ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2007, Vol. 259, pp. 82–100. © Pleiades Publishing, Ltd., 2007.
Original Russian Text © A.G. Khovanskii, 2007, published in Trudy Matematicheskogo Instituta imeni V.A. Steklova, 2007, Vol. 259, pp. 86–105.

Variations on the Theme of Solvability by Radicals

A. G. Khovanskii [a,b,c]

Received December 2006

To Vladimir Igorevich Arnold,
mathematical idol of my generation

Abstract—We discuss the problem of representability and nonrepresentability of algebraic functions by radicals. We show that the Riemann surfaces of functions that are the inverses of Chebyshev polynomials are determined by their local behavior near branch points. We find lower bounds on the degrees of equations to which sufficiently general algebraic functions can be reduced by radicals. We also begin to classify rational functions of prime degree whose inverses are representable by radicals.

DOI: 10.1134/S0081543807040074

Forty one years ago, in the spring of 1966, Vladimir Igorevich agreed to become my scientific adviser. I was nineteen years old, and Arnold was twenty nine. He started to deliver his "Classical Mechanics" in the fall of 1966. The students of our year were the first listeners. The first impression was that Arnold is a mathematician with extraordinarily broad interests and with his own view of a subject. Mathematics is a whole entity to him, which is permeated by a network of links known only to him.

His seminar on singularity theory dealt with virtually everything. For example, just about that time, the seminar intensively discussed the resolvent problem, which is a variant of Hilbert's 13th problem for algebraic, rather than continuous, functions. Arnold initiated a topological approach to this problem. He suggested considering an algebraic function as a multivalued analytic function of several variables and seeking topological obstacles to the representability of such functions as a composition of algebraic functions of a smaller number of variables.

A few years before that time, as he was training gifted schoolchildren in the Kolmogorov school, Arnold proved, using topological arguments, that a sufficiently general algebraic function of degree ≥ 5 of one variable cannot be represented by radicals. The reason is as follows. It was known even to Frobenius that the monodromy group of an algebraic function is isomorphic to the Galois group of the field of rational functions extended by adding all branches of the algebraic function to this field. According to the Galois theory, an algebraic equation is solvable by radicals if and only if its Galois group is solvable.

Arnold noted that since the monodromy group is a topological invariant, only topology can be responsible for the representability of algebraic functions by radicals. By means of purely topological arguments, without using the Galois theory, he proved that algebraic functions with nonsolvable monodromy group cannot be represented by radicals. Arnold gave a course of lectures on his proof in the Kolmogorov school. Later this course was revised and published by V.B. Alekseev [1].

[a] University of Toronto, Ontario M5S 2E4, Canada.

[b] Independent University of Moscow, Bol'shoi Vlas'evskii per. 11, Moscow, 119002 Russia.

[c] Institute of Systems Analysis, Russian Academy of Sciences, pr. 60-letiya Oktyabrya 9, Moscow, 117312 Russia.
E-mail address: askold@math.toronto.edu

According to Arnold, topological proofs of the unsolvability of some analytic problems are, as a rule, stronger than the proofs of unsolvability obtained by classical means [2–9].

Developing Arnold's approach, I have constructed a topological variant of the Galois theory that yields new, stronger, results on the unsolvability of algebraic and differential equations in an explicit form [10, 11].

In this paper, I present new theorems on the solvability and unsolvability of algebraic equations by radicals. I found these theorems in the fall of 2006 when giving a course of lectures on the Galois theory at the University of Toronto.

The paper is organized as follows. In Section 1, we give explicit formulas for inverting the Chebyshev polynomial of degree n that involve only arithmetic operations and radicals. In Section 2, following Euler, we solve a cubic equation using a formula for inverting the Chebyshev polynomial of degree 3. In Section 3, we recall how a fourth-degree equation can be reduced to a cubic equation.

In Sections 4–6, we calculate the monodromy groups of the functions F_n and $F_n \circ \sigma$ that are the inverses of the Chebyshev polynomial T_n of degree n and of the polynomial $-T_n$, respectively. We show that the Riemann surfaces of these functions are completely determined by their local behavior near the branch points.

In Section 7, we discuss transitive permutation groups. We show that a transitive permutation group of a set of n elements that contains at least one transposition is no less complicated than a symmetric group of p elements, where p is the least prime divisor of the number n. We formulate Galois theorems on a solvable transitive group that acts on a set containing a prime number of elements. These facts are used in the next sections.

In Section 8, we show that an algebraic function of degree n whose discriminant has at least one simple root cannot be reduced, by means of radicals and arithmetic operations, to algebraic functions of degree $p-1$, where p is the least prime divisor of the number n (here, it is assumed that $p \geq 5$).

The Galois theorems on a transitive solvable group acting on a set that contains a prime number p of elements imply very strong constraints on the local behavior of degree p algebraic functions that can be represented by radicals. These constraints affect the global invariants and are discussed in Section 9. For example, we show in Section 9 that all algebraic functions of degree 23 with Riemann surfaces of genus $g = 1$ cannot be represented by radicals.

In Section 10, we show that the inverse of a polynomial of a prime degree p is representable by radicals if and only if, by affine changes of coordinates in the target and source spaces, the polynomial can be reduced either to the Chebyshev polynomial T_p or to the function x^p.

In Section 11, we start a topological classification of rational functions of a prime degree p whose inverses are representable by radicals. In Section 12, we complete this classification for the case of $p \equiv -1 \bmod 12$.

1. CHEBYSHEV POLYNOMIALS AND THEIR INVERSES

The following propositions were likely to be known even to Moivre[1]:

(1) $\cos nx$ *can be represented as a polynomial in* $\cos x$;

(2) $\cos x$ *can be expressed in terms of* $\cos nx$ *by means of arithmetic operations and radicals.*

Let us dwell on these propositions in more detail.

It follows from de Moivre's formula $\cos nx + i \sin nx = (\cos x + i \sin x)^n$ that

$$\cos nx = \sum (-1)^k C_n^{2k} \cos^{n-2k} x \cdot \sin^{2k} x. \qquad (*)$$

[1] Abraham de Moivre (1667–1754), an English mathematician and a friend of Newton and Halley. He is the author of the rule for raising to power and taking the nth root of a complex number.

Definition. By a *normalized Chebyshev polynomial of degree* n we mean the polynomial T_n defined by the formula

$$T_n(u) = \sum (-1)^k C_n^{2k} u^{n-2k} (1-u^2)^k.$$

On the interval $-1 < u < 1$ the polynomial T_n has $n-1$ critical points with critical values 1 and -1. The equalities $T_n(1) = 1$ and $T_n(-1) = (-1)^n$ are valid. These properties define the polynomial T_n. It differs form the classical Chebyshev polynomial of degree n by the factor 2^{n-1}. In what follows, we will refer to the polynomial T_n simply as the *Chebyshev polynomial of degree* n, omitting the world "normalized." Formula $(*)$ implies the following proposition.

Proposition 1. *The equality* $\cos nx = T_n(\cos x)$ *holds.*

Definition. By the *inverse of the Chebyshev polynomial of degree* n we mean the multivalued algebraic function F_n defined by the formula

$$F_n(v) = \frac{\left(v + i\sqrt{1-v^2}\,\right)^{1/n} + \left(v - i\sqrt{1-v^2}\,\right)^{1/n}}{2}. \qquad (**)$$

Clearly, the function F_n is *representable by radicals.*

Proposition 2. *For any point* x*, there exists a branch of the function* F_n *such that the equality* $\cos x = F_n(\cos nx)$ *holds.*

Proof. Let $v = \cos nx$ and $u = \cos x$. By de Moivre's formula,

$$\left(v + i\sqrt{1-v^2}\,\right)^{1/n} = u + i\sqrt{1-u^2}, \qquad \left(v - i\sqrt{1-v^2}\,\right)^{1/n} = u - i\sqrt{1-u^2};$$

hence $u = F_n(v)$.

Corollary 3. *The function* F_n *defines the inverse of the polynomial* T_n*: if* $v = T_n(u)$*, then, for any point* v*, the equality* $u = F_n(v)$ *holds for a certain branch of the function* F_n*.*

2. FUNCTION F_3 AND SOLUTION OF A CUBIC EQUATION

Applying the function F_3, Euler solved a general cubic equation by radicals. Let us reproduce his arguments (in a modified form).

The Chebyshev polynomial $T_3 = 4u^3 - 3u$ has two critical points $u_{1,2} = \pm 1/2$, at which the derivative $T_3'(u) = 12(u^2 - 1/4)$ vanishes.

Proposition 4. *By affine changes of variables, the polynomial* T_3 *can be transformed into any third-degree polynomial* Q *with two critical points. More precisely, the identity* $Q(x) \equiv AT_3(B(x + x_0)) + C$ *holds, where the parameters* A*,* B*,* C*, and* x_0 *can be explicitly expressed in terms of the coefficients of the polynomial* Q *by arithmetic operations and square rooting.*

Proof. If $Q(x) = ax^3 + bx^2 + cx + d$, then $Q' = 3a(x^2 + px + q)$, where $p = 2b/3a$ and $q = c/3a$. By assumption, the discriminant D of the polynomial $x^2 + px + q$ is different from zero. The polynomial $T_3(B(x + x_0))$, where $B = 1/\sqrt{D}$ and $x_0 = p/2$, has the same critical points as the polynomial Q. Therefore, the derivatives of these polynomials differ by a constant factor. Comparing the leading coefficients and the free terms of these polynomials, we see that $Q(x) \equiv AT_3(B(x + x_0)) + C$, where $A = a/4B^3$ and $C = d - AT_3(B(x_0))$.

