Russian Math. Surveys **59**:4 661–736 ©2004 RAS(DoM) and LMS

Uspekhi Mat. Nauk **59**:4 69–146 DOI 10.1070/RM2004v059n04ABEH000759

To the memory of Andrei Andreevich Bolibrukh

On solvability and unsolvability of equations in explicit form

A. G. Khovanskii

Abstract. In this survey the classical results of Abel, Liouville, Galois, Picard, Vessiot, Kolchin, and others on the solvability and unsolvability of equations in explicit form are discussed. The one-dimensional topological version of Galois theory is presented in detail (this version describes topological obstructions to the representability of functions by quadratures).

Contents

This work was supported in part by OGP grant no. 0156833 (Canada).

AMS 2000 *Mathematics Subject Classification*. Primary 12F10, 12H05, 34M35; Secondary 32S40, 34M50, 30F99, 32D15, 20F16.

Numerous unsuccessful attempts to solve a series of algebraic and differential equations 'in explicit form' led mathematicians to the belief that explicit solutions for these equations simply do not exist. The present survey is devoted to the problem of unsolvability of equations in explicit form. This problem has a rich history.

The first proofs of unsolvability of algebraic equations by radicals were found by Abel and Galois. While considering the problem of explicitly finding an indefinite integral of an algebraic differential form, Abel founded the theory of algebraic curves. Liouville continued Abel's research and proved that indefinite integrals of many algebraic and elementary differential forms are non-elementary. The unsolvability by quadratures of some linear differential equations was also first proved by Liouville.

Galois connected the problem of solvability by radicals with the properties of a certain finite group (the so-called Galois group of the algebraic equation). As a matter of fact, the notion of finite group itself was introduced by Galois in connection with this very problem. Sophus Lie introduced the notion of continuous transformation group while trying to solve explicitly differential equations and reduce them to a simpler form. Picard assigned to each linear differential equation its Galois group, which is a Lie group (and, moreover, an algebraic matrix group). Picard and Vessiot showed that it is this group that is responsible for the solvability of the equation by quadratures. Kolchin developed the theory of algebraic groups and gave the Picard–Vessiot theory a definitive form.

Arnol'd discovered that many classical problems in mathematics are unsolvable for topological reasons. In particular, he showed that it is for topological reasons that the general algebraic equation of degree $\geqslant 5$ cannot be solved by radicals. I am immensely indebted to him for arousing my interest in this topic. Developing Arnol'd's approach, I constructed a peculiar one-dimensional topological version of Galois theory in the early 1970s. According to this theory, the topology of the arrangement of the Riemann surface of an analytic function over the complex plane of the variable can form an obstruction to the representability of this function by means of explicit formulae. In this way one obtains the strongest known results on the non-representability of functions by explicit formulae. Recently I succeeded in generalizing these topological results to the case of several variables.

In this survey a complete exposition of the one-dimensional topological version of Galois theory is given. This version is closely related both to the usual Galois theory and to the Picard–Vessiot theory. Of course, it is impossible to present in full these classical theories in this paper. The main theorems of the theories are formulated without proof, but at the same time it is explained in detail why these theories in principle answer questions about the solvability of algebraic equations by radicals and the solvability of linear differential equations by quadratures. In the survey we also discuss Liouville's beautiful construction of the class of elementary functions, the class of functions representable by quadratures, and so on, together with his theory, which influenced greatly all the subsequent work in this area.

Thus, in the paper we speak of three versions of Galois theory, namely, the usual, the differential, and the topological versions. These versions are unified by a general approach to problems concerning the solvability and unsolvability of equations, based on group theory. However, one cannot say that all solvability and unsolvability results are related to group theory. A series of brilliant results based on another approach is contained in the Liouville theory.

In this survey we sometimes violate the historical order. For instance, the Picard–Vessiot theorem on the solvability of linear differential equations by quadratures was proved earlier than the main theorem of the differential Galois theory. However, the Picard–Vessiot theorem is an immediate consequence of this main theorem, and this is the way it is presented below.

Some words about the references. The exposition of the Liouville approach and closely related work of Chebyshev, Mordukhai-Boltovskii, and others can be found in the remarkable book [33]. The usual Galois theory is well presented in many sources. A brief and clear exposition of the differential Galois theory can be found in [17]. For an interesting survey of research on the solvability and unsolvability of equations, together with a vast bibliography, see [36].

I did not publish a complete presentation of the one-dimensional topological version of Galois theory at the time. In the beginning I did not have the opportunity to delve into the complicated history of the subject, and then I began to do quite different mathematics. Many years later, Andrei Bolibrukh asked me to return to this topic and to prepare a paper for publication in his new journal. A part of the paper was prepared immediately [22]. Here the work is presented in entirety, its relations to the classical versions of Galois theory are discussed, and a new setting of the problem is given, which is necessary for constructing a multidimensional version of the theory. Without Bolibrukh's intervention the one-dimensional version would most likely not have been prepared for publication, and the multidimensional version would not have been discovered. I am indebted to my wife T. V. Belokrinitskaya for her help in the preparation of this paper.

This survey is dedicated to the memory of Andrei Andreevich Bolibrukh, a remarkable person and a first-class mathematician.

§ 1. Setting of the problem of solvability of equations in finite terms

Some algebraic and differential equations can be 'solved explicitly'. What does that mean? If a solution is presented, then it answers the question by itself. However, as a rule, all attempts to solve a given equation explicitly turn out to be unsuccessful. One wishes to prove that there are no explicit solutions for some equations.

To this end, we simply must define exactly what we are talking about (otherwise it is unclear just what we want to prove). From the contemporary point of view, the definitions and formulations of theorems in the classical works are lacking in preciseness. Liouville undoubtedly understood exactly what he was proving. He not only formulated problems on the solvability of equations by elementary functions and quadratures but also algebraized these problems. After his work it was possible to define all these notions over any differential field. However, at the time of Liouville the requirements regarding mathematical rigour differed from the present requirements. According to Kolchin (see [26]), even Picard's basic definitions were not precise enough. Kolchin's papers are quite modern, but his definitions are given for abstract differential fields from the very beginning.

Nevertheless, solutions of differential equations are functions rather than elements of an abstract differential field. Along with differentiation and arithmetic operations in function spaces one has, for example, the absolutely non-algebraic operation of composition. Generally, in function spaces one has more means for writing out 'explicit formulae' than in abstract differential fields. Along with this fact, one must take into account that functions can be multivalued, they can have singularities, and so on.

One can readily formalize the problem of the unsolvability of equations in explicit form in function spaces (in the survey this is the problem we are interested in). This can be done as follows: one can choose some class of functions and say that an equation can be solved explicitly if the solution belongs to this class. Different classes of functions correspond to different notions of solvability.

1.1. Definition of a class of functions by the lists of the basic functions and the admissible operations. A class of functions can be defined if one knows the list of the *basic functions* and the list of *admissible operations*. After this the corresponding class of functions is defined as the set of all functions that can be obtained from the basic functions by using the admissible operations. In 1.2 this is the way we define the classical classes of functions.

The classical classes of functions involved in problems of solvability in finite terms contain multivalued functions. In this connection the basic definitions have to be refined. In this subsection we present two versions of such a refinement. This subsection can be omitted at a first reading.

Let a class of basic functions and a family of admissible operations be fixed. Is it possible to express a given function (say, a solution of a given algebraic or differential equation or a function arising from some other considerations) in terms of basic functions with the help of admissible operations? We are interested in different *single-valued branches* of multivalued functions over different domains. We shall regard every function, even a multivalued one, as the family of all its single-valued branches. We shall apply admissible operations (like arithmetic operations or the operation of taking compositions) only to single-valued branches of functions over different domains. Since we deal with analytic functions, it suffices to consider only small neighbourhoods of points as domains.

The question is now modified as follows: *is it possible to express a given germ of a function at a given point in terms of the germs of basic functions by using the admissible operations*? Of course, the answer depends on the choice of a point and

on the choice of a single-valued germ of the given multivalued function at the given point. However, it turns out that (for the function classes we are interested in) either there is no desired expression for any germ of a given multivalued function at any point or, on the contrary, 'the same' representation fits all the germs of a given multivalued function at almost every point of the space. In the first case we shall say that *no branch of a given multivalued function can be expressed in terms of branches of the basic functions by means of admissible operations*. Otherwise we shall say that such an expression *exists*.

There is another way to work with multivalued functions, the so-called 'global version', which leads to a different (somewhat broader) understanding of the definition of the class of functions given by lists of basic functions and admissible operations. In this global version a multivalued function is regarded as a single object. Operations on multivalued functions are defined. The result of application of these operations is also multivalued: the result is a set of multivalued functions, and each of them is referred to as a function obtained by applying the given operation to the given functions. The class of functions is defined as the set of all (multivalued) functions that can be obtained from the basic functions by using the admissible operations.

For instance, let us define the sum of two multivalued functions of one variable in the sense of the global version.

Definition. Take an arbitrary point a in the complex line, one of the germs f_a of an analytic function f at a, and one of the germs g_a of an analytic function g at the same point a. We say that the multivalued function φ generated by the germ $\varphi_a = f_a + g_a$ *is representable as the sum of the functions* f *and* g.

For example, one can readily see that exactly two functions can be represented in the form $\sqrt{x} + \sqrt{x}$, namely, $f_1 = 2\sqrt{x}$ and $f_2 \equiv 0$. The other operations on multivalued functions are defined in an absolutely similar way. *Saying that some class of multivalued functions is closed under addition means that, together with any two functions in it, this class also contains all functions representable as their sum.* One can say the same about any other operation over multivalued functions that is understood in the above sense.

In the above definition an important role is played not only by the operation of addition itself but also by the operation of analytic continuation, which is hidden in the notion of multivalued function. Indeed, consider the following example. Let f_1 be an analytic function defined on a domain U in the complex line $\mathbb{C}^1$ and admitting no analytic continuation beyond the boundary of U, and let f_2 be the analytic function on U defined by $f_2 = -f_1$. According to the above definition, the function identically equal to zero is representable in the form $f_1 + f_2$ *on the whole complex line*. According to the conventional point of view, the equality $f_1 + f_2 = 0$ holds only on U and not outside it.

In the global version of dealing with multivalued functions we do not insist on the existence of a *common domain* in which all necessary operations are performed on single-valued branches of multivalued functions. One operation can be performed in one domain and another operation in another domain on analytic continuations of the functions obtained. In essence, this broader understanding of operations is equivalent to the inclusion of the operation of analytic continuation in the list of

admissible operations on analytic germs. For a function of a single variable one can obtain topological conditions even under the above broader understanding of operations on multivalued analytic functions. It is a bit shorter to speak about functions than about germs (because one need not fix a point at which the germ is considered and one need not specify the germ under consideration for a given multivalued function). *Therefore, when considering topological obstructions for single-variable functions to belong to some class, we mean the global variant of defining classes of functions by lists of basic functions and admissible operations.* One could not use this understanding in such an extended formulation for functions of several variables, and one must admit a more restrictive formulation connected with germs of functions; however, the latter formulation is not less natural (and possibly even more natural).

1.2. Classical classes of functions of a single variable. We list the classical classes of functions of a single variable, and we define these classes with the help of the lists of basic functions and admissible operations.

Functions of one variable that are representable by radicals.

The list of basic functions: all complex constants and an independent variable x.

The list of admissible operations: the arithmetic operations and the operation of extracting the nth root $\sqrt[n]{f}$, $n = 2, 3, \ldots$, of a given function f.

The function $g(x) = \sqrt[3]{5x + 2\sqrt[2]{x}} + \sqrt[7]{x^3 + 3}$ is an example of a function representable by radicals.

This class is involved in the famous problem of the solvability of equations by radicals. Let us consider an algebraic equation

$$y^n + r_1 y^{n-1} + \cdots + r_n = 0,$$

in which the r_i are rational functions of a single variable. The complete answer to the question of the solvability of such equations by radicals is given by Galois theory (see § 3).

To define the other classes, we need a list of the basic elementary functions. In essence, this list contains the functions that we encountered in high-school and that are often included on the keyboards of pocket calculators.

List of the basic elementary functions.

1) All complex constants and the independent variable x.

2) The exponential and logarithmic functions and the power-law functions of the form x^α, where α is an arbitrary complex constant.

3) The trigonometric functions: sine, cosine, tangent, and cotangent.

4) The inverse trigonometric functions: arcsine, arccosine, arctangent, and arccotangent.

Let us now pass to the list of classical operations on functions. We present here the beginning of the list. It will be continued in 2.1.

List of classical operations.

1) The *composition operation*, which assigns to functions f and g the function $f \circ g$.

2) The *arithmetic operations*, which assign to functions f and g the functions $f + g$, $f - g$, fg, and f/g.

3) The *operation of differentiation*, which assigns to a function f the function f'.

4) The *operation of integration*, which assigns to a function f an indefinite integral y of f (that is, an arbitrary function y such that $y' = f$; the function y is determined by the function f up to an additive constant).

5) The *operation of solving an algebraic equation*, which assigns to functions $f_1, \dots, f_n$ a function y such that $y^n + f_1 y^{n-1} + \dots + f_n = 0$ (the function y is determined by the functions $f_1, \dots, f_n$ not quite uniquely, because an algebraic equation of degree n can have n solutions).

We now return to the definition of the classical classes of functions of a single variable.

Elementary functions of a single variable.

List of the basic functions: the basic elementary functions.

List of admissible operations: compositions, the arithmetic operations, and differentiation.

An elementary function can be represented by a formula, for instance, by the formula

$$f(x) = \arctan(\exp(\sin x) + \cos x).$$

Functions of one variable that are representable by quadratures.

List of the basic functions: the basic elementary functions.

List of admissible operations: compositions, the arithmetic operations, differentiation, and integration.

For instance, the elliptic integral

$$f(x) = \int_{x_0}^{x} \frac{dt}{\sqrt{P(t)}},$$

where P is a cubic polynomial, is representable by quadratures. However, as was proved by Liouville, if the polynomial P has no multiple roots, then the function f is not elementary.

Generalized elementary functions of a single variable. This class of functions is defined in exactly the same way as the class of elementary functions, except that the operation of solving algebraic equations is added to the list of admissible operations.

Functions of one variable representable by generalized quadratures. This class of functions is defined in exactly the same way as the class of functions representable by quadratures, except that the operation of solving algebraic equations is added to the list of admissible operations.

We also introduce two classes of functions close to classical ones.

Functions of one variable representable by k-radicals. This class of functions is defined in exactly the same way as the class of functions representable by radicals, except that the operation of solving algebraic equations of degree $\leqslant k$ is added to the list of admissible operations.

Functions of one variable representable by k-quadratures. This class of functions is defined in exactly the same way as the class of functions representable by quadratures, except that the operation of solving algebraic equations of degree $\leqslant k$ is added to the list of admissible operations.

§ 2. Liouville theory

The first rigorous proofs of the unsolvability of some equations by quadratures and by elementary functions were obtained by Liouville in the middle of the nineteenth century (see [30]–[36)]). According to his theory, 'rather simple' equations either have 'rather simple' solutions or cannot be solved at all in an explicit form. For instance, the Liouville theory answers the following questions:

1) Under what conditions is an indefinite integral of an elementary function an elementary function?

2) Under what conditions can the solutions of a linear differential equation all be represented by generalized quadratures?

A more complete answer to the second question is given by the differential Galois theory (see § 4). In the present section we discuss how Liouville algebraized the solvability problem, and we formulate some results of his theory.

2.1. New definitions of classical classes of functions. Liouville algebraized the problem of solvability by elementary functions and by quadratures. The main obstruction on this path is the quite non-algebraic operation of composition. Liouville got around the obstruction as follows: to any function g in the list of basic functions he assigned the operation of composition with this function, which takes each function f to the function $g \circ f$. He noted that the basic elementary functions can be reduced to the logarithmic and the exponential functions (see Lemma 2.1 below). The compositions $y = \exp f$ and $z = \log f$ can be regarded as solutions of the equations $y' = f'y$ and $z' = f'/f$. Thus, within the classical classes of functions it suffices to consider the operation of solving simple differential equations instead of the quite non-algebraic operation of composition. After this, the solvability problem in the classical classes of functions becomes differential-algebraic and can be extended to abstract differential fields. We proceed to the realization of this programme.

Let us continue the list of classical operations.

List of classical operations (for the beginning of the list, see. 1.2)**.**

6) The *operation of taking the exponential function*, which assigns to a function f the function $\exp f$.

7) The *operation of taking the logarithm*, which assigns to a function f the function $\log f$.

We now present the new definitions of the transcendental classical classes of functions.

Elementary functions of a single variable.

List of the basic functions: all complex constants and the independent variable x.

List of admissible operations: taking the exponential, taking the logarithm, the arithmetic operations, and differentiation.

Functions of one variable representable by quadratures.

List of the basic functions: all complex constants.

List of admissible operations: taking the exponential, the arithmetic operations, differentiation, and integration.

Generalized elementary functions and the functions of a single variable representable by generalized quadratures and *k*-quadratures of a single variable are defined in exactly the same way as the corresponding non-generalized classes of functions, except that the operation of solving algebraic equations or the operation of solving the algebraic equations of degree at most k is added to the list of admissible operations, respectively.

Lemma 2.1. *The basic elementary functions can be expressed by means of complex constants, arithmetic operations, and compositions in terms of the exponential function and the logarithm.*

Proof. For the power-law function x^α the desired expression is given by the equality $x^\alpha = \exp(\alpha \log x)$. For the trigonometric functions the desired expressions follow from Euler's formula $e^{a+bi} = e^a(\cos b + i \sin b)$. For real values of x one has $\sin x = \dfrac{1}{2i}(e^{ix} - e^{-ix})$ and $\cos x = \dfrac{1}{2}(e^{ix} + e^{-ix})$. Since the functions are analytic, these formulae remain valid for complex values of x as well. The tangent and cotangent functions can be expressed in terms of sine and cosine. We show that if x is real, then $\arctan x = \dfrac{1}{2i} \log z$, where $z = \dfrac{1+ix}{1-ix}$. It is clear that $|z| = 1$, $\arg z = 2 \arg(1 + ix)$, and $\tan(\arg(1 + ix)) = x$, which proves the desired equality. Since the functions are analytic, the equality remains valid for complex values of x as well. The other inverse trigonometric functions can be expressed in terms of arctan. Namely, $\operatorname{arccot} x = \dfrac{\pi}{2} - \arctan x$, $\arcsin x = \arctan \dfrac{x}{\sqrt{1-x^2}}$, and $\arccos x = \dfrac{\pi}{2} - \arcsin x$. The square root entering the expression for the function arcsin can be represented in terms of the exponential function and the logarithm, $x^{1/2} = \exp(1/2) \log x$. This completes the proof of the lemma.

Theorem 2.2. *For each transcendental classical class of functions the old and new definitions* (see the present section and 1.2) *are equivalent.*

Proof. The theorem is obvious in one direction. It is clear that every function belonging to some classical class of functions in the sense of the new definition belongs to the same class in the sense of the old definition.

We now prove the theorem in the other direction. By Lemma 2.1, the basic elementary functions belong to the class of elementary and generalized elementary functions in the sense of the new definition. The same lemma implies that the classes of functions representable by quadratures, generalized quadratures, and k-quadratures in the sense of the new definition also contain the basic elementary functions. Indeed, the independent variable x belongs to these classes, being the result of integrating the constant 1, because $x' = 1$. Instead of the operation of taking the logarithm, which does not belong to the admissible operations of these classes, one can use the operation of integration, because $(\log f)' = f'/f$.

It remains to show that the classical classes of functions in the sense of the new definition are closed under compositions. The point here is that the operation of composition commutes with all the operations in the new definitions of classes of functions except for the operations of differentiation and integration. For instance, the result of applying the operation exp to the composition $g \circ f$ coincides with the result of applying the operation of composition to the functions

$\exp g$ and f, that is, $\exp(g \circ f) = (\exp g) \circ f$. Similarly, $\log(g \circ f) = (\log g) \circ f$, $(g_1 \pm g_2) \circ f = (g_1 \circ f) \pm (g_2 \circ f)$, $(g_1 g_2) \circ f = (g_1 \circ f)(g_2 \circ f)$, and $(g_1/g_2) \circ f = (g_1 \circ f)/(g_2 \circ f)$. If a function y satisfies an equation $y^n + g_1 y^{n-1} + \cdots + g_n = 0$, then the function $(y \circ f)$ satisfies the equation

$$(y \circ f)^n + (g_1 \circ f)(y \circ f)^{n-1} + \cdots + (g_n \circ f) = 0.$$

For the operations of differentiation and integration we have the following simple commutation relations with the operation of composition: $(g)' \circ f = (g \circ f)'(f')^{-1}$ (if the function f is constant, then the function $(g)' \circ f$ is also constant) and if y is an indefinite integral of a function g, then $y \circ f$ is an indefinite integral of the function $(g \circ f)f'$ (in other words, the composition of the integral of a function g with a function f corresponds to the integration of the function $g \circ f$ multiplied by the function f').

This implies that the classical classes in the sense of the new definition are closed under compositions. Indeed, if a function g is obtained from constants (or from constants and the independent variable) by means of the above operations, then the function $g \circ f$ is obtained from the function f by applying the same operations (or almost the same operations, as in the case of integration and differentiation). This completes the proof of the theorem.

Remark. One can readily see that the operation of differentiation can also be excluded from the list of admissible operations for classical classes of functions. For the proof, it suffices to use the explicit computation of the derivatives of the exponential function and of the logarithm together with the rules for differentiating formulae including compositions and arithmetic operations. However, the elimination of the operation of differentiation does not help to solve the problem of solvability of equations in finite terms.

2.2. Liouville extensions of abstract and differential function fields. A field K is said to be a *differential field* if an additive map $a \to a'$ satisfying the Leibniz relation $(ab)' = a'b + ab'$ is given. An element y of a differential field K is said to be *constant* if $y' = 0$. The constants of a differential field form a subfield that is called the *field of constants*. In all cases we are interested in, the field of constants is the field of complex numbers. *In what follows we always assume that the differential field is of characteristic zero and has an algebraically closed field of constants.* An element y of a differential field is said to be an *exponential of an element* a if $y' = a'y$, an *exponential of an integral of an element* a if $y' = ay$, a *logarithm of an element* a if $y' = a'/a$, and an *integral of an element* a if $y' = a$.

Let a differential field K and a set M belong to some differential field F. By *adjoining* the set M to the differential field K we mean taking the minimal differential field $K\langle M\rangle$ containing the field K and the set M.

A differential field F containing a differential field K and having the same field of constants is called an *elementary extension* of the field K if there is a chain of differential fields $K = F_1 \subseteq \cdots \subseteq F_n = F$ such that for any $i = 1, \ldots, n-1$ the field $F_{i+1} = F_i\langle x_i\rangle$ is obtained by adjoining an element x_i to the field F_i, where x_i is an exponential or a logarithm of some element a_i of F_i. An element $a \in F$ is said to be *elementary* over K, $K \subset F$, if a is contained in some elementary extension of the field K.

A *generalized elementary extension*, a *Liouville extension*, a *generalized Liouville extension*, and a *Liouville k-extension* of a field K are defined similarly. When we construct generalized elementary extensions, we can adjoin exponentials and logarithms and pass to algebraic extensions. When we construct Liouville extensions we can adjoin integrals and exponentials of integrals. In generalized Liouville extensions and Liouville k-extensions one also admits algebraic extensions and adjoining solutions of algebraic equations of degree $\leqslant k$, respectively. An element $a \in F$ is said to be a *generalized elementary element* over K for a field $K \subset F$ (*representable by quadratures*, *by generalized quadratures*, by *k-quadratures* over K) if a is contained in some generalized elementary extension (Liouville extension, generalized Liouville extension, Liouville k-extension, respectively) of the field K.

Remark. The equation for the exponential of an integral is simpler than that for an exponential. For this reason, one uses the adjoining of exponentials of integrals in the definition of Liouville extensions, and so on. Instead, one could adjoin exponentials and integrals separately.

Let us proceed to differential function fields. It is these fields we deal with in this survey (though some results can readily be extended to abstract differential fields).

Every subfield K of the field of all meromorphic functions on a connected domain U on the Riemann sphere such that K contains all complex constants and is closed under differentiation (that is, if $f \in K$, then $f' \in K$) gives an example of a differential function field. We now give the general definition. Let V, v be a pair formed by a connected Riemann surface V and a meromorphic vector field v on V. The Lie derivative L_v along the vector field v acts on the field F of all meromorphic functions on the surface V and defines a differentiation $f' = L_v f$ of the field. A *differential function field* is an arbitrary differential subfield of F that contains all complex constants.

It is sometimes more convenient to use another definition of differentiation of a function field in which a meromorphic vector field is replaced by a meromorphic 1-form α. The derivative f' of a function f can be defined by the formula $f' = df/\alpha$ (a quotient of two meromorphic 1-forms is a well-defined meromorphic function). The differentiation thus introduced is the Lie derivative L_v along the vector field v connected with the form α by the following relation: the value of the 1-form α on the field v is identically equal to 1.

The following construction is used to extend function fields. Let K be a subfield of the field of meromorphic functions on a connected Riemann surface V equipped with a meromorphic form α and let K be invariant under the differentiation $f' = df/\alpha$ (that is, if $f \in K$, then $f' \in K$). We consider an arbitrary connected Riemann surface W together with an analytic map $\pi\colon W \to V$. Let us fix the form $\beta = \pi^*\alpha$ on W. The differential field F of all meromorphic functions on W with the differentiation $\varphi' = d\varphi/\beta$ contains the differential subfield π^*K consisting of the functions of the form π^*f, where $f \in K$. The differential field π^*K is isomorphic to the differential field K and is a subfield of F. If one chooses a suitable surface W, then the extension procedure for the field π^*K isomorphic to K can be carried out in the field F.

