and disciplines during last two centuries.

We begin with Algebra. Due to Abel and Galua (the first part of XIX A.C.), theoretic-group methods (theory of groups) were created in this discipline. These methods played great role in modern Algebra and its application in Physics, Geometry and other branches of Mathematics. Studies by Abel and Galua were related to the proof of the absence of the radical solutions to algebraic equations of degree five and higher. Also works of Hilbert had great influence on the development of Algebra in XX-th century; his results leaded to the formation of Algebraic Geometry where such subjects as curves and surfaces are studied with the use of algebraic equations defining them.

In the middle of XX century, the creation of Mathematical Analysis was finished on the base of the notions of real number and limit (Cauchy, Weierstraß). In the frames of Analysis, a new discipline, function's theory of complex variables, appeared; it was successfully applied in Hydrodynamics, Aerodynamics, and also in modern Physics (Theory of Quantum Field). The
developments of Hydrodynamics, Elasticity Theory, and the formation of the Theory of Electromagnetic phenomena (Maxwell, XIX A.C.) generated in the frames of Analysis a new discipline: Theory of partial differential equations. We emphasize that the Theory of Electromagnetic phenomena resulted on the scale of the use of Mathematical Analysis as a tool for studying the Nature. Born on the base of de Kulon’s electrostatic law and Faraday’s electromagnetic law, the notion of the field became omnipresent in descriptions of many physical (and other) processes; besides, the notion dictates the use of mathematical analysis because fields are usually interpreted as vector functions. We also note the branch of functional analysis where the spaces (sets), which have functions of various classes as elements, are studied.

Geometric Science was devoted to the foundations of non-Euclidean Geometries (Gauß, Lobachevsky, Riemann). These geometries played significant role in construction of General Relativity Theory (Einstein). All the geometries are classified with respect to types (Klein): geometries have the same type if they study figures’ properties, invariant under some transforms. For instance, Euclidean Geometry (which was taught in the Secondary School) studies figures’ properties, invariant under transformations reduced to parallel transfer, rotation and mirror reflection. Without exaggeration one can say that the leading type of geometry of XX century is Topology, in particular, its part: Algebraic topology (Riemann, Poincaré). Topology studies figures’ properties, invariant under continuous transformations (deformations); one say that a topologist does not distinguish a sport wight and a bagel, or a coffee cup because each of them can be transformed into another one (it is easy to imagine if we suppose that they are rubber). At the beginning of the XX century an infinite-dimensional geometry was created (Hilbert); it was applied in Quantum Physics. Investigations in Physics, Chemistry and Microbiology greatly influenced on the Geometrical Science. As a result, Geometry became less visual because our eyes can not see phenomena at the level of micro cosmos: we need multi-dimensional and even infinite-dimensional spaces for their description.

Abundance of various theories and contradictions related to the use of
infinite sets demand revision of the Mathematics Foundations. As a result, the new directions (Sets’ Theory and Mathematical Logic) were created. Their foundations are exposed in Chapters I., II., III. and V. of the present book. Note that analysis of the main states of Sets’ Theory and Mathematical Logic leaded to the introduction of notions of computable number and recursive function which played an important role in the creation of computers.

To the middle of XX-th century Theory of Probabilities and Mathematical Statistics (Kolmogorov and others) were formed on the base of the notion of measure from Mathematical Analysis. Probabilistic methods are widely used in Physics, Biology, Economics.

In conclusion, we would like to emphasize the difference between words "to learn" and "to study" ("to investigate") used above. We understand "to learn" as mastering known results; "to study" means obtaining new results. Hence we may say that the professionality is specific for a modern mathematical investigation. Despite that the fashion in Mathematics is still defined by Physics (Quantum and Nuclear Physics) (Biology), Mathematics is made by professional mathematicians working in mathematical institutes or by professors/students of the universities. For instance, in Russia the main scientific mathematical institutes are Steklov Mathematical Institute in Moscow, Sobolev Institute of Mathematics in Novosibirsk, Calculation Centers in Moscow and other cities. Note that in the middle of XX-th century Moscow becomes a World Mathematical Center of the highest level as, for instance, Princeton in USA and Paris in France.

1.3. A scheme of practical application of Mathematics.

In order to communicate and to express thoughts Men created the greatest tool: Living Oral Language and its written version. However, despite that the Language is many-sided and very flexible, it is often insufficient for modern men even for the communication. For example, it is impossible to imagine that a building plan for an Atomic Power Station, a plane or a modern war ship was expressed on a daily language. In these cases people use drafts as an
additional language helping to communicate effectively (even without knowing the native language of the engineer prepared the droughts). It is not incidental that the droughts are written on the language of Mathematics (the Descriptive Geometry). It appears that Mathematics is a language of the most of Technical and Natural Sciences (Physics, Chemistry, Biology etc.) and, in the last time, of some Human Sciences (Economics, Linguistic, Psychology). Already in XVI century, one of the founder of Exact Natural Science, G. Galilei, said that "the great book of the Universe can be understood only by the person knowing its language and signs used to write it; but it is written in the language of Mathematics". There are many other aphorisms about the role of Mathematics and its interaction with other sciences. Among them we note the words of famous Renaissance encyclopedic scientist Leonardo da Vinci: "A men study can not be named a true science if it did not come through a mathematical proof". Summarizing this aphorism, the famous mathematician of XIX century Gauß said that Mathematics is a Queen of Sciences.

The experience of the last four centuries shows that mathematics is used as a language and a tool for solving problems of men. A scheme of application of Mathematics is shown on picture 1.

Let us explain this scheme and then let us demonstrate it on examples. The question is in the following. Investigating a natural phenomenon, technical, economical or social process we do a logical analysis of the problem and then we choose only essential for us properties from a variety of them; later we will use only the chosen properties. Of course, on this way we obliged to do some simplifying assumptions on the acting forces, connections, relations etc. in the consideration. As a result we obtain a model of the phenomenon which is not identical to the phenomenon itself; this model gives only its representation helping to understand the process, an approximation of the reality. Note that our assumptions might be very poor but nevertheless the model might give a very satisfactory approximation.

After the model is constructed we need reformulate the initial problem in the frames of the model on the language of Mathematics. For solving the obtained mathematical problem we need to choose corresponding apparatus
Lecture 1. The subject of Mathematics and its historical roots

A Problem

The Mathematical Model

Looking for a known or the creation of a new mathematical apparatus

Exact solution

Approximate numerical solution

The result (qualitative or quantitative)

The comparison with experiment

Pic. 1.
Lecture 1. The subject of Mathematics and its historical roots

(i.e. tools and methods). It happens that the method is already elaborated by other mathematicians otherwise we need to create it ourselves.

Mastering the method we solve the problem and obtain an answer in terms of exact formula or in terms of qualitative description or in terms of approximate numerical data. Then we compare the answer with experimental data and, if they are coherent, we may say that the model was well chosen. If we found that there is an essential difference between the answer and the experimental data then we need either to correct the model or to reject it.

Let us explain these on the example of the main problem of Celestial Mechanics. The problem is to predict positions of all the Planets in Solar System on great intervals of time. Creating the corresponding model, I. Newton made a logic analysis of already known at that time empiric J. Kepler’s Laws:

Law 1. the orbit of every planet is an ellips with the sun $S$ at a focal point (see picture 2);

Law 2. during equal intervals of time the radius-vector of the planet’s movement covers figures with equal squares (on the picture 2 these figures are shaded);

Law 3. the period of a planet’s movement around the sun is proportional to the size of the orbit at the degree $3/2$.

Trying to explain the empiric Kepler’s Laws, I. Newton suggested the Gravitational Law. Mathematical form of this law is a foundation of the model of Celestial Mechanics. This model is based on the following two assumptions:
1. The sun and the planet are material points placed at the mass centers of the corresponding bodies with the same masses;

2. every two celestial bodies with masses $m_1$ and $m_2$ respectively, posed at distance $r$ between them, generate a gravitational force which acts along the line, connecting the bodies, and equals to the quantity

$$F = f \frac{m_1 m_2}{r^2},$$

where $f$ is the gravitation constant (calculated on the base of experiments).

Constructing the model, the specialists in Celestial Mechanics first of all checked that it corresponded to the Kepler’s Laws. As an example, we give Newton’s deduction of the Second Kepler’s Law. The mathematical apparatus, used by Newton, was Elementary Geometry. Thus, assume that, in a given moment of time, the planet is at the point $P_0$ (pic. 3).

If the sun $S$ would not attract the planet at this moment then the planet would move uniformly along a part of a line; in this way, during the first time interval, it would pass the segment $P_0P_1$ and, during the second one, it would pass the segment $P_1P'_2$ belonging to the same line and having the same length as $P_0P_1$. Note that the squares of the triangles $SP_0P_1$ and $SP_1P'_2$ are equal because they have equal bases $P_0P_1$ and $P_1P'_2$ and the same height (the perpendicular from the apex $S$ to the extension of the bases of the triangles). But the sun does attract the planet, hence the true position of the planet after the second time interval would be the point $P_2$; according to the Parallelogram Rule, the point $P_2$ is defined by force vector $F$ (directing from $P_1$ to $S$) and the the
force, pushing the planet from force of inertia (and directing from $P_1$ to $P_2'$).
As a result, the point $P_2$ belongs to the line passing from $P_2'$ and parallel
to $SP_1$. Now we conclude that the triangles $SP_0P_1$ and $SP_1P_2$ have equal
heights lowered on the common base $SP_1$, and therefore their squares are also
equal. So, we established the Second Kepler’s Law. Similarly one could deduce
two other Kepler’s Law from the assumptions 1 and 2 of Celestial Mechanics.
Thus, we may assume that the model corresponds to the experimental data.
In fact, during last 150 years, using this model, it was possible to predict the
existence of two new planets of Solar System that were not seen in the sky
before. Namely, as the most remote planets moved irregularly with respect
to the model, the astronomers assumed the existence of one more unknown
planet. Comparing real planet’s deviations with the ones obtained under the
assumption of the existence of a new planet, astronomers calculated its unknown
mass, distance from the sun and position on the sky at a time moment. With
this method, the eighth planet Neptun (1846) and the ninth planet Pluton
(1930) were discovered.

The model is still served well even in the time of explorations of Cosmos.
However, as we already noted, any model is not a reality but its approximation
only. Hence it can not be used in all the situations. Even now there are problems
where the initial model of Celestial Mechanics is not fit and a modification of
it is necessary. For instance, the model could not explain the deviations of
Mercury at the beginning of XX-th century. An explanation was found after
the correction of the model with the use of A. Einstein’s General Relativity
Theory.

We can list a lot of mathematical models, playing important role
in Natural Sciences. Among them we note Maxwell’s model of Theory of
Electromagnetic Phenomena, various models of Quantum Physics, the model
of global biosphere processes in Ecology. For example, in the last model
three interacting blocks were considered: "Regions of the land", "Ocean",
"Atmosphere". The division of the land on the regions is made with respect to
natural and political borders. Ecologically, every region is characterized by the
quantity of carbon and nitrogen in the living and dead vegetable mass; besides
the interchange of carbon dioxide gas between the land and the atmosphere, the demographic and economical processes are taken into the consideration. In the block "Ocean", the interchange of carbon dioxide gas between the ocean and the atmosphere, the ocean pollutions, the actions of plants, animals and microbes are accounted. In the block "Atmosphere", the parameters of the climate, changing under human activities, are calculated. The model allows to calculate (with the use of computers) the changes in ecological, climatic and demographic processes in various regions of the World for long periods (up to tens of years) in various scenario of the human activity. In particular, probable consequences of a nuclear war were calculated with the use of this model. The model was constructed in Calculation Center of Soviet Academy of Science in Moscow.
Chapter I.

Language of Mathematics.

Elements of Mathematical Logic
A conclusion is one of the acts enriching the human cognition. The main purpose of Logic is to establish the methods of a "correct conclusion". Every mathematical proof consists of a chain of "correct" conclusions; it is based on the rules of the so-called Mathematical Logic which we now consider.
Lecture 2. Sentences and operations with them

We begin with simple narrative sentences. To denote them, the letters \( A, B, C, \ldots, a, b, c \ldots \) are usually used. For example,

\[ A = [\text{The number 5 is prime}] \]
\[ B = [\text{The number } n^2 + n + 41 \text{ is prime}] \]
\[ C = [\text{The sum of all angles in triangle is equal to } 180^\circ] \]

We can construct more complicated sentences using the following simple operations (constructions):

- the particle "not" (or the phrase "is not true that");
- the conjunction "and";
- the disjunction "or";
- the phrase "if ... then ...";
- the phrase "if and only if ...".

Each of these operations has a name. Let us list these names and simultaneously give the exact definitions of the operations.

**Definition 2.1.** The **negation** of a sentence \( A \) is the sentence [it is not true that \( A \)]. This sentence we denote by \( \overline{A} \).

**Definition 2.2.** The **conjunction** of two sentences \( A, B \) is the sentence [\( A \) and \( B \)]. We denote it by \( A \wedge B \) (or \( A \& B \)).

**Definition 2.3.** The **disjunction** of two sentences \( A, B \) is the sentence [\( A \) or \( B \)]. We denote it by \( A \vee B \).

**Definition 2.4.** The **implication** of two sentences \( A, B \) is the sentence [If \( A \) then \( B \)]. This sentence is denoted by \( A \rightarrow B \).

**Definition 2.5.** The **equivalence** of two sentences \( A, B \) is the sentence [\( A \) if and only if \( B \)]. This sentence is denoted by \( A \leftrightarrow B \).

Successively using the operations \( \neg, \wedge, \vee, \rightarrow, \leftrightarrow \) we can obtain any composite sentence.
Example 2.1.

\( A = [The \ trinomial \ x^2 + px + q \ has \ two \ different \ real \ roots]. \)
\( B = [The \ discriminant \ p^2 - 4q \ of \ the \ trinomial \ is \ greater \ than \ zero]. \)

Then the proposition

\[ A \leftrightarrow B \]

can be read in the following way.

\[ The \ trinomial \ x^2 + px + q \ has \ two \ different \ real \ roots \ if \ and \ only \ if \ the \ discriminant \ p^2 - 4q \ is \ greater \ than \ zero. \]

This proposition is the famous fact from the school mathematics.

Example 2.2.

\( p = [The \ angle \ B \ of \ the \ triangle \ ABC \ is \ right], \)
\( q = [The \ angle \ A \ equals \ to \ 30^\circ], \)
\( h = [|BC| = \frac{1}{2}|AC|]. \)

In this way the composite sentence

\[ (p \land q) \rightarrow h \]

is also a famous geometrical fact:

\[ in \ a \ right-angled \ triangle, \ the \ leg, \ facing \ the \ angle \ of \ 30^\circ, \ equals \ to \ the \ half \ of \ the \ hypotenuse. \]

We will pay attention not to all the sentences but to the propositions only; we will study them below.
Lecture 3. Propositions and their truth tables

Definition 3.1. The *proposition* is a sentence about which one can say it is either true or false.

For instance, among the sentences listed at the beginning of lecture 2, $A$ and $C$ are propositions but $B$ are not. Indeed, for $n = 1$ the number $1^2 + 1 + 41 = 43$ is prime and for $n = 41$ the number $41^2 + 41 + 41 = 41 \times 43$ is composite; thus we can not definitely say whether $B$ is true or false.

What can one say about the truth of a composite proposition if we know the truth or falseness of propositions containing in it? To solve the problem we accept the following agreements.

1. The negation $\overline{A}$ is true if and only if $A$ is false.

\[
\begin{array}{|c|c|}
\hline
A & \overline{A} \\
\hline
\text{true} & \text{false} \\
\text{false} & \text{true} \\
\hline
\end{array}
\]

2. The conjunctions $A \land B$ is true if and only if $A$ and $B$ are simultaneously true.

\[
\begin{array}{|c|c|c|}
\hline
A & B & A \land B \\
\hline
\text{true} & \text{true} & \text{true} \\
\text{true} & \text{false} & \text{false} \\
\text{false} & \text{true} & \text{false} \\
\text{false} & \text{false} & \text{false} \\
\hline
\end{array}
\]
3. The disjunction $A \lor B$ is true if and only if one of the propositions ($A$ and $B$) is true.

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \lor B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
</tbody>
</table>

4. The implication $A \rightarrow B$ is false if and only if $A$ is true and $B$ is false.

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \rightarrow B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
</tr>
</tbody>
</table>

5. The equivalence $A \leftrightarrow B$ is true if and only if $A$ and $B$ are simultaneously true or simultaneously false.

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \leftrightarrow B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
</tr>
</tbody>
</table>
Note that these agreements correspond to the sensual truth of the composite propositions. The listed agreements are reflected in the following tables.
**Lecture 4. Proposition Algebra, its principal laws and their application to electrical engineering**

As in Human Society the juridical laws should provide the "correct" relations of men, there are also laws of Mathematical Logic providing the "correct" proofs of theorems. Generally speaking, a law of Mathematical Logic is a scheme for constructing true propositions. For more exact definition we introduce the following notion. The set of all the propositions together with the operations defined in lecture 3 (the negation, the conjunction, the disjunction, the implication and the equivalence) and their truth tables is called *Propositional Algebra*.

**Definition 4.1.** A *law* of the propositional algebra is such a scheme (a sequence) consisting of (symbolic) propositions, connected by operations of the propositional algebra, that the resulting composite proposition has the true value under any truth values of the (symbolic) propositions in the scheme.

For instance, the scheme $A \rightarrow B$ is not a law, but the scheme $(A \rightarrow B) \rightarrow (\overline{A} \vee B)$ is a law of the propositional algebra. Indeed, the first scheme is false if $A$ is true and $B$ is false. For the second scheme we easily have the following truth table

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$\overline{A}$</th>
<th>$A \rightarrow B$</th>
<th>$\overline{A} \vee B$</th>
<th>$(A \rightarrow B) \rightarrow (\overline{A} \vee B)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

proving that the scheme is identically true.

Let us list some basic laws of the propositional algebra.

1. *The Law of the Double Negation*: $\overline{\overline{A}} \leftrightarrow A$. 

25
2. **The Non-contradiction Law**: $\overline{A} \land A$

3. **The Law of the Excluded Middle**: $A \lor \overline{A}$

4. **The Contraposition Law**: $(A \rightarrow B) \leftrightarrow (B \rightarrow \overline{A})$

The reader can easily check the listed schemes are identically true, i.e. they are laws.

The second law states: it is not true that $A$ and not $A$. The law means that $A$ can not be true simultaneously with its negation $\overline{A}$. The situation in Mathematical Logic is considered as *contradictory* if a proposition is true (false) simultaneously with its negation. That is why the law emphasizes that logic, we dealing with, is not contradictory.

The third law states: either $A$ or not $A$. It shows that, for any proposition $A$, either $A$ or its negation is true (recall that the disjunction is true if and only if a proposition in the disjunction is true. Thus, $A$ is either true or false and the middle (the third) possibility is excluded.

Let us have two schemes $M = M(A, B, ...)$ and $N = N(A, B, ...)$. **Agreement.** If a proposition of the type $M = M(A, B, ...) \leftrightarrow N = N(A, B, ...) \leftrightarrow N(A, B, ...)$ is a law of the propositional algebra then we write $M = M(A, B, ...) \leftrightarrow N = N(A, B, ...)$ and we say that $M$ and $N$ are equivalent.

For instance, if $M = A \rightarrow B$, $N = \overline{B} \rightarrow \overline{A}$ then, according to the Contraposition Law, $M = N$. The reader can easily prove the following equivalences.

1. $A \land B = B \land A$ *(the conjunction’s commutativity)*;
2. $A \lor B = B \lor A$ *(the disjunction’s commutativity)*;
3. $A \land (B \land C) = (A \land B) \land C$ *(the conjunction’s associativity)*;
4. $A \lor (B \lor C) = (A \lor B) \lor C$ *(the disjunction’s associativity)*;
5. $A \land (B \lor C) = (A \land B) \lor (A \land C)$ *(the distributivity)*;
6. $A \lor (B \land C) = (A \lor B) \land (A \lor C)$ *(de Morgan’s Laws)*;
7. $\overline{A} \lor B = \overline{A} \land B$
8. $\overline{A} \land B = \overline{A} \lor B$
9. $A \lor A = A; A \land A = A$;
10. $A \land \text{truth} = A; A \lor \text{lie} = A$. 
Let us show two applications of the laws of the propositional algebra.

First, we show how to solve "propositional" equations using the laws. For example, let us consider an equation of the following type:

\[(X \lor A) \lor (X \lor \overline{A}) = B,\]

where \(A\) and \(B\) are given propositions, and \(X\) is an unknown one.

Let us transform the left-hand side:

\[
\begin{align*}
(X \lor A) \lor (X \lor \overline{A}) &= \text{ /by de Morgan’s law/} \\
(X \lor A) \land (X \lor \overline{A}) &= \text{ /by the distributive law/} \\
X \lor (A \land \overline{A}) &= \text{ /by de Morgan’s law/} \\
\overline{X} \land (A \land \overline{A}) &= \text{ /by the non-contradiction law/} \\
\overline{X} \land (\text{truth}) &= \text{ /by law 10/ = } \overline{X}.
\end{align*}
\]

Therefore the left-hand side is equivalent to \(\overline{X}\), and hence we have \(\overline{X} = B\).

Applying the negation to the both sides of the last equality and using the Double Negation Law we obtain the answer:

\[X = \overline{B}.\]

Let us show how to use the laws of the propositional algebra for simplifying of electrical schemes. With this aim we note that two switches \(A\) and \(B\) connected sequentially conduct the current if and only if they are simultaneously switched on; in the case of the parallel connection they conduct the current if and only if one of them is switched on. Thus, if the position "on" of a switch corresponds to "truth" and the position "off" corresponds to "false" then the sequential connection can be interpreted as the conjunction \(A \land B\) and the parallel one can be interpreted as the disjunction \(A \lor B\).

Let us consider the electric chain 1 (see picture 4).

Obviously, this chain corresponds to the scheme (the symbolic proposition)

\[[(A_1 \lor A_3) \land A_2] \lor [A_1 \land \overline{A_2} \land A_3] \lor [\overline{A_1} \land \overline{A_2} \land A_3].\]
To transform it we use the distributivity law 5, taking out of the second and the third brackets the term $\overline{A}_2 \land A_3$ and obtaining:

$$[(A_1 \lor A_3) \land A_2] \lor [(A_1 \lor A_1) \land (\overline{A}_2 \land A_3)].$$

According to the Law of the Excluded Middle, the term $A_1 \lor A_1$ is true. That is why, using law 10, we conclude that the second bracket is equivalent to $\overline{A}_2 \land A_3$. Therefore the initial scheme is equivalent to the following one:

$$[(A_1 \lor A_3) \land A_2] \lor (\overline{A}_2 \land A_3) = \text{by law 5/}$$

$$[(A_1 \land A_2) \lor (A_3 \land A_2)] \lor (\overline{A}_2 \land A_3) = \text{by laws 4 and 5/}$$

$$(A_1 \land A_2) \lor (A_3 \land \overline{A}_2) = \text{by law 10/}$$

$$= (A_1 \land A_2) \lor A_3.$$ 

Thus, the initial chain is simplified up to (equivalent to) the chain 2 (see picture 5).
Lecture 5. Indefinite propositions, and operations with them

A lot of theorems are of type $A \rightarrow B$ and this means: if $A$ then $B$. Being a theorem, i.e. a true statement, this implication is a proposition. However the parts $A$ and $B$ of the proposition are not always propositions themselves. For instance, consider the following famous algebraic statement: if the discriminant $b^2 - 4ac$ of the quadratic equation

$$ax^2 + bx + c = 0 \tag{5.1}$$

is negative then this equation has no real roots. This statement is an implication of the sentences

$$A = [The \ \text{discriminant} \ b^2 - 4ac \ \text{of equation (5.1) is negative}],$$

$$B = [Equation \ (5.1) \ has \ no \ real \ roots];$$

each of the sentences is not a proposition. However these sentences are the so-called indefinite propositions, which we are to define.

**Definition 5.1.** A sentence (statement) on elements of $M$ which is true for a part of a set $M$ and is false for all the other elements of $M$ is called *indefinite proposition* $M$.

In the example above, the statements $A$ and $B$ are considered on the set of all the equations (5.1); of course, each of the equations is uniquely defined by a trinomial $P = ax^2 + bx + c$. Thus, we can say that $M = \{P\}$ is the set of all the trinomials and the sentences

$$A = A(P) = [The \ \text{discriminant} \ P \ is \ negative],$$

$$B = B(P) = [The \ \text{equation} \ P = 0 \ has \ no \ real \ roots]$$

are indefinite propositions on $M$.