Corollary 5. *The cubic equation* $Q(x) = ax^3 + bx^2 + cx + d = 0$*, where* Q *is a polynomial with two critical points, can be solved by means of arithmetic operations, square rooting, and composition with the function* F_3*.*

Proof. By Proposition 4, using only arithmetic operations and the operation of square rooting, one can choose the parameters A, B, C, and x_0 so that the identity $Q(x) \equiv AT_3(B(x+x_0))+C$ holds. By virtue of this identity, the roots of the equation $Q(x)=0$ can be represented as $x = B^{-1}F_3(-C/A) - x_0$.

Proposition 6. *By affine changes of variables, the polynomial x^3 can be transformed into any third-degree polynomial Q with one multiple critical point. More precisely, the identity $Q(x) \equiv A(x+x_0)^3+B$ holds, where the parameters A, B, and x_0 can be explicitly expressed in terms of the coefficients of the polynomial Q by means of arithmetic operations.*

Proof. By assumption, the derivative of the polynomial $Q(x)=ax^3+bx^2+cx+d$ has a multiple root. This root is equal to $-b/3a$. The polynomials Q and $(x+x_0)^3$, where $x_0=-b/3a$, have proportional derivatives. Comparing the leading coefficients and the free terms of these polynomials, we see that $Q(x) \equiv A(x+x_0)^3+B$ for $A=a$ and $B=d-ax_0^3$.

Corollary 7. *The cubic equation $Q(x)=ax^3+bx^2+cx+d=0$, where Q is a polynomial with one multiple critical point, is solvable by means of arithmetic operations and composition with the function $v^{1/3}$.*

Proof. By Proposition 6, using only arithmetic operations, one can choose parameters A, B, and x_0 so that the identity $Q(x) \equiv A(x+x_0)^3+B$ holds. By virtue of this identity, the roots of the equation $Q(x)=0$ can be represented as $x=(-B/A)^{1/3}-x_0$.

Thus, a general cubic equation can be explicitly reduced either to the equation $T_3(x)=C$ or to the equation $x^3=C$ and is solvable by radicals. It is well known that a general fourth-degree equation reduces to a cubic equation. Let us recall the corresponding procedure.

3. REDUCTION OF A FOURTH-DEGREE EQUATION TO A THIRD-DEGREE EQUATION

A fourth-degree equation can be reduced to a third-degree equation by considering a pencil of planar quadrics [12].

Proposition 8. *The coordinates of the intersection points of two planar quadrics $P=0$ and $Q=0$, where P and Q are given second-degree polynomials in x and y, can be found by solving one cubic and several quadratic equations.*

Proof. Each quadric of the pencil $P+\lambda Q=0$, where λ is an arbitrary parameter, passes through the required points. For a certain value λ_0 of the parameter λ, the quadric $P+\lambda Q=0$ splits into two straight lines. This value satisfies the cubic equation $\det(\widetilde{P}+\lambda\widetilde{Q})=0$, where $\widetilde{P}$ and $\widetilde{Q}$ are the 3×3 matrices of the quadratic forms corresponding to the equations of the quadrics in homogeneous coordinates. The equation of each of the two straight lines that constitute the quadric $P+\lambda_0 Q=0$ can be found by solving a quadratic equation: each straight line passes through the symmetry center of the quadric and through one of the points of intersection of the quadric with any fixed straight line. To determine the coordinates of the latter point, one should solve a quadratic equation; and the coordinates of the symmetry center are expressed in terms of the coefficients of the quadric by arithmetic operations. The equation of the straight line that passes through two given points can be found by arithmetic operations. If the equations of the straight lines into which the quadric $P+\lambda_0 Q=0$ splits are known, then the required points are determined by solving quadratic equations for the points of intersection of the quadric $P=0$ with each of the two straight lines that constitute the quadric.

Corollary 9. *A general fourth-degree equation can be reduced to a cubic equation by arithmetic operations and square rooting.*

Proof. The roots of the equation $a_0x^4+a_1x^3+a_2x^2+a_3x+a_4=0$ are the projections of the intersection points of the quadrics $y=x^2$ and $a_0y^2+a_1xy+a_2y+a_3x+a_4=0$ onto the x-axis.

4. PERMUTATION GROUP GENERATED BY TWO INVOLUTIONS WHOSE PRODUCT IS A CYCLIC ELEMENT

Let us represent the group $S(n)$ as the permutation group of a set A of n elements. In this section, we describe all possible triples a, b, c of elements of the group $S(n)$ such that

(1) $a^2 = b^2 = e$,

(2) $c = ab$,

(3) the element c defines a transformation of A that has a unique orbit of length n.

Consider two examples in which the set A is the ring $\mathbb{Z}/n\mathbb{Z}$ of residues modulo n.

Example 1. Let a_1 and b_1 be permutations of the set $\mathbb{Z}/n\mathbb{Z}$ that take any element $x \in \mathbb{Z}/n\mathbb{Z}$ to the elements $a_1(x) \equiv -x \bmod n$ and $b_1(x) \equiv -x - 1 \bmod n$, respectively. It is obvious that the permutations a_1^2 and b_1^2 are the identities, while the permutation $c_1(x) = a_1(b_1(x))$ is defined by the formula $c_1(x) \equiv x + 1 \bmod n$ and is cyclic.

If we interchange the permutations a_1 and b_1 in Example 1, then their product is still a cyclic permutation. Indeed, $b_1 a_1 = (a_1 b_1)^{-1}$. Example 2 is obtained from Example 1 by changing the order of permutations and reversing the cyclic order in the set A.

Example 2. Let a_2 and b_2 be permutations of the set $\mathbb{Z}/n\mathbb{Z}$ that take any element $x \in \mathbb{Z}/n\mathbb{Z}$ to the elements $a_2(x) \equiv -x + 1 \bmod n$ and $b_2(x) \equiv -x \bmod n$, respectively. It is easily seen that the permutations a_2^2 and b_2^2 are the identities, while the permutation $c_2(x) = a_2(b_2(x))$ is defined by the formula $c_2(x) \equiv x + 1 \bmod n$ and is cyclic.

Naturally, Example 1 is also obtained from Example 2 by changing the order of permutations and reversing the cyclic order. For odd n, each involution in Examples 1 and 2 has exactly one fixed point. It can easily be shown (see the proof of Theorem 10) that for any odd n there exists a one-to-one transformation of the ring $\mathbb{Z}/n\mathbb{Z}$ that takes the involutions a_1 and b_1 from Example 1 to the involutions a_2 and b_2 from Example 2. For even n the situation is different: the involution a_1 has two fixed points, while the involution a_2 has none.

Theorem 10. *Suppose that permutations a, b, and c in the group $S(n)$ satisfy the conditions listed at the beginning of this section.*

(1) *If n is odd, then A can be identified with $\mathbb{Z}/n\mathbb{Z}$ so that the permutations a, b, and c correspond to the elements a_1, b_1, and c_1 from Example 1, as well as so that they correspond to the elements a_2, b_2, and c_2 from Example 2.*

(2) *If n is even, then either a has two fixed points and b has none, or b has two fixed points and a has none. In the first case, A can be identified with $\mathbb{Z}/n\mathbb{Z}$ so that the permutations a, b, and c correspond to the elements a_1, b_1, and c_1 from Example 1, and in the second case, so that the permutations a, b, and c correspond to the elements a_2, b_2, and c_2 from Example 2.*

Proof. By assumption, the element c defines a cyclic transformation of the set A. Therefore, the set A can be identified with the ring $\mathbb{Z}/n\mathbb{Z}$ so that $c(x) \equiv x + 1 \bmod n$. Then $cb(x) \equiv b(x) + 1 \bmod n$ and $(cb)^2(x) \equiv b(b(x) + 1) + 1 \bmod n$. However, by assumption, $cb = a$ and $a^2 = e$; hence, $(cb)^2(x) \equiv x \bmod n$. Taking into account that $c(x) \equiv x + 1 \bmod n$, we obtain $b(b(x) + 1) \equiv x - 1 \bmod n$. Since $b^2 = e$, we have $b(x) + 1 \equiv b(x - 1)$, or $b(x) + x \equiv b(x - 1) + (x - 1) \bmod n$. The last equality implies that $b(x) + x \bmod n$ does not depend on x. Denote $b(x) + x$ by l. We have $b(x) \equiv -x + l \bmod n$. For any $q \in \mathbb{Z}/n\mathbb{Z}$, consider a new variable $u = x - q \bmod n$, $x = u + q \bmod n$. In terms of the variable u, the mapping c is defined, as before, by the formula $c(u) \equiv u + 1 \bmod n$. The mapping b is expressed as $b(u) \equiv -u - 2q + l \bmod n$. For odd n, the residue 2 is invertible in the ring $\mathbb{Z}/n\mathbb{Z}$; therefore, we can choose q such that $2q \equiv l + 1 \bmod n$ or $2q \equiv l \bmod n$. Accordingly, the mapping b is defined by the formula $b(u) \equiv -u - 1 \bmod n$ or the formula $b(u) \equiv -u \bmod n$. The formulas for the transformations b and c are identical to the formulas for b_1

and c_1 from Example 1 and to the formulas for b_2 and c_2 from Example 2, respectively. Therefore, for odd n, we can establish a one-to-one correspondence between the set A and the ring $\mathbb{Z}/n\mathbb{Z}$ so that the elements a, b, and c correspond to the elements a_1, b_1, and c_1 from Example 1, as well as so that they correspond to the elements a_2, b_2, and c_2 from Example 2.

If n is even, then we can choose q so that $2q \equiv l+1 \bmod n$ for odd l and so that $2q \equiv l \bmod n$ for even l. Under the change of the variable $x = u + q \bmod n$, $u = x - q \bmod n$, the formulas for the transformations b and c become identical to the formulas for b_1 and c_1 from Example 1 and to the formulas for b_2 and c_2 from Example 2, respectively.