Suppose that K is to be extended by, say, an integral y of some function $f \in K$. This can be done as follows. Over the Riemann surface V one can consider the Riemann surface W of an indefinite integral y of the 1-form $f\alpha$. By the very definition of the Riemann surface W, there is a natural projection $\pi\colon W \to V$, and the function y is a single-valued meromorphic function on the surface W. The differential field F of meromorphic functions on W with the operation of differentiation given by $f' = df/\pi^*\alpha$ contains both the element y and the field π^*K isomorphic to the field K. Therefore, the extension $\pi^*K\langle y\rangle$ is defined and is a subfield of F. When speaking of extensions of differential function fields, it is this construction we mean. The same construction enables us to adjoin to a differential function field K a logarithm, an exponential, an integral, or the exponential of an integral of any function f in the field K. In the same way for any functions $f_1, \dots, f_n \in K$ one can adjoin to K a solution y of an algebraic equation $y^n + f_1 y^{n-1} + \dots + f_n = 0$ or all solutions $y_1, \dots, y_n$ of this equation (one can adjoin all solutions $y_1, \dots, y_n$ over the Riemann surface of the vector function $\mathbf{y} = (y_1, \dots, y_n)$). For any functions $f_1, \dots, f_{n+1} \in K$ one can adjoin to K the n-dimensional affine space over $\mathbb{C}$ formed by all solutions of the linear differential equation $y^{(n)} + f_1 y^{(n-1)} + \dots + f_n y + f_{n+1} = 0$ in the same way. (We recall that the germ of any solution of a linear differential equation can be analytically continued along a curve on V that does not pass through poles of the functions $f_1, \dots, f_{n+1}$.)

Thus, *the above extensions of differential function fields can be carried out within the class of differential function fields*. When speaking of extensions of differential function fields, we always mean this procedure.

The differential field consisting of all complex constants and the differential field consisting of all rational functions of a single variable can be regarded as differential fields of functions defined on the Riemann sphere.

Let us reformulate Theorem 2.2 using the definitions from abstract differential algebra and the construction of extensions of differential function fields.

Theorem 2.2′. *A function of a single complex variable* (*possibly multivalued*) *belongs*:

1) *to the class of elementary functions if and only if it belongs to some elementary extension of the field of all rational functions of a single variable*;

2) *to the class of generalized elementary functions if and only if it belongs to some generalized elementary extension of the field of rational functions*;

3) *to the class of functions representable by quadratures if and only if it belongs to some Liouville extension of the field of all complex constants*;

4) *to the class of functions representable by k-quadratures if and only if it belongs to some Liouville k-extension of the field of all complex constants*;

5) *to the class of functions representable by generalized quadratures if and only if it belongs to some generalized Liouville extension of the field of all complex constants*.

2.3. Some results of the Liouville theory. In this subsection we present (without proofs) formulations of some results in the Liouville theory.

2.3.1. *Non-elementary indefinite integrals*. When we start learning analysis, we study integration of elementary functions, and this turns out to be far from simple.

As was proved by Liouville, an indefinite integral of an elementary function is not an elementary function as a rule.

Theorem 2.3 (on integrals). *An indefinite integral y of a function f belonging to a differential function field K belongs to some generalized elementary extension of this field if and only if the integral can be represented in the form*

$$y(x) = \int_{x_0}^{x} f(t)\,dt = A_0(x) + \sum_{i=1}^{n} \lambda_i \log A_i(x), \tag{1}$$

where the A_i, $i = 0, 1, \ldots, n$, are some functions in the field K.

In differential terms the condition (1) in Liouville's theorem means that the element $f \in K$ can be represented as

$$f = A_0' + \sum_{i=1}^{n} \lambda_i \frac{A_i'}{A_i}\,, \tag{2}$$

where the A_i, $i = 0, 1, \ldots, n$, are some elements of the field K. In abstract differential algebra one has an analogue of Liouville's theorem [34]. In the formulation of the abstract theorem one must replace K by an abstract differential field and use the condition (1) in the differential form (2).

Corollary 2.4. *An indefinite integral y of a generalized elementary function f is a generalized elementary function if and only if it can be represented as*

$$y(x) = A_0(x) + \sum_{i=1}^{n} \lambda_i \log A_i(x),$$

where the A_i, $i = 0, 1, \ldots, n$, are rational functions of the function f and its derivatives with complex coefficients.

A priori, an integral of an elementary function f could be a very complicated elementary function. Liouville's theorem shows that this is impossible. Either an integral of an elementary function is non-elementary or it has the simple form described in the corollary.

Is it possible to find an explicit form of an integral of an algebraic function? The pioneering papers of Abel, who founded the theory of algebraic curves and Abelian integrals and inspired Liouville to create his theory, were devoted to this problem. Roughly speaking, the answer to this question is as follows. If the Riemann surface of an algebraic function is of genus zero, then its integral can always be found in generalized elementary functions. However, if the genus of the Riemann surface is positive, then the integral is non-elementary as a rule and can be found in generalized elementary functions only in exceptional cases. A more detailed answer is given by Liouville's theorem on Abelian integrals which we formulate below.

Theorem 2.5 (on Abelian integrals). *An indefinite integral y of an algebraic function A of a complex variable x can be found in generalized elementary functions if and only if it is representable in the form*

$$y(x) = \int_{x_0}^{x} A(t)\,dt = A_0(x) + \sum_{i=1}^{k} \lambda_i \log A_i(x),$$

where the A_i, $i = 0, 1, \ldots, k$, are algebraic functions that are single-valued on the Riemann surface W of the integrand A.

Proof. The theorem follows from Liouville's theorem on integrals of elementary functions, applied to the field F of all meromorphic functions on W, equipped with the differentiation $f' = df/\alpha$, where $\alpha = \pi^* dx$ and $\pi\colon W \to \overline{\mathbb{C}}$ is the natural projection of the Riemann surface of the function A onto the Riemann sphere $\overline{\mathbb{C}}$ of the complex variable x.

Remark. Liouville's theorem on the Abelian integrals goes back to Abel. Abel considered the more special problem of the representability of Abelian integrals in the form of rational functions of algebraic functions and their logarithms and made similar conclusions.

We state Liouville's criterion for integrability in explicit form of functions of exponential type and present examples of integrals not representable by elementary functions.

Liouville's criterion. *Consider an indefinite integral of the form*

$$I(x) = \int_{x_0}^{x} f(t)e^{g(t)}\,dt,$$

where f and g are rational functions, the function g is non-constant, and f is not identically zero. If there is a rational function a such that $a' + ag' = f$, then $I = ae^g + c$, where c is a complex constant. If the equation $a' + ag' = f$ is not solvable by rational functions, then the integral I is not a generalized elementary function.

Examples of non-elementary integrals. *The indefinite integrals* $\int e^{t^2}\,dt$, $\int \frac{e^t}{t}\,dt$, $\int \frac{dt}{\log t}$, *and* $\int \frac{\sin t}{t}\,dt$ *are not generalized elementary functions.*

2.3.2. *Criterion of Liouville and Mordukhai-Boltovskii.* The first result on the unsolvability of a linear differential equation in explicit form is due to Liouville (see [32] and [33]).

Theorem 2.6 (Liouville). *An equation $y'' + py' + qy = 0$ with coefficients in a differential function field K all of whose elements are representable by generalized quadratures can be solved by generalized quadratures if and only if it has a solution of the form $y_1(x) = \exp \int_{x_0}^{x} f(t)\,dt$, where f is a function satisfying an algebraic equation with coefficients in the field K.*

The theorem is obvious in one direction. If one solution y_1 of the second-order linear differential equation is known, then the equation can be solved by reducing the order of the equation. It is rather difficult to prove the theorem in the other direction.

More than half a century was needed to generalize Liouville's theorem to equations of order n. Mordukhai-Boltovskii (1910) used Liouville's method to prove the following criterion, which enables one to reduce the solvability problem for an equation to the solvability problem for another equation of smaller order.

Criterion of Liouville and Mordukhai-Boltovskii. *An equation*

$$y^{(n)} + p_1 y^{(n-1)} + \cdots + p_n y = 0$$

of order n with coefficients in a differential function field K all of whose elements are representable by generalized quadratures is solvable by generalized quadratures if and only if, first, it has a solution of the form $y_1(x) = \exp \int_{x_0}^{x} f(t)\,dt$, where f is a function belonging to some algebraic extension K_1 of the field K and, second, the differential equation of order $(n-1)$ obtained from the original equation by the procedure of reducing the order (see 4.1.2*), which is a differential equation for the function $z = y' - \dfrac{y_1'}{y_1} y$ with coefficients in K_1, is solvable by generalized quadratures over the field K_1.*

The Picard–Vessiot theorem in which the solvability problem for linear differential equations is solved in quite another way, from the point of view of the differential Galois theory, appeared also in 1910.

Below we discuss the main facts of this theory. In essence, the criterion of Liouville and Mordukhai-Boltovskii is equivalent to the Picard–Vessiot theorem. The Picard–Vessiot theory not only explains this criterion but also makes it possible to develop it to an explicit algorithm that enables one to decide for an equation with coefficients in the field of rational functions (having the rational coefficients) whether or not this equation is solvable by generalized quadratures (see [37] and 4.7).

§ 3. Solvability of algebraic equations by radicals and Galois theory

Is a given algebraic equation solvable by radicals? Is it possible to solve a given algebraic equation of degree n by using radicals and the solutions of auxiliary algebraic equations of smaller degree? In this section we discuss how Galois theory solves these problems. We focus our attention mainly on solvability and unsolvability problems and present the main theorem of Galois theory without proof. The well-known properties of solvable groups and of the group $S(k)$ are also used without proof. In 3.4.1 we prove a much less known characteristic property of subgroups of the group $S(k)$. These facts of group theory are applied both in the usual Galois theory and in its differential and topological versions.

The 'solving' part of Galois theory (see 3.3.2) that enables one to solve an equation by radicals is very simple. It uses neither the main theorem of Galois theory nor the theory of fields at all and relates in fact to linear algebra. Only these linear algebra considerations are used in the topological version of Galois theory when discussing the problem of representability of algebraic functions by radicals. (However, the sufficient condition for the solvability of equations by means of solving auxiliary equations of smaller degree and radicals is based not only on linear algebra but also on the main theorem of Galois theory.)

The above problems on the solvability or algebraic equations are purely algebraic in nature and can be posed over an arbitrary field K. *In this section we assume that the field K is of characteristic zero and contains all roots of unity.* This case is somewhat simpler than the general case, and for our purposes the differential function fields that contain all complex constants are of principal interest.

3.1. Galois group of an algebraic equation. Let us consider an algebraic equation

$$a_n x^n + \cdots + a_1 x + a_0 = 0 \tag{3}$$

with coefficients in the field K. We assume that K is embedded into a larger field that contains all roots of the equation. By a *relation* among the roots of (3) that is defined over the field K we mean an arbitrary polynomial Q belonging to the ring $K[x_1, \ldots, x_n]$ and vanishing at the point $(x_1^0, \ldots, x_n^0)$, where $x_1^0, \ldots, x_n^0$ is the set of roots of (3), ordered in some way.

Definition. By the *Galois group of an algebraic equation* (3) over the field K we mean the subgroup G of the group $S(n)$ of all permutations of the roots of the equation that preserve all the relations defined over K among the roots (that is, if a permutation $\sigma \in S(n)$ belongs to the Galois group G, then the polynomial σQ obtained from a relation Q by the permutation σ of the variables $x_1, \ldots, x_n$ also vanishes at the point $(x_1^0, \ldots, x_n^0)$).

Definition. A field P is called a *Galois extension* of a field K if there is an algebraic equation (3) with coefficients in K such that the field P is obtained by adjoining all the roots of this equation to K. By the *Galois group of a Galois extension* P over a field K we mean the group of all automorphisms of the field P that leave fixed every element of K.

Every element σ of the Galois group of the field P over the field K permutes the roots of the equation (3) and preserves the relations among them defined over K. Thus, the Galois group of the field P over K has a representation in the Galois group G of the equation (3) defining the extension P. Obviously, this representation is a group isomorphism, that is, the Galois group of the equation and the Galois group of the extension defined by the equation are isomorphic.

To prove the unsolvability of equations, we need the following simple 'upper bounds' for the Galois group.

Lemma 3.1. *The Galois group of the equation $x^n - a = 0$ over a field K, where $a \in K$, is a subgroup of the cyclic group with n elements.*

Proof. Let x_0 be some root of the equation $x^n - a = 0$ and let ξ be a primitive nth root of unity. We index the roots of the equation $x^n - a = 0$ by the residues i modulo n, setting x_i equal to $\xi^i x_0$. Suppose that a transformation g in the Galois group takes the root x_0 to the root x_i. Then $g(x_k) = g(\xi^k x_0) = \xi^{k+i} x_0 = x_{k+i}$. That is, each transformation in the Galois group defines a cyclic permutation of the roots.

The following lemma is an immediate consequence of the definition of the Galois group of an algebraic equation.

Lemma 3.2. *The Galois group of an equation of degree $m \leqslant k$ is isomorphic to a subgroup of the group $S(k)$.*

3.2. Main theorem of Galois theory. Let P be a Galois extension of a field K and let G be the Galois group of the extension P.

The following maps between the set of fields lying between K and P and the set of subgroups of the Galois group G are defined.

1) The *map* Fd assigning to each subgroup Γ of the group G the field $Fd(\Gamma)$ consisting of the elements of the field P that remain fixed under the action of Γ (it is clear that $K \subseteq Fd(\Gamma)$).

2) The *map* Gp assigning to each intermediate field F, $K \subseteq F \subseteq P$, the subgroup $Gp(F) \subseteq G$ that is the Galois group of the Galois extension P of F (P is a Galois extension of the field K, and therefore it is automatically a Galois extension of the intermediate field F, $K \subseteq F \subseteq P$).

The maps Fd and Gp establish the *Galois correspondence* between the subgroups of the Galois group and the intermediate fields of the Galois extension.

We present the following theorem without proof.

Theorem 3.3 (the main theorem of Galois theory). *If P is a Galois extension of the field K with Galois group G, then*:

1) *the composition of the maps Fd and Gp is the identity map of the set of intermediate fields onto itself, that is, if F is a field and $K \subseteq F \subseteq P$, then $Fd(Gp(F)) = F$;*
2) *the composition of the maps Gp and Fd is the identity map of the set of subgroups of the Galois group onto itself, that is, if Γ is a subgroup of the Galois group, $\Gamma \subset G$, then $Gp(Fd(\Gamma)) = \Gamma$;*
3) *an intermediate field F, $K \subseteq F \subseteq P$, is a Galois extension of K if and only if the group $Gp(F)$ is a normal subgroup of G, and moreover, the Galois group of a Galois extension F of K is the quotient group of G by the normal subgroup $Gp(F)$.*

A field P is a Galois extension of a field K if and only if there is a finite group Γ of automorphisms of P that leaves fixed all the elements of K and only these elements.

What happens with the Galois group of an equation if one extends the field K of coefficients, replacing it by a larger field K_1? This problem is of special interest if the field K_1 is a Galois extension of K. We denote by G_1 the Galois group of the extension K_1 of K. The results on the unsolvability of algebraic equations are based on the following theorem.

Theorem 3.4 (on the change of the Galois group of an equation under a Galois extension of the field of coefficients). *When the coefficient field K is replaced by a Galois extension K_1 of K, the Galois group G of the equation is replaced by some normal subgroup H of G. The quotient group G/H of G by this normal subgroup is isomorphic to some quotient group of the Galois group G_1 of the new coefficient field K_1 over the old coefficient field K.*

Proof. Let Q be the smallest Galois extension of K that contains the extensions P and K_1 of K. (The extension Q can be obtained by adjoining to K all the roots of the product of the polynomial equations defining the Galois extensions P and K_1 of K.) The field K is elementwise fixed under the action of the Galois group Γ_Q of Q, and the fields K_1 and P are invariant under this action. Hence, the field $K_1 \cap P$ is invariant under the action of Γ_Q and is therefore a Galois extension of K.

The Galois group H of the Galois extension P of the field $K_1 \cap P$ is a normal subgroup of the Galois group of the Galois extension P of K, because $K_1 \cap P$ is a Galois extension of K and $K_1 \cap P \subset P$. On the other hand, G/H is a quotient

group of the Galois group of the Galois extension K_1 of K, because $K_1 \cap P$ is a Galois extension of K and $K_1 \cap P \subset K_1$.

It remains to show that the Galois group H of P over $K_1 \cap P$ coincides with the Galois group Γ of Q over K_1. Indeed, Γ is a subgroup of H, because each relation over the field $K_1 \cap P$ is in particular a relation among the roots of the same equation over the field K_1. Assume that $\Gamma \neq H$. By the main theorem applied to the extension P of K, the field F of invariants with respect to the action of Γ on P is strictly larger than $K_1 \cap P$. On the other hand, all the elements of F belong both to P and to K_1, a contradiction. This shows that $\Gamma = H$.

3.3. Solvability by radicals. Is a given algebraic equation solvable by radicals? Galois theory was created to answer this question. Let us begin with a formal definition.

An algebraic equation over a field K is said to be *solvable by radicals* if there is a chain of extensions $K = K_0 \subset \cdots \subset K_N$ such that the field K_{i+1} is obtained from the field K_i, $i = 0, 1, \ldots, N-1$, by adjoining a radical, and the field K_N contains all roots of the original algebraic equation.

Theorem 3.5. *An algebraic equation is solvable by radicals if and only if its Galois group is solvable.*

Proof. We shall prove below in 3.3.1 (see Corollary 3.10) that the solvability of the Galois group is sufficient for the solvability of the equation by radicals. Let us show that if an algebraic equation is solvable by radicals, then its Galois group is solvable. To this end, we trace what happens with the Galois group of an equation under the passage from a coefficient field K_i to the coefficient field K_{i+1}. We denote by G_i the Galois group of our equation over the field K_i. In this case, according to Theorem 3.4, the group G_{i+1} is a normal subgroup of G_i, and the quotient group G_i/G_{i+1} is a quotient group of the Galois group of the field K_{i+1} over the field K_i. Since the field K_{i+1} is obtained from K_i by adjoining a radical, it follows from Lemma 3.1 that the Galois group of K_{i+1} over K_i is commutative. Since all the roots of the algebraic equation belong to the field K_N by assumption, it follows that the Galois group G_N of the algebraic equation over the field K_N is trivial. Thus, for the Galois group G there is a chain of subgroups $G = G_0 \supset \cdots \supset G_N$ such that G_{i+1} is a normal subgroup of G_i with a commutative quotient group G_i/G_{i+1}, and the group G_N is trivial. This means that the Galois group G is solvable.

3.3.1. *Sufficient condition for solvability by radicals.* Let K be a subfield of the field P, and let the field P be equipped with the action of a finite automorphism group G that leaves fixed all the elements of K and only these elements. If P is obtained from K by adjoining all the roots of an algebraic equation over K, then such an automorphism group G exists (and is isomorphic to the Galois group of the equation). The existence of the group G is not self-evident and is one of the central facts of Galois theory (see 3.2). However, G is given *a priori* in some important cases. For instance, this is the case if K is the field of rational functions of a single variable, P is the field obtained by adjoining all branches of an algebraic function to K, and G is the monodromy group of this algebraic function (see 5.1.2). Another example is provided by the general algebraic equation of degree n (see 3.3.3).

Suppose that the group G in the above situation is solvable. Then each element of the field P can be represented by radicals in terms of elements of the field K. The construction of a representation of an element by radicals relates mainly to linear algebra. The fact that we are working with fields is used only marginally in this construction. To stress this fact, we shall describe this construction in which a field is replaced by an algebra V, which can even be non-commutative. In what follows we need not even multiply distinct elements of this algebra. We shall use only the operation of taking a non-negative integer power k and the homogeneity of this operation with respect to multiplication by an element of the ground field, that is, the property $(\lambda a)^k = \lambda^k a^k$ for $a \in V$ and $\lambda \in K$. Thus, let V be an algebra over a field K of characteristic zero and let K contain all roots of unity.

Proposition 3.6. *Let A be an automorphism of a finite order n of the algebra V, that is, $A^n = I$, and let V_0 be the subalgebra of invariants. Let the field K be of characteristic zero and let K contain all nth roots of unity. In this case each element x of V can be represented as a sum $x = x_1 + \cdots + x_n$ of elements $x_i \in V$ such that $x_i^n \in V_0$.*

Proof. Consider the finite-dimensional vector space in V spanned by the orbit $x, A(x), \ldots, A^{n-1}(x)$ of the element x with respect to the action of the automorphism A and its powers. Since by assumption the power A^n is the identity transformation of the space V, and the field K contains all eigenvalues of the linear transformation $A\colon V \to V$, it follows that V can be decomposed into the direct sum $V = V_1 \oplus \cdots \oplus V_n$ of the eigenspaces of A with the eigenvalues ξ_k, $1 \leqslant k \leqslant n$, which are nth roots of unity (some of the spaces V_i can be zero). Therefore, the vector x can be represented in the form $x = x_1 + \cdots + x_n$, where $A(x_k) = \xi_k x_k$. Hence, $A(x_k^n) = (A(x_k))^n = \xi_k^n x_k^n = x_k^n$. That is, the element x_k^n belongs to the algebra of invariants of the automorphism A.

We introduce the following definition.

Definition. We say that an element x of the algebra V is obtained by means of the *operation of extracting the nth root of an element a* if $x^n = a$.

Using this definition, one can interpret Proposition 3.6 as follows: every element x in the algebra V can be represented as a sum of nth roots of elements of the algebra of invariants. Proposition 3.6 can readily be generalized to the case of the action of a finite commutative group of automorphisms.

Proposition 3.7. *Let G be a finite commutative group of order n of automorphisms of the algebra V and let V_0 be the subalgebra of invariants. In this case every element x of V can be represented as a sum $x = x_1 + \cdots + x_n$ of elements $x_i \in V$ such that $x_i^m \in V_0$, where m is the least common multiple of the orders of the elements of G.*

The proof of Proposition 3.7 repeats almost literally that of Proposition 3.6. One only needs the fact that a finite commutative group of linear transformations can be reduced to diagonal form in some basis.

Theorem 3.8. *Let G be a finite solvable group of automorphisms of the algebra V, and let V_0 be the subalgebra of invariants. In this case every element x of V can be*

obtained from elements of the algebra V_0 of invariants by using extraction of roots and summation.

Let us first prove the following simple assertion about an action of a group on a set.

Suppose that a group G acts on a set X, let H be a normal subgroup of G, and let X_0 be the subset of X consisting of the fixed points with respect to the action of G.

Proposition 3.9. *The subset X_H of X consisting of the fixed points with respect to the action of the normal subgroup H is invariant under the action of G. The set X_H is equipped with the natural action of the quotient group G/H with the fixed-point set X_0.*

Proof. Let $g \in G$ and $h \in H$. Then the element $g^{-1}hg$ belongs to the normal subgroup H. Let $x \in X_H$. Then $g^{-1}hg(x) = x$, or $h(gx) = g(x)$, that is, the element $g(x) \in X$ is fixed under the action of the normal subgroup H. Thus, the set X_H is invariant under the action of the group G. Under this action all elements of H act trivially. Therefore, the action of G on X_H reduces to the action of the quotient group G/H.

Let us now pass to the proof of Theorem 3.8.

Proof. Since the group G is solvable, it admits a chain of nested subgroups $G = G_0 \supset \cdots \supset G_m = e$ such that the group G_m coincides with the identity element e, for $i = 1, \ldots, m$ the group G_i is a normal subgroup of the group G_{i-1}, and the quotient group G_{i-1}/G_i is commutative.

Such a chain of subgroups exists because the group G is solvable.

We denote by $V_0 \subset \cdots \subset V_m = V$ the chain of subalgebras of invariants of the algebra V with respect to the actions of the groups $G_0, \ldots, G_m$. By Proposition 3.9, the commutative quotient group G_{i-1}/G_i acts naturally on the algebra V_i of invariants, leaving fixed every element of the subalgebra V_{i-1} of invariants. By Proposition 3.7, every element of the algebra V_i can be expressed by summation and extraction of roots in terms of elements of V_{i-1}. Repeating this argument in succession, we express every element of V in terms of elements of V_0 by a chain of extractions of roots and summations.

Remark. One can choose a chain of normal subgroups of a finite solvable group G in such a way that all the quotient groups G_i/G_{i-1} are not only commutative but also cyclic. Therefore, to prove the theorem, it suffices to use Proposition 3.6.

We complete the proof of Theorem 3.5 on the solvability of equations by radicals.

Corollary 3.10. *If the Galois group of an algebraic equation over the field K is solvable, then the equation can be solved by radicals over this field.*

Proof. By the main theorem of Galois theory, the field of invariants with respect to the action of the Galois group coincides with the field K. Therefore, the corollary follows from Theorem 3.8.

3.3.2. *Solutions of the equations of second, third, and fourth degree.* Theorem 3.8 explains why the equations of small degree are solvable by radicals.

