V. B. Alekseev

Abel's Theorem in Problems & Solutions.

Translated by Sujit Nair

January 30, 2005

Translator's notes

This book is the product of a genuine effort to translate the original Russian version. I have tried to retain the intended approach and flavor of arguments as much as possible. This project started in May 2003 when I came across an article titled ”On teaching mathematics” by V. I. Arnold. (an excellent read for anyone interested in ”beautiful mathematics”). I have reproduced the text in the end of this book and duly acknowledge the source of this article http://www.ceremade.dauphine.fr/˜msfr/arn_art.html. This book has the same spirit expressed in the article. The reader will see how definitions and concepts come out naturally from observations. For example, groups are first introduced as transformation groups and then by ignoring the set on which the transformation acts, the definition of a group follows naturally. When a group is introduced this way, the ”abstract definition” looks very obvious. The author has avoided as much as axiomatics as possible and stayed very close to physics and was able to teach Moscow *schoolchildren* Abel's theorem in half a year. In the process, complex numbers, Riemann surfaces were also taught.

The original book consists of 352 problems and their solutions. I have only translated the problems and left out the solutions mainly due to time constraints. Given the busy life in Princeton grad school, it is only now in January 2005 that the book is almost in a complete form. Please send any comments or suggestions to sujit.nair@gmail.com.

Princeton, NJ

Sujit Nair

Contents

1 **Introduction.** 7

2 **Groups** 13
- 2.1 Examples 13
- 2.2 Transformation groups 16
- 2.3 Groups 17
- 2.4 Groups 18
- 2.5 Cyclic groups 20
- 2.6 Isomorphism 21
- 2.7 Subgroups 21
- 2.8 Direct product 23
- 2.9 Cosets and Lagrange's theorem 23
- 2.10 Inner automorphism 24
- 2.11 Normal subgroups 26
- 2.12 Quotient groups 27
- 2.13 Commutator 28
- 2.14 Homomorphism 30
- 2.15 Solvable groups. 32
- 2.16 Permutations 34

3 **Complex numbers** 37
- 3.1 Fields and polynomials 37
- 3.2 The field of complex numbers 41
- 3.3 Uniqueness of the field of complex numbers 43
- 3.4 Geometric description of complex numbers 45
- 3.5 Trigonometric form of complex numbers 46
- 3.6 Continuity 48
- 3.7 Continuous curves 50
- 3.8 Images of curves: the fundamental theorem of the algebra of complex numbers 55
- 3.9 Riemann surface of the function $w = \sqrt{z}$ 57
- 3.10 Riemann surfaces of more complicated functions 62
- 3.11 Functions expressible by radicals 67
- 3.12 Galois group of many-valued functions 71
- 3.13 Galois group of functions which are expressible in radicals 73
- 3.14 Abel's theorem 74

On teaching mathematics 77

Index 83

Preface

In high school syllabus algebraic equations of first (linear) and second degree (quadratic) with one unknown are studied in detail. In this case, for solving such equations, it happens that there are general formulas which expresses the roots of the equation in terms of its coefficients using arithmetic operations and radicals. But very few students know whether there exists similar formulas for solving algebraic equations of higher degree. In fact, such formulas also exist for equations of 3rd and 4th degree. We shall illustrate methods of solving these equations in the introduction. But if we consider the most general algebraic equation with one unknown of degree greater than four, it occurs that it is not solvable in radicals, i.e. there exists no formulas which expresses the roots of this equation in terms of the coefficients using arithmetic operations and radicals. This is the statement of Abel's theorem.

One of the aims of this book is to introduce to the reader a proof of Abel's theorem. We will not examine in details the results obtained a bit later by the French mathematician Evariste Galois. He considered not general, but specific algebraic equations with fixed coefficients and for these equations found conditions under which the roots are expressible in terms of coefficients using arithmetic operations and radicals. Those who want to learn the results of Galois in depth, we recommend the book by Postnikov on Galois theory[1].

From the general results of Galois it is possible, in particular, to obtain Abel's theorem. However, in this book we will proceed in a different direction: this will introduce the reader to two very important branches of contemporary mathematics, group theory and the theory of functions of one complex variable. The reader will learn about groups (in mathematics), fields and various properties they possess. S/He (translator's non-sexist note) will also learn what complex numbers are and why they are so defined and not otherwise. S/He (translator's non-sexist note) will learn Riemann surfaces and contents of the "fundamental theorem of complex number algebra".

The author will help the reader along the way, but will give the reader the possibility to test its own talents. For this purpose a large number of problems are proposed. Problems are posed directly within the text of the book and are actually the essential part of the book. The problems are labelled by increasing numbers in medium boldface type. Whenever some problems prove to be too difficult for the reader, the chapter "Hint, Solutions and Answers" will turn out helpful.

The book contains many concepts whicy may be new to the reader. To help the reader search these new concepts, an alphabetical list of concepts indicating the page numbers where they are defined is given at the end of the book.

The book is based on the lectures given by professor Vladimir Igorevich Arnold of Moscow University and by the author in the Moscow physics-mathematics 18th boarding school in different years. The author is grateful to V. I. Arnold who made a number of valuable observations during the preparation of the

[1] Postnikov M. M., Boron L.F., Galois E., Fundamentals of Galois theory, Nordhoff: Groningen, 1962

manuscript of this book. I also thank Aleksander Vasilyevich Mikhaleva who took the large labor of editing this book and also in many ways that contributed to its improvement.

V. B. Alekseev

Moscow, Russia *V. B. Alekseev*

1

Introduction.

We will begin this book with the study of the problem of solving algebraic equations with one unknown from the first to the fourth degree. Methods of solving algebraic equations of first and second degree were known to ancient mathematicians, but the methods of solving an algebraic equations of third and fourth degree were developed only in the XVI century. The equation of the form

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

where $a_0 \neq 0$,[1] is called the general algebraic equation in one unknown of degree n.

With $n = 1$ we obtain the linear equation

$$a_0x + a_1 = 0, \quad a_0 \neq 0$$

This equation has, obviously, the unique solution

$$x = -\frac{a_1}{a_0}$$

for any value of the coefficients.

With $n = 2$ we obtain the quadratic equation

$$ax^2 + bx + c = 0, \quad a \neq 0$$

(instead of a_0, a_1, a_2 we write a, b, c as learnt in school). After dividing both sides of this equation by a and substituting $p = \dfrac{b}{a}, q = \dfrac{c}{a}$ we get the following quadratic equation

$$x^2 + px + q = 0. \tag{1.1}$$

After some algebra, we obtain

$$x^2 + px + \frac{p^2}{4} = \frac{p^2}{4} - q \text{ and } \left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q \tag{1.2}$$

In high school only the case $\dfrac{p^2}{4} - 1 \geq 0$ is considered. If $\dfrac{p^2}{4} - q < 0$, then it is said that equality (1.2) cannot take place and equation (1.1) does not have any real roots.

To avoid such exceptions, henceforth, it will be more convenient for us to examine algebraic equations not in the domain of real numbers, but in the larger domain of complex numbers.

We will examine complex numbers in greater detail (together with the definition) in chapter II. So far it is sufficient for the reader to know, or to accept as true, the following assertions about complex numbers:

[1] Coefficients $a_0, a_1, ...a_n$ are considered to be real numbers

1. The set of complex numbers is an extension of the set of real numbers, i.e. real numbers are contained in the complex numbers, just as, for example, integers are contained in the real numbers;
2. Complex numbers can be added, subtracted, multiplied, divided, raised to a natural power - all the operations possessing all the basic properties of the corresponding operations on the real numbers;
3. If z is a complex number, not equal to zero, and n a natural number then there exists exactly n roots of z, i.e. n complex numbers w such that, that $w^n = z$. With z=0 we have $\sqrt[n]{0} = 0$. If w_1 and w_2 are the squareroots of 1 then $w_2 = -w_1$.

   In the following, we shall not only be interested in both the real and complex roots of equations, but will also examine these equations with arbitrary complex numbers as coefficients. In this case, the previous arguments about linear and quadratic equations will remain true, which follows from the above-indicated property (2) of complex numbers.

   Let us continue to study the quadratic equation. In the field of complex numbers, equality (2) with any values p and q is equivalent to

$$x + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q}$$

where by $\sqrt{\frac{p^2}{4} - q}$ is understood any one of the two values of square root.

Thus we have for future references

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \text{ i.e., in old notation} \tag{1.3}$$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1.4}$$

Theorem 1.1 (Theorem of Francois Viète) [2]*: The complex numbers x_1 and x_2 are the only roots of equation $x^2 + px + q = 0$, if and only if $x_1 + x_2 = -p, \;\; x_1x_2 = q$.*

Indeed, if x_1 and x_2 are the roots of $x^2 + px + q = 0$, then equality (1.3) holds. Hence $x_1 + x_2 = -p, x_1x_2 = q$. Conversely, if $x_1 + x_2 = -p, x_1x_2 = q$, then, by substituting p and q in the equation $x^2 + px + q = 0$ by their expressions in terms of x_1 and x_2, we will obtain $x^2 - (x_1 + x_2)x + x_1x_2 = (x - x_1)(x - x_2) = 0$, and therefore x_1 and x_2 are the roots of equation $x^2 + px + q = 0$;

The quadratic polynomial $ax^2 + bx + c$ is a perfect square (i.e. $ax^2 + bx + c = [\sqrt{a(x - x_0)}]^2$ for a certain complex number x_0) $\iff$ the roots of equation $ax^2 + bx + c = 0$ coincide (both of them must be equal to x_0). This occurs only in the case (see formula (1.4)) $b^2 - 4ac = 0$. Expression $b^2 - 4ac$ is called the discriminant of quadratic polynomial.

Let us examine now the following equation of third degree.

$$x^3 + ax^2 + bx + c = 0 \tag{1.5}$$

(a general equation of 3rd degree is reduced to that given above on division by a_0.) Let us make $x = y + d$, where we will chose d later.

We obtain

$$(y + d)^3 + a(y + d)^2 + b(y + d) + c = 0$$

Expanding all brackets and after collecting terms of same degree in y, we obtain the equation

$$y^3 + (3d + a)y^2 + (3d^2 + 2ad + b)y + (d^3 + ad^2 + bd + c) = 0$$

[2] Francois Viète (1540-1603) was a French mathematician.

The coefficient of y^2 in this equation is equal to $3d+a$. Therefore if we put $d = -\frac{a}{3}$, then after replacing x by $y - \frac{a}{3}$ we will get the equation:

$$y^3 + py + q \tag{1.6}$$

where p and q are polynomials in a, b, c.
Let y_0 be a root of equation (1.6). After writing it in the form $y_0 = \alpha + \beta$, (where α and also β are as of now unknown), we obtain

$$\alpha^3 + 3\alpha\beta(\alpha+\beta) + \beta^3 + p(\alpha+\beta) + q = 0$$

and

$$\alpha^3 + \beta^3 + (\alpha+\beta)(3\alpha\beta + p) + q = 0 \tag{1.7}$$

Let us see, if it is possible to choose α and β satisfying

$$\alpha\beta = -\frac{p}{3}$$

In this case we will obtain two equations for α and β

$$\alpha + \beta = y_0; \quad \alpha\beta = -\frac{p}{3}$$

By Vièta's theorem, for any y_0 such α and β indeed exists (possibly complex) and they are the roots of the equation

$$w^2 - y_o w - \frac{p}{3} = 0$$

.
If we take such α and β (still unknowns), then equation (1.7) will take the form

$$\alpha^3 + \beta^3 + q = 0 \tag{1.8}$$

Raising both parts of the equation of $\alpha\beta = -\frac{p}{3}$ to the third power, and comparing the obtained equation with (1.8), we will have

$$\alpha^3 + \beta^3 = -q; \quad \alpha^3\beta^3 = -\frac{p^3}{27}$$

By Vièta's theorem, α^3 and β^3 are the roots of the equation

$$w^2 + qw - \frac{p}{27} = 0$$

Thus we get,

$$\alpha^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and

$$\beta^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

where again $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ indicates one specific value of the square root. Hence the roots of equation (1.6) are expressed by the formula

$$y_{1,2,3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Moreover for each of three values of the first cubic root, [3] one must take the appropriate value of the second so that the condition $\alpha\beta = -\frac{p}{3}$ is satisfied.

The formula obtained is called Cardano's solution [4]. After substituting for p and q, their expression in terms of a, b, c and subtracting $\frac{a}{3}$, we will obtain a formula for the roots of equation (1.5). After the transformations $a = \frac{a_1}{a_0}, b = \frac{a_2}{a_o}, c = \frac{a_3}{a_0}$, we will obtain a formula for the roots of the most general equation of third degree.

Let us examine now the following given equation of fourth degree

$$x^4 + ax^3 + bx^2 + cx + d = 0 \tag{1.9}$$

(a general equation is reduced to this by dividing by a_0). After making the substitution $x = y - \frac{a}{4}$, similar to the one made in the case of equation of third degree, let us modify equation (1.9) to the form

$$y^4 + py^2 + qy + r = 0 \tag{1.10}$$

where p, q and r are polynomials in a, b, c, d.

We will solve equation (1.10) by a method called Ferrari's method [5]. We transform the left side of equation (1.10) as follows:

$$\left(y^2 + \frac{p}{2}\right)^2 + qy + \left(r - \frac{p^2}{4}\right) = 0$$

and

$$\left(y^2 + \frac{p}{2} + \alpha\right)^2 - \left[2\alpha\left(y^2 + \frac{p}{2}\right) + \alpha^2 - qy + \frac{p^2}{4} - r\right] = 0 \tag{1.11}$$

where α is an arbitrary number. Let us now try to chose α so that the polynomial of degree two in y

$$2\alpha y^2 - qy + \left(\alpha p + \alpha^2 + \frac{p^2}{4} - r\right)$$

in the square brackets become a perfect square. As was noted above, it is necessary and sufficient that the discriminant of this polynomial be equal to zero for it to be a perfect square, i.e.

$$q^2 - 8\alpha\left(\alpha p + \alpha^2 + \frac{p^2}{4} - r\right) = 0 \tag{1.12}$$

Removing the parentheses, we will obtain for α an equation of third degree, which we know how to solve. If α is taken to be one of the roots of equation (1.12), the expression in the square brackets in (1.11) will be a perfect square. In this case the left side of equation (1.11) is a difference of squares and therefore it can be decomposed into the product of two polynomials of degree two in y. After this, it remains to solve the two equations of degree two obtained.

Thus, equation of fourth degree can always be solved. Moreover, as in the case of third degree, it is possible to obtain a formula which expresses the roots of general equation of fourth degree in terms

[3] See the above-indicated property 3) of the complex numbers

[4] G. Cardano (1501-1576) was an Italian mathematician

[5] L. Ferrari (1522-1565) was an Italian mathematician and a student of the Cardano

of the coefficients of equation using the operations of addition, subtraction, multiplication, division, raising to a natural power and the extracting a root of natural degree.
For a long time mathematics attempted to find a method of solution by radicals of a general equation of fifth power. However, in 1824 the Norwegian mathematician Niels Henrik Abel (1802 - 1829) proved the following theorem.

Theorem 1.2 (Abel's theorem) *The general algebraic equation with one unknown of degree greater than 4 is insoluble in radicals, i.e. there do not exist a formula, which expresses the roots of a general equation of degree greater than four in terms of the coefficients involving the operations of addition, subtraction, multiplication, division, raising to a natural degree and extraction of roots of natural degree.*

We will be able to prove this theorem at the end of the book. However, we will require mathematical concepts such as group, soluble group, functions of complex variable, Riemann surface, etc. We will introduce the reader to all these and other mathematical concepts in the following pages of this book. We will begin examining the notion of a group: a very important concept in mathematics.

2

Groups

The study of algebraic equations in the beginning of the XIX century lead mathematicians to the need for a special mathematical notion: the concept of a group. This new concept proved to be fruitful and penetrated not only almost all divisions of contemporary mathematics, but also began to play an important role in some divisions of other sciences, for example in quantum mechanics and in crystallography. The studies connected with the concept of a group grew into a separate branch of contemporary mathematics known as the theory of groups. What is a group in mathematics? In order to answer this question, let us begin by examining some examples.

2.1 Examples

In arithmetic we have already encountered operations, which to two given numbers in a set associates a third number. The operation of addition puts the pair of numbers (3, 5) in correspondence with the number 8 and to the pair (2, 2) the number 4. The operation of subtraction if considered on the set of all integers also associates to each pair of integers a specific integer. In this case it is necessary to indicate not only the pair of numbers, but also the order of these numbers. So, to the pair (5, 3) subtraction assigns the number 2 and to the pair (3, 5) the number -2. Thus, pairs (5, 3) and (3, 5) must be considered as different.
We will call pairs of elements to which an order is assigned ordered pairs.

Definition 1 *Let M be a certain set of elements of arbitrary nature. If to the ordered pair of elements from M is assigned a specific element also belonging to M, then it is said that a binary operation is defined on M.*

Binary operations are, for example, addition on the set of natural or on the set of integers, subtraction on the set of integers. Subtraction on the set of natural numbers is not a binary operation, since, for example, subtraction assigns to the ordered pair (3, 5) no natural number.
Problem-1 On the sets: 1) all even natural numbers, 2) all odd natural numbers, 3) all negative integers you will examine the operations: a) addition, b) subtraction, c) multiplication. In what cases will it turn out to be a binary operation? [1]
Let us examine some more examples of binary operations. We will frequently encounter such examples in the following pages.

[1] Part of the problems in the sequel has a practical nature and serves for a better understanding of new concepts by examples. Other tasks are theoretical and their results are used later on. Therefore if the reader is unable to solve some problems, then she/he must become acquainted with its solution in the Hints, Solutions and Answers section.

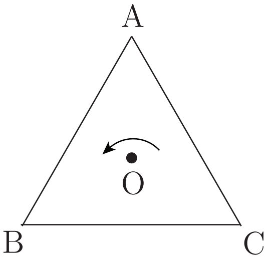


Fig. 2.1.

Example-1 Let A, B and C be the vertices of equilateral triangle ABC (Fig. 2.1). Let us rotate the triangle around its center O by 120° in the direction indicated by the arrow. Then vertex A goes to the vertex B, B to C and C to A. Thus, the triangle will return to its initial position (if we neglect the name of vertices), i.e. rotating by 120° around the point O is a transformation which takes this triangle into itself. Let us denote this transformation by $\tilde{a}$. It is possible to write it down in the form

$$\tilde{a} = \begin{pmatrix} ABC \\ BCA \end{pmatrix}$$

where in the upper line all the vertices of the triangle are enumerated and the lower line shows where each of them goes to. Rotation by 240° in the same direction around the point O is also a transformation which takes the triangle into itself. Let us denote this transformation by $\tilde{b}$. Then $\tilde{b} = \begin{pmatrix} ABC \\ CAB \end{pmatrix}$. There is one additional rotation which takes the triangle into itself different from $\tilde{a}$ and $\tilde{b}$ which is a rotation by 0°. Let us denote this conversion by $\tilde{e}$. Then $\tilde{e} = \begin{pmatrix} ABC \\ ABC \end{pmatrix}$ It is easy to see that there are only 3 different rotations of the plane [2], taking the equilateral triangle ABC into itself, namely $\tilde{a}, \tilde{b}$ and $\tilde{e}$.

Let g_1 and g_2 be two arbitrary transformations of the triangle. Then we denote by $g_1 \cdot g_2$ (or simply $g_1 g_2$) the transformation g_3 which will result if we first carry out transformation g_2 and then transformation g_1. We will call g_3 the product or composition of transformations g_2 and g_1.

Table 2.1.

	e	a	b
e			
a			e
b			

It is possible to compile a multiplication table (Table 1) where each row and each column corresponds to a certain rotation which takes the triangle ABC into itself. At the intersection of the row which corresponds to transformation g_1 and the column which corresponds to transformation g_2 we will place the transformation equal to $g_1 \cdot g_2$. Thus, for instance, in the chosen cell in table 1 we must

[2] i.e. rotation only around some axes perpendicular to the plane.

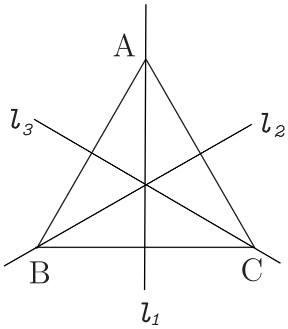


Fig. 2.2.

place the transformation $\tilde{a}\cdot\tilde{b}$ which will result if we first turn the triangle by 240° and then by another 120°. Consequently, $\tilde{a}\cdot\tilde{b}$ is a rotation by 360 degress i.e. coincides with $\tilde{e}$. We will obtain the same result if we reason as follows: transformation $\tilde{b}$ takes the vertex A to C, while transformation $\tilde{a}$ takes the vertex C to A . This means, transformation $\tilde{a}\cdot\tilde{b}$ will take the vertex A to A. In exactly the same manner it is possible to see that the vertex B goes to B, and C goes to C. Therefore, $\tilde{a}\cdot\tilde{b} = \begin{pmatrix} ABC \\ ABC \end{pmatrix}$, i.e., $\tilde{a}\tilde{b} = \tilde{e}$.

Problem-2 Fill the table completely.

Any transformation of a certain geometrical figure into itself that preserves the distances between all its points is called a symmetry of this figure. Thus, the rotations of the equilateral triangle examined in example 1 are its symmetries.

Example-2 Besides rotations, the equilateral triangle has three additional symmetries, namely, reflection relative to axes l_1, l_2 and l_3 (Fig. 2.2). We will denote these transformations by c, d, f, so that $c = \begin{pmatrix} ABC \\ ACB \end{pmatrix}, d = \begin{pmatrix} ABC \\ CBA \end{pmatrix}, f = \begin{pmatrix} ABC \\ BAC \end{pmatrix}$. Here, it is possible to understand in a different way the composition of two transformations. Let us examine for example, the composition of transformations $c \cdot d$. It is possible to see that after the transformation d, axis l_1 goes to the new position (namely to the position of the old axis l_3) and after this transformation to consider the reflection relative to the new position of axis l_1 (i.e. relative to the old axis l_3) - On the other hand, it is possible to consider that the axes are not connected rigidly with the figure and do not move with it; therefore, in the example, after the transformation d in question, transformation must be carried out as reflection relative to the old axis l_1. We will consider the composition of transformations this way. With this approach the arguments about the vertices of the figures, analogous to the reasonings given directly before problem two hold true. Such reasonings are conveniently used to calculate the multiplication table.

Problem-3 To compile multiplication table for all the symmetries of the equilateral triangle.

Example-3 Let e, a, b and c denote the rotations of a square by $0°, 180°, 90°$ and $270°$in the direction indicated by the arrow (Fig. 2.3).

Problem-4 To compile the multiplication table for the rotations of the square.

Example-4 Let d, f, g and h designate the reflections of square relative to the axes shown in (Fig. 2.4)

Problem-5 To compile the multiplication table for all the symmetries of the square.

Example-5 Let ABCD be a rhombus which is not square.

Problem-6 Find all symmetries of the rhombus and to write the multiplication table for it.

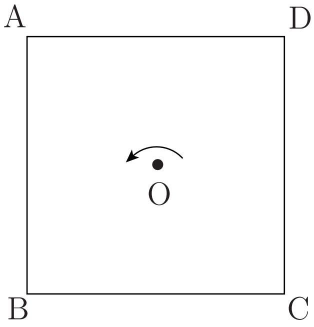


Fig. 2.3.

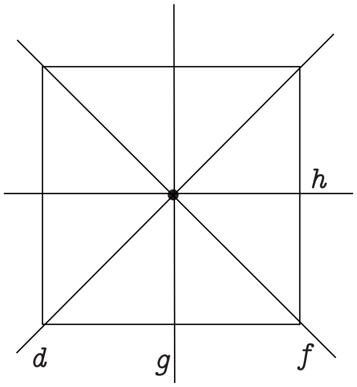


Fig. 2.4.

Example-6 Let ABCD be a rectangle which is not square.
Problem-7 Find all the symmetries of this rectangle and write the multiplication table.

2.2 Transformation groups

Let X and Y be two sets of elements of arbitrary nature and let to each element $x \in X$ be assigned unambiguously a specific element $y \in Y$. Then it is said that a certain mapping φ of set X into the set Y ($\varphi : X- > Y$) is defined. Element y is called the image of element x and x the pre-image of element y and is written as $\varphi(x) = y$.

Definition 2 *Mapping $\varphi : X \to Y$ is called a surjective mapping from set X to the set Y, if for each element $y \in Y$ there exists an element $x \in X$ such that $\varphi(x) = y$ i.e. for each $y \in Y$ there exists a pre-image in X.*

Problem-8 Let the mapping φ assign to each city of Soviet Union the first letter from its name in the Russian language (for example, φ(Moscow)=M). Will φ map all cities of the Soviet Union onto the entire Russian alphabet?

Definition 3 *Mapping $\varphi : X \to Y$ is called a one-to-one (or bijective) mapping of the set X onto the set Y, if for each $y \in Y$ there exists a unique pre-image in X.*

Problem-9 Let us examine following mappings from the set of all integers into the set of all non-negative integers:

$$a)\ \varphi(n) = n^2 \quad b)\ \varphi(n) = |n|$$
$$c)\ \varphi(n) = \begin{cases} 2n & \text{if } n \geq 0, \\ 2|n| - 1 & \text{if } n < 0. \end{cases}$$

Which of these mappings are surjective, which are bijective ?

Definition 4 *Let M be an arbitrary set. We will call an arbitrary one-to-one mapping of set M onto itself $g : M \to M$ a transformation of the set M.*

Two transformations g_1 and g_2 will be considered equal if $g_1(A) = g_2(A)$ for every element $A \in M$. Instead of the term transformation, the term permutation is used often. We will use this term only when the transformation is defined on a finite set. A permutation can thus be written down in the form

$$\begin{pmatrix} A_1, A_2, \ldots, A_n \\ A_{i_1}, A_{i_2}, \ldots, A_{i_n} \end{pmatrix}$$

where in the upper row contains all the elements of this set and the lower row indicates where each of these their elements maps to.

Since this transformation is a one-to-one mapping, for each transformation g there exists an inverse transformation g^{-1}, which is determined as follows: if $g(A) = B$, then $g^{-1}B = A$. Then, in example 1, $a = \begin{pmatrix} ABC \\ BCA \end{pmatrix}$, therefore $a^{-1} = \begin{pmatrix} ABC \\ CAB \end{pmatrix}$, i.e., $a^{-1} = b$.

Problem-10 Find the inverse transformations to all symmetries of equilateral triangle (examples 1, 2, p. 13).

Problem-11 Let $g(x) = 2x$ be a transformation of the real line. Find the inverse transformation.

The multiplication of transformations g_1 and g_2 is defined as follows: $(g_1g_2)(A) = g_1(g_2(A))$ (first by g_2 and then by g_1). If g_1 and g_2 are transformations of a set M, then g_1g_2 is also a transformation of M.

Definition 5 *Suppose the collection G of all transformations possess the following properties:1) if the transformations g_1 and g_2 belong to G, then their composition $g_3 = g_1g_2$ also belongs to G;2) if a transformation g belongs to G, then its inverse g^{-1} also belongs to G. Then this collection of transformations G will be called a transformation group. It is not difficult to verify that the set of transformations considered in examples 1-6 are transformation groups.*

Problem-12 Prove that any transformation group contains an identity transformation e such that $e(A) = A$ for any element $A \in M$.

Problem-13 Prove that $eg = ge = g$ for any transformation g.

Problem-14 Prove that for any three transformation g_1, g_2, g_3 the following equality holds

$$(g_1g_2)g_3 = g_1(g_2g_3)^3$$

2.3 Groups

To solve problems 6 and 7 we compiled the multiplication tables for the symmetries of the rhombus and the rectangle. In this case it turned out that in our notation for the symmetries (see the solutions) these tables coincide. For many purposes it is natural to consider such transformation groups as the same. Therefore we will ignore the nature of the elements of the set (in our case, of transformations) and the nature of the binary operation [4]) (in our case, the composition of transformations). We will simply consider only those binary operations on arbitrary sets for which the basic properties of a transformation groups holds true. In this case we will call the arbitrary binary operation a multiplication; and if to the pair (a, b) there corresponds the element c, then we will call c the roduct of a and b and write $ab = c$. In some special cases this operation will be called differently, for example, composition, addition and so forth.

Definition 6 *A group is a set G of elements of an arbitrary nature, on which a binary operation $a \cdot b$ is defined, such that the following conditions are satisfied:*

[3] This equality is true not only for transformations, but also for any three mappings g_1, g_2, g_3 such that $g_3 : M_1 \to M_2, g_2 : M_2 \to M_3, g_1 : M_3 \to M_4$

[4] See page 13 for the definitaion of a binary operation.

Problem-15 Prove that any transformation group contains an identity transformation e such that $e(A) = A$ for any element $A \in M$.
Problem-16 Prove that $eg = ge = g$ for any transformation g.
Problem-17 Prove that for any three transformation g_1, g_2, g_3 the following equality holds

$$(g_1 g_2) g_3 = g_1 (g_2 g_3)^5$$

2.4 Groups

To solve problems 6 and 7 we compiled the multiplication tables for the symmetries of the rhombus and the rectangle. In this case it turned out that in our notation for the symmetries (see the solutions) these tables coincide. For many purposes it is natural to consider such transformation groups as the same. Therefore we will ignore the nature of the elements of the set (in our case, of transformations) and the nature of the binary operation [6]) (in our case, the composition of transformations). We will simply consider only those binary operations on arbitrary sets for which the basic properties of a transformation groups holds true. In this case we will call the arbitrary binary operation a multiplication; and if to the pair (a, b) there corresponds the element c, then we will call c the roduct of a and b and write $ab = c$. In some special cases this operation will be called differently, for example, composition, addition and so forth.

a) associativity: $(ab)c = a(bc)$ for any elements a, b, c from G
b) in G there exists an element e, such that $ea = ae = a$ for any element $a \in G$; this element e is called the identity element (or neutral element or unit element) of the group G;
c) for any element $a \in G$ there is this element $a^{-1} \in G$, such that $aa^{-1} = a^{-1}a = e$; this element is called the inverse of a.