Indefinite propositions on a set $M$ will be denoted by $A(x)$, $B(x)$, ..., if they state on some elements $x \in M$, or by $A(x, y)$, $B(x, y)$, ..., if they state on
pairs of elements \( x, y \in M \), and so on. For instance, if \( M = \mathbb{R} \) is the set of real numbers then

\[
A(x) = [x \text{ is less than } 3], \quad A(x, y) = [x + y \text{ is less than } 1]
\]

are indefinite propositions on \( M \).

It is important to note that, though the indefinite propositions are not propositions, they become ones if we formulate them for a chosen element (pair of elements and so on) of \( M \). For example, for the last two indefinite propositions, setting \( x = 10 \) or \( x = 0 \) and \( y = 1/2 \) respectively, we obtain the propositions

\[
A(10) = [10 \text{ is less than } 3], \quad A(0, \frac{1}{2}) = [0 + \frac{1}{2} \text{ is less than } 1],
\]

the first one being false and the second one being true.

The operations, defined on propositions, are also applicable to the indefinite ones:

- the conjunction: \( A(x) \land B(x) \) (can be read as "\( A(x) \) and \( B(x) \)");
- the disjunction: \( A(x) \lor B(x) \) (can be read as "\( A(x) \) or \( B(x) \)");
- the negation: \( \lnot A(x) \) (can be read as "it is not true that \( A(x) \)");
- the implication: \( A(x) \rightarrow B(x) \) (can be read as "if \( A(x) \), then \( B(x) \)");
- the equivalence: \( A(x) \leftrightarrow B(x) \) (can be read as "\( A(x) \) if and only if \( B(x) \)").
Lecture 6. Universal and existential quantifiers, the negation rule

There are two more special operations for indefinite propositions (in addition to the five ones listed above). Let $A(x)$ be an indefinite proposition on a set $M$. Using it we construct two more sentences:

[For all elements $x$ from $M$ the proposition $A(x)$ is true];

[There exists such an element $x$ from $M$ that $A(x)$ is true].

The following symbols are used for these two propositions:

$(\forall x \in M)A(x)$ (in the first case),

$(\exists x \in M)A(x)$ (in the second case).

If it is clear that the elements $x$ belong to $M$ we can shorten the notations:

$(\forall x)A(x)$ or $\forall xA(x)$,

$(\exists x)A(x)$ or $\exists xA(x)$.

The symbols $\forall$ and $\exists$ are called the quantifiers; the symbol $\forall$ is the universal quantifier (the overturned $A$ because of "all"), and the symbol $\exists$ is the existential quantifier (the overturned $E$ because of "exist").

Example 6.1. If

$$A(n) = [\text{the trinomial } n^2 + 41n + 41 \text{ is prime number}],$$

then $\forall n A(n)$ means that for every natural number $n$ the number $n^2 + 41n + 41$ is prime. In this case the sentence $\forall n A(n)$ is a (false) proposition (see lecture 3). Further, if

$$B(n) = [n^5 + 5n \text{ can be divided by } 6],$$

then the sentence $\forall n B(n)$ is a (true) proposition, because

$$n^5 + 5n = (n - 1)n(n + 1)(n^2 + 1) + 6n$$

and the product $(n - 1)n(n + 1)$ can be divided by 6.
Example 6.2. This is a geometric example. Let $M$ be the set of all triangles on the plane (its elements we denote by $\Delta$) and $N$ be the set of all circles (its elements we denote by $O$). Consider an indefinite proposition

$$A(\Delta, O) = \text{[The circle } O \text{ is inscribed to the triangle } \Delta].$$

Then $(\forall \Delta)(\exists O)A(\Delta, O)$ means that for any triangle there is an inscribed circle.

It is very important to build negations for the propositions with quantifiers. Probably, the reader admits that the following arguments are altogether logic:

$$\neg(\forall x)A(x) = \text{[It is not true that for all } x \text{ the sentence } A(x) \text{ occurs]} = \text{[There is } x, \text{ such that } A(x) \text{ is not true]} = (\exists x)\neg A(x).$$

Similarly,

$$\neg(\exists x)A(x) = \text{[It is false that there is } x \text{ such that } A(x) \text{ is true]} = \text{[For all } x \text{ the sentence } A(x) \text{ is false]} = (\forall x)\neg A(x).$$

These arguments show that constructing the negation for a proposition with quantifiers we must replace quantifier $\forall$ by $\exists$ (and vice versa) and the indefinite proposition $A(x)$ by its negation $\neg A(x)$:

$$\neg(\forall x)A(x) = (\exists x)\neg A(x), \quad \neg(\exists x)A(x) = (\forall x)\neg A(x).$$

The same rule is valid for more complicated propositions with quantifiers. Namely, let $\Omega(\ldots, a, \ldots, b, c, \ldots, d, \ldots)$ be an indefinite proposition on elements of sets $\ldots, A, \ldots, B, C, \ldots, D, \ldots$. Consider a proposition of the type

$$\mathcal{M} = \{(\forall a \ldots \forall b)(\exists c \ldots \exists d)\ldots \Omega(\ldots, a, \ldots, b, c, \ldots, d, \ldots)\}.$$

Here in brackets an alternation of blocks with (universal and existential) quantifiers takes place (it is not important what block is the first or the last). The negation rule (the rule of the transition to $\neg \mathcal{M}$) is the following:
the quantifiers must be replaced by inverse (contrary) ones and the indefinite proposition $\Omega$ must be replaced by its negation,

$$\overline{M} = \{...(\exists a...\exists b)(\forall c...\forall d)...\Omega(..., a, ..., b, c, ..., d, ...)\}.$$  

**Example 6.3.** Let

$$M = [The \ sequence \ \{x_n\} \ is \ bounded].$$

This means that the absolute values of all the elements of the sequence $\{x_n\}$ are less than a real number $C$. Using quantifiers we can write the proposition as follows:

$$M = (\exists C)(\forall n)(|x_n| < C),$$

where the indefinite proposition $\Omega(C, n) = [|x_n| < C]$ is considered on the pairs $C \in \mathbb{R}, \ n \in \mathbb{N}$. The negation for $M$ states that $\{x_n\}$ is unbounded; according to the rule above it can be written as follows:

$$\overline{M} = (\forall C)(\exists n)(|x_n| \geq C).$$

**Example 6.4.** Let

$$N = [The \ number \ a \ is \ the \ limit \ of \ the \ sequence \ \{x_n\}].$$

By limit’s definition this means that for any positive number $\epsilon$ there is a number $N$ such that beginning with it the module of the deviation from $a$ for any element of the sequence $\{x_n\}$ is less than $\epsilon$. Thus,

$$N = (\forall \epsilon > 0)(\exists N)(\forall n \geq N)(|x_n - a| < \epsilon).$$

Hence the statement that the number $a$ is not the limit of the sequence $\{x_n\}$ can be written as follows:

$$\overline{N} = (\exists \epsilon > 0)(\forall N)(\exists n \geq N)(|x_n - a| \geq \epsilon).$$
Lecture 7. Types of theorems, methods of proofs.

The notions of necessary and sufficient condition

It is accepted in the school mathematics that an axiom is a proposition, true by the very definition (i.e. there is no need to prove it). It is more difficult to define a theorem, because it is not so easy to define the notion of a proof. With this purpose we admit the following agreement

Agreement. Let \( A = A(m, n, ...), B = B(m, n, ...) \) be indefinite propositions. If the implication \( A \rightarrow B \) is true every time when \( A \) is true then we write \( A \Rightarrow B \) (as before, it means "if \( A \) then \( B \) or, the same, "\( A \) implies \( B \)"").

In this case the implication \( A \Rightarrow B \) is called theorem.

Note that not all theorems are formulated in the implication’s form. For instance, the famous geometrical theorem states: diagonals of a rhombus are orthogonal. In order to reformulate the theorem in the form above, we consider on the set of all quadrangles \( MNPQ \) two indefinite propositions:

\[
A(MNPQ) = \left[ \text{For the quadrangles } MNPQ \text{ we have} \quad |MN| = |NP| = |PQ| = |QM| \right],
\]

\[
B(MNPQ) = [MP \perp NQ].
\]

Clearly the discussed theorem can be formulated as

\[
A(MNPQ) \Rightarrow B(MNPQ).
\]

The same arguments can be applied to the theorem from Analysis stating that every bounded sequence has supremum (infimum).

Definition 7.1. Theorems of the types \( A \Rightarrow B \) and \( B \Rightarrow A \) are called reciprocal inverse theorems. Besides, if the theorem \( A \Rightarrow B \) is declared direct theorem then the theorem \( B \Rightarrow A \) is called inverse one.
Sometimes both the direct and inverse theorems hold true. For instance, if we define the above propositions \( A(MNPQ) \) and \( B(MNPQ) \) on the set of all parallelograms (but not on the set of all quadrangles!) then the theorem

\[ B(MNPQ) \Rightarrow A(MNPQ) \]

also takes place. In this case, combining the direct and inverse theorems, we obtain "A holds true if and only if B is true". Then one writes \( A \iff B \). 

The proposition \( A \) in the theorem \( A \Rightarrow B \) is called the assumption or the condition while \( B \) is called the conclusion. As, by theorem's definition, the implication \( A \Rightarrow B \) is true every time \( A \) is true, the truth table for the implication implies that if \( A \) is true in the theorem \( A \Rightarrow B \) then necessarily \( B \) is true. That is why one can say that \( B \) is a necessary condition for \( A \) and, in its turn, \( A \) is a sufficient condition for \( B \). Thus, the theorem \( A \iff B \) can be read as "A is the necessary and sufficient condition for B or, the same "A holds if and only if B holds". For instance, the quadratic equation \( x^2 + px + q = 0 \) has no real roots if and only if the discriminant \( p^2 - 4q \) is negative.

Now we should say some words about the ways for proving theorems. Highly relatevely one can determine two principal methods of the proofs: the direct one and the rule of contraries. In order to prove the theorem \( A \Rightarrow B \) directly we need to present an evident chain of theorems \( A \Rightarrow A_1, A_1 \Rightarrow A_2, \ldots, A_{k-1} \Rightarrow A_k, A_k \Rightarrow B \) (or, shortly, \( A \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \ldots \Rightarrow A_k \Rightarrow B \)). The rule of contraries is based on the Contraposition Law stating that theorems

\[ A \Rightarrow B \text{ and } \overline{B} \Rightarrow \overline{A} \]

are equivalent. Thus, in order to prove theorem \( A \Rightarrow B \) it is enough to assume "not \( B \)" (i.e. \( \overline{B} \)) and then to conclude that "not \( A \)" (i.e. \( \overline{A} \)). This means that the assumption of "contrary proposition" (i.e. "not \( B \)" ) leads to a contradiction with \( A \).

Sometimes the rule of contraries is presented in an other form. Usually, the form is used by mathematicians being lazy to look for a direct proof. At first they assume that \( B \) is false and then they remember that \( A \) is true. Hence
they assume \( \overline{B} \land A \). If they succeed to deduce from the last proposition a false one then they can be sure the theorem \( A \Rightarrow B \) is proved. It is not surprising, because the reader can easily check with the use of the truth tables that the propositions

\[
A \rightarrow B \quad \text{and} \quad \overline{B} \land A \rightarrow (\text{false})
\]

are equivalent.

Finally, note that there is one more special method for the proofs relating with the establishment of the truth of an indefinite proposition \( A(n) \) for all natural \( n \). This method is called the Principle of the Mathematical Induction. Let us describe it.
Lecture 8. The Principle of Mathematical Induction

Let \( A(n) \) be an indefinite proposition on the set of the natural numbers \( n \in \mathbb{N} \). The Principle of Mathematical Induction states that the proposition \( A(n) \) is true for all \( n \in \mathbb{N} \) (i.e. the proposition \( \forall n A(n) \) is true) if

1) \( A(1) \) is true;

2) \( A(k) \Rightarrow A(k+1), \ k \geq 1 \), i.e. the truth of proposition \( A(k) \) implies the truth of the proposition \( A(k+1) \) for all \( k \geq 1 \).

We may argue the statement using the rule of contraries. Namely, assume that conditions 1) and 2) hold true but \( A(n) \) is not true for all \( n \in \mathbb{N} \). Consider the subset \( M \) in the set of the natural numbers \( \mathbb{N} \) consisting of all the numbers \( n \) that \( A(n) \) is false:

\[
M = \{ n \in \mathbb{N} : A(n) \text{ is false} \}.
\]

Let \( n_0 \) be the minimal element in \( M \). Note that \( n_0 \neq 1 \), because \( A(1) \) is true. Hence there is \( k \in \mathbb{N} \) such that \( n_0 = k + 1 \); besides, since \( n_0 \) is the minimal element in \( M \), \( A(k) \) is true. Now condition 2) yields \( A(k+1) = A(n_0) \) is also true. This contradicts with the choice of \( n_0 \).

**Remark 8.1.** Usually, the arguments above are not recognized as a proof of the Principle of Mathematical Induction because the principle itself is an axiom in the Peano’ axiomatics of the natural numbers (see Chapter II. below). In its turn, this axiom can be replaced by the used in the argumentation fact: every non-empty set of natural numbers contains its minimal element.

As an application of the Principle of Mathematical Induction, let us calculate the quantity of all subsets of a finite set with \( n \) elements. Let \( M = \{ m_1, ..., m_n \} \) be such a set. We include the empty set \( \emptyset \) (i.e. the set without elements) and the set in \( M \) itself into the set of subsets of \( M \).

**Statement.** If a set \( M \) has \( n \) elements then it has \( 2^n \) subsets.

To prove this we consider the following indefinite proposition:

\[
A(n) = [ \text{a set of } n \text{ elements has } 2^n \text{ subsets} ].
\]
Since a set with one element only has exactly two subsets (the empty set and the set itself), we see that

\[ A(1) = \text{[a set of 1 element has 2 subsets]} \]

is a true proposition.

Assume that a set \( M \) of \( k \) elements has \( 2^k \) subsets. Consider the set \( M' \) of \( k + 1 \) elements obtained from \( M \) by joining an element to \( M \). We claim that the number of subsets of \( M' \) is twice as much as the number of subsets of \( M \). Indeed, among the subsets of \( M' \) there are all the subsets of \( M \) and, in addition, all the subsets of \( M \) with the joined element. Thus, if \( M \) has \( 2^k \) subsets then the set \( M' \) has \( 2 \cdot 2^k = 2^{k+1} \) subsets. The statement is proved.
Chapter II.

Basic Notions of the Theory of Sets
The notion of set is one of the principal mathematical notions. Apparently, it is difficult to give an exact definition of set, because the nature of man’s mind is very complicated. That is why the notion of "set" belongs to the number of indefinable notions. From a naive point of view (which we will follow below), the word "set" is the synonym to the terms "collection" and "aggregate" of some elements or objects. For instance, one can say on a set of students in the room, on a collection of points of a geometric figure, on an aggregate of solutions to equation. In these cases, the students, the points and the solutions are elements of the corresponding sets. The most used among the sets of numbers are the following:

- $\mathbb{N}$, being the set of all the natural numbers $1, 2, 3 \ldots$;
- $\mathbb{Z}$, being the set of all the integers $0, \pm 1, \pm 2 \ldots$;
- $\mathbb{Q}$, being the set of all the rational numbers, i.e. fractions of the type $p/q$, where $p$ is an integer number and $q$ is a natural one;
- $\mathbb{R}$, being the set of all the real numbers (representable by decimal fractions);
- $\mathbb{C}$, being the set of all the complex numbers $a + ib$, where $a$ and $b$ are real numbers and $i$ is the imaginary unit.

It is considered that a set $A$ is defined if a characteristic property of the set’s elements is pointed out (i.e. the property which is possessed by the elements of $A$ only). In order to indicate the fact that an element $a$ belongs the set $A$ one writes $a \in A$. If $a$ does not belong to $A$ then one writes $a \notin A$. For instance, the definition of the set of all the rational numbers can be written as follows:

$$\mathbb{Q} = \{p/q : p \in \mathbb{Z}, \ q \in \mathbb{N}\},$$

where in the braces the characteristic property of elements of $\mathbb{Q}$ is written. In general case, if the characteristic property of a given element $x$ of the set $A$ is written as $P(x)$ (i.e. as the indefinite proposition $P(x)$, see s.5) then one writes

$$A = \{x : P(x)\}.$$
In this way, an interval and a segment of the real axis are defined as follows:

\[(a, b) = \{x : a < x < b\}, \quad [a, b] = \{x : a \leq x \leq b\}.
\]

It may happen that no element has the characteristic property, describing the set \(A\). In this case one says that the set \(A\) is *empty* and writes \(A = \emptyset\). For example, the set of all the real solutions to the equation \(x^2 = -1\) is empty; therefore we write

\[
\{x \in \mathbb{R} : x^2 = -1\} = \emptyset.
\]

If every element of a set \(A\) belongs to a set \(B\) then one says \(A\) is a *subset of \(B\)* and writes \(A \subset B\). By the definition, one says that the sets \(A\) and \(B\) are *equal* and writes \(A = B\) if simultaneously \(A \subset B\) and \(B \subset A\). Thus, in order to prove that \(A = B\) we need to establish the two implications: \(x \in A \Rightarrow x \in B\) and \(x \in B \Rightarrow x \in A\).
Lecture 9. Basic operations with sets

We will discuss the operations: the union, the intersection and the difference; these ones are called algebraic operations. They a similar to the operations in the propositional algebra (the disjunction, the conjunction and the negation). That is why the part of set’s theory studying these operations is called set’s algebra. Note that both the set’s algebra and the propositional algebra are partial cases of Theory of Boolean Algebra (the last is not discussed in this book).

Thus, we begin with exact definitions.

**Definition 9.1.** The **union** of two sets $A$ and $B$ is the collection of all the elements belonging to at least one of the sets $A$ or $B$. It is denoted by $A \cup B$.

**Definition 9.2.** The **intersection** of two sets $A$ and $B$ is the collection of all the elements belonging to $A$ and $B$ simultaneously. It is denoted by $A \cap B$.

**Definition 9.3.** The **difference** of two sets $A$ and $B$ is the collection of all the elements of $A$ which do not belong to $B$. It is denoted by $A \setminus B$.

If $B$ is a subset of $A$ (i.e. $B \subset A$) then the difference $A \setminus B$ is called the complement of $B$ in $A$; it is denoted by $\complement_A B$ (here the symbol $\complement$ is the raffinated letter C, because of "complement"). On the picture 6 the sets $A$ and $B$ are the circles and the shaded parts express the union, the intersection and the difference of these circles.

![Diagram](image)

**Pic. 6.**

Now let us define the union and the intersection operations of more than two sets.
Let a family of sets $A_i$, numbered (indexed) by elements $i$ from a set $I$, is given. In this case, one writes $\{A_i\}_{i \in I}$.

**Definition 9.4.** The *union* of sets $\{A_i\}_{i \in I}$ is the collection of all the elements belonging to at least one of the sets $A_i$.

The defined above union is denoted by \[ \bigcup_{i \in I} A_i. \]

Another definition of the union might be the following: \[ \bigcup_{i \in I} A_i = \{x : (\exists i \in I)(x \in A_i)\}. \]

**Definition 9.5.** The *intersection* of sets $\{A_i\}_{i \in I}$ is the collection of all the elements belonging all the sets $A_i$ simultaneously.

The defined above intersection is denoted by \[ \bigcap_{i \in I} A_i; \]

for it we have \[ \bigcap_{i \in I} A_i = \{x : (\forall i \in I)(x \in A_i)\}. \]

**Remark 9.1.** If the index set $I$ equals to the set of all the natural numbers $\mathbb{N}$ then also the symbols \[ \bigcup_{i=1}^{\infty} A_i, \quad \bigcap_{i=1}^{\infty} A_i \]

are used. If $I$ is a finite subset in $\mathbb{N}$ consisting of the numbers from 1 to $n$ then one writes \[ \bigcup_{i=1}^{n} A_i, \quad \bigcap_{i=1}^{n} A_i. \]

Let us consider some examples.
Example 9.1. Let \( \{A_i\}_{i \in I} \) be a family of intervals

\[
A_i = \left(\frac{1}{i}, 1 - \frac{1}{i}\right) = \left\{ x \in \mathbb{R} : \frac{1}{i} < x < 1 - \frac{1}{i} \right\}.
\]

Let us prove that the union of the family of these intervals is the interval \((0; 1)\):

\[
\bigcup_{i=1}^{\infty} A_i = (0; 1).
\]

According to the definition of the equality of sets, we need to prove two inclusions: the left-hand side in the last equation is a subset of the right-hand side and vice versa. Thus, let \( x \) belongs to the left set. According to the definition of the union, this means that \( \exists i \in \mathbb{N} (x \in A_i) \), i.e. \( \frac{1}{i} < x < 1 - \frac{1}{i} \). Then \( 0 < x < 1 \) and hence \( x \) belongs to the right set: \( x \in (0; 1) \). The Archimedean principle for positive numbers \( x \) and \( 1-x \) implies that there are natural numbers \( i_1, i_2 \) such that \( i_1 x > 1, i_2 (1-x) > 1 \). Combining all these inequalities we see that

\[
\frac{1}{i_1} < x < 1 - \frac{1}{i_2}.
\]

Obviously, if \( i_0 \) is the maximal from the numbers \( i_1, i_2 \) then \( x \) satisfies also the following inequalities \( \frac{1}{i_0} < x < 1 - \frac{1}{i_0} \). Therefore \( x \) belongs to the union of the intervals, i.e. to the left set.

Example 9.2. Consider the family of the intervals

\[
A_i = \{ x \in \mathbb{R} : 0 < x < \frac{1}{i} \} = (0, \frac{1}{i}), \ i \in \mathbb{N}.
\]

Let us prove that

\[
\bigcap_{i=1}^{\infty} A_i = \emptyset.
\]

For this it is enough to prove that every number \( x \) does not belong to one of the intervals \( A_i \). If \( 0 \leq x \) then it does not belong to any \( A_i \). If \( x > 0 \) then the Archimedean principle yields the existence of a number \( i_0 \) with \( i_0 x > 1 \), i.e. \( x > \frac{1}{i_0} \). This exactly means \( x \notin A_{i_0} \), which was to be proved.
Let us list some properties of the algebraic operations for the sets:

1. \( A \cap B = B \cap A \) (the commutativity of the intersection);
2. \( A \cup B = B \cup A \) (the commutativity of the union);
3. \( A \cap (B \cap C) = (A \cap B) \cap C \) (the associativity of the intersection);
4. \( A \cup (B \cup C) = (A \cup B) \cup C \) (the associativity of the union);
5. \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \);
6. \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \).

The identities 5 and 6 express the distributivity properties of the operations.

If \( A \) and \( B \) are subsets of a set \( X \), then the following properties, named de Morgan’s laws are fulfilled:

7. \( \mathcal{C}_X(A \cup B) = (\mathcal{C}_X A) \cap (\mathcal{C}_X B) \);
8. \( \mathcal{C}_X(A \cap B) = (\mathcal{C}_X A) \cup (\mathcal{C}_X B) \).

Property 7 states that the complement of the union is the intersection of the complements. Similarly, property 8 means that the complement of the intersection is the union of the complements.

The reader can easily note that all the eight properties relate to the properties of operations of the propositional algebra (see s.4). The conjunction \( \wedge \) corresponds to the intersection \( \cap \), the disjunction \( \vee \) corresponds to the union \( \cup \) and the negation \( \bar{A} \) corresponds to the complement \( \mathcal{C}_X A \).

Properties 5–8 can be extended to any family of sets:

5’. \( A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i) \);
6’. \( A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i) \).

Moreover, if \( \{A_i\}_{i \in I} \) is a family of subsets in \( X \) then

7’. \( \mathcal{C}_X(\bigcup_{i \in I} A_i) = \bigcap_{i \in I}(\mathcal{C}_X A_i) \);
8’. \( \mathcal{C}_X(\bigcap_{i \in I} A_i) = \bigcup_{i \in I}(\mathcal{C}_X A_i) \).
Properties 1–4 follow from the definitions of the union and the intersection. The proofs of properties 5 and 6 are similar, and we may say the same about the proofs of properties 7 and 8. That is why we will prove properties $6'$ and $8'$ only as they are more general than properties 6 and 8; the proofs of properties $5'$ and $7'$ we leave to the reader.

The proof of property $6'$. Let the element $x$ belongs to the left-hand side set in equality $6'$. According to the definition of the union of two sets, this means that $x$ is an element of $A$ or $(\bigcap_{i \in I} B_i)$. If $x \in A$ then $x \in A \cup B_i$ for all $i \in I$, and then, by the definition of the intersection, it belongs to the right-hand side set in equality $6'$. If $x \in \bigcap_{i \in I} B_i$, then for all $i \in I$ we have $x \in B_i$. Hence $x \in A \cup B_i$ for all $i \in I$. In this way we again obtain that $x$ lies in the right-hand side set in equality $6'$.