Let $K[x_1, \dots, x_n]$ be the polynomial ring in the variables $x_1, \dots, x_n$ over a field K of characteristic zero and let K contain all roots of unity. The group $S(n)$ of all permutations of n elements acts on this ring by permuting the variables $x_1, \dots, x_n$ in the polynomials in this ring. The algebra $K_S[x_1, \dots, x_n]$ of invariants with respect to this action consists of the symmetric polynomials. Every polynomial in this algebra can be represented explicitly in the form of a polynomial in the variables $\sigma_1, \dots, \sigma_n$, where $\sigma_1 = x_1 + \dots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, $\dots$, $\sigma_n = x_1 \cdots x_n$. For $n = 2, 3, 4$ the group $S(n)$ is solvable. Applying Theorem 3.8, we see that every polynomial in $x_1, \dots, x_n$, where $n \leqslant 4$, can be expressed in terms of the elementary symmetric polynomials $\sigma_1, \dots, \sigma_n$ by using extraction of roots, summation, and multiplication by rationals. Let us consider an algebraic equation

$$x^n + a_1 x^{n-1} + \dots + a_n = 0. \tag{4}$$

By the Viète formulae, the coefficients of this equation coincide (up to sign) with the elementary symmetric functions of the roots $x_1, \dots, x_n$, and therefore *Theorem* 3.8 *for* $n = 2, 3, 4$ *gives an explicit expression of the roots of the equation* (4) *in terms of the coefficients of this equation by means of extraction of roots*, *summation*, *and multiplication by rationals.*

3.3.3. *General algebraic equation and Abel's theorem.* By the *general algebraic equation of degree* n we mean the algebraic equation

$$x^n + a_1 x^{n-1} + \dots + a_n = 0, \tag{5}$$

whose coefficients $a_1, \dots, a_n$ are independent complex variables. The general algebraic equation is defined over the field K of rational functions in the variables $a_1, \dots, a_n$. Let a^0 be some point of the space $\mathbb{C}^n$ with coordinates $a_1, \dots, a_n$ at which the discriminant of the equation (5) is non-zero. In a small neighbourhood U of the point a^0 there are n algebraic functions $x_1, \dots, x_n$ satisfying the equation (5). Let us consider the field P_U of meromorphic functions on U that is generated by the functions $x_1, \dots, x_n$ over the field K_U isomorphic to K that consists of the restrictions of the rational functions to the domain U. By definition, the field P_U is the Galois extension of the field K_U corresponding to the equation (5) over K_U.

Let $V\colon \mathbb{C}^n \to \mathbb{C}^n$ be the Viète map taking every point $x = (x_1, \dots, x_n)$ to the point $a(x)$ with coordinates $a_1 = -(x_1 + \dots + x_n)$, $\dots$, $a_n = (-1)^n x_1 \cdots x_n$. The group $S(n)$ acts on the source space. The action of $S(n)$ can be extended to the field $R[x_1, \dots, x_n]$ of rational functions in the variables $x_1, \dots, x_n$. The field $R_S[x_1, \dots, x_n]$ of invariants with respect to this action consists of the symmetric rational functions in $x_1, \dots, x_n$.

Proposition 3.11.

1) *The pair of fields* $K_U \subset P_U$ *is isomorphic to the pair of fields* $R_S[x_1, \dots, x_n] \subset R[x_1, \dots, x_n]$.

2) *The Galois group of the general algebraic equation* (5) *is isomorphic to the symmetric group* $S(n)$.

Proof. 1) The functions $x_1, \dots, x_n$ satisfying the equation (5) in a small neighbourhood U define a local inversion of the Viète map, that is, $V(x(a)) = a$, where

$x(a) = (x_1(a), \dots, x_n(a))$. We denote by U_0 the image of the domain U under this local inversion. Let us consider a pair of function fields $V^*K_U \subset V^*P_U$ on the domain U_0 induced under the map V by the function fields $K_U \subset P_U$ on the domain U. The field V^*P_U is isomorphic to the field $R[x_1, \dots, x_n]$ of all rational functions in $x_1, \dots, x_n$. The field V^*K_U is isomorphic to the field $R_S[x_1, \dots, x_n]$ of all symmetric rational functions in $x_1, \dots, x_n$. Indeed, by the theorem on the symmetric rational functions, every such function is a rational function in $x_1 + \dots + x_n$, $\dots$, $x_1 \cdots x_n$.

2) The group $S(n)$ of permutations of the coordinates acts with trivial kernel on the field of rational functions, and the corresponding field of invariants is the field of symmetric rational functions. By the main theorem of Galois theory (see 3.2), the Galois group of the Galois extension $R_S[x_1, \dots, x_n] \subset R[x_1, \dots, x_n]$ is isomorphic to the group $S(n)$.

Theorem 3.12 (Abel). *The general algebraic equation of degree $\geqslant 5$ is not solvable by radicals.*

Proof. The group $S(n)$ is not solvable for $n \geqslant 5$.

Remark. This theorem was proved by Abel before the appearance of Galois theory and group theory. Abel's original proof is closer to Liouville's method than to Galois theory.

3.4. Reduction of the degree of an equation. Is it possible to express the roots of a given algebraic equation of degree n in terms of its coefficients by using arithmetic operations, adjoining radicals, and adjoining solutions of algebraic equations of degree $k < n$? In 3.4.2 we give an answer to this question in terms of the Galois group of the equation. To this end, we need some properties of subgroups of the symmetric group.

3.4.1. *Subgroups of the symmetric group on k elements.* We need the following lemma.

Lemma 3.13 [21]. *A group Γ is isomorphic to a subgroup of $S(k)$ if and only if the group Γ has a set of subgroups Γ_i, $i = 1, \dots, m$, such that*:

1) *the group $\bigcap_{i=1}^m \Gamma_i$ contains no non-trivial normal subgroups of Γ;*
2) $\sum_{i=1}^m \operatorname{ind}(\Gamma, \Gamma_i) \leqslant k$.

Proof. Let Γ be a subgroup of $S(k)$. Consider a representation of the group Γ as a subgroup of permutations of a set M having k elements. Suppose that the set M decomposes into m orbits under the action of the group Γ. In each orbit we choose a point x_i. The set of the stationary subgroups (stabilizers) Γ_i of the points x_i satisfies the conditions in the lemma.

Conversely, let a group Γ have a set of subgroups satisfying the conditions of the lemma. We denote by P the disjoint union of the sets $P_i = \{P_i^j\}$, that is, of the sets of right cosets P_i^j of the subgroup Γ_i in the group Γ. The group Γ acts naturally on the set P. The representation of Γ in the group $S(P)$ thus obtained is faithful, because the kernel of this representation belongs to the group $\bigcap_{i=1}^m \Gamma_i$. The group $S(P)$ can be embedded in the group $S(k)$, because the set P contains $\sum_{i=1}^m \operatorname{ind}(\Gamma, \Gamma_i) \leqslant k$ elements.

Corollary 3.14. *Every quotient group of a subgroup of the symmetric group $S(k)$ is isomorphic to a subgroup of $S(k)$.*

Proof. Let a group G be isomorphic to a subgroup of the group $S(k)$ and let Γ_i be a family of subgroups of G satisfying the conditions of Lemma 3.13. Let π be an arbitrary homomorphism of G. Then the family of subgroups $\pi(\Gamma_i)$ of the group $\pi(G)$ also satisfies the conditions of the lemma.

Definition. We say that a *normal subgroup H* of a group G *is of profundity at most k* if G has a subgroup G_0 with index at most k and such that H is equal to the intersection of all the subgroups conjugate to G_0. We say that a *group G is of profundity at most k* if the identity element of this group is a normal subgroup of profundity at most k.

Definition. By a *normal tower* of a group G we mean a chain of nested subgroups $G = G_0 \supset \cdots \supset G_n = e$ such that G_0 coincides with the original group G, G_n is trivial, and for any $i = 0, 1, \ldots, n-1$ the group G_{i+1} is a normal subgroup of the group G_i.

Corollary 3.15. *If a group G is a subgroup of the group $S(k)$, then G admits a normal tower $G = G_0 \supset \cdots \supset G_n = e$ such that the group G_i has profundity at most k in the group G_{i-1} for any $i = 1, \ldots, n$.*

Proof. Let Γ_i be the family of subgroups of the group G that satisfy the conditions of Lemma 3.13. We denote by F_i the normal subgroup of G equal to the intersection of all the subgroups conjugate to the group Γ_i. The chain of subgroups $G_0 = F_0$, $G_1 = F_0 \cap F_1$, $\ldots$, $G_m = F_0 \cap \cdots \cap F_m$ satisfies the conditions of the corollary.

3.4.2. *Condition for the reducibility of the degree of an equation with the help of radicals.* Let us begin with formal definitions.

Definition. An algebraic equation over a field K is said to be *solvable by radicals and roots of equations of degree at most k* (or, briefly, *solvable by k-radicals*) if there is a chain of extensions $K = K_0 \subset \cdots \subset K_N$ such that the field K_i is obtained from the field K_{i-1}, $i = 1, \ldots, N$, by adjoining either a radical or all the roots of an algebraic equation of degree at most k with coefficients in the field K_{i-1}, and the field K_N contains all the roots of the original algebraic equation.

Definition. A group G is said to be *k-solvable* if there is a normal tower

$$G = H_0 \supset \cdots \supset H_N = e$$

such that for any $i = 1, \ldots, N$ either the profundity of the normal subgroup H_i of the group H_{i-1} is at most k or the quotient group H_{i-1}/H_i is commutative.

Theorem 3.16. *An algebraic equation is solvable by k-radicals if and only if its Galois group G is k-solvable.*

The following lemma holds.

Lemma 3.17. *Let a finite group of automorphisms act on a field P, with field of invariants P_0. Let the orbit of a point $x \in P$ contain exactly m elements. Then x satisfies some algebraic equation of degree m with coefficients in the field P_0.*

Proof. Let $x_1, \dots, x_m$ be the points of the orbit. The elementary symmetric functions $\sigma_1, \dots, \sigma_m$ of these points remain fixed under the action of the group, and hence belong to the field of invariants. The points of the orbit are roots of an algebraic equation of degree m, namely,

$$x^m - \sigma_1 x^{m-1} + \cdots + (-1)^m \sigma_m = 0,$$

with coefficients in the field P_0 of invariants.

Lemma 3.18. *Let a finite group of automorphisms G act on a field P, with field of invariants P_0. Let the profundity of the group G be at most k. Then the field P can be obtained from the field P_0 by adjoining all roots of some algebraic equation of degree at most k with coefficients in P_0.*

Proof. Let G_0 be a subgroup of G of index m at most k such that the intersection of all the subgroups conjugate to G_0 contains only the identity element of G. By the main theorem of Galois theory, corresponding to the subgroup G_0 is an intermediate field P_1, that is, $P_0 \subseteq P_1 \subseteq P$. The field P_1, as well as any other finite algebraic extension of P_0, is generated over P_0 by some element x. The point x has the following property: an element g of G leaves x fixed if and only if $g \in G_0$. The orbit of x with respect to the action of G contains exactly m points, because the index of the stabilizer of x is equal to m. A non-identity element of G determines a non-identity permutation of the points of the orbit, because the intersection of the subgroups conjugate to G_0 coincides with the identity element of G. The field generated over P_0 by the elements of the orbit coincides with P. Indeed, this field corresponds to the trivial subgroup of the Galois group. Lemma 3.18 follows now from Lemma 3.17.

We return to the proof of Theorem 3.16.

Proof of Theorem 3.16. 1) The necessity of the condition on the Galois group is proved just as we proved that solvability of the Galois group is necessary for solvability of the equation by radicals. One need only consider what happens with the Galois group G_i of our equation over the field K_i upon passage to the field K_{i+1} if K_{i+1} is obtained from K_i by adjoining all the roots of an equation of degree $\leqslant k$. In this case the Galois group of K_{i+1} over K_i is a subgroup of the group $S(k)$ (see Lemma 3.2). By Theorem 3.4 on the behaviour of the Galois group under a change of the ground field, the quotient group G_i/G_{i+1} is a quotient group of some subgroup of $S(k)$. According to Corollaries 3.14 and 3.15, the group G_i/G_{i+1} admits a normal tower $G_i/G_{i+1} = \Gamma_0 \supset \cdots \supset \Gamma_m = e$ such that the group Γ_{i+1} is of profundity $\leqslant k$ in the group Γ_i. It suffices to insert a chain of subgroups

$$G_i = \Gamma_{0i} \supset \cdots \supset \Gamma_{mi} = G_{i+1}$$

between the groups $G_i \supset G_{i+1}$, where Γ_{pi} is the pre-image of Γ_p under the natural homomorphism $G_i \to G_i/G_{i+1}$. It is clear that $\Gamma_{p+1,i}$ is a normal subgroup of

profundity $\leqslant k$ in Γ_{pi}. This fills the gap in the proof of the necessity of the condition on the Galois group.

2) The sufficiency of the condition on the Galois group is proved by induction on the length N of a normal tower in G. The group G has a k-solvable normal subgroup H_1 with a normal tower of length $N-1$. We denote by P_1 the field of invariants of H_1. By the induction assumption, the field P is obtained from the field P_1 by adjoining radicals and roots of equations of degree at most k. The quotient group G/H_1 acts on the field P_1, with field of invariants P_0. If G/H_1 is commutative, then P_1 is obtained from P_0 by adjoining radicals (see Proposition 3.7). If G/H_1 is of profundity at most k, then P_1 is obtained from P by adjoining all roots of an algebraic equation of degree at most k (see Lemma 3.18).

Theorem 3.19. *The general algebraic equation* (see 3.3.3) *of degree* $n \geqslant 5$ *is not solvable by radicals and roots of algebraic equations of degree less than* n.

Proof. The Galois group of the general algebraic equation of degree n is isomorphic to the group $S(n)$ (see 3.3.3).

For $n \geqslant 5$ the group $S(n)$ has only two distinct towers of normal subgroups: the trivial tower $e \subset S(n)$ and the tower $e \subset A(n) \subset S(n)$, where e is the identity subgroup and $A(n)$ is the alternating subgroup. Therefore, $S(n)$ is not k-solvable for $k < n$ and $n \geqslant 5$.

§ 4. Solvability of linear differential equations by quadratures and the Picard–Vessiot theory

Picard noted an analogy between linear differential equations and algebraic equations and started the construction of a differential analogue of Galois theory. This theory was crowned by the Picard–Vessiot theorem, in which the problem of solvability or unsolvability of a linear differential equation is related to the problem of solvability or unsolvability of a certain algebraic Lie group.

4.1. Analogy between linear differential equations and algebraic equations. Let us recall the simplest properties of linear differential equations and their analogues for algebraic equations.

4.1.1. *Division with remainder and the greatest common divisor of differential operators.* By a *linear differential operator of order* n over a differential field K we mean an operator $L = a_n D^n + \cdots + a_0$, where $a_i \in K$ and $a_n \neq 0$, acting on any element y of the field K by the formula

$$L(y) = a_n y^{(n)} + \cdots + a_0 y.$$

For operators L_1 and L_2 over K their product $L = L_1 \circ L_2 = L_1(L_2)$ is also an operator over K. Generally, the product of operators is non-commutative, but this fact is not apparent at the leading term. Namely, the *leading term* $a_n D^n$ *of the operator* $L = L_1 \circ L_2$ *is equal to* $b_m c_k D^{m+k}$, *where* $b_m D^m$ *and* $c_k D^k$ *are the leading terms of the operators* L_1 *and* L_2, *respectively.*

For operators L and L_2 of orders n and k over K there exist operators L_1 and R over K such that $L = L_1 \circ L_2 + R$ and the order of R is strictly less than k, and these operators L_1 and R are unique. The operator R is called the

remainder upon right division of the operator L by the operator L_2. The operators L_1 and R can be constructed explicitly from the operators L and L_2; the algorithm for division with remainder for operators is based on the above formula for the leading term of the product of operators and is quite analogous to the algorithm for division with remainder for polynomials in one variable.

For any two operators L_1 and L_2 over K one can explicitly find the right greatest common divisor N, that is, an operator N over K of the greatest possible order such that N divides the operators L_1 and L_2 from the right, that is, $L_1 = M_1 \circ N$ and $L_2 = M_2 \circ N$, where M_1 and M_2 are some operators over K. The process of finding the operators M_1, M_2, and N for given operators L_1 and L_2 is quite analogous to the Euclidean algorithm for finding the greatest common divisor of two polynomials in one variable and is based on the algorithm for division with remainder for operators. As in the commutative case, the greatest common divisor N is representable in the form $N = AL_1 + BL_2$, where A and B are some operators over K.

It is clear that y is a solution of the equation $N(y) = 0$ if and only if $L_1(y) = 0$ and $L_2(y) = 0$.

4.1.2. *Passage to a linear differential equation of lower order as an analogue of the Bézout theorem.* Let L be a linear differential operator over K, let y_1 be a non-zero element of the field K, let $p = \dfrac{y_1'}{y_1}$ be the logarithmic derivative of y_1, and let $L_2 = D - p$ be a first-order operator annihilating y_1. The remainder R upon right division of L by L_2 is the operator of multiplication by c_0, where $c_0 = \dfrac{1}{y_1} L(y_1)$. Indeed, the desired equality is obtained by substituting $y = y_1$ in the identity $L(y) \equiv L_1 \circ L_2(y) + c_0 y$. The operator L is right divisible by the operator L_2 if and only if the element y_1 satisfies the identity $L(y_1) \equiv 0$.

Using a non-zero solution y_1 of an equation $L(y) = 0$ of order n, one can reduce the order of this equation. To this end, one must represent the operator L in the form $L = L_1 \circ L_2$, where L_1 is an operator of order $(n-1)$. *The coefficients of the operator L_1 belong to the extension of the differential field K by the logarithmic derivative p of the element y_1.* If some solution u of the equation $L_1(u) = 0$ is known, then from this solution one can construct a solution y of the original equation $L(y) = 0$. To this end, it suffices to solve the equation $L_2(y) = y' - py = u$. The procedure described above is called *reduction of the order of a differential equation.*

Remark. An operator annihilating y_1 is defined up to multiplication by an arbitrary function, and the procedure of reducing the order depends on this function. It is simpler to divide by the operator $\widetilde{L}_2 = D \circ y_1^{-1}$ that is the composition of multiplication by the element y_1^{-1} and differentiation. To this end, it suffices to compute the operator $L_3 = L \circ y_1$ that is the composition of multiplication by the element y_1 and the operator L. The operator L_3 is right divisible by D, that is, $L_3 = \widetilde{L}_1 \circ D$ (because $L_3(1) \equiv L \circ y_1(1) \equiv 0$). It is clear that $L = \widetilde{L}_1 \circ \widetilde{L}_2$. The original equation $L(y) = 0$ is reduced to the equation $\widetilde{L}_1(u) = 0$ of smaller order. This procedure for lowering the order is usually presented in handbooks and manuals on differential equations. We note that the coefficients of the operator $\widetilde{L}_1$

belong to the extension of the differential field K by the element y_1 itself rather than by its logarithmic derivative p, and this sometimes makes $\widetilde{L}_1$ less convenient than L_1.

The following analogues of the above facts are known in algebra: 1) the remainder upon division by $(x-a)$ of a polynomial P in a variable x is equal to the value of P at the point a (the Bézout theorem); 2) if a solution x_1 of an equation $P(x)=0$ is known, then one can reduce the degree of the equation, namely, the other roots of the polynomial P satisfy an equation $Q(x)=0$ of smaller degree, where $Q=P/(x-x_1)$. Along with the analogues, there is a difference: a solution of a differential equation obtained by using the procedure of reduction of the order is not a solution of the original equation in general.

Remark. Exponentials are eigenfunctions of differential operators $P(D)$ with constant coefficients. This fact is equivalent to the Bézout theorem. Indeed, if $P=Q(x-a)+P(a)$, then $P(D)=Q(D)\circ(D-a)+P(a)$. Therefore, a solution y_1 of the differential equation $(D-a)y=0$ is an eigenvector of the operator $P(D)$ with the eigenvalue $P(a)$.

4.1.3. *Analogue of the Viète formulae for differential operators.* If all the roots $x_1,\dots,x_n$ of a polynomial P of degree n with leading coefficient 1 are known, then P can be recovered; namely, by the Viète formulae one has $P(x)=x^n+p_1x^{n-1}+\dots+p_n$, where $p_1=-\sigma_1$, …, $p_n=(-1)^n\sigma_n$ and $\sigma_1=x_1+\dots+x_n$, …, $\sigma_n=x_1\cdots x_n$. The functions $\sigma_1,\dots,\sigma_n$ remain the same under any permutation of the roots and are called the *elementary symmetric functions*.

Similarly, if n linearly independent solutions $y_1,\dots,y_n$ of a linear differential equation $L=0$ of order n are known, where L is an operator whose coefficient with the highest derivative is equal to 1, then the operator L can be recovered. Indeed, we note first that there is at most one operator of this kind, because the difference L_1-L_2 between two operators having these properties is an operator of order $<n$ having n linearly independent solutions, which is possible only if L_1 coincides with L_2.

The Wronskian W of n independent solutions $y_1,\dots,y_n$ of a linear differential equation cannot vanish. Let us consider the equation $W(y,y_1,\dots,y_n)=0$, where $W(y,y_1,\dots,y_n)$ is the Wronskian of an unknown function y and the functions $y_1,\dots,y_n$. Expanding the Wronskian

$$W(y,y_1,\dots,y_n)=\begin{vmatrix} y & y_1 & \dots & y_n \\ \vdots & \vdots & & \vdots \\ y^{(n)} & y_1^{(n)} & \dots & y_n^{(n)} \end{vmatrix}$$

with respect to the first column and dividing it by W, we obtain the equation

$$y^{(n)}+p_1y^{(n-1)}+\dots+p_ny=0 \tag{6}$$

in which $p_1=-\varphi_1,\dots,p_n=(-1)^n\varphi_n$, where

$$\varphi_1=\frac{\begin{vmatrix} y_1 & \dots & y_n \\ \vdots & & \vdots \\ y_1^{(n-2)} & \dots & y_n^{(n-2)} \\ y_1^{(n)} & \dots & y_n^{(n)} \end{vmatrix}}{W},\quad\dots,\quad \varphi_n=\frac{\begin{vmatrix} y_1' & \dots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-1)} & \dots & y_n^{(n-1)} \\ y_1^{(n)} & \dots & y_n^{(n)} \end{vmatrix}}{W}. \tag{7}$$

The functions $y_1, \dots, y_n$ and their linear combinations are solutions of the equation (6). The formulae (6) and (7) are quite similar to the Viète formulae.

The functions $\varphi_1, \dots, \varphi_n$ are rational functions in the functions $y_1, \dots, y_n$ and their derivatives up to order n. These functions depend only on the linear space V spanned by the functions $y_1, \dots, y_n$ and do not depend on the choice of a specific basis $y_1, \dots, y_n$ in the space V. In other words, the functions $\varphi_1, \dots, \varphi_n$ of $y_1, \dots, y_n$ and their derivatives are $GL(V)$-invariant. We refer to the functions $\varphi_1, \dots, \varphi_n$ as the *elementary differential invariants* of $y_1, \dots, y_n$.

4.1.4. *Analogue of the theorem on the symmetric functions for differential operators.* As is known in algebra, every rational function in the variables $x_1, \dots, x_n$ that is invariant under permutations of the variables is in fact a rational function in the elementary symmetric functions $\sigma_1, \dots, \sigma_n$ of the variables $x_1, \dots, x_n$. In other words, every rational expression depending symmetrically on the roots of a polynomial of degree n can be expressed rationally in terms of the coefficients of this polynomial.

A similar theorem for linear differential equations was discovered by Picard.

Theorem 4.1. *Every rational function R in linearly independent functions $y_1, \dots, y_n$ and their derivatives that is $GL(V)$-invariant* (that is, that remains the same when the functions $y_1, \dots, y_n$ are replaced by their linear combinations $z_1 = a_{11}y_1 + \dots + a_{1n}y_n, \dots, z_n = a_{n1}y_1 + \dots + a_{nn}y_n$ under the assumption that the matrix $A = \{a_{ij}\}$ is non-singular) *is in fact a rational function in the elementary differential invariants $\varphi_1, \dots, \varphi_n$ of the functions $y_1, \dots, y_n$ and the derivatives of these invariants.*

Proof. Each function y in the space V spanned by the functions $y_1, \dots, y_n$ satisfies the identity $y^{(n)} - \varphi_1 y^{(n-1)} + \dots + (-1)^n \varphi_n y = 0$. Differentiating this identity, one can express every derivative of the function y of order $\geqslant n$ in terms of the function y, its derivatives of orders $< n$, the elementary differential invariants, and their derivatives. Substituting these expressions for the higher derivatives of the functions $y_1, \dots, y_n$ into the rational function R, we obtain a rational function $\widetilde{R}$ in the functions $\varphi_1, \dots, \varphi_n$, their derivatives, and the elements of the fundamental matrix Y, where

$$Y = \begin{pmatrix} y_1 & \dots & y_n \\ \vdots & & \vdots \\ y_1^{(n-1)} & \dots & y_n^{(n-1)} \end{pmatrix}.$$

The function $\widetilde{R}$ is preserved under any linear transformation of the space V spanned by $y_1, \dots, y_n$. Every non-singular $n \times n$ matrix can be obtained as the image of the fundamental matrix Y under some linear transformation of the space V. The rational function $\widetilde{R}$ must be constant on the set of non-singular matrices, and therefore it is constant on the set of all matrices, does not depend on the matrix Y, and depends only on the differential invariants and their derivatives.

Corollary 4.2. *Every rational function in independent solutions $y_1, \dots, y_n$ of a linear differential equation and their derivatives that remains invariant under the choice of another basis $z_1, \dots, z_n$ in the space of solutions is a rational function in the coefficients of the differential equation and their derivatives.*

4.2. Galois group of a linear differential equation. Let us consider a linear differential equation

$$y^{(n)} + p_1 y^{(n-1)} + \cdots + p_n y = 0 \tag{8}$$

with coefficients in some differential function field K. (As usual, we always assume that the field K contains all complex constants.)

By a *differential polynomial* over K in functions $u_1, \ldots, u_n$ we mean a polynomial in the functions $u_1, \ldots, u_n$ and their derivatives with coefficients in K. By a *differential relation* over K among the solutions $y_1, \ldots, y_n$ of the equation (8) we mean a differential polynomial over K in the functions $u_1, \ldots, u_n$ that vanishes under the substitution $u_1 = y_1, \ldots, u_n = y_n$.

Definition. By the *Galois group of a differential equation* (8) *over a differential field* K we mean the subgroup G of the group $GL(V)$ of all linear transformations of the solution space V of the equation (8) that preserve all differential relations over K among the solutions of the equation (that is, if $A \in G$ and if Q is an arbitrary relation over K among some solutions $y_1, \ldots, y_n$, then the solutions $Ay_1, \ldots, Ay_n$ must satisfy the same relation Q).