From the results of problems 12-14 we see that any transformation group is a group (in some sense the converse is also true (see 55)). Thus, we already have several examples of groups. All these groups contain finite number of elements and such groups are called finite groups. The number of elements in a finite group is called the order of group. The groups, which contain an infinite number of elements are called infinite groups.
Let us consider some examples of infinite groups.
Example-7 Let us consider the set of all integers. The binary operation on this set will be the usual addition. Then we obtain a group. Indeed, the role of the identity element in this case is played by 0, since $0+n = n+0 = n$ for any integer n. Furthermore, for each n there exists the inverse element $-n$ (which is in this case called the negative of n), since $n + (-n) = (-n) + n = 0$. Associative property in this case follows from the rules of arithmetic. The group obtained is called the group of integers under addition.
Problem-18 Do the following sets form a group under multiplication: 1) all real numbers, 2) all real numbers without O?
Problem-19 Do all positive real numbers form a group under multiplication ?
Problem-20 Do natural numbers form a group :a) under addition, b) under multiplication?
Problem-21 Prove that any group has a unique identity element.
Problem-22 Prove that for any element a in a group there is a unique inverse element a^{-1}.
Problem-23 Prove that a)$e^{-1} = e$, b)$(a^{-1})^{-1} = a$.
If a and b are elements of a certain group, then by the definition of binary operation, the expression given by $a{\cdot}b$ is also an element of the group. Therefore expressions of the form $(a{\cdot}b){\cdot}c$, $a{\cdot}(b{\cdot}c)$, $(a{\cdot}b){\cdot}(c{\cdot}d)$

[5] This equality is true not only for transformations, but also for any three mappings g_1, g_2, g_3 such that $g_3 : M_1 \to M_2, g_2 : M_2 \to M_3, g_1 : M_3 \to M_4$

[6] See page 13 for the definitaion of a binary operation.

are also elements of the group. Any two of these elements can again be multiplied with another element of the group and so on. We will put in brackets the two elements which are to be multiplied at each step. In this way, at each step, there is a unique way to perform the next step (we may choose not to enclose a single letter in brackets). Let us call all possible expressions which can be built this way correctly arranged products. For example, $(a \cdot b) \cdot (a \cdot (a \cdot c))$ is a correctly arranged product but $(a \cdot b) \cdot c \cdot (c \cdot d)$ is not a correctly arranged product since it is not clear in what order the multiplication is performed. In the product $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ of several real numbers $a_1, a_2, \ldots, a_n$ we have not placed brackets since it happens that the result does not depend on the order in which the operations are performed i.e., any arrangement of brackets which gives correctly arranged products, the result corresponding to this product will be the same. It turns out that this property holds in any group, as follows from the result of the following problem.

Problem-24 Let the binary operation $a \cdot b$ have the associativity property, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any elements a, b, c. Prove that any correctly arranged product, in which the elements from left to right are $a_1, a_2, \ldots a_n$ gives the same element as the product $(\ldots((a_1 \cdot a_2) \cdot a_3) \cdot \ldots \cdot a_{n-1}) \cdot a_n$.

Thus, if $a_1, a_2, \ldots a_n$ are elements of a certain group, then all correctly arranged products containing $a_1, a_2, \ldots a_n$ in this order and differing only by the arrangement of brackets gives one and the same element which we will denote by $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ (without indicating brackets).

The multiplication of real numbers has one additional very important property: the product $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ will not change if we arbitrarily swap two factors. However, this property does not hold true in an arbitrary group.

Definition 7 *Two elements a and b of a group are called adjustable or or commutating, if $ab = ba$. If any two elements of a group commutate, then this group is called a commutative or abelian.*

There exists non-commutative groups. For example, the symmetry group of triangle (see example 2, where the $ac = f, ca = d$ and $ac \neq ca$) is non-commutative.

Problem-25 To explain whether the following groups are commutative (see 2, 4 -7): 1) the rotation group of the triangle, 2) the rotation group of the square, 3) the symmetry group of the square, 4) the symmetry group of the rhombus, 5) the symmetry group of the rectangle.

Problem-26 Prove that in an arbitrary group: $1)(ab)^{-1} = b^{-1}a^{-1}, 2)(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1}$.

Observation. A jacket is put on after the shirt, but taken off before it.

If there is certain identity $a = b$ in an arbitrary group G (the left and right expression giving the same element), then its possible to obtain a new identity by multiplying both sides of the initial identity by a certain element from the group G. However, since multiplication in a group may depend on the order of its factors, one can multiply both sides of the identity by a certain element to the right:$ac = bc$, or multiply both sides by a certain element to the left:$ca = cb$.

Problem-27 Let a and b be arbitrary elements of a certain group G. Show that, each of the equations $ax = b$ and $ya = b$ has an unique solution in the group G.

The uniqueness condition from problem 24 can be stated as follows: if $ab_1 = ab_2$ or $b_1a = b_2a$, then $b_1 = b_2$

Problem-28 Let $a \cdot a = e$ for any element a of a group G. Show that the group G is commutative.

By a^m, where m is a natural number and a an arbitrary element of group G, we will denote the product $a \cdot a \cdot \ldots \cdot a$ where the number of factors is equal to m.

Problem-29 Prove that $(a^m)^{-1} = (a^{-1})^m$ where m is a natural number. Thus, $(a^m)^{-1}$ and $(a^{-1})^m$ with m a natural number indicates one and the same element, which we will denote by a^{-m}. Furthermore, we will assume for any element a, $a^0 = e$

Problem-30 Prove that $a^m \cdot a^n = a^{m+n}$ for any integers m and n.

Problem-31 Prove that $(a^m)^n = a^{mn}$ for any integers m and n.

2.5 Cyclic groups

The simplest and at the same time very important groups are the cyclic groups, which we will now study.

Definition 8 *Let a be an element of a certain group G. If there exists a natural number n such that $a^n = e$, then n is called the order of the element a. If such a n does not exist, then it is said that element a has infinite order.*

Problem-32 Find the order of all elements in the symmetry groups of the equilateral triangle, the square and rhombus (see 3, 5, 6).
Problem-33 Let the element a be of order n. Prove that: 1) elements $e, a, a^2, \dots, a^{n-1}$ all are different; 2) for any integer m, the element a^m coincides with one of the elements listed above.

Definition 9 *If an element a has order n and there are no elements besides $e, a, a^2, \dots a^{n-1}$ in the group G, then G is called a cyclic group of order n generated by the element a and element a is called a generator of this group*

Example-8 Let a regular n-polygon be given on the plane. Let us examine all the rotations of the plane which takes the regular n-polygon into itself.
Problem-34 Prove that these rotations form a cyclic group of order n.
Problem-35 Find all the generators in the rotation groups of the triangle and the square (examples 1 and 3, page ?? and ??).
Problem-36 Let the element a have order n. Prove that $a^m = e \iff m = nd$, where d is an arbitrary integer.
Problem-37 Let a have prime order p and m an arbitrary integer. Prove that either $a^m = e$ or a^m has order p. .
Problem-38 Let the greatest common divisor of the natural numbers m and n be equal to d and a have order n. Prove that the order of element a^m is $\dfrac{n}{d}$.
Problem-39 Find all the generators in the rotation group of a regular 12 sided polygon.
Problem-40 Let a be an element of infinite order. Prove that the elements $\dots a^{-1}, a^0, a, a^2, \dots$ are all different

Definition 10 *If a is an element of infinite order and the group G has no elements other than $\dots a^{-2}, a^{-1}, e, a, a^2, \dots$, then G is called an infinite cyclic group and a its generator.*

Problem-41 Prove that the group of integers under addition (example 7, p. 18) is an infinite cyclic group. Find all generators. *Example-9* Let n be a natural number. Consider all possible remainders, which can be obtained by dividing integers by n, i.e., the numbers $0, 1, 2, \dots, n-1$. Let us define on these remainders the following binary operation. We will add remainders as usual, but for the result take the remainder from the division of the obtained number by n. We will call this operation addition modulo n. Thus, under addition modulo 4, we have $1 + 2 = 3$ and $3 + 3 = 2$.
Problem-42 To compile the tables of addition modulo: a) 2, b) 3, c) 4.
Problem-43 Prove that the remainders with the operation of addition modulo n form a group; moreover this group is cyclic of order n.
Consider again an arbitrary cyclic group of order n: $\{e, a, a^2, \dots a^{n-1}\}$.
Problem-44 Prove that $a^m \cdot a^r = a^k$ where $0 \leq m < n, 0 \leq r < n$ and $0 \leq k < n \iff$ under addition modulo n we have $m + r = k$.
It follows that from the result of the previous problems, it follows that the multiplication in an arbitrary cyclic group of order n corresponds to the addition of remainders modulo n. In exactly the same manner, multiplication of elements in an infinite cyclic group corresponds to the addition of integers (see 27). Here we have arrived at an important concept in group theory: the concept of an isomorphism.

2.6 Isomorphism

Definition 11 *Let G_1 and G_2 be two groups and with a one-to-one mapping φ from group G_1 into group G_2 (see chap 2) with the property: if $\varphi(a) = a', \varphi(b) = b', \varphi(c) = c'$ and, $ab = c$ in group G_1 , then $a'b' = c'$ in the group G_2. Then φ is call an isomorphism from the group G_1 to the group G_2 and groups between which it is possible to establish an isomorphism are called isomorphic groups. The condition that the one-to-one mapping φ is an isomorphism can be written down as follows: $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ for any elements a and b of G_1; here product ab is taken in the group G_1 , and product $\varphi(a) \cdot \varphi(b)$ in the group G_2.*

Problem-45 Which of the following groups are isomorphic:1) the rotation group of a square, 2) the symmetry group of a rhombus, 3) the symmetry group of a rectangle, 4) the group of remainders under addition modulo 4?
Problem-46 Let $\varphi : G_1 \to G_2$ be an isomorphism. Prove that the inverse mapping $\varphi^{-1} : G_2 \to G_1$ is also an isomorphism
Problem-47 Let $\varphi_1 : G_1 \to G_2$ and $\varphi_2 : G_2 \to G_3$ be isomorphisms. Prove that $\varphi_2\varphi_1 : G_1 \to G_3$ is also an isomorphism
It follows from the last two tasks that two groups isomorphic to a third group are themselves isomorphic.
Problem-48 Prove that any cyclic group of order n is isomorphic to the group of remainders on division by n under addition modulo n.
Problem-49 Prove that any infinite cyclic group is isomorphic to the group of integers under addition.
Problem-50 Let $\varphi : G \to F$ be an isomorphism. Prove that $\varphi(e_G) = e_F$ where e_G and e_F are the identity elements in groups G and F respectively.
Problem-51 Let $\varphi : G \to F$ be an isomorphism. Prove that $\varphi(g^{-1}) = (\varphi(g))^{-1}$ for all $g \in G$.
Problem-52 Let $\varphi : G \to F$ be an isomorphism and $\varphi(g) = h$. Prove that g and h have equal orders.
If we are interested in the group operation by itself and not the nature of elements of the group (which does not play any role), then isomorphic groups cannot be distinguished. Thus for instance, we will say that there is only one (see 45) cyclic group of order n upto isomorphism which we denote by Z_n and one (see 46) infinite cyclic group upto isomorphism which we denote by Z.
If the group G_1 is isomorphic to the group G_2, then we write $G_1 \cong G_2$
Problem-53 Find all the groups (upto isomorphism), which contain: a) 2 elements, b) 3 elements.
Problem-54 To give an example of two non-isomorphic groups with identical number of elements.
Problem-55 Prove that the group of all real numbers under addition is isomorphic to the group of all positive real numbers under multiplication
Problem-56 Let a be an arbitrary element of group G. Consider the set of mappings φ_a of the elements of group G into itself defined as follows: $\varphi_a(x) = ax$ for any element $x \in G$. Prove that φ_a is a transformation of the set of the elements of group G (i.e. a one-to-one mapping of the set of the elements of group G into itself).
Problem-57 Let for each element a of group G, φ_a be the previous transformation (see the previous problem). Prove that the set of all these transformations φ_a form a group with the usual operation of composition of transformations.
Problem-58 Prove that the group G is isomorphic to the transformation group constructed in the previous problem.

2.7 Subgroups

Let us examine a certain subset of elements H in a group G . It may happen that H is itself a group with the same binary operation defined on G. In this case H is called a subgroup of group G. Thus, for

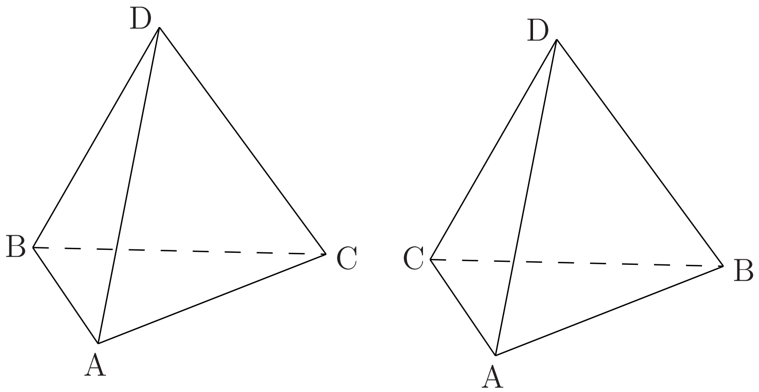


Fig. 2.5.

instance, rotation group of a regular n-polygon is the subgroup of the group of all of the symmetries of the regular n-polygon.

If a is an element of group G, the set of all elements of the form a^m is a subgroup of group G (this subgroup which we saw in section 4 is cyclic)

Problem-59 Let H be a subgroup of the group G. Prove that:a) identity elements in G and H coincide; b) if a is an element of subgroup H, then the inverse of a in G and H coincide.

Problem-60 For H to be a subgroup of the group G (relative to the same binary operation), it is necessary and sufficient that the following conditions are satisfied: 1) if a and b are contained in H, then ab (product in group G) is contained in H; 2) e (identity element in G) is contained in H; 3) if a is contained in H, then a^{-1} (in the group G) is contained in H. Prove this.

Observation.From conditions 1) and 3) follow condition 2).

Problem-61 Find all subgroups in the groups:1) the symmetry group of an equilateral triangle, 2) the symmetry group of a square.

Problem-62 Find all subgroups in the cyclic groups: a)Z_5; b)Z_8; c)Z_{15}

Problem-63 Prove that all subgroups in Z_n take the form $e, a^d, a^{2d}, \ldots, a^{(\frac{n}{d}-1)d}$ where d divides n and and a is the generator of group Z_n.

Problem-64 Prove that all subgroups of infinite cyclic group take the form $\ldots, a^{-2r}, a^{-r}, e, a^r, a^{2r}, \ldots$, where a generates the group , and r is an arbitrary natural number.

Problem-65 Prove that in any infinite group there are infinitely many subgroups.

Problem-66 Prove that the intersection of any number of subgroups [7] of a certain group G is also a subgroup of group G.

Example-10 Let us consider a regular tetrahedron whose vertices are designated by letters A, B, C and D. If we look at triangle ABC from point D, then the points A, B, C can be oriented clockwise or anti-clockwise (Fig. 2.5). We will distinguish these two orientations of the tetrahedron.

Problem-67 Do the following permutations preserve the orientation of tetrahedron: $a = \begin{pmatrix} ABCD \\ BCAD \end{pmatrix}$ - rotation by 120° around the altitude from D and perpendicular to the base; $b = \begin{pmatrix} ABCD \\ DCBA \end{pmatrix}$ - rotation by 180° around the axis passing through the middle of edges AD and BC; $c = \begin{pmatrix} ABCD \\ ACBD \end{pmatrix}$ - reflection

[7] The intersection of several sets consists of all the elements which belong to all the given sets

with respect to the plane containing edge AD and the middle of edge BC; the permutation which generates the cyclic substitution of the vertices $d = \begin{pmatrix} ABCD \\ BCDA \end{pmatrix}$.

All symmetries of a regular tetrahedron obviously form a group which is called the symmetry group of the tetrahedron.

Problem-68 How many elements does the symmetry group of a tetrahedron have?

Problem-69 Find the subgroups in the symmetry group of tetrahedron isomorphic to: a) to the symmetry group of triangle, b) to cyclic group Z_4.

Problem-70 Prove that all symmetries of a tetrahedron which preserve the orientation form a group. How many elements does it have ?

The symmetry group of a tetrahedron that preserves orientation is called the rotation group of the tetrahedron.

Problem-71 Find subgroups in the rotation group of the tetrahedron isomorphic to the cyclic groups: a) Z_2, b) Z_3.

2.8 Direct product

From two groups it is possible to form a new group.

Definition 12 *The direct product of two groups G and H (denoted by $G \times H$) is the set of all possible ordered pairs (g, h), where g is an arbitrary element from G and is h an arbitrary element from H with the following binary operation: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$ where the product $g_1 g_2$ is taken in the group G and $h_1 h_2$ is taken in H.*

Problem-72 Prove that $G \times H$ is a group.

Problem-73 Let G and H have n and k elements respectively. How many elements does $G \times H$ have ?

Problem-74 Prove that the groups $G \times H$ and $H \times G$ are isomorphic.

Problem-75 Find subgroups in $G \times H$ isomorphic to groups G and H.

Problem-76 Let the groups G and H be commutative. Prove that the group $G \times H$ is also commutative.

Problem-77 Let G_1 and H_1 be subgroups of groups G and H respectively. Prove that $G_1 \times H_1$ is a subgroup of $G \times H$.

Problem-78 Let G and H be arbitrary groups. Is it true that any subgroup in the group $G \times H$ can be represented in the form of $G_1 \times H_1$ where G_1 and H_1 are subgroups of groups G and H respectively.

Problem-79 Prove that the symmetry group of a rhombus is isomorphic to group $Z_2 \times Z_2$.

Problem-80 Prove the isomorphisms: 1)$Z_2 \times Z_3 \cong Z_6$, 2) $Z_2 \times Z_4 \cong Z_8$.

Problem-81 Prove that $Z_m \times Z_n \cong Z_{mn} \iff$ the numbers m and n are mutually coprime.

2.9 Cosets and Lagrange's theorem

To each subgroup H of the group G we can associate the following partition of the elements of group G into subsets. For any element $x \in G$ let us consider the set of all elements of the form xh where h runs over all possible elements in H. This subset denoted by xH is called *the left coset of H generated by the element x*.

Problem-82 Find all left cosets of the group of symmetry of triangle by: a) the subgroup of rotations of triangle; b) subgroup of reflections with respect to a single axis $\{e, c\}$ (see examples 1 and 2, p. 13).

Problem-83 Prove that given a subgroup H, each element of the group belongs to a certain left coset of the subgroup H.

Problem-84 Let element y belong to the left coset of H generated by element x. Prove that left coset of H generated by elements x and y coincide.

Problem-85 Let left cosets of H generated by elements x and y contain a common element. Prove that these cosets coincide.

Thus, left cosets generated by any two elements either do not intersect or they coincide and we obtain a partition of all elements of the group G into non-intersecting classes. This partition is called the left decomposition of group G by the subgroup H.

The number of elements in a subgroup is called the order of subgroup. Let m be the order of the subgroup H. If $h_1 \neq h_2$, then $xh_1 \neq xh_2$, therefore each left coset also contains m elements. Consequently, if n is the order of the group G and r the number of left cosets in the decomposition of G by H, then $m \cdot r = n$ and we have proved:

Theorem 2.1 (Lagrange's theorem [8]) *The order of a subgroup divides the order of the group.*

Problem-86 Prove that the order of any element (see p. 20) divides the order of the group.

Problem-87 Prove that any group of prime order is cyclic and any element in it different from e is its generator.

Problem-88 Group G contains 31 elements. How many subgroups can group G contain ?

Problem-89 Prove that all groups of prime order p are isomorphic to each other.

Problem-90 Suppose m divides m. Build a group of order n containing a subgroup isomorphic to a group G of order m.

Problem-91 Suppose m divides m. Is it possible that a group of order n does not contain any subgroup of order m ?

It is also possible to build right cosets Hx and right decomposition of a group G by a subgroup H. If the order of a subgroup H is equal to m, then each right coset contains m elements and number of cosets equal to the natural number $\frac{n}{m}$, where n the order of group. Thus, the number of right cosets coincides with the number of left cosets

Note For the practical construction of expansions of finite group it is not necessary to construct cosets for each element, since in this case identical classes will be obtained, and it is necessary to take the elements which are not yet in the cosets already constructed. Since $eH = He = H$, the subgroup itself always forms both right and left coset.

Problem-92 To build the left and right decomposition of the symmetry group of an equilateral triangle by: a) the subgroup of rotations $\{e, a, b\}$, b) subgroup of reflections relative to one axis $\{e, c\}$.

Problem-93 To build the left and right decomposition of the symmetry group of a square by: a) the subgroup of reflections relative to center $\{e, a\}$, b) the subgroup of reflections relative to one diagonal $\{e, d\}$.

Problem-94 To build the decomposition of the group of all integers (under addition) by the subgroup of the numbers under addition modulo 3. [9].

Problem-95 Find all groups (upto isomorphism) of order: a)4, b)6, c)8.

2.10 Inner automorphism

Let us start with an example. Consider the symmetry group of an equilateral triangle. If we denote the vertices of the triangle by the letters A, B, C, then each element of this group is uniquely determined by a permutation of three letters A, B, C. For example, the reflection of the triangle with respect

[9] We do not mention here what type of decomposition we want since in a commutative group the left and right decompositions coincide

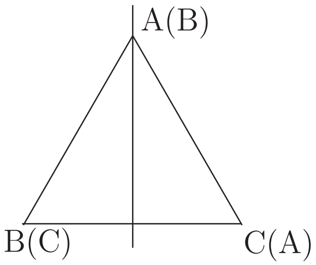


Fig. 2.6.

to the altitude from the vertex A to the side BC is written as $\begin{pmatrix} ABC \\ ACB \end{pmatrix}$. In order to multiply two elements of this symmetry group, it suffices to carry out the corresponding permutations one after the another. In this way we obtain an isomorphism from the symmetry group of the triangle and the permutation group of three letters A, B, C. Note that this isomorphism is not uniquely determined: it depends on how we labelled the vertex of the triangle by A, B and C. The relabeling of vertices can also be considered as a permutation of the three letters A, B, C. For example, $g = \begin{pmatrix} ABC \\ BCA \end{pmatrix}$ corresponds to the following relabelling of vertices:

Table 2.2.

Old notation	A	B	C
New notation	B	C	A

Under the new labelling of the vertices each element of the symmetry group of the triangle will have a new notation in terms of permutation of the letters A, B, C. For example, the reflection of triangle relative to its vertical altitude (Fig. 2.6) is denoted as follows:

the old labelling $\begin{pmatrix} ABC \\ ACB \end{pmatrix}$

the new labelling $\begin{pmatrix} ABC \\ CBA \end{pmatrix}$

Problem-96 Consider an element of the symmetry group of the triangle, which, in a certain labelling of vertices corresponds to a permutation h. What permutation will correspond to the same element of the symmetry group of the triangle after the relabelling of vertices given by g ?

Note Observe now that the relabelling g sends the element h of a certain transformation group to ghg^{-1} not only in the example of the symmetry group of triangle considered, but also in the most general case. So, the study of relabelling leads to the following definition.

Definition 13 *Let G be a group and g one of its element. Define the mapping φ_g of the group G into itself by the formula of $\varphi_g(h) = ghg^{-1}$ (where h is any element of the group). This mapping is called the inner automorphism of group G generated by element g.*

Problem-97 Prove that the inner automorphism of a group is an isomorphism of the group into itself.

Problem-98 What is the image of the reflection of the triangle with respect to its altitude under all possible inner automorphism of the symmetry group of the triangle ?

Problem-99 What is the image of the rotation of the triangle by 120° under all possible inner automorphism of the symmetry group of triangle transform ?
Problem-100 What are the pairs of elements of the symmetry group of the tetrahedron that can be sent into each other by an inner automorphism ? Which element pairs cannot ? The same question for the rotation group of the tetrahedron.
Problem-101 Prove that the orders of elements ab and ba in any group are equal.
Note that in general, the image of a subgroup under any inner automorphism of a group (as well as under any isomorphism) is in general different. (for example, reflections with respect to one altitude of a triangle mapt to reflections with respect to another altitude). However, some "especially symmetrical" subgroups are invariant under all inner automorphism (for example, the subgroup of the rotations of triangle in the symmetry group of triangle). We will now studey such subgroups.

2.11 Normal subgroups

Definition 14 *A subgroup of a group is called a normal subgroup if it invariant under all inner automorphism of the group. In other words, a subgroup H of a group G is called a normal subgroup in G if for any element $h \in H$ and any element $g \in G$ element ghg^{-1} belongs to H.*

Thus, the subgroup of rotations is a normal subgroup in the symmetry group of a triangle but the subgroup of reflections with respect to an altitude from the vertex A to the side BC (consisting of two elements) is not a normal subgroup of the symmetry group of triangle.
Problem-102 Prove that in a commutative group any subgroup is a normal subgroup
Problem-103 Is the subgroup of the symmetry group of a square which consists of two elements $\{e, a\}$ (examples 3, 4, page. 15) a normal subgroup ?

Theorem 2.2 *The subgroup H of a group G is normal subgroup $\iff$ left and right decompositions (see section 8) of the group G by the subgroup H coincide.* [10]

Problem-104 Prove the above theorem.
Problem-105 Let n be the order of a group G, m the order of subgroup H and $m = \frac{n}{2}$. Prove that H is a normal subgroup of the group G.
Problem-106 Prove that the intersection (see footnote on page 22) of any number of normal subgroups of a group G is a normal subgroup of the group G.

Definition 15 *The set of all the elements of a group G which commute with all the elements of the group is called the center of the group G.*

Problem-107 Show that center of a group G is a subgroup and moreover, a normal subgroup of the group G.
Problem-108 Let N_1 and N_2 be normal subgroups respectively in the groups G_1 and G_2. Prove that $N_1 \times N_2$ is a normal subgroup in the group $G_1 \times G_2$.
The following example shows that the normal subgroup of a normal subgroup of group G may not be a normal subgroup of the group G itself.
labelnormal-normal-notnormal
Example-11 Let us examine the subgroup of the symmetry group of square which consists of the reflections with respect to diagonals and the center (see examples 3, 4, page 15 , the subgroup $\{e, a, d, f\}$). This subgroup contains half of the elements of the symmetry group of the square and is therefore a normal subgroup (see problem 102). The subgroup $\{e, d\}$ which consists of the reflections relative to one of the diagonals contains half of the elements of the subgroup $\{e, a, d, f\}$ is therefore

[10] In this case the decomposition obtained will simply be called the decomposition by the normal subgroup

a normal subgroup in it. On the other hand the subgroup $\{e, d\}$ is not a normal subgroup of the entire symmetry group of square, since under an inner automorphism, d goes to a reflection relative to another diagonal: $bdb^{-1} = f$.

2.12 Quotient groups

Let us start with an example. Consider the decomposition of the symmetry group of square by the normal subgroup which consists of the identity and rotation by 180°, i.e., the subgroup $\{e, a\}$ (see examples 3, 4, page 15). It is easy to see that the decomposition of our group into four cosets takes the form, indicated in table 2.3. Denote each coset by a letter, for example E, A, B, C. If we multiply any element from coset A with any element from coset B, then the result belongs to coset C and is independent of the particular coset elements chosen from of A and B. From the solution of the next problem it follows that this not a coincidence.

Table 2.3.

e	b	d	g
a	c	f	h
E	A	B	C

Problem-109 Let the decomposition of a group G by a normal subgroup N be given and let the elements x_1 and x_2 belong to one coset and elements y_1 and y_2 belong to another coset. Prove that the elements x_1y_1 and x_2y_2 belong to the same coset.

In this way, multiplying in a given order representatives of two cosets, we will obtain an element of a coset which will not depend on the particular representatives we chose. Hence, under the decomposition of a group by a normal subgroup N, it is possible to define a binary operation on the set of cosets as follows: if $A = xN, B = yN$, we write $AB = (xy)N$. The result of problem 105 shows that this operation is uniquely defined and does not depend on the elements x and y generating cosets A and B. Then, in the example considered above $AB = C$.

In problems 107 to 109, the discussion deals with decomposition by normal subgroup. Assume the subgroups are normal in these problems.

Problem-110 Let T_1, T_2, T_3 be cosets. Prove $(T_1T_2)T_3 = T_1(T_2T_3)$.

Problem-111 Let the normal subgroup containing e be denoted by the letter E. Show that $ET = TE = T$ for any coset T.

Problem-112 Prove that for any coset T there exists a coset T^{-1} such that $TT^{-1} = T^{-1}T = E$

From the results of problems 107 to 109 it follow that the set of all cosets with the binary operation defined above forms a group. This group is called *the quotient group of group G by the normal subgroup* N and is denoted by G/N

It is obvious that $G/e = G$ and $G/G = e$. It is also evident that the order of quotient group is equal to the natural number $\frac{n}{m}$, where n is the order of group G, and m the order of normal subgroup N. For example, the quotient group of the symmetry group of square by the subgroup $\{e, a\}$ consisting of the identity and rotation by 180° about an axis contains 4 elements.

Problem-113 Is the quotient of the symmetry group of a square by the subgroup $\{e, a\}$ isomorphic to the rotation group of a square or to the symmetry group of rhombus.