The theorem implies the following

Corollary 11. *Under the conditions of Theorem* 10*, the transformation group of A generated by the elements a, b, and c is isomorphic to the group of self-mappings of the ring $\mathbb{Z}/n\mathbb{Z}$ that have the form $x \to ax + b \bmod n$, where $a = \pm 1$ and b is an arbitrary element of the ring $\mathbb{Z}/n\mathbb{Z}$.*

Let us rewrite Examples 1 and 2 in a different form that will be used below.

Example 3. Consider a set $A = \{V_0, \dots, V_{n-1}\}$ and the following two involutions a and b of A whose product ab defines a cyclic permutation of A:

(1) under the involution a, the point V_0 is fixed; the points V_{2m-1} and V_{2m}, where $0 < 2m < n$, change places; for even n, the last point V_{n-1} is fixed;

(2) under the involution b, the points V_{2m} and V_{2m+1}, where $0 \le 2m < n-1$, change places; for odd n, the last point V_{n-1} is fixed.

Corollary 12. *There exists an identification of the set A from Example* 3 *with the ring $\mathbb{Z}/n\mathbb{Z}$ such that the involutions a and b correspond to the involutions a_1 and b_1 from Example* 1*. For odd n, there also exists an identification such that the involutions a and b correspond to the involutions a_2 and b_2 from Example* 2*.*

The following example is obtained from Example 3 by interchanging the involutions a and b.

Example 4. Consider a set $\widetilde{A} = \{\widetilde{V}_0, \dots, \widetilde{V}_{n-1}\}$ and the following two involutions $\widetilde{a}$ and $\widetilde{b}$ of $\widetilde{A}$ whose product $\widetilde{a}\widetilde{b}$ defines a cyclic permutation of $\widetilde{A}$:

(1) under the involution $\widetilde{a}$, the points $\widetilde{V}_{2m}$ and $\widetilde{V}_{2m+1}$, where $0 \le 2m < n-1$, change places; for odd n, the last point $\widetilde{V}_{n-1}$ is fixed;

(2) under the involution $\widetilde{b}$, the point $\widetilde{V}_0$ is fixed; the points $\widetilde{V}_{2m-1}$ and V_{2m}, where $0 < 2m < n$, change places; for even n, the last point $\widetilde{V}_{n-1}$ is fixed.

Corollary 13. *There exists an identification of the set $\widetilde{A}$ from Example* 3 *with the ring $\mathbb{Z}/n\mathbb{Z}$ such that the involutions $\widetilde{a}$ and $\widetilde{b}$ correspond to the involutions a_2 and b_2 from Example* 1*. For odd n, there also exists an identification such that the involutions $\widetilde{a}$ and $\widetilde{b}$ correspond to the involutions a_1 and b_1 from Example* 1*.*

5. MONODROMY REPRESENTATIONS OF THE FUNCTIONS F_n AND $F_n \circ \sigma$

Consider the algebraic function F_n, which is the inverse of the Chebyshev polynomial T_n of degree n (see Section 1). The polynomial T_n has two critical values: 1 and -1. Therefore, the algebraic function F_n has three branch points on the Riemann sphere $\overline{\mathbb{C}}$: $+1$, -1, and ∞. Let $\sigma\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ be the involution defined by the formula $\sigma(x) = -x$. The algebraic function $F_n \circ \sigma$ has the same branch points as F_n. For odd n, the Chebyshev polynomial is an odd function. Therefore, for odd n, the functions F_n and $F_n \circ \sigma$ differ only by sign, $F_n \circ \sigma = -F_n$.

Let U be the complement $\overline{\mathbb{C}} \setminus \{1, -1, \infty\}$ of the branch points of the functions F_n and $F_n \circ \sigma$ on the Riemann sphere. Consider the fundamental group $\pi_1(U, 0)$ of the domain U with the marked point 0. Take the loops γ_1 and γ_2 described below as generators in the group $\pi_1(U, 0)$.

The loop $\gamma_1\colon [0,1] \to U$ corresponds to the following motion of the point $\gamma_1(t)$: first, the point moves along the real line segment $I_1 = [0, 1-\varepsilon]$, where $\varepsilon > 0$ is a small positive number, from zero to the point $1-\varepsilon$, then it goes around the point 1 in the counterclockwise direction along the circle of radius ε, and then returns to zero along the segment I_1.

The loop $\gamma_2\colon [0,1] \to U$ is defined by the formula $\gamma_2(t) = -\gamma_1(t)$.

The definitions of the loops γ_1 and γ_2 show that in the fundamental group $\pi_1(U, 0)$ the loop $\gamma_3 = \gamma_2\gamma_1$ is equal to the loop that winds around the point ∞ in the clockwise direction.

Proposition 14. *After going around the loop $\gamma_2\gamma_1$,*

(1) *the branches of the function F_n are cyclically permuted,*

(2) *the branches of the function $F_n \circ \sigma$ are cyclically permuted.*

Proof. The functions F_n and $F_n \circ \sigma$ are the inverses of the polynomials T_n and $-T_n$, and the loop $\gamma_2\gamma_1$ in the domain U is homotopic to the loop that winds once around the point ∞.

The restriction of the polynomial T_n to the interval $-1 \le u \le 1$ has two boundary and $n-1$ internal extremum points u_i, where $-1 = u_0 < \ldots < u_n = 1$. If $n - i \equiv 0 \bmod 2$, then $T_n(u_i) = 1$. If $n - i \equiv 1 \bmod 2$, then $T_n(u_i) = -1$. The points u_i divide the interval $[-1, 1]$ into n segments with common endpoints. On the segments $I_{2m} = [u_{n-2m-1}, u_{n-2m}]$, where $0 \le 2m < n$, the function T_n increases monotonically from -1 to $+1$. On the segments $I_{2m-1} = [u_{n-2m}, u_{n-2m+1}]$, where $0 < 2m \le n$, it decreases monotonically from $+1$ to -1.

On the segments $I_0, \ldots, I_{n-1}$ defined above, the function T_n is monotonic and takes all values between -1 and 1; therefore, the inverse function F_n has n real branches on the interval $-1 \le v \le 1$. We will call a branch of F_n that takes values on the segment I_j the *j th branch* and denote it by V_j. Theorems 15 and 16 given below describe the monodromy group of the function F_n for odd and even n, respectively.

Theorem 15. *After going around the loops γ_1 and γ_2, the permutation of the set $V_0, \ldots, V_{n-1}$ of branches of the function F_n is given by the involutions a and b described in Example* 3.

Proof. Let us describe the monodromy transformation of the branches of the function F_n after going around the loop γ_1. When moving along the segment $[0, 1]$, the branch V_{2m} increases to u_{n-2m}, while the branch V_{2m-1} decreases to u_{n-2m}. For $0 < 2m < n$, the point u_{n-2m} is a point of nondegenerate local maximum of the function T_n, and the two branches V_{2m} and V_{2m-1} of the inverse function F_n, which take the value u_{n-2m} at the point 1, permute after going around the point 1 (just as the two branches of the function $\sqrt{z}$ permute when z winds once around the point 0). At the point $u_n = 1$, the derivative $T_n'(1)$ is different from zero; therefore, the branch V_0 of the function F_n is analytically continued to a neighborhood of the point 1 and preserves its value after going around the point 1. Similarly, for even n, the branch V_{n-1} is equal to 1 at the point 1, is regular at this point, and returns to its previous value after going around this point.

For the monodromy transformation corresponding to the loop γ_2, the assertion of the theorem is proved in a similar way.

Denote by $\widetilde{V}_j$ the branch of the function $F_n \circ \sigma$ on $[-1, 1]$ defined by the formula $\widetilde{V}_j = V_j \circ \sigma$, where $j = 0, \ldots, n-1$.

Theorem 16. *After going around the loops γ_1 and γ_2, the permutation of the set $\widetilde{V}_0, \ldots, \widetilde{V}_{n-1}$ of branches of the function $F_n \circ \sigma$ is given by the involutions $\widetilde{a}$ and $\widetilde{b}$ described in Example* 4.

Theorem 16 is a direct corollary to Theorem 15.

Corollary 17. *The monodromy groups of the functions F_n and $F_n \circ \sigma$ are isomorphic to the group of all transformations of the form $x \to \pm x + b \bmod n$ of the ring $\mathbb{Z}/n\mathbb{Z}$.*

6. RIEMANN SURFACES OF THE FUNCTIONS F_n AND $F_n \circ \sigma$ ARE DEFINED BY LOCAL DATA

In this section, we describe the Riemann surfaces of the algebraic functions F_n and $F_n \circ \sigma$ in terms of their local behavior in a neighborhood of the branch points.

Consider a triple $(\pi, R, \overline{\mathbb{C}})$ consisting of a connected Riemann surface R of some n-valued algebraic function and its natural projection $\pi\colon R \to \overline{\mathbb{C}}$ onto the Riemann sphere $\overline{\mathbb{C}}$. Suppose that the n-sheeted branched covering $\pi\colon R \to \overline{\mathbb{C}}$ has three branch points -1, 1, and ∞. Suppose that

(1) after going around each of the points 1 and -1, one obtains an involution of the set of sheets of the algebraic function in the monodromy group of the covering;

(2) after going around ∞, the sheets of the algebraic function are cyclically permuted.

Theorem 18. *Under conditions* (1) *and* (2), *the triple* $(\pi, R, \overline{\mathbb{C}})$ *is either the Riemann surface of the function* F_n *or the Riemann surface of the function* $F_n \circ \sigma$.