Conversely, let $x$ belongs to the right-hand side set in equality $6'$. Using the definition of the intersection we see that $x \in A \cup B_i$ for all $i \in I$, and hence $x \in A$ or $x \in B_i$ for all $i \in I$. However this means that $x$ belongs to $A \cup (\bigcap_{i \in I} B_i)$, i.e. to the left-hand side set $6'$.

The proof of property $8'$. Let us show another form for the proof of the identity of two sets. For an element $x \in X$ we have:

$$ [x \in X \setminus \bigcap_i A_i] \iff [x \notin \bigcap_i A_i] \iff [(\exists i)(x \notin A_i)] \iff [(\exists i)(x \in X \setminus A_i)] \iff [x \in \bigcup_i (X \setminus A_i)]. $$

Obviously, this chain of the equivalences proves property $8'$. 
Lecture 10. The direct product of sets

Except the operations defined in lecture 9, there is one more universal operation (construction); it is called the direct or Cartesian product. For the beginners we emphasize that there is no common between the product of numbers and the direct product. Moreover the last operation is defined for any sets, but not for the numerical only.

Thus, let $A$ and $B$ be some sets.

**Definition 10.1.** The direct or Cartesian product of the sets $A$ and $B$ is the collection of any ordered pairs $(a, b)$ where $a \in A$, $b \in B$. The set of all such pairs is denoted by $A \times B$.

As the pair $(a, b)$ is ordered, $a$ must stand on the first place and $b$ must stand on the second one. Hence the pairs $(a, b)$ and $(b, a)$ are not equal in general. Moreover, the pairs $(a_1, b_1)$, $(a_2, b_2)$ are equal (represent the same element of $A \times B$) if and only if $a_1 = a_2$ and $b_1 = b_2$.

Historically, the notion of the direct set appeared as an instrument to define the position of a point of the plane via two numbers. This pair of numbers is realized as the distances from the point to two fixed orthogonal lines (axis).

This realization was made by R. Decartes (Cartesius); G. Leibniz called the corresponding distances "coordinates" of the point. Thus, choosing two orthogonal axis on the plane, we can define any point by a pair $(x, y)$ where $x, y$ are real numbers. Therefore the plane can be interpreted as the direct product $\mathbb{R} \times \mathbb{R}$ of two copies of real line $\mathbb{R}$.

The notion of the direct product for three sets can be defined as the collection of ordered triplets; similarly, for four sets we should use ordered quadruplets and so on. Let us define the direct set for any number of sets $A_1, \ldots, A_n$.

**Definition 10.2.** The direct product of the sets $A_1, \ldots, A_n$ is the collection of any ordered lines $(a_1, \ldots, a_n)$ with $n$ components, where $a_1 \in A_1$, $\ldots$, $a_n \in A_n$. The set of all such lines is denoted by $A_1 \times \ldots \times A_n$. 

47
If all the sets $A_1, \ldots, A_n$ coincide with a set $A$ then, for the direct product $A \times \ldots \times A$, one writes $A^n$. According to this agreement, the plane with chosen coordinate (axis) system will be identified with $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Similarly the real space is identified with $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Let us give some examples of direct products.

1. The product of two segments $[a, b] \times [c, d]$ can be presented as a rectangle on the plane (see picture 7).

2. The product $S \times [a, b]$ of a circumference $S$ and a segment $[a, b]$ can be interpreted as the side surface of a cylinder (see picture 8).

3. The product of a circle and a segment can be represented by the points of a cylinder.

4. The product $S \times S$ of two circumferences is presented as a the surface from the picture 9). This surface is called two-dimensional torus; it has a form of an inner tube of bicycle (or a bagel). In order to see this, it is sufficient to choose a meridian $S_1$ and a parallel $S_2$ on the surface; then every point $p$ of the surface corresponds to a pair $(a, b)$, where $a$ is the projection to the
circumference $S_1$ and $b$ is the projection to the circumference $S_2$ (see picture 10).
Lecture 11. Set’s mappings

The notion of set’s mapping is a generalization for the school notion of function. Recall that a function, defined on a set \( M \subset \mathbb{R} \), is a rule relating to a number \( x \in M \) a definite (i.e. unique) number \( y \in \mathbb{R} \). Now we can take any set (also non-numerical) instead of \( M \) and \( \mathbb{R} \). Thus, let \( M \) and \( N \) be some sets.

**Definition 11.1.** The *mapping* (or map) from the set \( M \) to the set \( N \) is a rule relating to each element \( x \in M \) a definite (i.e. unique) element \( y \in N \).

If the rule is denoted by \( f \) then for the element \( y \) related to \( x \) one writes \( y = f(x) \). A more complete denotion for the mapping is the following: \( f : M \rightarrow N \). In this case the element \( y \) is called the *image* of the element \( x \) and \( x \) is called the *preimage* of \( y \).

It may happens that an element \( y \in N \) has no preimages; but often there can be more than one preimages too. In the last case, one can speak on a *full preimage* of the element \( y \in N \) being the set \( f^{-1}(y) := \{ x \in M : f(x) = y \} \).

Thus, by the definition, the full preimage is the set of all the elements \( x \) related to the element \( y \), i.e. such that \( f(x) \) is equal to \( y \). Similarly, for a set \( B \subset N \), its full preimage is defined as \( f^{-1}(B) := \{ x \in M : f(x) \in B \} \).

If \( A \) is a subset of \( M \) then its image under the mapping \( f \) is the set \( f(A) := \{ f(x) : x \in A \} \).

Consider some examples.

1. Every function \( y = f(x) \), defined on the real line \( \mathbb{R} \), is a map \( f : \mathbb{R} \rightarrow \mathbb{R} \), i.e. a map of \( \mathbb{R} \) in to \( \mathbb{R} \).

2. It is known that curves on the plane \( \mathbb{R}^2 \) (with variables \((y_1, y_2)\)) can be defined with the use of a parametric representation, i.e. as vector function
(y_1(x), y_2(x)) depending on the variable x. Hence a curve on the plane can be presented by the mapping $f : \mathbb{R} \to \mathbb{R}^2$, defined by the relation

$$x \to (y_1(x), y_2(x)).$$

For instance the unit circumference with the center at the origin is given by the map

$$x \to (\cos x, \sin x).$$

Similarly, curves at the space $\mathbb{R}^3$ can be presented with the use of a map $f : \mathbb{R} \to \mathbb{R}^3$, defined by the relation

$$x \to (y_1(x), y_2(x), y_3(x)).$$

3. Every function of several real variables $x_1, ..., x_n$ can be interpreted as a map $f : \mathbb{R}^n \to \mathbb{R}$, because it relates to each collection of values $x_1, ..., x_n$, i.e. to the vector $x = (x_1, ..., x_n)$, a definite real number $y \in \mathbb{R}$.

4. Using examples 1, 2, 3, one can do the following step to generalize the notion of the function. Consider the problem on the structure of a map $f : \mathbb{R}^n \to \mathbb{R}^m$ with arbitrary numbers $n$ and $m$. Every such a map relates to each vector $x = (x_1, ..., x_n) \in \mathbb{R}^n$ a vector $y = (y_1, ..., y_m) \in \mathbb{R}^m$. As the image $y$ depends on its preimage $x$, the dependence takes place for coordinates $y_1, ..., y_m$ of the element $y$ too. Thus, the relation has the form

$$x = (x_1, ..., x_n) \to y = (y_1(x), ..., y_m(x)),$$

i.e. the mapping $f$ is defined by $m$ functions

$$y_1 = f_1(x) = f_1(x_1, ..., x_n),$$

$$\ldots \ldots$$

$$y_m = f_m(x) = f_m(x_1, ..., x_n).$$

Thus, every map $f : \mathbb{R}^n \to \mathbb{R}^m$ is given by the system (vector–function)

$$f = (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$$

of $n$ variables.
5. Consider the set of all the integrable functions on the segment \([a, b] \subset \mathbb{R}\) as \(M\). On this set we define a map to the real line \(\mathbb{R}\) as follows: to each function \(\varphi(x) \in M\) we set

\[
f(\varphi(x)) = \int_a^b \varphi(x) \, dx.
\]

Hence the map \(f\) relates to a function \(\varphi(x) \in M\) the number being equal to the integral of this function over the segment \([a, b]\).

6. Let \(M\) be the set of all the differentiable functions on the interval \((a, b) \subset \mathbb{R}\), with continuous derivatives and \(N\) be the set of all the continuous functions on \((a, b)\). For these sets special symbols are used: \(C^1(a, b)\) for \(M\) and \(C(a, b)\) for \(N\). Then one can define the mapping

\[
f : C^1(a, b) \to C(a, b),
\]

relating to every function \(\varphi(x) \in C^1(a, b)\) its derivative \(\varphi'(x)\):

\[
f(\varphi(x)) = \varphi'(x) = \frac{d\varphi(x)}{dx}.
\]

Let us continue to study the mappings.

**Definition 11.2.** A map \(f : M \to N\) is called *injective* if it relates different elements of \(N\) to different elements of \(M\), i.e. if for \(x_1, x_2 \in M\)

\[
x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).
\]

Thus, the injective maps are one-to-one mappings. For example, the function \(y = \tan x\) is injective, if we define it on the interval \(M = (-\frac{\pi}{2}, +\frac{\pi}{2})\). At the same time, the functions \(y = x^2\), \(y = \sin x\) are not injective on \(\mathbb{R}\), since, for instance, the squares \((-1)^2\) and \((1)^2\) coincide for the different numbers \(-1\) and 1.

**Definition 11.3.** The mapping \(f : M \to N\) is called *surjective*, if the image \(f(M)\) equals to \(N\). This means that for every element \(y \in N\) there exists \(x \in M\) with \(f(x) = y\).

Sometimes, the surjective mapping is called the "mapping onto" emphasizing that it maps onto the whole set \(N\).
Definition 11.4. The map $f : M \to N$ is called bijective, if it is simultaneously injective and surjective. Hence a bijective map is a one-to-one map between $M$ and $N$.

For instance, the function $y = \tan x : (-\frac{\pi}{2}, +\frac{\pi}{2}) \to \mathbb{R}$ is bijective but the function $y = x^2$ is not.

Note that for a bijective map $f : M \to N$ one can define the inverse map

$$f^{-1} : N \to M$$

from the set $N$ to the set $M$. Namely, given element $y \in N$, we can find the unique element $x \in M$, mapped under $f$ into $y$. We relate it to the element $y$, obtaining the rule $x = f^{-1}(y)$. Clearly, the mapping $f$ and its inverse one have the following properties:

$$f^{-1}(f(x)) = x, \ f(f^{-1}(y)) = y.$$

Let us list some properties of mappings.

1. For $A, B \subset N$ we have $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
2. For $A, B \subset N$ we have $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
3. For $C, D \subset M$ we have $f(C \cup D) = f(C) \cup f(D)$.

However, the identity

$$f(C \cap D) = f(C) \cap f(D)$$

is not always true. Consider, for instance, the projection map acting from the plane $\mathbb{R}^2$ onto the axis $x_1$, i.e. $f : \mathbb{R}^2 \to \mathbb{R}$, where

$$f(x_1, x_2) = x_1.$$

If $C$ and $D$ are two different lines, parallel to the axis $x_1$ (see picture 11), then $D \cap C = \emptyset$, $f(C) = f(D) = \mathbb{R}$. Therefore $f(C \cap D) = \emptyset$ while $f(C) \cap f(D) = \mathbb{R}$.
At the end of this lecture we define a generalization to composite function. Let two maps

$$f : A \rightarrow B, \quad g : B \rightarrow C$$

be given. Then one can define the map from $A$ to $C$, relating to every element $a \in A$ the element $g(f(a))$. This map is denoted by $g \circ f$; it is called the *composition* of $f$ and $g$.

Let us give two geometric examples of the compositions; note that the maps acting from the plane to the plane (or from the space to the space) are often called transformations of the plane (of the space). Among canonic plane transformations are the "parallel translation", "symmetry with respect to points or planes", "rotation" of the plane on a fixed angle. It is not difficult to check that the composition of two symmetries with respect to points $O_1$ and $O_2$ coincides with the parallel translation on the vector $\overrightarrow{O_1O_2}$. Similarly, the composition of two symmetries with respect to lines $l_1$ and $l_2$, intersecting at the point $O$ under the angle $\alpha$, can be reduced to the rotation of the plane around this point on the angle $2\alpha$. 

![Pic. 11.](image)
Lecture 12. Binary relations, relations of equivalence and partitions of sets

The elements of sets can not be interesting themselves (without their mutual relations) in mathematics. For instance, the set of all the natural numbers is one of the most important sets because of the possibility to confer the numbers with respect to the relation "more" or "less" between them. The effective use of geometric ideas is impossible without the relation of the belonging a point to the line, the relation of the parallelism of lines, the relation of the similarity for figures. Any axiomatic theory in Mathematics proceeds from two things: the sets of objects (elements) and the collection of the relations between the objects. Then axioms are defined on the language of the relations. For instance, Peano’s axiomatics of the natural series has natural numbers as the objects; its principal undefined relation is the relation "to follow immediately after". Besides, the following axioms must hold:

1) There is an object, i.e. a natural number which does not follow after any natural number; this number is called the unit and it is denoted by 1.

2) for every natural number \( n \), there is a unique natural number \( n' \), following immediately after \( n \);

3) for every natural number \( n \neq 1 \), there is a unique natural number \( n' \) followed immediately by \( n \);

4) if a set \( A \) of natural numbers contains the unit and contains any number \( n \) as well as the number \( n' \) following immediately after it, then \( A \) equals to the set of all natural numbers.

Similarly, constructing the Euclidean Geometry, one starts from points, lines, planes, as objects, and from relations expressed, by words "to belong", "between", "congruent". Hilbert’s axiomatic of the Euclidean geometry has 20 axioms on the objects above. For instance, there are the following among them:

– for every two points \( A \) and \( B \) there exists a line \( l \), containing these point;

– for every two points \( A \) and \( B \) on a line \( l \) there is at least one point \( C \)
such that $B$ lies between $A$ and $C$.

Note that the relation "to follow immediately after" in the axiomatics of the natural series is defined for a pair $(n, n')$ of natural numbers while, in the axiomatics of Euclidean Geometry, the relation "to belong" is defined for the triplet of objects $(A, B, l)$ in the first axiom above and for the quadruplets $(A, B, l, C)$ in the second one. The relations, defined for pairs, triplets and quadruplets of objects, are called binary, ternary and quaternary respectively; the relations defined for $n$ objects are called $n$–ary.

Let us consider binary relations in detail. If a pair of objects $a, b$ are binarily related then one writes $a \varphi b$ where the symbol $\varphi$ denotes the relation. In fact, the term $a \varphi b$ means that $a$ relates to $b$ with respect to $\varphi$. For instance, $\varphi$ may expresses the equality relation $a = b$, the order relation $a < b$ on the set of real numbers, the relation "to belong" $a \in l$, where $a$ is a point and $l$ is a line on the plane. If, for example, $\varphi$ is the order relation "<" then we can write $2 \varphi 3$ (because 2 is less than 3), but we can not write $3 \varphi 2$ or $9 \varphi 5$. If the binary relation $\varphi$ is defined on pairs of elements from sets $A$ and $B$ then, obviously, to define the relation $\varphi$ is the same as to distinguish the collection of all "marked" ordered pairs $(a, b)$. Thus, every binary relation is defined by a subset $\Phi$ of the direct product $A \times B$ with the following property:

$$a \varphi b \iff (a, b) \in \Phi.$$  

Thus, the discussion above gives the possibility to abstract the notion of the binary relation in the form of the following formal definition.

**Definition 12.1.** A binary relation on the elements of sets $A, B$ is a subset $\Phi$ of the direct product $A \times B$.

We are interested in binary relations on elements of the same set $A$, i.e. subsets $\Phi \subset A \times A$, corresponding to the case where $A = B$. The very important among them are the so-called relations of the equivalence.

**Definition 12.2.** A binary relation $\Phi \subset A \times A$ is called the relation of the equivalence if it is satisfied the following conditions:
1) \((a, a) \in \Phi\) for all \(a \in A\) (reflexivity);

2) \((a, b) \in \Phi \Rightarrow (b, a) \in \Phi\) (symmetry);

3) \((a, b) \in \Phi, (b, c) \in \Phi \Rightarrow (a, c) \in \Phi\) (transitivity).

In the symbolics \(a \varphi b\), these properties are written as follows:
1) \((a \varphi a)\) for all \(a \in A\);

2) \(a \varphi b \Rightarrow b \varphi a\);

3) \(a \varphi b, b \varphi c \Rightarrow a \varphi c\).

For example, the reflexivity property means that every element of \(A\) relates to itself with respect to \(\varphi\).

For the relation of the equivalence, the symbol \(\sim\) (tilde) instead of \(\varphi\) is often used: \(a \sim b\).

Obviously, the relation of the equality on any set is the relation of the equivalence. The relation of inequality \(<\) is not reflexive and not symmetric, that is why it is not the relation of the equivalence. Consider a less trivial example on the set of real numbers \(\mathbb{R}\):

\[a \sim b \iff a - b \in \mathbb{Q}\]

(recall that \(\mathbb{Q}\) is the set of all the rational numbers).

For this binary relation the reflexivity \(a \sim a\) holds true because \(a - a = 0 \in \mathbb{Q}\). Moreover, if \(a \sim b\), i.e. \(a - b \in \mathbb{Q}\) then \(b - a = -(a - b) \in \mathbb{Q}\) and hence \(b \sim a\); this means that symmetry holds too. Let us prove the transitivity. Let \(a \sim b, b \sim c\), i.e. the numbers \(a - b\) and \(b - c\) are rational. Then the number \(a - c = (a - b) + (b - c)\) is also rational as the sum of two rational number, which means the transitivity is fulfilled.

We ask the reader to prove that the reflexivity, symmetry and transitivity properties in the definition of the relation of the equivalence are independent. With this aim, one needs to find three binary relations where one of the properties 1)-3) is not fulfilled but another two hold true.
The relations of the equivalence, defined on a set $A$, are very closely connected with partitions of the set $A$ on the non-intersecting subsets (classes). Here the *partition* is such a system of non-empty subsets of $A$ (the classes of the partition) that every element of $A$ belongs to one and only one of these subsets.

**Theorem 12.1.** Every partition of a set $A$ defines a relation of equivalence on $A$. Conversely, every relation of the equivalence on $A$ defines a partition of $A$.

**Proof.** Let a partition of a set $A$ with the use of a system of non-empty pairwise non-intersecting sets $\{A_i\}$ be given. We define a binary relation $\varphi$ on $A$ setting:

$$ a \varphi b \iff \text{both } a \text{ and } b \text{ belong to the same class } A_i. $$

The reflexivity and the symmetry of this relation are obvious; let us prove that it is transitive. Assume that $a \varphi b, b \varphi c$. This means that both $a$ and $b$ belong to the same class (let it be the class $A_i$) and both $b$ and $c$ belong to the same class (let it be the class $A_j$). By the definition of the partition, either the two arbitrary classes are equal or they do not intersect. In this case $A_i$ and $A_j$ has the common element $b$ and hence they coincide. Therefore both $a$ and $c$ belong to the same class, i.e. $a \varphi c$.

Conversely, let a relation of the equivalence $\sim$ is defined on $A$. For each $a \in A$ we define $K_a$ in $A$ as the set of all the elements $x \in A$, relating to $a$ with respect of $\sim$. Thus,

$$ K_a = \{ x \in A : a \sim x \}. $$

We will call $K_a$ the *class* of the element $a$. The reflexivity of the relation $\sim$ implies that $a \in K_a$ and hence the system of classes $\{K_a\}_{a \in A}$ covers the set $A$.

Let us prove that for any two elements $a, b \in A$ the classes $K_a$ and $K_b$ do not intersect or coincide. Suppose that the intersection $K_a \cap K_b$ is not empty and let $c$ be an element of the intersection. By the definition of the class, this means that $a \sim c, b \sim c$. Using the symmetry of the relation $\sim$ we have $c \sim b$;
besides that the transitivity implies $a \sim b$. Let us show that $K_a \subset K_b$. We pick an element $d$ in $K_a$. By the definition of the class $K_a$, we have $a \sim d$. We have already proved $a \sim b$ and hence $b \sim a \sim d$. Therefore $b \sim d$ (first, we have used the symmetry and then the transitivity). This means $d \in K_b$ and thus, the inclusion $K_a \subset K_b$ is established. Similarly, the inverse inclusion can be proved, and hence the identity $K_a = K_b$ is proved. Finally, we conclude that the family of classes $\{K_a\}$ defines a partition of the set $A$.

At the end we note that, together with the relation of the equivalence, the very important type of binary relations consists of relations of order, having the following properties: reflexivity, transitivity and anti-symmetry ($a \neq b, b \neq c \Rightarrow a \neq c$). Such relations will be considered in chapter V.
Chapter III.

Cardinalities of sets
Lecture 13. The notion of equinumerousity

If $A$ and $B$ are two finite sets then in order to decide whether the quantities of their elements are equal we can do as follows: to count elements of each set and to compare the resulting numbers.

However we can obtain the answer counting no elements in the sets. For example, in order to see whether the numbers of tables and students in the room are equal, it is sufficient to place a student at each table. Indeed, if no table will be free and every student will seat then the numbers of tables and students coincide. This method for comparison of numbers of set’s elements is based on the notion of the one-to-one mapping. The advantage of using this method is the following: it is fit to compare both finite and infinite sets. For instance, the correspondence

\[
\begin{array}{cccccccc}
1 & 2 & 3 & \ldots & n & \ldots \\
\downarrow & \downarrow & \downarrow & \ldots & \downarrow & \ldots \\
2 & 4 & 5 & \ldots & 2n & \ldots
\end{array}
\]

shows that the numbers of the natural numbers and the even numbers coincide.

Let us formulate this precisely.

**Definition 13.1.** The sets $A$ and $B$ are *equinumerous* if there is a one-to-one correspondence $A \leftrightarrow B$ between the elements of the sets $A$ and $B$.

Taking into the consideration the notions of lecture 11, this definition can be reformulated in this way: The sets $A$ and $B$ are *equipotential* if there is a bijection $f: A \to B$. The equipotential sets $A$ and $B$ are also called *equivalent* or it is said that they have the same *Cardinality* and one writes

$A \sim B$.

It is easy to see that two finite sets are equipotential if and only if they consist of the same quantity of elements.

Let us give examples of equipotential sets.
Example 13.1. The sets of the natural numbers and the integers are equipotential:

\[ \mathbb{N} \sim \mathbb{Z}. \]

Indeed, the bijection \( \mathbb{N} \leftrightarrow \mathbb{Z} \) is given by the following correspondence

\[
\begin{align*}
\mathbb{N} &: 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad \ldots \quad 2n \quad 2n+1 \quad \ldots \\
&\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \ldots \quad \downarrow \quad \downarrow \quad \ldots \\
\mathbb{Z} &: 0 \quad 1 \quad -1 \quad 2 \quad -2 \quad \ldots \quad n \quad -n \quad \ldots
\end{align*}
\]

Example 13.2. The hypotenuse of the right-angled triangle is equipotential to its legs (see picture 12).

Example 13.3. Any two segments \([a, b]; \quad [c, d]\) of real line are equipotential. The bijective map is given on the picture 13: it maps \( x \in [a, b] \) into \( y \in [c, d] \) via the rule \( y = f(x) \), where \( f \) is the linear function with the line containing points with the coordinates \((a, c)\) and \((b, d)\) as the graph.

Example 13.4. Arguing as in example 13.3, we see that any two intervals are equipotential:

\((a, b) \sim (c, d)\).
Example 13.5. The interval \((-\frac{\pi}{2}, \frac{\pi}{2})\) is equipotential to the real line \((-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}\). The bijective map is realized by the function \(y = \tan x\). Using example 13.4 we obtain that any interval is equipotential to \(\mathbb{R}\).

Example 13.6. The segment \([0,1]\) is equipotential to its \((0,1)\):

\([0,1] \sim (0,1)\).

In order to prove this we pick in \([0,1]\) the sequence

\[\{x_n\} = \{0, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}\].