Problem-114 Find all normal subgroups and the corresponding quotient groups [11] in the following groups: a) the symmetry group of triangle, b) $Z_2 \times Z_2$ c) the symmetry group of square, g) the group of quaternions.
Problem-115 To describe all normal subgroups and quotient groups in the groups: a)Z_n, b)Z.
Problem-116 Find all normal subgroups and quotient groups in the rotation group of the tetrahedron.
Problem-117 Consider the subgroup $G_1 \times e_2$ in the direct product of the groups $G_1 \times G_2$. Prove that this is a normal subgroup and that the corresponding quotient group is isomorphic to the group G_2.

2.13 Commutator

Recall that two elements a and b of a group G are called commutating if $ab = ba$. The degree of the noncommutativity of two elements of group can be measured by the product $aba^{-1}b^{-1}$, which is equal to one $\iff$ a and b commute (prove this).

Definition 16 *The element $aba^{-1}b^{-1}$ is called the commutator of elements a and b. The commutator $K(G)$ of a group G is the collection of all possible finite number of commutators of elements of the group G.*

Problem-118 Prove that the commutator of a group is a subgroup.
Problem-119 Prove that the commutator of a group is a normal subgroup.
Problem-120 Prove that the commutator coincides with the single element subgroup {e} if and only if group is commutative.
Problem-121 Find the commutator in the groups: a) the symmetry group of a triangle, b) the symmetry group of a square, c) the group of quaternions.
Problem-122 Prove that the commutator in the symmetry group of a regular n-polygon is isomorphic to group Z_n with n odd and group $Z_{\frac{n}{2}}$ if n is even.
Problem-123 Find the commutator in the symmetry group of a tetrahedron.
Problem-124 Prove that if a normal subgroup of the rotation group or of the symmetry group of a tetrahedron contains at one rotation around an axis passing through a vertex, then it contains all the rotations of the tetrahedron.
Problem-125 Find a commutator in the symmetry group of the tetrahedron.
Let us examine the 2 additional groups: the rotation group of a cube and the rotation group of a regular octahedron (Fig. 2.7).
Problem-126 How many elements are there in each of these groups ? Enumerate the elements of the rotation group of the cube.
Problem-127 Prove that the rotation group of a cube and an octahedron are isomorphic.
Problem-128 In how many different ways is it possible to paint the faces of a cube with 6 colors (different color for each face) if two coloured cubes which do not coincide even after some rotation are considered different. The same question for a box of match.
Problem-129 Which of the groups known to you is isomorphic to the rotation group of a match box ?
To calculate the commutator of the rotation group of a cube inscribe a tetrahedron in the cube as shown in figure (Fig. 2.8). In this case if we join the remaining vertices B, D, A_1 and C_1, one obtains

[11] In the sequel finding a quotient group will mean finding a group, among those already studied, which is isomorphic to the desired quotient group.

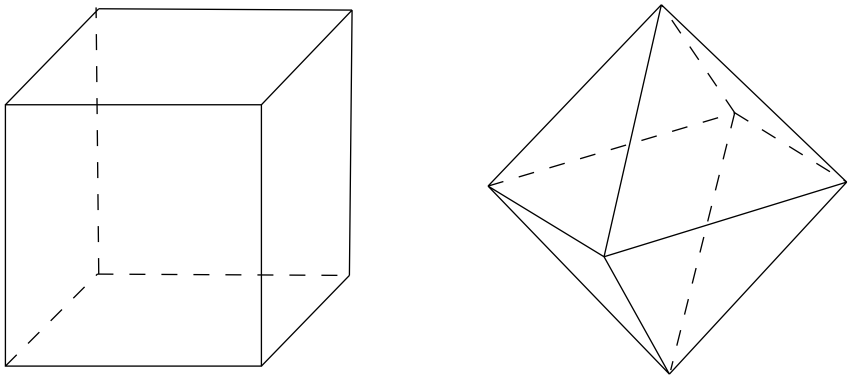


Fig. 2.7.

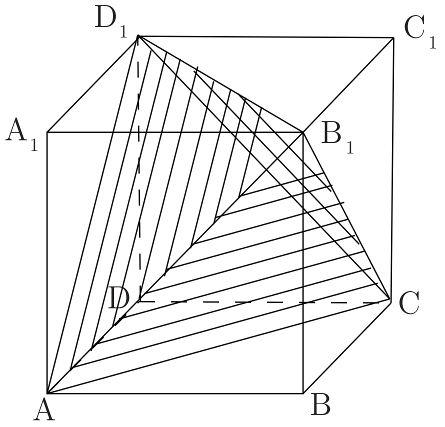


Fig. 2.8.

a second tetrahedron. Any rotation of cube either sends each tetrahedron into itself or it swaps their positions.

Problem-130 Prove that all the rotations of a cube which sends each tetrahedron onto itself form: a) a subgroup, b) a normal subgroup of the rotation group of cube.

Problem-131 Prove that the commutator of the rotation group of cube is isomorphic to the rotation group of tetrahedron.

Let us now prove the following 3 properties of commutator which will be of use later on.

Problem-132 Prove that the quotient group of an arbitrary group G by its commutator is commutative.

Problem-133 Let N be a normal subgroup of a group G and let the quotient group G/N be commutative. Prove that N contains the commutator of the group G.

Problem-134 Let N be a normal subgroup of a group G and $K(N)$ the commutator of the subgroup N. Prove that $K(N)$ is a normal subgroup of the group G (compare it with the example 11 on page **??**).

2.14 Homomorphism

A homomorphish is a mapping $\varphi : G \to F$ from group G to group F such that $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ for any elements a and b in groups G (here the product ab is taken in the group G and the product $\varphi(a) \cdot \varphi(b)$ in group F). A homomorphism is different from an isomorphism as it need not be bijective. *Example-12* Let G be the rotation group of a cube and Z_2 the permutation group of two tetrahedrons inscribed in it (see page. ???). To each rotation of the cube there corresponds a well defined permutation of the tetrahedra. When we have two rotations of the cube one after the other, the resulting permutation of the tetrahedra is the product of the permutations of the tetrahedra corresponding to these rotations. Thus, the mapping of the group of rotations of the cube into the permutations of two tetrahedra is a homomorphism.

Problem-135 Let $\varphi : G \to F$ be a surjective homomorphism of a group G onto a group F. If the group G is commutative, then F is commutative. Prove this. Is the converse correct ?

Problem-136 Prove that a homomorphism of the group G into group F carries the identity of group G to the identity of the group F.

Problem-137 Prove that $\varphi(g^{-1}) = (\varphi(g))^{-1}$, where $\varphi : G \to F$ is a homomorphism and on the left side the inverse is taken in the group G and in the right side it is taken in the group F.

Problem-138 Let $\varphi_1 : G \to F$ and $\varphi_2 : F \to H$ be two homomorphisms. Prove that $\varphi_2\varphi_1 : G \to H$ is a homomorphism.

Important examples of homomorphisms are obtained using the following construction of ”natural homomorphism”.

Let N be a normal subgroup of a group G. Consider the following mapping φ of the group G to quotient group G/N. Map each element g in the group G to the coset of N which contains the element g.

Problem-139 Prove that $\varphi : G \to G/N$ is a homomorphism from the group G to the group G/N.

Definition 17 *The mapping φ is called the natural homomorphism from the group G to the quotient group G/N.*

We showed that to each normal subgroup, there corresponds a certain homomorphism. Let us now show that conversely, every surjective homomorphism of a group G onto group F can be seen as a natural homomorphism from G to the quotient group G/N by a suitable normal subgroup.

Definition 18 *Let $\varphi : G \to F$ be a group homomorphism. Then the set of elements g of G such that $\varphi(g) = e_F$ is called the kernel of the homomorphism φ and is denoted Ker φ.*

Problem-140 Prove that Ker φ is a subgroup of the group G.

Problem-141 Prove that Ker φ is a normal subgroup of the group G.

Consider the decomposition of the group G by Ker φ.

Problem-142 Prove that g_1 and g_2 lie in one coset if and only if $\varphi(g_1) = \varphi(g_2)$.

Theorem 2.3 *Let $\varphi : G \to F$ be a homomorphism of a group G to a group F. Then the mapping $\psi : G/\text{Ker } \varphi \to F$ which sends each coset to the image $\varphi(g)$ for some element g of the coset (and thus any element (see problem 139)) is an isomorphism.*

The proof of this theorem is contained in the solutions of the following problems.

Problem-143 Prove that ψ is an onto mapping .

Problem-144 Prove that ψ is a bijective mapping.

Problem-145 Prove that ψ is an isomorphism.

Let us give examples of applications of the above theorem.

Example-13 In problem 110 it was asked whether the quotient group of the symmetry group of square by the normal subgroup consisting of the identity and rotation by 180° about the centre was

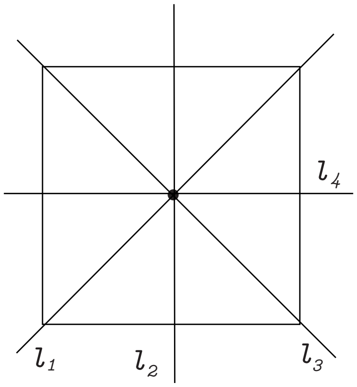


Fig. 2.9.

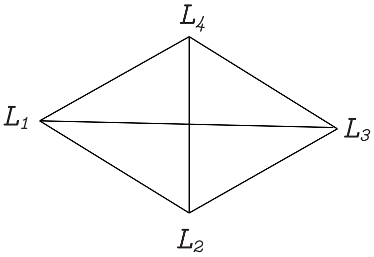


Fig. 2.10.

isomorphic to the rotation group of square or to the symmetry group of rhombus. To each element of the symmetry group of the square there corresponds a certain permutation of axes of symmetry l_1, l_2, l_3, l_4 (Fig. 2.9). This permutation can swap the diagonals l_1 and l_3 as well as the axis l_2 and l_4. We thus obtain a mapping from the symmetry group of the square to the permutation group of four elements: l_1, l_2, l_3 and l_4. This mapping is surjective homomorphism onto the entire group of permutations which send $\{l_1, l_3\}$ to $\{l_1, l_3\}$ and $\{l_2, l_4\}$ to $\{l_2, l_4\}$ (verify). This group consists of four permutations and is isomorphic to the symmetry group of rhombus $L_1L_2L_3L_4$ (Fig. 2.10).

The kernel of the homomorphism constructed contains all the symmetries of the square sending each axis of symmetry onto itself. It is not difficult to verify that a and e are the only such transformations. Therefore, by Theorem 3 the subgroup $\{e, a\}$ is a normal subgroup of the symmetry group of the square and the corresponding quotient group is isomorphic to the symmetry group of rhombus.

Similarly it is possible to solve the following problems.

Problem-146 Prove that the rotations of tetrahedron by 180° around the axes through the middle points of opposite edges together with the identity transformation form a normal subgroup of the symmetry group of tetrahedron. Find the corresponding quotient group.

Problem-147 Prove that the rotations of the cube by 180° around the axes through the centers of opposite faces together with the identity transformation form a normal subgroup of the rotation group of the cube. Find the corresponding quotient group.

Problem-148 Consider a reguler n-polygon on a plane with center O. Let R be the group of all rotations of plane around the point O. Let Z_n be the subgroup of all rotations of plane which sends the regular n-polygon into itself. Prove that this is a normal subgroup of the group R and that $R/Zn = R$

Problem-149 Let N_1 and N_2 be two normal subgroups of G_1 and G_2 respectively. Prove that $N_1 \times N_2$ is a normal subgroup of $G_1 \times G_2$ and $(G_1 \times G_2)/(N1 \times N_2) = (G_1/N1) \times (G_2/N_2)$.

Problem-150 Can two nonisomorphic groups have isomorphic normal subgroups and isomorphic corresponding quotient groups ?

Problem-151 Can a group have two isomorphic normal subgroups but nonisomorphic corresponding quotient groups ?

Problem-152 Can groups have nonisomorphic normal subgroups but with the corresponding quotient groups isomorphic ?

Let us observe what happens to subgroups, normal subgroups and commutators under a homomorphism. Let $\varphi : G \to F$ be a homomorphism and let M be a subset of G. Then the set of all elements in F which have at least one pre-image in M under the homomorphism φ is called the image of M (denoted by $(\varphi(M))$. Conversely, let P be subset of F. Then the set of all elements of G having an image in P is called the pre-image of P (denoted by $\varphi^{-1}(P)$). Note that the symbol φ^{-1} without

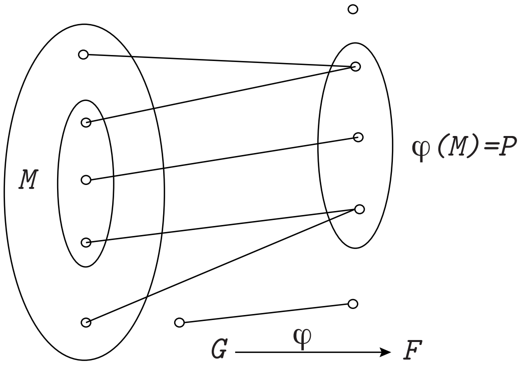


Fig. 2.11.

P has no meaning: a homomorphism, in general has no inverse. Note also that if $\varphi(M) = P$, then $\varphi^{-1}(P)$ is contained in M, but is does not necessarily equal to M (Fig. 2.11).

Problem-153 Prove that the image of a subgroup H of a group G under the homomorphism $\varphi : G \to F$ is a subgroup of the group F.

Problem-154 Let H be a subgroup of F and $\varphi : G \to F$ a homomorphism. Prove that $\varphi^{-1}(H)$ is a subgroup of G.

Problem-155 Let N be a normal subgroup of G and $\varphi : G \to F$ be a homomorphism. Prove that $\varphi^{-1}(N)$ is a normal subgroup of the group G.

Problem-156 Let $\varphi : G \to F$ be a homomorphism and K_1, K_2 be the commutators of groups G and F respectively. Prove that $\varphi(K_1)$ is contained in K_2 and K_1 is contained in $\varphi^{-1}(K_2)$

Problem-157 Let N be a normal subgroup of F and $\varphi : G \to F$ be a surjective homomorphism. Prove that $\varphi(N)$ is a normal subgroup in F.

Problem-158 Let $\varphi : G \to F$ be a surjective homomorphism and K_1, K_2 be the commutators of groups G and F respectively. Prove that $\varphi(K_1) = K_2$. Is it true that $K_1 = \varphi^{-1}(K_2)$

2.15 Solvable groups.

There is an important class of groups which are similar to commutative groups: solvable groups. They are called solvable because the possibility to solve algebraic equation in radicals, as we will see later on, depends on the solvability of a certain group.

Let G be a certain group and $K(G)$ its commutator. The commutator $K(G)$ itself is a group and it is possible to consider the commutator $K(K(G))$. In the obtained group one can again consider its commutator and so forth. We will for brevity denote $K(K(\ldots(K(G))\ldots))$ by $K_r(G)$. Thus, $K_{r+1}(G) = K(K_r(G))$.

Definition 19 *A group G is called solvable if the sequence of groups $G, K(G), K_1(G), K_2(G), \ldots$ ends, for a finite n, with the group consisting of the single element e, i.e., for some finite n we obtain $K_n(G) = \{e\}$.*

For example, any commutative group is solvable: if G is a commutative group, then we already obtain $K(G) = \{e\}$ at the first step. A group G is solvable if its commutator is commutative, since $K_2(G) = \{e\}$.

Problem-159 Are the following groups solvable: a) the cyclic group Z_n b) the symmetry group of a triangle, c) the symmetry group of a square, g) the group of quaternions, d) the rotation group of a tetrahedron, e) the symmetry group of a tetrahedron, f) the rotation group of a cube.

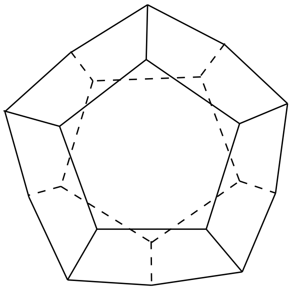


Fig. 2.12.

All the groups considered in problem 156 are solvable. It is thus natural to ask whether there are non-soluble groups. Below we will show that the rotation group of a regular dodecahedron (Fig. 2.12) is insoluble.

Problem-160 How many elements does the rotation group of a dodecahedron have ?

All rotations of a dodecahedron can be broken into 4 classes: 1) the identity transformation; 2) rotation around the axes through the centers of opposite faces; 3) rotation around the axes through opposite vertices; 4) rotation around the axes through the middle points of opposite edges.

Problem-161 How many elements are there in each class (without counting the identity transformation in classes in 2 - 4)?

Problem-162 Let N be an arbitrary normal subgroup of the rotation group of a dodecahedron and suppose N contains at least one element from a certain class from 1-4. Prove that then N contains the entire class of this element.

Thus, each of the classes 1- 4 either belongs entirely to N or has no elements in N.

Problem-163 Prove that in the rotation group of a dodecahedron there are no other normal subgroups except {e} and entire group.

Problem-164 Let group G be non-commutative with no normal subgroups other than {e} and G. Prove that the group G is non-solvable.

It follows that from problems 160 and 161 that the rotation group of a dodecahedron is non-solvable. Lets consider some problems whose results will be of use later on.

Problem-165 Prove that every subgroup of a solvable group is solvable.

Problem-166 Let $\varphi : G \to F$ be a homomorphism from group G to group F with group G solvable. Prove that the group F is also solvable.

Problem-167 Give an example in which group F is solvable and group G is non-solvable (see the previous problem).

Problem-168 Let group G be solvable with N a normal subgroup in G. Prove that the quotient group G/N is solvable.

Problem-169 Prove that if groups N and G/N are solvable, then the group G is solvable.

Problem-170 Let groups G and F be solvable. Prove that the group $G \times F$ is solvable.

Problem-171 Let group G be solvable. Prove that there exists a sequence of groups $G_0, G_1, \ldots, G_n$ such that: 1) $G_0 = G$, 2) each group $G_i (1 \leq i \leq n)$ is a normal subgroup of group G_{i-1} and all the quotient groups G_{i-1}/G_i are commutative; 3) the group G_n is commutative.

Problem-172 Suppose that for a group G there exists a sequence of groups with the properties described in the previous problem. Prove that the group G is solvable.

The results of problems 168 and 169 show that for a group G the existence of a sequence of groups with the properties described in problem 168 is equivalent to the condition of solvability itself can as well be taken as the definition of solvability. Yet another equivalent definition of solvability can be obtained using results of two following problems.

Problem-173 Let group G be solvable. Prove that then there is a sequence of groups $G_0, G_1, \ldots, G_n$ such that: 1) $G_0 = G$, 2) each group $G_i (0 \leq i \leq n-1)$ contains a certain commutative normal subgroup N_i such that $G_i/N_i = G_{i+1}$; 3) the group G_n is commutative.

Problem-174 Suppose that for a group G there exists a sequence of groups with the properties described in the previous problem. Prove that the group G is solvable.

2.16 Permutations

Let us study in more details the permutation (i.e. transformation) of the set of first n natural numbers $1, 2, \ldots, n$; we will call these permutations of degree n. Note that the permutations on an arbitrary set with n elements can be considered as a permutation of degree n: it is sufficient to number the elements of the set by natural numbers $1, 2, \ldots, n$. It is possible to write down an arbitrary permutation of degree n in the form $\begin{pmatrix} 12 \ldots n \\ i_1 i_2 \ldots i_n \end{pmatrix}$ where i_m is the image of element m under the given permutation. Recall that a permutation is a one-to-one mapping; therefore all the elements in the lower line are different.

Problem-175 How many different permutations of degree n do we have ?

Definition 20 *The group of all permutations of degree n with the usual operation of multiplication (i.e. composition) of permutations* [12] *is called the symmetric group of degree n and are denoted by* S_n.

Problem-176 Prove that for $n \geq 3$ the group S_n is non-commutative.

A permutation can move some elements and leave some fixed. It may happen that the permuted elements change their position in a cyclic manner. For example, the permutation $\begin{pmatrix} 1234567 \\ 4263517 \end{pmatrix}$ fixes the elements 2, 5 and 7, and the remaining elements are permuted cyclically: $1 \to 4, 4 \to 3, 3 \to 6, 6 \to 1$. Permutations of this kind are called cyclic permutations or simply cycles. We will use a different notation for cyclic permutation. For example, the expression (1436) will denote the permutation sending $1 \to 4, 4 \to 3, 3 \to 6, 6 \to 1$ and which fixes the remaining elements of the set. So if our permutation has degree 7, then then coincides with the permutation considered above.

Not all permutations are cyclic. For example, the permutation $\begin{pmatrix} 123456 \\ 354126 \end{pmatrix}$ is not cyclic but it can be represented as the product of two cycles: $\begin{pmatrix} 123456 \\ 354126 \end{pmatrix} = (134) \cdot (25)$.

The cycles obtained permute different elements and such cycles are called independent. It is easy to see that the product of two independent cycles does not depend on the order of their factors. If we do not distinguish products of independent cycles which differ in their factor sequence then the following proposition holds true.

Problem-177 Any permutation is uniquely (upto different ordering of factors) decomposed into the product of several independent cycles. Prove this.

The cycles of the form (i, j) which swaps only two elements are called transpositions.

[12] According to our definition for the product of transformations, the product of permutations are carried out from right to left. Sometimes the product of permutations are carried out from left to right. The groups obtained by these two rules are isomorphic.

Problem-178 Prove that an arbitrary cycle can be decomposed into the product of transpositions (not necessarily independent).
Transpositions $(1,2),(2,3),\dots,(n-1,n)$ are called elementary transpositions.
Problem-179 Prove that an arbitrary transposition can be represented in the form of a product of elementary transpositions.
From the results of problems 174- 176 it follows that an arbitrary permutation of the degree n can be represented as the product of elementary transpositions. In other words, the following theorem is true.

Theorem 2.4 *If a subgroup of the symmetrical group S_n contains all the elementary transpositions, then this subgroup coincides with the entire group S_n*

Suppose the numbers $1,2,\dots,n$ are written in a line in a certain arbitrary order. We say that the pair of numbers i,j is an inversion in this line if $i<j$ but j is appears before i in the line. The number of inversions characterizes the disorder in this line with respect to the usual order $1,2,\dots,n$.
Problem-180 Find the number of inversions in line 3, 2, 5, 4, 1.
From now on, we will not be interested in the number of inversions in a line, but in its parity.
Problem-181 Prove that the parity of the number of inversions in a line changes if we interchange the position two arbitrary numbers.

Definition 21 *The permutation $\begin{pmatrix} 12\dots n \\ i_1 i_2 \dots i_n \end{pmatrix}$ is called an even or odd depending on whether there are even or odd number of inversions in the lower line. For example, the identity permutation $\begin{pmatrix} 12\dots n \\ 12\dots n \end{pmatrix}$ is an even permutation, since the number of inversions in the lower line is equal to zero.*

Problem-182 To determine the parity of the permutation $\begin{pmatrix} 12345 \\ 25413 \end{pmatrix}$
Problem-183 Prove that by multiplying an even permutation to the right by an arbitrary transposition we get an odd permutation and on the other hand by multiplying an odd permutation to the right by an arbitrary transposition we get an even permutation.
Problem-184 Prove that an even permutation can be decomposed into the product of only even number of transpositions and an odd permutation into the product of only an odd number of transpositions.
Problem-185 To determine the parity of an arbitrary cycle of the length: a) 3, b) 4, c) m.
Problem-186 Prove that by multiplying two permutations of identical parity we get an even permutation and by multiplying two permutations of different parity we get an odd permutation.
Problem-187 Prove that the permutations a and a^{-1} have the same parity where a is an arbitrary permutation.
It follows that from the results of problems 183 and 184 that all the even permutations form a subgroup of the group S_n.

Definition 22 *The group of all even permutations of the degree n is called the alternating group of degree n and is denoted by A_n.*

Problem-188 Prove that for $n \geq 4$, A_n is noncommutative.
Problem-189 Prove that the alternating group A_n is a normal subgroup of the symmetric group S_n and to build the decomposition of the group S_n by A_n.
Problem-190 To determine the number of elements in the group A_n.
Problem-191 Prove that the groups S_2, S_3 and S_4 are solvable.
We now prove that the alternating group A_5 is non-solvable. One of the proofs consists of the following. Inscribe five tetrahedrons labelled by 1, 2, 3, 4, 5 in a dodecahedron in such a way that to every

rotation of the dodecahedron there corresponds an even permutation of the tetrahedra and different rotations correspond to different permutations. By this, we have established an isomorphism between the rotation group of the dodecahedron and the group of even permutations of the degree 5 A_5. Then the non-solvability of the group A_5 will follow from the non-solvability of the rotation group of dodecahedron.

Problem-192 To inscribe five tetrahedrons in a dodecahedron in the required manner prescribed above.

Another proof of the non-solvability of the group A_5 consists in repeating the proof of the non-solvability of the rotation group of a dodecahedron. For this it is necessary to solve the following problems.

Problem-193 Prove that any even permutation of the degree 5 different from the identity permutation can be decomposed into independent cycles in one of the following three way: A) $(i_1i_2i_3i_4i_5)$, b)$(i_1i_2i_3)$, c)$(i_1i_2)(i_3i_4)$.

Problem-194 Let N be a normal subgroup of group A_5. Prove that if N contains at least one permutation which splits into independent cycles indicated in Problem 190 then N contain all the permutations splitting into independent cycles this way.

Problem-195 Prove that the group A_5 does not contain normal subgroups except single element subgroup and entire group.

From the results of problems 192, 161 and from the fact that group A_5 is noncommutative the insolvability of group A_5 follows.

Problem-196 Prove that the symmetrical group S_n for $n \geq 5$ contains a subgroup isomorphic to group A_5.

From the results of problems 193 and 162 we obtain the theorem.

Theorem 2.5 *The symmetrical group S_n is non-solvable for $n \geq 5$.*

The proof of this theorem and other results in this chapter will be required in the following chapters for the proof of non-solvability in radicals of a general algebraic equations of degree greater than four[13].

[13]

The following books are recommended to students who wish to study the theory of groups more deeply:

Kargapolov M. I., Merzlyakov Y. I., Fundamentals of the Theory of Groups, Graduate Texts in Mathematics, Springer-Verlag: New York.

Kurosh A. G., The Theory of Groups, Chelsea Publishing Co., New York, 1960

Hall M., The Theory of Groups, Chelsea Publishing Co., New York, 1976.

3

Complex numbers

In our high school mathematics curriculum, the set of numbers being studied kept gradually expanding. The reason for this was that such expansions gave more freedom in operating with numbers Thus, when we expand from the natural numbers to integers it is possible to subtract two numbers, when we expand to rational numbers it is possible to divide two numbers and so on. But the more useful result of such expansions is that the properties of the extended system often allow us to obtain new results about the original system. Thus, for instance, many difficult problems of number theory which concerning integers were solved with the use of real and even complex numbers.

Historically, complex numbers appeared just as a means for solving some problems about real numbers. For instance, the Italian mathematician Cardano (1501-1576) found real roots while solving cubic equations, using in the intermediate calculations, non-existent square roots of negative numbers.

In the course of time complex numbers occupied an ever more important place in mathematics and applications. First of all they were heavily used in the theory of algebraic equations, because the domain of complex numbers proved to be considerably more convenient for the study of such equations. For example, every algebraic equation of degree $n(n \geq 1)$ with real or complex coefficients has at least one complex root (see the fundamental theorem of algebra of complex numbers, page 55). At the same time not all algebraic equations with real coefficients have at least one real root.

After the interpretation of complex numbers as points and vectors in a plane, it became possible to apply geometric concepts such as continuity and geometric transformation to the study of complex numbers. The relation between complex numbers and vectors allowed to reduce many problems of mechanics to problems in complex numbers and their equations: especially hydrodynamics and aerodynamics and also the theory of electricity, thermodynamics, etc.

At present, the study of complex numbers has developed into a large and important division of contemporary mathematics - the theory of functions of complex variables.

The reader can expect to be introduced to a sufficiently indepth study of complex numbers and functions of complex variable.

3.1 Fields and polynomials

Real numbers can be added, multiplied, and inverse operations of subtraction and division are possible. In any addition of several numbers it is possible to arbitrarily swap terms and arbitrarily rearrange brackets without changing the result. The same holds true for products. All these properties and the relation between addition and multiplication can be briefly expressed as follows. The real numbers possess the following three properties:

a) They form a commutative group (see Chapter I, Section 3) under addition (the identity element of this group is denoted by 0 and is called zero).

b) If we exclude 0 the remaining numbers form a commutative group under multiplication.
c) Addition and multiplication are related with by distributivity: for any numbers a, b and c we have $a(b+c) = ab + ac$

The existence of these three properties is very important because they allow us to simplify arithmetical and algebraic expressions, to solve equations, etc. The set of real numbers is not the only set which possesses these three properties. A special concept is introduced to single out of all these sets in mathematics.

Definition 23 *If on a certain set two binary operations (addition and multiplication) are defined which possesses the above three properties, then this set is called a field.*

Problem-197 Are the following subsets of real numbers with the usual operations of addition and multiplication fields ? a) all natural numbers; b) all integers; c) all rational numbers; g) all numbers of form $r_1 + r_2\sqrt{2}$, where r_1 and r_2 are arbitrary rational numbers.
Problem-198 Prove that in any field $a \cdot 0 = 0 \cdot a = 0$ for any element a.
Problem-199 Prove that in any field: 1)$(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$, 2) $(-a) \cdot (-b) = ab$ for any elements a and b.
Problem-200 Let a, b be elements of an arbitrary field and $a \cdot b = 0$. Prove that either $a = 0$ or $b = 0$.
Example-14 Suppose that in the set $\{0, 1, \ldots, n\}$, besides the operation of addition modulo n (see example 9, page 20) we also have multiplication modulo n in which the result of multiplication of two numbers is the remainder under division by n.
Problem-201 To build tables of multiplication modulo 2, 3 and 4.
Problem-202 Prove that the remainders modulo n under the operations of addition and multiplication form a field *iff* n is prime number.