More precisely, either there exists a biholomorphic map $h_1\colon \mathbb{C} \to R$ *such that* $\pi \circ h_1 = T_n$, *or there exists a biholomorphic map* $h_2\colon \mathbb{C} \to R$ *such that* $\pi \circ h_2 = -T_n$. *For odd* n *these two possibilities hold simultaneously, while for even* n *only one of them holds.*

Proof. Let U be the complement of the branch point set of the covering $\pi\colon R \to \overline{\mathbb{C}}$ on the Riemann sphere and $M\colon \pi_1(U, 0) \to S(n)$ be the monodromy homomorphism. According to Theorem 10, if n is odd, then up to conjugation of the group $S(n)$ there exists a unique homomorphism M satisfying the conditions of Theorems 18. By Theorems 15 and 16, the functions F_n and $F_n \circ \sigma$ have precisely such a monodromy homomorphism. For even n, according to Theorem 10, there are two such homomorphisms. By Theorems 15 and 16, the monodromy homomorphisms of the functions F_n and $F_n \circ \sigma$ correspond precisely to these two homomorphisms. (The difference between them is as follows: the monodromy transformation corresponding to the loop γ_1 has two fixed points for the function F_n and no fixed point for the function $F_n \circ \sigma$.)

The following classical theorem is known (see, for example, [12]): If the monodromy homomorphisms of two n-sheeted branched coverings $\pi_1\colon R_1 \to \overline{\mathbb{C}}$ and $\pi_2\colon R_2 \to \overline{\mathbb{C}}$ with identical branch point sets coincide up to conjugation of the group $S(n)$, then there exists a biholomorphic mapping $h\colon R_1 \to R_2$ such that $\pi_1 = \pi_2 \circ h$. The coverings $T_n\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ and $-T_n\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ represent the Riemann surfaces of the functions F_n and $F_n \circ \sigma$, respectively. Theorem 18 is proved.

We will need one (obvious) proposition of the same nature as Theorem 18. Consider a triple $(\pi, R, \overline{\mathbb{C}})$ consisting of a connected Riemann surface R of some n-valued algebraic function and its natural projection $\pi\colon R \to \overline{\mathbb{C}}$ onto the Riemann sphere $\overline{\mathbb{C}}$. Suppose that the n-sheeted branched covering $\pi\colon R \to \overline{\mathbb{C}}$ has two branch points 0 and ∞.

Proposition 19. *Under the above-listed conditions, the triple* $(\pi, R, \overline{\mathbb{C}})$ *is the Riemann surface of the function* $v^{1/n}$. *More precisely, there exists a biholomorphic mapping* $h_1\colon \mathbb{C} \to R$ *such that* $\pi \circ h_1 = u^n$.

Proof. The fundamental group of the domain $U = \overline{\mathbb{C}} \setminus \{0, \infty\}$ is isomorphic to the additive group of integers $\mathbb{Z}$. Up to conjugation of the group $S(n)$, there exists a unique homomorphism of the group $\mathbb{Z}$ to the group $S(n)$ such that the image of the group $\mathbb{Z}$ is transitive. Therefore, any two n-sheeted branched coverings with branch points 0 and ∞ are equivalent to each other and, hence, to the Riemann surface of the function $v^{1/n}$.

7. TRANSITIVE GROUPS OF PERMUTATIONS OF FINITE SETS

Here we discuss a few propositions on transitive permutation groups that will be needed below.

Suppose that a group G acts transitively on a set A. Fix a point x in A and denote by G_x the stabilizer subgroup of the point x. The action of G on A can be recovered by the pair of groups

$G_x \subset G$: the points of the set A can be identified with the right cosets of the subgroup G_x in the group G (the right coset of an element h is the set of elements of the group that can be represented as hg, where $g \in G_x$). Under this identification, the action of the group G on A turns into the action of G on the right cosets of the subgroup G_x by left multiplication.

Suppose that an equivalence relation is introduced in A. This relation is said to be *G-invariant* if the relation $g(a) \approx g(b)$ holds for any element g of the group G and any pair of equivalent points $a \approx b$ of the set A. Let us describe all possible G-invariant equivalence relations on the set A.

Let F be an arbitrary subgroup in G that contains the subgroup G_x. Then F generates the following equivalence relation on the set A: points a and b are said to be *F-equivalent* if $a = g_1(x)$, $b = g_2(x)$, and the elements g_1 and g_2 belong to the same right coset of the subgroup F. One can easily verify the following proposition.

Proposition 20. *The F-equivalence is well defined and G-invariant. For different subgroups F, the F-equivalence relations are different. Every G-invariant equivalence relation is the F-equivalence for some subgroup $F \supseteq G_x$.*

Corollary 21. *Suppose that a group G acts transitively on a finite set A and a G-invariant equivalence relation is introduced. Then each equivalence class contains the same number of points.*

Suppose that a transitive group G of transformations of a set A contains a transposition. With the set A and the group G, we associate the following graph A_G: the vertices of the graph are points of the set A; two vertices $a, b \in A$ are connected by an edge if and only if the group G contains a transposition that permutes the points a and b.

Proposition 22. *Suppose that vertices a and b of the graph A_G are connected by an edge. Then, for any element g of the group G, the vertices $g(a)$ and $g(b)$ are also connected by an edge.*

Proof. Suppose that a transposition $\sigma \in G$ permutes the points a and b. Then $g\sigma g^{-1}$ is an involution that permutes the points $g(a)$ and $g(b)$.

Suppose that a group containing a transposition acts transitively on a set A. Introduce the following equivalence relation on the set A: *two points $a, b \in A$ are equivalent if the vertices a and b of the graph A_G belong to the same connected component of this graph.*

Corollary 23. *The equivalence relation introduced is G-invariant. In particular, all equivalence classes contain the same number of points.*

Proof. The first assertion of the corollary follows from Proposition 22, and the second follows from Corollary 21.

Proposition 24. *If a transitive group of permutations of a finite set A is generated by transpositions, then it coincides with the group of all permutations of the set A.*

A proof of this simple proposition can be found, for example, in [10].

Suppose that a group G acts transitively on a set A and contains at least one transposition. Then the following theorem holds.

Theorem 25. *There exists a G-invariant equivalence relation on A such that*

(1) *each equivalence class contains at least two points*;

(2) *the set H of all permutations of A that preserve the equivalence relation is a normal subgroup of the group G.*

Proof. Consider the same equivalence relation in A as in Corollary 23. It follows from Proposition 24 that the group G contains all permutations of the set A that preserve this equivalence relation. These permutations form the normal subgroup H mentioned in the theorem.

Corollary 26. *Suppose that the conditions of Theorem 25 hold and the set A contains n elements. Then the number n has a divisor $k > 1$, $n = km$, such that the group G contains a normal*

subgroup H isomorphic to the direct sum of m copies of the symmetric group $S(k)$. Therefore, in particular, the group G contains a subgroup isomorphic to the symmetric group $S(p)$, where p is the least prime divisor of the number n.

Galois obtained remarkable results on solvable groups that act transitively on sets with a prime number of elements. Below we formulate his results (we call them the first and the second Galois theorems on solvable groups) and discuss their corollaries.

First, we introduce necessary notation. Let $m \in \mathbb{Z}$ be a natural number, $\mathbb{Z}/m\mathbb{Z}$ be the ring of residues modulo m, and $(\mathbb{Z}/m\mathbb{Z})^*$ be the multiplicative group of elements in $(\mathbb{Z}/m\mathbb{Z})^*$ that are invertible with respect to multiplication. The *metacyclic group* M_m is the group of all permutations g of the set $\mathbb{Z}/m\mathbb{Z}$ of the form $g(x) \equiv ax + b \bmod m$, where $a \in (\mathbb{Z}/m\mathbb{Z})^*$ and $b \in \mathbb{Z}/m\mathbb{Z}$. The map $\pi\colon M_m \to \mathbb{Z}/m\mathbb{Z}$ that takes each element $g \in M_m$, where $g(x) \equiv ax+b$, to the element $a \in (\mathbb{Z}/m\mathbb{Z})^*$ is a homomorphism of the group M_m onto the group $(\mathbb{Z}/m\mathbb{Z})^*$. Denote by $H(m)$ the cyclic group of order m that consists of all permutations g of the set $\mathbb{Z}/m\mathbb{Z}$ of the form $g(x) \equiv x + b \bmod m$, where $b \in \mathbb{Z}/m\mathbb{Z}$. The group $H(m)$ is the kernel of the above homomorphism. The groups H_m and $(\mathbb{Z}/m\mathbb{Z})^*$ are commutative. Therefore, *the metacyclic group M_m is solvable.*

The first Galois theorem on solvable groups. *Let G be a transitive group of permutations of a finite set A that contains a prime number p of elements. Then the group G is solvable if and only if there exists an identification $\phi\colon A \to (\mathbb{Z}/p\mathbb{Z})^*$ of the set A with the field of residues modulo p such that the group corresponding to G under this identification lies in the metacyclic group M_p and contains the normal subgroup H_p.*

The second Galois theorem on solvable groups. *A transitive group of transformations of a finite set containing a prime number of elements is solvable if and only if any transformation in this group that has at least two fixed points is the identity transformation.*

The elegant and simple Galois theorems on solvable groups are closely related to each other. In slightly different formulations they are given, for example, in the book [14]. The second Galois theorem imposes strong constraints on the cyclic type of each permutation g in the group G. Namely, the following proposition holds.