Now consider the correspondence \(f : [0,1] \to (0,1]\)

<table>
<thead>
<tr>
<th>0</th>
<th>1/2</th>
<th>1/3</th>
<th>1/4</th>
<th>\ldots</th>
</tr>
</thead>
<tbody>
<tr>
<td>↓</td>
<td>↓</td>
<td>↓</td>
<td>↓</td>
<td>\ldots</td>
</tr>
<tr>
<td>\frac{1}{2}</td>
<td>\frac{1}{3}</td>
<td>\frac{1}{4}</td>
<td>\frac{1}{5}</td>
<td>\ldots</td>
</tr>
</tbody>
</table>

but all the other point of \([0,1]\) it keeps unchanged. The corresponding map can be written as follows:

\[ f(x) = \begin{cases} 
  x_{n+1}, & \text{if } x = x_n; \\
  x, & \text{if } x \notin \{x_n\}.
\end{cases} \]

It is easy to check that \(f\) is bijective. A visual idea of the map \(f\) is presented on picture 14.

Let us formulate the following simple statement.

**Theorem 13.1.** The relation of the equicardinality of sets has the following properties:

a) always we have \(A \sim A\);

b) if \(A \sim B\) then \(B \sim A\);

c) if \(A \sim B, B \sim C\) then \(A \sim C\).
This theorem shows that the binary relation of the equicardinality of sets is the relation of the equivalence (see s.12). Indeed, the symmetry property b) follows because if there is a bijective map \( f : A \rightarrow B \), then there is a bijective map \( g : B \rightarrow A \) (it is sufficient to take \( f^{-1} \) as \( g \)). In order to prove the transitivity property c), one needs to use the notion of the composition of maps; the reflexivity property a) is obvious.

**Definition 13.2.** The sets \( A \) is called *infinite* if it has an equipotential subset which does not coincide with \( A \). If there is no such set then \( A \) is called *finite*.

Example 13.1 implies that the set of all integers is infinite. Of course, a segment, an interval with non-zero length are infinite too. Obviously, the set \( \{1\} \) consisting of the unit only is finite and the set \( \{1, 2\} \) is finite too.

Mathematics has the branch, called *Enumerative Combinatorics* where algorithms and formulae for calculation of the number of elements in finite sets are elaborated. Chapter IV. is devoted to this branch. Here we consider powers (massiveness) of infinite sets only. The "smallest" sets among the infinite ones are the countable sets which we will study below.
Lecture 14. Countable sets

Definition 14.1. Every set $A$, equipotential to the set of all the natural numbers $\mathbb{N}$, is called countable.

Examples of lecture 13 show that the set of all even numbers $2 \cdot \mathbb{N}$ and the set of all the integers $\mathbb{Z}$ are countable. Another examples of countable sets are the following:

$$A = \{1, 4, 9, \ldots, n^2, \ldots\},$$
$$B = \{1, 1/2, 1/3, \ldots, 1/n, \ldots\}.$$  

Here the first set is the result of the correspondence $n \leftrightarrow n^2$. Similarly, the set $B$ is obtained with the use of the correspondence $n \leftrightarrow 1/n$.

Obviously, a set $A$ is countable if and only if its elements can be enumerated with the use of the natural numbers, i.e. the set can be presented as a sequence

$$A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\} \quad (14.1)$$

The following theorem demonstrates that the countable sets are the smallest one, in a sense, among the infinite sets.

Theorem 14.1. Every infinite set contains a countable subset.

Proof. Let us pick an arbitrary element $a_1$ from $M$. As $M$ is infinite, the set can not consist of one element $a_1$ only, that is why one can pick an element $a_2$ in the set $M \setminus a_1$. The same argument yields that the set $M \setminus \{a_1, a_2\}$ is not empty and hence one can pick an element $a_3$ in it. Since the set $M$ is infinite we can continue this process without end. As a result, we will obtain a sequence $a_1, a_2, \ldots, a_n, \ldots$, which is a countable subset of $M$.

Later we will prove several properties of countable sets; using them one can construct new countable sets. Now we establish that the very important set of all the rational numbers is countable.

Theorem 14.2. The set of all the rational numbers $\mathbb{Q}$ is countable.
Proof. Recall that every rational number $r$ can be presented as a fraction $p/q$, where $p$ is an integer (it can be positive or negative) and $q$ is a natural one. Hence we can correspond to every rational number $r$ the pair $(p, q)$; the set of all such pairs can be geometrically expressed as a set of knots of the lattice on the plane $pOq$.

Consider all the knots (i.e. the set of all the points at the plane with integer coordinates $p$ and $q$). As the knots are rarely placed on the plane, one can try to find a broken line going through all the knots and to enumerate them in this way. For instance, this can be done with the use of the spiral type line, drawn on picture 15. This line goes from the origin $(0, 0)$ to the point $(1, 0)$ with the number 1, then it goes to the point $(1, 1)$ with the number 2 and so on (for example, the point $(1, 2)$ has the number 13). Thus, we enumerate all the pairs $(p, q)$ with the integer coordinates. However we need to enumerate the pairs with $q \geq 1$ only; moreover some different pairs represent the same rational numbers (for instance, the pairs $(2, 3)$ and $(4, 6)$ represent number $2/3$). In order to the relation between the pairs $(p, q)$ and numbers $p/q$ be one-
to-one, it is sufficient to consider only the pairs \((p, q)\) with \(q \geq 1\) and \(p, q\) being relatively prime; in this case the fraction \(p/q\) is irreducible. Now we delete from the enumeration all the pairs which does not satisfy these conditions and then we renumerate the remaining pairs:

\[(1, 1), (0, 1), (-1, 1), (2, 1), (1, 2), (-1, 2), (-2, 1), \ldots.\]

The corresponding enumeration of the rational numbers has the following form:

\[1, 0, -1, 2, 1/2, -1/2, -2, \ldots\]

Since, moving along the spiral type line, we do not miss any point with the integer coordinates, then every rational number will get a unique number. It is also clear that, for every natural number \(n\), there exists a rational number, which corresponds to \(n\) in the enumeration above. This exactly means that \(\mathbb{Q}\) is countable.

Let us prove some properties of countable sets.

**Theorem 14.3.** *Every subset of a countable set is either finite or countable.*

**Proof.** Let \(A\) be a countable set, presented as the following sequence of its elements

\[A = \{a_1, a_2, \ldots, a_n, \ldots\},\]

and let \(B \subset A\) be its subset. Enumerating the set \(A\), we will count also elements of \(B\). Let these be elements \(a_{n_1}, a_{n_2}, \ldots\). If among the numbers \(n_1, n_2, \ldots\) there exists a largest one then \(B\) is a finite set, else \(B\) is countable because its elements \(a_{n_1}, a_{n_2}, \ldots\) are enumerated by the numbers \(1, 2, \ldots\).

To formulate the next property, we note that adding a finite set \(B\) to a countable set \(A\) we obtain a countable set. Indeed, if \(A\) is presented by the sequence (14.1) then the union \(A \cup B\) can be presented as the sequence

\[b_1, b_2, \ldots, b_k, a_1, a_2, \ldots, a_n, \ldots,\]

where \(a_1\) has number \(k + 1\), \(a_2\) has the number \(k + 2\) and so on.
Theorem 14.4. The union of any finite or countable set of countable sets is again a countable set.

Proof. First we consider the case where a finite number of countable sets $A_1, \ldots, A_k$ is given. Assume that any two of these sets have no intersection. We place their elements as follows:

\[
\begin{array}{cccccc}
  a_{11} & a_{12} & \cdots & a_{1n} & \cdots \\
  a_{21} & a_{22} & \cdots & a_{2n} & \cdots \\
  \vdots & \vdots & \ddots & \vdots & \ddots \\
  a_{k1} & a_{k2} & \cdots & a_{kn} & \cdots,
\end{array}
\]

where the elements of $A_1$ are placed in the first row, the elements of $A_2$ are placed in the second row and so on. One can enumerate the elements of the union "by columns": at the beginning we count $k$ elements of the first column, then we count $k$ elements of the second column (in this enumeration the element $a_{12}$ has number $k + 1$ and the element $a_{k2}$ has number $2k$). Besides, Theorem 14.3 implies that the "no intersection" assumption does not influence on the countability of the union.

Now let us handle the case where a countable set of countable sets $A_1, \ldots, A_k, \ldots$ is given. As before, we assume that every two of these sets have no intersection. We place the elements of the union as follows:
We already can not enumerate them "by columns" because we need all the natural numbers to count the first column. However one can do the enumeration "by diagonals": the first element being \(a_{11}\), the second one being \(a_{21}\), the third one being \(a_{12}\) and so on moving at the order indicated by the arrows in (14.2).

Using the idea of the proof of this theorem, a reader can easily prove the following statement.

**Theorem 14.5.** The union of countable set of pairwise non-intersecting finite sets is a countable set.

Now let us formulate a possibly more surprising fact.

**Theorem 14.6.** If \(M\) is an infinite set and \(A\) is either countable or finite one then \(M \cup A\) and \(M\) are equipotential; or, the same, the addition a finite or countable set to an infinite one does not increase the Cardinality of the infinite set.

This theorem emphasizes once more that the power of countable sets is "small": the infinite sets do not "feel" the addition of countable sets to them.

In order to prove theorem 14.6, we choose, according to theorem 14.1, a countable subset \(A'\) in \(M\); we denote by \(B\) the complement \(M - A'\). Then

\[
M = B \cup A', \quad M \cup A = B \cup (A' \cup A).
\]
Lecture 14. Countable sets

Theorem 14.4 and the remark above this theorem imply that both the sets $A'$ and $A' \cup A$ are countable, i.e. these sets are equipotential:

$$A' \sim A' \cup A.$$ 

Let $\varphi : A' \rightarrow A' \cup A$ be the bijection. Consider the map $f : M \rightarrow M \cup A$, defined by $a_0, a_1, \ldots, a_{n-1}, a_n$,

$$f(x) = \begin{cases} 
  x, & \text{if } x \in B, \\
  \varphi(x), & \text{if } x \in A'.
\end{cases}$$

Let us show that $f$ is a bijection. First, we establish that $f$ is injective. Let $x_1, x_2$ be different points in $M$. If both $x_1$ and $x_2$ belong to $B$ then $f(x_1) = x_1, f(x_2) = x_2$ and hence $f(x_1) \neq f(x_2)$. If both $x_1$ and $x_2$ belong to $A'$ then $f(x_1) = \varphi(x_1), f(x_2) = \varphi(x_2)$ then again $f(x_1) \neq f(x_2)$ because $\varphi$ is bijective. If $x_1 \in B, x_2 \in A'$, then $f(x_1) = x_1 \in B, f(x_2) = \varphi(x_2) \notin B$ and therefore $f(x_1) \neq f(x_2)$ and the injectivity of $f$ is proved. Let us prove the surjectivity. Let $y$ be an element of $M \cup A = B \cup (A' \cup A)$. If $y \in B$ then $y$ is the image of itself under the map $f$. If $y \in A' \cup A$, then for the element $x = \varphi^{-1}(y) \in A' \subset M$ we have $f(x) = y$. Theorem is proved.

Now we are ready to prove the countability of one more important numerical set, the set of algebraic numbers. The notion of the algebraic number plays a great role in Algebra and Theory of Numbers; besides, algebraic numbers played significant historical role in the Theory of Set’s Cardinalities.

**Definition 14.2.** The complex number (in particular, a real one) $x_0$ is called algebraic if it satisfies an equation of the type

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$  \hspace{1cm} (14.3)

where $a_0, a_1, \ldots, a_n$ are the integers being not all zeros and $n$ is natural. Any non-algebraic complex number is called transcendental.

Note that any rational number $r = p/q$ is algebraic because it satisfies the equation $p - qx = 0$ with the integer coefficients $a_0 = p, a_1 = -q$ (of degree $n = 1$).
Of course, the set of all the algebraic numbers does not coincide with the set of rational ones. For instance, it is well-known that $\sqrt{2}$ is not rational but, as it easy to see, it satisfies the equation $2 - x^2 = 0$ with the integer coefficients and hence it is algebraic. Also the imaginary unit $i = \sqrt{-1}$ is algebraic as the root of the equation $1 + x^2 = 0$.

The existence of the non-algebraic, i.e. transcendental, numbers was established by J. Liouville in 1844. The set of the transcendental numbers contains the number $e$ (it was proved by C. Hermite in 1873) and the number $\pi$ (it was proved by F. Lindemann in 1882).

The quantity of algebraic numbers is described in the following theorem.

**Theorem 14.7.** The set of algebraic numbers is countable.

Thus, despite the set of algebraic numbers contains the set of all the rational numbers, these sets are equipotential. Below we will see that the set of all real numbers (and hence the set of complex ones) is not countable. This fact and theorem 14.7 emphasize once more that transcendental numbers exist. Theorem 14.7 and the non-countability of $\mathbb{R}$ were proved by G. Cantor; he developed the Theory of Set’s cardinalities and created the principles of the modern Set’s Theory.

**Proof of theorem 14.7.** Let us prove that the set of all the equations of the type (14.3) is countable. Since every such an equation has a finite number of roots (because of the main theorem of Algebra, the number of roots, with accounted multiplicities, equals to the degree $n$ of the equation), theorem 14.5 implies the statement of theorem 14.7.

Thus, let us establish the countability of the set of all the equations of the type (14.3). The set of all the equations can be presented as the union $\bigcup_{n=1}^{\infty} A_n$ of sets $A_n$, consisting of the equations of degree $n$. According to theorem 14.4, this union is countable if each set $A_n$ is countable. Thus, our problem is to prove that, for any fixed $n$, the set of equations of the type (14.3) (with the integer coefficients) is countable. With this aim, we note that every such an equation is uniquely defined by its coefficients $a_0, a_1, ..., a_n$. Any such a collection defines an element of the Cartesian product $\mathbb{Z}^{n+1}$. Using the Mathematical Induction
Principle, let us prove the countability of \( \mathbb{Z}^{n+1} \). We know that \( \mathbb{Z} \) is countable, that is why the statement is true for \( n = 0 \). Assume that it is true for \( k = n \), i.e., that \( \mathbb{Z}^n \) is countable. It is not difficult to understand that the set \( \mathbb{Z}^{n+1} \), consisting of all the rows \( a_0, a_1, ..., a_{n-1}, a_n \) of the length \( n+1 \), can be presented as the union:

\[
\mathbb{Z}^{n+1} = \bigcup_{l=-\infty}^{\infty} B_l = \bigcup_{l \in \mathbb{Z}} B_l,
\]

where each set \( B_l \) consists of rows of the length \( n+1 \), having on the last place the same fixed number \( l \) while all the previous numbers are independently chosen in the set of the integers; this fact can be expressed as follows:

\[
B_l = \{(a_0, a_1, ..., a_{n-1}, l) : (a_0, a_1, ..., a_{n-1}) \in \mathbb{Z}^n\}.
\]

Obviously, any element of \( B_l \) is uniquely defined by the first \( n \) coordinates \( a_0, a_1, ..., a_{n-1} \), i.e. by an element of \( \mathbb{Z}^n \). This means that \( B_l \) and \( \mathbb{Z}^n \) are equipotential. By the induction assumption, the set \( \mathbb{Z}^n \) is countable and hence \( \mathbb{Z}^{n+1} \) is countable as the union of countable set of countable sets (theorem 14.4). This proves theorem 14.7.
Lecture 15. Continuum Cardinality

All the countable sets belong to the same class of equipotential sets; besides, the model set in this class is the set of all the natural numbers \( \mathbb{N} \). Now we present a non-countable set, which we will use as the model set in its class of the equipotential sets.

**Theorem 15.1.** The segment \([a, b]\) is not countable.

**Proof.** Recall that the set of all the real numbers \( \mathbb{R} \) consists of all the decimals of the type

\[
m, a_1a_2 \ldots a_n \ldots = m + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} + \ldots, \tag{15.1}
\]

where \( m \in \mathbb{Z} \) is an integer and \( a_1, a_2, \ldots, a_n \) are numbers (figures) from the the range 0, 1, \ldots, 9. Any such a fraction we can read as follows: "\( m \) plus \( a_1 \) over ten plus \( a_2 \) over hundred and so on plus \( a_n \) over \( 10^n \) and so on". The segment \([0, 1]\) can be characterized as a subset of \( \mathbb{R} \) consisting of fractions of the type (15.1) with the integral part \( m \) being zero:

\[
[0, 1] = \{0, a_1a_2 \ldots a_n \ldots\}.
\]

Indeed, for numbers from the half-interval \([0, 1)\) it is obvious because their integral parts are equal to zero, but the number 1 can be presented as the infinite decimals 0, (9) with nine at the period:

\[
1 = \frac{9}{10} + \frac{9}{10^2} + \ldots.
\]

This identity follows from the formula for the sum of the infinite progression with the exponent \( 1/10 \):

\[
\frac{9}{10} + \frac{9}{10^2} + \ldots = \frac{9}{10}(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots) = \frac{9}{10} \cdot \frac{1}{1 - \frac{1}{10}} = 1.
\]

Not all the numbers from the segment \([0, 1]\) have the unique decimal representation \( 0, a_1a_2 \ldots a_n \ldots \). For instance, the number 1/2 admits two representations:

\[
0, 5(0) = 0, 4(9);
\]
the first one uses the periodical zero and the second one uses the periodical nine. All the numbers with decimals without periodical zero and periodical nine have the unique representation. Hence, in order to obtain the unique representation for all the numbers, it is sufficient to use the only one (either with periodical zero or periodical nine) for numbers with non-unique representation. As the number $1$ can not be represented as a decimal $0, a_1a_2 \ldots a_k(0)$ with periodical zero and the number $0$ can not be represented as a decimal $0, a_1a_2 \ldots a_k(0)$ with periodical nine, we do not want to consider one of these numbers. It is not a problem because the segment $[0, 1]$ and half-interval $(0, 1]$ are equipotential (see example 13.6 from lecture 13).

Thus, we will prove that the half-interval $(0, 1]$, consisting of the decimals of the type

$$0, a_1a_2 \ldots a_n \ldots ,$$

is not countable; besides, we will not use the representation with periodical zero in order to have the uniqueness of the representation.

We prove the non-countability using the rule of contraries. Assume that the set $(0, 1]$ is countable, i.e. all its elements can be enumerated as a sequence of decimals:

$$x_1 = 0, a_{11}a_{12} \ldots a_{1n} \ldots$$

$$x_2 = 0, a_{21}a_{22} \ldots a_{2n} \ldots$$

........................................

$$x_k = 0, a_{k1}a_{k2} \ldots a_{kn} \ldots$$

........................................

Now consider the decimal

$$x = 0, b_1b_2 \ldots b_n \ldots ,$$

where the number $b_1$ does not coincide with $a_{11}$, the number $b_2$ does not equal to $a_{22}$ and so on; in general, for any $n$ the number $b_n$ differs from $a_{nn}$:

$$b_1 \neq a_{11}, b_2 \neq a_{22}, \ldots, b_n \neq a_{nn}, \ldots.$$
Besides we assume that each $b_n$ is not zero (in order to guarantee the absence of repeating zeros; do you remember our agreement?!).

It turned out that the fraction $x$ is not enumerated in the procedure above. Really, the number $x$ differs from the number $x_1$ at least by the first figure, it differs from the number $x_2$ at least by the second figure and so on. But it is completely clear that the fraction $x$ represents a number from the half-interval $(0, 1]$, so we come to a contradiction with the assumption that all the numbers of this half-interval are enumerated by the sequence $\{x_n\}$. The theorem is proved.

The segment $[0, 1]$ does not belong to the class of countable sets; let it be a model set of other class (see the definition below).

**Definition 15.1.** If a set $A$ is equipotential to the segment $[0, 1]$:

$$A \sim [0, 1],$$

then it is said that $A$ has the *continuum* cardinality, or, it is *continual*. Briefly, one can say that $A$ has cardinality $c$.

The term "continuum" (from Latin word continuum) expresses the continuity property or the connection property. The simplest geometric figure having this property is a segment, this fact explains the given definition.

Examples 13.3, 13.4, 13.6 from lecture 13 yield the following statement.

**Corollary 15.1.** *Every segment* $[a, b]$, *interval* $(a, b)$, *half-intervals* $[a, b)$ and $(a, b]$ are continual.*

Then, using example 13.5 from lecture 13, we obtain the result below.

**Corollary 15.2.** The cardinality of the set $\mathbb{R}$ of all the real numbers is continuum.

Recall that the set $\mathbb{Q}$ of all the rational numbers is countable (see theorem 14.2 from lecture 14), that is why theorem 14.6 from lecture 14 means that the addition the set to any infinite set does not change the cardinality of the last one.
In particular, if we add \( \mathbb{Q} \) to the set of all the irrational numbers then we obtain the real line \( \mathbb{R} \). Hence, using corollary 15.2, we conclude that the following statement holds.

**Corollary 15.3.** The set of all the irrational numbers is continual.

Similarly, using theorems 14.6 and 14.7 from lecture 14, we obtain the following statement.

**Corollary 15.4.** The set of all the transcendental numbers has continuum cardinality.

Since any two segments are equipotential to each other and equipotential to the real line then the following statement is not surprising.

**Theorem 15.2.** The union of any finite or countable set of continual pairly non-intersecting sets is a continual set.

**Proof.** First, let a finite family of sets \( A_1, ..., A_n \) of continual cardinality be given; besides we assume that \( A_i \cap A_j = \emptyset \), if \( i \neq j \). Pick a half-interval \([0, 1)\) and divide it by points \( 0 < c_1 < c_2 < ... < c_{n-1} < 1 \) on \( n \) half-intervals

\[
[0, c_1), [c_1, c_2), ..., [c_{n-1}, 1).
\]

We know that each half-interval is continual, that is why we can indicate bijective maps between \( A_1 \) and \([0, c_1)\), \( A_2 \) and \([c_1, c_2)\), ..., \( A_n \) and \([c_{n-1}, 1)\). Having these maps, we automatically obtain a one-to-one relation between the unions

\[
A_1 \cup A_2 \cup ... \cup A_n
\]

and

\[
[0, c_1) \cup [c_1, c_2) \cup ... \cup [c_{n-1}, 1) = [0, 1).
\]

This proves the theorem for the case of finite number of sets.

If we have a countable set of sets \( A_1, A_2, ..., \) non-intersecting pairwise, then we can do the following. We divide the half-interval \([0, 1)\) with the use of
a monotonically increasing sequence $0 < c_1 < c_2 < \ldots$, convergent to the unit ($c_k \to 1$ for $k \to \infty$), on the countable set of half-intervals

$$[0, c_1), [c_1, c_2), \ldots, [c_{k-1}, c_k), \ldots.$$ 

Again, choosing one-to-one maps between $A_k$ and $[c_{k-1}, c_k)$ for all $k$, we construct a bijective map between the union of all the sets $A_k$ and the half-interval $[0, 1)$. The theorem is proved.

We have obtained first impression of countable and continual sets on the real line $\mathbb{R}$. Probably, the reader wants to know the situation for sets on the plane and in the space. In particular, it is interesting to know whether the number of points on the plane or in the space is greater than on the line. Strangely enough, the plane and the space has the same amount of points as the line. Before proving this, we show that a cube and a square have the same number of points as a segment.

**Theorem 15.3.** Square and cube are continual.

**Proof.** We argue for the square (the arguments for the cube are the similar). The square is defined as the direct product

$$K = [0, 1] \times [0, 1]$$

of two segments. It is easy to see that this square is the union of the direct product

$$K' = (0, 1] \times (0, 1]$$

of two half-intervals with two sides of the square $K$ (on the picture 16 these are sides $a$ and $b$, placed on the coordinate axis). Theorem 15.2 implies that the union of sides $a$ and $b$ is continual, hence, by the same theorem, the continual cardinality of the square

$$K = K' \cup (a \cup b)$$
follows from the continual cardinality of $K'$, i.e. from the equivalence

$$(0, 1] \times (0, 1] \sim (0, 1].$$

Elements of $K'$ are the ordered pairs $(x, y)$, where the numbers $x, y$ are taken from the half-interval $(0, 1]$ and are presented as decimals

$$x = 0, x_1 x_2 \ldots x_n \ldots,$$

$$y = 0, y_1 y_2 \ldots y_n \ldots.$$

Our aim is to find a one-to-one correspondence between pairs and fractions. This can be done, for instance, as follows:

$$(x, y) \rightarrow z = 0, x_1 y_1 x_2 y_2 \ldots x_n y_n \ldots,$$

i.e. one can place the figures of the fractions $x$ and $y$ in the alternative order. However, under this map, the fraction $0, 11010101\ldots$ is the image of the pair $x = 0, 1(0), y = 0, (1)$, but $x$ has the periodic zero (we don’t consider such representation of decimals!).

In order to avoid this difficulty, we introduce the notion of "block" representation of decimals. A block of the decimal

$$a = 0, a_1 a_2 \ldots a_n \ldots$$

is a non-zero figure $a_n$ together with all zeros after the comma placed in succession directly before $a_n$. For instance, the blocks of the fraction

$$a = 0, 03008690005 \ldots$$
are \( \alpha_1 = 03, \alpha_2 = 008, \alpha_3 = 6, \alpha_4 = 9, \alpha_5 = 0005 \). Since we excluded the fractions with periodical zero, any block consists of finite numbers of zeros and a non-zero figure.