Definition 24 *By the difference between elements b and a in an arbitrary field (denoted $b - a$) we mean the element which solves the equation $x + a = b$ (or $a + x = b$). The quotient obtained by dividing element b by a for $a \neq 0$ (denoted by $\frac{b}{a}$) is the element which solves the equation $y \cdot a = b$ (or $a \cdot y = b$).*

From the result of problem 24 and the fact that addition and multiplication are commutative in a field, it follows that elements $b - a$ and $\frac{b}{a}$ (with $a \neq 0$) are uniquely determined in any field.
Since a field is a group under addition and if we exclude zero, under multiplication, the equation $x + a = b$ is equivalent to equation $x = b + (-a)$ and the equation $ya = b$ with $a \neq 0$ is equivalent to the equation $y = ba^{-1}$. Thus we have $b - a = b + (-a)$ and $\frac{b}{a} = ba^{-1}$
The reader can easily prove that the operations of addition, subtraction, multiplication and division in any field possess all the basic properties these operations have in the field of real numbers. In particular, in any field both sides of any equation can be multiplied or divided by any non-zero element; it is possible to take any term from one side to the other of the equation after a sign change and so forth. For example let us examine one of the properties which relates subtraction and multiplication.
Problem-203 Prove that in any field $(a - b)c = ac - bc$ for any elements a, b, c.
If K is a field, then just as for the real number field, it is possible to consider polynomials with coefficients from the field K or in other words polynomials over the field K.

Definition 25 *By a polynomial of degree n (n a natural number) in one variable x over the field K we mean any expression of the form*

$$a_0x^n + a_nx^{n-1} + \ldots + a_{n-1}x + a_n \tag{3.1}$$

where $a_0, a_1, \ldots, a_n \in K$ and $a_0 \neq 0$.

If a is an element of the field K, the expression a is also considered to be a polynomial over the field K. Moreover if $a \neq 0$, then this is a polynomial of degree zero, but if $a = 0$, then the degree of this polynomial is undefined.

Elements $a_0, a_1, \ldots, a_n$ are called the coefficients of the polynomial (**??**) and a_0 the leading coefficient. Two polynomials in variable x are considered to be equal $\iff$ their same degree coefficients are equal.

Let

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

If on the right side, we substitute for x a certain element a from the field K and carry out the calculations, i.e., the operations of addition and multiplication as operations in the field K, then the result will be a a certain element b from the field K. In this case write $P(a) = b$. If $P(a) = 0$, where 0 is the zero element of the field K, then a is called a root of the equation $P(x) = 0$; a is also called a root of the polynomial $P(x)$.

Polynomials over an arbitrary field K can be added, subtracted and multiplied.

The sum of the polynomials $P(x)$ and $Q(x)$ is the polynomial $R(x)$, in which the coefficient of $x^k (k = 0, 1, 2, \ldots)$ is equal to the sum (in the field K) of coefficients of x^k in the polynomials $P(x)$ and $Q(x)$. The difference of two polynomials is defined similarly. It is obvious that the degree of sum or difference in two polynomials is not more than maximum of the degrees of the two polynomials.

To calculate the product of two polynomials $P(x)$ and $Q(x)$, we multiply each term ax^k of the polynomial $P(x)$ by the term bx^l of the polynomial $Q(x)$ using the rule: $ax^kbx^l = abx^{l+k}$, where ab is the product in the field K, and $k+l$ the usual sum of integers. All the expressions obtained this way are added, i.e., collect all terms with the same degree r in variable x and substitute $d_1x^r + d_2x^r + ... + d_sx^r$ by the expression $(d_1 + d_2 + \ldots + d_s)x^r$.

Let

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$
$$Q(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{n-1}x + b_m,$$

then,

$$P(x) \cdot Q(x) = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + \ldots + a_nb_m{}^1$$

Since $a_0 \neq 0$ and $b_0 \neq 0$, the degree of the polynomial $P(x) \cdot Q(x)$ is equal to $n + m$, i.e., the degree of the product of two polynomials (different from 0) is equal to the sum of the degrees of each polynomial.

Taking into account that the operations of addition and multiplication of elements in the field K are commutative, associative and distributive, it is not difficult to verify that the operations of addition and multiplication of polynomials over the field K defined above are also commutative, associative and distributive.

If $P(x) + Q(x) = R_1(x), P(x) - Q(x) = R_2(x), P(x) \cdot Q(x) = R_3(x)$
and a is an arbitrary element of the field K, then is easy to see that $P(a)+Q(a) = R_1(a), P(a)-Q(a) = R_2(a), P(a) \cdot Q(a) = R_3(a)$

The polynomials over an arbitrary field K can be divided by one another with a remainder. To divide the polynomial $P(x)$ by the polynomial $Q(x)$ with a remainder means finding polynomials $S(x)$ (quotient) and $R(x)$ (remainder) such that $P(x) = S(x) \cdot Q(x) + R(x)$

Moreover the degree of the polynomial $R(x)$ must be less than the degree of the polynomial $Q(x)$, or $R(x) = 0$.

Let $P(x)$ and $Q(x)$ be arbitrary polynomials over the field K and $Q(x) \neq 0$. Let us show that it is possible to divide the polynomial $P(x)$ by the polynomial $Q(x)$ with a remainder. Let

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$
$$Q(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{n-1}x + b_m,$$

If $n < m$ choose $S(x) = 0$ and $R(x) = P(x)$ and we obtain the required quotient and remainder. If $n \geq m$, then consider the polynomial

$$P(x) - \frac{a_0}{b_0}x^{n-m}Q(x) = R_1(x)$$

$R_1(x)$ does not contain term x^n, therefore its degree is not more than $n-1$, or $R_1(x) = 0$. If

$$R_1(x) = c_0x^k + c_1x^{k-1} + \ldots + c_k$$

and $k \geq m$, consider the polynomial

$$R_1(x) - \frac{c_0}{b_0}x^{k-m}Q(x) = R_2(x), \text{ etc}$$

Since the degree of the polynomial obtained is strictly less than the degree of the previous polynomial this process must end, i.e. at a certain step we will obtain

$$R_{s-1}(x) - \frac{d_0}{b_0}x^{l-m}Q(x) = R_s(x)$$

and the degree of the polynomial $R_s(x)$ will be less than the degree of the polynomial $Q(x)$ or $R_s(x) = 0$. Then we obtain

$$\begin{aligned} P(x) &= \frac{a_0}{b_0}x^{n-m}Q(x) + R_1(x) \\ &= \frac{a_0}{b_0}x^{n-m}Q(x) + \frac{c_0}{b_0}x^{k-m}Q(x) + R_2(x) = \ldots \\ &= \frac{a_0}{b_0}x^{n-m}Q(x) + \frac{c_0}{b_0}x^{k-m}Q(x) + \ldots + \frac{d_0}{b_0}x^{l-m}Q(x) + R_s(x) \\ &= \left(\frac{a_0}{b_0}x^{n-m} + \frac{c_0}{b_0}x^{k-m} + \ldots + \frac{d_0}{b_0}x^{l-m}\right) \cdot Q(x) + R_s(x). \end{aligned}$$

Thus, the expression in the brackets is the quotient of the division of the polynomial $P(x)$ by $Q(x)$ and $R_s(x)$ the remainder. This method of dividing a polynomial by another polynomial is called the process of division by *Euclidean algorithm.*

The following problem shows that if $P(x)$ and $Q(x)$ are two polynomials and $Q(x) \neq 0$, then no matter how we divide $P(x)$ by $Q(x)$, the quotient and the remainder are uniquely defined.

Problem-204 Let

$$P(x) = S_1(x) \cdot Q(x) + R_1(x)$$
$$P(x) = S_2(x) \cdot Q(x) + R_2(x)$$

for which the degree of polynomials $R_1(x)$ and $R_2(x)$ are less than the degree of the polynomial $Q(x)$ (it could be the $R_1(x) = 0$ or $R_2(x) = 0$). Prove that $S_1(x) = S_2(x), R_1(x) = R_2(x)$.

3.2 The field of complex numbers

From the solution of problem 194 it follows that there exists fields, smaller than the field of real numbers; for example, the field of rational numbers. We will now construct a field larger than field of real numbers; namely, the field of complex numbers.
Consider all possible ordered pairs of real numbers, i.e., pairs of the form (a, b), where a and b are arbitrary real numbers. We will say that $(a, b) = (c, d) \iff a = b$ and $c = d$. In the set of all such pairs define two binary operations, addition and multiplication as follows:

$$(a, b) + (c, d) = (a + c, b + d) \tag{3.2}$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc) \tag{3.3}$$

(the operations within the right hand side brackets are the usual operations over the real numbers). For example, we obtain

$$(\sqrt{2}, 3) + (\sqrt{2}, 1) = (2\sqrt{2}, 2)$$
$$(0, 1) \cdot (0, 1) = (-1, 0)$$

Definition 26 *The set of all possible ordered pairs of real numbers with the operations of addition and multiplication defined by (3.2) and (3.3) is called the set of the complex numbers.*

From this definition it is clear that there is nothing "super-natural" about complex numbers: they actually exist as pairs of real numbers. However, the following question can arise: is it justifiable to call such objects numbers ? We will discuss this question at the end of this paragraph. Another question which the reader might raise is why are the operations of addition and multiplication for complex numbers (the operation of multiplication looks especially strange) defined like this and not in any other way ? We will answer this question in section 3.
Let us explain some good properties of the set of complex numbers defined above.
Problem-205 Prove that the complex numbers form a commutative group under addition. Which is the identity element (zero) of this group?
From now on, complex numbers will be denoted by one letter for convenience, for example z (or w).
Problem-206 Prove that the operation of the multiplication of complex numbers is commutative and associative, i.e. $z_1 \cdot z_2 = z_2 \cdot z_1$ and $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$ for any complex numbers z_1, z_2, z_3.
It is easy to verify that

$$(a, b) \cdot (1, 0) = (1, 0) \cdot (a, b) = (a, b)$$

for any complex number (a, b). Thus, the complex number $(1, 0)$ is the identity element in the set of the complex numbers under multiplication.
Problem-207 Let z be an arbitrary complex number and $z \neq (0, 0)$. Prove that there exists complex number z^{-1} such that

$$z \cdot z^{-1} = z^{-1} \cdot z = (1, 0).$$

The results of problems 203 and 204 show that the complex numbers form a commutative group under multiplication.
Problem-208 Prove that the operations of addition and multiplication of complex numbers possess the distributive law, i.e. $(z_1 + z_2) \cdot z_3 = z_1 \cdot z_3 + z_2 \cdot z_3$ for all complex numbers z_1, z_2, z_3.
From the results of problems 202-205, it follows that the complex numbers with the operations of addition and multiplication defined by (3.2) and (3.3) form a field. This is the field of complex numbers.

For the complex numbers of the type $(a,0)$, where a is an arbitrary real number, formulas (3.2) and (3.3) give

$$(a,0)+(b,0)=(a+b,0)$$
$$(a,0)\cdot(b,0)=(a\cdot b,0)$$

Thus, if we assign to each complex number of the form $(a,0)$ the real number a, then the operations on the numbers of the form $(a,0)$ will correspond to the usual operations on real numbers. Therefore we will simply identify the complex number $(a,0)$ with the real number a and [2] we will say that the field of the complex numbers includes field of real numbers.

The complex number $(0,1)$ is not real (under our identification) and we will denote it by i, i.e. $i=(0,1)$. Since the field of complex numbers does contain all real numbers and number i, it also contains numbers of the form $b\cdot i$ and $a+b\cdot i$, where a and b are arbitrary real numbers and the operations of addition and multiplication are understood as the operations on the complex numbers.

Problem-209 Let (a,b) be a complex number. Prove that $(a,b)=a+b\cdot i$.

From the result of task 206, we obtain that $a+b\cdot i=c+d\cdot i$ iff $a=b$ and $c=d$.

Thus, it is possible to represent any complex number uniquely in the form $a+b\cdot i$, where a and b are real numbers. If $z=a+b\cdot i$, then following historical traditions we call a the real part of the complex number z, $b\cdot i$ the imaginary part and b the coefficient of the imaginary part.

The representation of a complex number z in the form $z=a+b\cdot i$ is called the algebraic form of the complex number z.

Formulas (3.2) and (3.3) for complex numbers in algebraic form will be rewritten as follows.

$$(a+bi)+(c+di)=(a+c)+(b+d)i \tag{3.4}$$
$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i \tag{3.5}$$

Problem-210 Solve the equation (to find the formula for the difference)

$$(a+bi)+(x+yi)=c+di$$

Problem-211 Solve the equation (to find the formula for the quotient)

$$(a+bi)\cdot(x+yi)=c+di \text{ where } \quad a+bi\neq 0$$

It is easy to verify that $i\cdot i=(0,1)\cdot(0,1)=(-1,0)=-1$, i.e., $i^2=-1$. Thus, square roots of negative numbers are well defined in the field of complex numbers.

Problem-212 Calculate: a)i^3, b)i^4, c)i^n.

Problem-213 Find all complex numbers $z=x+yi$ such that: a)$z^2=1$, b)$z^2=-1$, c)$z^2=a^2$, d)$z^2=-a^2$ (where a is a real number).

Definition 27 *The complex number $a-bi$ is called the conjugate of the complex number $z=a+bi$ and is denoted by $\overline{z}$.*

It is easy to verify that

$$z+\overline{z}=2a,\ z\cdot\overline{z}=a^2+b^2$$

.

[2] Just as the rational number $\frac{n}{1}$ is identified with the integer n.

Problem-214 Let z_1 and z_2 be arbitrary complex numbers. Prove that: a) $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$, b)$\overline{z_1 - z_2} = \overline{z}_1 - \overline{z}_2$, c) $\overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2$, d)$\overline{\frac{z_1}{z_2}} = \frac{\overline{z}_1}{\overline{z}_2}$.

Problem-215 Let

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

where z is a complex number and all a_is are real numbers. Prove that $\overline{P(z)} = P(\overline{z})$.

The passage to complex numbers is a step in the sequence: natural numbers - integers - rational numbers - real numbers - complex numbers. The reader may form the opinion that upto real numbers one deals with numbers in reality and complex numbers are no longer numbers but objects of more complex nature. Of course, any terminology can be used. However, in reality complex numbers completely deserve to be called numbers.

The first objection against this can be the fact that this not a number but pairs of numbers. Recall however, that rational numbers introduced in a similar way (for example, see Kochetkov E. S., Kochetkova E. S., Algebra and Elementary Functions, h. I, publ. 10, education, 1975). A rational number is an equivalence class of fractions and a fraction is a pair of integers of the form $\frac{m}{n}$ (where $n \neq 0$); in this way the operations on rational numbers are simply operations on pairs of integers. Therefore the first objection seems unfounded. Another objection can be: how it is possible to measure something with this number ? If we look at it this way, then one must exclude for example, negative numbers from the set of numbers, since there are no segments with length -3 cm and a train cannot travel -4 hours. But if we think that numbers are objects using which it is possible (or convenient) to measure at least one quantity, then complex numbers aren't worse off than other numbers: using complex numbers, it is very convenient to describe, for example, currents, voltages and resistances in the electrical alternating current circuits and this widely is used in electrical engineering [3].

Thus, the passage from real numbers to complex numbers is as natural as, for example the passage from integers to rationals.

3.3 Uniqueness of the field of complex numbers

Let us now move on to examine the question as to why complex numbers were defined this way and not otherwise. The answer to this question is this: we want to get a field which is an extension of the real numbers. But is it not possible to construct another field which is also a field extension of the real numbers ? We will answer this question in this paragraph.

Definition 28 *By an isomorphic mapping (or simply an isomorphism) from one field to another we mean a one-to-one mapping φ which is an isomorphism relative to both addition and multiplication, i.e., $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$. Two fields are called isomorphic if its possible to establish an isomorphism between them.*

If in a field only the operations of addition and multiplication considered, then all isomorphic fields have identical properties. Therefore, just as in the case of groups, isomorphic fields cannot be distinguished.

As we saw in the previous paragraph, in the field of the complex numbers there is only element i such that $i^2 = -1$. The following problem shows that the addition of this element to the field of real numbers leads to the field of complex numbers.

Problem-216 Let M a certain field which contains the field of real numbers and a certain element i_0 such that $i_o^2 = -1$. Prove that M contains a certain field M' which is isomorphic to the field of complex numbers.

[3] See, for example, the theoretical bases of electrical engineering, in three volumes, pod.0bshchey.redaktsiyey Polivanova Pi. M., Vol. I. Polivanov k. M., linear electrical lumped circuits, energy, 1972,

We will say that a certain field is a minimal field with some properties if it possesses these properties and does not contain other fields with the same properties.
In this case the result of problem 213 can be formulated as follows: the minimum field which contains the field of real numbers and an element i_0 such that $i_0^2 = -1$ is the field of complex numbers. This result proves in a certain sense the uniqueness of the field of the complex numbers. However, there is a substantially stronger result. Namely, let us do away with the requirement that the field M contains an element i_0 such that $i_0^2 = -1$ and let us pose the problem of finding all fields which are the minimum field extensions of real numbers. It occurs that there are only two such expansions (upto isomorphism), one of them being the field of complex numbers. Let us prove this now.
Let the field M contain the field of real numbers i.e., M contains all real numbers and operations on them in the field M coincide with the usual operations on real numbers. Suppose moreover, the field M contains an element j different from all real numbers. Then the element equal to

$$j^n + a_1 j^{n-1} + \ldots + a_n \tag{3.6}$$

belongs to M for any real numbers $a_1, a_2, \ldots, a_n \in M$. We will call n the degree of expression (3.6).
There are two cases:
a) a certain expression of the form (3.6) with $n \geq 1$ is equal to 0;
b) no expression of the form (3.6) with $n \geq 1$ is equal to 0.
Let us assume that the first case is true.

Definition 29 *A polynomial with coefficients from a certain field K is called reducible above the field K if it can be represented as the product of two polynomials of smaller degree with coefficients from K. Otherwise it is called irreducible above the field K.* [4]

For example, polynomials $x^3 - 1$ and $x^2 - x - 1$ are reducible over the field of real numbers since $x^3 - 1 = (x-1)(x^2+x+1)$ and $x^2 - x - 1 = \left(x - \dfrac{1+\sqrt{5}}{2}\right)\left(x - \dfrac{1-\sqrt{5}}{2}\right)$,
and polynomials x^2+1 and x^2+x+1 are irreducible over the field of real numbers. It is obvious that polynomials of first degree above any field are irreducible.
Problem-217 Let us choose among all expressions of the form (3.6) equal to 0, the expression with the smallest degree n where $(n \geq 1)$. Let this be given by the expression

$$j^n + a_1 j^{n-1} + \ldots + a_n = 0$$

Prove that the polynomial

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

is irreducible over the field of real numbers.
In the sequel we will show (see 272) that any polynomial with real coefficients of degree greater than two is reducible over the field of real numbers. Therefore, the n in problem 214 cannot be more than 2. But since $n \neq 1$, (otherwise we would get $j + a = 0$ and j is equal to real number $-a$) we get that $n = 2$
Thus, in the case a) there exists some real numbers p and q in the field M such that the equation

$$j^2 + pj + q = 0$$

holds. Moreover the polynomial $x^2 + px + q$ must be irreducible over the field of real numbers.
Problem-218 Prove that in case a) the field M contains an element i_0 such that $i_0^2 = -1$.
It follows from the results of problems 215 and 213 that in the case a) the field M contains a field M' isomorphic to the field of complex numbers. Hence, if the field M is the minimal field extension of

[4] Ireducible polynomials over the field K are the analogue of prime numbers in the set of integers.

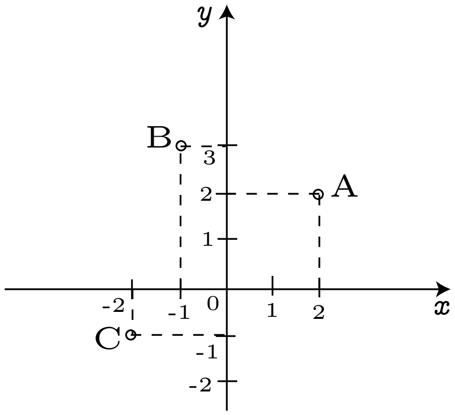


Fig. 3.1.

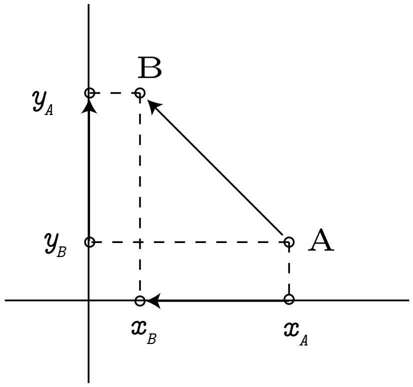


Fig. 3.2.

real numbers, then field M must coincide with M'. Thus, in the case a) any field which is the minimal field extension of the real numbers coincides (i.e. is isomorphic) to the field of complex numbers. Thus, in case a) there is a unique (upto isomorphism) field which is the minimal field extension of real numbers, namely, the field of complex numbers.

Problem-219 Find all fields which are the minimal field extensions of real numbers in the case b).

3.4 Geometric description of complex numbers

Introduce on the plane a rectangular coordinate system XOY and associate to each complex number $a + bi$ the point in the plane with coordinates (a, b). We will obtain a one-to-one correspondence between all complex numbers and all points of the plane. This introduces us to the first geometric idea of complex numbers.

Problem-220 What complex numbers correspond to the points indicated in Fig. 3.1

Problem-221 Let the complex numbers be depicted as the points of plane. What is the geometric meaning of the transformation φ, if for any complex number z: a)$\varphi(z) = -z$, b)$\varphi(z) = 2z$, c)$\varphi(z) = \overline{z}$ ($\overline{z}$ is the complex conjugate of z).

Let $A(x_A, y_A)$ and $B(x_B, y_B)$ be two points in the plane (Fig. 3.2). The ray AB directed from A to B as shown is called the vector $\overrightarrow{AB}$. The coordinates of the vector $\overrightarrow{AB}$ are calculated as follows: $x_{\overrightarrow{AB}} = x_B - x_A$, $y_{\overrightarrow{AB}} = y_B - y_A$. Two vectors are considered equal, if they are parallel, in the same direction and of equal length.

Problem-222 Prove that two vectors are equal $\iff$ their corresponding coordinates are equal.

The so-called "free vectors" is the set of equal vectors usually considered as one and the same vector and characterized only by its coordinates. After assigning to each complex number $a + bi$ the free vector with the coordinates (a, b), we get the second geometric idea of complex numbers.

Problem-223 Assign to each complex number z_1, z_2 and z_3 the corresponding free vectors u, v and w. Prove that $z_1 + z_2 = z_3 \iff u + v = w$, where the sum of vectors is calculated using the parallelogram law.

Problem-224 Prove the following relationship between the two geometric ideas of complex number: if z_1, z_2 and $z_{\overrightarrow{AB}}$ are complex numbers which correspond to points A, B and to vector $\overrightarrow{AB}$, then $z_{\overrightarrow{AB}} = z_B - z_A$.
From the definition of equal vectors we obtain that equal vectors have equal length. This length is equal to the length of the free vector which corresponds to this set of equal vectors.

Definition 30 *The magnitude or modulus of a complex number z (denoted by $|z|$) is called the length of the corresponding free vector.*[5]

Problem-225 If $z = a + bi$. Prove that

$$|z|^2 = a^2 + b^2 = z \cdot \overline{z}$$

where $\overline{z}$ is the complex conjugate of z.
Problem-226 Prove the inequalities:

$$|z_1 + z_2| \leq |z|_1 + |z|_2$$
$$|z_1 - z_2| \geq \Big||z|_1 - |z|_2\Big|$$

where z_1, z_2 are arbitrary complex numbers. In what cases does the equality occur ?
Problem-227 Prove with the aid of complex numbers that in an arbitrary parallelogram the sum of the squares of lengths of the diagonals is equal to the sum of the squares of the lengths of all sides.

3.5 Trigonometric form of complex numbers

Let us recall that the angle between the rays OA and OB about O is the angle, required to rotate ray OA about the point O counterclockwise in order to get to the ray OB (if the rotation is done clockwise, then the angle is assigned a "minus" sign). In this case the angle is not uniquely determined but upto rotations by $2k\pi$ where k any integer.
Let point O be the origin of coordinates and let the vector OA with the coordinates (a, b) correspond to the complex number $z = a + bi$ (Fig. 3.3). The argument of the complex number z (denoted Arg z) is the angle between the positive direction of axis OX and the ray OA (Fig. 3.3) (if $z = 0$, then Arg z is not defined).
Since for $z \neq 0$ the angle is not defined uniquely, by Arg z we mean a many-valued function which assumes for each $z \neq 0$ the infinite set of the values whose difference is an integral multiple of 2π.
By Arg $z = \varphi$ we will mean one of the values of the argument equal to φ.
Let $z = a + bi \neq 0$ and $|z| = r$. The vector $\overrightarrow{OA}$ with coordinates (a, b) correspond to the complex number $a+bi$ and therefore its length is equal to r. Let furthermore Arg $z = \varphi$. Then by the definition of trigonometric functions (see Fig. 3.3)

$$\cos\varphi = \frac{a}{r}, \ \ \sin\varphi = \frac{b}{r}$$

Hence

[5] For the real numbers (as a special case of the complex numbers) the concept of magnitude introduced above coincides with the usual concept of absolute value. In fact, the real number $a + 0i$ corresponds to the vector with coordinates $(a, 0)$, parallel to the X-axis and length equal to $|a|$ - to the absolute value of the number a.

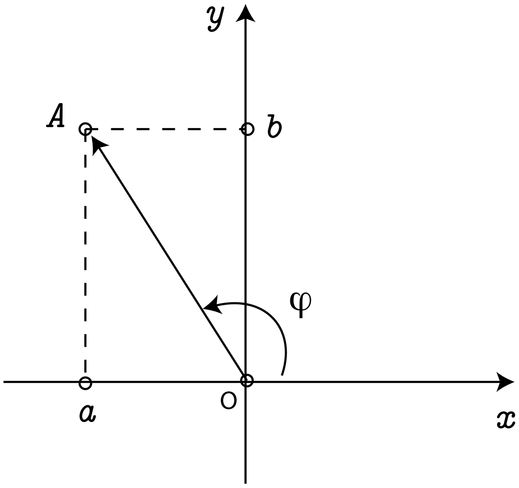


Fig. 3.3.

$$z = a + bi = r \cdot \cos\varphi + i \cdot r \cdot \sin\varphi =$$
$$= r(\cos\varphi + i\sin\varphi),$$

where $r = |z|, \varphi = \mathrm{Arg} z$ and we have obtained the *trigonometric form* of the complex number z. For example, if $z = -1\sqrt{3}i$, then $|z| = \sqrt{1+3} = 2$ (see 222) and $\cos\varphi = -\dfrac{1}{2}$, $\sin\varphi = \dfrac{\sqrt{3}}{2}$. If we take $\varphi = \dfrac{2\pi}{3}$, then $z = -1 + \sqrt{3}i = 2\left(\cos\dfrac{2\pi}{3} + i\sin\dfrac{2\pi}{3}\right)$.

Problem-228 Represent in trigonometric form the following complex numbers: a) $1+i$, b)$-\sqrt{3}-i$, c)$3i$, d)-5, e)$1+2i$.

Problem-229 If $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ and $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Prove that,

$$z_1 \cdot z_2 = r_1 r_2 \left(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)\right),$$
$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\left(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)\right) \quad (z_2 \neq 0).$$

Thus, under multiplication of complex numbers, their magnitudes are multiplied and arguments are added and under division their magnitudes are divided and their arguments are subtracted.

Problem-230 Prove the De Moivre formula [6]:

$$[r(\cos\varphi + i\sin\varphi)]^n = r^n(\cos n\varphi + i\sin n\varphi)$$

for every integer $n > 0$.

Problem-231 Compute $\dfrac{(1-\sqrt{3}i)^{100}}{2^{100}}$.

Problem-232 If $z = r(\cos\varphi + i\sin\varphi)$ is a fixed complex number and n a natural number, find all complex numbers w which satisfy the equality

[6] A. de Moivre (1667-1754) was a French mathematician who lived in England

$$w^n = z \tag{3.7}$$

Definition 31 *The expression* $\sqrt[n]{z}$ *(* n^{th} *root of* z *), denotes a many-valued function which assigns to each complex number* $z \neq 0$ *the solutions of equation (3.7) for all* n*.*

If $z = 0$, then $\sqrt[n]{0} = 0$.
Problem-233 Find all values of the roots: a)$\sqrt{-1}$, b)$\sqrt[3]{8}$, c)$\sqrt[4]{\cos 100^\circ + i \sin 100^\circ}$ d)$\sqrt[3]{1+i}$.
For future purposes it will be convenient to introduce the following notation:

$$\varepsilon_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

Problem-234 Prove that all the values of $\sqrt[n]{-1}$ are $1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}$.
Observation. Since $\varepsilon_n^n = 1$ *the set of elements* $1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}$ *form a cyclic group under multiplication.*
Problem-235 Let z_1 be one of the values of $\sqrt[n]{z_0}$. Find all the values of $\sqrt[n]{z_0}$.
From now on, we will represent complex numbers as points in a plane, i.e., to the complex number $z = a + bi$ we will assign the point with coordinates (a, b). In this case instead of the point which corresponds to the complex number z we will speak simply of the point z.
Problem-236 Let the complex numbers be depicted as the points of plane. Make geometric sense of the expressions: a)$|z|$, b)Arg z, c)$|z_1 - z_2|$, d) Arg $\dfrac{z_1}{z_2}$?
Problem-237 Find the locus z, which satisfy the following conditions (z_1, z_2, z_3 are fixed complex numbers and R a fixed real number): a)$|z| = 1$, b)$|z| = R$, c) $|z - z_0| = R$, d)$|z - z_0| \leq R$, e)$|z - z_1| = |z - z_2|$, f)Arg $z = \pi$, g)Arg $z = \dfrac{9\pi}{4}$, h)Arg $z = \varphi$.
Problem-238 Where are all the values of $\sqrt[n]{z}$ located on the plane, where z is a fixed complex number.