Corollary 27. *A transitive group G of transformations of a set A containing a prime number p of elements is solvable if and only if the action of any nonidentity transformation $g \in G$ splits the set A*

(1) *either into one orbit of length p;*
(2) *or into one orbit of length 1 and $(p-1)/l$ orbits of length l, where $l > 1$ is an arbitrary natural divisor of the number $p-1$.*

Proof. According to the second Galois theorem, a group G satisfying the conditions of the corollary is solvable. Suppose that G is solvable and a transformation $g \in G$ has two orbits of different lengths k and m each of which contains more than one point. We can assume that $k > m > 1$. The transformation g^m has at least $m > 1$ fixed points; however, it is not the identity transformation. By the second Galois theorem, the group G is nonsolvable. This implies the assertion of the corollary.

8. LOCAL MONODROMY AND UNSOLVABILITY OF ALGEBRAIC EQUATIONS IN AN EXPLICIT FORM

Consider an irreducible algebraic equation

$$y^n + R_1 y^{n-1} + \ldots + R_n = 0 \qquad (***)$$

whose coefficients belong to the field $\mathbb{C}\langle x\rangle$ of rational functions of one variable x. It was known even to Frobenius that *the Galois group of equation $(***)$ over the field $\mathbb{C}\langle x\rangle$ is isomorphic to the*

monodromy group of the algebraic function y of the variable x defined by equation $(***)$ (see, for example, [11–13]).

An algebraic equation over a field K *is solvable by k-radicals* if there exists a chain of extensions $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$ such that the field K_{j+1} is obtained from the field K_j by adding either a radical or an algebraic element of degree $\leq k$ over the field K_j and the field K_m contains all solutions of equation $(***)$. An algebraic function of x *is representable by k-radicals* if the irreducible algebraic equation that defines this function is solvable by k-radicals over the field $\mathbb{C}\langle x\rangle$. The solvability of an equation by k-radicals can be determined by its Galois group. A group G is said to be k-solvable if it has a normal tower of subgroups $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = e$ such that each factor group G_i/G_{i+1} is either commutative or isomorphic to a subgroup of the group $S(k)$. The following criterion holds.

Criterion of solvability by k-radicals (see [11, 13])**.** *An algebraic equation over a field of characteristic zero is solvable by k-radicals if and only if its Galois group is k-solvable.*

It is easily seen that *the subgroups and factor groups of a k-solvable group are k-solvable.* Therefore, *for $m > k \geq 4$, the group $S(m)$ is not k-solvable*: the group $S(m)$ contains the simple subgroup $A(m)$, which is not commutative and not isomorphic to a subgroup of the group $S(k)$.

Theorem 28. *Suppose that an irreducible algebraic equation of degree n over a field K of characteristic zero is such that its Galois group, considered as a group of permutations of the roots of the equation, contains at least one transposition. Let the least prime divisor p of n be greater than* 3*. Then the equation is unsolvable by $(p-1)$-radicals over the field K.*

Proof. By Theorem 25, the Galois group contains a subgroup isomorphic to $S(p)$. By hypothesis, $p \geq 5$; therefore, the Galois group is not $(p-1)$-solvable. Now, Theorem 28 follows from the criterion of solvability by k-radicals.

Corollary 29. *Suppose that the monodromy group of an n-valued algebraic function y contains at least one transposition, and let the least prime divisor p of n be greater than* 3*. Then the function y is not representable by $(p-1)$-radicals.*

Corollary 30. *Suppose that an n-valued algebraic function y is defined by an irreducible equation $P_0y^n + \ldots + P_{n-1}y + P_n = 0$ with polynomial coefficients. Suppose that the discriminant of this equation has at least one simple root at which the polynomial P_0 does not vanish, and let the least prime divisor p of n be greater than* 3*. Then the function y is not representable by $(p-1)$-radicals.*

Proof. Indeed, after going around a simple root of the discriminant that is not a root of the leading coefficient, two branches of the algebraic function are transposed.

Proposition 31. *The estimate in Corollary* 29 *is sharp*; *i.e., there exists an algebraic function y that satisfies the conditions of Theorem* 28 *and is representable by p-radicals.*

Proof. Let $p \geq 5$ be the least prime divisor of the number n and $n = pk$. Consider an arbitrary general algebraic function w of degree k all of whose branch points are nonmultiple (after going around such points, two branches of the algebraic function w are transposed) and are different from 0 and ∞. The algebraic function y defined by the formula $y(x) = w(x^{1/k})$ is of degree n, and all branch points of this function, except the points 0 and ∞, are nonmultiple. By construction, the function y is representable by p-radicals. By Theorem 28, it is not representable by $(p-1)$-radicals.

Corollary 29 can be strengthened as follows.

Theorem 28′. *If y satisfies the conditions of Corollary* 29 (*and, in particular, if it satisfies the conditions of Corollary* 30)*, then y cannot be expressed in terms of meromorphic functions by means of compositions, arithmetic operations, solutions of algebraic equations of degree $< p$, square rooting, and indefinite integration.*

Proof. Theorem 28′ follows from Corollary 29 and from an assertion that was proved in the topological version of the Galois theory (see [11]) and that is a necessary condition for the representability of functions by $(p-1)$-quadratures.

9. ALGEBRAIC FUNCTIONS OF PRIME DEGREE THAT ARE REPRESENTABLE BY RADICALS

Galois found the following

Criterion of solvability by radicals (see [13, 14])**.** *An algebraic equation over a field of characteristic zero is solvable by radicals if and only if its Galois group is solvable.*

The second Galois theorem on solvable groups (see Section 7) allows one to reformulate this criterion for irreducible equations of prime degree as follows.

Galois theorem. *An irreducible algebraic equation of prime degree over a field of characteristic zero is solvable by radicals over this field if and only if each nonidentity transformation in its Galois group has at most one fixed point among the roots of the equation.*

Since the monodromy group of an algebraic function is isomorphic to the Galois group of its equation over the field of rational functions, the Galois criterion gives necessary and sufficient conditions for the representability of an algebraic function by radicals in terms of its monodromy group (see [11, 12]). In particular, if an algebraic function of prime degree is representable by radicals, then its behavior near the branch points must obey very strong constraints imposed by the Galois criterion.

Theorem 32. *If an algebraic function y of prime degree p is representable by radicals, then, after going around any of its branch points, one obtains either a cyclic permutation of the sheets of the function y or a permutation that can be decomposed into cycles one of which has unit length and all the other have equal lengths.*

Proof. Theorem 32 follows from the Galois theorem and Corollary 27.

Let $\pi\colon R \to \overline{\mathbb{C}}$ be the natural projection of the Riemann surface of an algebraic function onto the Riemann sphere $\overline{\mathbb{C}}$ and $a \in \overline{\mathbb{C}}$ be a branch point of π. The *defect* $\mu(a)$ of the branch point $a \in \overline{\mathbb{C}}$ is defined as the sum of the multiplicities of zeros of the differential of the map π over all preimages of the point a.

Let us define a *defect set* A_p for each prime number p as a finite set of natural numbers whose elements are given by

(1) the number $p-1$,

(2) the number $(p-1)(1-1/l)$, where $l>1$ is a divisor of the number $p-1$.

Example 5. Suppose that p and $q=(p-1)/2$ are prime numbers. Then the set A_p is equal to $\{q, 2q-2, 2q-1, 2q\}$. Indeed, the prime factor decomposition of the number $p-1$ has the form $p-1=2q$; hence the divisors of $p-1$ that are greater than unity are given by 2, q, and $2q$. In particular, consider prime numbers $p=23$ and $q=11=(23-1)/2$. In this case $A_{23}=\{11, 20, 21, 22\}$.

Proposition 33. *The defect of every branch point of an algebraic function of prime degree p that is representable by radicals belongs to the set A_p.*

Proof. This proposition follows from Theorem 32. Indeed, if, after going around a branch point, one obtains a cyclic permutation of the sheets of the algebraic function, then the defect of the branch point is equal to $p-1$. Suppose that after going around a branch point, one sheet of the algebraic function is fixed and the other sheets are partitioned into cycles of equal length l. Then the number $p-1$ is divisible by l. Above this branch point, there are $(p-1)/l$ critical points at

each of which the differential of the projection has a zero of multiplicity $l-1$. The defect of such a branch point is equal to $(l-1)(p-1)/l = (p-1)(1-1/l)$.

The concept of defect is related to the following classical result.

Riemann–Hurwitz formula. *The genus g of a Riemann surface R satisfies the following relation*:

$$2-2g = 2p - \sum \mu(a),$$

where the summation is over the branch points a of the function.

For every prime p, consider the *semigroup* P_p generated by the defect set A_p. By definition, $m \in P_p$ if there exist nonnegative integers m_i such that $m = \sum m_i k_i$, where $k_i \in A_p$. We will need the *set B_p consisting of natural numbers q that do not belong to the semigroup P_p and satisfy the following condition*: *q is an even number greater than or equal to $2p-2$.*

The set B_p is finite for any prime p (see Corollary 35 below); for many prime numbers p, it is empty.

Theorem 34. *An algebraic function of prime degree p whose genus is equal to $[N-(2p-2)]/2$, where N is an even number from the set B_p, is not representable by radicals.*

Proof. According to the Riemann–Hurwitz formula, the genus g of an algebraic function y of degree p satisfies the relation $2-2g = 2p - \sum \mu(a)$. By Proposition 33, if the function y is representable by radicals, then the defect $\mu(a)$ of each of its branch points a lies in the set A_p. Let $\sum \mu(a) = D$. Then $D \in P_p$ and the genus g can be represented as $[D-(2p-2)]/2$, where D is an even number from the semigroup P_p. This implies the assertion of the theorem.

The Sylvester theorem gives information on the semigroup $P(m,n)$ generated by coprime numbers n and m. Define a number $N(m,n)$ by the formula $N(m,n) = (m-1)(n-1)-1$.