Now, using the block representation, we define the correspondence:

\[
(0, \alpha_1 \alpha_2 \ldots \alpha_n \ldots; 0, \beta_1 \beta_2 \ldots \beta_n \ldots) \rightarrow 0, \alpha_1 \beta_1 \alpha_2 \beta_2 \ldots \alpha_n \beta_n \ldots.
\]

Clearly, for any fraction \( 0, \delta_1 \delta_2 \ldots \delta_n \ldots \) there is a unique pair

\[
(0, \delta_1 \delta_3 \ldots; 0, \delta_2 \delta_4 \ldots),
\]

corresponded to it, i.e. this map (correspondence) is bijective. This proves the theorem.

**Corollary 15.5.** *The plane \( \mathbb{R}^2 \) and the space \( \mathbb{R}^3 \) are continual.*

**Proof.** Indeed, the plane \( \mathbb{R}^2 \) can be presented as the union

\[
\mathbb{R}^2 = \bigcup_{m,n=\infty} K'_{mn}
\]

of squares of the type (see picture 17)

\[
K'_{mn} = \{ (x,y) : m-1 < x \leq m, n-1 < y \leq n \}.
\]

By Theorem 15.3, any such a square is continual. Therefore, by Theorem 15.2 the plane \( \mathbb{R}^2 \) is continual too as the union of countable set of continua.
Corollary 15.6. *Continuum of continua is continual.* In other words, the cardinality of the union of a continual family of continual sets is continuum, if any two of these sets have no intersection.

**Proof.** Let a family \( \{A_i\}_{i \in I} \) of pairwise non-intersecting sets, indexed by elements \( i \) of continual set \( I \), be given; besides, let any set \( A_i \) be continual. We can assume that \( I \) is the segment \([0, 1]\). According to Theorem 15.3, in order to prove that the union is continual,

\[
A = \bigcup_{i \in [0, 1]} A_i,
\]

it is sufficient to construct a bijective map from \( A \) to the square \( I^2 = [0, 1] \times [0, 1] \). With this aim, we note that the square itself can be presented as the union of continual family of continua: the family of vertical segments

\[
B_i = \{(i, y) : 0 \leq y \leq 1\}, \quad i \in [0, 1],
\]

defines a division of the square (see picture 18).

Since any set \( A_i \) is continual, there is a bijective map \( \varphi_i : A_i \leftrightarrow B_i \) and hence the bijection

\[
A = \bigcup_{i \in [0, 1]} A_i \leftrightarrow \bigcup_{i \in [0, 1]} B_i = I^2
\]

is defined automatically. Thus, the statement is proved. \( \Box \)
Lecture 16. The notion of cardinality, comparison of the cardinalities

We have studied in details two classes of infinite sets: the countable sets and the continual ones; as a rule, infinite sets in Analysis belong to one of these classes. In order to continue the study of "massiveness" properties of infinite sets, we will try to define precisely the notion of the cardinality of set.

If two finite sets are equipotential then one corresponds them a natural number expressing their common property, i.e. the number of their elements. If two infinite sets are equipotential then we also say that they have equal cardinality. Thus, we can say that the cardinality is the common property of any equipotential infinite sets. Let us express this more formally.

**Definition 16.1.** According to theorems of lectures 12 and 13, all the sets are divided on equivalence classes in such a way that two sets belong to one class if and only if they are equipotential. We associate a symbol to any such a class; we call this symbol the cardinality of any set within the given class.

Besides, if the symbol $\alpha$ corresponds to a given class then for any $A$ from the class one writes:

$$|A| = \alpha, \quad \text{or} \quad \bar{A} = \alpha, \quad \text{or} \quad m(A) = \alpha.$$

We will use the first notation: $|A| = \alpha$.

The cardinality symbols for finite sets are the natural numbers; for instance,

$$|\{1\}| = 1, \quad |\{1, 2\}| = 2, \quad |\{a_1, a_2, \ldots, a_{56}\}| = 56.$$

For the cardinality of continual sets the symbol $c$ is used:

$$|[0, 1]| = c,$$

and the symbol $\aleph_0$ (one reads "aleph zero") is used for the cardinality of countable sets:

$$|\mathbb{N}| = \aleph_0.$$

Let us consider the problem of comparison of cardinalities.
Definition 16.2. It is said that a set $A$ has greater cardinality than a set $B$ if

1) these sets are not equipotential: $A \sim B$;
2) the set $A$ has a part $A^*$, being equipotential to $B$:

\[ A \supset A^* \sim B. \]

If the cardinality of the set $A$ is greater than the cardinality the of $B$, then one writes

\[ |A| > |B| \quad \text{or} \quad |B| < |A|. \]

We know (see theorem 15.1 and corollary 15.2 in lecture 15) that the sets of real numbers is not equipotential to the natural series: $\mathbb{R} \sim \mathbb{N}$. As $\mathbb{N} \subset \mathbb{R}$, according to definition 16.2, we have $|\mathbb{N}| < |\mathbb{R}|$. Using the symbols above, one can write

\[ \aleph_0 < c. \]

Since the cardinality $\aleph_0$ of a countable set is the "smallest" one for infinite sets (lecture 14, theorem 14.1), the natural questions arise:

1) is there a Cardinality greater than $c$ (the power of continuum)?;
2) is there the biggest Cardinality?;
3) is there a power $\mu$, intermediate between $\aleph_0$ and $c$:

\[ \aleph_0 < \mu < c? \]

The positive answer for the first question is given in the following theorem.

Theorem 16.1. The set $F$ of all the real functions defined on the segment $[0, 1]$ has a cardinality greater than $c$.

Proof. We need to check that $|F| > c$; with this aim, according to definition 16.2, we show that:

a) $F$ is not equipotential to $[0, 1]$;

b) there is a subset $F^*$ in $F$ being equipotential to $[0, 1]$. 
The property b) is easily to be checked: for example, the family \( \{ f(x) = c \} \) of constant functions, \( c \) running through the segment \([0, 1]\), is the subset which is equipotential to \([0, 1]\); one also can take the family \( \{ f(x) = x + c \}_{c \in [0,1]} \).

Let us prove the property a). We argue by the rule of contraries: assume that there is a bijective map \( \varphi \) from the segment \([0, 1]\) to \( F \). Given \( t \in [0, 1] \), let the function \( f_t = f_t(x) \) corresponds to \( t \) under the map \( \varphi \). Recall that functions from \( F \) are defined on \([0, 1]\). Hence \( f_t(x) \) is a function defined for \( x \in [0, 1] \) for every fixed \( t \in [0, 1] \).

Consider the function \( g(x) = f_x(x) + 1 \); it belongs to \( F \) because it is defined for \( x \in [0, 1] \). Under the assumed bijective map \( \varphi : [0, 1] \leftrightarrow F \), this function should correspond to a number \( t_0 \in [0, 1] \), i.e. \( g(x) \) should be the function \( f_{t_0}(x) \). This means that for every \( x \in [0, 1] \) the equality

\[
f_x(x) + 1 = f_{t_0}(x)
\]

holds. But, for \( x = t_0 \), this is impossible and therefore we obtain a contradiction. The theorem is proved.

**Theorem 16.2.** Let \( M \) be a set and let \( \mathcal{M} \) be the set of all the subsets in \( M \). Then the cardinality of the set \( \mathcal{M} \) is greater than the cardinality of \( M \).

This theorem gives the negative answer to the second question. Indeed, for any set with any cardinality there is a set with a greater cardinality and so on, obtaining a scale of cardinalities, unbounded from above.

**Proof.** It is easy to see that \( \mathcal{M} \) has a subset \( \mathcal{M}^* \) which is equipotential to \( M \): one can take the set of all the subsets with one element only as \( \mathcal{M}^* \). Let us prove that \( \mathcal{M} \sim M \). Let there is a ono-to-one map between elements of the set \( M \) and the set \( \mathcal{M} \):

\[
m \leftrightarrow A_m;
\]

here \( A_m \) is the element in \( \mathcal{M} \) corresponded to the element \( m \in M \). Let us show that we can not exhaust all the set \( \mathcal{M} \) under this map. Consider the set \( A \subset M \) consisting of all the elements \( m \in M \) which do not belong to the set \( A_m \) corresponded to \( m \):

\[
A = \{ m \in M : m \notin A_m \}.
\]
It appears that for this subset $A$, being element of $M$, there is no element of $M$ corresponding to it. Assume that such an element exists; we denote it by $m_*$. Thus, we assumed that

$$m_* \leftrightarrow A,$$

i.e. that $A = A_{m_*}$. Let us clarify whether $m_*$ belongs to $A$ or not. If $m_* \in A$ then $m_* \in A_{m_*}$ (because $A = A_{m_*}$ by the assumption); but, according to the definition of $A$, we have $m_* \notin A$. Conversely, if $m_* \notin A$ then, according to the definition of $A$, we see that $m_* \in A_{m_*}$; as $A = A_{m_*}$ we obtain $m_* \in A$. Therefore $m_*$ can not belong both $A$ and its complement $M \setminus A$. This contradicts with the assumption that the set $A$ corresponds to an element in $M$. The theorem is proved.

In lecture 8 we have proved that if $M$ is a finite set with $m$ elements then the set $\mathcal{M}$ has $2^m$ elements. This is the reason for the following definition.

**Definition 16.3.** If a set $M$ (not necessarily finite) has a cardinality $m$ and the set of all its subsets $\mathcal{M}$ has a cardinality $m$ then it is said that $m = 2^m$.

**Theorem 16.3.** It is true that $2^{\aleph_0} = c$, i.e. the set of all the subsets of natural series is continual.

**Proof.** Let $\mathcal{M}$ be the set of all subsets of the natural series. In order to prove that $\mathcal{M} \sim [0, 1]$, we will present numbers of the segment $[0, 1]$ by binary fractions:

$$x = 0, a_1a_2\ldots a_n\ldots = \frac{a_1}{2} + \frac{a_2}{2^2} + \ldots + \frac{a_n}{2^n} + \ldots ,$$

(16.1)

where each of $a_n$ equals either to 0 or to 1. The binary fractions admit more simple geometric interpretation than the decimals. If a number $x \in [0, 1]$ is given then the figures $a_n$ are defined as follows. We define the figure $a_1$ to be equal to 0 (if $x$ belongs to the left half of the segment $[0, 1]$) or 1 (if $x$ belongs to the right one); then we choose the half of the segment containing $x$ and define the figure $a_2$ to be equal to 0 (if $x$ belongs to the left half of the chosen part of $[0, 1]$) or 1 (if $x$ belongs to the right one); and so on. If during this process $x$ never meets the middle of the corresponding segment then we obtain a uniquely
defined binary fraction (16.1) representing $x$. If on a step (say, on $n$-th step) $x$ meets the middle of the corresponding segment then one may ascribe $x$ either to its left or right part, or, the same, to set $a_n$ to be either 0 or 1. If we ascribe $x$ to the left part then on every further steps the number $x$ will be in the right half of the corresponding segments, and vice versa. This means that for such a number $x$ there are two representations as binary fractions:

$$x = 0, a_1 \ldots a_{n-1}1011 \ldots ,$$
$$x = 0, a_1 \ldots a_{n-1}100 \ldots .$$

One of these representations has the periodical 1 and another one has the periodical zero. For example,

$$\frac{5}{8} = 0, 10100 \ldots = 0, 10011 \ldots .$$

In order to achieve the uniqueness of the representation, let us consider no fraction with periodical zero; for this we need to exclude 0 from the segment $[0, 1]$ (because 0 admits the representation $0, 00 \ldots$ with zero period). We will prove that $\mathbb{M} \sim (0, 1]$. With this aim we present the set $\mathbb{M}$ of all the subsets of the natural series $\mathbb{N}$ as the union

$$\mathbb{M} = \mathbb{M}_0 \cup \mathbb{M}_1,$$

where $\mathbb{M}_0$ is the set of all the finite subsets of $\mathbb{N}$ and $\mathbb{M}_1$ is the set of all the infinite subsets of $\mathbb{N}$. Say,

$$\{1\} \in \mathbb{M}_0, \ \{5, 11\} \in \mathbb{M}_0, \ \{1, 4, 9, \ldots, n^2, \ldots\} \in \mathbb{M}_1.$$

Obviously, $\mathbb{M}_0$ is countable. In order to see this, we first enumerate all the sets with only one element, then all the sets with only two elements and so on; after that we easily get the countability of $\mathbb{M}_0$ with the use of theorem 14.4 from lecture 14. The possibility of the enumeration of sets with only one element, sets with only two elements and, in general, sets with only $n$-elements, follows from the countability of sets $\mathbb{N}^2, \mathbb{N}^3, \mathbb{N}^n$ (see the arguments of the proof of theorem 14.7 from lecture 14).
Since $\mathcal{M}_0$ is countable, theorem 14.6 implies $\mathcal{M} \sim \mathcal{M}_1$. Thus, in order to finish the proof, it is enough to prove that
\[ \mathcal{M}_1 \sim (0, 1). \]

With this aim, for every element of $\mathcal{M}$, being a sequence $\{k_1, k_2, \ldots\}$ of increasing natural numbers, we associate the number $x \in (0, 1]$ with the binary representation $0.a_1a_2\ldots$, where $a_n$ equals to 1 if $n$ belongs to the sequence $\{k_1, k_2, \ldots\}$ and equals to 0 if $n$ does not belong to it. As we have agreed above, every number $x \in (0, 1]$ can be (uniquely!) represented by a binary fraction with infinitely many units. Hence $x$ corresponds to a (obviously, unique) sequence from $\mathcal{M}_1$. The theorem is proved.

Consider now the question 3), formulated above, about the existence of intermediate cardinality between "countable power" $\aleph_0$ and "continual cardinality" $c$. This question was stated by G. Kantor in 1878; he conjectured that there is no such a cardinality. By other words, Kantor’s conjecture, named by continuum conjecture or continuum problem, means that every infinite subset of real line $\mathbb{R}$ is equipotential either to the natural series $\mathbb{N}$ or to $\mathbb{R}$. For a long period there were no progress in confirmation of this conjecture in frames of traditional approaches of Set’s Theory. In 1939, K. Gödel proved that the continuum conjecture could not be disproved. Namely, adding the statement of the conjecture to the axiomatic system of Set’s Theory, Gödel obtained a non-contradictory system of axioms. This means that it is possible to assume the absence of the intermediate cardinality between "countable power" $\aleph_0$ and "continual Cardinality" $c$. However, a paradoxical situation appears in 1963, when P. Cohen have proved that the conjecture could not be proved. According to Cohen’s result one can assume that the intermediate cardinality exists.

These two results mean that any mathematician may choose himself a Set’s Theory: the one with the intermediate cardinality or another one without it.

The following statement plays an essential role in the problem of comparison of sets.
Theorem 16.4 (Theorem by Kantor and Bernstein). If a set $A$ is equipotential to a part of a set $B$ and the set $B$ is equipotential to a part of the set $A$ then $A$ and $B$ are equipotential.

Proof. Under the hypothesis of the theorem, $A \sim B^* \subset B$ and $B \sim A^* \subset A$. Actually this means that there are two injective maps:

$$f : A \to B, \quad g : B \to A.$$ 

To any element $x \in A$ we relate a countable or finite sequence $\{x_n\}_{n=0,1,2,...}$ having elements with even numbers in $A$ and elements with odd numbers in $B$. Namely, we take $x$ as $x_0$. If $x$ does not belong to the image of $g$ then the related sequence is finite and consists of the element $x = x_0$ only. If $x_0$ belongs to the image of $g$ then we take its pre-image $g^{-1}(x_0)$ as $x_1$, i.e. $g(x_1) = x_0$ in this case. Further, the sequence $\{x_n\}_{n=0,1,2,...}$ can be constructed as follows. Let an element $x_n$ is already defined. For even $n$ we take an element $x_{n+1}$ from $B$ with $g(x_{n+1}) = x_n$ (of course, if such an element exists) and for odd $n$ we take an element $x_{n+1}$ from $A$ with $f(x_{n+1}) = x_n$ (if such an element exists). If on a step $n$ there are no elements with the properties described above then the sequence related to $x$ is constructed and consists of $n + 1$ elements $x_0$, $x_1$, $\ldots$, $x_n$. In this case, the number $n$ is called the order of the element $x$. Otherwise, the sequence is infinite and we ascribe to $x$ the infinite order.

Let us divide the set $A$ on three classes: $A_0$ (consisting of elements of an even order), $A_0$ (consisting of elements of an odd order), and $A_\infty$ (consisting of elements of the infinite order). Similarly, let us divide $B$ on classes $B_0$, $B_1$ and $B_\infty$. It is not difficult to see that $f$ bijectively maps $A_0$ to $B_1$ and $A_\infty$ to $B_\infty$ because $f$ is injective. Similarly, $g$ bijectively maps $B_0$ to $A_1$. Now let us consider the map $\varphi : A \to B$, coinciding with $f$ on $A_0 \cup A_\infty$ and with $g^{-1}$ on $A_1$. One can see on the picture 19 that $\varphi$ is a bijective map from $A$ to $B$.

The theorem is proved.

Let us again consider the problem of the comparison of sets. Let $A$ and $B$ be two arbitrary sets. Then the following cases are logically possible:

1) $A$ is equipotential to a part of $B$ and $B$ is equipotential to a part of $A$;
Lecture 16. The notion of cardinality, comparison of the cardinalities

Pic. 19.

2) $A$ is equipotential to a part of $B$ and there is no part of $B$ which is equipotential to $A$;

3) $B$ is equipotential to a part of $A$ and there is no part of $A$ which is equipotential to $B$;

4) Both $A$ and $B$ has no parts which are equipotential the corresponding sets.

In the first case the sets $A$ and $B$ are equipotential according to Kantor-Bernstein’s theorem, i.e. $|A| = |B|$. In the second case, $B$ is more powerful than $A$, i.e. $|B| > |A|$. Similarly, in the third case $|A| > |B|$. Finally, in the forth case we would consider that the cardinalities of $A$ and $B$ are incomparable. However this case is impossible (the proof will follow from corollary 25.1, see lecture 25). Thus, the following theorem holds true.

**Theorem 16.5.** For any two sets $A$ and $B$, one of the following properties holds:

1) $|A| = |B|$;
2) $|A| > |B|$;
3) $|A| < |B|$.

Thus, any two cardinalities are comparable.
Chapter IV.

Enumerative Combinatorics
Chapter IV. Enumerative Combinatorics

The main problem of the Enumerative Combinatorics is to count number of elements in a finite set. We have seen the problems of such kind in the lecture 8 where we had to found the number of elements of the set $\mathcal{M}$ of all the subsets of a finite set $M$ with $n$ elements (recall that this number equals to $2^n$).

Frequently, an enumerative problem on "the number of elements of a set" is formulated in terms of "the number of modes of arrangements" with given rules for some objects. For instance, one of the problem of this kind is the classical problem on married couples: how many variants are there for arrangements around a table of $n$ married couples (of course, on $2n$ places) in such a way that no husband sits near his wife. As another example, we may consider the enumerative problem "on hats": $n$ men give their $n$ hats to a cloakroom attendant; it is necessary to find how many versions are there for returning the hats in such a way that any man gets a hat but no man gets his own one. If $f(n)$ is the numbers of the versions then, obviously, $f(1) = 0$, $f(2) = 1$, $f(3) = 2$. A formula, expressing the number $f(n)$ for arbitrary value $n$, will be given in lecture 21 where we will also show that the problem "on hats" is equivalent to the problem on the number of bijective maps without fixed points on sets consisting of $n$ elements.

The arrangements rules for objects of some given sets, discussed above, define modes for building the constructions which are called "combinatoric configurations". The simplest examples of combinatoric configurations are combinations, permutations and arrangements; we begin this chapter with the discussion of them.
Lecture 17. Combinations and Newton’s binomial formula

Let $M$ be a set consisting of $n$ elements:

$$\{a, b, \ldots c\}.$$  

**Definition 17.1.** Any subset in $M$, consisting of $k$ elements is called a *combination of $n$ things $k$ at a time*.

For example, if $M = \{1, 2, 3, 4\}$ is the set of four elements (in this case elements of the set are numbers) then the list of its subsets

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$$

gives all the combinations of 4 things 2 at a time and the list

$$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}$$

exhausts all the combinations of 4 elements 3 at a time.

It is important to emphasize that two different combination of $n$ elements $k$ at a time differ by the composition of their elements: if two combinations do not coincide then one of them has at least an element which does not belong to another combination.

**Denotation:** the number of all the combinations of $n$ elements $k$ at a time is denoted by $C^k_n$ or by $\binom{n}{k}$.

In the example above we had: $C^2_4 = \binom{4}{2} = 6$, $C^3_4 = \binom{4}{3} = 4$.

Our problem is to obtain a formula for $C^k_n$, the number of all the combinations of $n$ elements $k$ at a time.

In order to get the formula, we note that, since we are not interested in properties of the set’s elements, we may take as the set a definite set. Let it will be the set

$$M = \{1, 2, \ldots, n\}$$

of the first $n$ numbers of the natural series.
The combinations of \( n \) elements 1 (one) at a time are all the subsets consisting of 1 element: \{1\}, \{2\}, ..., \{n\}. Clearly, the number of them equals to \( n \); hence the number of all the combinations of \( n \) elements 1 (one) at a time equals to

\[
C_n^1 = n. \tag{17.1}
\]

The combination of \( n \) elements \( n \) at a time is the one subset in \( M \) only; this is the set \( M \) itself. Therefore

\[
C_n^n = 1. \tag{17.2}
\]

Formulas (17.1) and (17.2) express \( C_n^k \) for \( k = 1 \) and \( k = n \).

The value of \( C_n^k \) for \( k = 0 \) expresses the number of subsets in \( M \) with 0 elements, but it is the empty set only. Hence

\[
C_n^0 = 1. \tag{17.3}
\]

In general the expression for \( C_n^k \) is given in the following theorem.

**Theorem 17.1.** The combination of \( n \) elements \( k \) at a time equals to

\[
C_n^k = \frac{n!}{k!(n-k)!}, \tag{17.4}
\]

or (for \( k \neq 0 \))

\[
C_n^k = \frac{n(n-1) \ldots (n-k+1)}{1 \cdot 2 \ldots k}, \tag{17.5}
\]

where the symbol \( n! \) is the product of all the natural numbers not greater than \( n \) (i.e. \( n! = 1 \cdot 2 \cdot \ldots \cdot n \)); besides 0! = 1.

**Proof.** For \( k = 0 \) and \( k = 1 \) formula (17.4) gives

\[
C_n^0 = \frac{n!}{0!n!} = 1, \quad C_n^1 = \frac{n!}{1!(n-1)!} = n,
\]

therefore formulas (17.3) and (17.1) show that the statement of the theorem holds for \( k = 0, 1 \).

Using the Principle of Mathematical Induction, we prove that formula (17.4) for all the values \( k = 0, 1, \ldots, n \). With this aim, we found the connection
between the numbers $C_{n}^{k-1}$ and $C_{n}^{k}$. Shortly we will call the combination of $n$ elements $k$ at a time by $k$-combination in $M$.

We note that, for any $(k-1)$-combination, one can construct $n-k+1$ copies of $k$-combinations, adding an element from the non-used ones. For instance, for $(k-1)$-combination \{1, 2, ..., $k-1$\}, one constructs the following $k$-combinations:

$$\{1, \ldots, k-1, k\}$$
$$\{1, \ldots, k-1, k+1\}$$
$$\ldots\ldots\ldots$$
$$\{1, \ldots, k-1, n\}.$$  

If in this construction every $k$-combination would be built from a $(k-1)$-combination only, then the first ones would be $(n-k+1)$ times greater than the second ones. But every $k$-combination is obtained from exactly $k$ copies of $(k-1)$-combinations: in order to list all the $(k-1)$-combinations, generating a given $k$-combination, it is sufficient to delete in turn an element from the last combination.

Thus, each of $C_{n}^{k-1}$ copies of $(k-1)$-combinations generates $n-k+1$ copies of $k$-combinations: totally we get $(n-k+1)C_{n}^{k-1}$ copies of $k$-combinations; besides each of $k$-combinations meets $k$ times. Therefore

$$C_{n}^{k} = \frac{n-k+1}{k}C_{n}^{k-1}. \quad (17.6)$$

Now assume that formula (17.4) holds if we replace $k$ by $k-1$ (the inductive assumption):

$$C_{n}^{k-1} = \frac{n!}{(k-1)!(n-k+1)!}.\quad (17.4)$$

Then, according (17.6),

$$C_{n}^{k} = \frac{n-k+1}{k}C_{n}^{k-1} = \frac{n-k+1}{k} \cdot \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!}{k!(n-k)!}.$$
Lecture 17. Combinations and Newton’s binomial formula

which proves formula (17.4), because of the Mathematical Induction Principle.