Proposition 4.3. *The Galois group of a linear differential equation is an algebraic subgroup of* $GL(V)$.

Proof. It is clear that the set of linear transformations A for which the relation Q holds for $Ay_1, \ldots, Ay_n$ is an algebraic set for any differential relation Q among the solutions $y_1, \ldots, y_n$. The intersection of arbitrarily many algebraic varieties is an algebraic variety.

Definition. A differential function field P is called a *Picard–Vessiot extension* of a differential function field K if there is a linear differential equation (8) with coefficients in K such that P is obtained by adjoining all the solutions of (8) to K. By the *Galois group of a Picard–Vessiot extension* P over a field K we mean the group of all automorphisms of the differential field P that leave fixed every element of K.

Every element τ of the Galois group of a differential field P over a differential field K defines a linear transformation of the solution space and preserves all differential relations defined over K among the solutions. Thus, the Galois group of P over K has a representation into the Galois group G of the corresponding equation (8) defining the Picard–Vessiot extension P. Obviously, this representation is a group isomorphism, that is, the Galois group of the equation and the Galois group of the Picard–Vessiot extension given by the equation are isomorphic. Using this isomorphism, one can define a structure of an algebraic group on the Galois group of the Picard–Vessiot extension. If two distinct linear differential equations over the field K define the same Picard–Vessiot extension, then the Galois groups of the equations are isomorphic not only as abstract groups but also as algebraic groups. Therefore, the structure of an algebraic group is well defined on the Galois group of a Picard–Vessiot extension.

4.3. Main theorem of the Picard–Vessiot theory. Let P be a Picard–Vessiot extension of a differential field K and let G be the Galois group of P.

The following maps between the set of intermediate differential fields F, $K \subseteq F \subseteq P$, and the set of subgroups of the Galois group G are defined.

1) The *map* Fd that assigns to every subgroup Γ of G the differential field $Fd(\Gamma)$ consisting of the elements of P that are fixed under the action of Γ (it is clear that $K \subseteq Fd(\Gamma)$).

2) The *map* Gp that assigns to every intermediate differential field F, $K \subseteq F \subseteq P$, the subgroup $Gp(F) \subseteq G$ that is the Galois group of the Picard–Vessiot extension P of the field F (P is a Picard–Vessiot extension of K, and therefore it is automatically a Picard–Vessiot extension of any intermediate field F, $K \subset F \subset P$).

The maps Fd and Gp establish the *Galois correspondence* between the subgroups of the Galois group and the intermediate differential fields of the Picard–Vessiot extension. We present the following theorem without proof.

Theorem 4.4 (main theorem of the Picard–Vessiot theory). *For any Picard–Vessiot extension P of a differential field K with Galois group G:*

1) *the composition of the maps Fd and Gp is the identity map of the set of intermediate fields onto itself, namely, if F is a differential field and $K \subseteq F \subseteq P$, then $Fd(Gp(F)) = F$;*

2) *the composition of the maps Gp and Fd assigns to every subgroup Γ of the Galois group G the algebraic closure $\overline{\Gamma}$ of Γ in G, namely, if Γ is a subgroup of the Galois group, $\Gamma \subset G$, then $Gp(Fd(\Gamma)) = \overline{\Gamma}$;*

3) *an intermediate differential field F, $K \subseteq F \subseteq P$, is a Picard–Vessiot extension of the field K if and only if the group $Gp(F)$ is a normal subgroup of G, and moreover, the Galois group of a Picard–Vessiot extension F of the field K is the quotient group of G by the normal subgroup $Gp(F)$.*

Let us prove a useful characteristic property of the Picard–Vessiot extensions that follows immediately from the main theorem.

Corollary 4.5. *A differential field P is a Picard–Vessiot extension of a differential field K, $K \subseteq P$, if and only if there is a group Γ of automorphisms of the differential field P such that* 1) *this group leaves fixed all elements of K and only these elements*; 2) *there is a finite-dimensional linear space V over the field of constants such that V belongs to P, V is Γ-invariant, and P is the smallest differential field containing V and K.*

Proof. The properties indicated in the corollary are satisfied for any Picard–Vessiot extension. This follows from the assertion 1) of the main theorem applied to the field $F = K$. Conversely, let $y_1, \dots, y_n$ be a basis of the linear space V in the assertion 2) of the corollary. The coefficients of a linear differential equation of order n on the functions $y_1, \dots, y_n$ are invariant under all linear transformations of the space V. Therefore, they are invariant under the group Γ, and thus all these coefficients belong to K. Hence, the field P is obtained from K by adjoining all solutions of the above equation, and thus P is a Picard–Vessiot extension of the field K.

What happens with the Galois group of a linear differential equation if one extends the differential field K of coefficients by replacing it by a larger differential field K_1? This question is of special interest if K_1 is a Picard–Vessiot extension

of K. We denote by G_1 the Galois group of the extension K_1 of K. The results on unsolvability of linear differential equations are based on the following theorem of the Picard–Vessiot theory (we present this theorem without proof; its formulation is quite similar to that of Theorem 3.4).

Theorem 4.6 (on the change of the Galois group of an equation under a Picard–Vessiot extension of the field of coefficients). *If the differential field K of the coefficients is replaced by a Picard–Vessiot extension K_1 of K, then the Galois group G of the equation is replaced by some algebraic normal subgroup H of G. The quotient group G/H of G by H is isomorphic to some algebraic quotient group of the Galois group G_1 of the new differential field K_1 over the old differential field K.*

4.4. Simplest Picard–Vessiot extensions. In this subsection we treat the following simplest Picard–Vessiot extensions: an algebraic extension, adjoining an integral, and adjoining the exponential of an integral.

4.4.1. *Algebraic extension.* Let us consider an algebraic equation

$$Q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \tag{9}$$

over a differential function field K and the Galois extension P obtained by adjoining all the solutions of the equation (9) to K.

Lemma 4.7. *The field P is a differential field. Every automorphism of P over K that preserves only the arithmetic operations in P preserves automatically the operation of differentiation as well.*

Proof. Modifying the algebraic equation (9) if necessary, one can assume that it is irreducible over K and that every root x_i of (9) generates the field P over K. Differentiating the identity $Q(x_i) = 0$, we obtain $\dfrac{\partial Q}{\partial x}(x_i)x_i' + \dfrac{\partial Q}{\partial t}(x_i) = 0$, where $\dfrac{\partial Q}{\partial t} = \sum_{i=1}^{n-1} a_i' x^i$. The polynomial $\dfrac{\partial Q}{\partial t}$ cannot vanish at the point x_i, because the equation $Q = 0$ is irreducible. We obtain the algebraic expression $x_i' = -\dfrac{\partial Q}{\partial x}(x_i) \Big/ \dfrac{\partial Q}{\partial t}(x_i)$ for the derivative of the root x_i, which is the same for all roots x_i of the polynomial Q. This implies both the assertions of the lemma.

The Galois group Γ of a Galois extension P over the field K leaves fixed only the elements of the field K. The linear space V (over the field of constants) spanned by the roots $x_1, \ldots, x_n$ of the equation (9) is invariant under the action of the group Γ. By Corollary 4.5, the differential field P is a Picard–Vessiot extension. The Galois group of the Picard–Vessiot extension P of K coincides with the Galois group of the algebraic equation (9). *The main theorem of the Picard–Vessiot theory for the Picard–Vessiot extension P of the differential field K coincides with the main theorem of Galois theory for the Galois extension P of the field K.*

4.4.2. *Adjoining an integral.* Let y_1 be an integral over a differential function field K and let $y_1' = a$, $a \in K$, and $a \neq 0$.

A homogeneous differential equation $ay'' - a'y' = 0$ has independent solutions given by the function y_1 and the function identically equal to 1. Therefore, the extension of the differential field K obtained from K by adjoining the element y_1 is a Picard–Vessiot extension (because we always assume that K contains all complex constants).

Lemma 4.8. *The integral y_1 either belongs to the field K or is transcendental over it.*

Proof. Suppose that the integral y_1 is algebraic over the field K. Let $Q(y) = a_n y^n + \cdots + a_0 = 0$ be an equation irreducible over K such that $Q(y_1) = 0$. One can assume that $n > 1$ and $a_n = 1$. Differentiating the identity $Q(y) = 0$, we get that y_1 satisfies the equation $na_n y^{n-1} + \cdots + a_0' = 0$ of smaller degree. This contradicts the condition that the polynomial Q is irreducible.

Let the element y_1 be transcendental over K. We show that the only independent differential relation for y_1 over K is of the form $y_1' = a$. Indeed, using this relation, one can rewrite every differential polynomial in y_1 over K as a polynomial in y_1 with coefficients in K. However, no non-trivial polynomial of this kind can vanish, because y_1 is transcendental over K. Therefore, the Galois group of the equation $ay'' - a'y' = 0$ consists of the linear transformations of the form $Ay_1 = y_1 + C$, $A(1) = 1$, where C is an arbitrary complex number. Thus, *the Galois group of a non-trivial extension by an integral is isomorphic to the additive group of complex numbers.*

In Kolchin's terminology [26] an algebraic group is said to be *anticompact* if it contains no non-identity finite-order elements. Obviously, the *Galois group of a non-trivial extension by an integral is anticompact.*

Proposition 4.9. *There are no differential fields between the fields K and $K\langle y\rangle$, where y is an integral over K not belonging to K.*

Proof. Indeed, let F be a differential field such that $K \subset F \subseteq K\langle y\rangle$. Let $b \in F$ and $b \notin K$. Then the element b is representable in the form of a non-trivial rational function in y with coefficients in K. The existence of such a function means that y is algebraic over F. However, y is an integral over F, because $y' = a \in K$. An integral is algebraic over a differential field if and only if it belongs to this field (see Lemma 4.8), that is, $F = K\langle y\rangle$.

This proposition proves the main theorem of the Picard–Vessiot theory for any adjoining of an integral. Indeed, the Galois group G of the field $K\langle y\rangle$ over the field K has no algebraic subgroups, and the pair of differential fields $K \subset K\langle y\rangle$ contains no intermediate differential fields.

4.4.3. *Adjoining the exponential of an integral.* Let y_1 be the exponential of an integral over a differential function field K, that is, $y_1' = ay_1$, where $a \in K$. By definition, the extension of the field K by the element y_1 is a Picard–Vessiot extension.

Lemma 4.10. *Let the exponential y_1 of an integral be algebraic over the field K. Then y_1 is a radical over K.*

Proof. Let $Q(y) = a_n y^n + \cdots + a_0 = 0$ be an irreducible equation over K such that $Q(y_1) = 0$. One can assume that $n > 1$, $a_n \neq 0$, and $a_0 = 1$. Differentiating the identity $Q(y_1) = 0$, we obtain the equation $\sum(a_k' + ka_k a)y^k = 0$ on y_1. This equation is of degree $\leqslant n$ and contains no constant term. All the coefficients of this equation must be identically zero, because otherwise we obtain a contradiction to the irreducibility of the polynomial Q. The equality $a_n' + na_n a = 0$ means that

the quotient $a_n/y_1^n = c$ is constant. Indeed, it follows from the relation $y_1' = ay_1$ that $(y_1^{-n})' + na(y_1^{-n}) = 0$, or, in other words, the functions y_1^{-n} and a_n satisfy the same equation. Therefore, $y_1^n = a_n/c$. This proves the lemma.

We assume that the element y_1 is transcendental over K. Let us show that in this case the only independent differential relation on y_1 over K is of the form $y_1' = ay_1$. Indeed, using this relation, one can rewrite every differential polynomial in y_1 over K as an algebraic polynomial in y_1 with coefficients in K. However, no non-trivial polynomial of this kind can vanish, because y_1 is transcendental over K. Therefore, the Galois group of the equation $y' = ay$ consists of the linear transformations of the form $Ay_1 = Cy_1$, where $C \neq 0$ is an arbitrary non-zero complex number. Thus, the *Galois group of a non-algebraic extension given by adjoining the exponential of an integral coincides with the multiplicative group $\mathbb{C}^*$ of the non-zero complex numbers.*

The exponential of an integral over K is an algebraic element y over K if and only if y is a radical over K. Therefore, *if the adjoining of the exponential of an integral is an algebraic extension, then the Galois group of this extension is a finite multiplicative subgroup of $\mathbb{C}^*$.*

In Kolchin's terminology [26] an algebraic group is said to be *quasi-compact* if each non-identity subgroup of G contains non-identity finite-order elements. Obviously, the Galois group of a non-algebraic extension obtained by adjoining the exponential of an integral is quasi-compact.

Proposition 4.11. *Let y be the exponential of an integral over K and let y be transcendental over K. In this case to every non-negative integer n one can assign a differential field between the fields K and $K\langle y\rangle$, namely, the differential field K_n consisting of the rational functions in the element y^n with coefficients in K. The fields K_n are different for different non-negative integers n. Every intermediate differential field coincides with some field K_n.*

Proof. Let F be a differential field that contains strictly the field K and is contained in the field $K\langle y\rangle$. Repeating the arguments in Proposition 4.9, we see that y is algebraic over F. The element y is the exponential of an integral over F. Therefore, the irreducible algebraic equation on y over the field F is of the form $y^n - a = 0$, where $a \in F$ (see Lemma 4.10), and hence $K_n \subseteq F$. The field K_n must coincide with F. Indeed, otherwise there is an element $b \in F$ such that $b \notin K_n$. The element b is a rational function R of y, and the relation $R(y)$ is not a consequence of the equation $y^n = a$. This contradicts the fact that the equation $y^n = a$ is irreducible. The contradiction shows that $K_n = F$. The fields K_n differ for different n because y is transcendental over K.

The proposition proves the main theorem of the Picard–Vessiot theory for any adjoining of the exponential of an integral. Indeed, every proper algebraic subgroup of the group $\mathbb{C}^*$ is the group of nth roots of unity for some n. A differential field that is intermediate between K and $K\langle y\rangle$ consists of the elements of the field $K\langle y\rangle$ that are left fixed under the action of the group of nth roots of unity on $K\langle y\rangle$.

4.5. Solvability of differential equations. An *algebraic group* G is said to be *solvable*, *k-solvable*, or *almost solvable in the category of algebraic groups*, respectively, if it admits a normal tower of algebraic subgroups $G = G_0 \supset \cdots \supset G_m = e$ with the following properties:

a) (for solvable groups) the quotient group G_{i-1}/G_i is commutative for any $i = 1, \ldots, m$;
b) (for k-solvable groups) either the profundity of G_i in G_{i-1} is at most k or G_{i-1}/G_i is commutative for any $i = 1, \ldots, m$;
c) (for almost solvable groups) either the index of G_i in G_{i-1} is finite or G_{i-1}/G_i is commutative for any $i = 1, \ldots, m$.

Theorem 4.12 (Picard–Vessiot). *A linear differential equation over a differential field K is solvable by quadratures, by k-quadratures, or by generalized quadratures, respectively, if and only if the Galois group of the equation over the field K is solvable, k-solvable, and almost solvable, respectively, in the category of algebraic groups.*

Remark. The question of the solvability of equations by k-quadratures is not discussed in the classical Picard–Vessiot theorem. We have included this in the theorem because, first, it has an answer analogous to the answers to the classical questions and, second, it can be extended to the topological version of Galois theory.

In this subsection we prove only the necessity of the conditions on the Galois group for the solvability of the equation. We postpone the proof of the sufficiency until 4.7. Thus, the following theorem holds.

Theorem 4.13. *If a linear differential equation is solvable by quadratures, by k-quadratures, or by generalized quadratures, then the Galois group G of this equation is solvable, k-solvable, or almost solvable in the category of algebraic groups, respectively.*

Proof. The solvability of an equation by generalized quadratures over the field K means the existence of a chain of differential fields $K = K_0 \subset \cdots \subset K_N$ in which the first field coincides with the original field K, the last field K_N contains all the solutions of the differential equation, and for any $i = 1, \ldots, N$ the field K_i is obtained from the field K_{i-1} by adjoining an integral, the exponential of an integral, or all the solutions of an algebraic equation. (In the case of solvability by quadratures the last type of extension is forbidden; in the case of solvability by k-quadratures only adjoining the roots of algebraic equations of degree at most k is allowed.)

Let $G = G_0 \supset \cdots \supset G_m = e$ be a descending chain of groups in which G_i is the Galois group of the original equation over the field K_i. By the main theorem (Theorem 4.4), G_{i-1}/G_i is the quotient group of the Galois group of the Picard–Vessiot extension K_i of the field K_{i-1}. If this extension is obtained by adjoining an integral or the exponential of an integral, then the group G_{i-1}/G_i is commutative as a quotient group of a commutative group (see 4.4.2 and 4.4.3). If the extension K_i of the field K_{i-1} is obtained by adjoining all the roots of an algebraic equation, then the quotient group G_{i-1}/G_i is finite. If this algebraic equation is of degree $\leqslant k$, then one can insert a chain of normal subgroups $G_i = G_{i1} \supset \cdots \supset G_{ip} = G_{i-1}$

between the groups G_i and G_{i-1}, $G_i \supset G_{i-1}$, such that the profundity of the group G_{ij} in the group $G_{i,j-1}$ is at most k (see 3.4.2). This completes the proof of the theorem.

The previous theorem can be formulated as follows.

If a Picard–Vessiot extension is a Liouville extension, a Liouville k-extension, or a generalized Liouville extension, then the Galois group of this extension is solvable, k-solvable, or almost solvable, respectively, in the category of algebraic groups.

In this reformulation the theorem becomes applicable to algebraic equations over differential fields. It gives stronger results about the unsolvability of algebraic equations.

Theorem 4.14. *If the Galois group of an algebraic equation over a differential field K is not solvable, then this algebraic equation is unsolvable not only by radicals but also by quadratures. If the Galois group is not k-solvable, then the algebraic equation is unsolvable by k-quadratures over K.*

4.6. Algebraic matrix groups and necessary solvability conditions. The Galois group of a linear differential equation is an algebraic matrix group. These groups have general properties that help to reformulate the solvability, k-solvability, and almost solvability conditions for a Galois group and to prove that these conditions are sufficient (see 4.7) for the solvability of the equation.

We note first that *every algebraic matrix group is a Lie group.* Indeed, the set of singular points of every algebraic variety is of codimension $\geqslant 1$. However, any point of a group can be taken to any other point by a group transformation. Therefore, the group looks the same near each point of the group, and hence the set of singular points of every algebraic group is empty. *The connected component of the identity of an algebraic group is a normal subgroup of finite index in this group.* Indeed, the connected component (of the identity) is a normal subgroup in any Lie group, and every algebraic variety has only finitely many connected components.

In what follows, the crucial role is played by the following famous theorem of Lie, which we present without proof.

Theorem 4.15 (Lie's theorem). *Any connected solvable matrix Lie group can be reduced in some basis to triangular form.*

Proposition 4.16. *An algebraic matrix group is an almost solvable group in the category of algebraic groups if and only if all the matrices in its connected component can be simultaneously reduced in some basis to triangular form.*

Proof. Every group consisting of triangular matrices is solvable. This proves the proposition in one direction. Let $G = G_0 \supset \cdots \supset G_n = e$ be a normal tower of algebraic subgroups of G such that every quotient group G_i/G_{i-1} is either commutative or finite. Consider the connected components of these groups. They form a normal tower $G^0 = G_0^0 \supset \cdots \supset G_n^0 = e$ of algebraic subgroups of the connected component G^0 of the identity of G. Moreover, if the quotient group G_{i-1}/G_i is commutative, then so is the quotient group G_{i-1}^0/G_i^0. If the quotient group G_{i-1}/G_i is finite, then the groups G_{i-1}^0 and G_i^0 coincide. This proves the proposition.

Proposition 4.17. *An algebraic matrix group G is solvable or k-solvable in the category of algebraic groups if and only if all the matrices in the connected component G^0 of the identity in G can be reduced to triangular form in some basis and the finite quotient group G/G_0 is solvable or k-solvable, respectively.*

Proof. According to Proposition 4.16, the group G^0 is triangular. Moreover, G^0 is a normal subgroup of finite index in G. The finite quotient group G/G_0 is solvable or k-solvable, respectively. In the converse direction the proposition is obvious.

Matrix groups admit the remarkable Zariski topology that assigns to every group $\Gamma \subset GL(V)$ the algebraic closure $\overline{\Gamma}$ of Γ. This operation enables one to generalize Propositions 4.16 and 4.17 to arbitrary matrix groups.

Proposition 4.18. 1) *A matrix group G is an almost solvable group if and only if it admits a triangular normal subgroup H of finite index. A matrix group is k-solvable or solvable if and only if the finite quotient group G/H of G by some triangular normal subgroup H of finite index is k-solvable or solvable, respectively.*

2) *An algebraic matrix group G is an almost solvable group, a k-solvable group, or a solvable group in the category of algebraic groups if and only if it is an almost solvable group, a k-solvable group, or a solvable group, respectively.*

Proof. Let $G = G_0 \supset \cdots \supset G_n = e$ be a normal tower of the group G. In this case the closures of the groups in this tower in the Zariski topology form a normal tower for the algebraic group $\overline{G} = \overline{G}_0 \supset \cdots \supset \overline{G}_n = e$. Moreover, if G_{i-1}/G_i is commutative or finite or if G_i is of profundity $\leqslant k$ in G_{i-1}, then $\overline{G}_{i-1}/\overline{G}_i$ is commutative or finite or $\overline{G}_i$ is of profundity $\leqslant k$ in $\overline{G}_{i-1}$, respectively. This proves all the assertions of the proposition in one direction. In the other direction, all the assertions are obvious.

4.7. Sufficient condition for the solvability of differential equations. An automorphism group Γ of a differential field F with the differential field K of fixed elements is said to be an *admissible automorphism group* if there is a finite-dimensional space V over the field of constants such that G is Γ-invariant and $K\langle V\rangle = F$. According to the Picard–Vessiot theory (see Corollary 4.5), the differential field F is a Picard–Vessiot extension of the differential field K if and only if there is an admissible automorphism group of F with the differential field K of fixed elements. In the general case the existence of an admissible transformation group for a Picard–Vessiot extension is by no means evident and is a part of the main theorem of this theory. However, for a large class of cases the existence of an admissible automorphism group is known *a priori*. For example, such a group exists for any extension of the field of rational functions by all the solutions of some Fuchsian linear differential equation (see 6.1.1). In these cases the monodromy group of the equation plays the role of the group Γ.

If the group Γ is solvable, then the elements of the field F can be represented by quadratures in terms of elements of the field K. In essence, the construction of such a representation relates to linear algebra and makes no use of the main theorems of the Picard–Vessiot theory. The admissible automorphism group Γ is isomorphic to the induced group of linear transformations of the space V, and thus Γ can be regarded as a matrix group.

Lemma 4.19 (Liouville). *If all the transformations in an admissible group Γ can be reduced to triangular form in some basis, then the differential field F is a Liouville extension of the differential field K.*

Proof. Let $e_1, \dots, e_n$ be a basis of V in which every transformation $\mu \in \Gamma$ is of the form $\mu(e_i) = \sum_{j \leqslant i} a_{ij} e_j$. Consider the vector space $\widetilde{V}$ spanned by the vectors $\widetilde{e}_i = \left(\dfrac{e_i}{e_1}\right)'$, $i = 2, \dots, n$. The space $\widetilde{V}$ is Γ-invariant, and every transformation μ in the group Γ has a triangular form in the basis $\widetilde{e}_i$. Indeed,

$$\mu(\widetilde{e}_i) = \mu\left(\left[\frac{e_i}{e_1}\right]'\right) = \left(\frac{a_{i1}}{a_{11}} + \sum_{2 \leqslant j \leqslant i} \frac{a_{ij}}{a_{11}} \frac{e_j}{e_1}\right)' = \sum_{2 \leqslant j \leqslant i} \frac{a_{ij}}{a_{11}} \widetilde{e}_j.$$

The dimension of $\widetilde{V}$ is less than that of V, and therefore one can assume that the differential field $K\langle \widetilde{V} \rangle$ is a Liouville extension of the differential field K. For any $\mu \in \Gamma$ one has $\mu\left(\dfrac{e_1'}{e_1}\right) = \dfrac{a_{11} e_1'}{a_{11} e_1} = \dfrac{e_1'}{e_1}$, and hence the element $\dfrac{e_1'}{e_1} = a$ belongs to the differential field of invariants, that is, to K. The differential field F is obtained from K by adjoining the element e_1 (which is the exponential of an integral of a) and the elements $\dfrac{e_i}{e_1}$ (which are integrals of the elements $\widetilde{e}_i$) for $i = 2, \dots, n$.

Proposition 4.20. *If a group Γ of admissible automorphisms of the field F with the field K of fixed elements is almost solvable, then there is a Γ-invariant field K_0 such that* 1) *F is a Liouville extension of K_0,* 2) *the induced automorphism group of the field K_0 is finite, and every element of K_0 is algebraic over K,* 3) *if the group Γ is solvable, then every element of K_0 is representable by radicals over the field K.*

Proof. Let V be a Γ-invariant subspace such that $K\langle V \rangle = F$.

It follows from Proposition 4.16 that the group Γ has a finite-index normal subgroup Γ_0 that can be reduced to a triangular form in some basis of the space V. Let K_0 be the differential field of invariants of Γ. By Lemma 4.19, the differential field F is a Liouville extension of K_0.

Obviously (see Proposition 3.9), the field K_0 is invariant under the action of Γ, and the induced group $\widetilde{\Gamma}_0$ of automorphisms of this field is a finite quotient group of Γ. Therefore, every element of K_0 is algebraic over K (see Lemma 3.17). If the original group Γ is solvable, then so is the finite quotient group $\widetilde{\Gamma}_0$ of Γ. In this case every element of K_0 can be expressed by radicals in terms of elements of K (see 3.3.1).

The proof of the following proposition uses Galois theory.