3.6 Continuity

The notion of continuity will play an important role for us from now on and in particular the notion of a smooth curve. The reader who doesn't know the rigourous definition of these concepts, nevertheless understands intuitively what a smooth curve is and what a continuous function of a real variable is (intuitively, it is possible to say that this is function which has a smooth curve as its graph). However, if the function is fairly complicated (for example $f(x) = \dfrac{x^3 - 2x}{x^2 - \sin x + 1}$) then to conclude it is continuous using only intuition is quite difficult. Therefore, we will give a rigourous definition of continuity and with it's help prove several basic properties of continuous functions. In this case we will give the definition of continuity both for functions of real argument and for functions of complex argument.
Consider the graph of a function with real argument. Then this graph can be continuous at some points and at some points it can have gaps. Therefore it is natural to first introduce the definition of continuity of a function at a particular point rather than the general definition of continuity.
If we try to define more precisely our intuitive idea about the continuity of a function $f(x)$ at a particular point x_0 then we see that continuity means the following: with small changes in the argument near point x_0 the change in the function is also small with respect to the value $f(x_0)$. Moreover it is possible to obtain as small a change in the value of the function about $f(x_0)$ by choosing a sufficiently small interval of variation for the argument around x_0. It is possible to formulate it rigourously as follows.
indexcontinuous function

Definition 32 *Let $f(z)$ be a function of a real or complex variable z. The function $f(z)$ is continuous at a point z_0, if for any real number $\varepsilon > 0$, it is possible to select a real number $\delta > 0$ (depending on z_0 and ε), such that for all numbers z, which satisfy the condition $|z - z_0| < \delta$, we have $|f(z) - f(z_0)| < \varepsilon$.* [7]

Example-15 Let us prove that the function with complex argument $f(z) = 2z$ is continuous at any point z_0. Let the point z_0 and an arbitrary real number $\varepsilon > 0$ be given. We have to choose this real number $\delta > 0$ such that for all numbers z which satisfy the condition $|z - z_0| < \delta$ the inequality $|f(z) - f(z_0)| = |2z - 2z_0| < \varepsilon$ is satisfied. It is not difficult to see that it is possible to choose $\delta = \frac{\varepsilon}{2}$ (independent of point z_0). Indeed, from the condition $|z - z_0| < \delta$ it follows that:

$$|2z - 2z_0| = |2(z - z_0)| = \text{see } 226 = |2||z - z_0| < 2\delta = \varepsilon$$

i.e., $|2z - 2z_0| < \varepsilon$. Therefore, the function $f(z) = 2z$ is continuous at any point z_0. In particular, it is continuous for all real values of the argument z. Therefore, if we limit ourselves to only real valued arguments, we see that the function with real argument $f(x) = 2x$ is continuous for all real values x.

Problem-239 Let a be a fixed complex (or, as a particular case, real) number. Prove that the function with complex (or real) argument $f(z) = a$ is continuous for all values of the argument.

Problem-240 Prove that the function with complex argument $f(z) = z$ and the function with real argument $f(x) = x$ are continuous for all values of the argument.

Problem-241 Prove that the function with complex argument $f(z) = z^2$ is continuous with all values of the argument z.

Definition 33 *Let $f(z)$ and $g(z)$ be two functions of a complex (or real) argument. The function with complex (or real) argument $h(z)$, which is called the sum of the functions $f(z)$ and $g(z)$, satisfies at each point z_0 the equation $h(z_0) = f(z_0) + g(z_0)$ holds. In case the value of $f(z_0)$ or $g(z_0)$ is not defined then the value of $h(z_0)$ is also not defined. In the same way one defines the difference, product and quotient of two functions.*

Problem-242 Let the functions $f(z)$ and $g(z)$ of complex (or real) argument be continuous at the point z_0. Prove that the functions: a)$h(z) = f(z) + g(z)$, b)$h(z) = f(z) - g(z)$, c)$h(z) = f(z) \cdot g(z)$ are continuous at z_0.

From the result of problem 239(c) we obtain, in particular, that if the function $f(z)$ is continuous at a point z_0 and n is a natural number then the function $[f(z)]^n$ is also continuous at the point z_0.

Problem-243 Let the functions $f(z)$ and $g(z)$ with complex or real argument be continuous at point z_0 and $g(z_0) \neq 0$. Prove that the functions: a)$h(z) = \frac{1}{g(z)}$, b) $h(z) = \frac{f(z)}{g(z)}$ are continuous at the point z_0.

Definition 34 *Let $f(z)$ and $g(z)$ be two functions with complex or real argument. The function $h(z)$ which is called the composition of functions $f(z)$ and $g(z)$ satisfies at each point z_0 the equation $h(z_0) = f(g(z_0))$. In case $g(z)$ is not defined at z_0 or the function $f(z)$ is not defined at the point $g(z_0)$ then $h(z_0)$ is also not defined.*

Problem-244 Let $f(z)$ and $g(z)$ be functions with complex or real argument. Let $g(z_0) = z_1$ and let the function $g(z)$ be continuous at point z_0 and the function $f(z)$ be continuous at the point z_1. Prove that the function $h(z) = f(g(z))$ is continuous at the point z_0.

From the results of the problems 239-241 it follows that if a certain expression is built from several continuous functions with complex (or real) argument using the operations of addition, subtraction,

[7] The geometric meaning of the inequalities $|z - z_0| < \delta$ and $|f(z) - f(z_0)| < \varepsilon$ is given in problems 233 and 234).

multiplication, division, raising to a natural power and composition, then the obtained expression will also be a continuous function whenever none of it's denominator vanish.
For example, from the results of problems 236 and 237 we obtain that the function $f(z) = z^n, f(z) = az^n$ and in general $f(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_n$ are continuous functions of z for any complex numbers $a, a_0, a_1, \ldots, a_n$.
Problem-245 Prove that the functions with real argument $f(x) = \sin x$ and $f(x) = \cos x$ are continuous for all values of x.
Problem-246 Consider for all real values $x \geq 0$ the function $f(x) = \sqrt[n]{x}$, where n a non-zero integer and $\sqrt[n]{x}$ is taken to be non-negative. Prove that this function is continuous for all $x > 0$.
During the study of continuity it is necessary to be contended with some statements, which intuitively seem completely obvious but a strict proof is technically difficult and requires a definition of real numbers more rigourous than that done in school, as well as the study of principles of set treory and topology.
The following statement serves as an example: if a function with real argument $f(x)$ is continuous in a certain interval and takes only integer values in this interval, then it takes one and the same value in the entire interval. It seems intuitively obvious that during the motion of point x along the interval the value of the function $f(x)$ must change continuously and cannot "jump" from one integer value into another. However, to prove this assertion strictly is quite difficult.
In the following presentation we will be more oriented toward the intuition of the reader and we will accept several "intuitively clear" statements related to continuity without a proof. In particular, we will accept the statement formulated above as an example without proof. A rigourous proof of this statement can be found, for example, in the book: Steenrod N. and Chinn U., First concepts of topology, Mir, 1967.

3.7 Continuous curves

Let the parameter t take real values in the interval $0 \leq t \leq 1$ and let a certain complex number be assigned to each such value t as

$$z(t) = x(t) + iy(t)$$

We will henceforth call the plane on which the values z are depicted as "z plane". If the function $x(t)$ and $y(t)$ are continuous for $0 \leq t \leq 1$, then as t goes from 0 to 1 the point $z(t)$ will describe a certain continuous curve in the z plane. We will consider this curve with a direction, taking the point $z_0 = z(0)$ to be the initial point and the point $z_1 = z(1)$ to be the the final point. We will call the function $z(t)$ the parametric equation of this curve.
Example-16 Let $z(t) = t + it^2$.Then $x(t) = t$ and $y(t) = t^2$. Therefore $y(t) = x^2(t)$ for any t, i.e. the point $z(t)$ for any t lies on the parabola $y = x^2$. As t varies from 0 to 1 $x(t)$ also varies from 0 to 1 and the point $z(t)$ traces the arc of the parabola $y = x^2$ from the point $z_0 = 0$ to the point $z_1 = 1 + i$ (Fig. 3.4).
Problem-247 Construct on the z plane the curves given by the following parametric equations: a)$z(t) = 2t$, b)$z(t) = it$, c)$z(t) = it^2$, d)$z(t) = t - it$, e)$z(t) = t^2 + it$, f)$z(t) = R(\cos 2\pi t + i \sin 2\pi t)$, g)$z(t) = R(\cos 4\pi t + i \sin 4\pi t)$, h)$z(t) = R(\cos \pi t + i \sin \pi t)$, and i)

$$z(t) = \begin{cases} \cos 2\pi t + i \sin 2\pi t & \text{for } 0 \leq t \leq \dfrac{1}{2} \\ 4t - 3 & \text{for } \dfrac{1}{2} < t \leq 1 \end{cases}$$

Problem-248 Write a parametric equation for the segment joining the points $z_0 = a_0 + b_0 i$ and $z_1 = a_1 + b_1 i$.

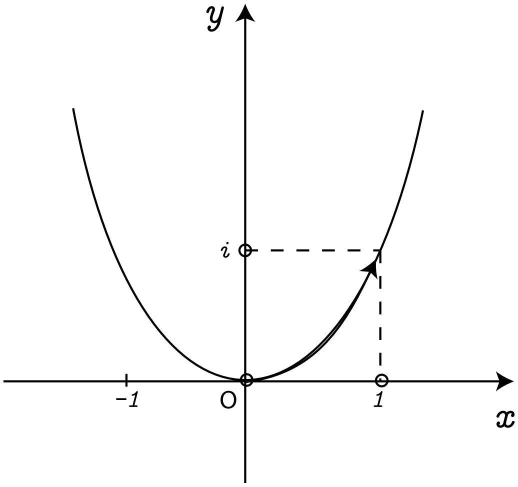


Fig. 3.4.

Observation.In the following problems the parametric equations have some labels. These numbers indicate the label of the curve, and they all lie in the same z plane.

Problem-249 What geometric transformations takes the curve C_1 with equation $z_1(t)$ to the curve C_2 with equation $z_2(t)$, if

a) $z_2(t) = z_1(t) + z_0$ (z_0 is a fixed complex number).
b) $z_2(t) = a \cdot z_1(t)$ (where a is a the real positive number).
c) $z_2(t) = z_0 \cdot z_1(t)$, where $|z_0| = 1$
d) $z_2(t) = z_0 \cdot z_1(t)$ where z_0 is a fixed complex number

Problem-250 Let $z_1(t)$ be a parametric equation of the curve C. What curve is described by the equation $z_2(t)$ if $z_2(t) = z_1(1-t)$?

Problem-251 Let $z_1(t)$ and $z_2(t)$ be parametric equations of the curves C_1 and C_2 and let $z_1(1) = z_2(0)$. What curve is described by the equation $z_3(t)$ if:

$$z_3(t) = \begin{cases} z_1(2t) & \text{for } 0 \leq t \leq \dfrac{1}{2} \\ z_2(2t-1) & \text{for} \dfrac{1}{2} < t \leq 1? \end{cases}$$

Problem-252 Let $z(t) = \cos \pi t + i \sin \pi t$ (Fig. 3.5). Find all values of Arg $z(t)$ as a function of t.

Problem-253 Let $z(t) = \cos \pi t + i \sin \pi t$. Select one of the values of Arg $z(t)$ for each t so that the selected values vary continuously as t varies from 0 to 1 if Arg $z(0)$ is chosen to be: a)0, b)2π, c)-4π, d) $2\pi k$ (k is a fixed integer)

The following statement seems intuitively quite obvious and we will state it without a proof.

Theorem 3.1 *Assume that a continuous curve C with parametric equation $z(t)$ not pass through the origin of coordinates (i.e. $z(t) \neq 0$ with $0 \leq t \leq 1$) and let the argument of initial point of curve C (i.e. Arg $z(0)$) be chosen to be equal to φ_0. Then it is possible to select one of the values of the*

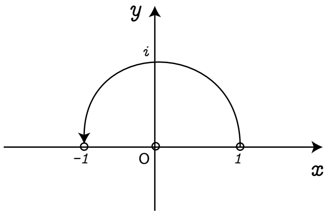


Fig. 3.5.

argument for all the points on the curve C such that along the entire curve its argument changes continuously starting from the value φ_0.

In other words, one can choose for each t one of the values $\varphi(t)$ of Arg $z(t)$ so that the function $\varphi(t)$ is continuous for $0 \leq t \leq 1$ and $\varphi(0) = \varphi_0$ [8].

Problem-254 Let $\varphi(t)$ and $\varphi'(t)$ be two functions which describes a continuous change in Arg $z(t)$ along the curve C. Prove that $\varphi(t) - \varphi'(t) = 2\pi k$ where k is a fixed integer which does not depend on t.

Problem-255 Prove that if a certain value $\varphi(0) = \varphi_0$ is chosen, then the function $\varphi(t)$ which describes a continuous change in Arg $z(t)$ along the curve C is uniquely defined.

Problem-256 Let the function $\varphi(t)$ describe a continuous change in Arg $z(t)$. Prove that the function $\psi(t) = \varphi(t) - \varphi(0)$is uniquely defined by the function $z(t)$ and does not depend on the selection $\varphi(0)$. From the statement of problem 253 it follows, in particular for $t = 1$, that for a continuous curve C not passing through the point $z = 0$, the value $\varphi(1) - \varphi(0)$ is uniquely defined by the condition that $\varphi(t)$ is continuous.

Definition 35 *We will call the value $\varphi(1) - \varphi(0)$ the change in the argument along the curve C.*

Problem-257 What is the change in the argument along the curves with the following parametric equations:
a) $z(t) = \cos \pi t + i \sin \pi t$,
b) $z(t) = \cos 2\pi t + i \sin 2\pi t$,
c) $z(t) = \cos 4\pi t + i \sin 4\pi t$,
d) $z(t) = (1 - t) + it$

Problem-258 What is the change in the argument along the curves depicted in Fig. 3.6
If a continuous curve C is closed, i.e. $z(1) = z(0)$, then the value $\varphi(1) - \varphi(0)$ does have the form $2\pi k$ where k is an integer.

Definition 36 *If for a continuous closed curve C not passing through the point $z = 0$ the change in the argument equals $2\pi k$, then we will say that the curve C goes around the point $z = 0$ k times.*

Problem-259 How many times do the following curves go around the point $z = 0$:
a) $z(t) = 2 \cos 2\pi t + 2i \sin 2\pi t$, (Fig. 3.7)
b) $z(t) = \frac{1}{2} \cos 4\pi t - \frac{1}{2} i \sin 4\pi t$ (Fig 3.8)
c) Curve in Fig. 3.9
d) Curve in Fig. 3.10

[8] In the book Steenrod N., Chinn W.G., First Concepts of Topology, "Mir",1967,20-23, the angle swept by this curve is rigourously defined. Using this angle, it is easy to obtain the assertion of theorem 6: it suffices to consider $\varphi(t) = \varphi_0 + \varphi_1(t)$ where $\varphi_1(t)$ is the angle swept by the part of this curve from $z(0)$ to $z(t)$.

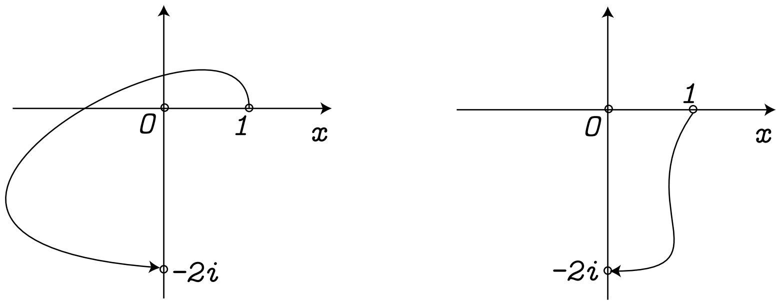


Fig. 3.6.

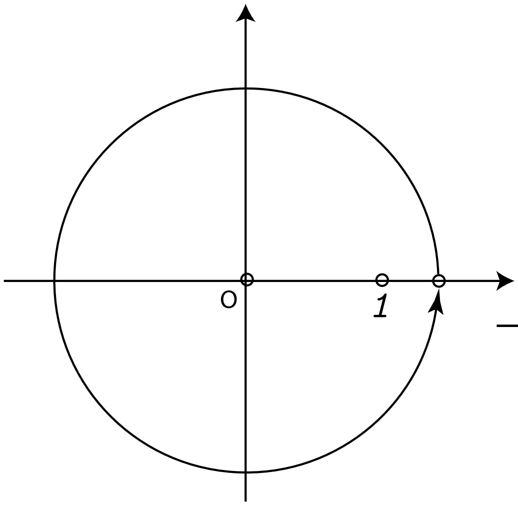


Fig. 3.7.

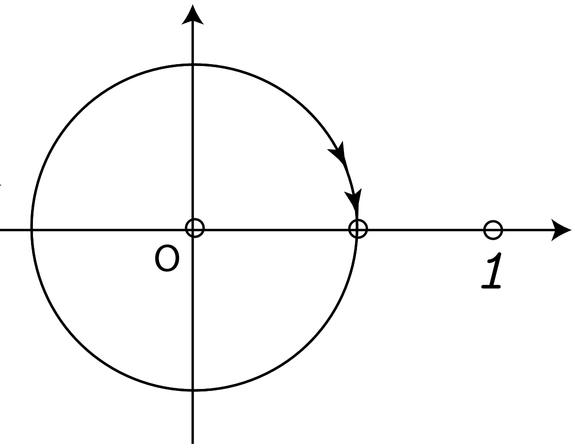


Fig. 3.8.

Problem-260 Prove that the number of turns of a continuous closed curve around the point of $z = 0$ does not depend on the selection of initial point but depends only on the direction of curve.

Problem-261 Let the curve C with equation $z_1(t)$ go around the point $z = 0$ k times. How often do the curve with the equation $z_2(t)$, go around the point $z = 0$ if: a) $z_2(t) = 2z_1(t)$, b)$z_2(t) = -z_1(t)$, c)$z_2(t) = z_0 \cdot z_1(t)$, where $z_0 \neq 0$, d) $z_2(t) = \overline{z}_1(t)$ where $\overline{z}$ is the complex conjugate of z?

Let the closed smooth curve C with equation $z_1(t)$ not pass through the point $z = 0$. Then we will say that the curve C goes around the point $z = z_0$ once if the curve with equation $z_2(t) = z_1(t) - z_0$ goes around the point $z = 0$ once (Fig. 3.11).

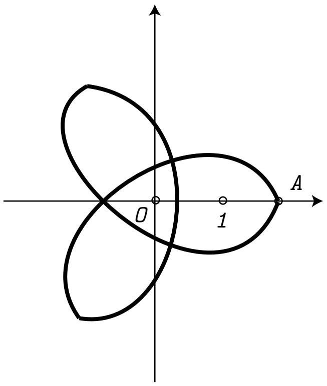


Fig. 3.9.

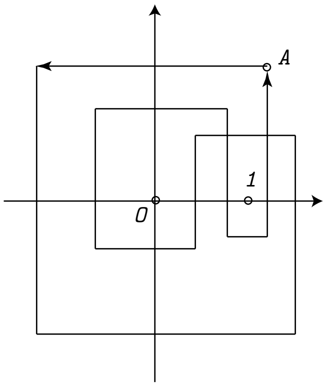


Fig. 3.10.

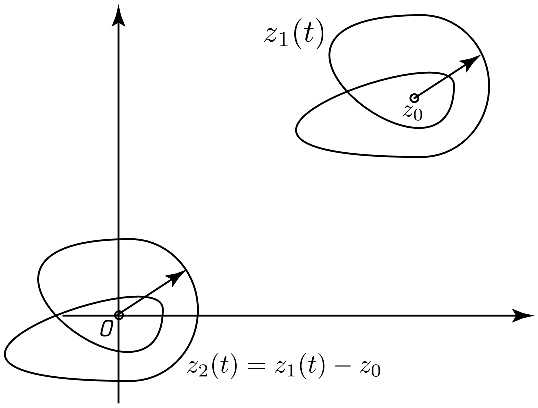


Fig. 3.11.

Thus, to define the number of turns of a curve around the point $z = z_0$ it is necessary to follow the rotation of the vector $z_1(t) - z_0$ which can be considered as the vector which connects the points z_0 and $z_t(t)$ (see 221).

Problem-262 How many times do the curves described in problem 256 go around the point $z = 1$?

Problem-263 Let $z_1(t)$ and $z_2(t)$ be the equations of two curves C_1 and C_2 not passing through the point $z = 0$. Let the changes in the argument along these curves be ϕ_1 and ϕ_2 respectively. What is the change in the argument along the curve C with equation $z(t)$ if: a) $z(t) = z_1(t) \cdot z_2(t)$, b) $z(t) = \dfrac{z_1(t)}{z_2(t)}$?

3.8 Images of curves: the fundamental theorem of the algebra of complex numbers

Consider two planes of complex numbers: the z plane and w plane, and assume that a function $w = f(z)$ is defined which to each value z assigns in a unique way, the value w. If on z plane there is continuous curve C with equation $z(t)$, then by the function $w = f(z)$ every point of this curve is sent to a point in the w plane. If the function $f(z)$ is continuous, then we will obtain a continuous curve in the w plane with equation $w_0(t) = f(z(t))$. We will denote this curve by $f(C)$, which is the image of the curve C.

Problem-264 What is the curve $f(C)$ if $w = f(z) = z^2$ and the curve C is:

a) quadrant: $z(t) = R(\cos\frac{\pi t}{2} + i\sin\frac{\pi t}{2})$,
b) the semicircle: $z(t) = R(\cos\pi t + i\sin\pi t)$,
c) the circle: $z(t) = R(\cos 2\pi t + i\sin 2\pi t)$

Problem-265 Let the change in the argument along a curve be equal to φ. What is the change in the argument along the curve $f(C)$ if: a) $f(z) = z^2$, b) $f(z) = z^3$, c) $f(z) = z^n$, where n arbitrary integer?

Problem-266 Suppose the curve C goes around the point $z = z_0$ k times . How many times does the curve $f(C)$ go around the point $w = 0$ if $f(z) = (z - z_0)^n$?

Problem-267 Let the curve C go around around the points $z = 0$, $z = 1$,$z = i$,$z = -i$ k_1, k_2, k_3, k_4 times respectively . How many times does the curve $f(C)$ go around point $w = 0$ if: a) $f(z) = z^2 - z$, b) $f(z) = z^2 + 1$, c) $f(z) = (z^2 + +iz)^4$, g) $f(z) = z^3 - z^2 - z - 1$?

Consider the equation

$$a_0 z^n + a_1 z^{n-1} + \ldots + a_n = 0$$

where all a_is are arbitrary complex numbers, $n \geq 1$ and $a_0 \neq 0$. Our immediate objective to show that this equation has at least one complex root. From now on we will assume that $a_n \neq 0$.

Let us denote the maximum of the numbers $|a_0|, |a_1|, \ldots, |a_n|$ by A. Since $a_0 \neq 0$, $A > 0$. Choose two positive real numbers R_1 and R_2 such that: R_1 is small enough that the two inequalities: $R_1 \leq 1$ and $R_1 < \frac{|a_n|}{10An}$ are satisfied; and R_2 so large that the two inequalities: $R_2 \geq 1$ and $R_2 > \frac{10An}{|a_0|}$ are also satisfied.

Problem-268 Let $|z| = R_1$. Prove that $|a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1} z| < \frac{|a|_n}{10}$

Problem-269 Let $|z| = R_2$. Prove that $|\frac{a_1}{z} + \ldots + \frac{a_n}{z}| < \frac{|a|_0}{10}$

Let us denote by C_R the curve with equation $z(t) = R(\cos 2\pi + i\sin of 2\pi t)$ (i.e. the circle with radius R oriented counterclockwise). Since the curve C_R is closed ($z(1) = z(0)$), the curve $f(C_R)$, where $f(z) = a_0 z^n + \ldots + a_n$ is also closed ($f(z(1)) = f(z(0))$). Let $\nu(R)$ be the number of turns of the curve $f(C_R)$ around the point $w = 0$ (if $f(C_R)$ does not pass through point $w = 0$).

Problem-270 What are the values of $\nu(R_1)$ and $\nu(R_2)$?

We will now change the radius R from R_1 to R_2 continuously. In this case the curve $f(C_R)$ will be continuously deformed from $f(C_{R_1})$ to $f(C_{R_2})$. If for a certain value of R^* the curve $f(C_{R^*})$ does not pass through point $w = 0$, then for a sufficiently small change in R near R^* the curve $f(C_R)$ will be deformed by a small amount such that the number of turns it makes around the point $w = 0$ will not change, i.e., the function $\nu(R)$ is continuous at this value R^*. If the curves $f(C_R)$ for all the values R such that $R_1 \leq R \leq R_2$ does not pass through the point $w = 0$, then $\nu(R)$ will be a continuous function for all $R_1 \leq R \leq R_2$. Since the function $\nu(R)$ takes only integer values, it can be continuous only if $\nu(R)$ a unique value for all R in the interval $R_1 \leq R \leq R_2$; in particular $\nu(R_1) = \nu(R_2)$. But it follows from the solution of problem 267 that $\nu(R_1) = 0$, a $\nu(R_2) = n$. Hence, the assumption that the curves $f(C_R)$ for all $R_1 \leq R \leq R_2$ do not pass through the point $w = 0$ is erroneous. This means that for a certain z, $f(z) = 0$. Thus we obtain the following theorem[9] .

Theorem 3.2 (The fundamental theorem of the algebra of complex numbers [10]) *The equation $a_0z^n + \ldots + a_n = 0$ with each a_i an arbitrary complex numbers, $n \geq 1$ and $a_0 \neq 0$, has at least one complex root.*

Problem-271 Prove Bezout's theorem [11]: If z_0 is a root of the equation $a_0z^n + \ldots + a_n = 0$, then the polynomial $a_0z^n + \ldots + a_n$ is divisible by $z - z_0$ without a remainder.

Problem-272 Prove that the polynomial $a_0z^n + \ldots + a_n$ where $a_0 \neq 0$ can be represented in the form

$$a_0z^n + \ldots + a_n = a_0(z - z_1)(z - z_2) \cdot \ldots \cdot (z - z_n)$$

Observation. Assume that polynomial P(z) is decomposed into factors:

$$P(z) = a_0(z - z_1)(z - z_2) \cdot \ldots \cdot (z - z_n)$$

The right side is equal to 0 $\iff$ at least one of the factors is equal to 0 (see 195, 197). Therefore the roots of the equation $P(z) = 0$ are the numbers $z_1, z_2, \ldots, z_n$ and them alone.

Problem-273 Let z_0 be a root of the equation $a_0z^n + \ldots + a_n = 0$ where all a_is are real numbers. Prove that the number $\overline{z}_0$, the conjugate of z_0 is also a root of this equation.

Problem-274 Suppose that the equation $a_0z^n + \ldots + a_n = 0$ with real coefficients has a complex root z_0 which is not a pure real number. Prove that polynomial $a_0z^n + \ldots + a_n$ has a polynomial of second degree with real coefficients as a factor.

Problem-275 Prove that any polynomial with real coefficients can be represented in the form of a product of polynomials of first and second degree with the real coefficients.

Observation. It follows that from the result of task 272 that the only irreducible polynomials (see page 44) over the field of real numbers are the polynomials of first and second degree with no real roots. We did use this in section 3 of this chapter. Over the field of complex numbers, as it follows from the result of problem 269, the only irreducible polynomials are polynomials of first degree.

Let us return again to polynomials with arbitrary complex coefficients.

Definition 37 *Let z_0 be the root of the equation $a_0z^n + \ldots + a_n = 0$. We say that z_0 is a root with multiplicity k (or order k) if the polynomial $a_0z^n + \ldots + a_n$ is divisible by $(z - z_0)^k$ but not by $(z - z_0)^{k+1}$.*

Problem-276 What is the multiplicity of the roots $z = 1$ and $z = -1$ in the equation

$$z^5 - z^4 - 2z^3 + 2z^2 + z - 1 = 0$$

.

Definition 38 *The derivative of the polynomial $P(z) = a_0z^n + a_1z^{n-1} + \ldots + a_kz^{n-k} + \ldots + a_{n-1}z + a_n$ is the polynomial $P'(z) = a_0nz^{n-1} + a_1(n-1)z^{n-2} + \ldots + a_k(n-k)z^{n-k-1} + \ldots + a_{n-1}$. The derivative is usually denoted by a prime.*

Problem-277 Let $P(z)$ and $Q(z)$ be two polynomials. Prove the equalitites: a)$(P(z) + Q(z))' = P'(z) + Q'(z)$, b)$(c \cdot P(z))' = c \cdot P'(z)$, c) $(P(z) \cdot Q(z))' = P'(z) \cdot Q(z) + P(z) \cdot Q'(z)$.

Problem-278 Let $P(z) = (z - z_0)^n$ $(n \geq 1 -$ integer). Prove that $P'(z) = n(z - z_0)^{n-1}$.

Problem-279 Prove that if the equation $P(z) = 0$ has a root z_0 with multiplicity $k > 1$, then the equation $P'(z) = 0$ has a root z_0 with multiplicity $k - 1$ and that if the equation $P(z) = 0$ has a root z_0 with multiplicity one then $P'(z_0) \neq 0$.

[9] Our reasoning contains some lack of rigour and must be considered, in general, as an idea of the proof. However, this reasoning can be (although it is not simple) made rigourous (see for example Chinn W.G., Steenrod N.E, First Concepts of Topology.

[11] Bezout (1730-1783) was a French mathematician.