It is worth to note the following properties of the combination numbers $C^n_k$.

**Proposition 17.1.**

(a) $C^n_k = C^n_{n-k}$,

(b) $C^{k-1}_{n-1} + C^n_k = C^n_k$.

These properties can be easily obtained from formula (17.4). However it is not difficult to deduce them from the initial definition of the numbers $C^n_k$. For instance, in order to prove (a), it is sufficient to note that any set $M$ of $n$ elements has as many $k$–combinations as $(n – k)$–combinations. Indeed, to any $k$–combination (i.e. to any subset of $k$ elements) we associate its complement in $M$, which is a $(n – k)$–combination. Clearly, this correspondence is one-to-one.

In order to prove property (b), we pick in $M$ an element, say, the last one. All the combinations of $n$ elements $k$ at a time we divide on two groups: the combinations containing the element and the ones do not containing it. The first group consists of $C^{k-1}_{n-1}$ combinations and the second one consists of $C^n_k$ ones; this implies property (b).

**Theorem 17.2.** For any natural number $n$ the following formula holds true:

$$(x + y)^n = \sum_{k=0}^{n} C^n_k x^k y^{n-k}, \quad (17.7)$$

where the coefficients $C^n_k$ before the degrees of the variables $x$ and $y$ are the combination numbers, defined by formula (17.4).

Formula (17.7) is called *Newton’s binomial formula*. It expresses the $n$-th degree of a binomial $(x + y)$; that is why the numbers $C^n_k$ are also called *binomial coefficients*. 
Proof. Let us use the Mathematical Induction Principle. For $n = 1$, formula (17.7) has the form:

$$(x + y) = C_1^0 x^0 y^1 + C_1^1 x^1 y^0 = x + y;$$

it is obviously true.

Assume that formula

$$(x + y)^{n-1} = \sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-1-k},$$

is also true (this one is obtain replacing $n$ by $n - 1$ in (17.7)). Then

$$(x + y)^n = \left(\sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-1-k}\right) (x + y) =$$

$$= \sum_{k=0}^{n-1} C_{n-1}^k x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-k}.$$

In the first of the last two sums we do a "shift" in the summation, replacing $k$ by $k - 1$, and in the second one we separate the summand corresponding to $k = 0$. We obtain

$$(x + y)^n = \sum_{k=1}^{n} C_{n-1}^{k-1} x^k y^{n-k} + \sum_{k=1}^{n-1} C_{n-1}^k x^k y^{n-k} + C_{n-1}^0 x^0 y^n =$$

$$= \sum_{k=1}^{n} (C_{n-1}^{k-1} + C_{n-1}^n) x^k y^{n-k} + C_{n-1}^0 x^0 y^n.$$

Taking into the account property (b) for numbers of combinations and the fact that $C_{n-1}^0 = 1 = C_n^0$, we get (17.7).
Lecture 18. Permutations and arrangements

Definition 18.1. A permutation of \( n \) elements is a finite sequence of the length \( n \) which has no coinciding elements.

As examples of permutations one may take the following sequences: \{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\}.

Please, pay attention, that the permutations, listed above, has the same elements. However we consider them as different ones because in definition 18.1 we used the notion of sequence for which both the order and the collection of elements are important. Hence we can define a permutation also in the following way.

Definition 18.2. Any ordered finite set is called a permutation generated by its elements.

Any given set \( M \), containing more than one element, can be ordered by several methods; that is why one can generate several permutations from its elements. The number of such permutations is discussed in the following statement.

Theorem 18.1. The number of all the possible permutations, generated by \( n \) elements, equals to

\[ n! = 1 \cdot 2 \cdots n. \]

Proof. Let a set \( M \) consisting of \( n \) elements be given. Without loss of the generality, we may assume that \( M \) is the set of all the first \( n \) natural numbers: \( M_n = \{1, 2, \ldots, n\} \). We will prove the theorem by the induction with respect to \( n \). For \( n = 1 \) the set \( M_1 = \{1\} \) consists of one element and we can generate one permutation only. Assume that the theorem is true for sets of \( n - 1 \) elements, i.e. the set \( M_{n-1} = \{1, 2, \ldots, n - 1\} \) generates \((n - 1)!\) permutations. The permutations, generated by \( M_{n-1} \), are sequences \( \{i_1, \ldots, i_{n-1}\} \) of pairly non-coinciding natural numbers from 1 to \( n - 1 \). To any such a permutation one can relate exactly \( n \) copies of permutations of \( n \) elements from the set \( M_n \). Namely, these are the
permutations \( \{n, i_1, \ldots, i_{n-1}\}, \{i_1, n, i_2, \ldots, i_{n-1}\}, \ldots, \{i_1, \ldots, i_{n-1}, n\} \). Each of these permutations of \( n \) elements can be obtained by the insertion to the initial permutation (consisting of \( n - 1 \) elements) the number \( n \), at the beginning, to the first place, then, to the second one, and so on, and, finally, to the \( n \)-th place (the last one).

Thus, the number of all the permutations of \( n \) elements is exactly \( n \) times greater than the number of all the permutations of \( n - 1 \) elements. Therefore, using the inductive assumption, we conclude that it equals to \( n \cdot (n - 1)! = n! \).

Let us show that using the theorem one can calculate the number of all the bijective maps (one-to-one relations) \( f : A \to B \) for sets \( A \) and \( B \) with the same number of elements: \(|A| = |B| = n\) (recall that \(|M|\) denotes the power, i.e. the number of elements, of the set \( M \)). Let \( A = \{a_1, \ldots, a_n\}, B = \{b_1, \ldots, b_n\} \). If \( n = 1 \) then there is one bijective map only, mapping \( a_1 \) to \( b_1 \). If \( n = 2 \) then there are two bijective maps:

\[
\begin{align*}
a_1 &\to b_1 & a_1 &\to b_2 \\
a_2 &\to b_2 & a_2 &\to b_1
\end{align*}
\]

For \( n = 3 \) there are already 6 bijection; let us list them:

\[
\begin{align*}
a_1 &\to b_1 & a_1 &\to b_1 & a_1 &\to b_2 \\
a_2 &\to b_2 & a_2 &\to b_3 & a_2 &\to b_1 \\
a_3 &\to b_3 & a_3 &\to b_2 & a_3 &\to b_3
\end{align*}
\]

\[
\begin{align*}
a_1 &\to b_2 & a_1 &\to b_3 & a_1 &\to b_3 \\
a_2 &\to b_3 & a_2 &\to b_1 & a_2 &\to b_2 \\
a_3 &\to b_1 & a_3 &\to b_3 & a_3 &\to b_1
\end{align*}
\]

Let us prove that for any number \( n \) the number of the bijective maps equals to \( n! \).
Any bijective map \( f : A \rightarrow B \) is a rule according to which every element \( a_k \) of the set \( A \) corresponds to a definite element \( b_{i_k} \) of the set \( B \):

\[
\begin{align*}
a_1 &\rightarrow b_{i_1} \\
a_2 &\rightarrow b_{i_2} \\
\ddots & \\
a_n &\rightarrow b_{i_n},
\end{align*}
\]

besides, different elements of \( A \) correspond to different elements of \( B \). Obviously, such a rule is completely defined by the choice of the ordered sequence \( b_{i_1}, \ldots, b_{i_n} \) from the set \( B \), i.e. by the choice of the permutation of \( n \) elements. According to the theorem, the number of all the possible permutations, generated by \( n \) elements, equals to \( n! \), and we obtain the proclaimed above statement on the number of the bijective maps.

Let us pass to the notion of arrangement.

**Definition 18.3.** Any ordered part of \( k \) elements of a set of \( n \) elements is called an arrangement of \( n \) elements \( k \) at a time.

In order to define an arrangement of \( n \) elements \( k \) at a time, one needs to choose a combination of \( k \) elements from a set \( M \) of \( n \) elements and then to define on this combination a permutation (fixing the running order for elements of the combination).

**Example 18.1.** All the arrangements of 3 elements 2 at a time are written below: \( \{1,2\}, \{2,1\}, \{1,3\}, \{3,1\}, \{2,3\}, \{3,2\} \). Here the first two arrangements are the permutations of combination of elements \( \{1,2\} \), the second two arrangements are the permutations of combination of elements \( \{1,3\} \), and the third arrangements are the permutations of combination of elements \( \{2,3\} \).

The number of different arrangements of \( n \) elements \( k \) at a time is denoted by \( A_n^k \).
Theorem 18.2. The number of different arrangements of $n$ elements $k$ at a time is expressed by the following formula:

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

**Proof.** Obviously, the number $A_n^k$ of all the arrangements of $n$ elements $k$ at a time equals to the number of all the combinations of $n$ elements $k$ at a time multiplied over the number of all the permutations of $k$ elements. Hence, by theorem 17.1 from lecture 17 and theorem 18.1 of this lecture, we have:

$$A_n^k = C_n^k \cdot k! = \frac{n!}{k!(n-k)!} \cdot k! = \frac{n!}{(n-k)!},$$

which was to be proved.
Lecture 19. Permutations with repetitions

Definition 19.1. Let a finite set \( M = \{a, b, ..., c\} \) be given. A permutation of the set \( A \) with repetitions of type the \((\alpha, \beta, ..., \gamma)\) is an (ordered) sequence of elements of the set \( M \) where \( a \) meets \( \alpha \) times, \( b \) meets \( \beta \) times, and so on, \( c \) meets \( \gamma \) times. The number \( k = \alpha + \beta + ... + \gamma \) is called the degree of the permutation.

The usual permutations, considered in lecture 18, has the type \((1, 1, ..., 1)\), because each elements meets there one time only; respectively, the degree of the usual permutation equals to its length (the number of elements used in the permutation).

Example 19.1. Let \( M = \{a, b, c\} \) is a set of 3 elements. Let us list for this set all the permutations with repetitions of the type \((\alpha, \beta, \gamma) = (2, 1, 1)\):

\[
\begin{align*}
& bcaa \quad cbaa \quad baca \quad caba \\
& baac \quad caab \quad abca \quad acba \\
& abac \quad acab \quad aabc \quad aacb
\end{align*}
\]

Theorem 19.1. The number of all the different permutations with repetitions of the type \((\alpha, \beta, \ldots, \gamma)\) equals to

\[
\frac{(\alpha + \beta + ... + \gamma)!}{\alpha! \beta! ... \gamma!}.
\]

In the example above, 12 permutations were listed; this corresponds to the theorem because for \( \alpha = 2, \beta = 1, \gamma = 1 \) we have:

\[
\frac{(2 + 1 + 1)!}{2! 1! 1!} = \frac{4!}{2!} = 12.
\]

Proof. Let us denote by \( \Pi \) the set of all permutations (without the repetitions) of the length \( k = \alpha + \beta + ... + \gamma \) consisting of the numbers \( 1, 2, ..., k \), and let us denote by \( \hat{\Pi} \) the set of all the permutations with repetitions of the type \((\alpha, \beta, ..., \gamma)\). As, according to lecture 18, the set \( \Pi \) consists of \( k! \) permutations, in order to prove the theorem, it is sufficient to establish that
the number of elements in $\hat{\Pi}$ is exactly $\alpha!\beta!...\gamma!$ times smaller than in $\Pi$. With this aim, we consider the map $\Pi \to \hat{\Pi}$, under which to any element of $\hat{\Pi}$ goes exactly $\alpha!\beta!...\gamma!$ elements of $\Pi$.

Each permutation $\pi \in \Pi$ we write in the form

$$\pi : i_1, ..., i_\alpha, j_1, ..., j_\beta, ..., k_1, ..., k_\gamma$$

and we correspond to it a permutation $\hat{\pi}$ with the repetitions of the type $(\alpha, \beta, ..., \gamma)$ by the following rule: the element $a$ we put on the places with numbers $i_1, ..., i_\alpha$, the element $b$ we put on the places with numbers $j_1, ..., j_\beta$ and so on, the element $c$ we put on the places with numbers $k_1, ..., k_\gamma$. For instance, for $\alpha = 2, \beta = 1, \gamma = 1$ and the permutation $\pi: 4132$, in the corresponding to it permutation $\hat{\pi}$, the element $a$ is placed on places with the numbers 4 and 1, the element $b$ is placed on place with the number 3, and the element $c$ is placed on place with the number 2, i.e. $\hat{\pi}$ is the permutation with the repetitions $acba$. The correspondence $\pi \to \hat{\pi}$ is not one-to-one. Say, both $4132$ and $1432$, it maps to $acba$.

Let us explain how many permutations from $\Pi$ correspond to a permutation from $\hat{\Pi}$. Consider two arbitrary permutations from $\Pi$:

$$\pi : i_1, ..., i_\alpha, j_1, ..., j_\beta, ..., k_1, ..., k_\gamma,$$

$$\pi' : i'_1, ..., i'_\alpha, j'_1, ..., j'_\beta, ..., k'_1, ..., k'_\gamma.$$  

In the permutation $\hat{\Pi}$, corresponding to $\pi$, the element $a$ is placed on the places with the numbers $i_1, ..., i_\alpha$, and, in $\hat{\pi}'$, the element $a$ is on the places with the numbers $i'_1, ..., i'_\alpha$. Therefore, the element $a$ is on the same places in both $\hat{\pi}$ and $\hat{\pi}'$ if and only if the following identities hold:

$$\{i_1, ..., i_\alpha\} = \{i'_1, ..., i'_\alpha\}$$

$$\{j_1, ..., j_\beta\} = \{j'_1, ..., j'_\beta\}$$

....................

$$\{k_1, ..., k_\gamma\} = \{k'_1, ..., k'_\gamma\}.$$
Since the first group \( \{i_1, ..., i_\alpha\} \) generates \( \alpha! \) different permutations, the second group \( \{j_1, ..., j_\beta\} \) generates \( \beta! \) ones and so on, the last group \( \{k_1, ..., k_\gamma\} \) generates \( \gamma! \) different permutations, then, totally, \( \alpha! \beta! ... \gamma! \) permutations from \( \Pi \) correspond to a permutation from \( \hat{\Pi} \).

As an application of theorem 19.1, we will prove a formula for \((x_1 + ... + x_n)^k\).

**Theorem 19.2.** The following formula takes place:

\[
(x_1 + ... + x_n)^k = \sum_{\alpha_1+...+\alpha_n=k} \frac{k!}{\alpha_1! ... \alpha_n!} x_1^{\alpha_1} ... x_n^{\alpha_n}
\]  

(19.1)

In the case \( n = 2 \) formula (19.1) coincides with Newton’s binomial formula. Comparing with Newton’s binomial formula, (19.1) has in the left-hand side the polynomial \( x_1 + ... + x_n \) instead of binomial \( x_1 + x_2 \); that is why formula (19.1) is called the polynomial formula.

**Proof.** The left-hand side of (19.1) is the product of \( k \) equal factors

\[
(x_1 + ... + x_n) \cdot (x_1 + ... + x_n) \cdot ... \cdot (x_1 + ... + x_n).
\]  

(19.2)

In order to do the multiplication in (19.2) we need to make all the possible selections with respect to every term from every factor, to multiply all selection’s terms and to do summation with respect to all the selections. For instance, if we take \( x_{i_1} \) from the first factor, \( x_{i_2} \) from the second one and so on, \( x_{i_k} \) from the \( k \)-th factor, then this selection corresponds to the term

\[
x_{i_1} x_{i_2} ... x_{i_k},
\]  

(19.3)

where for each of the indices \( i_1, ..., i_k \) it is possible to relate arbitrary values \( 1, 2, ..., n \). Clearly, the number of the selections (and, hence, the numbers of the items in (19.3)) equals to \( n^k \). Among summands in (19.3)) there are similar ones. Namely, these are that containing \( x_1 \) as a factor \( \alpha_1 \) times, containing \( x_2 \) as a factor \( \alpha_2 \) times, and so on, containing \( x_n \) as a factor \( \alpha_n \) times, where \( \alpha_1 + ... + \alpha_n = k \). Thus, all the summands in (19.3)), similar to \( x_1^{\alpha_1} ... x_n^{\alpha_n} \) with \( \alpha_1 + ... + \alpha_n = k \), form the set of all the permutations with repetitions where \( x_1 \) is found \( \alpha_1 \) times, \( x_2 \) is found \( \alpha_2 \) times, and so on, \( x_n \) is found \( \alpha_n \) times.
According to theorem 19.1 the number of such permutations equals to \[\frac{k!}{\alpha_1! \ldots \alpha_n!}\]. That is why the item \(x_1^{\alpha_1} \ldots x_n^{\alpha_n}\) will be with such a factor after the summation.
Lecture 20. The inclusion-exclusion principle

The inclusion-exclusion principle is one of the version of the "sieve method"; this is a method for calculating the number of the elements (the power) of a set $M$. It is based on the following: starting with a larger set, one excludes (sifts) the unnecessary elements. For instance, if we need to find the power of a set $M$, being the union $A \cup B$ of two sets then, first, we take the number $|A| + |B|$ being the sum of powers of these sets. But if the sets $A$ and $B$ has common elements then this sum is greater than real value of $|M|$ because the elements of the intersection $A \cap B$ are counted twice. Hence, subtracting the power of the intersection from the sum $|A| + |B|$, we obtain the true power of the set $M$:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$  \hspace{1cm} (20.1)

Let us try to calculate the power $|A \cup B \cup C|$ of the union of three sets. Let us consider the number

$$|A| + |B| + |C|$$

as the starting approximation of the calculated power. In this sum the elements, belonging to one of the intersections

$$A \cap B, \quad B \cap C, \quad A \cap C,$$

are counted at least twice. For instance, the elements of $A \cap B$ are counted in both $|A|$ and $|B|$, and the elements of the triple intersection $A \cap B \cap C$ are counted three times.

Let us subtract (exclude) from the starting approximation the number of elements counted at least twice; then we obtain the following approximation:

$$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C|.$$  

Now it appears that the elements counted in the starting approximation three times (i.e. the elements of $A \cap B \cap C$) are not counted. Adding (including) the
power of this "triple" intersection, we obtain the true power formula:

\[ |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| \]  

\[ |A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|. \]  

Let us give a different proof of formula (20.2), based upon formula (20.1). With this aim, we present the union \( A \cup B \cup C \) as the union of two sets \( A \cup B \) and \( C \), then we apply formula (20.1) to them:

\[ |A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|. \]

As, by the distribution rule, \( (A \cup B) \cap C = (A \cap C) \cup (B \cap C) \), we conclude that

\[ |A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cap C) \cup (B \cap C)|. \]

Applying once more formula (20.1) (to the first and the third summands of the last expression) we get:

\[ |A \cup B \cup C| = |A| + |B| - |A \cap B| + |C| - |A \cap C| \]
\[ -|B \cap C| + |(A \cap C) \cap (B \cap C)|. \]

It is easy to see that the intersection \( (A \cap C) \cap (B \cap C) \) coincides with the intersection \( A \cap B \cap C \), and thus, we obtain formula (20.2).

The second proof of formula (20.2) can be called inductive, because the case of the triple union was reduced to the union of two sets. One can use Mathematical Induction Principle for proving the following statement on the power of the union of any numbers of (finite) sets.

**Theorem 20.1.** If \( A_1, ..., A_n \) are finite sets then

\[ |A_1 \cup ... \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - ... \]
\[ +(-1)^{n-1}|A_1 \cap ... \cap A_n|. \]  

\[ (20.4) \]
The combinatoric interpretation of formula (20.4) is the following. Assume that $n$ independent counters mark the elements of $A_i$ by "sticks"; the first counter marks the elements of $A_1$ only, the second one marks the elements of $A_2$ only and so on. Including in the consideration the sum of all the "sticks" we obtain, in general, a number which is equal or greater than the power of the union of all the sets. If we exclude from the sum the number of elements counted at least twice then we obtain a number which is equal or less than the power of the union of all the sets. Including to the sum the number of elements counted at least trice we again obtain a number which is equal or greater than the power of the union of all the sets. Continuing the inclusion-exclusion process we get on $n$-th step the true value of the power of the union.

The given combinatoric interpretation is the reason why formula (20.4) is called the inclusion-exclusion principle.

We will not prove theorem 20.1. We note only that it can be proved with the use of the Mathematical Induction Principle. In this way the passage from (20.4) for $n$ sets to the one for $n+1$ sets is similar to the deduction of formula (20.2) from formula (20.1).

In lecture 21 we will apply theorem 20.1 for solving "the hut problem", formulated at the beginning of the chapter. Now we show how to use this theorem in order to calculate values of Euler’s function, playing an important role in Numbers’ Theory. First, let us define this function.

Definition 20.1. Euler’s function is the function $\varphi(m)$, defined on the set of the natural numbers $\mathbb{N}$, which equals to the number of all the natural numbers which are less than $m$ being reciprocal to it.

For example, $\varphi(1) = 0$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$. But the value $\varphi(10^6)$, i.e. the number of all the natural numbers which are less than one million being reciprocals to it, is not so easy to compute. Let us find it with the use of the following consequence of theorem 20.1.

Corollary 20.1. If $m = p_1^{a_1} \ldots p_n^{a_n}$ is the decomposition of $m$ onto the
prime factors then

\[ \varphi(m) = m \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_n}\right). \]  

(20.5)

**Proof.** Let us denote by \([1, m]\) the initial segment of the natural series, consisting of the numbers 1, 2, ..., \(m\). For any number \(i\) from \([1, n]\) we consider the set \(A_i\) of all the numbers from the segment \([1, m]\) which can be divided by \(p_i\):

\[ A_i = \{k \in [1, m] : p_i | k\}. \]

The union \(A_1 \cup \ldots \cup A_n\) consists of all the numbers which can be divided on at least one of the numbers \(p_1, \ldots, p_n\). Therefore the complement

\[ [1, m] \setminus (A_1 \cup \ldots \cup A_n) \]

contains all the numbers which can not be divided on each of the numbers \(p_1, \ldots, p_n\) (i.e. they are reciprocal to \(m\)). The power of this complement is exactly the value of \(\varphi(m)\) of Euler’s function. Thus, by formula (20.4),

\[ \varphi(m) = m - |A_1 \cup \ldots \cup A_n| = m - \sum_{i=1}^{n} |A_i| + \sum_{i<j} |A_i \cap A_j| - \ldots + (-1)^n |A_1 \cap \ldots \cap A_n|. \]

Let us calculate the power of each of the sets \(A_i\), each of the intersections \(A_i \cap A_j\) and so on. By the definition, the set \(A_i\) consists of all the numbers from 1 to \(m\) which can be divided by \(p_i\), i.e. of the numbers \(p_i, 2p_i, \ldots, \frac{m}{p_i} \cdot p_i\). These are \(m/p_i\) numbers and hence

\[ |A_i| = \frac{m}{p_i}, \quad i = 1, \ldots, n. \]

Similarly, the intersection \(A_i \cap A_j\) consists of all the numbers from the segment \([1, m]\) which can be divided by both \(p_i\) and \(p_j\); that is why they can be divided by the product \(p_i p_j\). Therefore

\[ |A_i \cap A_j| = \frac{m}{p_i p_j}. \]
Now it is clear that the power of the triple intersection $A_i \cap A_j \cap A_k$ equals to $m/p_i p_j p_k$ and so on. Finally, we obtain

$$\varphi(m) = m - \sum_i \frac{m}{p_i} + \sum_{i<j} \frac{m}{p_i p_j} - ... + (-1)^n \frac{m}{p_1 ... p_n} =$$

$$m \left(1 - \sum_i \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - ... + (-1)^n \frac{1}{p_1 ... p_n}\right) \quad (20.6)$$

It is time to establish that the right-hand side of (20.5) coincides with the last expression. With this aim we multiply

$$(1 - \frac{1}{p_1}) (1 - \frac{1}{p_2}) ... (1 - \frac{1}{p_n}).$$

First, in each of $n$ factors (binomials) we take the first summand (the unit); multiplying it $n$ times we obtain the unit. Then we take the unit $n - 1$ times and we take one of the numbers $-1/p_1, ..., -1/p_n$. The sum of all these products equals to $- \sum_i \frac{1}{p_i}$. After that we take the unit $n - 2$ times and in last two binomials we take $-1/p_i$ and $-1/p_j$. The summation of these multiplications gives $\sum_{i<j} \frac{1}{p_i p_j}$. These arguments show that the expression (20.6) is the result of the multiplication of the binomials in the right-hand side of (20.5).