Proposition 4.21. *Under the assumptions of Proposition* 4.20 *if the group Γ is k-solvable, then every element of the field K_0 can be expressed in terms of elements of the field K by means of radicals and solutions of algebraic equations of degree at most k.*

Proof. Since the group $\widetilde{\Gamma}_0$ is finite, it follows that the extension K_0 of K is a Galois extension of K. If the group Γ_0 is k-solvable, then every finite quotient group of Γ_0 is also k-solvable. Proposition 4.21 follows now from Theorem 3.16.

We now complete the proof of the Picard–Vessiot theorem (see 4.5).

By the main Theorem 4.4, for any linear differential equation over a differential field K the Galois group of this equation leaves fixed only the elements of K. Therefore, Propositions 4.20 and 4.21 proved above can be applied here, and this proves the sufficiency of the conditions on the Galois group in the Picard–Vessiot theorem.

The Picard–Vessiot theorem not only proves the criterion of Liouville and Mordukhai-Boltovskii (see 2.3.2) but also enables one to generalize it to the case of solvability by quadratures and by k-quadratures. Namely, the following assertions hold.

A linear differential equation of order n is solvable by generalized quadratures over a differential field K if and only if, first, it admits a solution y_1 satisfying an equation of the form $y_1' = ay_1$, where a is an element belonging to some algebraic extension K_1 of K and, second, the differential equation of order $(n-1)$ for $z = y' - ay$ with coefficients in K_1 that is obtained from the original equation by the procedure of reducing the order (see 4.1.2) is solvable by generalized quadratures. Similar assertions hold for the solvability of a linear differential equation by quadratures and by k-quadratures. For solvability by quadratures (by k-quadratures) one must assume in addition that the algebraic extension K_1 can be obtained from K by adjoining radicals (by adjoining radicals and roots of algebraic equations of degrees $\leqslant k$, respectively). To prove these assertions, it suffices to look at the construction of solutions of differential equations.

Differential algebra enables one to refine substantially this criterion. *For linear differential equations whose coefficients are rational functions with rational coefficients there is a finite algorithm that enables us to determine whether a given equation is solvable by generalized quadratures, and to find a solution if one exists* [37]. The algorithm uses: 1) a bound for the degree of the extension K_1 of the field K, depending only on the order of the equation and following from general considerations of group theory (see 6.2.2); 2) the theory of normal forms of linear differential equations in a neighbourhood of a singular point; 3) the elimination theory for differential equations and inequalities with several functions (found by Seidenberg and generalizing the Tarski–Seidenberg theorem to the case of differential fields).

4.8. Other forms of solvability. Kolchin completed the Picard–Vessiot theorem [26]. He considered problems concerning the solvability of linear equations by integrals and by exponentials of integrals separately, and he studied versions of these problems in which algebraic extensions are admitted.

When defining the Liouville extensions, we used three forms of extensions: algebraic extensions, adjoining an integral, and adjoining the exponential of an integral. One can define more specific forms of solvability using as 'building blocks' only some of these extensions (and using only special algebraic extensions). We list the main versions.

1) Solvability by integrals.
2) Solvability by integrals and radicals.
3) Solvability by integrals and algebraic functions.
4) Solvability by exponentials of integrals.
5) Solvability by exponentials of integrals and algebraic functions.

We decipher the third of these definitions.

Let us consider an arbitrary chain of differential fields $K = K_0 \subseteq \cdots \subseteq K_n$ in which every field K_i, $i = 1, \ldots, n$, either is obtained from the previous field K_{i-1} by adjoining an integral over K_{i-1} or is an algebraic extension of K_{i-1}. By definition, every element of K_n is said to be *representable by integrals and algebraic functions* over the field K. An equation is *solvable over K by integrals and algebraic functions* if each of its solutions can be represented by integrals and algebraic functions.

The other forms of solvability in 1)–5) can be deciphered in a similar way.

Remarks. 1) There is no need to consider solvability by radicals and exponentials of integrals separately, because every radical is the exponential of an integral.

2) We have treated the above special algebraic extensions obtained by adjoining the roots of algebraic equations of degree at most k. One could define, say, k-solvability by integrals by combining algebraic extensions of this kind with extensions by adjoining integrals. We do not deal with this case so as not to overload the text and also because there are no interesting examples.

Definition 1. We say that a matrix group G is a *special triangular group* if there is a basis in which all the matrices of G are simultaneously reduced to triangular form and all the eigenvalues of each of the matrices in G are equal to 1.

Definition 2. We say that a matrix group is *diagonal* if there is a basis in which all the matrices of the group are diagonal.

Theorem 4.22 (Kolchin's theorem on the solvability by integrals). *A linear differential equation over a differential field K is solvable by integrals* (*by integrals and radicals*, *by integrals and algebraic functions*, *respectively*) *if and only if the Galois group of the equation over K is a special triangular group* (*is solvable and contains a special triangular normal subgroup of finite index*, *contains a special triangular normal subgroup of finite index*, *respectively*).

Theorem 4.23 (Kolchin's theorem on the solvability by exponentials of integrals). *A linear differential equation over a differential field K is solvable by exponentials of integrals* (*by exponentials of integrals and algebraic functions*, *respectively*) *if and only if the Galois group over K of this equation is solvable and contains a diagonal normal subgroup of finite index* (*contains a diagonal normal subgroup of finite index*, *respectively*).

A few words about the proofs of these theorems. The Galois group of an extension by adjoining an integral is anticompact (see 4.4.2). The Galois group of an extension by adjoining the exponential of an integral is quasi-compact (see 4.4.3). Kolchin developed a theory of anticompact and quasi-compact algebraic matrix groups. We present a rather simple proposition of this theory.

Proposition 4.24 [26]. 1) *An algebraic matrix group is quasi-compact if and only if every matrix of the group can be reduced to diagonal form.* 2) *An algebraic matrix group is anticompact if and only if all the eigenvalues of any matrix in the group are equal to* 1.

The theory of quasi-compact and anticompact groups together with the main theorem of the Picard–Vessiot theory enabled Kolchin to prove his theorems on solvability by integrals and solvability by exponentials of integrals.

Of course, Kolchin's theorems, as well as the Picard–Vessiot theorem, hold not only for linear differential equations but also for Picard–Vessiot extensions (each of these extensions is generated by the solutions of a linear differential equation). Let us formulate a criterion for diverse forms of representability of all elements of a Picard–Vessiot extension having a triangular Galois group. The criterion readily follows from Kolchin's theorems and the Picard–Vessiot theorem. We shall apply this criterion below in 6.2.3 when discussing diverse forms of solvability for systems of Fuchsian equations with small coefficients.

Extension with a triangular Galois group (cf. [26]). *Let a Picard–Vessiot extension F of a differential field K have a triangular Galois group. Then every element of the field F is*:

1) *representable by quadratures over the field K*;
2) *representable by integrals and algebraic functions or by integrals and radicals*[1] *over K if and only if the eigenvalues of all the matrices in the Galois group are roots of unity*;
3) *representable by integrals over K if and only if all the eigenvalues of all the matrices in the Galois group are equal to* 1;
4) *representable by exponentials of integrals and algebraic functions or by exponentials of integrals*[1] *over K if and only if the Galois group is diagonal*;
5) *representable by algebraic functions or by radicals*[1] *over K if and only if the Galois group is diagonal and all the eigenvalues of all the matrices in it are roots of unity*;
6) *an element of K if and only if the Galois group is trivial.*

§ 5. One-dimensional topological version of Galois theory

5.1. Preliminary remarks. In 5.1.1 we present the Galois theory for fields of meromorphic functions on algebraic curves, which has a transparent geometric interpretation and is closely related to the one-dimensional topological version of Galois theory. In 5.1.2 we discuss the topological non-representability of functions by radicals and the topological non-elementarity of elliptic functions, both proved by V. I. Arnol'd. In 5.1.3 we discuss the idea of the topological version of Galois theory and complications in the realization of this idea.

5.1.1. *Galois theory of fields of meromorphic functions on algebraic curves.* From the algebraic point of view, we speak in this subsection of fields that are extensions of transcendence degree 1 of the field $\mathbb{C}$ of complex numbers and are finitely generated over $\mathbb{C}$. The Galois theory for these fields has a simple geometric meaning.

First of all, such a field is isomorphic to the field P_M of meromorphic functions on some connected compact Riemann surface M defined up to an analytic diffeomorphism. The simplest example of a field of this kind is given by the field of rational functions of a single complex variable, that is, the field of meromorphic functions on the Riemann sphere.

Corresponding to a homomorphism $\tau\colon P_{M_1} \to P_{M_2}$ between such fields extending the identity map between the subfields of complex numbers is a regular map $\rho\colon M_2 \to M_1$ of the Riemann surfaces such that $\rho^* f = \tau(f)$, where f and $\tau(f)$ are

[1] These forms of solvability differ if one omits the condition that the Galois group be triangular.

meromorphic functions on M_1 and M_2, respectively. If the map ρ is non-constant, then the image $\tau(P_{M_1}) = \rho^*(P_{M_1})$ of the field P_{M_1} is isomorphic to the field P_{M_1}, and P_{M_2} is a finite algebraic extension of the subfield $\tau(P_{M_1}) = \rho^*(P_{M_1})$.

A non-constant analytic map $\rho\colon M_2 \to M_1$ of a connected compact Riemann surface M_2 to a connected compact Riemann surface M_1 determines a finite ramified covering over the surface M_1. Ramified coverings $\rho_1\colon M_2 \to M_1$ and $\rho_2\colon M_3 \to M_1$ determine isomorphic extensions of the field P_{M_1} if and only if they are isomorphic, that is, there is an invertible analytic map $\rho\colon M_2 \to M_3$ commuting with the projections: $\rho_1 = \rho_2 \circ \rho$. Thus, the theory of finite algebraic extensions of the fields of this type is equivalent to the theory of finite ramified coverings over compact Riemann surfaces. In particular, the theory of finite algebraic extensions of the field of meromorphic functions is equivalent to the theory of finite-sheeted ramified coverings over the Riemann sphere.

We now go into the details concerning the above facts and the related geometry. Every finite algebraic extension of any field of characteristic zero is generated over this field by a single element y satisfying some irreducible algebraic equation over the original field. Let an extension of the field P_M be generated by an element y satisfying an irreducible equation

$$y^n + r_1 y^{n-1} + \cdots + r_n = 0 \tag{10}$$

in which all the coefficients r_i are meromorphic functions on M. There are n analytic germs $y_{1a}, \ldots, y_{na}$ satisfying (10) defined in a small neighbourhood of a point a. The equation (10) is irreducible if and only if each of these germs y_{ia} can be obtained from any other germ y_{ja} by analytic continuation along some curve belonging to the surface M (see [14]). Let us consider the Riemann surface M_i of the germ y_{ia} over the surface M, $\rho_i\colon M_i \to M$. The surface M_i is a connected compact manifold. The field of meromorphic functions on M_i is generated over the field $\rho_i^* P_M$ by an element y_i (see [14]). The irreducibility of the equation also means that the ramified coverings $\rho_i\colon M_i \to M$ and $\rho_j\colon M_j \to M$ corresponding to the Riemann surfaces of different solutions y_{ia} and y_{ja} of the equation (10) are isomorphic when regarded as coverings. Thus, *to every finite algebraic extension of the field P_M given up to isomorphism we have assigned an equivalence class of finite ramified coverings over M.*

The construction of the inverse map assigning to every finite ramified covering $\rho\colon M_1 \to M$ over M a finite extension of the field M is based on the Riemann existence theorem. According to this theorem, on every one-dimensional complex manifold and for any finite set of points on this manifold there is a meromorphic function taking distinct values at the points of the set. Let us consider a meromorphic function on M_1 taking pairwise distinct values at the distinct pre-images of some regular value $a \in M$ of the map ρ. A function y having this property is a multi valued algebraic function on M, and it generates the entire field of meromorphic functions on M_1 over the subfield $\rho^*(P_M)$.

We proceed to a geometric description of the ramified coverings over a compact Riemann surface M. To define such a covering, it suffices to choose a finite set $A \subset M$ and a finite-index subgroup F of the fundamental group $\pi_1(M \setminus A)$ of the

complement of A. A ramified covering over M is constructed from these data as follows. From the subgroup F we first construct a covering over the set $M \setminus A$ such that the image of the fundamental group of this covering under the projection onto $M \setminus A$ coincides with F (see, for instance, [12]). The number of pre-images of any point in $M \setminus A$ under this covering coincides with the index of the subgroup F in the group $\pi_1(M \setminus A)$. The covering thus obtained can be uniquely compactified by adding some points lying over the set A (the set of points added over a point $a \in A$ corresponds to the set of the cycles in the permutation of sheets of the covering that corresponds to a loop around a).

Two ramified coverings constructed from sets $A_1 \subset M$ and $A_2 \subset M$ and from groups $F_1 \subset \pi_1(M \setminus A_1)$ and $F_2 \subset \pi_1(M \setminus A_2)$ are isomorphic if and only if for a finite set B containing the sets A_1 and A_2 the subgroups $\widetilde{F}_1$ and $\widetilde{F}_2$ of the group $\pi_1(M \setminus B)$ are conjugate in this group, where $\widetilde{F}_1$ and $\widetilde{F}_2$ are the pre-images of the groups F_1 and F_2 under the group homomorphisms of $\pi_1(M \setminus B)$ into $\pi_1(M \setminus A_1)$ and $\pi_1(M \setminus A_2)$ induced by the natural embeddings. It is easy to see that the above condition does not depend on the choice of a finite set B containing A_1 and A_2.

A ramified covering $\rho\colon M_1 \to M$ corresponds to a Galois extension of the field P_M if and only if the finite-index subgroup H of $\pi_1(M \setminus A)$ determining this covering is a normal subgroup of $\pi_1(M \setminus A)$ (here A stands for an arbitrary finite set containing all the critical values of the map ρ; the above condition does not depend on the specific choice of the set A). *The Galois group of this Galois extension coincides with the quotient group $\pi_1(M \setminus A)/H$, which is isomorphic to the group of one-to-one transformations of the surface M_1 into itself that commute with the projection ρ.*

Corresponding to an intermediate extension of the field P_M is an intermediate ramified covering, that is, a covering $\rho_2\colon M_2 \to M$ such that there is a map $\rho_1\colon M_1 \to M_2$ for which $\rho_2 \circ \rho_1 = \rho$. An intermediate covering corresponds to an intermediate subgroup F of $\pi_1(M \setminus A)$, that is, to a subgroup F such that $H \subseteq F$.

An intermediate field is a Galois extension if and only if F is a normal subgroup of $\pi_1(M \setminus A)$. The Galois group of an intermediate Galois extension is a quotient group of the Galois group of the original extension, because the quotient group $\pi_1(M \setminus A)/H$ maps naturally onto the quotient group $\pi_1(M \setminus A)/F$.

We have presented above a geometric interpretation of the main theorem of the Galois theory for fields of meromorphic functions on algebraic curves. It remains to describe geometrically the behaviour of the Galois group of an algebraic equation under an extension of the ground field. Thus, let $\rho_1\colon M_1 \to M$ be a ramified covering corresponding to a Galois extension of the field P_M, and let $\rho_2\colon M_2 \to M$ be another covering corresponding to another Galois extension of the same field P_M. Let B be an arbitrary finite set on M that contains the critical points of the maps ρ_1 and ρ_2 and let $G = \pi_1(M \setminus B)$ be the fundamental group of the complement of B. The coverings $\rho_1\colon M_1 \setminus B_1 \to M \setminus B$ and $\rho_2\colon M_2 \setminus B_2 \to M \setminus B$, where $B_1 = \rho_1^{-1}(B)$ and $B_2 = \rho_2^{-1}(B)$, correspond to normal subgroups H_1 and H_2 of G that are isomorphic to the fundamental groups of the manifolds $M_1 \setminus B_1$ and $M_2 \setminus B_2$, respectively. The projection $\rho_2\colon M_2 \setminus B_2 \to M \setminus B$ takes the manifold $M_2 \setminus B_2$ to the base of the covering $\rho_1\colon M_1 \setminus B_1 \to M \setminus B$. Using the map ρ_2, one induces the covering $\rho\colon U \to M_2 \setminus B_2$ over $M_2 \setminus B_2$ from the covering $\rho_1\colon M_1 \setminus B_1 \to S \setminus B$. The manifold U is not connected in general.

Each connected component $U_i \subset U$ determines a covering $\rho\colon U_i \to M_2 \setminus B_2$. One can readily see that the coverings connected with different components U_i are equivalent as coverings, and each of them corresponds to the normal subgroup $H_1 \cap H_2$ of the group H_2. Let us consider an arbitrary component $U_i = V$. The covering $\rho\colon V \to M_2 \setminus B_2$ admits a compactification $\rho\colon M_3 \to M_2$, where $V = M_3 \setminus B_3$ and $B_3 = \rho^{-1}(B_2)$, which corresponds to the original Galois extension over the field P_{M_2}. The Galois group of this covering is the quotient group $H_2/(H_1 \cap H_2)$. This very fact is stated in Theorem 3.4.

Thus, all assertions of the Galois theory for fields of meromorphic functions on curves have a transparent geometric explanation. Moreover, the *geometric construction of the ramified coverings together with the Riemann existence theorem give a complete description of all finite extensions of fields in the class under consideration*. For example, this solves instantly the inverse problem of Galois theory for these fields (that is, the problem of constructing a Galois extension with a given Galois group). We note that the inverse problem of Galois theory is still unsolved for the field of rational numbers.

5.1.2. *Topological non-representability of functions by radicals*. Before passing to the topological version of Galois theory, we dwell on another topological interpretation of the Galois group for an algebraic equation over the field of rational functions.

Let

$$y^n + r_1 y^{n-1} + \cdots + r_n = 0 \tag{11}$$

be an irreducible equation over the field P_S of rational functions ($r_i \in P_S$).

The following proposition is well known.

Proposition 5.1. *The Galois group of the equation* (11) *over the field of rational functions is isomorphic to the monodromy group of a* (*multivalued*) *algebraic function* y *defined by the equation* (11).

Proof. Let D be the discriminant of the equation (11). We denote by $[D]$ the set of zeros and poles of D. In a small connected neighbourhood U of a point $a \notin [D]$ on the Riemann sphere, n holomorphic solutions $y_{1a}, \ldots, y_{na}$ of (11) are defined. We denote by Q the field of meromorphic functions on U that is obtained by adjoining all these solutions to the field P_S. Let γ be a curve on the Riemann sphere that begins and ends at the point a and that is disjoint from the set $[D]$. Every solution $y_{1a}, \ldots, y_{na}$ of (11) has a regular continuation along γ, and therefore every element z of the field Q has a meromorphic continuation along γ. The map $z \to z(\gamma)$ assigning to an element z its meromorphic continuation along γ is obviously an automorphism of the field Q. This automorphism is uniquely determined by the permutation $y_{ia} \to y_{ia}(\gamma)$ of the elements $y_{1a}, \ldots, y_{na}$, it depends only on the class $[\gamma]$ of the curve γ in $\pi_1(S \setminus [D], a)$, and preserves (leaves fixed) all rational functions. Conversely, the elements of Q that remain fixed under all automorphisms $z \to z(\gamma)$ are single-valued algebraic functions, that is, are rational functions. Hence, the group of automorphisms of Q of the form $z \to z(\gamma)$ coincides with the Galois group of Q over the field P_S. On the other hand, this group is isomorphic to the group of permutations of the branches $y_{1a}, \ldots, y_{na}$ of the algebraic function y that correspond to the analytic continuations $y_{ia} \to y_{ia}(\gamma)$ along

the paths $\gamma \in \pi_1(S \setminus D, a)$, that is, it is isomorphic to the monodromy group of the function y. This completes the proof of the proposition.

Galois theory, together with the last proposition, gives us the following corollary.

Corollary 5.2. 1) *An algebraic function is representable by radicals if and only if its monodromy group is solvable.* 2) *An algebraic function is representable by k-radicals if and only if its monodromy group is k-solvable.*

V. I. Arnol'd proved the topological unsolvability of a series of classical problems [2]–[9]. We present a definition due to him.

Definition (Arnol'd). A map $f\colon X \to Y$ is said to be *topologically bad* (for example, a topologically non-elementary function) if among (left-right) topologically equivalent maps there are no good maps (for example, elementary maps).

To any multivalued analytic function f of a complex variable one can associate its Riemann surface M_f and the projection $\pi_f\colon M_f \to S^2$ of this surface onto the Riemann sphere S^2.

Corollary 5.3. *Let the projections π_f and π_g of the Riemann surfaces M_f and M_g of the functions f and g onto the Riemann sphere be topologically equivalent. In this case f and g are simultaneously representable or non-representable by radicals* (*by k-radicals*) (that is, the topological type of the projection of the Riemann surface of a function onto the Riemann sphere is responsible for the representability of the function by radicals and by k-radicals).

Proof. Corollary 5.3 follows immediately from Corollary 5.2. Indeed, the algebraicity of a function is related to the compactness of its Riemann surface, its representability by radicals is related to the solvability of its monodromy group, and its representability by k-radicals is related to the k-solvability of its monodromy group. All these properties are topological.

In the 1960s Arnol'd proved the topological non-representability by radicals for general algebraic functions (see Corollary 5.3) by using direct topological tools without employing Galois theory, and he gave a lecture course on this topic in Kolmogorov's boarding school. Alekseev significantly elaborated on this course and published the result as the book [1]. According to Arnol'd, a topological proof of the unsolvability of some problem implies new corollaries as a rule. For instance, it readily follows from the topological proof of non-representability by radicals of any function with unsolvable monodromy group that such a function cannot be represented by any formula including not only radicals but also arbitrary entire functions [19].

In the 1960s Arnol'd also found results about the topological non-elementarity of elliptic functions and integrals (and other closely related objects), but published nothing in this direction. In December 2003 he wrote me a letter on this subject. The following theorem, as well as the above definition, is taken from that letter.

Theorem 5.4 (Arnol'd). *If a meromorphic function $g\colon U \to \mathbb{C}P^1$ defined on a complex domain $U \subset \mathbb{C}$ is topologically equivalent to an elliptic function $f\colon \mathbb{C} \to \mathbb{C}P^1$, then g is an elliptic function* (*possibly with different periods than for f*).

Proof. An elliptic function f is invariant under a group of translations isomorphic to $\mathbb{Z}^2$ ($z \to z + k_1 w_1 + k_2 w_2$, $(k_1, k_2) \in \mathbb{Z}^2$). Therefore, the function g is invariant under a $\mathbb{Z}^2$-group of homeomorphisms of the domain U. Every homeomorphism h belonging to this group is in fact a biholomorphic map of the domain U into itself. Indeed, by the inverse function theorem it follows from the identity $g(z) \equiv g(h(z))$ that h is holomorphic in a neighbourhood of every point not belonging to the pre-image (under h) of the set of critical points of g. The map h is holomorphic at the points of this pre-image by the removable singularity theorem. By our assumption, the domain U is homeomorphic to $\mathbb{C}$. Hence, by the Riemann mapping theorem, U either coincides with $\mathbb{C}$ or is biholomorphically equivalent to the interior of the unit disc. The domain U coincides with $\mathbb{C}$, because the group of biholomorphic transformations of the unit disc contains no closed subgroup isomorphic to $\mathbb{Z}^2$. Every subgroup isomorphic to $\mathbb{Z}^2$ in the group of biholomorphic transformations of $\mathbb{C}$ that acts on $\mathbb{C}$ without fixed points is a group of translations (of the form $z \to k_1\tau_1 + k_2\tau_2$, $(k_1, k_2) \in \mathbb{Z}^2$). Therefore, g is an elliptic function.

As is well known, the elliptic functions are non-elementary[2]. This classical result and the theorem proved above imply that the elliptic functions are topologically non-elementary.

Below I quote from Arnol'd's letter.

"As far as I remember, these considerations proved the topological non-elementarity both of the elliptic functions f and the elliptic integrals f^{-1}, and of many other things. Moreover, all this can be generalized to curves of other genera (with other coverings, or at least with universal coverings). I have forgotten whether or not I proved these facts rigorously, but I think that I had grasped reasons for which the multidimensional assertions analogous to the above theorem must be *wrong*: as far as I remember, *preservation of the topological type in the multidimensional case does not ensure preservation of algebraicity.* This in itself is not an obstruction to a topological non-elementarity (badness), but it blocks my proof of it, the proof by reduction to non-elementary properties of classical (algebraic) objects like elliptic functions."

5.1.3. *On the one-dimensional topological version of Galois theory.* The monodromy group coincides with the Galois group for the class of algebraic functions and is responsible for the representability of a function by radicals (see 5.1.2). However, the monodromy group is defined not only for algebraic functions but also for the logarithm, arctangent, and many other functions for which the Galois group is not defined. It is natural to try to use the monodromy group for such functions

[2]The non-elementarity of the elliptic functions follows from Kolchin's generalization of the Picard–Vessiot theory [27]. This generalization can be applied not only to linear but also to some non-linear differential equations, for instance, to the equation for the Weierstraß $\wp$-function. The Galois group of the differential field of elliptic functions over the field of constants $\mathbb{C}$ obviously contains the quotient group $\mathbb{C}/\mathbb{Z}^2$ of the group of translations $f(z) \to f(z + a)$ by the subgroup $\mathbb{Z}^2$ of periods of elliptic functions. (One can readily show that the Galois group coincides with this group.) According to Kolchin, the fact that the elliptic functions cannot be represented by generalized quadratures follows from the non-existence of a normal tower of subgroups in the group $\mathbb{C}/\mathbb{Z}^2$ such that every quotient group with respect to this tower is a finite group, the additive group of complex numbers, or the multiplicative group of complex numbers.

(instead of the Galois group) to prove that some function does not belong to some classical class. This is the approach realized by the topological version of Galois theory [18]–[22].

We present an example that shows what complications must be overcome in this way.

Let us consider an elementary function f defined by the formula

$$f(z) = \log\left(\sum_{j=1}^{n} \lambda_j \log(z - a_j)\right),$$

where a_j, $j = 1, \dots, n$, are distinct points in the complex line and λ_j, $j = 1, \dots, n$, are complex constants. We denote by Λ the additive group of complex numbers generated by the constants $\lambda_1, \dots, \lambda_n$. It is clear that if $n > 2$, then the group Λ is dense in the complex line for almost every set of constants $\lambda_1, \dots, \lambda_n$.