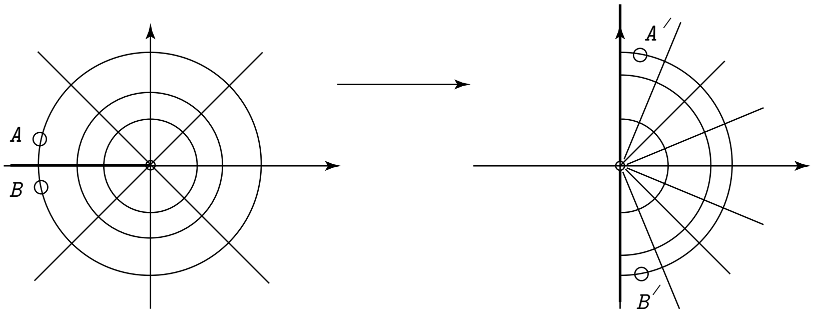


Fig. 3.12.

3.9 Riemann surface of the function $w = \sqrt{z}$

We considered single-valued functions for which there is a unique value of the function corresponding to each value of the variable. From now on, we will mainly be interested in many-valued functions, which assigns several values of the function to a particular value of the argument [12]. We will explain the reason for our interest in such functions. Actually, the final goal of our study is the proof of Abel's theorem, according to which a function which expresses the roots of a general equation of degree five in terms of coefficients is not expressible in radicals. But this function is many-valued since equation of degree five with fixed coefficients has in general five roots. The functions which are expressed in radicals are also many-valued.

The principal idea of the proof of Abel's theorem is the following. To each many-valued function of a complex variable, we will assign a certain group, the so-called Galois group [13]. It will be shown that the Galois's group for the function which expresses the roots of a certain equation of degree five in terms of a parameter z cannot be the Galois's group for a function expressed in radicals and hence this function cannot be expressed in radicals.

In order to introduce the concept of Galois's group, we will first introduce another very important concept in the theory of functions of a complex variable: the concept of a Riemann [14] surface of many-valued function. We will begin with the construction of Riemann surface for one of the simplest examples of a many-valued function, namely the function $w = \sqrt{z}$.

As we know, the function $w = \sqrt{z}$ takes one value $w = 0$ for $z = 0$ and two values for all $z \neq 0$ (see 229). If w_0 is one of the values of $\sqrt{z}_0$, then the other value of $\sqrt{z}_0$ is equal $-w_0$.

Problem-280 Find all values of: a) $\sqrt{1}$, b)$\sqrt{-1}$, c) $\sqrt{i}, t$ d) $\sqrt{1 + i\sqrt{3}}$ (here $\sqrt{3}$ is the positive value of root).

On the z plane, let us make a cut on the negative part of the real axis from 0 to $-\infty$ and for all z which do not lie in the cut let us choose the value $w = \sqrt{z}$ which lies on the right half-plane of the w plane. We will obtain a certain single-valued and continuous function over the entire z plane, excluding the cut. We will denote this function by ${}_1\sqrt{z}$. This function definea a single-valued and continuous mapping of plane z excluding the cut to the right-half of w plane (Fig. 3.12).

[12] Whenever the context is clear the term many-valued will be omitted.

[13] Evarist Galois (1811-1832)? the French mathematician who established the general conditions of solvability of equations in radicals, that placed principles of group theory. We advise to read: Sinfeld l., Evarist Galois (Izbrannik gods), publishing house young guards, M., 1958.

[14] Riemann (1826-1866) was a German mathematician.

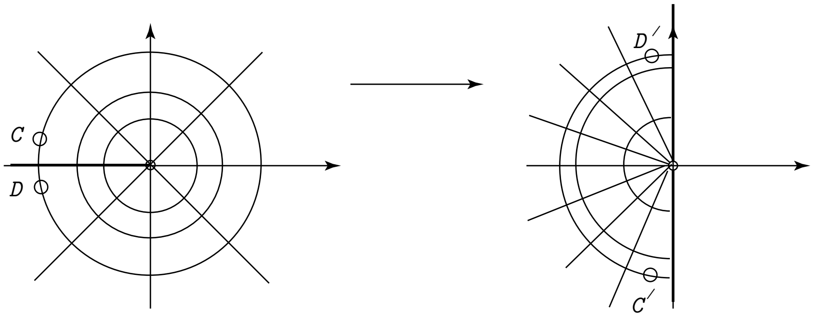
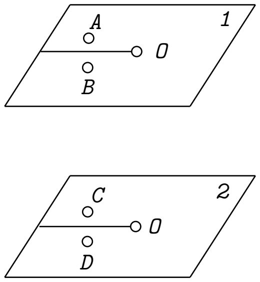


Fig. 3.13.



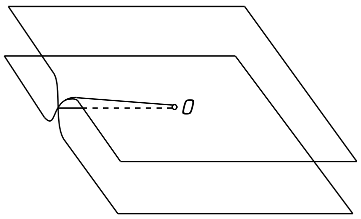


Fig. 3.15.

Fig. 3.14.

Observation. If we choose Arg z so that $-\pi <$ Arg $z < \pi$, then for the function ${}_1\sqrt{z}$ we get Arg ${}_1\sqrt{z} = \dfrac{1}{2}$ Arg z. (see 229). Under the mapping $w = {}_1\sqrt{z}$, the plane z shrinks like a fan to the positive part of the real axis, with the decrease in the angle of the fan being half and a certain change in the lengths along the rays of fan.

If we now choose, for all z which do not lie in the cut, the value $w = \sqrt{z}$ which lies on the left half of w plane, then we will obtain another single-valued continuous function on the entire z plane excluding the cut. This function, which we will denote by ${}_2\sqrt{z}$, defines a single-valued continuous mapping of the z plane excluding the cut to the left half of w plane (Fig. 3.13). Here ${}_2\sqrt{z} = -\,{}_1\sqrt{z}$.

Functions ${}_1\sqrt{z}$ and ${}_2\sqrt{z}$ so defined are called the single-valued continuous branches of the function $w = \sqrt{z}$ (for this cut).

Now take two copies of the plane z which we will call sheets and on each sheet cut out the negative part of the real axis from 0 to $-\infty$ (Fig. 3.14). Let us assign on the first sheet the function ${}_1\sqrt{z}$ and on the second sheet the function ${}_2\sqrt{z}$. We can consider the two functions ${}_1\sqrt{z}$ and ${}_2\sqrt{z}$ together as a certain single-valued function not on the z plane but on a more complex surface which consists of two separate sheets. So, if a point z moves continuously on the first sheet (or on the second sheet) without crossing the cut, then the single-valued function defined changes continuously. But if the point z, moving, for example, on the first sheet crosses the cut then continuity is lost. This follows,

for example, from the fact that the two close points A and B in the z plane, under the mapping, ${}_1\sqrt{z}$ maps to the points A' and B' respectively, which are far from each other. (see Fig. 3.12).
On the other hand, from Fig. 3.12 and 3.13 it is easy to note that the image of the point A under the mapping $w = {}_1\sqrt{z}$ (point A') is close to the image of the point D under the mapping $w = {}_2\sqrt{z}$ (point D').
Hence, when crossing the cut if the point z goes from the upper part of the cut on one sheet to the lower part of the cut on the other sheet, then the single-valued function defined will vary continuously. In order to ensure that the point z moves as wanted, we will consider the upper side of the cut on the first sheet glued to the lower side of the cut on the second sheet and the upper side of the cut on the second sheet glued to the lower side of the cut on the first sheet (Fig. 3.15).
When we are glueing, we will add a ray from the point 0 to ∞ between the glued parts. During the first glueing, for the points z which lie on this ray, we will choose the values $w = \sqrt{z}$ lying on the positive part of imaginary axis and for the second glueing, we choose the the values $w = \sqrt{z}$ which lie on the negative part of the imaginary axis.
After the required glueings we see that the two-valued function $w = \sqrt{z}$ is replaced with another function which is single-valued and continuous not on the z plane but on a more complex surface. This surface is called the Riemann surface of the function $w = \sqrt{z}$.
Attempts to produce glueings without intersections (without turning over plane) leads to failure. In spite of this, we will consider that Fig. 3.15 is the image of Riemann surface of the function $w = \sqrt{z}$ assuming that the intersection on the negative part of the real axis is only apparent. For comparison consider the following example. Fig. 2.7 depicts the frame of a cube. Although some segments in the figure intersect, we agree that this intersection is only apparent and this allows us to avoid errors.
The Riemann surface of an arbitrary many-valued function $w(z)$ can be constructed the way we built the Riemann surface of the function $w = \sqrt{z}$. For this it is necessary to first separate the single-valued continuous branches of the function $w(z)$ excluding some points z which belong to the cuts. Then the branches are glued together along the cuts so as to get a single-valued continuous function on the surface constructed. The surface obtained will be called Riemann surface of the many-valued function $w(z)$[15].
Thus, it remains to explain how to separate the continuous single-valued branches of an arbitrary many-valued function $w(z)$ and how to glue them. For explaining these questions let us consider again in more details the function $w = \sqrt{z}$.
Let $w(z)$ be a many-valued function and let us fix one of the values w_0 of the function $w(z)$ at a certain point z_0. Let $w'(z)$ be a continuous single-valued branch of the function $w(z)$ defined on some region of the z plane (for example, on the entire plane excluding some cuts) such that $w'(z_0) = w_0$. Assume that there exists a continuous curve C from the point z_0 to a certain point z_1 lying entirely in the region of z plane being considered. Then as the point z moves along the curve C the function $w'(z)$ will vary continuously from $w'(z_0)$ to $w'(z_1)$.
Actually, it is possible to use this property conversely, namely for defining the function $w'(z)$. Suppose that at a certain point z_0 one of the values w_0 of the function $w(z)$ be chosen and let C be a continuous curve from the point z_0 to a certain point z_1. We will move along the curve C, selecting for each point z which lies on C, one of the values of the function of $w(z)$ such that these values change continuously z moves along the curve C starting from the value w_0. In this case, when we reach point z_1, we will have a value $w_1 = w(z_1)$. We will indicate by w_1 the value $w(z_1)$ defined using continuity along the curve C under the condition $w(z_0) = w_0$. If we depict on the w plane the value of the function $w(z)$ chosen for all points on the curve C, then we get a continuous curve which begins at the point w_0 and ends at the point w_1. This curve is one of the continuous images of the curve C under the mapping $w = w(z)$.

[15] Such constructions cannot be made for each many-valued function; however, for the functions which we will be examining later, such constructions can always be possible

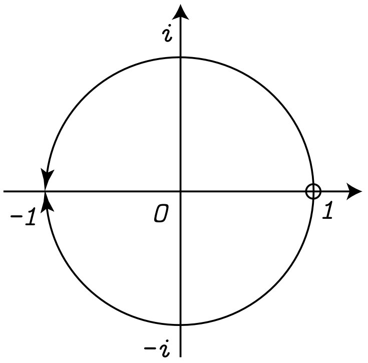


Fig. 3.16.

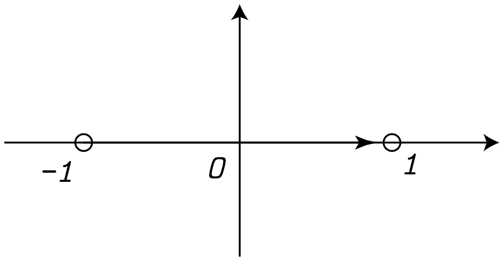


Fig. 3.17.

Problem-281 For the function $w(z) = \sqrt{z}$ let us choose $w(1) = 1$. Determine $w(-1) = \sqrt{-1}$ using continuity along: a) the upper semicircle of radius 1 with the center in the beginning of coordinates, b) lower semicircle (Fig. 3.16).
In fact, defining the function using continuity along a certain curve can lead to some problems. Let us consider an appropriate example.
Problem-282 Find all continuous images $w_0(t)$ of the curve C with the parametric equation $z(t) = 2t - 1$ (Fig. 3.17) under the mapping $w(z) = \sqrt{z}$ that begins: a) at the point i, b) at the point $-i$.
From the solution of problem 279 we see that even by fixing the image of initial point of curve C, the continuous image of the curve C under the mapping $w(z) = \sqrt{z}$ may be defined ambiguously. Moreover uniqueness is lost when the curve C passes through the point $z = 0$. In fact, for the function $w(z) = \sqrt{z}$ the uniqueness of images is lost only in this case, since only in this case do both images of the point $z(t)$ approach close to each other and merge into one point.
In order to avoid non-uniqueness of continuous images of curves under the mapping $w(z) = \sqrt{z}$, we may exclude the point $z = 0$ and not allow curves to pass through this point. This restriction however, does not always allow us to separate the single-valued continuous branches of the function $w(z) = \sqrt{z}$. Indeed, if we fix at a certain point z_0 one of the values $w_0 = w(z_0)$ and we define $w(z)$ at a certain point z_1 using continuity along different curves from z_0 to z_1, then we can obtain different values for $w(z_1)$ (for example, see 278). Let us see how to avoid this ambiguity.
Problem-283 Let the change in the argument of $z(t)$ along the curve C be equal to ϕ. Find the change in the argument $w_0(t)$ along any continuous image of the curve C under the mapping $w(z) = \sqrt{z}$.
Problem-284 Let $w(z) = \sqrt{z}$ and choose $w(1) = \sqrt{1} = -1$ Determine the value of $w(i) = \sqrt{i}$ using continuity along: a) the segment which connects points $z = 1$ and $z = i$; b) curve with parametric equation $z(t) = \cos \frac{3}{2}\pi t - i \sin \frac{3}{2}\pi t$; c) curve with parametric equation $z(t) = \cos \frac{5}{2}\pi t - i \sin \frac{5}{2}\pi t$
Problem-285 Let $w(z) = \sqrt{z}$ and choose at the initial point of a curve C $w(1) = \sqrt{1} = 1$. Determine using continuity along the curve C the value $w(1) = \sqrt{1}$ at the final point if the curve C has the equation: a) $z(t) = \cos 2\pi t + i \sin 2\pi t$; b)$z(t) = \cos 4\pi t - i \sin 4\pi t$; c) $z(t) = 2 - \cos 2\pi t - i \sin 2\pi t$

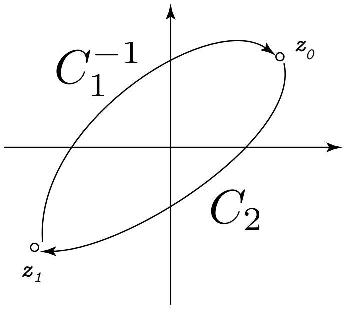


Fig. 3.18.

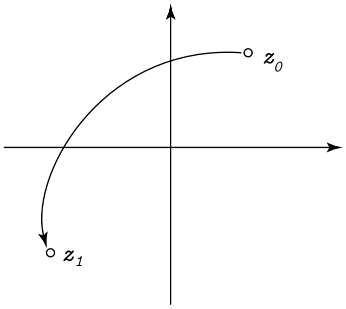


Fig. 3.19.

Problem-286 Let C be a closed curve on the z plane (i.e. $z(1) = z(0)$). Prove that the value of the function $\sqrt{z}$ at the end point of the curve C defined using continuity, coincides with the value at initial point $\iff$ curve C goes around around point $z = 0$ an even number of times.
For future reference it is convenient to introduce the following notation.

Definition 39 *Let C be a continuous curve with the parametric equation $z(t)$. We will denote the curve geometrically identical to C but travelled in the opposite direction by C^{-1} ; its equation (see 247) being $z_1(t) = z(1-t)$.*

Definition 40 *Suppose the initial point of a curve C_2 coincides with the end point of a curve C_1. We will denote by C_1C_2 the curve obtained by first traversing C_1 and then C_2 (see 248).*

Problem-287 Let C_1 and C_2 be two curves joining the point z_0 to the point z_1 and assume that one of the values of $\sqrt{z}_0 = w_0$ is selected. Prove that the value $\sqrt{z}_1$ defined using continuity along the curves C_1 and C_2 will be identical $\iff$ the curve $C_1^{-1}C_2$ (Fig. 3.18) goes around the point $z = 0$ an even number of times.
From the statement of the last problem it follows that if the curve $C_1^{-1}C_2$ goes around the point $z = 0$ zero times, then the value of the function $\sqrt{z}$ at the final points of the curves C_1 and C_2 defined using continuity coincides if the values at initial points are identical and it goes around the point $z = 0$ an even number of times.
To separate the single-valued continuous branches of the function $w = \sqrt{z}$ it suffices that the curve $C_1^{-1}C_2$ not go around the point $z = 0$ once. For this it suffices to make any cut from point $z = 0$ into infinity and to forbid curves to intersect this cut. Specifically, in the above example, a cut from point $z = 0$ to $-\infty$ on the negative part of the real axis is made.
If after making a cut we fix at a certain point z_0 one of the values $w_0' = \sqrt{z}_0$ and determine the value at any other point z_1 using continuity along any curve C that goes from z_0 to z_1 and not crossing the cut, then on the entire plane excluding the cut, a certain single-valued continuous branch ${}_1\sqrt{z}$ of the function $w = \sqrt{z}$ will be defined. If at the point z_0 we fix the other value $w_0'' = \sqrt{z}_0$ then this will define another branch ${}_2\sqrt{z}$ of the function $w = \sqrt{z}$.
Problem-288 Prove that ${}_1\sqrt{z} \neq {}_2\sqrt{z}$ for any point z which does not lie on the cut.
Problem-289 Fix at a certain point z' the value $w' = {}_1\sqrt{z'}$ and define the values of the function $w = \sqrt{z}$ at other points of the plane z (excluding the cut) using continuity along curves starting from point z' but not crossing the cut. Prove that the single-valued continuous branch obtained coincides with the function ${}_1\sqrt{z}$ (defined by the value at point z').

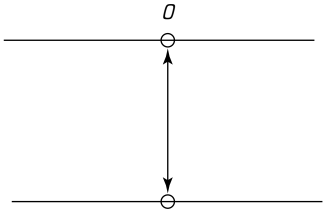


Fig. 3.20.

It follows that from the result of problem 286 that selecting different points of the z plane as initial points, one obtains the same splitting of the Riemann surface into single-valued continuous branch. This splitting depends only on how the cuts are made.

Problem-290 Let the points z_0 and z_1 not lie in the cut and let the curve C that connects point z_0 with z_1 cross the cut once (Fig. 3.19). Choose a value $w_0 = \sqrt{z}_0$ and by continuity along C define the value $w_1 = \sqrt{z}_1$. Prove that the values w_0 and w_1 correspond to different branches of the function $w = \sqrt{z}$.

Thus, on crossing cuts we go from one branch of the function $w = \sqrt{z}$ to another branch, i.e. branches are connected precisely in the manner we connected them earlier (see Fig. 3.15). In this way, we get the Riemann surface of the function $w = \sqrt{z}$.

We will say that a certain property holds for a closed loop around the point z_0 if it holds for a single closed loop counterclockwise for all circles with the center at the point z_0 and with a sufficiently small radius [16].

Problem-291 Prove that by a turn around the point z_0 we remain on the same sheet of the Riemann surface of the function $w = \sqrt{z}$ if $z_0 \neq 0$ and we go to another sheet if $z_0 = 0$.

The following concept is very important for future reference.

Definition 41 *If we go from one branch to another (the value of the function changes) on moving along a loop around a point, then the point is called a branch point of the given many-valued function.*

The Riemann surface of the function $w = \sqrt{z}$ can be depicted in the form of a diagram (Fig. 3.20). This diagram shows that the Riemann surface of the function $w = \sqrt{z}$ has 2 sheets, that the point $z = 0$ is the branch point of the function $w = \sqrt{z}$ and that with a loop around point $z = 0$ we go from one sheet to the other. In this case the arrows at point $z = 0$ show passages from one sheet to the other not only under a loop around the point $z = 0$ but also by crossing the cut which goes from the point $z = 0$ to infinity. Below we will see that this relationship between the branch points and cuts from these branch points is not an accident.

Henceforth, instead of Riemann surfaces of many-valued functions we will represent its diagram.

3.10 Riemann surfaces of more complicated functions

Consider the many-valued function $w = \sqrt[3]{z}$.

Problem-292 Let the change in the argument along the curved $z(t)$ be ϕ and let $w_0(t)$ be the continuous image of the curve $z(t)$ under the mapping $w = \sqrt[3]{z}$. Find the change in the argument along the curve $w_0(t)$.

[16] More precisely, this means the following: there exists a real number $\delta > 0$ such that the property mentioned holds for any turn along any circles with center z_0 with radius less than δ

Problem-293 Find the branch points of the function $w = \sqrt[3]{z}$.
Problem-294 Assume that a cut is made from the point $z = 0$ to $z = -\infty$ on the negative part of the real axis and assume that the continuous single-valued branches of function $w = \sqrt[3]{z}$ are given by the conditions: $f_1(1) = 1$,

$$f_2(1) = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

,

$$f_2(1) = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

. Find: a)$f_1(i)$, b)$f_2(i)$, c)$f_1(8)$, d)$f_3(8)$,e) $f_3(-i)$
Problem-295 Contruct the Riemann surface and its diagram for the function $w = \sqrt[3]{z}$.
Problem-296 Let C be a continuous curve with parametric equation $z(t)$ and let w_0 be one of the values of $\sqrt[n]{z(0)}$. Prove that there exists at least one continuous image of the curve C under the mapping $w = \sqrt[n]{z}$ starting at the point w_0.
Problem-297 Suppose the change in the argument along the curve $z(t)$ be is ϕ and let $w_0(t)$ be the continuous image of the curve $z(t)$ under the mapping $w = \sqrt[n]{z}$. Find the change in the argument along the curve $w_0(t)$.
Problem-298 Find the branch points of the function $w = \sqrt[n]{z}$.
We introduced the notation

$$\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

in section five and considered some of its properties.
Problem-299 Suppose that the curve $z(t)$ does not go through the point $z = 0$ and let $w_0(t)$ be one of the continuous images of the curve $z(t)$ under the mapping $w = \sqrt[n]{z}$. Find all the continuous images of the curve $z(t)$ under the mapping $w = \sqrt[n]{z}$.
Consider two continuous curves C_1 and C_2 starting at a certain point z_0 and ending at a certain point z_1. Just as for the function $w = \sqrt{z}$ (see 284), it is true that if the curve $C_1^{-1}C_2$ never goes around around the point $z = 0$, then the function $w = \sqrt[n]{z}$ is uniquely defined using continuity along the curves C_1 and C_2. Therefore, just as for the function $w = \sqrt{z}$ if we make a cut from the point $z = 0$ to infinity, then the function $w = \sqrt[n]{z}$ is decomposed into continuous single-valued branches.
Problem-300 Make a cut from the point $z = 0$ to ∞, not passing through the point $z = 1$ and define the continuous single-valued branches of the function $\sqrt[n]{z}$ by the conditions: $f_i(1) = \varepsilon_n^i$, where i takes integer values from 0 to $n-1$. How are the branches $f_i(z)$ expressed in terms of $f_0(z)$?
Problem-301 Draw the diagram of the Riemann surface of the function of $w = \sqrt[n]{z}$.
Problem-302 Find the branch points and draw the Riemann surface diagram for the function $\sqrt{z-1}$.
Problem-303 Find the branch points and draw the Riemann surface diagram for the function $\sqrt[n]{z+i}$.
When a many-valued function has several branch points, we will make cuts from each branch point into infinity along non-intersecting lines to separate the continuous single-valued branches.
In this way the Riemann surface diagram of this function may depend on the cuts made from the branch points to infinity (corresponding examples are examined below in problems 327 and 328). When this occurs, we will mention what cuts are made. But if this is not important then we will not indicate them.
The Riemann surfaces diagram made by the reader during the solution of the problems posed below can differ from the diagrams given in the solutions due to different labelling of sheets. With the appropriate renumbering of sheets these diagrams should coincide.
Problem-304 Let $f(z)$ be a single-valued continuous function and let C be a continuous curve on the z plane which starts at the point z_0. Let w_0 be one of the values of $\sqrt[n]{f(z_0)}$. Prove that there

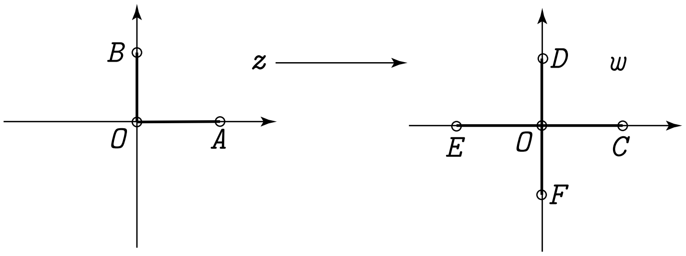


Fig. 3.21.

exists at least one continuous image of the curve C under the mapping $w = \sqrt[n]{f(z)}$ that starts at the point w_0.

From the results of problem 301 it follows that it is possible to define the function $w = \sqrt[n]{f(z)}$ using continuity along any curve not passing through points at which uniqueness of continuous image is lost.

Problem-305 Let $f(z)$ be a single-valued continuous function and $w_0(z)$ be one of the continuous single-valued branches (under appropriate cuts) of the function $w(z) = \sqrt[n]{f(z)}$. Find all single-valued continuous branches (using the same cuts) of the function $w(z)$.

Problem-306 Find all branch points and draw the of the Riemann surface diagrams for the functions: a)$\sqrt{z(z-i)}$, b)$\sqrt{z^2+1}$

Problem-307 Draw the Riemann surfaces diagrams for the following functions: a)$\sqrt[3]{z^2-1}$, b)$\sqrt[3]{(z-1)^2 z}$, c)$\sqrt[3]{(z^2+1)^2}$

Problem-308 Separate the continuous single-valued branches and the diagram Riemann surface build for the function $\sqrt{z^2}$

Observation. From the solution of problem 305 we see that the point $z = 0$ is not a branch point of function $\sqrt{z^2}$. At the same time the images of curves passing through the point $z = 0$ are not uniquely defined. For example, the continuous image of broken AOB (Fig. 3.21) under the mapping $\sqrt{z^2}$ are the broken lines COD, COF, EOD and EOF (Fig. 3.21). When passing the point $z = 0$ we can remain on the same sheet (the lines COD and EOF) or go to another sheet (the lines COF and EOD). The Riemann surface of the function $w(z) = \sqrt{z^2}$ takes the form shown in Fig. 3.22.

Definition 42 *The points at which the uniqueness of continuous images of curves is lost but which are not branch points are called the ambiguity points of the given function.*

When drawing the Riemann surfaces diagram oen should make no cuts from ambiguity points to infinity: it suffices to exclude these points, i.e., not allow curves to pass through them.

Problem-309 Draw the Riemann surfaces diagrams of the following functions: a)$\sqrt[4]{z^2+2}$, b)$\sqrt[4]{z^2}$, c)$\sqrt[4]{(z-1)^2(z+1)^3}$, d)$\sqrt[4]{(z^2-1)^3(z+1)^3}$, d)$\sqrt[4]{z(z^3-1)}$.

Problem-310 Draw the Riemann surface diagram of the function $\sqrt{\dfrac{1}{z}}$

Problem-311 Draw the Riemann surface diagrams of the following functions: a) $\sqrt{\dfrac{1}{z-i}}$, b) $\sqrt[3]{\dfrac{z-1}{z+1}}$, c) $\sqrt[4]{\dfrac{(z+1)^4}{z(z-1)^3}}$

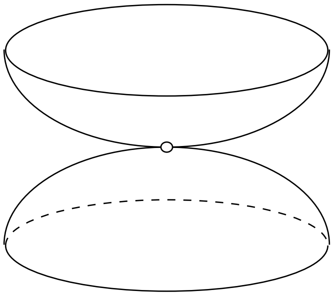


Fig. 3.22.

During the solution of problems in this section, we saw that after making nonintersecting cuts from all branch points to infinity the function in question split into single-valued continuous branches, which are then glued in a specific manner along the cuts. It occurs that a sufficiently broad class of many-valued functions possesses this property. In particular, all the functions considered below possess this property, namely functions which are expressed in radicals (section 11) and algebraic functions (section 14) [17].

The proof of this statement exceeds the scope of this book. Therefore we simply refer to the literature [18] on this question and accept the statement formulated above without proof. The reader can if wanted jump immediately to section 11.

However, a certain feeling of dissatisfaction can remain in the reader. And although we will not be able to completely free the reader from this feeling, we will nevertheless show that the property formulated above follows from another property, the so-called monodromy property which looks more obvious.

We know that to separate the single-valued continuous branches of the many-valued function $w(z)$ (in a certain region of the z plane) it is necessary that the function $w(z)$ be defined using continuity equally along any two curves C_1 and C_2 lying in this region and going from an arbitrary point z_0 to another point z_1. The property of monodromy is connected with this condition.

Let the many-valued function $w(z)$ be such that after fixing one of the values of w_0 at an arbitrary point z_0 the function $w(z)$ can be defined using continuity (possibly ambiguously) along any continuous curve which starts at point z_0 (and not passing through the points at which the function $w(z)$ is not defined). Let us say that the many-valued function $w(z)$ possesses the property of monodromy if the following assertion holds true.

Monodromy Property . Let C_1 and C_2 be two continuous curves on the z plane which begins at a certain point z_0 and which ends at a certain point z_1 and not pass through the branch and ambiguity points of the many-valued function $w(z)$. Suppose that the curve C_1 can be continuously deformed into the curve C_2 such that none of the the curves obtained during the deformation pass through the branch points of the function $w(z)$ and their ends remain fixed (In Fig. 3.23 a, b are branch points). If the value $w(z_1)$ is uniquely defined using continuity along the curves C_1 and C_2 (when a certain value $w_0 = w(z_0)$ is chosen).

Let us explain the consequences that follow from the monodromy property.

Problem-312 Suppose that the function $w(z)$ possesses the monodromy property. Let us make nonintersecting cuts on the z plane from all branch points of the function $w(z)$ to infinity and pick

[17] Both of these functions are special cases of the broader class of the so-called analytic functions, which also possess the above property.

[18] See for example, Springer G., Introduction to Riemann Surfaces.