Sylvester theorem. *Every integer greater than $N(m,n)$ belongs to the semigroup $P(m,n)$. For any pair of nonnegative integers whose sum is equal to $N(m,n)$, one of the numbers belongs to the semigroup $P(m,n)$, while the other does not. In particular, there exist exactly $(m-1)(n-1)/2$ nonnegative integers that do not belong to the semigroup $P(m,n)$.*

Corollary 35. *For any prime $p>2$, the set B_p is finite.*

Proof. The set A_p contains two coprime numbers: the number $p-1$ and the number $p-2 = (p-1)(1-1/(p-1))$. By the Sylvester theorem, the complement of the semigroup P_p to the set of natural numbers is finite.

Let us describe the semigroup P_p in the case when $q=(p-1)/2$ is a prime number. According to Example 5, to this end it suffices to describe the semigroup P generated by the numbers q, $2q-2$, $2q-1$, and $2q$.

Proposition 36. *The semigroup P generated by the numbers q, $2q-2$, $2q-1$, and $2q$ is the union of the following sets of natural numbers*:

(1) *the set of solutions of the inequalities $2l(q-1) \le x \le 2lq$ for every even number $2l \ge 0$;*

(2) *the set of solutions of the inequalities $2l(q-1)+q \le x \le (2l+1)q$ for every odd number $2l+1>0$.*

Proof. The numbers in the semigroup have the form $k_0 q + k_1(2q-2) + k_2(2q-1) + k_3(2q)$, where $k_0, k_1, k_2, k_3 \ge 0$. Consider the following two cases.

1. The number k_0 is even. Then, taking the number $k_3 + k_0/2$ instead of k_3, we can assume that $k_0 = 0$. Thus, the required numbers have the form $(k_1+k_2+k_3)2q-(k_2+2k_1)$. Set $k_1+k_2+k_3 = l$. We have the constraints $k_1, k_2, k_3 \ge 0$ and $k_1+k_2+k_3 = l$. Under these constraints, the expression k_2+2k_1 takes all values from zero to $2l$. Therefore, for even k_0, we obtain the union of segments of the natural sequence $2lq-2l \le x \le 2lq$ with $l \ge 0$.

2. The number k_0 is odd. Then, taking the number $k_3+(k_0-1)/2$ instead of k_3, we can assume that $k_0 = 1$. Thus, the required numbers have the form $(k_1 + k_2 + k_3)2q - (k_2 + 2k_1) + q$. Set $k_1+k_2+k_3 = l$. We have the constraints $k_1, k_2, k_3 \geq 0$ and $k_1+k_2+k_3 = l$. Under these constraints, the expression $k_2 + 2k_1$ takes all values from zero to $2l$. Therefore, for odd k_0, we obtain the union of segments of the natural sequence $2l(q-1)+q \leq x \leq (2l+1)q$ with $l \geq 0$.

The proposition is proved.

Example 6. For the number $p = 23$, the number $q = 11$. We have $A_{23} = \{11, 20, 21, 22\}$. Applying Proposition 36, we find that the semigroup P_{23} contains the following numbers: 0, 11, 20–22, 31–33, 40–44, 51–55, 60–66, 71–77, 80–88, 91–99, 100–110, and all greater natural numbers. Thus, the even numbers ≥ 44 that are not included in P_{23} are given by 46, 48, 50, 56, 58, 68, 70, 78, and 90.

Theorem 37. *An algebraic function of degree* 23 *whose genus* g *is equal to one of the numbers* 1, 2, 3, 6, 7, 12, 13, 17, *or* 23 *is not representable by radicals.*

Proof. Theorem 37 follows from Theorem 34 and the calculations of Example 6.

Oleg Ivrii, a student at the University of Toronto who attended my lectures on the Galois theory, compiled a program for calculating all pairs p, g, where $p < 60$ is a prime number and $g \leq 2$ is an even number for which, according to Theorem 34, any algebraic function of degree p and genus g is not representable by radicals. It turned out that among the numbers $p < 60$ there are six numbers for which such pairs exist. Here is the list of these numbers: 23, 29, 43, 47, 53, and 59. For the prime numbers $p = 23$, 47, 59 from this list, the numbers $(p-1)/2$ are prime. For such p, there are many suitable genera g (9, 81, and 144, respectively); all of them can be found without a computer, using Proposition 36. Here, I reproduce Oleg's answer for the remaining three prime numbers. For $p = 29$, the corresponding genera are $g = 1$, 2; for $p = 43$, the genera are $g = 1$, 5; and for $p = 53$, the genera are $g = 1$, 2, 3, 4, 5, 7, 8, 14, 15, 16, 27, 28, 29, 40, 53.

In these computations, we used Theorem 34. Apparently, there exist pairs p, g that are not covered by Theorem 34 but for which any algebraic function of degree p and genus g is not representable by radicals. In the remaining part of this section, we discuss why Theorem 34 is most likely inexact.

The point is that the monodromy transformations corresponding to the branch points (i.e., obtained when one goes around the branch points) of an algebraic function are not arbitrary: the product of these transformations must be the identity transformation, and they must generate a transitive monodromy group.

The monodromy group of a degree p algebraic function representable by radicals is a subgroup of the metacyclic group. The metacyclic group M_p has a homomorphism $\pi\colon M_p \to (\mathbb{Z}/p\mathbb{Z})^*$ to the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of the ring $\mathbb{Z}/p\mathbb{Z}$. Assume that there are no cyclic permutations among the monodromy transformations corresponding the branch points of an algebraic function. In this case, the image $\pi(g)$ of a monodromy transformation g determines the lengths of the cycles into which the transformation g is decomposed. The element $g(x) = ax + b \bmod p$ with $a = \pi(g) \neq 1 \bmod p$ is decomposed into cycles of equal lengths l and one cycle of length 1, where l is the order of the element $a = \pi(g)$. The product of operations corresponding to the branch points is equal to the identity monodromy element. Let us number the branch points. Let g_j be the monodromy transformation corresponding the jth branch point, $a_j = \pi(g_j)$, and the order of the element a_j be equal to l_j. We have $a_1 \cdot \ldots \cdot a_k = 1$, where k is the number of branch points. This identity implies some constraints on the orders l_j. Here is an example: decompose l_j into prime factors. Let $p_1, \ldots, p_m$ be the set of prime numbers that appear in the decompositions of the orders l_j. Let μ_q be the maximum multiplicity of the prime number p_q in the decompositions of the numbers $l_1, \ldots, l_k$.

Proposition 38. *For every* q, *the prime number* p_q *is contained in the decompositions of at least two numbers* l_i *and* l_j *with the maximum multiplicity* μ_q.

Proof. Consider the number $N = p_1^{\mu_1} \cdot \ldots \cdot p_m^{\mu_m}$. Set $N_q = N/p_q$. Suppose that the maximum multiplicity μ_q is encountered in exactly one number $l_{j(q)}$. Then $(a_1 \cdot \ldots \cdot a_m)^{N_q} \neq 1$, which is impossible. Indeed, when raising to the power N_q, all elements a_i except $a_{j(q)}$ become units. The contradiction proves the proposition.

10. CLASSIFICATION OF POLYNOMIALS OF PRIME DEGREE WHOSE INVERSES ARE REPRESENTABLE BY RADICALS

We begin with the following obvious proposition.

Proposition 39. *If a function is the inverse of a polynomial of degree n, then the sum of defects of its finite branch points is equal to $n-1$.*

Proof. The defect of a finite branch point a of a function inverse to a polynomial P is defined as the sum of multiplicities of zeros of the derivative P' over the points of the set $P^{-1}(a)$. But the sum of multiplicities of all zeros of the function P' is equal to $n-1$.

Proposition 40. *If a function that is the inverse of a polynomial of prime degree is representable by radicals, then the function has*

(1) *either one finite branch point such that, after going around it, one obtains a cyclic permutation of the sheets*;

(2) *or two finite branch points such that, after going around each of them, one obtains an involution of the set of sheets.*

Proof. Suppose that an algebraic function y is the inverse of a polynomial of degree p and is representable by radicals. According to Proposition 33, the defect of each finite branch point of the function y is equal to either $p-1$ or $(p-1)(1-1/l)$, where $l>1$ is a divisor of the number $p-1$. By Proposition 39, the sum of all defects is equal to $p-1$. For $l>2$, the number $(p-1)(1-1/l)$ is greater than half the number $p-1$. Consequently, the defect of a branch point may only be equal to either $p-1$ or $(p-1)(1-1/2)$. There exist only two possibilities: either there is only one branch point with defect $p-1$, or there are two branch points with defects $(p-1)(1-1/2)$. By Theorem 32, in the first case, after going around the finite branch point, one obtains a cyclic permutation of the sheets of the function y. By the same Theorem 32, in the second case, after going around each finite branch point, one obtains an involution of the set of its sheets.

Theorem 41. *The inverse of a polynomial of prime degree p is representable by radicals if and only if this polynomial can be reduced to one of the following two forms by affine changes of variables in the target and source spaces*:

(1) *to the power function x^p*;

(2) *to the Chebyshev polynomial T_p.*

Proof. Let us apply the previous proposition. Suppose that the polynomial has two critical values. Consider the composition of the polynomial with the affine transformation that maps the two critical values to the points 1 and -1. According to Theorem 18, the polynomial obtained can be reduced to the Chebyshev polynomial T_p by an affine change of the variable.

Suppose that the polynomial has one critical value. Consider the composition of the polynomial with an affine transformation that maps the critical value to the point 0. By Proposition 19, the polynomial obtained can be reduced to the power function x^p by an affine change of the variable.

Thus, we have shown that among polynomials of prime degree, up to affine changes of the variable, only for the Chebyshev polynomial and the power function the inverse functions are representable by radicals. Recall that a general cubic equation is solvable by radicals precisely because any cubic polynomial can be reduced to either the polynomial T_3 or the function x^3 by affine changes of coordinates.