Proposition 5.5. *If the group Λ is dense in the complex line, then the elementary function f has a dense set of logarithmic ramification points.*

Proof. Let g_a be one of the germs of the function g defined by the formula $g(z) = \sum_{j=1}^{n} \lambda_j \log(z - a_j)$ at a point $a \neq a_j$, $j = 1, \dots, n$. After going around the points $a_1, \dots, a_n$, the number $2\pi i\lambda$ is added to the germ g_a, where λ is an element of the group Λ. Conversely, every germ $g_a + 2\pi i\lambda$, where $\lambda \in \Lambda$, is obtained from the germ g_a by analytic continuation along some curve. Let U be a small neighbourhood of the point a and let $G\colon U \to C$ be an analytic function whose germ at a is equal to g_a. The image V of the domain U under the map $G\colon U \to \mathbb{C}$ is open. Therefore, the domain V contains a point of the form $2\pi i\lambda$, where $\lambda \in \Lambda$. The function $G - 2\pi i\lambda$ is one of the branches of the function g over the domain U, and the set of zeros of this branch in U is non-empty. Therefore, one of the branches of the function $f = \log g$ has a logarithmic ramification point in U.

One can readily see that under the assumptions of the proposition the monodromy group of the function f has the cardinality of the continuum (which is not surprising, because the fundamental group $\pi_1(S \setminus A)$, where A is a countable dense set on the Riemann sphere, obviously contains a continuum of elements).

One can also show that the image of the fundamental group $\pi_1(S^2 \setminus \{A \cup b\})$ (where $b \notin A$ is an arbitrary point in the complex line) in the group of permutations of the branches of the function f is a proper subgroup of the monodromy group of f. (The fact that the monodromy group can change when a single extra point is removed somewhat complicates all the proofs.)

Thus, already the simplest elementary functions can have a dense set of singular points and a monodromy group with the cardinality of the continuum.

In the topological version of Galois theory we regard functions representable by quadratures as multivalued analytic functions of a single complex variable. It turns out that there are topological restrictions on the covering of the complex line by the Riemann surface of a function representable by quadratures. If a function does not satisfy these conditions, then it cannot be expressed by quadratures.

Besides geometric clarity, this approach has the following advantage. The topological obstructions relate to the character of the multivaluedness of the function. These obstructions are preserved not only for functions representable by quadratures but also for a much wider class of functions. This wider class is obtained if one combines all meromorphic functions with the functions representable by quadratures and allows meromorphic functions in all formulae. For this reason, the topological results on non-representability by quadratures turn out to be stronger than the algebraic results. The point is that the composition of functions is not an algebraic operation. In differential algebra one can avoid the operation of composition of functions by considering a differential equation satisfied by the desired composition. However, for example, the Euler Γ-function satisfies no algebraic differential equation. Therefore, it is hopeless to seek an equation on the function $\Gamma(\exp x)$. All the known results on non-representability of functions by quadratures and, say, by the Euler Γ-function have been obtained only by using our approach.

On the other hand, when using this approach it is impossible to prove the non-representability by quadratures for any single-valued meromorphic function.

Using the differential Galois theory (to be more precise, the linear-algebraic part of the theory, which deals with algebraic matrix groups and their differential invariants), one can show that the only reason for the unsolvability by quadratures of a Fuchsian linear differential equation is topological (cf. § 6). In other words, if there are no topological obstructions to the solvability by quadratures for a Fuchsian differential equation, then it is solvable by quadratures.

We list the possible topological obstructions to the representability of functions by quadratures, by generalized quadratures, and by k-quadratures.

First, the functions representable by generalized quadratures and, in particular, the functions representable by quadratures and by k-quadratures can have at most countably many singular points in the complex line (see 5.2). (However, the set of singular points can be dense even for the simplest functions representable by quadratures.)

Second, the monodromy group of a function representable by quadratures must be solvable (see 5.5.2). (However, the monodromy group can contain a continuum of elements even for the simplest functions representable by quadratures.)

Similar restrictions on the covering of the Riemann sphere by the Riemann surface exist for functions representable by generalized quadratures and by k-quadratures. However, the formulation of these conditions is more complicated. Under these conditions the monodromy group is regarded as a group of permutations of the set of branches of the function rather than an abstract group. In other words, the conditions involve not just the monodromy group but the *monodromy pair* of the function under consideration, the pair consisting of the monodromy group of the function and the stabilizer of some germ (see 5.3.3).

We proceed to a detailed description of this geometric approach to the solvability problem.

5.2. Functions whose singular sets are at most countable. In this subsection we introduce a vast class of functions of a single complex variable, a class needed for the construction of the topological version of Galois theory.

5.2.1. *Forbidden sets.* We introduce a class of functions in which the subsequent arguments will be carried out. A multivalued analytic function of a single complex variable is called an $\mathcal{S}$-*function* if the set of singular points of f is at most countable. Let us refine this definition.

Two regular germs f_a and g_b given at points a and b of the Riemann sphere S^2 are said to be *equivalent* if the germ g_b can be obtained from the germ f_a by a regular continuation along some curve. Every germ g_b that is equivalent to the germ f_a is also called a *regular germ of the multivalued analytic function f generated by the germ f_a*.

A point $b \in S^2$ is said to be *singular* for the germ f_a if there is a curve $\gamma\colon [0,1] \to S^2$ with $\gamma(0) = a$ and $\gamma(1) = b$ such that the germ has no regular continuation along this curve, but for any t with $0 \leqslant t < 1$ the germ admits a regular continuation along the shortened curve $\gamma\colon [0,t] \to S^2$. One can readily see that the sets of singular points of equivalent germs coincide.

A regular germ is called an $\mathcal{S}$-*germ* if the set of its singular points is at most countable. A multivalued analytic function is called an $\mathcal{S}$-*function* if each of its regular germs is an $\mathcal{S}$-germ.

In what follows we need a lemma according to which a curve in the plane can be moved away from a countable set by using a small deformation.

Lemma 5.6 (on releasing a curve from a countable set). *Let A be an at most countable set in the plane $\mathbb{C}$, let $\gamma\colon [0,1] \to \mathbb{C}$ be a curve, and let φ be a continuous positive function on the interval $0 < t < 1$. Then there is a curve $\widehat{\gamma}\colon [0,1] \to \mathbb{C}$ such that $\widehat{\gamma}(t) \notin A$ and $|\gamma(t) - \widehat{\gamma}(t)| < \varphi(t)$ for any $0 < t < 1$.*

The 'scientific' proof of the lemma is as follows. In the function space of curves $\overline{\gamma}$ that are close to the curve γ, $|\gamma(t) - \overline{\gamma}(t)| < \varphi(t)$, the curves not containing one of the points of the set A form an open dense set. The intersection of countably many open dense sets in such function spaces is non-empty.

We present an elementary proof of the lemma (it can be extended, almost literally, to a more general case in which the set A is uncountable but has Hausdorff length zero; cf. 5.5.3). Let us first construct a broken line $\overline{\gamma}$ with infinitely many links and with vertices not belonging to A and such that $|\gamma(t) - \overline{\gamma}(t)| < \frac{1}{2}\varphi(t)$. A broken line of this kind can be constructed, because the complement of the set A is dense. We show how to modify each link $[p,q]$ of the broken line $\overline{\gamma}$ in such a way that the new link becomes disjoint from the set A. Consider the segment $[p,q]$. Let m be the perpendicular to the segment at its middle point. We introduce the two-linked broken lines $[p,b]$, $[b,q]$ with $b \in m$ and b sufficiently close to the segment. These broken lines intersect only at the endpoints p and q, and there are a continuum of such broken lines. Thus, among them there is a broken line that is disjoint from the set A. Modifying in this way each link of the broken line with infinitely many links, we obtain a desired curve.

Along with the set of singular points, it is also convenient to consider other sets outside which the function admits unrestricted analytic continuation. An at most countable set A is said to be a *forbidden set* for a regular germ f_a if f_a has a regular continuation along any curve $\gamma(t)$ with $\gamma(0) = a$ that can intersect the set A only at the initial moment.

Theorem 5.7 (on a forbidden set). *An at most countable set is forbidden for a germ if and only if it contains the set of singular points of the germ. In particular, a germ has a forbidden set if and only if this is a germ of an $\mathcal{S}$-function.*

Proof. Suppose that there is a singular point b of a germ f_a that does not belong to some forbidden set A of the germ. By definition, there must be a curve $\gamma\colon [0,1] \to S^2$ with $\gamma(0) = a$ and $\gamma(1) = b$ along which there is no regular continuation of f_a, but the germ has a regular continuation along the curve up to any point with $t < 1$. Without loss of generality one can assume that the points a and b and the curve $\gamma(t)$ belong to the finite part of the Riemann sphere, that is, $\gamma(t) \neq \infty$ for $0 \leqslant t \leqslant 1$. We denote by $R(t)$ the radius of convergence of the series $f_{\gamma(t)}$ obtained by continuing the germ f_a along the curve $\gamma(t)$. The function $R(t)$ is continuous on the half-interval $[0,1)$. According to Lemma 5.6, there is a curve $\widehat{\gamma}(t)$ with $\widehat{\gamma}(0) = a$ and $\widehat{\gamma}(1) = b$ such that $|\gamma(t) - \widehat{\gamma}(t)| < \frac{1}{3}R(t)$ and $\widehat{\gamma}(t) \notin A$ for $t > 0$. By the assumption, the germ f_a can be continued along the curve $\widehat{\gamma}$ up to the point 1. But this would readily imply that f_a can be continued along the curve γ. The contradiction shows that the set of singular points of f_a is contained in any forbidden set of this germ. The converse assertion (a countable set containing the set of singular points of a germ is forbidden for the germ) is obvious.

5.2.2. *Closedness of the class of $\mathcal{S}$-functions.* Let us prove that the function class introduced above is closed with respect to all the natural operations.

Theorem 5.8 (on the closedness of the class of $\mathcal{S}$-functions). *The class $\mathcal{S}$ of all $\mathcal{S}$-functions is closed under the following operations*:

1) *differentiation, that is, if $f \in \mathcal{S}$, then $f' \in \mathcal{S}$;*
2) *integration, that is, if $f \in \mathcal{S}$ and $g' = f$, then $g \in \mathcal{S}$;*
3) *composition, that is, if $g, f \in \mathcal{S}$, then $g \circ f \in \mathcal{S}$;*
4) *meromorphic operations, that is, if $f_i \in \mathcal{S}$, $i = 1, \dots, n$, $F(x_1, \dots, x_n)$ is a meromorphic function of n variables, and $f = F(f_1, \dots, f_n)$, then $f \in \mathcal{S}$;*
5) *solution of algebraic equations, that is, if $f_i \in \mathcal{S}$, $i = 1, \dots, n$, and $f^n + f_1 f^{n-1} + \dots + f_n = 0$, then $f \in \mathcal{S}$;*
6) *solution of linear differential equations, that is, if $f_i \in \mathcal{S}$, $i = 1, \dots, n$, and $f^{(n)} + f_1 f^{(n-1)} + \dots + f_n = 0$, then $f \in \mathcal{S}$.*

Proof. 1)–2). Let f_a, $a \neq \infty$, be a germ of an $\mathcal{S}$-function and let A be the set of singular points of f_a. If the germ f_a has a regular continuation along some curve γ belonging to the finite part of the Riemann sphere, then the integral and the derivative of this germ have regular continuations along the curve γ as well. Therefore, it suffices to take the set $A \cup \{\infty\}$ as a forbidden set for an integral and for the derivative of the germ f_a.

3) Let f_a and g_b be germs of $\mathcal{S}$-functions, let A and B be the sets of singular points of f_a and g_b, respectively, and let $f_a(a) = b$. We denote by $f^{-1}(B)$ the full pre-image of the set B under the multivalued correspondence generated by the germ f_a. In other words, $x \in f^{-1}(B)$ if and only if there is a germ ψ_x equivalent to the germ f_a and such that $\psi(x) \in B$. The set $f^{-1}(B)$ is at most countable. It suffices to take the set $A \cup f^{-1}(B)$ as a forbidden set of the germ $g_b \circ f_a$.

4) Let the germs f_{ia} be germs of $\mathcal{S}$-functions, let A_i be the set of singular points of f_{ia}, and let F be a meromorphic function of n variables. We assume that the germs f_{ia} and the function F are such that the germ $f_a = F(f_{1a}, \dots, f_{na})$ is a well-defined meromorphic germ. Replacing the point a by a nearby point if necessary, one can assume that f_a is regular. If a curve $\gamma(t)$ is disjoint from the set $A = \bigcup A_i$ for $t > 0$, then f_a can be meromorphically continued along this curve. Let B be the projection to the Riemann sphere of the set of poles of the function f generated by the germ f_a. It suffices to take the set $A \cup B$ as a forbidden set of the germ.

5) Let the germs f_{ia} be germs of $\mathcal{S}$-functions, let A_i be the set of singular points of f_{ia}, and let f_a be a regular germ satisfying the equality

$$f_a^n + f_{1a} f_a^{n-1} + \dots + f_{na} = 0.$$

If a curve $\gamma(t)$ is disjoint from the set $A = \bigcup A_i$ for $t > 0$, then there is a continuation of the germ f_a along this curve that contains, generally, meromorphic and algebraic elements. Let B be the projection to the Riemann sphere S^2 of the set of poles of f and ramification points of the Riemann surface of f. It suffices to take the set $A \cup B$ as a forbidden set of the germ f_a.

6) If the coefficients of an equation

$$f_a^{(n)} + f_{1a} f_a^{(n-1)} + \dots + f_{na} = 0$$

have regular continuations along some curve γ belonging to the finite part of the Riemann sphere, then every solution f_a of this equation also has a regular continuation along the curve γ. Therefore, it suffices to take the set $A = \bigcup A_i \cup \{\infty\}$, where A_i is the set of singular points of the germ f_{a_i}, as a forbidden set of f_a.

Remark. The arithmetic operations and exponentiation are examples of meromorphic operations, and therefore the *class of $\mathcal{S}$-functions is closed under the arithmetic operations and the exponentiation.*

Corollary 5.9. *If a multivalued function f can be constructed from single-valued $\mathcal{S}$-functions by integration, differentiation, meromorphic operations, compositions, and solutions of algebraic equations and linear differential equations, then f has at most countably many singular points. In particular, any function having uncountably many singular points cannot be represented by generalized quadratures.*

5.3. Monodromy group. In this subsection we discuss diverse notions related to the monodromy group.

5.3.1. *Monodromy group with a forbidden set.* The monodromy group of an $\mathcal{S}$-function f with a forbidden set A is the group of all those permutations of branches of the function f that occur upon going around the points of the set A. We now give an exact definition.

Let F_a be the set of all germs of an $\mathcal{S}$-function f at some point a that does not belong to some forbidden set A. We take a closed curve γ in $S^2 \setminus A$ that begins at the point a. The continuation of every germ in the set F_a along the curve γ leads to a germ in F_a.

Thus, corresponding to every curve γ is a map of F_a into itself, this map is the same for homotopy equivalent curves in $S^2 \setminus A$, and corresponding to a product of curves is a product of maps. A homomorphism τ of the fundamental group of the

set $S^2 \setminus A$ into the group $S(F_a)$ of one-to-one transformations of the set F_a thus arises. We refer to this homomorphism as the *A-monodromy homomorphism*. By the monodromy group of an $\mathcal{S}$-function f with a forbidden set A (or, briefly, by the *A-monodromy group*) we mean the image of the fundamental group $\pi_1(S^2 \setminus A, a)$ in the group $S(F_a)$ under the homomorphism τ.

Proposition 5.10. 1) *The A-monodromy group of an $\mathcal{S}$-function does not depend on the choice of the point a.*

2) *The A-monodromy group of an $\mathcal{S}$-function f acts transitively on the branches of the function f.*

Both the assertions admit simple proofs, which use Lemma 5.6. For instance, let us dwell on the proof of the second assertion.

Proof. Let f_{1a} and f_{2a} be some germs of f at a point a. Since f_{1a} and f_{2a} are equivalent, there is a curve γ such that f_{2a} is obtained when f_{1a} is continued along γ. By Lemma 5.6, there is an arbitrarily close curve $\widehat{\gamma}$ that is disjoint from the set A. If $\widehat{\gamma}$ is sufficiently close to γ, then the permutation of branches that corresponds to this curve still takes the germ f_{1a} to the germ f_{2a}.

5.3.2. *Closed monodromy group.* The dependence of the A-monodromy group on the choice of the set A (see 5.1.3) leads us to introduce the Tikhonov topology on the group of permutations of the branches. It turns out that the closure of the A-monodromy group does not depend on the set A.

We equip the group $S(M)$ of one-to-one transformations of a set M with the following topology. For any finite set $L \subset M$ we define the neighbourhood U_L of the identity transformation as the family of all transformations p such that $p(l) = l$ for $l \in L$. A basis of neighbourhoods of the identity transformation is defined as the set of neighbourhoods of the form U_L, where L ranges over all finite subsets of M.

Lemma 5.11 (on the closure of the monodromy group). *Let Γ be the monodromy group of an $\mathcal{S}$-function f with a forbidden set A. The closure of the group Γ in the group $S(F)$ of all permutations of branches of f does not depend on the choice of the forbidden set A.*

Proof. Let A_1 and A_2 be two forbidden sets of f and let F_a be the set of all branches of f at a point $a \notin A_1 \cup A_2$. Let $\Gamma_1, \Gamma_2 \subseteq S(F_a)$ be the monodromy groups of f with these forbidden sets. It suffices to show that for any permutation $\mu_1 \in \Gamma_1$ and any finite set $L \subseteq F_a$ there is a permutation $\mu_2 \in \Gamma_2$ such that $\mu_1|_L = \mu_2|_L$. Let a curve $\gamma \in \pi_1(S^2 \setminus A_1, a)$ determine the permutation μ_1. Since the set L is finite, every curve $\widehat{\gamma} \in \pi_1(S^2 \setminus A_1, a)$ that is sufficiently close to γ determines a permutation $\widehat{\mu}_1$ coinciding with μ_1 on the set L: $\mu_1|_L = \widehat{\mu}_1|_L$. By Lemma 5.6, $\widehat{\gamma}$ can be chosen to be disjoint from the set A_2. In this case the permutation $\widehat{\mu}_1$ belongs to the group Γ_2.

This lemma makes the following definition correct. By the *closed monodromy group* of an $\mathcal{S}$-function f we mean the closure in the group $S(F)$ of the monodromy group of f with some forbidden set A.

5.3.3. *Transitive action of a group on a set and the monodromy pair of an $\mathcal{S}$-function.* A monodromy group of a function f is not only an abstract group but also a transitive group of permutations of branches of this function. In this subsection we recall an algebraic description of transitive actions of groups on sets.

By an *action* of a group Γ on a set M one means a homomorphism τ of Γ into the group $S(M)$. Two actions $\tau_1\colon \Gamma \to S(M_1)$ and $\tau_2\colon \Gamma \to S(M_2)$ are said to be *equivalent* if there is a one-to-one map $q\colon M_1 \to M_2$ such that $\overline{q} \circ \tau_1 = \tau_2$, where $\overline{q}\colon S(M_1) \to S(M_2)$ is an isomorphism induced by the map q.

By the *stationary subgroup* or *stabilizer* Γ_a of a point $a \in M$ under the action τ one means the subgroup consisting of all elements $\mu \in \Gamma$ such that $\tau\mu(a) = a$. An action τ is said to be *transitive* if for any two points $a, b \in M$ there is an element $\mu \in \Gamma$ such that $\tau\mu(a) = b$. The following proposition is obvious.

Proposition 5.12. 1) *An action τ of a group Γ is transitive if and only if the stabilizers of any two points $a, b \in M$ are conjugate. The image of Γ under a transitive action τ is isomorphic to the quotient group $\Gamma/\bigcap_{\mu\in\Gamma} \mu\Gamma_a\mu^{-1}$.*

2) *For any subgroup of Γ there is a transitive action of the group for which the given subgroup is the stabilizer of some point, and this action is unique up to equivalence.*

Thus, the transitive actions of a group Γ are described by pairs of groups. A pair $[\Gamma, \Gamma_a]$ of groups, where Γ_a is the stabilizer of some point a under a transitive action τ of Γ, will be called the *monodromy pair of the point a* with respect to the action τ. We refer to the group $\tau(\Gamma) \sim \Gamma/\bigcap_{\mu\in\Gamma} \mu\Gamma_a\mu^{-1}$ as the monodromy group of the pair $[\Gamma, \Gamma_a]$.

An A-monodromy homomorphism τ defines a transitive action of the fundamental group $\pi_1(S^2 \setminus A)$ on the set F_a of branches of the function f at the point a.

In this case we refer to the monodromy pair of a germ f_a with respect to the action τ as the *monodromy pair of the germ f_a with the forbidden set A*. The monodromy pair of f_a under the action of the closed monodromy group will be called the *closed monodromy pair of the germ f_a*. Different germs of an $\mathcal{S}$-function f have isomorphic monodromy pairs with the forbidden set A, and therefore one can speak of the monodromy pair with a forbidden set A and of the closed monodromy pair of an $\mathcal{S}$-function f. We denote by $[f]$ the closed monodromy pair of an $\mathcal{S}$-function f.

5.3.4. *Almost normal functions.* A pair $[\Gamma, \Gamma_0]$ of groups, $\Gamma_0 \subseteq \Gamma$, is called an *almost normal pair* if there is a finite set $P \subset \Gamma$ such that

$$\bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1} = \bigcap_{\mu\in P} \mu\Gamma_0\mu^{-1}.$$

Lemma 5.13 (on a discrete action). *The image $\tau(\Gamma)$ of a group Γ under a transitive action $\tau\colon \Gamma \to S(M)$ is a discrete subgroup of $S(M)$ if and only if the monodromy pair $[\Gamma, \Gamma_0]$ of some element $x_0 \in M$ is almost normal.*

Proof. Let the group $\tau(\Gamma)$ be discrete. We denote by $\overline{P}$ a finite subset of M such that the neighbourhood $U_{\overline{P}}$ of the identity transformation contains no transformations in $\tau(\Gamma)$ other than the identity transformation. This means that corresponding to the intersection $\bigcap_{x\in\overline{P}} \Gamma_x$ of the stabilizers of the points $x \in \overline{P}$ is the trivial action on the set M, that is, $\bigcap_{x\in\overline{P}} \Gamma_x \subseteq \bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$. The groups Γ_x are conjugate to the group Γ_0, and therefore one can choose a finite set $P \subset \Gamma$ such that $\bigcap_{\mu\in P} \mu\Gamma_0\mu^{-1} = \bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$. The converse assertion can be proved in a similar way.

An $\mathcal{S}$-function f is said to be *almost normal* if its monodromy group is discrete. It follows from the lemma that a function f is almost normal if and only if its closed monodromy pair $[f]$ is almost normal.

By a *differential rational function* in several functions one means a rational function in these functions and their derivatives.

Lemma 5.14 (on finitely generated functions). *Let every germ of an $\mathcal{S}$-function f at a point a be a differential rational function in finitely many fixed germs of f at the point a. Then f is almost normal.*

Indeed, if the fixed germs of the function are preserved when continued along a closed curve, then the differential rational functions in these germs are also preserved.

It follows from the lemma on finitely generated functions that every solution of a linear differential equation with rational coefficients is an almost normal function. The same holds for many other functions naturally arising in differential algebra.

5.3.5. *Classes of pairs of groups.* In the next subsection we shall describe how closed monodromy pairs of functions change under composition, integration, differentiation, and so on. To this end, we need some notions related to pairs of groups.

By a *pair of groups* we always mean a pair consisting of a group and some subgroup of it. We identify the group with the pair of groups consisting of the group itself and its identity subgroup.

Definition. A family $\mathcal{L}$ of pairs is called an *almost complete class of pairs of groups* if

1) for any pair $[\Gamma, \Gamma_0] \in \mathcal{L}$ of groups, $\Gamma_0 \subseteq \Gamma$, and each homomorphism $\tau\colon \Gamma \to G$, where G is a group, the pair $[\tau\Gamma, \tau\Gamma_0]$ also belongs to $\mathcal{L}$,
2) for any pair $[\Gamma, \Gamma_0] \in \mathcal{L}$, $\Gamma_0 \subseteq \Gamma$, and each homomorphism $\tau\colon G \to \Gamma$, where G is a group, the pair $[\tau^{-1}\Gamma, \tau^{-1}\Gamma_0]$ also belongs to $\mathcal{L}$,
3) for any pair $[\Gamma, \Gamma_0] \in \mathcal{L}$, $\Gamma_0 \subseteq \Gamma$, and each group G equipped with a T_2-topology and containing Γ, $\Gamma \subseteq G$, the pair $[\overline{\Gamma}, \overline{\Gamma}_0]$ also belongs to $\mathcal{L}$, where $\overline{\Gamma}$ and $\overline{\Gamma}_0$ are the closures of the groups Γ and Γ_0 in the group G, respectively.

Definition. An almost complete class $\mathcal{M}$ of pairs of groups is said to be a *complete class of pairs of groups* if

1) for any pair $[\Gamma, \Gamma_0] \in \mathcal{M}$ of groups and each group Γ_1 with $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma$ the pair $[\Gamma, \Gamma_1]$ also belongs to $\mathcal{M}$,
2) for any two pairs $[\Gamma, \Gamma_1], [\Gamma_1, \Gamma_2] \in \mathcal{M}$ the pair $[\Gamma, \Gamma_2]$ also belongs to $\mathcal{M}$.

The minimal almost complete class and the minimal complete class of pairs of groups containing a fixed set $\mathcal{B}$ of pairs of groups are denoted by $\mathcal{L}\langle\mathcal{B}\rangle$ and $\mathcal{M}\langle\mathcal{B}\rangle$, respectively.