Let us use formula (20.5) in order to compute $\varphi(10^6)$. Since $10^6 = 2^6 5^6$, then $p_1 = 2$, $p_2 = 5$, and hence

$$\varphi(10^6) = 10^6 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 4 \cdot 10^5.$$
Lecture 21. The hats problem

We will discuss the following problem: $n$ men give their $n$ huts to a cloak-room attendant; it is necessary to find how many versions are there for returning the huts in such a way that any man gets a hut but no man gets his own one. Here the cloak-room attendant is present in order to adorn the perception of the problem. Clearly, the equivalent formulation of the problem consists of the following: to find the numbers of ways of exchanging the huts by $n$ men. If enumerate the men by numbers from 1 to $n$ then each way of the exchanging can be interpreted as a one-to-one map in the set $M_n = \{1, ..., n\}$ under which no elements goes to itself. The one-to-one map $\varphi : M_n \to M_n$ can be characterized by the following correspondence:

\[
\begin{align*}
1 & \rightarrow i_1 \\
2 & \rightarrow i_2 \\
\vdots \\
n & \rightarrow i_n,
\end{align*}
\]

showing that the hut of the first man was obtained by the man with number $i_1$, the hut of the second man was obtained by the man with number $i_2$ and so on; besides the condition that no man gets his own hut is equivalent to the following:

\[
i_1 \neq 1, \ i_2 \neq 2, \ ..., \ i_n \neq n.
\]

Recall that the one-to-one map $\varphi : M_n \to M_n$ of the set $M_n$ onto itself we call a bijection. The last condition above can be written in the form

\[
\varphi(1) \neq 1, \ \varphi(2) \neq 2, \ ..., \ \varphi(n) \neq n;
\]

if it is fulfilled then it is said that the bijection $\varphi$ has no fixed (elements) points, because no element goes to itself under this bijection. Respectively, it is said that an element $k \in M_n$ is fixed with respect to the map $\varphi$ if $\varphi(k) = k$. For
instance, if \( n = 3 \) then among the bijective maps

\[
\begin{align*}
1 & \rightarrow 3 & 1 & \rightarrow 1 & 1 & \rightarrow 3 & 1 & \rightarrow 1 \\
2 & \rightarrow 1 & 2 & \rightarrow 3 & 2 & \rightarrow 2 & 2 & \rightarrow 2 \\
3 & \rightarrow 2 & 3 & \rightarrow 2 & 3 & \rightarrow 1 & 3 & \rightarrow 3
\end{align*}
\]

the first one has no fixed elements, for the second and for the third ones, the fixed points are 1 and 2 respectively, and, for the forth one, all the elements are fixed.

The given arguments shows that the number \( f(n) \), expressing the number of ways for exchanging the huts of \( n \) men in the problem above, coincides with the number of the bijections on the set \( M_n \), having no fixed points. The expression for \( f(n) \), as a function of \( n \), is given in the following theorem.

**Theorem 21.1.** We have \( f(1) = 0 \) and

\[
f(n) = n! \left( \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{(-1)^n}{n!} \right), \text{ if } n \geq 2. \tag{21.1}
\]

**Proof.** For each \( i \in \{1, \ldots, n\} \), we denote by \( A_i \) the set of all the bijective maps \( \varphi : M_n \rightarrow M_n \), having the element \( i \) as fixed: \( \varphi(i) = i \). For example, if \( n = 3 \) then, among the 6 bijections

\[
\begin{align*}
1 & \rightarrow 1 & 1 & \rightarrow 1 & 1 & \rightarrow 2 & 1 & \rightarrow 2 & 1 & \rightarrow 3 & 1 & \rightarrow 3 \\
2 & \rightarrow 2 & 2 & \rightarrow 3 & 2 & \rightarrow 1 & 2 & \rightarrow 3 & 2 & \rightarrow 1 & 2 & \rightarrow 2 \\
3 & \rightarrow 3 & 3 & \rightarrow 2 & 3 & \rightarrow 3 & 3 & \rightarrow 1 & 3 & \rightarrow 2 & 3 & \rightarrow 1,
\end{align*}
\]

the first two belong to \( A_1 \), the first and the sixth ones belong to \( A_2 \), and the first and the third ones belong to \( A_3 \) (the forth and the fifth ones have no fixed points).

Clearly, the union \( A_1 \cup \ldots \cup A_n \) is the set of all the bijective maps \( \varphi : M_n \rightarrow M_n \), having at least one fixed point. That is why

\[
f(n) = (\text{the number of all the bijective maps}) - |A_1 \cup \ldots \cup A_n|.
\]

But from section 18 we know that the number of all the bijective maps equals to \( n! \), and hence, having in mind the inclusion-exclusion principle, we get:

\[
f(n) = n! - |A_1 \cup \ldots \cup A_n| =
\]
\begin{equation}
n! - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - ... + (-1)^n |A_1 \cap ... \cap A_n|.
\end{equation}

Let us compute $|A_i|$. The set $A_i$ consists of all the possible bijections $\varphi : M_n \rightarrow M_n$ under the following condition: $\varphi(i) = i$. The number of such bijective maps is the same as the number of all the possible bijections of the set $M_n \setminus \{i\}$ onto itself, i.e., according to lecture 18, this number equals to $(n-1)!$.

Similarly, $A_i \cap A_j$ consists of all the bijections $\varphi : M_n \rightarrow M_n$, satisfying $\varphi(i) = i$, $\varphi(j) = j$. The number of such bijective maps is the same as the number of all the possible bijections of the set $M_n \setminus \{i,j\}$ onto itself, i.e., this number equals to $(n-2)!$.

The arguments above can be applied to any intersection $A_{i_1} \cap ... \cap A_{i_k}$:

$|A_{i_1} \cap ... \cap A_{i_k}| = (n-k)!$.

As a result we get

$$f(n) = n! - C_n^1(n-1)! + C_n^2(n-2)! - ... + (-1)^n C_n^n,$$

because in (21.2) we have $n = C_n^1$ summands in the first sum, $C_n^2$ summands in the second one and so on. Now, using formula for the number of combinations $C_n^k$, we obtain:

$$f(n) = n! - n! + \frac{n(n-1)}{2!}(n-2)! - ... + (-1)^n.$$

This implies formula (21.1).

**Remark.** According to (21.1) and the result, known from the standard course of Mathematical Analysis, we obtain

$$\lim_{n\rightarrow \infty} \frac{f(n)}{n!} = \frac{1}{e}.$$ 

Thus the function $f(n)$ expresses the combinatorial interpretation of the number $e$, which is important in Mathematical Analysis, Probability Theory and other branches of Mathematics.
Chapter V.

Order Relations and Axiom of Choice
The natural numbers are used not only to answer the question "How many?" but also to answer the question "What with respect to the order?". In other words, they are used as both cardinal and ordinal numbers. The powers can be use as cardinal numbers only. For description of order we need different notions. Even the simplest infinite set, the set of natural numbers, can be ordered by infinitely many ways. For instance, instead of the standard disposition 1, 2, 3, 4, 5, 6 ... one can do as follows. First we take all the odd numbers (with the usual order) and then we take the even ones; then we obtain the following disposition 1, 3, 5 ..., 2, 4, 6 ... Under this disposition each even number follows any odd number.

A description of an order on a given set $M$ can be done with the use of the comparison of pairs of elements from $M$, i.e. via finding out what element of $a, b \in M$ follows another one. By other words, the notion of the order is one of the binary relations; besides it is very important, on a level with the equivalence relations (see section 12). The most general of order relations is the relation of partial order; with this relation we begin this chapter.
Lecture 22. Partially ordered and ordered sets

Definition 22.1. A binary relation $\varphi$ on a set $M$ is called relation of partial order, if it is reflexive, transitive and antisymmetric.

The reflexivity and transitivity properties of binary relations were defined in lecture 12; the antisymmetry property of the relation $\varphi$ consists of the following:

$$a \varphi b, \ b \varphi a \implies a = b.$$  

A set $M$, with a given relation of partial order on it, is called partially ordered set.

As for the equivalence relation the special sign $\sim$ is used, one uses the sign $\leq$ for the relation of the partial order. Thus, a relation of the partial order on a set $M$ is a binary relation with the following properties:

1) $a \leq a$ for all $a \in M$ (reflexivity);

2) $a \leq b, \ b \leq c \implies a \leq c$ (transitivity);

3) $a \leq b, \ b \leq a \implies a = b$ (antisymmetry).

Let us give examples of partially ordered sets.

Example 22.1. The relation of non-strict inequality on the set of all the real numbers $\mathbb{R}$ is a relation of partial order.

Example 22.2. Any set can be (trivially) considered as partially ordered if one sets

$$a \leq b \text{ if and only if } a = b.$$  

This relation is called trivial.

Example 22.3. Let $M$ be a set of all the continuous functions on a segment $[a, b]$. For a pair of functions $f = f(x)$ and $g = g(x)$ from $M$ we set

$$f \leq g \iff f(x) \leq g(x) \text{ for all } x \in [a, b].$$
The functions $f$ and $g$, with graphs drawn on picture (20), are in the relation $f \leq g$, but the functions $\varphi$ and $\psi$, with graphs drawn on picture (21), are not in the relation $\varphi \leq \psi$.

**Example 22.4.** The set $\mathcal{M}$ of all the subsets of a fixed set $M$ is partially ordered with respect to the inclusion: for two sets $A, B \subset M$ (at the same time $A, B \in \mathcal{M}$ are elements of $\mathcal{M}$)

$$A \leq B \iff A \subset B.$$  

**Example 22.5.** The following relation on the set of all the natural numbers $\mathbb{N}$ is a relation of partial order:

$$a \leq b \iff b \text{ can be divided on } a.$$  

An example of a binary relation being not a partial order relation is the parallelism relation for lines (it is not antisymmetric).

Let $M$ be a partially ordered set. If the elements $a, b \in M$ are in the relation of partial order $a \leq b$ it is said that $a$ precedes $b$ or $a$ is equal or less than $b$; sometimes it is said $b$ follows $a$ or $b$ is equal or greater than $a$.

Let us "decode"the meaning of the word "partial" in the notion of partial order. With this aim, we call elements $a, b \in M$ comparable if $a \leq b$ or $b \leq a$. Not all the elements of $M$ are comparable at all; this is the very reason why we say about "partial" order. The discussion allows us to introduce the following definition.
Definition 22.2. A partially ordered set is called ordered, if any its elements are comparable.

Note that in some books the defined above ordered sets are called linearly ordered.

The reader can easily convince yourself that sets from examples 22.2-22.5 are not ordered, but the set from example 22.1, i.e. the set of the real numbers \( \mathbb{R} \) with the usual order "equal or less than", is. Of course, any subset in \( \mathbb{R} \), in particular, the natural series \( \mathbb{N} \), the set of the rational numbers \( \mathbb{Q} \), are ordered with the relation of order in the consideration.
Lecture 23. Ordinal types

Let us remember how we came to the notion of set’s power. At the beginning we defined the power as something common for all the equipotent sets. Then, in order to interpret "this general we ascribed the notion of the power to any equivalence class, consisting of all the equipotent sets. Besides, sets $A$ and $B$ were called equipotent if there was a one-to-one correspondence between them. The power, ascribed to a class of all the equipotent sets, can be called also a "cardinal type" of sets. Our aim is to define a notion of "ordinal type", including all the ordered (or partially ordered) sets which admits a one-to-one correspondence between them preserving the order. Let us give the precise definition.

**Definition 23.1.** Let $M$ and $M'$ be two partially ordered sets, and let $f$ be a map from $M$ to $M'$. It is said that the map preserves the order if $a \leq b$, with $a, b \in M$, implies $f(a) \leq f(b)$ in $M'$.

**Definition 23.2.** A map $f : M \to M'$ of partially ordered sets is called isomorphism of sets $M$ and $M'$ if
1) $f$ is a bijective map (i.e. one-to-one correspondence);
2) both $f$ and $f^{-1}$ preserve order.

In other words, the map $f$ is isomorphism if $f$ is bijective and $f(a) \leq f(b)$ if and only if $a \leq b$.

If there is isomorphism between $M$ and $M'$ then these sets are called isomorphic.

Let, for instance, $M$ be the set of all the natural numbers, partially ordered with respect to the "division"property (see example 22.5), and $M'$ be the same set ordered in the natural way:

$$a \leq b \iff b - a \text{ is not negative.}$$

Consider the identity map $f : M \to M'$, mapping any element $n$ to itself. This map is bijective and it preserves the order, because if $b$ can be divided by $a$ then $b - a$ is not negative. However, the inverse map does not preserve
the order: for example, the numbers $a = 3$ and $b = 4$ is in the natural order but 4 cannot be divided by 3; hence 3 does not precedes 4 with respect to the "division". Thus, the map $f$ is not an isomorphism.

Now consider as $M$ the set of all the whole numbers with the following order:

$$n \leq m \iff \begin{cases} |n| < |m|, & \text{or} \\ |n| = |m|, & n \geq 0, \ m \leq 0, \ \text{or} \\ n = m \end{cases}.$$ 

It is not difficult to see that $M$ is ordered set. Besides, the map $f : M \to \mathbb{N}$, defined by the rule

$$f(n) = \begin{cases} 2n, & \text{if } n \geq 1, \\ -2n + 1, & \text{if } n \leq 0, \end{cases}$$

is an isomorphism, if the natural order is introduced on the set of all the natural numbers (please, check it!).

The isomorphism relation between partially ordered sets is the equivalency relation (it is reflexive, symmetric and transitive). Therefore all the totality of partially ordered sets can be divided on the classes of isomorphic sets.

**Definition 23.3.** It is said that isomorphic partially ordered sets has the same ordinal type.

Thus, the ordinal type is that common for all the isomorphic partially ordered sets.
Lecture 24. Well-ordered sets

The discussion of order relations we begun with the partial order, then we introduced the notion of ordered sets as a particular case of the partial order. More narrow, but very important notion, is the notion of well ordered sets.

Definition 24.1. An ordered set is called well ordered if its any non-empty subset contains minimal element, i.e. an element preceding all the other elements of the subset.

Obviously, any finite ordered set is well-ordered. The natural series with the natural order is well-ordered too. Indeed, if \( A \) is a non-empty subset of \( \mathbb{N} \) then, choosing in \( A \) an element \( n_0 \), it is easy to find in \( A \) the minimal element among the numbers \( 1, 2, ..., n_0 \).

Not all the ordered sets are well ordered. For instance, the set of all the real numbers \( \mathbb{R} \) with the natural order is not the one. Indeed, the half-segment \( (0, 1] \) contains no minimal element because for any \( a \) from the half-segment the number \( a/2 \) preceds \( a \).

Of course, these arguments show that the set of all the rational numbers \( \mathbb{Q} \) with the natural order is not well ordered too. However, similarly to any other countable set, \( \mathbb{Q} \) can be turned into a well ordered set (can be endowed with the well order), inducing the order of the natural series by the enumeration of the elements of \( \mathbb{Q} \). At the same times, it is not easy to imagine how to define a well order on the set of all the real numbers. But it is possible to do. Moreover, Zermelo Theorem, which will be proved in the next lecture, states that any set can be well-ordered.

Now we consider the problem of the comparison of ordinal types for well-ordered sets. Since the class of well-ordered sets is very important, it is appropriate to give the following definition.

Definition 24.2. The ordinal type of a well-ordered set is called ordinal number.

In order to compare the ordinal numbers we introduce the notion of the segment of an ordered set \( M \); it is defined by a point \( a \in M \) and consists of all
elements $x$ being less than $a$:

$$P_a = \{x \in M : x < a\}.$$

**Definition 24.3.** Let $\alpha$ and $\beta$ be two ordinal numbers, and $M$ and $N$ be the sets of types $\alpha$ and $\beta$ respectively. It is said that $\alpha = \beta$, if the sets $M$ and $N$ are isomorphic, that $\alpha < \beta$, if $M$ is isomorphic to a segment in $N$, and that $\alpha > \beta$, if $N$ is isomorphic to a segment in $M$.

The following theorem states that any two ordinal numbers are comparable.

**Theorem 24.1.** Any two ordinal numbers are connected by one and only one of the following relations:

$$\alpha = \beta, \quad \alpha < \beta, \quad \alpha > \beta.$$  \hfill (24.1)

Before proving the theorem, we see that, the introduced in definition 24.3, comparison of the ordinal numbers is a relation of partial order. Namely, for two ordinal numbers $\alpha$ and $\beta$ we set

$$\alpha \leq \beta \iff \alpha = \beta \text{ or } \alpha < \beta$$ \hfill (24.2)

**Proposition 24.1.** The relation $\leq$ on the totality of all the ordinal numbers, defined by property (24.2), is a relation of partial order.

**Proof.** The reflexivity of the relation is obvious. Also it easy to establish the transitivity property. With this aim, we assume that three ordinal numbers $\alpha, \beta$ and $\gamma$ are connected via properties

$$\alpha \leq \beta, \quad \beta \leq \gamma,$$

and $M, N, L$ are the sets of types $\alpha, \beta, \gamma$ respectively. The relations above mean that there exist an isomorphism $f$ of the set $M$ onto $N$ or onto a segment in $N$ and an isomorphism $g$ of the set $N$ onto $L$ or onto a segment in $L$. The composition $g \circ f$ of these maps is an isomorphism of the set $M$ onto $L$ or onto a segment in $L$ (please, prove it!). Hence the transitivity is proved. In order to prove the antisymmetry, we use the following statement.
**Lemma 24.1.** A well-ordered set cannot be isomorphic to its segment.

For proving the lemma we use the rule contraries. Let us assume that a well-ordered set $M$ is isomorphic to its segment $P_a = \{x \in M : x < a\}$, and let $f : M \to P_a$ be the assumed isomorphism. Consider in $M$ the subset

$$B = \{x \in M : f(x) < x\},$$

which is not empty because it contains the element $a$. Since $M$ is well-ordered, $B$ has the minimal element. Denote it by $x_0$; let $y_0 = f(x_0)$ be its image. As $x_0 \in B$, we have $y_0 < x_0$, and hence $f(y_0) < f(x_0) = y_0$ (recall that, being an isomorphism, $f$ preserves the order). But the inequality $f(y_0) < y_0$ means that $y_0$ belongs to $B$. However we proved that it is less than $x_0$. This contradicts the minimal property of $x_0$ and therefore the lemma is proved.

Now we return to the proof of the proposition. Namely, let us establish the antisymmetry property for relation (24.2). Thus, assume that two ordinal numbers $\alpha$ and $\beta$ satisfy the properties

$$\alpha \leq \beta \quad \text{and} \quad \beta \leq \alpha.$$

This means that, for the sets $M$ and $N$ of types $\alpha$ and $\beta$ respectively, there are an isomorphism $f$, mapping $M$ to $N$ or to a segment in $N$, and an isomorphism $g$ mapping $N$ to $M$ or to a segment in $M$. Then the composition $g \circ f$ is an isomorphism of $M$ onto a subset $A$ of $M$. There are two possibilities only: either $A = M$ or $A$ is a segment in $M$. Indeed, if $f(M) = N$ then $A = g(N)$ and hence $A$ is either $M$ or a segment in $M$. If $f(M) \neq N$ then $f(M)$ is a segment in $N$ and hence its image $g(f(M)) = A$ is a segment in $M$.

Thus, the first possibility gives $f(M) = N$ and $\alpha = \beta$, and the second possibility is excluded because of the statement of the lemma. The proof of the proposition is finished.

**Proof of the theorem.** Part 1: the existence of at least one of the correlations (24.1). To any ordinal number $\alpha$ we correspond a set $W(\alpha)$ consisting of ordinal numbers which are equal or less than $\alpha$. Define on $W(\alpha)$ the order relation with respect to the value of ordinal numbers; show that $W(\alpha)$ is a well-ordered set with the ordinal number $\alpha$. With this aim, consider
a set $A$ with a ordinal type (number) $\alpha$ and correspond to any element $a \in A$ the ordinal number $\xi_a$ of the segment $P_a$. The correspondence $a \to \xi_a$ is an isomorphism $f : A \to W(\alpha)$, and hence $W(\alpha)$ has the type $\alpha$. Indeed, first we note that $\xi_a < \alpha$, and $f$ maps $A$ into $W(\alpha)$. This is injective, because for different elements $a, b \in A$ we have either $a < b$ or $b < a$ for $A$ is well ordered. That is why, either $P_a < P_b$ or $P_b < P_a$, which means $\xi_a = f(a) \neq f(b) = \xi_b$. This also shows that $f$ preserves the order: $a < b \implies f(a) < f(b)$. Further, $f$ is surjective because, according to definition 24.3, for any ordinal number $\xi \in W(\alpha)$, i.e. the number which less than $\alpha$, there is a segment $P_a \in A$ with the ordinal number $\xi$. Thus, $f$ is bijective map preserving the order. Finally, we see that, if $f(a) \leq f(b)$ then $P_a \subseteq P_b$, and hence, $a \leq b$, i.e. $f$ is an isomorphism.

Now let us begin the proof of part 1 itself. Let $\alpha$ and $\beta$ be two ordinal numbers. Consider the corresponding sets $W(\alpha)$ and $W(\beta)$ of types $\alpha$ and $\beta$ respectively. Let us prove that either the sets $W(\alpha)$ and $W(\beta)$ coincide or one of them is a segment in another one; this would mean that one of the correlations (24.1) is fulfilled.

Denote $W(\alpha)$ and $W(\beta)$ by $A$ and $B$ respectively and consider their intersection $C = A \cap B$. Obviously, it is sufficient to prove that $C$ coincides with at least one of the sets $A$ and $B$; besides, if it coincides with one only then it is a segment in another one. If $C = A \cap B$ then there is nothing to prove. Let $C \neq B$ and $\gamma$ be the minimal element in $B \setminus C$ (as $B$ is well ordered, such an element exists). Let us show that $C$ coincides with the segment $P_\gamma$, defined by the element $\gamma$ in $B$. Indeed, if $\xi \in P_\gamma$ then $\xi < \gamma < \beta$, and, since $\gamma$ is the minimal element in $B$ does not belonging to $C$, we obtain $\xi \in C$. Back, let $\xi \in C$. Belonging to an ordered set $B$, the elements $\xi$ and $\gamma$ are comparable: $\xi \geq \gamma$. But the correlation $\gamma < \xi$ is impossible because in this case we would have $\gamma < \xi < \alpha, \gamma < \xi < \beta$, i.e. $\gamma \in A \cap B = C$. Therefore $\xi < \gamma$, and that is why $\xi \in P_\gamma$.

Thus, $C = P_\gamma$. It is left to show that $P_\gamma = A$. The inclusion $P_\gamma \subset A$ is obvious because $P_\gamma = A \cap B$. If there would be an element $\eta$ in $A$ with $\eta > \gamma$ then we would have $\gamma < \eta < \alpha, \gamma < \beta$, i.e. $\gamma \in C$. Therefore $P_\gamma = A$, and the
first part of the theorem is proved.

Part 2: for any pair of ordinal numbers \( \alpha, \beta \) there is the only one of correlations (24.1). By the lemma, the correlations \( \alpha = \beta \) and \( \alpha < \beta \) can not be fulfilled simultaneously. Similarly, it is impossible to have \( \alpha = \beta \) and \( \alpha > \beta \) at the same time. Finally, the correlations \( \alpha < \beta, \ \beta < \alpha \) are incompatible too because otherwise the transitivity property (see the proposition) implies \( \alpha < \alpha \), which is impossible as we have seen above. The theorem is proved.
Lecture 25. Zermelo Theorem and Axiom of Choice

Theorem 24.1 on the comparability of ordinal numbers allows us to do the conclusion on the comparability of powers of well-ordered sets:

if $A$ and $B$ are well-ordered sets then they are either equipotent or the power of one of them is greater than the power of another one.

Indeed, according to this theorem, the sets $A$ and $B$ are either isomorphic (then $A$ and $B$ are equipotent) or one of them isomorphic to a segment of another one (then the first one is equipotent to a part of another one). In the second case, if, in its turn, the first set has a part which is equipotent to the second set then, by Kantor-Bernstein theorem, we again conclude that $A$ and $B$ are equipotent; if there is no such a part then we see that the power of the first set is greater than the power of the second one.

The possibility to compare the powers of well-ordered sets hints us ask the following question:

is it possible to turn any set into a well-ordered one, i.e. to introduce an order relation on it, under which its any non-empty subset has the minimal element?

The following theorem gives a positive answer to the question:

**Theorem 25.1** (Zermelo Theorem). Any set can be well-ordered.

Zermelo proved this theorem in 1904. Till now not all the mathematicians agree with its statement. The matter is not an error in the theorem’s proof; the matter is that its proof is based on a very "non-constructive"statement which is called Axiom of Choice. This is its essence.