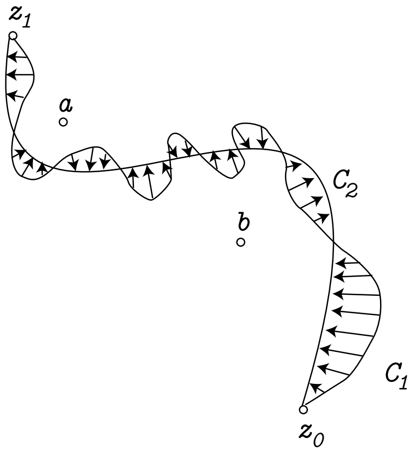


Fig. 3.23.

out the ambiguity points of the function $w(z)$. Prove that in this case the function $w(z)$ is decomposed into single-valued continuous branches.

Problem-313 Suppose that in the conditions of the previous problem the cuts do not pass through the ambiguity points of the function $w(z)$ and that $w(z)$ has a finite number of branch points. Prove that on crossing a certain cut (in a particular direction) one moves from a particular branch of the function $w(z)$ to another unique branch which does not depend upon where we cross the cut.

Observation 1. During a loop around the branch point we cross the cut which goes from this point to infinity once. Therefore using the result of problem 310 the passage from some branch to other during the crossing of a certain cut in an arbitrary place coincides with the passage obtained under a loop (with the appropriate direction) around the branch point from which the cut is made and hence they coincide with the passage indicated by the corresponding arrows at the point in the Riemann surface diagram.

Observation 2. It follows from the results of problems 309 and 310 that if the many-valued function $w(z)$ possesses the monodromy property, then one can build its Riemann surface. Moreover to understand the structure of this surface it suffices to find the branch points of the function $w(z)$ and to define the passages between the branches of the function $w(z)$ corresponding to loops around these points.

All functions which we shall consider below possess the monodromy property. Here we will not be able to rigourously prove this statement since this requires the concept of an analytic function. However, we will give a sketch of the proof of the statement that a certain many-valued function $w(z)$ possesses the monodromy property assuming that this function is "sufficiently good". What this means will be clear from the sketch of the proof.

Suppose the conditions required for the monodromy property are satisfied. Let C_1' and C_2' be continuous images of two curves C_1 and C_2 under the mapping $w(z)$ begining at the point $w_0 = w(z_0)$. We have to prove that the curves C_1' and C_2' ends at the same point.

Assume that the curves which are obtained during the deformation of C_1 into C_2 neither pass through the branch points nor through the ambiguity points of the function $w(z)$. Let C be one of these curves. Then there is a unique continuous image C' of the curve C under the mapping $w(z)$ which begins at the point $w_0 = w(z_0)$. If the function $w(z)$ is "sufficiently good"[19], then during the continuous

[19] The monodromy property is usually proved for arbitrary analytic functions. See, for example, Springer G., Introduction to Riemann Surfaces.

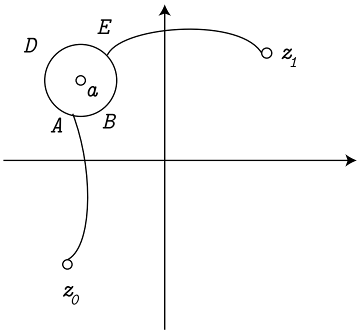


Fig. 3.24.

deformation of the curve C from the position C_1 to the position C_2 the curves C' are continuously deformed C'_1 to C'_2. The end point of the curve C' is also deformed continuously. But the curve C ends at the point z_1; therefore the end point curve C' must coincide with one of the images $w(z_1)$ of the point of z_1. If the function $w(z_1)$ is assumed to take only a finite number of values for each z (in particular for z_1) (but we will examine only such functions), then the end point of the curve C' cannot jump from one image of the point z_1 to another image since in this case the continuity of deformation will be lost. Hence, end points of all the curves C' and in particular of the curves C'_1 and C'_2 coincide.

Consider now what happens when the curve C crosses an ambiguity point of the function $w(z)$ (which is not a branch point). Consider the special case when curve changes only near the ambiguity point (Fig. 3.24). If at the point z_0 the value $w_0 = w(z_0)$ then using continuity the value $w(z)$ at point A will be determined uniquely.

After this the value of $w(z)$ at point E will be uniquely defined using continuity along the curves ADE and ABE since otherwise on tracing the loop $EDABE$ the value of the function $w(z)$ would change and the point would be a branch point of the function $w(z)$. After the value of $w(z)$ at the point E is uniquely defined along the two curves, using continuity along the curve Ez_1 the value of $w(z)$ at the point z_1 is also defined uniquely.

Thus, the "dark place" in our exposition remains the claim that all functions considered below are "sufficiently good".

The reader either has to accept this statement by faith or to turn to a deeper study of analytic functions. [20]

3.11 Functions expressible by radicals

Definition 43 *Let $f(z)$ and $g(z)$ be two many-valued functions. By $f(z) + g(z)$ we will denote the many-valued function whose value at the point z_0 is the sum of $f(z_0)$ and $g(z_0)$. Similarly the functions $f(z) - g(z), f(z) \cdot g(z), \dfrac{f(z)}{g(z)}$ are defined. By $f(z)^n$, where n is a natural number we mean the function whose value at a point z_0 will be the value of $f(z_0)$ raised to the power n. By $\sqrt[n]{f(z)}$, where n is natural number we mean the function whose value at a point z_0 will be all the n values of $\sqrt[n]{f(z_0)}$ for each value of $f(z_0)$.*

[20] See for example, Shabat B. V., Introduction to Complex Analysis.

Problem-314 Find all values of: a) $\sqrt[3]{-8}$, b)$\dfrac{1-\sqrt{-2i}}{\sqrt{-4}}$, c)$\sqrt{i+\sqrt{-1}}$, d)$\left(\sqrt[4]{(1+i)^2}\right)^2$, e)$\left(\sqrt{i}+\sqrt{i}\right)^2$

Definition 44 *We will say that the many-valued function $h(z)$ is expressible in radicals if it can be obtained from the function $f(z) = z$ and the constant functions $g(z) = a$ (a is an arbitrary complex number) using the operations of addition, subtraction, multiplication, division, raising to a natural power and extracting roots of integer order.*

For example, the function $\left(\sqrt[3]{\sqrt{z}+3z^2}-\dfrac{i}{\sqrt{z}}\right)^4$ is expressible in radicals. We have already examined above some functions which are expressible in radicals.
Problem-315 Let the function $h(z)$ be expressible in radicals and let C be a continuous curve on the z plane starting at the point z_0 and not passing through the points at which the function $h(z)$ is not defined. Prove that if w_0 is one of the values of $h(z_0)$, then there exists at least one continuous image of the curve C under the mapping $w = h(z)$ which starts at a point w_0. (We consider that the parametric equation $w(t) = a$, where a is a fixed complex number describes a continuous curve degenerated into a point)
From the result of problem 312 we obtain that an arbitrary function $h(z)$ that is expressible in radicals can be defined using continuity along by any continuous curve C not passing through the points at which the function $h(z)$ is not defined. Moreover, if the curve C does not pass through the branch and ambiguity points of the function $h(z)$ then the function $h(z)$ is uniquely defined using continuity along the curve C.
We already noted in the previous paragraph that the functions which are expressible in radicals are "sufficiently good" [21],i.e., they possess the monodromy property. Therefore for any function which is expressible in radicals one can build the Riemann surface (see 309 and 310)[22]. Let us study the structure of these Riemann surfaces.
Henceforth, everywhere in the text we will assume that the discussion deals with functions which are expressible in radicals.
Problem-316 Let $h(z) = f(z)+g(z)$. Pick out from the plane all the ambiguity points of the function $h(z)$ and let us make nonintersecting cuts from all the branch points of $f(z)$ and $g(z)$ to infinity. Let $f_1(z), \ldots, f_n(z)$ and $g_1(z), \ldots, g_m(z)$ be the continuous single-valued branches of the functions $f(z)$ and $g(z)$ respectively on the plane obtained after making the cuts. Find the continuous single-valued branches of the function of $h(z)$.
If with a loop around the point z_0 we go from the branch $f_{i_1}(z)$ to the branch $f_{i_2}(z)$ and also from the branch $g_{j_1}(z)$ to the branch $g_{j_2}(z)$, then obviously, we go from the branch $h_{i_1,j_1}(z) = f_{i_1}(z) + g_{j_1}(z)$ to the branch $h_{i_2,j_2}(z) = f_{i_2}(z) + g_{j_2}(z)$. This hints us the following formal method of constructing the Riemann surface diagram of the function $h(z) = f(z) + g(z)$ when the Riemann surface diagram of the functions $f(z)$ and $g(z)$ are built (under the same cuts). To each pair of branches $f_i(z)$ and $g_j(z)$ we assign the sheet which we consider as the branch $h_{i,j}(z) = f_i(z) + g_j(z)$. If we go from the branch $f_{i_1}(z)$ to the branch $f_{i_2}(z)$ and from the branch $g_{j_1}(z)$ to the branch $g_{j_2}(z)$ in the of Riemann surface diagram of the functions $f(z)$ and $g(z)$ at the point z_0 respectively, then in the Riemann surface diagram of the function $h(z)$ we indicate at point z_0, the passage from the branch $h_{i_1,j_1}(z)$ to the branch $h_{i_2,j_2}(z)$.
Problem-317 Build the of Riemann surface diagrams of the following functions: a)$\sqrt{z}+\sqrt{z-1}$, b)$\sqrt[3]{z^2-1}+\sqrt{\dfrac{1}{z}}$,c) $\sqrt{z}+\sqrt[3]{z}$, d)$\sqrt{z^2-1}+\sqrt[4]{z-1}$.
The informal method of constructing the of Riemann surface diagram of the function $h(z) = f(z)+g(z)$ described above does not always give the correct result, since it does not consider the fact that some

[21] All functions which are expressible in the radicals are analytical
[22] Any function which is expressible in radicals has a finite number of branch points.

of the branches $h_{i,j}(z)$ can coincide. For simplicity, we will consider that the cuts do not pass through the ambiguity points of the function $h(z)$. In this case, during the crossing of any cut we go from the sheet which corresponds to the equal branches of the function $h(z)$, in view of uniqueness to sheets which also correspond to equal branches. Hence, if we glue together the sheets which correspond to identical branches of the function $h(z)$, i.e., replace many such sheets with one sheet, then the passages between the obtained sheets along loops around a branch point z_0 will be uniquely defined.

Problem-318 Find all the values of $f(1)$ if: a)$f(z) = \sqrt{z} + \sqrt{z}$, b) $f(z) = \sqrt{z} + \sqrt[4]{z^2}$, c)$\sqrt[3]{z} + \sqrt[3]{z}$.

Problem-319 To build the Riemann surface diagram by the informal method and the true diagram of Riemann surface for the following functions: a)$f(z) = \sqrt{z} + \sqrt{z}$, b) $f(z) = \sqrt{z} + \sqrt[4]{z^2}$, c)$\sqrt[3]{z} + \sqrt[3]{z}$.

Finally we see that for constructing the Riemann surface diagram of the function $h(z) = f(z) + g(z)$ using the Riemann surface diagrams of the functions $f(z)$ and $g(z)$ (under the same cuts) it is sufficient to build the diagram by the informal method described above and then to glue the corresponding sheets.

It is easy to see that this algorithm can also be used to construct the Riemann surface diagram of the functions $h(z) = f(z) - g(z), h(z) = f(z) \cdot g(z), h(z) = \dfrac{f(z)}{g(z)}$

Problem-320 Build the Riemann surface diagram of the following functions: a)$i\sqrt{z} - \sqrt[4]{z^2}$, b)$\sqrt{z-1} \cdot \sqrt[4]{z}$, c)$\dfrac{\sqrt{z^2-1}}{\sqrt[4]{z+1}}$, d)$\dfrac{\sqrt{z}+\sqrt{z}}{\sqrt{z(z-1)}}$.

Problem-321 Let $f_1(z), f_2(z), \ldots, f_m(z)$ be all the continuous single-valued branches of the function $f(z)$. Using the same cuts, find all the continuous single-valued branches of the function $h(z) = f(z)^n$, where n is a non-zero integer.

It easily follows that from the result of last problem that the Riemann surface diagram of the function $h(z) = f(z)^n$ will coincide with the Riemann surface diagram of the function $f(z)$ if all the branches of $h_i(z) = f_i(z)^n$ were different. However, this is not always the case. If there are equal branches, then on crossing the cuts, because of uniqueness, we will go from equal branches to equal branches.

Finally we obtain that for constructing the Riemann surface diagram of the function $h(z) = f(z)^n$ using the Riemann surface diagram of the function $f(z)$ it is sufficient to consider the branches $h_i(z) = f_i(z)^n$ instead of branches $f_i(z)$. If we get identical branches, then one has to glue together the appropriate sheets.

Problem-322 Build the Riemann surfaces diagram of the following functions: a)$\left(\sqrt[4]{z}\right)^2$, b)$\left(\sqrt{z}+\sqrt{z}\right)^2$, c)$\left(\sqrt{z} \cdot \sqrt[3]{z-1}\right)^3$.

Let us now analyze the relation between the Riemann surface diagram of the function $\sqrt[n]{f(z)}$ with the Riemann surface diagram of the function $f(z)$.

Problem-323 What are the branch points of the function $\sqrt[n]{f(z)}$?

On the z plane make the cuts from the branch points of the function $f(z)$ to infinity such that they do not pass through the points at which the function $f(z)$ vanishes and separate the continuous single-valued branches of the function $f(z)$. Let $f_1(z), f_2(z), \ldots, f_m(z)$ be these branches. Make additional cuts from the points at which the function $f(z)$ vanishes to infinity. Let $g(z)$ be one of the continuous single-valued branches of the function $\sqrt[n]{f(z)}$ under these cuts.

Problem-324 Prove that the function $g(z)^n$ coincides with one of the functions $f_i(z)$ everywhere except on the cuts.

It follows that from the result of the proceeding problem that every branch of the function $\sqrt[n]{f(z)}$ corresponds to a some branch of the function $f(z)$.

Problem-325 Let $g(z)$ be a continuous single-valued branch of the function $\sqrt[n]{f(z)}$, corresponding to the branch $f_i(z)$ of the function $f(z)$. Find all continuous single-valued branches of function $\sqrt[n]{f(z)}$ corresponding to the branche $f_i(z)$.

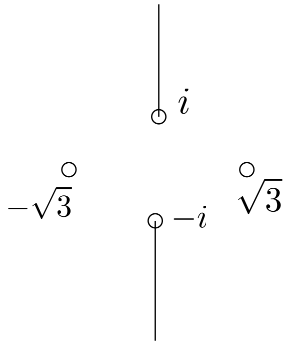


Fig. 3.25.

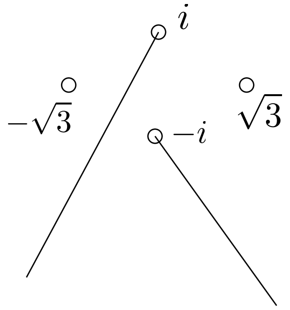


Fig. 3.26.

From the result of last problem we obtain that to every branch $f_i(z)$ of the function $f(z)$ there corresponds a bundle which consists of n branches of the function $\sqrt[n]{f(z)}$. We will number the branches in this bundle $f_{i,0}(z), f_{i,1}(z), \ldots, f_{i,n-1}(z)$ such that for every k the equation $f_{i,k}(z) = f_{i,0} \cdot \varepsilon_n^k$ holds. Let z_0 be a branch point of the function $f(z)$ and suppose that with a loop around the point z_0 we go from the branch $f_i(z)$ to the branch $f_j(z)$. Then obviously, for the function $\sqrt[n]{f(z)}$ we obtain the following: on going around a loop about the point z_0 we will go from all branches of the bundle corresponding to the branch $f_i(z)$ to all branches of the bundle which corresponds to the branch $f_j(z)$.

Problem-326 Let C be a curve on the z plane with the parametric equation $z(t)$ and let the curve on the w plane with the equation $w_0(t)$ be continuous image of curve C under the mapping $w = \sqrt[n]{f(z)}$. Prove that the curve with the equation $w_k(t) = w_0(t) \cdot \varepsilon_n^k$ is also the continuous image of the curve C under the mapping $w = \sqrt[n]{f(z)}$.

Problem-327 Let the curve C on the z plane not pass through the branch and ambiguity points of the function $\sqrt[n]{f(z)}$. Prove that if on moving along the curve C one moves from the branch $f_{i,s}(z)$ to the branch $f_{j,r}(z)$, then one moves from the branch $f_{i,s+k}(z)$ to the branch $f_{j,r+k}(z)$, where the sums $s + k$ and $r + k$ are calculated modulo n (see 40).

Thus, to define where we one goes from the branches of a given bundle on moving along a loop about a branch point of the function $\sqrt[n]{f(z)}$, it suffices to define where we one goes from one of the branches of this bundle; for other branches transitions will be automatically defined in view of the result of problem 324.

Problem-328 Build the Riemann surface diagram of the function $\sqrt{\sqrt{z} - 1}$

Problem-329 Build the Riemann surfaces diagram of the following functions: a) $\sqrt[3]{\sqrt{z} - 2}$, b) $\sqrt{\sqrt[3]{z} - 1}$

In the following two problems examples where the Riemann surface diagram of function depends on the cuts made is considered.

Problem-330 Build the Riemann surface diagram of the function $f(z) = \sqrt{z^2 + 1} - 2$ using the cuts depicted: a) in Fig. 3.25 , b)Fig. 3.26. In both cases, determine whether the points z such that $f(z) = 0$ lie on the same sheet or on different sheets.

Problem-331 Build the Riemann surface diagram of the function $f(z) = \sqrt{\sqrt{z^2 + 1} - 2}$ using the cuts depicted:a) in Fig. 3.27 , b) Fig. 3.28.

Let us formulate once again the results of this section which will be useful in the sequel.

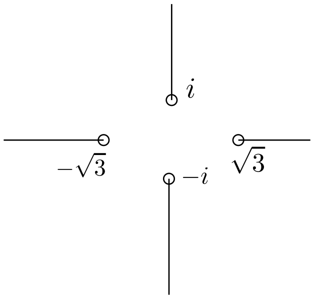


Fig. 3.27.

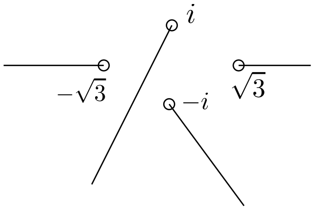


Fig. 3.28.

Theorem 3.3 *To construct the Riemann surface diagram of the functions $h(z) = f(z)+g(z), h(z) = f(z) - g(z), h(z) = f(z) \cdot g(z), h(z) = \frac{f(z)}{g(z)}$ using the Riemann surface diagrams of the functions $f(z)$ and $g(z)$, using the same cuts, it suffices to do the following:*

- *a) to each pair of branches $f_i(z)$ and $g_j(z)$ a sheet on which the branch of $h(z)$ denoted by $h_{i,j}(z)$, equal to $= f_i(z) + g_j(z), f_i(z) - g_j(z), f_i(z) \cdot g_j(z), \frac{f_i(z)}{g_j(z)}$ is defined;*
- *b) if on moving along a loop around the point z_0, one moves branch $f_{i_1}(z)$ to the branch $f_{i_2}(z)$ and from the branch $g_{j_1}(z)$ to the branch $g_{j_2}(z)$, then for the function $h(z)$, on the same loop, one moves from the branch $h_{i_1,j_1}(z)$ to the branch $h_{i_2,j_2}(z)$;*
- *c) glue together the sheets on which the branches $h_{i,j}(z)$ coincide.*

Theorem 3.4 *To build the Riemann surface diagram of the function $h(z) = f(z)^n$ using the Riemann surface diagram of the function $f(z)$ defined by the same cuts, it is suffices to do the following:*

- *a) in the Riemann surface diagram of the function $f(z)$, consider instead of the branches $f_i(z)$, the branches $h_i(z) = f_i(z)^n$;*
- *b) identify the sheets on which the branches $h_i(z)$ coincide.*

Theorem 3.5 *To build the Riemann surface diagram of the function $h(z) = \sqrt[n]{f(z)}$ using the Riemann surface diagram of the function $f(z)$ using the same cuts, if suffices to do the following:*

- *a) replace every sheet of the Riemann surface diagram of the function $f(z)$ by a bundle of n sheets;*
- *b) on moving along a loop around any branch point of the function $h(z)$ one moves from all the sheets of one bundle to all the sheets of a different bundle;*
- *c) the passages from one bundle to another correspond to the passages between the sheets of the Riemann surface of the function $f(z)$;*
- *d) if the branches in the bundles are enumerated such that $f_{i,k}(z) = f_{i,0} \cdot \varepsilon_n^k$ then on passage from one bundle to another, the sheets of the bundle are not mixed, but permuted cyclically (see 324).*

3.12 Galois group of many-valued functions

We now associate a certain permutation group with each Riemann surface diagram.

Problem-332 Let the curve C on the z plane not pass through the branch and ambiguity points of the function $w(z)$. Prove that on moving along the curve C we will go from different sheets of the Riemann surface diagram of the function $w(z)$ to different sheets.

Thus, in view of the result of problem 329, to any loop (counterclockwise) around any branch point of the function of $w(z)$ there corresponds a permutation of the sheets of the Riemann surface diagram of the function $w(z)$.

Problem-333 Let the Riemann surface diagram for the functions enumerated in task 314 be built in the same way as its done in the solutions of this peoblem (see the chapter "Hint, Solutions and Answers") and let the sheets on these diagrams be numbered from bottom to top by the numbers $1, 2, 3, \ldots$. Write down the permutation of the sheets corresponding to one loop around each branch point.

Problem-334 Let $g_1, g_2, \ldots, g_s$ be elements of an arbitrary group G. Consider all elements of G which can be obtained from $g_1, g_2, \ldots, g_s$ by repeated application of the operations of multiplication and of taking inverse element. Prove that the set obtained forms a subgroup of the group G.

Definition 45 *The subgroup obtained in task 331 is called the subgroup generated by the elements* $g_1, g_2, \ldots, g_s$

Definition 46 *Let $g_1, g_2, \ldots, g_s$ be the permutations of the sheets of a certain Riemann surface diagram corresponding to loops (counterclockwise) around all the branch points. We will call the subgroup generated by the elements $g_1, g_2, \ldots, g_s$ the permutation group of the sheets of the give Riemann surface diagram.*

Observation 1.If the number of sheets in the diagram is finite (but we consider only such diagrams), then while constructing the permutation group of the sheets of this diagram, it suffices to use the operation of composition of permutations and exclude the operation of taking inverse permutation. In this case any permutation of sheets g has a finite order k: $g^k = e$; therefore $g^{-1} = g^{k-1} = g \cdot g \cdot \ldots \cdot g$.
Observation 2. The permutation group of the sheets which will be constructed below are defined, as usual, upto isomorphism. The numbering of these sheets will be not important, since for different numberings, we obtain different but isomorphic subgroups of the group S_n.

Problem-335 Which of the groups you already know are isomorphic to the permutation group of the Riemann surface diagram of the following functions: a)$\sqrt{z}$, b)$\sqrt[3]{z}$, c)$\sqrt[n]{z}$, d)$\sqrt[3]{z^2-1}$ (see 304), e)$\sqrt[4]{(z-1)^2(z+1)^3}$(see 306)

Problem-336 To which of the groups you already know are the permutation group of the Riemann surface diagram of functions enumerated in the problems :1) 314, 2) 317, 3) 319 isomorphic?

Problem-337 Describe the permutation group of both the Riemann surface diagrams of the function $h(z) = \sqrt{\sqrt{z^2+1}-2}$ built in solution of the problem 328.

Let the point z_0 be neither the branch point nor the ambiguity point of the many-valued function $w(z)$ and let $w_1, w_2, \ldots, w_n$ be all the values of the function $w(z)$ at the point z_0. Consider a continuous curve C begining and ending at the point z_0 and not passing through any branch and ambiguity points of the function $w(z)$. Select a certain value $w_i = w(z_0)$ and define the new value $w_j = w(z_0)$ using continuity along the curve C. Starting with different values w_i we will obtain different values for w_j (otherwise uniqueness will be lost on the curve C^{-1}). Hence, to the curve C there corresponds a certain permutation of the values $w_1, w_2, \ldots, w_n$. In this case, if the permutation g corresponds to the curve C, then the curve C^{-1} corresponds to the permutation g^{-1} and if to the two curves C_1 and C_2 (with both ending at point z_0) there corresponds the permutations g_1 and g_2 then to the curve C_1C_2 there corresponds the permutation g_2g_1 (let us recall that the permutations are carried out from right to left).

Thus, if we consider all possible curves which begin and end at the same point z_0 the permutations corresponding to them will form a group, the permutation group of the values $w(z_0)$.

Problem-338 Let G_1 be the permutation group of the values $w(z_0)$ and G_2 the permutation group of some Riemann surface diagram of the function $w(z)$. Prove that the groups G_1 and G_2 are isomorphic.

Note that in the definition of the permutation group of the values $w(z_0)$ the Riemann surface diagram of the function $w(z)$ was not used. Therefore from the result of problem 335 it follows that the permutation group of the values $w(z_0)$ for an arbitrary point z_0 and the permutation group of the any Riemann surface diagram of the function $w(z)$ are isomorphic. Hence, the permutation groups of the values $w(z_0)$ for all points z_0 and the permutation group of the Riemann surface diagram of the function $w(z)$ are isomorphic, i.e., they are one and the same group. We will call this group the Galois group of the many-valued function $w(z)$ [23].

3.13 Galois group of functions which are expressible in radicals

Let us now move on to prove one of the main theorems of this book.

Theorem 3.6 *If the many-valued function $h(z)$ is expressible in radicals, then the Galois group of the function $h(z)$ is solvable (see Chapter I, Section 14)*

The proof of the above theorem is included in the solutions of the following problems.

Problem-339 Let $h(z) = f(z) + g(z)$ or $h(z) = f(z) - g(z)$ or $h(z) = f(z) \cdot g(z)$ or $h(z) = \dfrac{f(z)}{g(z)}$ and let the Riemann surface diagram of the function $h(z)$ be built from the Riemann surface diagram of the functions $f(z)$ and $g(z)$ by the formal method (theorem 8(a)). Prove that if F and G are the permutation groups of the initial diagrams, then the permutation group of the diagram constructed is isomorphic to a subgroup of the direct product $F \times G$ (see Chapter I, Section 7)

Problem-340 Let H_1 be the permutation group of the diagram built by the formal method in the previous problem and let H_2 be the permutation group of the the true Riemann surface diagram of the function $h(z)$. Prove that there exists a surjective homomorphism (see Chapter I, section 13) of the group H_1 onto the group H_2.

Problem-341 Suppose the Galois group of the functions $f(z)$ and $g(z)$ are solvable. Prove that Galois group of the following functions are also solvable: $h(z) = f(z)+g(z), h(z) = f(z)-g(z), h(z) = f(z) \cdot g(z), h(z) = \dfrac{f(z)}{g(z)}$

Problem-342 Let the Galois group of the function $f(z)$ be solvable. Prove that the Galois group of the function $h(z) = f(z)^n$ is also solvable.

Problem-343 Let H be the permutation group of the Riemann surface diagram of the function $h(z) = \sqrt[n]{f(z)}$ and F the permutation group of the Riemann surface diagram of the function $f(z)$ built using the same cuts. Define a surjective homomorphism from the group H onto the group F.

Problem-344 Prove that the kernel of the homomorphism (see Chapter I, Section 13) defined in the solution of the previous problem is commutative.

Problem-345 Suppose that the Galois group of the function $f(z)$ is solvable. Prove that the Galois group of the function $h(z) = \sqrt[n]{f(z)}$ is also solvable.

The function $h(z) = a$ and the function $h(z) = z$ are single-valued continuous functions on the entire z plane. Therefore, their Riemann surfaces consist of a single sheet and the Galois group corresponding to it is the single element group $\{e\}$ and are therefore solvable. Hence, taking into account the definition of the functions expressible in radicals (Chapter 2, Section 11) and the results of the problems 338, 339 and 342, we obtain the statement of the above theorem.

Observation. For readers familiar with the theory of analytic functions we have the following. If we define the Galois group of the function $h(z)$ as the permutation group of the values of the function $h(z)$ at a certain point z_0, then theorem 11 will be valid for a broader class of functions. For example, to define the function $h(z)$, in addition to constants, identity function, and functions expressible by arithmetic operations and radicals, we can use any single-valued analytic functions (for example, $\exp z, \sin z$, etc.), the many-valued function $\ln z$ and some other functions. In this case the Galois group of the function $h(z)$ will be solvable although it may not be no longer be necessarily finite.

[23] This group is also called the monodromy group

3.14 Abel's theorem

Consider the equation

$$3w^5 - 25w^3 + 60w - z = 0 \tag{3.8}$$

We consider z as a parameter and for each complex value of z will look for all complex roots w of this equation. By virtue of the result of problem 269, this equation for each z has 5 roots (taking into account the multiplicities).

Problem-346 What values of w can be the multiple roots (with multiplicity greater than 1, see Section 8) of the equation $3w^5 - 25w^3 + 60w - z = 0$. For what values of z will there be multiple roots?

It follows that from the solution of the previous problem that for $z = \pm 38$ and $z = \pm 16$, equation (3.8) has 4 different roots and for the remaining values of z this equation has 5 distinct roots. Thus, the function $w(z)$ which expresses the roots of the equation (3.8) in terms of the parameter z takes 4 different value with $z = \pm 38$ and $z = \pm 16$ and takes 5 different values for other values of z. Let us study this function $w(z)$.

First we prove that with a small change in the parameter z the roots of equation (3.8) also vary slightly. This property is made more rigourous in the following problem.