Lemma 5.15. 1) *If the monodromy group of a pair $[\Gamma, \Gamma_0]$ is contained in some complete class $\mathcal{M}$ of pairs, then the pair $[\Gamma, \Gamma_0]$ also belongs to $\mathcal{M}$.*

2) *If an almost normal pair $[\Gamma, \Gamma_0]$ is contained in some complete class $\mathcal{M}$ of pairs, then the monodromy group of this pair also belongs to $\mathcal{M}$.*

Let us dwell on the proof of the second assertion. Let Γ_i, $i = 1, \dots, n$, be finitely many subgroups conjugate to Γ_0 and such that $\bigcap_{i=1}^{n} \Gamma_i = \bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$. The pairs

$[\Gamma, \Gamma_i]$ are isomorphic to the pair $[\Gamma, \Gamma_0]$, and therefore $[\Gamma, \Gamma_i] \in \mathcal{M}$. Let $\tau\colon \Gamma_2 \to \Gamma$ be the inclusion homomorphism. In this case $\tau^{-1}(\Gamma_1) = \Gamma_2 \cap \Gamma_1$, and therefore $[\Gamma_2, \Gamma_2 \cap \Gamma_1] \in \mathcal{M}$. The class $\mathcal{M}$ contains the pairs $[\Gamma, \Gamma_2]$ and $[\Gamma_2, \Gamma_2 \cap \Gamma_1]$, and hence $[\Gamma, \Gamma_1 \cap \Gamma_2] \in \mathcal{M}$. Continuing this argument, we see that the class $\mathcal{M}$ contains the pair $[\Gamma, \bigcap_{i=1}^{n} \Gamma_i]$, and therefore also the group $\Gamma / \bigcap_{\mu \in \Gamma} \mu \Gamma_0 \mu^{-1}$.

Proposition 5.16 (on the class $\mathcal{L}\langle[f]\rangle$). *An almost complete class of pairs $\mathcal{L}$ contains the closed monodromy pair $[f]$ of an $\mathcal{S}$-function f if and only if this class contains a monodromy pair of the function f for some forbidden set A.*

Proof. Let $[\Gamma, \Gamma_0]$ be a monodromy pair of the function f for a forbidden set A. In this case $[f] = [\overline{\Gamma}, \overline{\Gamma}_0]$. Therefore, every almost complete class $\mathcal{L}$ containing the pair $[\Gamma, \Gamma_0]$ must also contain the pair $[f]$. Conversely, if $[\overline{\Gamma}, \overline{\Gamma}_0]$ is contained in the class $\mathcal{L}$, then $[\Gamma, \Gamma_0] \in \mathcal{L}$. Indeed, the topology in the permutation group is such that $\Gamma_0 = \Gamma \cap \overline{\Gamma}_0$. Therefore, the pair $[\Gamma, \Gamma_0]$ is the pre-image of the pair $[\overline{\Gamma}, \overline{\Gamma}_0]$ under the inclusion of the group Γ in its closure.

5.4. Main theorem. In this subsection we formulate and prove the main theorem of the topological version of Galois theory.

Theorem 5.17 (main theorem). *The class $\widehat{\mathcal{M}}$ of $\mathcal{S}$-functions formed by the $\mathcal{S}$-functions whose closed monodromy pair belongs to some complete class $\mathcal{M}$ of pairs is closed under differentiation, composition, and meromorphic operations.*

Moreover, if the class $\mathcal{M}$ contains the group $\mathbb{C}$ of complex numbers with respect to addition, then the class $\widehat{\mathcal{M}}$ is closed with respect to integration. If $\mathcal{M}$ contains the symmetric group $S(k)$ formed by the permutations on k elements, then $\widehat{\mathcal{M}}$ is closed with respect to the solution of algebraic equations of degree at most k.

The proof of the main theorem consists of the following lemmas.

Lemma 5.18 (on the derivative). $[f'] \in \mathcal{M}\langle[f]\rangle$ *for any $\mathcal{S}$-function f.*

Proof. Let A be the set of singular points of the $\mathcal{S}$-function f and let f_a be a germ of f at a non-singular point a. We denote by Γ the fundamental group $\pi_1(S^2 \setminus A, a)$ and by Γ_1 and Γ_2 the stabilizers of the germs f_a and f'_a, respectively. The group Γ_1 is contained in the group Γ_2. Indeed, the germ f_a is preserved upon continuation along the curve $\gamma \in \Gamma_1$, and hence its derivative is also preserved. It follows from the definition of a complete class of pairs that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle[\Gamma, \Gamma_1]\rangle$. Using Proposition 5.16, we see that $[f'] \in \mathcal{M}\langle[f]\rangle$.

Lemma 5.19 (on composition). $[g \circ f] \in \mathcal{M}\langle[f], [g]\rangle$ *for any $\mathcal{S}$-functions f and g.*

Proof. Let A and B be the sets of singular points of f and g. Let $f^{-1}(B)$ be the pre-image of the set B under the multivalued correspondence generated by the multivalued function f. We set $Q = A \cup f^{-1}(B)$. Let f_a be a germ of the function f at a point $a \notin Q$ and let g_b be a germ of the function g at the point $b = f(a)$. The set Q is forbidden for the germ $g_b \circ f_a$. Denote by Γ the fundamental group $\pi_1(S^2 \setminus Q, a)$ and by Γ_1 and Γ_2 the stabilizers of the germs f_a and $g_b \circ f_a$, respectively. Denote by G the fundamental group $\pi_1(S^2 \setminus B, b)$ and by G_0 the stabilizer of the germ g_b.

We define a homomorphism $\tau\colon \Gamma_1 \to G$. To every curve $\gamma \in \Gamma_1$ we assign the curve $\tau \circ \gamma(t) = f_{\gamma(t)}(\gamma(t))$, where $f_{\gamma(t)}$ is the germ obtained by continuing f_a along

γ up to the point t. The curves $\tau \circ \gamma$ are closed, because the germ f_a is preserved under continuation along every curve in Γ_1. Under a homotopy of the curve γ in the set $S^2 \setminus Q$ one obtains a homotopy of the curve $\tau \circ \gamma$ in the set $S^2 \setminus B$, because $f^{-1}(B) \subseteq Q$. Hence, the homomorphism is well defined.

The germ $g_b \circ f_a$ is preserved under any continuation along a curve in the group $\tau^{-1}(G_0)$, or in other words, $\tau^{-1}(G_0) \subseteq \Gamma_2$. This implies the lemma. Indeed, we obtain the inclusions $\Gamma \supseteq \Gamma_2 \supseteq \tau^{-1}(G_0) \subseteq \tau^{-1}(G) = \Gamma_1 \subseteq \Gamma$ which imply that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle [G, G_0], [\Gamma, \Gamma_1] \rangle$. Using Proposition 5.16, we see that $[g \circ f] \in \mathcal{M}\langle [f], [g] \rangle$.

Lemma 5.20 (on the integral). $[\int f(x)\,dx] \in \mathcal{M}\langle [f], \mathbb{C} \rangle$ *for any* $\mathcal{S}$*-function* f, *where* $\mathbb{C}$ *is the group of complex numbers with respect to addition.*

Proof. Let A be the set of singular points of the function f and let $Q = A \cup \{\infty\}$. Let f_a be a germ of the function f at a point $a \notin Q$ and let g_a be a germ of a function $\int f(x)\,dx$ at this point, $g_a' = f_a$. For a forbidden set for the germs f_a and g_a one can take the set Q. Denote by Γ the fundamental group $\pi_1(S^2 \setminus Q, a)$ and by Γ_1 and Γ_2 the stabilizers of the germs f_a and g_a, respectively.

We define a homomorphism $\tau\colon \Gamma_1 \to \mathbb{C}$. To every curve $\gamma \in \Gamma_1$ we assign the number $\int_\gamma f_{\gamma(t)}(\gamma(t))\,dx$, where $f_{\gamma(t)}$ is the germ obtained by continuing f_a along γ up to the point t and $x = \gamma(t)$. The stabilizer Γ_2 of the germ g_a coincides with the kernel of the homomorphism τ, which implies that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle [\Gamma, \Gamma_1], \mathbb{C} \rangle$. Using Proposition 5.16, we see that $[\int f(x)\,dx] \in \mathcal{M}\langle [f], \mathbb{C} \rangle$.

In what follows it is convenient to use vector functions. The definitions of forbidden set, $\mathcal{S}$-function, and monodromy group can be extended immediately to vector functions.

Lemma 5.21 (on vector functions). *For each vector* $\mathcal{S}$*-function* $\mathbf{f} = (f_1, \dots, f_n)$

$$\mathcal{M}\langle [\mathbf{f}] \rangle = \mathcal{M}\langle [f_1], \dots, [f_n] \rangle.$$

Proof. Let A_i be the set of singular points of the function f_i. The set of singular points of the vector function $\mathbf{f}$ is the set $Q = \bigcup A_i$. Let $\mathbf{f}_a = (f_{1a}, \dots, f_{na})$ be a germ of the vector function $\mathbf{f}$ at a point $a \notin Q$. We denote by Γ the fundamental group $\pi_1(S^2 \setminus Q, a)$, by Γ_i the stabilizer of the germ f_{ia}, and by Γ_0 the stabilizer of the vector germ $\mathbf{f}_a$. The stabilizer Γ_0 is exactly equal to $\bigcap_{i=1}^n \Gamma_i$, and hence

$$\mathcal{M}\langle [\Gamma, \Gamma_0] \rangle = \mathcal{M}\langle [\Gamma, \Gamma_1], \dots, [\Gamma, \Gamma_n] \rangle.$$

Using Proposition 5.16, we obtain

$$\mathcal{M}\langle [\mathbf{f}] \rangle = \mathcal{M}\langle [f_1], \dots, [f_n] \rangle.$$

Lemma 5.22 (on the meromorphic operation). *For any vector* $\mathcal{S}$*-function* $\mathbf{f} = (f_1, \dots, f_n)$ *and any meromorphic function* $F(x_1, \dots, x_n)$ *such that the function* $F \circ \mathbf{f}$ *is defined one has* $[F \circ \mathbf{f}] \in \mathcal{M}\langle [\mathbf{f}] \rangle$.

Proof. Let A be the set of singular points of $\mathbf{f}$ and let B be the projection to the Riemann sphere of the set of poles of the function $F \circ \mathbf{f}$. For a forbidden set for

the functions $F \circ \mathbf{f}$ and $\mathbf{f}$ one can take the set $Q = A \cup B$. Let $\mathbf{f}_a$ be a germ of the function $\mathbf{f}$ at a point $a \notin Q$. We denote by Γ the fundamental group $\pi_1(S^2 \setminus Q, a)$ and by Γ_1 and Γ_2 the stabilizers of the germs $\mathbf{f}_a$ and $F \circ \mathbf{f}_a$. The group Γ_2 is contained in the group Γ_1. Indeed, the vector function is preserved when continued along any curve $\gamma \in \Gamma_1$, and hence the meromorphic function of this vector function is also preserved. It follows from the inclusion $\Gamma_2 \subseteq \Gamma_1$ that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle[\Gamma, \Gamma_1]\rangle$. Using Proposition 5.16, we see that

$$[F \circ \mathbf{f}] \in \mathcal{M}\langle[\mathbf{f}]\rangle.$$

Lemma 5.23 (on an algebraic function). *For each vector $\mathcal{S}$-function $\mathbf{f} = (f_1, \dots, f_n)$ with n components and any algebraic function y of it determined by the equality*

$$y^k + f_1 y^{k-1} + \cdots + f_k = 0 \tag{12}$$

one has the relation $[y] \in \mathcal{M}\langle[f], S(k)\rangle$, where $S(k)$ is the group of permutations on k elements.

Proof. Let A be the set of singular points of the function $\mathbf{f}$ and let B be the projection to the Riemann sphere of the set of algebraic ramification points of the function y. For a forbidden set for the functions y and $\mathbf{f}$ one can take the set $Q = A \cup B$. Let y_a and $\mathbf{f}_a$ be some germs of the functions y and $\mathbf{f}$ at a point $a \notin Q$ that are related by the equality

$$y_a^k + f_{1a} y_a^{k-1} + \cdots + f_{ka} = 0.$$

We denote by Γ the fundamental group $\pi_1(S^2 \setminus Q, a)$ and by Γ_1 and Γ_2 the stabilizers of the germs $\mathbf{f}_a$ and y_a, respectively. The coefficients of the equation (12) are preserved upon continuation along any curve $\gamma \in \Gamma_1$, and hence the roots of the equation (12) are permuted upon continuation along γ. A homomorphism τ of the group Γ_1 into the group $S(k)$ is obtained, $\tau\colon \Gamma_1 \to S(k)$. The group Γ_2 is contained in the kernel of τ, which implies that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle[\Gamma, \Gamma_1], S(k)\rangle$. Using Proposition 5.16, we see that

$$[y] \in \mathcal{M}\langle[f], S(k)\rangle.$$

This completes the proof of the main theorem.

5.5. Group obstructions to the representability by quadratures. In this subsection we compute the classes of pairs of groups occurring in the main theorem and formulate the necessary conditions for the representability of functions by quadratures, k-quadratures, and generalized quadratures.

5.5.1. *Computation of some classes of pairs of groups.* The main theorem makes it an important problem to describe the smallest class of pairs of groups that contains the additive group $\mathbb{C}$ of complex numbers and also the smallest pairs of classes of pairs of groups that contain both the group $\mathbb{C}$ and all finite groups and also both the group $\mathbb{C}$ and the group $S(k)$, respectively. In this subsection we present the solution of these problems.

Proposition 5.24. *The smallest complete class of pairs $\mathcal{M}\langle\mathcal{L}_\alpha\rangle$ that contains given almost complete classes of pairs $\mathcal{L}_\alpha$ consists of the pairs of groups $[\Gamma,\Gamma_0]$ for which there is a chain of subgroups $\Gamma=\Gamma_1\supseteq\cdots\supseteq\Gamma_m\subseteq\Gamma_0$ such that for $1\leqslant i\leqslant m-1$ the pair of groups $[\Gamma_i,\Gamma_{i+1}]$ belongs to some almost complete class $\mathcal{L}_{\alpha(i)}$.*

To prove this proposition, it suffices to show that, first, the pairs of groups $[\Gamma,\Gamma_0]$ satisfying the assumption of the proposition belong to the complete class $\mathcal{M}\langle\mathcal{L}_\alpha\rangle$ and, second, these pairs form a complete class of pairs. Both facts follow immediately from the definitions.

One can also readily verify the following propositions.

Proposition 5.25. *The family of pairs of groups $[\Gamma,\Gamma_0]$ such that Γ_0 is a normal subgroup of the group Γ and the group Γ/Γ_0 is commutative forms the smallest almost complete class of pairs $\mathcal{L}\langle\mathcal{A}\rangle$ that contains the class $\mathcal{A}$ of all Abelian groups.*

Proposition 5.26. *The family of pairs of groups $[\Gamma,\Gamma_0]$ such that Γ_0 is a normal subgroup of the group Γ and the group Γ/Γ_0 is finite forms the smallest almost complete class of pairs $\mathcal{L}\langle\mathcal{K}\rangle$ that contains the class $\mathcal{K}$ of all finite groups.*

Proposition 5.27. *The family of pairs of groups $[\Gamma,\Gamma_0]$ such that $\operatorname{ind}(\Gamma,\Gamma_0)\leqslant k$ forms an almost complete class of groups.*

We denote the class of pairs of groups in Proposition 5.27 by $\mathcal{L}\langle\operatorname{ind}\leqslant k\rangle$. Proposition 5.27 is of interest for us in connection with the characteristic property of subgroups of the group $S(k)$ in Lemma 3.13. A chain of subgroups Γ_i, $i=1,\dots,m$, $\Gamma=\Gamma_1\supseteq\cdots\supseteq\Gamma_m\subseteq\Gamma_0$, is said to be a *normal tower of a pair of groups* $[\Gamma,\Gamma_0]$ if the group Γ_{i+1} is a normal subgroup of the group Γ_i for any $i=1,\dots,m-1$. The family of quotient groups Γ_i/Γ_{i+1} is called the family of divisors with respect to the normal tower.

Theorem 5.28 (on the classes of pairs $\mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle$, $\mathcal{M}\langle\mathcal{A},S(k)\rangle$, and $\mathcal{M}\langle\mathcal{A}\rangle$). 1) *A pair of groups $[\Gamma,\Gamma_0]$ belongs to the smallest complete class $\mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle$ containing all finite and commutative groups if and only if this pair admits a normal tower such that every divisor with respect to this tower is either a finite group or a commutative group.*

2) *A pair of groups $[\Gamma,\Gamma_0]$ belongs to the smallest complete class $\mathcal{M}\langle\mathcal{A},S(k)\rangle$ containing the group $S(k)$ and all commutative groups if and only if this pair admits a normal tower such that every divisor with respect to this tower is either a subgroup of $S(k)$ or a commutative group.*

3) *A pair of groups $[\Gamma,\Gamma_0]$ belongs to the smallest class $\mathcal{M}\langle\mathcal{A}\rangle$ if and only if the monodromy group of this pair is solvable.*

Proof. The first assertion of the theorem follows from the description of the classes $\mathcal{L}\langle\mathcal{A}\rangle$ and $\mathcal{L}\langle\mathcal{K}\rangle$ in Propositions 5.25 and 5.26 and from Proposition 5.24.

To prove the second assertion, we consider the smallest complete class of pairs of groups containing the classes $\mathcal{L}\langle\mathcal{A}\rangle$ and $\mathcal{L}\langle\operatorname{ind}\leqslant k\rangle$. This class consists of pairs of groups $[\Gamma,\Gamma_0]$ for which there is a chain of subgroups $\Gamma=\Gamma_1\supseteq\cdots\supseteq\Gamma_m\subseteq\Gamma_0$ such that for $1\leqslant i\leqslant m-1$ either Γ_i/Γ_{i+1} is commutative or $\operatorname{ind}(\Gamma_i,\Gamma_{i+1})\leqslant k$ (see Propositions 5.26 and 5.27 and Proposition 5.24). The class of pairs of groups

thus described contains the group $S(k)$ (see Lemma 3.13) and all commutative groups, and it is obviously the smallest complete class of pairs that has these properties. It remains to reformulate the answer. Let us transform the chain of subgroups $\Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$ step by step into a normal tower of the pair $[\Gamma, \Gamma_0]$. Suppose that the group Γ_{j+1} is a normal subgroup of the group Γ_j for any $j < i$ and that $\operatorname{ind}(\Gamma_i, \Gamma_{i+1}) \leqslant k$. We denote by $\overline{\Gamma}_{i+1}$ the largest normal subgroup of Γ_i contained in Γ_{i+1}. It is clear that the quotient group $\Gamma_i/\overline{\Gamma}_{i+1}$ is a subgroup of $S(k)$. Instead of the original chain of subgroups, we consider the chain $\Gamma = G_1 \supseteq \cdots \supseteq G_m = \Gamma_0$ in which $G_j = \Gamma_j$ for $j \leqslant i$ and $G_j = \Gamma_j \cap \overline{\Gamma}_{i+1}$ for $j > i$. Continuing this process (at most m times), we pass from the original chain of subgroups to a normal tower and obtain a description of the class $\mathcal{M}\langle \mathcal{A}, S(k)\rangle$ in the desired terms.

Let us prove the assertion 3). By Propositions 5.25 and 5.26, a pair of groups $[\Gamma, \Gamma_0]$ belongs to the class $\mathcal{M}\langle \mathcal{A}\rangle$ if and only if there is a chain $\Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$ such that Γ_i/Γ_{i+1} is a commutative group. Consider a chain of groups $\Gamma = G^1 \supseteq \cdots \supseteq G^m$ in which G^{i+1} is the commutator subgroup of G^i for $i = 1, \ldots, m-1$. Every automorphism of the group Γ takes the chain of groups G^i into itself, and therefore every group G^i is a normal subgroup of Γ. By induction on the number i one can show that $G^i \subseteq \Gamma_i$ and, in particular, $G^m \subseteq \Gamma_m \subseteq \Gamma_0$. The group G^m is a normal subgroup of the group Γ, and since $G^m \subseteq \Gamma_0$, it follows that $G^m \subseteq \bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$. By the definition of the chain G^i, the group Γ/G^m is solvable. The group $\Gamma/\bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$ is solvable as a quotient group of the group Γ/G^m. The converse assertion (a pair of groups with solvable monodromy group belongs to the class $\mathcal{M}\langle \mathcal{A}\rangle$) is obvious.

Proposition 5.29. *Each commutative group Γ with cardinality at most that of the continuum belongs to the class $\mathcal{L}\langle \mathbb{C}\rangle$.*

Proof. The complex numbers $\mathbb{C}$ form a vector space over the rational numbers, with dimension the cardinality of the continuum. Let $\{e_\alpha\}$ be a basis of this space. The subgroup $\widetilde{\mathbb{C}}$ of $\mathbb{C}$ generated by the numbers $\{e_\alpha\}$ is a free Abelian group with a continuum of generators. Every commutative group Γ with cardinality at most that of the continuum is a quotient group of $\widetilde{\mathbb{C}}$, and hence $\Gamma \in \mathcal{L}\langle \mathbb{C}\rangle$.

It follows from Proposition 5.29 and from the results on computation of the classes $\mathcal{M}\langle \mathcal{A}, \mathcal{K}\rangle$, $\mathcal{M}\langle S(n)\rangle$, and $\mathcal{M}\langle \mathcal{A}\rangle$ that a pair of groups $[\Gamma, \Gamma_0]$ such that the cardinality of the group Γ is at most the cardinality of the continuum belongs to the class $\mathcal{M}\langle \mathbb{C}, \mathcal{K}\rangle$ ($\mathcal{M}\langle \mathbb{C}, S(n)\rangle$, $\mathcal{M}\langle \mathbb{C}\rangle$) if and only if it belongs to the class $\mathcal{M}\langle \mathcal{A}, \mathcal{K}\rangle$ ($\mathcal{M}\langle \mathcal{A}, S(n)\rangle$, $\mathcal{M}\langle \mathcal{A}\rangle$, respectively).

We may confine ourselves to this result, because the cardinality of the group of permutations of branches of a function has cardinality at most that of the continuum.

Lemma 5.30. *Every free non-commutative group Λ does not belong to the class $\mathcal{M}\langle \mathcal{A}, \mathcal{K}\rangle$.*

Proof. Suppose that $\Lambda \in \mathcal{M}\langle \mathcal{A}, \mathcal{K}\rangle$, that is, suppose that Λ has a normal tower $\Lambda = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m = e$ and every divisor with respect to this tower is a finite group or a commutative group. Each group Γ_i is free as a subgroup of a free group

(see [28]). The group $\Gamma_m = e$ is commutative. Let Γ_{i+1} be the commutative group with the least index. For any elements $a, b \in \Gamma_i$ there is a non-trivial relation: if Γ_i/Γ_{i+1} is commutative, then, for instance, the elements $aba^{-1}b^{-1}$ and $ab^2a^{-1}b^{-2}$ commute, and if Γ_i/Γ_{i+1} is finite, then some powers a^p, b^p of the elements a, b commute. Hence, the group Γ_i cannot have more than one generator and is therefore commutative. The contradiction shows that $\Lambda \notin \mathcal{M}\langle \mathcal{A}, \mathcal{K}\rangle$.

Lemma 5.31. *For $k > 4$ the symmetric group $S(k)$ does not belong to the class $\mathcal{M}\langle \mathbb{C}, S(k-1)\rangle$.*

Proof. For $k > 4$ the alternating group $A(n)$ is simple and non-commutative. For this group the condition of the criterion for a group to belong to the class $\mathcal{M}\langle \mathbb{C}, S(k-1)\rangle$ certainly fails. Hence, $S(n)$ does not belong to the class $\mathcal{M}\langle \mathbb{C}, S(k-1)\rangle$ for $k > 4$.

Lemma 5.32. *The only transitive group of permutations of k elements generated by transpositions is the symmetric group $S(k)$.*

Proof. Let Γ be a transitive group of permutations of a set M containing n elements and let Γ be generated by transpositions. A subset $M_0 \subseteq M$ is said to be *complete* if every permutation of M_0 can be extended to some permutation of M belonging to the group Γ. Complete subsets really do exist. For example, two elements of M that are transposed by a basis transposition form a complete subset. Let M_0 be a complete subset of maximal cardinality. Suppose that $M_0 \neq M$. Since the group Γ is transitive, there is a basis transposition μ transposing some element $a \notin M_0$ and some element $b \in M_0$. The group of permutations generated by the transposition μ and the group $S(M_0)$ is the group $S(M_0 \cup \{a\})$. The set $M_0 \cup \{a\}$ is complete and contains the set M_0. This contradiction shows that Γ is the group $S(M)$.

5.5.2. *Necessary conditions for the representability of functions by quadratures, by k-quadratures, and by generalized quadratures.* The main theorem (see 5.4) and the computation of classes of pairs of groups give topological obstructions to the representability of functions by generalized quadratures, by k-quadratures, and by quadratures. In this subsection we collect the information obtained above. Let us begin with the definition of the class of functions representable by means of single-valued $\mathcal{S}$-functions and quadratures (k-quadratures, generalized quadratures). As in 1.2, we define these classes by listing the basic functions and the admissible operations.

The functions representable by means of single-valued $\mathcal{S}$-functions and quadratures.

List of the basic functions: the single-valued $\mathcal{S}$-functions.

List of admissible operations: compositions, meromorphic operations, differentiation, and integration.

The functions representable by means of single-valued $\mathcal{S}$-functions and k-quadratures. This class of functions is defined in exactly the same way. One need only adjoin the operation of solving algebraic equations of degree $\leqslant k$ to the list of admissible operations.

The functions representable by means of single-valued $\mathcal{S}$-functions and generalized quadratures. This class of functions is defined in exactly the same way.