Imagine, you see some heaps of apples. Clearly, one can choose an apple from any heap and to put them into a new one. There are no abstractions to do this in the case where each of the heaps contains of infinitely many apples, and the heaps themselves are infinitely many too. This is precisely the Axiom of Choice:

given a totality of sets, it is possible to choose from any set an element (not giving in advance a rule for choosing, which is exactly the non-structural choice).
Many mathematicians used Axiom of choice long before Zermelo Theorem appeared; they considered it as absolutely obvious. But after the appearing, mathematicians begun to think deeply about this axiom; it became to be more an more mysterious. Many theorems, proved with its use, contradict the visual experience (one of these, expressing Banach-Tarski paradox, will be discussed in the next lecture). Famous logician B. Rassel said about it: "At first it seems to be obvious; but the more one thinks about it the more strange seem its conclusions. At the end one stops to understand what does it mean."

Note that the refusion of the Axiom of Choice make the constructions of Set's Theory more poor. At the same time, the attempt not to use it leaded to the creation of such constructive notions as "computable number" and "recursive functions", played a great role in the creation of computers.

Let us reformulate the Axiom of choice in order to use it more conveniently.

**Axiom of Choice.** Given set $M$, there is a function (map) $\varphi$, corresponding to any non-empty subset $A$ from $M$ a definite element $\varphi(A)$ of the subset.

In other words, the function $\varphi$ marks an element in each non-empty subset of the set $M$.

We note that, for countable sets $M$, Axiom of Choice can be easily proved. Indeed, if $M$ is a sequence $\{a_1, a_2, \ldots, a_n \ldots\}$, the one can choose (mark) in each non-empty subset $A$ from $M$ the element having minimal possible number.

It is not difficult to see that the arguments for countable sets, automatically ordered by the enumeration of its elements, can be applied to any well-ordered set. Namely, for a well-ordered set, in any its non-empty subsets one can choose the minimal element.

This discussion means that *Zermelo Theorem implies Axiom of Choice*: if any subset can be well-ordered then Axiom of Choice is fulfilled. And since now we will deduce Zermelo theorem from Axiom of Choice, we can state that *Axiom of Choice is equivalent to Zermelo Theorem*.

**Proof of Zermelo Theorem.** We reproduce the arguments from the book [8] by A.G. Kurosh.
Let a set $M$ be given. Using Axiom of Choice, we mark in each of its non-empty subsets $N$ an element $\varphi(N)$. A non-empty subset $A$ from $M$ is called marked, if it can be well-ordered in such a way that for any $a \in A$

$$a = \varphi(M \setminus A'),$$

where $A'$ is the segment of the set $A$ in the well-order above, defined by the element $a$. The marked sets in $M$ exist; for instance, a subset, consisting of the only one element $\varphi(M)$ is the one.

Let $A$ and $B$ be two marked subsets with the chosen well-orders having property (25.1). Then both these sets have $\varphi(M)$ as the first element and hence they have non-empty coinciding segments. The union of all the coinciding subsets of these sets is, obviously, a segment in each of the sets; actually, this is the largest among the coinciding segments. If this segment $C$ would differ from both $A$ and $B$ then, by the definition of the marked set, the segment $C$ would be given in both $A$ and $B$ by an element $\varphi(M \setminus C)$, and then $A$ and $B$ would have a greater than $C$ coinciding segments (consisting of $C$ and the element $\varphi(M \setminus C)$). This contradiction with the definition of $C$ shows that one of the marked sets $A$ and $B$ is a segment in another one.

This implies that the union $L$ of all the marked subsets in $M$ is marked itself. Really, if $a$ and $b$ from $L$ belong to the marked subsets $A$ and $B$ respectively then they both belong to the largest of these sets, say, $A$. Setting $a \geq b$ in $L$, if $a \geq b$ in $A$, we turn $L$ into an ordered set. Let us show that $L$ is well-ordered. With this aim we take in $L$ a non-empty subset $E$ and, for an element $x_0 \in E$, we consider in $E$ the subset $E'$ of all the elements which are equal or less than $x_0$. Since the set $\{x \in L : x \leq x_0\}$ is included to a marked (and hence, a well-ordered) subset $A$, the set $E'$ is well-ordered too. That is why $E'$ contains the minimal element which is the minimal for $E$ too; this implies that $L$ is well-ordered. Finally, if $a \in L$ then $a$ is contained in a marked set $A$ and defines in both $L$ and $A$ the same segment $A'$, besides, $a = \varphi(M \setminus A')$. This proves that the set $L$ is marked.

In order to finish the proof of the theorem we note that if $L$ would differ from $M$ then, contradicting with the definition of $L$, we would obtain, a greater
than \( L \) marked subset (adding to \( L \) an element \( \varphi(M \setminus L) \) and considering this element following after all the elements of \( L \).

\[ \square \]

**Corollary 25.1.** For any two sets \( A \) and \( B \), one can say that either they are equipotent or one of them is equipotent to a part of another one.

The statement of the corollary follows from Zermelo Theorem and theorem from the previous lecture on the comparability of ordinal numbers (we have already discussed this above).
Lecture 26. The Banach-Tarski Paradox

One of the most wonderful corollaries of Axiom of Choice is the paradox on the dividing a ball, discovered in 1924 by S. Banach and A. Tarski. They succeeded to divide a ball on ten parts in such a way that the first six parts give together a ball of the same radius and the second four parts together give a ball of the same radius too. In this process, nothing is added to the parts above and the parts are moved as whole solid bodies. This statement (on the possibility of such a division of a ball) has a theoretical value and it is rather naive to hope, say, to produce two apples from the one. This would contradict the Law of the Conservation of the Substance. The matter is that, constructing a model of an apple as a geometric figure, we assume that this figure consists of points having no size. Geometrical parts, the ball is divided to, can consists of densely distributed points, which does not form a continuous body (a substance). However, Axiom of Choice allows the formal construction of such parts. Moreover, even without Axiom of Choice, it is possible to divide a figure in two parts, which are congruent to the figure itself. Let us give an example of such a figure; its construction is taken from the paper by K. Stromberg [13].

We recall that two figures are called congruent if one can be obtained from another by a movement, i.e. by the parallel shift and the rotation (of the figure as a solid body). The fact that a figure can be congruent to its part is of no wonder. For instance, a half-line \( \{ x \in \mathbb{R} : x \geq 0 \} \) on the real axis \( \mathbb{R} \) turns into a congruent half-line \( \{ x \in \mathbb{R} : x \geq 1 \} \), contained in the initial one, by the parallel shift on 1 to the right.

Now consider a more interesting example. We will construct a set \( X \) on the plane which can be divided on two parts \( X_1 \) and \( X_2 \), each of them is congruent to the set \( X \) itself.

Thus, we consider the plane, interpreted as the set of all the complex numbers \( z = x + iy \), where \( i = \sqrt{-1} \) is the imaginary unit. On the unit circumference \( |z| = 1 \) we choose a point \( z_0 \), being transcendental. As the circumference is continual and the set of all the non-transcendental (algebraic)
numbers is countable, then such a point $z_0$ exists. One can show that the number

$$z_0 = e^i = \cos 1 + i \sin 1,$$

characterized by the angle of one radian (approximately $57^\circ 17'\!$) on the unit circumference, is transcendental.

As the set $X$ we consider all the complex numbers $z$ which can be presented in the form

$$z = \sum_{k=0}^{n} a_k z_0^k,$$  \hspace{1cm} (26.1)

where all the coefficients $a_0, a_1, ..., a_n$ are whole non-negative numbers and the number $n$ may be arbitrary from the set of the whole non-negative numbers. For $n = 0$, the numbers $z = a_0$ (i.e. all the whole non-negative numbers) have type (26.1); for $n = 1$, these are all the numbers presented as $a_0 + a_1 z_0$, for $n = 2$, these are all the numbers in the form $a_0 + a_1 z_0 + a_2 z_0^2$ and so on. The set $X$ is very densely distributed on the plane. For instance, for $z_0 = e^i$, already the numbers $z_0^k$, $k = 1, ..., 90$ are very densely distributed on the unit circumference; similarly, the numbers $2z_0^l$, $l = 1, ..., 180$ are very densely distributed on the circumference of radius 2 (see 22). All the possible sums of sets \{ $z_0^k$ \}, \{ $2z_0^l$ \} are already very densely distributed in the circle of radius 4 (see 23).

If one takes all the possible sums of numbers from sets

$$\{a_0\}, \{z_0^k\}, \{2z_0^l\}, \{3z_0^j\}, ... ,$$

i.e. all the numbers of type (26.1), then they will be densely distributed on the plane.

It is important to note that any number in $X$ admits the only one form of type (26.1). Indeed, let a number $z$ from $X$ can be presented in a form:

$$z = \sum_{k=0}^{m} b_k z_0^k,$$
Lecture 26.

The Banach-Tarski Paradox

Pic. 22.

Pic. 23.
with the whole coefficients $b_k$, different from the ones in (26.1). Then, subtracting one representation from another one, we obtain

$$\sum_{k=0}^{s} (a_k - b_k) z_0^k = 0, \quad s = max\{n, m\},$$

i.e. $z_0$ is a solution to an algebraic equation with the whole coefficients. As $z_0$ is transcendental, the only situation is possible, where $a_k = b_k$ for all $k$. At the same time, we note that $X$ is countable and hence it does not coincide with the plane.

Now let us divide $X$ on two parts. As the first set we take all the numbers $z \in X$ having zero coefficient $a_0$ in the representation (26.1). Let $X_2$ be the complement of $X_1$ in $X$. Since each element in $X$ is uniquely presented in the form (26.1), $X_1$ contains all the numbers from $X$ with $a_0 \geq 1$.

Let us show that the rotation of all the set $X$ on the angle, being equal to the argument of the complex number $z_0$ (one radian, if $z_0 = e^i$) gives the set $X_1$. Indeed, we know that, under the multiplication, the moduli of complex numbers are multiplied and their arguments are summarized. The module of the number $z_0$ equals to 1 and hence the multiplication operation $z_0 \cdot z$ of the complex number $z$ on $z_0$ corresponds to the rotation of the number $z$ on the angle $\theta = argz_0$ (counter clock-wise). Let $\rho$ be the rotation operation on the angle $\theta$, and $\rho(X)$ be the result of the rotation of the set $X$, i.e. the set, obtained by the multiplication of any number from $X$ over $z_0$:

$$\rho(X) = \{z_0 \cdot z : z \in X\}.$$  

Taking into the account the representation of any number $z \in X$ in the form (26.1), we obtain that $\rho(X)$ is the set of all the numbers admitting the representation (26.1) with the zero coefficient for zero degree of $z_0$. But this precisely means $\rho(X) = X_1$.

Finally, let us prove that, by the shift to the right, the set $X$ turns into $X_2$. Let $\tau$ be the shift operation, i.e. $\tau(z) = z + 1$. Then the result of the shift is the set

$$\tau(X) = \{z + 1 : z \in X\}.$$
Taking into the account (26.1), where $a_k \geq 0$ for all $k$, we see that the number $z+1$ has $a_0 \geq 1$ in the representation (26.1), i.e. the number $z+1$ belong to $X_2$ if $x \in X$. Therefore $\tau(X) = X_2$, and the statement on the mutual congruence of the sets $X, X_1, X_2$ is proved.
Abel, Niels Henrik (1802-1829) – Norway mathematician proved the absence of radical solutions of algebraic equations of 5-th order, one of the founders of modern criterion for a rigorous proof in Mathematical Analysis.

Aristoteles (384-322 B.C.) – ancient Greek philosopher, encyclopedic scientist, a student of Plato and the teacher of Alexander the Great. His principal works were devoted to Logic and Geometry.

Bernstein, Felix (1878-1956) – German mathematician; his main studies were devoted to Number’s Theory, Theory of Sets and Mathematical Statistics.

Bolyai, János (1802-1860) – Hungarian mathematician. Created independently from N.I. Lobachevsky (and somewhat later than N.I. Lobachevsky) a Non-Euclidean Geometry.


Bourbaki, Nikolas – the collective pseudonym of the group of modern French mathematicians, publishing the treatise "Elements of Mathematics" in many volumes.

Cantor, Georg (1845-1918) – German mathematician, the creator of Set’s Theory.

Cauchy, Augustin Louis (1736-1857) – French mathematician, the creator of Complex Function’s Theory. He built Mathematical Analysis on the base of the notion of limit.

Cohen, Paul J. (born in 1934) – American mathematician, solved Continuum Problem.
**Desargues**, Gérard (1593-1662) – French mathematician, engineer and architect. He worked out the Projective and Descriptive Geometries.

**Decartes (Cartesius)**, René (1596-1650) – French mathematician and philosopher, creator of Analytic Geometry. He introduced the Coordinates Method and the notion of the variable.

**Diofant** (appr. 250 A.C.) – mathematician of the Hellenistic Period, one of the founder of Algebra. He lived and worked in Alexandria, being the last great mathematician of the ancient world.

**Dürer**, Albrecht (1471-1528) – German artist and graphic artist. As a theorist of Arts wrote "Four books about human proportions".

**Einstein**, Albert (1879-1955) – theoretical physicist, one of the founders of modern Physics. He created Special and General Relativity Theories. He wrote fundamental works on Quantum Theory of Light and Fluctuation Theory.

**Euclidean** (appr. 340 - appr. 287 B.C.) – mathematician of the Hellenistic Period. Probably, he was born and has lived in Alexandria. His famous work "Principles consisting of 13 books, was a mathematical textbook for nearly 2000 years. He was a founder of axiomatic approach in Mathematics.

**Euler**, Leonhard (1707-1783) – mathematician, physicist, mechanic and astronomer. Born in Switzerland he lived mostly in Russia. Scientific interests of Euler belonged to all the branches of Natural Science where the mathematical methods can be used (Mechanics, Hydrodynamics, Celestial Mechanics, Optics etc.).

**Faraday**, Michael (1791-1867) – English physicist, founder of Electromagnetic Field’s Theory. He discovered the electromagnetic induction, introduced the notions of the electric and magnetic fields.

**Galilei**, Galileo (1564-1642) – Italian mathematician, one of the founders of Exact Natural Science. He put forward the idea of the relativity of movements, established Inertia Law, Law of free fall and Law of movements’ composition. He also actively defended Heliocentric World System.

**Gauss**, Carl Friedrich (1777-1855) – German mathematician obtained a series of fundamental results in Algebra, Geometry, Numbers’ Theory, Mathematical Analysis, Electromagnetic Theory.
Gödel, Kurt (1906-1978) – Austrian mathematician and logician. He proved theorems on the impossibility of complete formalization of the process of the logic deduction, on the completeness and non-completeness of Predicate Calculus.

Hadamard, Jacques (1865-1963) – French mathematician, the author of outstanding works in Mathematical Physics, Theory of Functions and Number’s Theory.

Hermite, Charles (1822-1901) – French mathematician, the author of many investigations in Mathematical Analysis, Algebra, Number’s Theory.

Hilbert, David (1862-1943) – German mathematician, the author of fundamental works in Invariants Theory, Algebraic Geometry, Variational Calculus, Foundations of Mathematics, Functional Analysis. He introduced the notion of infinitely dimensional space. In 1900, during the second international mathematical congress in Paris, he formulated the 23 most important problems; their solution played a great role for the development of Mathematics of XX-th century.

Kepler, Johannes (1571-1630) – German astronomer, mathematician and mechanic. Founded Celestial Mechanics establishing Movements Laws for planets.

Klein, Felix Christian (1849-1925) – German mathematician. He gave a classification of Geometries’ types, developed Continuous Group Theory and Theories of elliptic and automorphic functions.

Kovalewsky, Sofia Vasil’evna (1850-1891) – Russian mathematician and mechanic. She studied the problem of the rotation of a solid body around a fixed point, proved the famous theorem on the solvability for systems of partial differential equations.


de Kulon, Charles Augustin (1736–1806) – French engineer and physicist, one of the founders of Electrostatic. He invented the turning balances and discovered the law, named after him.
Lavrent’ev, Michail Alexeevich (1900–1980) – Soviet mathematician and mechanic, one of the founder of the Siberian branch of Soviet Academy of Science, the author of the outstanding works on Function’s Theory, Theory of Quasiconformal Maps, Aero- and Hydrodynamics.

de Laplace, Piére Simon (1749–1827) – French mathematician, physicist and astronomer. He finished the creation of Celestial Mechanics on the base of the Gravitation Law by Newton. He introduced some integration methods for ordinary differential equations, proved binomial law of the probability distribution. He also was a minister of the interior affairs in France.

von Leibniz, Gottfried Wilhelm (1646–1716) – German mathematician and philosopher, one of the founder of Mathematical Analysis. He developed Differential and Integral Calculus. He worked on the project of Public Education in Russia with Russian Tsar Peter the Great.


Lindemann, Ferdinand (1852–1939) – German mathematician, proved that the number $\pi$ is transcendental.

Liouville, Joseph (1809–1882) – French mathematician, the author of works in Mathematical Analysis and Number’s Theory.

Lobachewsky, Nikolai Ivanovich (1792–1856) – Russian mathematician, created Non-Euclidean Geometry.

Maxwell, James Clerk (1831–1879) – English physicists, created Electrodynamics. He predicted the existence of electrodynamic waves, put forward the idea of electromagnetic nature of light.

Newton, Isaak (1643–1727) – English mathematician, physicist, founder of modern Mechanics. He discovered several fundamental laws of Physics, and, moreover, (simultaneously with G. Leibniz) he elaborated Differential and Integral Calculus, spread binomial formula on rational degrees and obtained interpolation formula.

Papp (2–nd part of III-rd century) – mathematician and mechanic of the late Hellenistic period, apparently lived in Alexandria.

Peano, Giuseppe (1858–1932) – Italian mathematician. He was engaged
with the studies of Differential Equation’s Theory and the formal logic base of Mathematics.

**Ptolemei**, Claudio (appr. 100–178 A.C.) – astronomer, mathematician and geographer of the Hellenistic Period, developed Geocentric World System. Born in Egypt he lived and worked in Alexandria.

**Poincaré**, Henri (1854–1912) – French mathematician, physicists and astronomer. He had outstanding works in all the branches of Mathematics.

**Russell**, Bertrand (1872–1970) – English logician, philosopher, mathematician and public figure. He was a founder of the trend in Mathematics trying to reduce it to Logic.

**Riemann**, Georg Friedrich Bernhard (1826–1866) – German mathematician. He created Riemannian Geometry and introduced rigorous definition of the integral. He also was a founder of Topology.

**Thales**, of Milet (624–548 B.C.) – Ancient Greek philosopher, mathematician and astronomer. He first introduced the notion of the proof into Mathematics. He also proved several geometric theorems.

**Weierstrass**, Carl Theodor Wilhelm (1817-1897) – German mathematician, one of the creators of Theory of Functions of Complex Variable. He constructed Theory of Real Numbers and (on its base) rebuilt Mathematical Analysis. He also proved that every continuous function can be approximated by polynomials.


**Weyl**, Hermann (1885-1955) – German mathematician, studied Group Theory, Mathematical Logic, Relativity Theory, Quantum Mechanics. He spared a lot of time to foundations of Philosophy of Mathematics representing Intuition trend in Mathematics.

**Wiener**, Norbert (1894-1964) – American scientists, the founder of Cybernetics. A series of his works was devoted to Functional Analysis and the study of finitely dimensional spaces where he introduced a probabilistic measure.
Zenon Eleat (appr. 490 - 430 B.C.) – ancient Greek mathematician, the author of *aporia* (seeming logic unsurmountable difficulties) related to the infinity, to the movement and to the naive notion of the continuity.

Subject Index

antisymmetry, 114
arrangement, 98
axiom of choice, 125
cardinality, 81
    continuum, 75
class, 58
combination, 91
complement, 42
composition, 54
conjunction, 20
    associativity, 26
    commutativity, 26
continuum conjecture, 86
continuum problem, 86
difference, 42
disjunction
    associativity, 26
    commutativity, 26
distributivity, 26
element fixed, 109
elements
    comparable, 115
equivalence, 20
Euler’s function, 106
hats problem, 109
image, 50
implication, 20
inclusion-exclusion principle, 106
intersection, 42
    associativity, 45
    commutativity, 45
isomorphism, 117
law
    contraposition, 26
de Morgan’s, 26, 45
double negation, 25
excluded middle, 26
non-contradiction, 26
of the propositional algebra, 25
map
    inverse, 53
    preserves the order, 117
mapping, 50
    bijective, 53
    injective, 52
    surjective, 52
negation, 20
number
    algebraic, 70
    ordinal, 119
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>transcendental</td>
<td>70</td>
</tr>
<tr>
<td>order</td>
<td></td>
</tr>
<tr>
<td>element</td>
<td>87</td>
</tr>
<tr>
<td>infinite</td>
<td>87</td>
</tr>
<tr>
<td>permutation</td>
<td>96</td>
</tr>
<tr>
<td>with repetitions</td>
<td>100</td>
</tr>
<tr>
<td>polynomial formula</td>
<td>102</td>
</tr>
<tr>
<td>preimage</td>
<td>50</td>
</tr>
<tr>
<td>full</td>
<td>50</td>
</tr>
<tr>
<td>Principle of Mathematical Induction</td>
<td>37</td>
</tr>
<tr>
<td>proof</td>
<td></td>
</tr>
<tr>
<td>direct</td>
<td>35</td>
</tr>
<tr>
<td>rule of contraries</td>
<td>35</td>
</tr>
<tr>
<td>proposition</td>
<td>22</td>
</tr>
<tr>
<td>indefinite</td>
<td>29</td>
</tr>
<tr>
<td>propositional Algebra</td>
<td>25</td>
</tr>
<tr>
<td>reflexivity</td>
<td>57, 114</td>
</tr>
<tr>
<td>relation</td>
<td></td>
</tr>
<tr>
<td>n–ary</td>
<td>56</td>
</tr>
<tr>
<td>binary</td>
<td>56</td>
</tr>
<tr>
<td>of partial order</td>
<td>114</td>
</tr>
<tr>
<td>of the equivalence</td>
<td>56</td>
</tr>
<tr>
<td>quaternary</td>
<td>56</td>
</tr>
<tr>
<td>ternary</td>
<td>56</td>
</tr>
<tr>
<td>set</td>
<td>40</td>
</tr>
<tr>
<td>continual</td>
<td>75</td>
</tr>
<tr>
<td>countable</td>
<td>65</td>
</tr>
<tr>
<td>empty</td>
<td>41</td>
</tr>
<tr>
<td>finite</td>
<td>64</td>
</tr>
<tr>
<td>infinite</td>
<td>64</td>
</tr>
<tr>
<td>ordered</td>
<td>116</td>
</tr>
<tr>
<td>partially ordered</td>
<td>114</td>
</tr>
<tr>
<td>well ordered</td>
<td>119</td>
</tr>
<tr>
<td>set’s algebra</td>
<td>42</td>
</tr>
<tr>
<td>sets</td>
<td></td>
</tr>
<tr>
<td>equal</td>
<td>41</td>
</tr>
<tr>
<td>equinumerous</td>
<td>61</td>
</tr>
<tr>
<td>equivalent</td>
<td>61</td>
</tr>
<tr>
<td>intersection</td>
<td>43</td>
</tr>
<tr>
<td>isomorphic</td>
<td>117</td>
</tr>
<tr>
<td>ordinal type</td>
<td>118</td>
</tr>
<tr>
<td>product</td>
<td></td>
</tr>
<tr>
<td>Cartesian</td>
<td>47</td>
</tr>
<tr>
<td>direct</td>
<td>47</td>
</tr>
<tr>
<td>union</td>
<td>43</td>
</tr>
<tr>
<td>simplifying of electrical schemes</td>
<td>27</td>
</tr>
<tr>
<td>subset</td>
<td>41</td>
</tr>
<tr>
<td>symmetry</td>
<td>57</td>
</tr>
<tr>
<td>theorem</td>
<td>34</td>
</tr>
<tr>
<td>assumption</td>
<td>35</td>
</tr>
<tr>
<td>conclusion</td>
<td>35</td>
</tr>
<tr>
<td>condition</td>
<td>35</td>
</tr>
<tr>
<td>necessary</td>
<td>35</td>
</tr>
<tr>
<td>sufficient</td>
<td>35</td>
</tr>
<tr>
<td>direct</td>
<td>34</td>
</tr>
<tr>
<td>inverse</td>
<td>34</td>
</tr>
<tr>
<td>reciprocal inverse</td>
<td>34</td>
</tr>
<tr>
<td>Zermelo</td>
<td>124</td>
</tr>
<tr>
<td>torus</td>
<td>48</td>
</tr>
<tr>
<td>transitivity</td>
<td>57, 114</td>
</tr>
</tbody>
</table>
truth tables, 22

union, 42
  associativity, 45
  commutativity, 45
Bibliography