Problem-347 Let z_0 be an arbitrary complex number and w_0 be one of the roots of the equation (3.8) with $z = z_0$. Consider a circle with conveniently small radius r with center at the point w_0. Prove that there exists a real number $\rho > 0$, such that if $|z_0' - z_0| < \rho$ then the disc contains at least one root of the equation (3.8) for $z_0' = z$.

Suppose the function $w(z)$ expresses the roots of the equation (3.8) in terms of the parameter z and let w_0 be one of the values of $w(z_0)$. It follows from the result of problem 344 that if z varies continuously along a curve which starts at the point z_0, then one can choose one of the values $w(z)$ so that the point w, too, moves continuously along a curve starting at the point w_0. In other words, the function $w(z)$ can be defined using continuity along any curve C. If the curve C does not pass through the branch and ambiguity points (p. 98) of the function $w(z)$, then the function $w(z)$ is uniquely defined using continuity along the curve C.

Problem-348 Prove that the points different from $z = \pm 38$ and $z = \pm 16$, can be neither the branch points nor the ambiguity points of the function $w(z)$ which expresses the roots of the equation (3.8) in terms of the parameter z.

The function $w(z)$ which expresses the roots of the equation (3.8) in terms of the parameter z being an algebraic function[24] is "sufficiently good" (see Chapter 2, Section 10), i.e., it possesses the monodromy property. Therefore, one can build the Riemann surface (see 309 and 310) for the function $w(z)$. This Riemann surface has 5 sheets.

In view of the result of problem 345, the only branch points of the function $w(z)$ are the points $z = \pm 38$ and $z = \pm 16$, but so far its not yet fully clear if that is the case.

Problem-349 Suppose it is known that the point $z_0 = +38$ (or $z_0 = -38$, or $z_0 = \pm 16$) is a branch point of the function $w(z)$ which expresses the roots of the equation (3.8) in terms of the parameter z. How are the sheets of the Riemann surface of this function $w(z)$ at the point z_0 joined? (more precisely, along a cut made from the point z_0 to infinity; see observation 2 in Chapter 2, Section 10).

Problem-350 Let $w(z)$ be the function which expresses the roots of the equation (3.8) in terms of the parameter z. Let furthermore, z_0 and z_1 be arbitrary points different from $z = \pm 38$ and $z = \pm 16$ and w_0 and w_1 their images under the mapping $w(z)$. Prove that it is possible to draw a continuous

[24] The many-valued function $w(z)$ is called algebraic, if it expresses in terms of the parameter z all the roots of some equation

$$a_0(z)w^n + a_1(z)w^{n-1} + \ldots + a_n(z)$$

in which all the $a_i(z)$s are polynomials in z. All algebraic functions are analytical.

curve from the point z_0 to the point z_1 not passing through the points $z = \pm 38$ and $z = \pm 16$ and such that its continuous image starting at point w_0 ends at the point w_1.

Problem-351 Prove that all four points $z = \pm 38$ and $z = \pm 16$ are the branch points of function $w(z)$. How does the Riemann surface diagram of the function $w(z)$ look like? Draw all different cases. (we consider two diagrams different if it is not possible to obtain one from the other by a permutation of the sheets and of the branch points).

Problem-352 Find the Galois group of the function $w(z)$ that expresses the roots of equation $3w^5 - 25w^3 + 60w - z = 0$ in terms of parameter z.

Problem-353 Prove that function $w(z)$ which expresses the roots of equation $3w^5 - 25w^3 + 60w - z = 0$ in terms of the parameter z cannot be expressible in radicals.

Problem-354 Prove that the general algebraic equation of degree five $a_0w^5 + a_1w^4 + a_2w^3 + a_3w^2 + a_4w + a_5 = 0$ ($a_0, a_1, a_2, a_3, a_4, a_5$ are complex parameters, $a_0 \neq 0$) is not solvable in radicals, i.e., there are no formulas which expresses the roots of this equation in terms of the coefficients using the operations of addition, subtraction, multiplication, division, raising to a natural degree and extracting root of integer degree.

Problem-355 Consider the equation

$$(3w^5 - 25w^3 + 60w - z)w^{n-5} = 0 \tag{3.9}$$

and prove that for $n > 5$ a general algebraic equation with degree n is not solvable in radicals.

The results of problems 351 and 352 contain the main theorem of this book. We have indeed proved the following theorem.

Theorem 3.7 *Abel's theorem. For $n \geq 5$ the most general algebraic equation of degree n*

$$a_0w^n + a_1w^{n-1} + \ldots + a_{n-1}w + a_n = 0$$

is not solvable in radicals.

Observation 1. The Cardano formula for solving the general algebraic equation of degree three was obtained in the introduction. Moreover the roots of equation were not all the values given by this formula but only those for which an additional condition was satisfied. Therefore the question arises, if for a general equation of degree $n(n \geq 5)$, is it possible to compute a formula in radicals so that its roots are only part of the values given by the formula. Let us show that this cannot be the case even for equation (3.8).

Indeed, if the values of the function $w(z)$ which expresses the roots of the equation (3.8) in terms of the parameter z are only part of the values of a function $w_1(z)$, expressible in radicals, then the Riemann surface of the function $w(z)$ is a separate part of the Riemann surface of the function $w_1(z)$. If G is the Galois group of the function $w_1(z)$, then to every permutation from the group G there corresponds a permutation of the five sheets of the function $w(z)$. This mapping is a homomorphism from the group G to the group S_5. Since the group S_5 is not solvable, the group G is also not solvable (see 163). On the other hand, the group G must be solvable as its the Galois group of a function which is expressible in radicals. This is a contradiction.

Observation 2. From the observation 1 in section 13 of this chapter, it follows that Abel's theorem will hold true if besides radicals we permit, some other functions, for example any single-valued analytic functions ($\exp z, \sin z$ etc.), the function $\ln z$ and some others.

Observation 3. Consider equation (3.8) in the domain of real numbers. Let the function $y(x)$ express the real roots of the equation

$$3y^5 - 25y^3 + 60y - x = 0$$

in terms of the real parameter x. Is it possible to express the function $y(x)$ in radicals? It occurs that we cannot. For those who are familiar with the theory of analytic functions, let us point out that *this follows from the theorem on analytical continuation. Indeed, the function $w(z)$ which expresses the roots of the equation (3.8) in terms of the parameter z is an analytic function. Therefore, if the function $y(x)$ was expressible in radicals, then the same formula considered in the domain of complex numbers will, in view of the theorem about the analytical continuation be the function $w(z)$, i.e., the function $w(z)$ will be expressible in radicals.*

Hence, Abel's theorem will hold true when we consider only the real roots of a general equation of degree $n(n \geq 5)$ with real coefficients. In view of observation 2 above, the theorem will be true even in the case where we permit besides radicals, some other functions, for example all functions which allow single-valued analytical continuation ($\exp x, \sin x$, etc.), the function $\ln x$ and some others.

Observation 4. The class of algebraic functions (see footnote on page 74 is sufficiently rich and interesting. In particular, one can show that all functions which are expressible in radicals are algebraic. We proved that any function which is expressible in radicals has a solvable Galois group (Theorem 11). It turns out that if we limit ourselves to algebraic functions then the converse is true: if the Galois group of a certain algebraic function is solvable then this function is expressible in radicals. Thus, algebraic functions are expressible in radicals $\iff$ its Galois group is solvable. This result is a special case of the general Galois theory (see for example, Chebotarev N. G., (Grundzge der Galois'schen Theorie) Fundamentals of Galois theory:).

On teaching mathematics

On Teaching Mathematics[25]

Mathematics is a part of physics. Physics is an experimental science, a part of natural science. Mathematics is the part of physics where experiments are cheap.

The Jacobi identity (which forces the heights of a triangle to cross at one point) is an experimental fact in the same way as that the Earth is round (that is, homeomorphic to a ball). But it can be discovered with less expense.

In the middle of the twentieth century it was attempted to divide physics and mathematics. The consequences turned out to be catastrophic. Whole generations of mathematicians grew up without knowing half of their science and, of course, in total ignorance of any other sciences. They first began teaching their ugly scholastic pseudo-mathematics to their students, then to schoolchildren (forgetting Hardy's warning that ugly mathematics has no permanent place under the Sun).

Since scholastic mathematics that is cut off from physics is fit neither for teaching nor for application in any other science, the result was the universal hate towards mathematicians – both on the part of the poor schoolchildren (some of whom in the meantime became ministers) and of the users.

The ugly building, built by undereducated mathematicians who were exhausted by their inferiority complex and who were unable to make themselves familiar with physics, reminds one of the rigorous axiomatic theory of odd numbers. Obviously, it is possible to create such a theory and make pupils admire the perfection and internal consistency of the resulting structure (in which, for example, the sum of an odd number of terms and the product of any number of factors are defined). From this sectarian point of view, even numbers could either be declared a heresy or, with passage of time, be introduced into the theory supplemented with a few "ideal" objects (in order to comply with the needs of physics and the real world).

Unfortunately, it was an ugly twisted construction of mathematics like the one above which predominated in the teaching of mathematics for decades. Having originated in France, this pervertedness quickly spread to teaching of foundations of mathematics, first to university students, then to school pupils of all lines (first in France, then in other countries, including Russia).

To the question "what is 2 + 3" a French primary school pupil replied: "3 + 2, since addition is commutative". He did not know what the sum was equal to and could not even understand what he was asked about!

Another French pupil (quite rational, in my opinion) defined mathematics as follows: "there is a square, but that still has to be proved".

[25] This is an extended text of the address at the discussion on teaching of mathematics in Palais de Découverte in Paris on 7 March 1997

Judging by my teaching experience in France, the university students' idea of mathematics (even of those taught mathematics at the École Normale Supérieure – I feel sorry most of all for these obviously intelligent but deformed kids) is as poor as that of this pupil.

For example, these students have never seen a paraboloid and a question on the form of the surface given by the equation $xy = z^2$ puts the mathematicians studying at ENS into a stupor. Drawing a curve given by parametric equations (like $x = t^3 - 3t$, $y = t^4 - 2t^2$) on a plane is a totally impossible problem for students (and, probably, even for most French professors of mathematics).

Beginning with l'Hospital's first textbook on calculus ("calculus for understanding of curved lines") and roughly until Goursat's textbook, the ability to solve such problems was considered to be (along with the knowledge of the times table) a necessary part of the craft of every mathematician.

Mentally challenged zealots of "abstract mathematics" threw all the geometry (through which connection with physics and reality most often takes place in mathematics) out of teaching. Calculus textbooks by Goursat, Hermite, Picard were recently dumped by the student library of the Universities Paris 6 and 7 (Jussieu) as obsolete and, therefore, harmful (they were only rescued by my intervention).

ENS students who have sat through courses on differential and algebraic geometry (read by respected mathematicians) turned out be acquainted neither with the Riemann surface of an elliptic curve $y^2 = x^3+ax+b$ nor, in fact, with the topological classification of surfaces (not even mentioning elliptic integrals of first kind and the group property of an elliptic curve, that is, the Euler-Abel addition theorem). They were only taught Hodge structures and Jacobi varieties!

How could this happen in France, which gave the world Lagrange and Laplace, Cauchy and Poincaré, Leray and Thom? It seems to me that a reasonable explanation was given by I. G. Petrovskii, who taught me in 1966: genuine mathematicians do not gang up, but the weak need gangs in order to survive. They can unite on various grounds (it could be super-abstractness, anti-Semitism or "applied and industrial" problems), but the essence is always a solution of the social problem – survival in conditions of more literate surroundings.

By the way, I shall remind you of a warning of L. Pasteur: there never have been and never will be any "applied sciences", there are only *applications of sciences* (quite useful ones!).

In those times I was treating Petrovskii's words with some doubt, but now I am being more and more convinced of how right he was. A considerable part of the super-abstract activity comes down simply to industrialising shameless grabbing of discoveries from discoverers and then systematically assigning them to epigons-generalizers. Similarly to the fact that America does not carry Columbus's name, mathematical results are almost never called by the names of their discoverers.

In order to avoid being misquoted, I have to note that my own achievements were for some unknown reason never expropriated in this way, although it always happened to both my teachers (Kolmogorov, Petrovskii, Pontryagin, Rokhlin) and my pupils. Prof. M. Berry once formulated the following two principles:

The Arnold Principle. If a notion bears a personal name, then this name is not the name of the discoverer.

The Berry Principle. The Arnold Principle is applicable to itself.

Let's return, however,to teaching of mathematics in France.

When I was a first-year student at the Faculty of Mechanics and Mathematics of the Moscow State University, the lectures on calculus were read by the set-theoretic topologist L. A. Tumarkin, who conscientiously retold the old classical calculus course of French type in the Goursat version. He told us that integrals of rational functions along an algebraic curve can be taken if the corresponding Riemann surface is a sphere and, generally speaking, cannot be taken if its genus is higher, and that for the sphericity it is enough to have a sufficiently large number of double points on the curve of a given degree (which forces the curve to be unicursal: it is possible to draw its real points on the projective plane with one stroke of a pen).

These facts capture the imagination so much that (even given without any proofs) they give a better and more correct idea of modern mathematics than whole volumes of the Bourbaki treatise. Indeed, here we find out about the existence of a wonderful connection between things which seem to be completely different: on the one hand, the existence of an explicit expression for the integrals and the topology of the corresponding Riemann surface and, on the other hand, between the number of double points and genus of the corresponding Riemann surface, which also exhibits itself in the real domain as the unicursality.

Jacobi noted, as mathematics' most fascinating property, that in it one and the same function controls both the presentations of a whole number as a sum of four squares and the real movement of a pendulum.

These discoveries of connections between heterogeneous mathematical objects can be compared with the discovery of the connection between electricity and magnetism in physics or with the discovery of the similarity between the east coast of America and the west coast of Africa in geology.

The emotional significance of such discoveries for teaching is difficult to overestimate. It is they who teach us to search and find such wonderful phenomena of harmony of the Universe.

The de-geometrisation of mathematical education and the divorce from physics sever these ties. For example, not only students but also modern algebro-geometers on the whole do not know about the Jacobi fact mentioned here: an elliptic integral of first kind expresses the time of motion along an elliptic phase curve in the corresponding Hamiltonian system.

Rephrasing the famous words on the electron and atom, it can be said that a hypocycloid is as inexhaustible as an ideal in a polynomial ring. But teaching ideals to students who have never seen a hypocycloid is as ridiculous as teaching addition of fractions to children who have never cut (at least mentally) a cake or an apple into equal parts. No wonder that the children will prefer to add a numerator to a numerator and a denominator to a denominator.

From my French friends I heard that the tendency towards super-abstract generalizations is their traditional national trait. I do not entirely disagree that this might be a question of a hereditary disease, but I would like to underline the fact that I borrowed the cake-and-apple example from Poincaré.

The scheme of construction of a mathematical theory is exactly the same as that in any other natural science. First we consider some objects and make some observations in special cases. Then we try and find the limits of application of our observations, look for counter-examples which would prevent unjustified extension of our observations onto a too wide range of events (example: the number of partitions of consecutive odd numbers 1, 3, 5, 7, 9 into an odd number of natural summands gives the sequence 1, 2, 4, 8, 16, but then comes 29).

As a result we formulate the empirical discovery that we made (for example, the Fermat conjecture or Poincaré conjecture) as clearly as possible. After this there comes the difficult period of checking as to how reliable are the conclusions .

At this point a special technique has been developed in mathematics. This technique, when applied to the real world, is sometimes useful, but can sometimes also lead to self-deception. This technique is called modelling. When constructing a model, the following idealisation is made: certain facts which are only known with a certain degree of probability or with a certain degree of accuracy, are considered to be "absolutely" correct and are accepted as "axioms". The sense of this "absoluteness" lies precisely in the fact that we allow ourselves to use these "facts" according to the rules of formal logic, in the process declaring as "theorems" all that we can derive from them.

It is obvious that in any real-life activity it is impossible to wholly rely on such deductions. The reason is at least that the parameters of the studied phenomena are never known absolutely exactly and a small change in parameters (for example, the initial conditions of a process) can totally change the result. Say, for this reason a reliable long-term weather forecast is impossible and will remain impossible, no matter how much we develop computers and devices which record initial conditions.

In exactly the same way a small change in axioms (of which we cannot be completely sure) is capable, generally speaking, of leading to completely different conclusions than those that are obtained from theorems which have been deduced from the accepted axioms. The longer and fancier is the chain of deductions ("proofs"), the less reliable is the final result.

Complex models are rarely useful (unless for those writing their dissertations).

The mathematical technique of modelling consists of ignoring this trouble and speaking about your deductive model in such a way as if it coincided with reality. The fact that this path, which is obviously incorrect from the point of view of natural science, often leads to useful results in physics is called "the inconceivable effectiveness of mathematics in natural sciences" (or "the Wigner principle").

Here we can add a remark by I. M. Gel'fand: there exists yet another phenomenon which is comparable in its inconceivability with the inconceivable effectiveness of mathematics in physics noted by Wigner – this is the equally inconceivable ineffectiveness of mathematics in biology.

"The subtle poison of mathematical education" (in F. Klein's words) for a physicist consists precisely in that the absolutised model separates from the reality and is no longer compared with it. Here is a simple example: mathematics teaches us that the solution of the Malthus equation $dx/dt = x$ is uniquely defined by the initial conditions (that is that the corresponding integral curves in the (t, x)-plane do not intersect each other). This conclusion of the mathematical model bears little relevance to the reality. A computer experiment shows that all these integral curves have common points on the negative t-semi-axis. Indeed, say, curves with the initial conditions $x(0) = 0$ and $x(0) = 1$ practically intersect at $t = -10$ and at $t = -100$ you cannot fit in an atom between them. Properties of the space at such small distances are not described at all by Euclidean geometry. Application of the uniqueness theorem in this situation obviously exceeds the accuracy of the model. This has to be respected in practical application of the model, otherwise one might find oneself faced with serious troubles.

I would like to note, however, that the same uniqueness theorem explains why the closing stage of mooring of a ship to the quay is carried out manually: on steering, if the velocity of approach would have been defined as a smooth (linear) function of the distance, the process of mooring would have required an infinitely long period of time. An alternative is an impact with the quay (which is damped by suitable non-ideally elastic bodies). By the way, this problem had to be seriously confronted on landing the first descending apparata on the Moon and Mars and also on docking with space stations – here the uniqueness theorem is working against us.

Unfortunately, neither such examples, nor discussing the danger of fetishising theorems are to be met in modern mathematical textbooks, even in the better ones. I even got the impression that scholastic mathematicians (who have little knowledge of physics) believe in the principal difference of the axiomatic mathematics from modelling which is common in natural science and which always requires the subsequent control of deductions by an experiment.

Not even mentioning the relative character of initial axioms, one cannot forget about the inevitability of logical mistakes in long arguments (say, in the form of a computer breakdown caused by cosmic rays or quantum oscillations). Every working mathematician knows that if one does not control oneself (best of all by examples), then after some ten pages half of all the signs in formulae will be wrong and twos will find their way from denominators into numerators.

The technology of combatting such errors is the same external control by experiments or observations as in any experimental science and it should be taught from the very beginning to all juniors in schools.

Attempts to create "pure" deductive-axiomatic mathematics have led to the rejection of the scheme used in physics (observation – model – investigation of the model – conclusions – testing by observations) and its substitution by the scheme: definition – theorem – proof. It is impossible to understand an unmotivated definition but this does not stop the criminal algebraists-axiomatisators. For example, they would readily define the product of natural numbers by means of the long multiplication rule. With this the commutativity of multiplication becomes difficult to prove but it is still possible to deduce it as a theorem from the axioms. It is then possible to force poor students to learn this theorem and its proof (with the aim of raising the standing of both the science and the persons teaching it). It is obvious that such definitions and such proofs can only harm the teaching and practical work.

It is only possible to understand the commutativity of multiplication by counting and re-counting soldiers by ranks and files or by calculating the area of a rectangle in the two ways. Any attempt to do without this interference by physics and reality into mathematics is sectarianism and isolationism which destroy the image of mathematics as a useful human activity in the eyes of all sensible people.

I shall open a few more such secrets (in the interest of poor students).

The *determinant* of a matrix is an (oriented) volume of the parallelepiped whose edges are its columns. If the students are told this secret (which is carefully hidden in the purified algebraic education), then the whole theory of determinants becomes a clear chapter of the theory of poly-linear forms. If determinants are defined otherwise, then any sensible person will forever hate all the determinants, Jacobians and the implicit function theorem.

What is a *group*? Algebraists teach that this is supposedly a set with two operations that satisfy a load of easily-forgettable axioms. This definition provokes a natural protest: why would any sensible person need such pairs of operations? "Oh, curse this maths" – concludes the student (who, possibly, becomes the Minister for Science in the future).

We get a totally different situation if we start off not with the group but with the concept of a transformation (a one-to-one mapping of a set onto itself) as it was historically. A collection of transformations of a set is called a group if along with any two transformations it contains the result of their consecutive application and an inverse transformation along with every transformation.

This is all the definition there is. The so-called "axioms" are in fact just (obvious) *properties* of groups of transformations. What axiomatisators call "abstract groups" are just groups of transformations of various sets considered up to isomorphisms (which are one-to-one mappings preserving the operations). As Cayley proved, there are no "more abstract" groups in the world. So why do the algebraists keep on tormenting students with the abstract definition?

By the way, in the 1960s I taught group theory to Moscow *schoolchildren.* Avoiding all the axiomatics and staying as close as possible to physics, in half a year I got to the Abel theorem on the unsolvability of a general equation of degree five in radicals (having on the way taught the pupils complex numbers, Riemann surfaces, fundamental groups and monodromy groups of algebraic functions). This course was later published by one of the audience, V. Alekseev, as the book *The Abel theorem in problems.*

What is a *smooth manifold*? In a recent American book I read that Poincaré was not acquainted with this (introduced by himself) notion and that the "modern" definition was only given by Veblen in the late 1920s: a manifold is a topological space which satisfies a long series of axioms.

For what sins must students try and find their way through all these twists and turns? Actually, in Poincaré's *Analysis Situs* there is an absolutely clear definition of a smooth manifold which is much more useful than the "abstract" one.

A smooth k-dimensional submanifold of the Euclidean space R^N is its subset which in a neighbourhood of its every point is a graph of a smooth mapping of $\mathbf{R}^k$ into $\mathbf{R}^{N-k}$ (where $\mathbf{R}^k$ and $\mathbf{R}^{N-k}$ are coordinate subspaces). This is a straightforward generalization of most common smooth curves on the plane (say, of the circle $x^2 + y^2 = 1$) or curves and surfaces in the three-dimensional space.

Between smooth manifolds smooth mappings are naturally defined. Diffeomorphisms are mappings which are smooth, together with their inverses.

An "abstract" smooth manifold is a smooth submanifold of a Euclidean space considered up to a diffeomorphism. There are no "more abstract" finite-dimensional smooth manifolds in the world (Whitney's theorem). Why do we keep on tormenting students with the abstract definition? Would it not be better to prove them the theorem about the explicit classification of closed two-dimensional manifolds (surfaces)?

It is this wonderful theorem (which states, for example, that any compact connected oriented surface is a sphere with a number of handles) that gives a correct impression of what modern mathematics is and not the super-abstract generalizations of naive submanifolds of a Euclidean space which in fact do not give anything new and are presented as achievements by the axiomatisators.

The theorem of classification of surfaces is a top-class mathematical achievement, comparable with the discovery of America or X-rays. This is a genuine discovery of mathematical natural science and it is even difficult to say whether the fact itself is more attributable to physics or to mathematics. In its significance for both the applications and the development of correct Weltanschauung it by far surpasses such "achievements" of mathematics as the proof of Fermat's last theorem or the proof of the fact that any sufficiently large whole number can be represented as a sum of three prime numbers.

For the sake of publicity modern mathematicians sometimes present such sporting achievements as the last word in their science. Understandably this not only does not contribute to the society's appreciation of mathematics but, on the contrary, causes a healthy distrust of the necessity of wasting energy on (rock-climbing-type) exercises with these exotic questions needed and wanted by no one.

The theorem of classification of surfaces should have been included in high school mathematics courses (probably, without the proof) but for some reason is not included even in university mathematics courses (from which in France, by the way, all the geometry has been banished over the last few decades).

The return of mathematical teaching at all levels from the scholastic chatter to presenting the important domain of natural science is an espessially hot problem for France. I was astonished that all the best and most important in methodical approach mathematical books are almost unknown to students here (and, seems to me, have not been translated into French). Among these are *Numbers and figures* by Rademacher and Töplitz, *Geometry and the imagination* by Hilbert and Cohn-Vossen, *What is mathematics?* by Courant and Robbins, *How to solve it* and *Mathematics and plausible reasoning* by Polya, *Development of mathematics in the 19th century* by F. Klein.

I remember well what a strong impression the calculus course by Hermite (which does exist in a Russian translation!) made on me in my school years.

Riemann surfaces appeared in it, I think, in one of the first lectures (all the analysis was, of course, complex, as it should be). Asymptotics of integrals were investigated by means of path deformations on Riemann surfaces under the motion of branching points (nowadays, we would have called this the Picard-Lefschetz theory; Picard, by the way, was Hermite's son-in-law – mathematical abilities are often transferred by sons-in-law: the dynasty Hadamard – P. Levy – L. Schwarz – U. Frisch is yet another famous example in the Paris Academy of Sciences).

The "obsolete" course by Hermite of one hundred years ago (probably, now thrown away from student libraries of French universities) was much more modern than those most boring calculus textbooks with which students are nowadays tormented.

If mathematicians do not come to their senses, then the consumers who preserved a need in a modern, in the best meaning of the word, mathematical theory as well as the immunity (characteristic of any sensible person) to the useless axiomatic chatter will in the end turn down the services of the undereducated scholastics in both the schools and the universities.

A teacher of mathematics, who has not got to grips with at least some of the volumes of the course by Landau and Lifshitz, will then become a relict like the one nowadays who does not know the difference between an open and a closed set.

V. I. Arnold
Translated by A. V. GORYUNOV

Index

Abel's theorem, 11, 71
absolute value of a complex number, 44
addition modulo n, 19
algebraic equation in one variable, 7
algebraic representation of complex numbers, 40
alternating group, see group, alternating 34
ambiguity point, 61
argument of a complex number, 44
associativity, 17

Bezout's theorem, 53
bijective mapping, 16
binary operation, 13
branch point, 59
branches of a many-valued function, 54
bundle of branches, 66
bundle of sheets, 68

Cardano's formula, 10
centre of a group, 25
change in the argument, 50
commutative group, 18
commutator, 27
Complex numbers, 35
complex numbers, 39
composition of functions, 47
composition of transformations, 14
continuity, 46
continuous curve, 48
coset
  left coset, 22, 23
cubic equation, 8
cycle, 32
cyclic group, 19
cyclic permutation, 32

De Moivre formula, 45
decomposition of a group by a subgroup
  left decomposition, 23
  right decomposition, 23
derivative of a polynomial, 53
direct product of groups, 22
distributivity, 36
division of polynomials, 38

elementary transpositions, 33
equation of degree four, 10
Euclidean algorithm, 38
even permutation, 33

Ferrari's method, 10
field, 35
field of complex numbers, 39
finite group, 17
free vector, 43
functions expressible by radicals, 64
fundamental theorem of algebra, 53

Galois group, 69
generator of a group, 19
geometrical description of complex numbers, 43
group
  of transformations , 16
  alternating, 34
  commutative , 18
  cyclic, 19
  finite , 17
  Galois , 69
  generator , 19
  infinite , 17
  infinite cyclic , 19
  isomorphism, 20
  monodromy, 69
  of permutations, 32
  of quaternion, 26
  of rotations
    of the cube, 27
    of the dodecahedron, 31

of the octahedron, 27
of symmetries
of a rectangle, 16
of a rhombus, 15
of a square, 15
of a tetrahedron, 22
of a triangle, 15
order, 17
solvable, 31

homomorphism, 28

identity element, 17
identity transformation, 17
image
of a curve, 52
of a set, 30
imaginary part of a complex number, 40
independent cycles, 33
infinite cyclic group, 19
infinite group, 17
inner automorphism, 24
inverse element, 17
inverse mapping, 16
inverse transformation, 16
inversion, 33
irreducible polynomial, 42
isomorphic groups, 20
isomorphism, 20
of fields, 41
of groups, 20

kernel of a homomorphism, 29

Lagrange's theorem, 23
leading coefficient, 37

mapping
bijective, 16
inverse , 16
surjective , 16
minimal extension of a field, 42
modulus of a complex number, 44
monodromy group, 69
monodromy property, 62
multiplication
modulo n, 36
of transformations, 16
table, 14

natural homomorphism, 28
neutral element, 17
normal subgroups, 25

odd permutation, 33
order of a group, 17

parametric equation of a curve, 48
partition of a group by a subgroup
left partition, 23
right partition, 23
permutation, 32
cyclic , 32
even , 33
odd , 33
permutation group , 32
polynomial, 36
irreducible , 42
over a field, 36
reducible , 42
remainder , 38
root, 37
polynomial sums, 37
pre-image, 16
product
of groups, 22
of many-valued functions, 64
of polynomials, 37
of transformations, 14

quadratic equation, 7
quaternions, 26
quotient
group, 26
polynomial, 38
quotient groups, 26

real numbers, 35
real part of a complex number, 40
reducible polynomial, 42
remainder polynomial, 38
Riemann surface, 55
Riemann surface diagram, 59
Riemann surface sheets, 55
root of a polynomial, 37
root of order k, 53
root with multiplicity k, 53

sheets of Riemann surface, 55
solvable groups, 31
subgroup, 21
normal, 25
sum
of many-valued functions, 64
of polynomials, 37
surjective mapping, 16
symmetric group of degree n, 32
symmetry of a geometric object, 14

theorem

Abel, 11
Bezout , 53
fundamental theorem of algebra, 53
Lagrange, 23
Viète, 8
transformation groups, 16
transpositions, 33

trigonometric form of complex numbers, 45

uniqueness of the image, 57
unit element, 17

vector, 43
Viète's theorem, 8