11. ON RATIONAL FUNCTIONS OF PRIME DEGREE WHOSE INVERSES ARE REPRESENTABLE BY RADICALS

We begin with the following obvious proposition.

Proposition 42. *If the degree of an algebraic function is equal to n and the genus of its Riemann surface is equal to zero, then the sum of defects of its branch points is equal to $2(n-1)$.*

Proof. According to the Riemann–Hurwitz formula, $2 = 2n - \sum \mu(a)$, or $\sum \mu(a) = 2(n-1)$.

The number $\mu(a)/(n-1)$, where $\mu(a)$ is the defect of a branch point a of an n-valued algebraic function whose Riemann surface has genus zero, is called the *reduced defect* of this branch point. By the Riemann–Hurwitz formula, *the sum of reduced defects is equal to* 2.

Suppose that an algebraic function y of prime degree p whose Riemann surface has genus 0 is representable by radicals. *What set can be the set of reduced defects of its branch points*?

For any prime p, the defects of branch points of the function y are elements of the set A_p, which contains the number $p-1$ and the numbers $(p-1)(1-1/l)$, where $l > 1$ is a divisor of the number $p-1$. Denote by $\overline{A}_\infty = \{1, 1/2, 3/4, 4/5, \dots\}$ the union of two sets one of which consists of the number 1 and the other of all numbers of the sequence $k/(k+1)$, where $k = 1, 2, \dots$. One can see that *the reduced defect of each branch point of the function y is contained in the set $\overline{A}_\infty$.*

Problem. List all unordered collections of numbers such that each number belongs to the set $\overline{A}_\infty$ and the sum of all numbers in the collection is equal to 2.

Proposition 43. *Only the following six collections of numbers satisfy the conditions formulated in the problem*:

(1) 1, 1;

(2) 1, 1/2, 1/2;

(3) 1/2, 1/2, 1/2, 1/2;

(4) 1/2, 2/3, 5/6;

(5) 1/2, 3/4, 3/4;

(6) 2/3, 2/3, 2/3.

Proof. 1. Suppose that a collection contains either the number 1 or the subcollection $\{1/2, 1/2\}$. The sum of the remaining numbers of the collection must be equal to 1. The remaining numbers may only be units or halves. Indeed, if a number $x \in \overline{A}_\infty \setminus \{1, 1/2\}$ is contained in the collection, then $x < 1$ and so the collection must contain another number of the set $\overline{A}_\infty$, which is impossible because $x > 1/2$ and all the numbers of the set $\overline{A}_\infty$ are no less than $1/2$. The remaining possibilities are easily analyzed, which yields collections (1)–(3).

2. Suppose that a collection does not contain unity and contains one half. The sum of the remaining numbers of the collection must be equal to $3/2$. In addition to $1/2$, the collection must contain exactly two numbers. Indeed, all numbers in the set $\overline{A}_\infty \setminus \{1/2\}$ are greater than $(3/2)/3$. Among the remaining numbers there are numbers $\le (3/2)/2 = 3/4$: these are the numbers $2/3$ and $3/4$. Hence, there is either $2/3$ or $3/4$ among the remaining numbers. Both these cases are possible and correspond to collections (4) and (5).

3. Suppose that a collection does not contain the numbers 1 and $1/2$. All numbers x of the set $\overline{A}_\infty \setminus \{1, 1/2\}$ satisfy the inequalities $2/3 \le x < 1$. This may only happen when the collection contains exactly three numbers and all of them are equal to $2/3$. This possibility corresponds to collection (6).

Corollary 44. *For a prime number $p > 2$, the functions that are representable by radicals and are the inverses of rational functions of degree p may only have the following collections of reduced defects*: *collections* (1) *and* (2), *which are realized if and only if the rational functions can be reduced*

either to the power function x^p or to the Chebyshev polynomial T_p by linear fractional changes in the target and source spaces; *collection* (3); *collections* (4) *and* (6), *which may occur only for* $p \equiv 1 \mod 3$; *and collection* (5), *which may occur only for* $p \equiv 1 \mod 4$.

I am going to return to the topological classification of functions that are representable by radicals and are the inverses of rational functions. Let us dwell on the topological classification of such functions with a collection of reduced defects of type (3).

12. CLASSIFICATION OF RATIONAL FUNCTIONS OF PRIME DEGREE p, $p \equiv -1 \mod 12$, WHOSE INVERSES ARE REPRESENTABLE BY RADICALS

Recall general facts on the topological classification of degree n analytic maps $\varphi\colon R \to \overline{\mathbb{C}}$ of connected compact Riemann surfaces to the Riemann sphere $\overline{\mathbb{C}}$. Each such map induces a monodromy homomorphism $M\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$, where A is the set of critical values of the map φ and $\pi_1(\overline{\mathbb{C}} \setminus A, *)$ is the fundamental group of the complement $\overline{\mathbb{C}} \setminus A$ with a marked point $*$. The homomorphism M is defined up to conjugation of the group $S(n)$. The image of the fundamental group under the monodromy homomorphism is transitive.

Maps $\varphi_1\colon R_1 \to \overline{\mathbb{C}}$ and $\varphi_2\colon R_2 \to \overline{\mathbb{C}}$ are called *equivalent as branched coverings* if there exists a homeomorphism $h\colon R_1 \to R_2$ such that $\varphi_2 \circ h = \varphi_1$. *Maps are equivalent as branched coverings if and only if the sets A_1 and A_2 of their critical values are equal and the monodromy homomorphisms $M_1\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$ and $M_2\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$, where $A = A_1 = A_2$, of these branched coverings coincide up to conjugation in the group $S(n)$.*

Let us number the points of the set of critical values $A = \{v_1, \dots, v_{m+1}\}$. As generators $\gamma_1, \dots, \gamma_{m+1}$ of the group $\pi_1(\overline{\mathbb{C}} \setminus A, *)$, we take disjoint loops that wind once around the points $v_1, \dots, v_{m+1}$ in the counterclockwise direction and are related by the formula $\gamma_1 \dots \gamma_{m+1} = e$. Upon fixing the generators, the definition of a homomorphism $q\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$ is equivalent to the choice of an ordered collection of elements $g_1 = q(\gamma_1), \dots, g_{m+1} = q(\gamma_{m+1})$ in the group $S(n)$ such that $g_1 \dots g_{m+1} = e$.

Since the monodromy homomorphism is defined up to conjugation in the group $S(n)$ and its image is transitive, we will focus on the ordered collections $g_1, \dots, g_{m+1}$, defined up to conjugation, of elements of the group $S(n)$ that generate a transitive subgroup. On such collections one can define an action of the braid group $B(m+1)$ on $m+1$ strands with generators $p_1, \dots, p_m$. The action is introduced by the following rule: all elements of the collection $g_1, \dots, g_{m+1}$ except g_i and g_{i+1} are invariant under the action of the generator p_i, while $p_i(g_i) = g_{i+1}$ and $p_i(g_{i+1}) = g_{i+1}^{-1} g_i g_{i+1}$.

Maps $\varphi_1\colon R_1 \to \overline{\mathbb{C}}$ and $\varphi_2\colon R_2 \to \overline{\mathbb{C}}$ are called *topologically equivalent* if there exist orientation-preserving homeomorphisms $h\colon R_1 \to R_2$ and $\rho\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ such that $\varphi_2 \circ h = \rho \circ \varphi_1$. Branched coverings with a branch set A *are topologically equivalent if and only if the ordered collection of elements $g_1, \dots, g_{m+1} \in S(n)$ corresponding to the monodromy homomorphism of the first covering is equal, up to conjugation in the group $S(n)$ and the above-described action of the braid group, to the collection of elements $l_1, \dots, l_{m+1} \in S(n)$ corresponding to the monodromy homomorphism of the second covering* [15].

In the metacyclic group M_p, consider the subgroup SM_p generated by all second-order elements. The group SM_p consists of transformations g of the ring $\mathbb{Z}/p\mathbb{Z}$ that have either the form $g(x) \equiv -x + a \mod p$ (each such transformation has order 2) or the form $g(x) \equiv x + b \mod p$. Let us introduce the following notation: for any element a of the ring $\mathbb{Z}/p\mathbb{Z}$, denote by σ_a the transformation $g(x) \equiv x + a \mod p$ and by $\widetilde{\sigma}_a$ the transformation $g(x) \equiv -x + a \mod p$. Let us write down the multiplication table in the group SM_p. One can easily verify the following proposition.

Proposition 45. *For any $a, b \in \mathbb{Z}/p\mathbb{Z}$,*

$$\sigma_a \sigma_b = \sigma_{a+b}, \qquad \sigma_a \widetilde{\sigma}_b = \widetilde{\sigma}_{a+b}, \qquad \widetilde{\sigma}_a \widetilde{\sigma}_b = \sigma_{a-b}, \qquad \widetilde{\sigma}_a \sigma_b = \widetilde{\sigma}_{a-b}.$$

Theorem 46. *Suppose that $\widetilde{\sigma}_a$, $\widetilde{\sigma}_b$, $\widetilde{\sigma}_c$, and $\widetilde{\sigma}_d$ are four second-order elements in the group SM_p that are related by $\widetilde{\sigma}_a\widetilde{\sigma}_b\widetilde{\sigma}_c\widetilde{\sigma}_b = e$ and generate a transitive group. Each such quadruple can be transformed by means of conjugation in the group SM_p and the action of the braid group $B(4)$ into a quadruple such that $\widetilde{\sigma}_a(x) \equiv \widetilde{\sigma}_c(x) \equiv -x+1 \bmod p$ and $\widetilde{\sigma}_b(x) \equiv \widetilde{\sigma}_d(x) \equiv -x-1 \bmod p$.*

Proof. The relation $\widetilde{\sigma}_a\widetilde{\sigma}_b\widetilde{\sigma}_c\widetilde{\sigma}_d = e$ means that $(\widetilde{\sigma}_a\widetilde{\sigma}_b)(\widetilde{\sigma}_c\widetilde{\sigma}_d) = \sigma_{(a-b)}\sigma_{(c-d)} = \sigma_{(a-b+c-d)} = e$, i.e., that $a+c = b+d$.

The generator p_1 of the braid group $B(4)$ takes the quadruple g_1, g_2, g_3, g_4 to the quadruple $g_2, g_2^{-1}g_1g_2, g_3, g_4$. For $g_1 = \widetilde{\sigma}_a$ and $g_2 = \widetilde{\sigma}_b$ we have $g_2^{-1}g_1g_2 = \widetilde{\sigma}_b \circ \widetilde{\sigma}_a \circ \widetilde{\sigma}_b = \widetilde{\sigma}_{2b-a}$. Thus, the generator p_1 takes the pair $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ to the pair $\widetilde{\sigma}_b, \widetilde{\sigma}_{2b-a}$ and does not change the last two elements in the quadruple. Denote $a-b$ by q. Using this notation, write the pair of elements $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ as $\widetilde{\sigma}_a, \widetilde{\sigma}_{a-q}$ and its image as the pair $\widetilde{\sigma}_{a-q}, \widetilde{\sigma}_{a-2q}$. Therefore, the element $p_1^m \in B(4)$ takes the pair $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ to the pair $\widetilde{\sigma}_{a-mq}, \widetilde{\sigma}_{a-(m+1)q}$.

Suppose that $q \neq 0 \bmod p$. In this case, without changing the elements $\widetilde{\sigma}_c$ and $\widetilde{\sigma}_d$, we can map the pair $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ to a pair $\widetilde{\sigma}_l, \widetilde{\sigma}_{-l}$, where $2l \equiv q \bmod p$. Indeed, for $q \neq 0 \bmod p$, the equation $a + mq = l$ in the field $\mathbb{Z}/p\mathbb{Z}$ is solvable with respect to m. For m equal to the solution of this equation, the element p_1^m takes the pair a, b to the pair $l, -l$, where $2l \equiv a-b \bmod p$.

By hypothesis, the elements a, b, c, and d are related by $a+c = b+d$. Hence, if $a-b = 2l \neq 0$, then $c-d = -2l \neq 0$. Repeating the previous calculations, we find that some power of the generator p_3 of the braid group $B(4)$ takes the pair $\widetilde{\sigma}_c, \widetilde{\sigma}_d$ to the pair $\widetilde{\sigma}_{-l}, \widetilde{\sigma}_l$. Thus, under the action of some powers of the generators p_1 and p_3, the quadruple $\widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_c, \widetilde{\sigma}_d$ is mapped to the quadruple $\widetilde{\sigma}_l, \widetilde{\sigma}_{-l}, \widetilde{\sigma}_{-l}, \widetilde{\sigma}_l$.

Now, consider the case $q \equiv 0 \bmod p$. If $q = 0$, then $c = d$ because, by hypothesis, $a-b = c-d$; i.e., the quadruple has the form $\widetilde{\sigma}_a, \widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_b$. The elements a and b cannot be equal: otherwise, all four transformations have the common fixed point 0, which contradicts the transitivity of the group. For $a \neq b$, the generator p_2 of the braid group $B(4)$ takes the original quadruple to the quadruple $\widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_{2b-a}, \widetilde{\sigma}_b$. Now the calculations performed above can be applied to this quadruple because $a \neq b$ and $b \neq 2b-a$.

Hence, by the action of the braid group $B(4)$, one can reduce the original quadruple to the form $\widetilde{\sigma}_l, \widetilde{\sigma}_{-l}, \widetilde{\sigma}_{-l}, \widetilde{\sigma}_l$, where $l \neq 0$. Now, performing the affine change $g(x) \equiv lx \bmod p$ in the field $\mathbb{Z}/p\mathbb{Z}$, we can make it so that l equals 1. Indeed, $g^{-1}\widetilde{\sigma}_l g = \widetilde{\sigma}_1$ and $g^{-1}\widetilde{\sigma}_{-l}g = \widetilde{\sigma}_{-1}$.

Corollary 47. *Up to topological equivalence, there exists a unique rational map $\pi\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ of prime degree $p > 2$ such that the inverse map is representable by radicals and the monodromy transformation corresponding to each branch point is an involution. Such a rational map has four critical values. The monodromy homomorphism of the inverse function is described in Theorem* 46.

According to Corollary 44, if a prime number p satisfies the conditions $p \neq 1 \bmod 3$ and $p \neq 1 \bmod 4$, then a function that is representable by radicals and is the inverse of a rational function of degree p may have the collection of reduced defects of types (1)–(3) only. A prime number $p > 3$ satisfies the relations $p \neq 1 \bmod 3$ and $p \neq 1 \bmod 4$ if and only if $p \equiv -1 \bmod 12$.

Corollary 48. *Let $p > 3$ be a prime number such that $p \equiv -1 \bmod 12$. Then there exist three topological types of rational functions of degree p whose inverses are representable by radicals. These are the function x^p, the Chebyshev polynomial T_p, and the function described in Theorem* 46. *The functions of the first two types can be reduced to their normal forms by linear fractional transformations in the target and source spaces. The functions of the third type with respect to this transformation group depend on a modulus given by the double ratio of four critical values.*

Remark. After the paper was accepted for publication, I found the following remarkable paper: J. F. Ritt, "On Algebraic Functions Which Can Be Expressed in Terms of Radicals," Trans. Am. Math. Soc. **24** (1), 21–30 (1922). In many respects, Ritt advanced further than me. He showed that a polynomial (not necessarily of prime degree) whose inverse is representable by radicals is

a composition of first- and fourth-degree polynomials, functions of the form z^p, and Chebyshev polynomials. He also classified rational functions of prime degree whose inverses are representable by radicals. However, Ritt's paper lacks some of my results. Here are examples: (1) the Riemann surface of a function that is the inverse of a Chebyshev polynomial is determined by its local behavior near the branch points; (2) an algebraic function of degree n that has at least one nonmultiple branch point cannot be reduced by radicals to algebraic functions of degree $< p$, where p is the least prime divisor of the number n (here we assume that $p \geq 5$).

ACKNOWLEDGMENTS

This work was supported in part by a Canadian grant, project no. 156833-2.

REFERENCES

1. V. B. Alekseev, *Abel's Theorem in Problems and Solutions* (MTsNMO, Moscow, 2001) [in Russian].
2. V. I. Arnol'd, "Algebraic Unsolvability of the Problem of Lyapunov Stability and the Problem of Topological Classification of Singular Points of an Analytic System of Differential Equations," Funkts. Anal. Prilozh. **4** (3), 1–9 (1970) [Funct. Anal. Appl. **4**, 173–180 (1970)].
3. V. I. Arnol'd and O. A. Oleinik, "Topology of Real Algebraic Manifolds," Vestn. Mosk. Univ., Ser. 1: Mat. Mekh., No. 6, 7–17 (1979) [Moscow Univ. Math. Bull. **34** (6), 5–17 (1979)].
4. V. I. Arnol'd, "Compositions," in A. N. Kolmogorov, *Selected Works: Mathematics and Mechanics* (Nauka, Moscow, 1985), pp. 444–451 [in Russian].
5. V. I. Arnol'd, "Topological Proof of the Transcendence of Abelian Integrals in 'Mathematical Principles of Natural Philosophy' by Newton," Istor.–Mat. Issled. **31**, 7–17 (1989).
6. V. I. Arnold and V. A. Vassiliev, "Newton's 'Principia' Read 300 Years Later," Notices Am. Math. Soc. **36** (9), 1148–1154 (1989); Addendum: **37** (2), 144 (1989).
7. V. I. Arnold, "Problèmes résolubles et problèmes irrésolubles analytiques et géométriques," in *Passion des formes. Dynamique qualitative, sémiophysique et intelligibilité. Á René Thom* (ENS Éditions, Fontenay–St.-Cloud, 1994), pp. 411–417.
8. V. I. Arnold, "Sur quelques problèmes de la théorie des systèmes dynamiques," Topol. Methods Nonlinear Anal. **4** (2), 209–225 (1994).
9. V. I. Arnol'd, "I.G. Petrovskii, Hilbert's Topological Problems, and Modern Mathematics," Usp. Mat. Nauk **57** (4), 197–207 (2002) [Russ. Math. Surv. **57**, 833–845 (2002)].
10. A. G. Khovanskii, "Topological Obstructions to the Representability of Functions by Quadratures," J. Dyn. Control Syst. **1** (1), 91–123 (1995).
11. A. G. Khovanskii, "On Solvability and Unsolvability of Equations in Explicit Form," Usp. Mat. Nauk **59** (4), 69–146 (2004) [Russ. Math. Surv. **59**, 661–736 (2004)].
12. M. Berger, *Géométrie 1–5* (Cedic, Paris, 1978; Mir, Moscow, 1984; Springer, Berlin, 1987), Vols. 1, 2.
13. A. G. Khovanskii, *Galois Theory, Coverings, and Riemann Surfaces* (MTsNMO, Moscow, 2006) [in Russian].
14. N. G. Chebotarev, *Foundations of Galois Theory* (Editorial URSS, Moscow, 2004), Part 1 [in Russian].
15. A. G. Khovanskii and S. Zdravkovska, "Branched Covers of S^2 and Braid Groups," J. Knot Theory Ramifications **5** (1), 55–75 (1996).

Translated by I. Nikitin