One need only adjoin the operation of solving algebraic equations to the list of admissible operations.

It follows from the definition that the class of functions representable by means of single-valued $\mathcal{S}$-functions and quadratures (k-quadratures, generalized quadratures) contains the class of functions representable by quadratures (k-quadratures, generalized quadratures). It is clear that the function classes just defined are incomparably wider than their classical analogues. Therefore, for example, the assertion that a function f does not belong to the class of functions representable by means of single-valued $\mathcal{S}$-functions and quadratures is much stronger than the assertion that f is not representable by quadratures.

Proposition 5.33. *The class of functions representable by means of single-valued $\mathcal{S}$-functions and quadratures (k-quadratures, generalized quadratures) is contained in the class of $\mathcal{S}$-functions.*

This proposition follows immediately from the theorem on the closedness of the class of $\mathcal{S}$-functions (see 5.2.2).

Result on generalized quadratures. *The closed monodromy pair $[f]$ of a function f representable by generalized quadratures admits a normal tower such that every divisor with respect to this tower is either a finite group or a commutative group. Moreover, this condition holds for the closed monodromy pair $[f]$ of every function f representable by means of single-valued $\mathcal{S}$-functions and generalized quadratures. If it is known in addition that f is almost normal, then the above condition also holds for the monodromy group of $[f]$.*

Result on k-quadratures. *The closed monodromy pair $[f]$ of a function f representable by k-quadratures admits a normal tower such that every divisor with respect to this tower is either a subgroup of the group $S(k)$ or a commutative group. Moreover, this condition holds for the closed monodromy pair $[f]$ of every function f representable by means of single-valued $\mathcal{S}$-functions and k-quadratures. If it is known in addition that f is almost normal, then the above condition also holds for the monodromy group of $[f]$.*

Result on quadratures. *The closed monodromy pair $[f]$ of a function f representable by quadratures is solvable. Moreover, the closed monodromy group of every function f representable by means of single-valued $\mathcal{S}$-functions and quadratures is solvable.*

To prove these results, it suffices to apply the main theorem to the classes $\widehat{\mathcal{M}}\langle\mathbb{C}, \mathcal{K}\rangle$, $\widehat{\mathcal{M}}\langle\mathbb{C}, S(k)\rangle$, and $\widehat{\mathcal{M}}\langle\mathbb{C}\rangle$ of $\mathcal{S}$-functions and to use the above computation of the classes $\mathcal{M}\langle\mathbb{C}, \mathcal{K}\rangle$, $\mathcal{M}\langle\mathbb{C}, S(k)\rangle$, and $\mathcal{M}\langle\mathbb{C}\rangle$.

We now present examples of functions that are not representable by generalized quadratures. Let the Riemann surface of a function f be the universal covering of the domain $S^2 \setminus A$, where S^2 is the Riemann sphere and A is a finite set containing at least three points. Then the *function f cannot be expressed by means of single-valued $\mathcal{S}$-functions and generalized quadratures.* Indeed, f is almost normal. The closed monodromy group of f is free and non-commutative, because the fundamental group of the domain $S^2 \setminus A$ is free and non-commutative.

Example 1. Let us consider a function f that maps the upper half-plane conformally onto a regular triangle with zero angles that is bounded by arcs of circles. The function f is the inverse of the Picard modular function. The Riemann surface of f is the universal covering of the sphere with three punctures, and therefore f cannot be expressed by means of single-valued $\mathcal{S}$-functions and generalized quadratures.

We note that the function f is closely related to the elliptic integrals

$$K_1(k) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \quad \text{and} \quad K_2(k) = \int_0^{\frac{1}{k}} \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}\,.$$

Among the functions K_1, K_2, and f, any two of them can be expressed in terms of each other by quadratures (see [13]). Therefore, *each of the integrals K_1 and K_2 cannot be expressed by means of single-valued $\mathcal{S}$-functions and generalized quadratures.*

Example 1 admits a substantial generalization. In [21] (see also [22]) one can find a list of all those polygons bounded by arcs of circles onto which the upper half-plane can be mapped by a function representable by generalized quadratures.

Example 2. Let f be a k-valued algebraic function with non-multiple ramification points located at different points of the Riemann sphere. *If $k > 4$, then f cannot be expressed by means of single-valued $\mathcal{S}$-functions and $(k-1)$-quadratures, compositions, and meromorphic operations. In particular, f is not representable by $(k-1)$-quadratures.*

Indeed, on going around a non-multiple ramification point of f, one obtains a transposition of the set of branches of this function. The monodromy group of f is a transitive group of permutations generated by transpositions, that is, the monodromy group is the group $S(k)$. For $k > 4$ the group $S(k)$ does not belong to the class $\mathcal{M}\langle\mathbb{C}, S(k-1)\rangle$.

In the papers [23]–[25] the topological results on non-representability of functions by quadratures (k-quadratures and generalized quadratures) are generalized to the case of functions of several complex variables.

5.5.3. *Classes of singular sets and a generalization of the main theorem.* In § 5 we have considered $\mathcal{S}$-functions, that is, multivalued analytic functions of a complex variable with at most countable sets of singular points. Let $\mathcal{S}$ be the class of all at most countable subsets of the Riemann sphere S^2. We list the properties of the class $\mathcal{S}$ that were used in an essential way:

1) if $A \in \mathcal{S}$, then the set $S^2 \setminus A$ is dense and locally arcwise connected,
2) there is a non-empty set A such that $A \in \mathcal{S}$,
3) if $A \in \mathcal{S}$ and $B \subseteq A$, then $B \in \mathcal{S}$,
4) if $A_i \in \mathcal{S}$, $i = 1, 2, \ldots$, then $\bigcup_{i=1}^{\infty} A_i \in \mathcal{S}$,
5) if U_1 and U_2 are open subsets of the sphere and $f\colon U_1 \to U_2$ is an invertible analytic map and if $A \subseteq U_1$ and $A \in \mathcal{S}$, then $f(A) \in \mathcal{S}$.

By a *complete class of sets* we mean any set of subsets of the Riemann sphere that has the properties 1)–5). A multivalued analytic function is said to be a

Q-function if the set of its singular points belongs to some complete class Q of sets. The definitions and theorems of § 5 can all be extended to Q-functions. For instance, the following version of the main theorem holds.

A version of the main theorem. *For any complete class Q of sets and any complete class $\mathcal{M}$ of pairs the class $\widehat{\mathcal{M}}$ consisting of all Q-functions f such that $[f] \in \mathcal{M}$ is closed under differentiation, composition, and meromorphic operations.*

If in addition $\mathbb{C} \in \mathcal{M}$, then the class $\widehat{\mathcal{M}}$ of Q-functions is closed with respect to integration.

If $S(k) \in \mathcal{M}$, then the class $\widehat{\mathcal{M}}$ of Q-functions is closed with respect to solving algebraic equations of degree at most k.

We present examples of complete classes of sets. Let X_α be the set of all subsets of the Riemann sphere that have zero Hausdorff measure of weight α. One can readily show that if $\alpha \leqslant 1$, then the set X_α forms a complete class of subsets of the sphere.

We note that the new formulation of the main theorem enables us to strengthen all negative results. For instance, let us dwell on the result on non-representability of functions by quadratures. (The results on non-representability by k-quadratures and by generalized quadratures can be generalized in the same way.) We introduce the following class of functions.

The functions representable by means of single-valued X_1-functions and quadratures.

List of the basic functions: single-valued X_1-functions.

List of admissible operations: composition, meromorphic operations, differentiation, integration.

According to the new formulation of the main theorem, an $\mathcal{S}$-function having an unsolvable monodromy group is not only non-representable by quadratures but also non-representable by single-valued X_1-functions and quadratures.

§ 6. Solvability by quadratures of Fuchsian linear differential equations and the topological version of Galois theory

6.1. The Picard–Vessiot theory for Fuchsian equations. In this subsection we show that the topology of the covering of the complex plane by the Riemann surface of a generic solution of a Fuchsian linear differential equation is completely responsible for the solvability of the equation in explicit form.

6.1.1. *Monodromy group of a linear differential equation, and its relation to the Galois group.* We consider a linear differential equation

$$y^{(n)} + r_1 y^{(n-1)} + \cdots + r_n y = 0, \tag{13}$$

where the coefficients r_i are rational functions in a complex variable x. The poles of the rational functions r_i and the point ∞ are called *singular points* of the equation (13).

In a neighbourhood of a non-singular point x_0 the solutions of the equation form an n-dimensional space V^n. Let us now take in the complex plane an arbitrary curve $\gamma(t)$ going from x_0 to a point x_1 and not passing through the singular points a_i.

The solutions of the equation can be analytically continued along the curve, and the continuations are still solutions of the equation. Therefore, corresponding to every curve γ is a linear map M_γ of the solution space $V^n_{x_0}$ at the point x_0 into the solution space $V^n_{x_1}$ at the point x_1.

If one slightly deforms the curve γ, leaving the ends fixed and not touching the singular points, then the map M_γ remains unchanged. Corresponding to closed curves are linear transformations of the space V^n into itself. The family of all these linear transformations of V^n is a group, called the *monodromy group of the equation* (13). Thus, the monodromy group of the equation is the group of linear transformations (of the solutions) that arise when going around singular points. The monodromy group of an equation characterizes the multivaluedness of its solutions.

Lemma 6.1. 1) *The monodromy group of almost every solution of an equation* (13) *is isomorphic to the monodromy group of this equation.*

2) *The monodromy pair of every solution of an equation of the form* (13) *is almost normal.*

Proof. The second assertion of the lemma follows from Lemma 5.14. We dwell on the proof of the first assertion. The monodromy group of an equation of the form (13) is a matrix group containing at most countably many elements. The set of fixed points of every non-identity element of this group is an eigenspace of the finite-dimensional space formed by the solutions of (13). The set of solutions that are fixed under at least one non-identity transformation belonging to the monodromy group is of measure zero in the space of solutions (because the union of at most countably many proper subspaces of a finite-dimensional space is of measure zero in this space). The monodromy group of the other solutions of (13) is isomorphic to the monodromy group of the equation.

In a neighbourhood of a non-singular point x_0 there are n linearly independent solutions $y_1, \dots, y_n$ of (13). In this neighbourhood one can consider the field $\mathcal{R}\langle y_1, \dots, y_n\rangle$ of functions obtained by adjoining all solutions y_i and all their derivatives to the field $\mathcal{R}$ of rational functions.

Every transformation M_γ of the space of solutions belonging to the monodromy group can be extended to an automorphism of the entire field $\mathcal{R}\langle y_1, \dots, y_n\rangle$. Indeed, together with the functions $y_1, \dots, y_n$, every element of the field $\mathcal{R}\langle y_1, \dots, y_n\rangle$ admits a meromorphic continuation along the curve γ. This continuation defines the desired automorphism, because the continuation preserves the arithmetic operations and differentiation, and every rational function returns to its previous value because it is single-valued.

Thus, the *monodromy group of an equation* (13) *is contained in the Galois group of this equation over the field of rational functions.*

The field of invariants of the monodromy group is the subfield of $\mathcal{R}\langle y_1, \dots, y_n\rangle$ that consists of the single-valued functions. For differential equations, in contrast to algebraic equations, the field of invariants with respect to the action of the monodromy group can be larger than the field of rational functions.

For example, if all the coefficients $r_i(x)$ of a differential equation of the form (13) are polynomials, then all the solutions of the equation are entire functions. However, the solutions of these equations are certainly far from being always polynomial.

The point is that a solution of a differential equation can have exponential growth when approaching a singular point. There is a wide class of linear differential equations for which this complication is absent, that is, the class of equations all of whose solutions admit at most power-law growth when approaching any singular point (along any sector with vertex at the singular point). Differential equations having this property are called *Fuchsian* differential equations (see [11], [16]). The following theorem of Frobenius holds for Fuchsian differential equations.

Theorem 6.2 (Frobenius). *For any Fuchsian differential equation the subfield formed by the single-valued functions in the differential field $\mathcal{R}\langle y_1, \dots, y_n\rangle$ coincides with the field of rational functions.*

Before proving the Frobenius theorem, let us dwell on its immediate corollaries.

Corollary 6.3. *The algebraic closure of the monodromy group M (that is, the smallest algebraic group containing M) of a Fuchsian equation coincides with the Galois group of this equation over the field of rational functions.*

Proof. The corollary follows from the Frobenius theorem and from the main theorem of the differential Galois theory (see 4.3).

Theorem 6.4. *A Fuchsian linear differential equation is solvable by quadratures, by k-quadratures, or by generalized quadratures if and only if the monodromy group of this equation is solvable, k-solvable, or almost solvable, respectively.*

The proof follows from the Picard–Vessiot theorem (see 4.5) and the previous corollary.

The differential Galois theory now proves two results.

1) *If the monodromy group of a Fuchsian differential equation is solvable* (*k-solvable*, *almost solvable*), *then this equation is solvable by quadratures* (*by k-quadratures*, *by generalized quadratures*, *respectively*).

2) *If the monodromy group of a Fuchsian differential equation is not solvable* (*not k-solvable*, *not almost solvable*), *then this equation is not solvable by quadratures* (*by k-quadratures*, *by generalized quadratures*, *respectively*).

The first of these results does not need the main theorem of Galois theory and in essence relates to linear algebra. The point is that one needs no special construction of the group of automorphisms of the differential field $\mathcal{R}\langle y_1, \dots, y_n\rangle$ that preserve only the points of the field of rational functions. The desired group is the monodromy group. Therefore, to prove solvability by quadratures and by the generalized quadratures for Fuchsian equations with solvable or almost solvable monodromy group, it suffices to use the linear-algebraic considerations in 4.7. These linear-algebraic considerations are insufficient to prove solvability by k-quadratures of a Fuchsian equation with k-solvable monodromy group. One must also use Galois theory of algebraic extensions of the field of rational functions (see Proposition 4.21). However, the Galois theory of algebraic extensions of the field $\mathcal{R}$ is quite intuitive and geometric (see 5.1.1).

Our theorem enables one to strengthen the negative result 2). For this strengthening, see 6.2.4. We now proceed to the proof of the Frobenius theorem.

6.1.2. *Proof of the Frobenius theorem.* Let us show that every single-valued function in the differential field $\mathcal{R}\langle y_1, \dots, y_n\rangle$ is meromorphic on the Riemann sphere, and hence rational. Let $p \in S$ be a singular point of a Fuchsian equation and let x be a local parameter near this point such that $x(p) = 0$. By the Fuchs theory, every solution y can be represented near the point p as a finite sum $y = \sum f_{\alpha k} x^\alpha \log^k x$, where the factors $f_{\alpha k}$ are meromorphic functions near p. It is clear that the functions representable in the form $\sum f_{\alpha k} x^\alpha \log^k x$, where the functions $f_{\alpha k}$ are meromorphic near p, form a differential ring containing the field of functions that are meromorphic near p. We must prove that the quotient of two functions in this differential ring is a single-valued function near p if and only if this function is meromorphic. The proof of this fact is based on Proposition 6.5 formulated below. We need the following notation: $U(0,\varepsilon)$ is the ε-neighbourhood of the point 0 in the complex plane; $\widehat{U}(0,\varepsilon)$ is the punctured ε-neighbourhood of the point 0, that is, $\widehat{U}(0,\varepsilon) = U(0,\varepsilon)\setminus\{0\}$; $M(0,\varepsilon)$ and $\widehat{M}(0,\varepsilon)$ are the fields of meromorphic functions on the domains $U(0,\varepsilon)$ and $\widehat{U}(0,\varepsilon)$, respectively.

Two meromorphic germs f_a and g_b are said to be *equivalent over a domain* U, where $a, b \in U$, if the germ g_b is obtained from the germ f_a by continuation along some curve contained in U.

We now define the ring $K_a(0,\varepsilon)$. A meromorphic germ f_a given at a point $a \in \widehat{U}(0,\varepsilon)$ belongs to the *ring* $K_a(0,\varepsilon)$ if

1) the germ f_a can be meromorphically continued along all curves belonging to $\widehat{U}(0,\varepsilon)$,
2) the complex vector space spanned by all the meromorphic germs at the point a that are equivalent to f_a over the neighbourhood $\widehat{U}(0,\varepsilon)$ is finite-dimensional.

The ring $K_a(0,\varepsilon)$ contains the field $\widehat{M}(0,\varepsilon)$ and is a vector space over this field.

Proposition 6.5 (on a basis). *For any choice of branches of the functions* $\log x$ *and* x^α, $[\operatorname{Re}\alpha] = 0$, *the germs* $x_a^\alpha \log_a^k x$, $k = 0, 1, 2, \dots$, *form a basis of the space* $K_a(0,\varepsilon)$ *over the field* $\widehat{M}(0,\varepsilon)$.

Let us first prove a lemma.

Lemma 6.6. *The germs* $1, \log_a x, \dots, \log_a^k x, \dots$ *are linearly independent over the field* $\widehat{M}(0,\varepsilon)$.

Proof. Indeed, the existence of a non-trivial relation $\sum a_k \log_a^k x = 0$ with $a_k \in \widehat{M}(0,\varepsilon)$ implies that the function $\log x$ takes finitely many values in a neighbourhood of zero.

The proof of the proposition is based on a consideration of the monodromy operator $A\colon K_a(0,\varepsilon) \to K_a(0,\varepsilon)$ that assigns to every germ its continuation along a closed curve going around the point 0.

Lemma 6.7. *The germs* $x_a^\alpha \log_a^k x$, $[\operatorname{Re}\alpha] = 0$, $k = 0, 1, \dots, n-1$, *form a basis in the space* $\ker(A - \lambda E)^n$, *where* λ *and* α *are connected by the relation* $\lambda = e^{2\pi i\alpha}$.

Proof. We note that the dimension of the space $\ker(A - \lambda E)$ is at most 1. Indeed, if $Af_a = \lambda f_a$ and $Ag_a = \lambda g_a$, then $A(f_a/g_a) = f_a/g_a$. Hence, the germ $\psi_a = f_a/g_a$

is the germ of some function ψ in the field $\widehat{M}(0,\varepsilon)$, and so $f_a = \psi g_a$. Therefore, the dimension of the space $\ker(A-\lambda E)^n$ is at most n. On the other hand, one can readily see that this space contains the germs $x_a^\alpha \log_a^k x$, $[\operatorname{Re}\alpha]=0$, $k=0,1,\dots,n-1$. By Lemma 6.6, these germs are linearly independent, and therefore form a basis of the space $\ker(A-\lambda E)^n$.

Any two spaces of the form $\ker(A-\lambda E)^n$ with different values of λ have zero intersection. Therefore, all the germs $x_a^\alpha \log_a^k x$ are linearly independent. Let us show that every germ f_a in the space $K_a(0,\varepsilon)$ can be expanded in these functions. By definition, f_a belongs to some finite-dimensional space V that is invariant under the monodromy operator. Let $\widetilde{A}$ be the restriction of the operator A to the space V. As is known in linear algebra, V can be decomposed into the direct sum of the subspaces $\ker(\widetilde{A}-\lambda E)^{n_\lambda}$, where λ is an eigenvalue of the operator $\widetilde{A}$ and n_λ is the multiplicity of this eigenvalue. It follows from Lemma 6.7 that every element of the space V can be expanded in the vectors $x_a^\alpha \log_a^k x$.

Remark. The choice of different branches of the functions $\log x$ and x^α leads to different bases in the space $K_a(0,\varepsilon)$. The coefficients of expansion of the vectors in these bases with respect to another such basis are complex numbers.

Definition. 1) One says that a meromorphic germ f_a, $a\in\widehat{U}(0,\varepsilon)$, has an *entire Fuchsian singularity* over the neighbourhood $\widehat{U}(0,\varepsilon)$ if $f_a\in K_a(0,\varepsilon)$ and the coefficients of the expansion of f_a with respect to the basis $x_a^\alpha\log_a^k x$ are meromorphic, that is, if

$$f_a=\sum f_{\alpha,k}\log_a^k x\cdot x_a^\alpha,\quad \text{where}\quad f_{\alpha,k}\in M(0,\varepsilon).$$

2) A meromorphic germ f_a, $a\in\widehat{U}(0,\varepsilon)$, is said to have a *Fuchsian singularity* over the neighbourhood $\widehat{U}(0,\varepsilon)$ if this germ is representable as the quotient of two germs ψ_a and g_a each having an entire Fuchsian singularity over the neighbourhood $\widehat{U}(0,\varepsilon)$, that is, $f_a=\psi_a/g_a$.

Corollary 6.8. *A germ $f_a\in K_a(0,\varepsilon)$ has a Fuchsian singularity over the neighbourhood $\widehat{U}(0,\varepsilon)$ if and only if it has an entire Fuchsian singularity over this neighbourhood.*

Proof. One has $f_a\in K_a(0,\varepsilon)$, and hence $f_a=\sum r_{\alpha,k}x_a^\alpha\log_a^k x$, where $r_{\alpha,k}\in\widehat{M}(0,\varepsilon)$ are the coefficients of the expansion of f_a with respect to the basis. The germ f_a has a Fuchsian singularity as well, and therefore we have the equality

$$\frac{\sum p_{\alpha,k}x_a^\alpha\log_a^k x}{\sum q_{\alpha,k}x_a^\alpha\log_a^k x}-\sum r_{\alpha,k}x_a^\alpha\log_a^k x=0,$$

where $p_{\alpha,k}$ and $q_{\alpha,k}$ are some elements of the field $M(0,\varepsilon)$. Let us multiply the last equality by the sum $\sum q_{\alpha,k}x_a^\alpha\log_a^k x$, get rid of the parentheses, and reduce the germ $x_a^\beta\log_a^k x$ to the form $x^n\cdot x_a^\alpha\log_a^k x$ if necessary, where n is an integer and $[\operatorname{Re}\alpha]=0$. Since the germs $x_a^\alpha\log_a^k x$ are linearly independent over the field $\widehat{M}(0,\varepsilon)$,

it follows that the above equality is equivalent to the system of equations obtained by equating the coefficients with these functions to zero. The system thus obtained is a system of linear equations with respect to the functions $r_{\alpha,k}$ with coefficients in the field $M(0,\varepsilon)$. The system has a unique solution because the functions $r_{\alpha,k}$ are uniquely determined. Hence, the functions $r_{\alpha,k}$ belong to the field $M(0,\varepsilon)$.

Corollary 6.9. *If a germ f_a of a function f that is meromorphic in the neighbourhood $\widehat{U}(0,\varepsilon)$ has a Fuchsian singularity in this neighbourhood, then f is meromorphic in $U(0,\varepsilon)$.*

Proof. One has $f_a \in K_a(0,\varepsilon)$, and its expansion with respect to the basis is of the form $f_a = f \cdot 1$. By Corollary 6.8, the germ f_a has an entire Fuchsian singularity, and therefore $f \in M(0,\varepsilon)$.

Corollary 6.9 completes the proof of the Frobenius theorem.

6.1.3. *Monodromy group of a system of linear differential equations, and the relation of this group to the Galois group.* The results in 6.1.1 can automatically be extended to systems of linear differential equations with regular singular points.

We consider a linear differential equation

$$\mathbf{y}' = \mathbf{A}(x)\mathbf{y}, \tag{14}$$

where $\mathbf{y} = (y_1(x), \dots, y_n(x))$, $\mathbf{A}(x) = (a_{i,j}(x),\ 1 \leqslant i, j \leqslant n)$ is a matrix of rational functions, and x is a complex variable. Let $a_1, \dots, a_k$ be the poles of the matrix $\mathbf{A}(x)$. In a neighbourhood of a non-singular point x_0 with $x_0 \neq \infty$ and $x_0 \neq a_i$, $i = 1, \dots, k$, the solutions of the equation (14) form an n-dimensional space V^n. Let us now take an arbitrary curve $\gamma(t)$ on the complex plane that goes from the point x_0 to the point x_1 and does not pass through the singular points a_i, that is, $\gamma(0) = x_0$, $\gamma(1) = x_1$, and $\gamma(t) \neq a_i$. The solutions of the equation admit analytic continuation along the curve, and these continuations are still solutions of the equation. Therefore, corresponding to any curve γ is a linear map M_γ from the space $V^n_{x_0}$ of solutions at x_0 into the space V_{x_1} of solutions at x_1.

If one slightly deforms the curve γ, leaving the ends fixed and not touching the singular points, then the map M_γ remains unchanged. Corresponding to closed curves are linear transformations of the space V^n into itself. The family of all these linear transformations of the space V^n is a group, called the *monodromy group of the system* (14). Thus, the monodromy group of the system is the group of linear transformations of solutions that arise when going around singular points. The monodromy group of a system characterizes the multivaluedness of its solutions.

Lemma 6.10. 1) *The monodromy group of almost every solution of the system* (14) *coincides with the monodromy group of the system* (14). 2) *The monodromy pair of every component of every solution of* (14) *is almost normal.* 3) *If the monodromy group of* (14) *does not belong to some complete class $\mathcal{M}$ of pairs of groups, then the monodromy pair of one of the components of almost every solution of this system does not belong to $\mathcal{M}$.*

Proof. The first two assertions in the lemma are proved like Lemma 6.1. The assertion 3) follows from 1) and Lemma 5.21.

In a neighbourhood of a non-singular point x_0 all the solutions $\mathbf{y}_1, \dots, \mathbf{y}_n$ of the system (14) exist. In this neighbourhood one can consider the differential function field $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ obtained by adjoining all the components $y_{i1}, \dots, y_{in}$ of all the solutions $\mathbf{y}_i$ and all their derivatives $y_{ij}^{(p)}$ to the field $\mathcal{R}$ of rational functions.

Every transformation M_γ of the solution space in the monodromy group can be extended to an automorphism of the whole differential field $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ over the field $\mathcal{R}$. Indeed, together with the vector functions $\mathbf{y}_1, \dots, \mathbf{y}_n$, every element of the field $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ can also be meromorphically continued along the curve γ. This extension gives the desired automorphism, because continuation preserves the arithmetic operations and differentiation, and every rational function returns to its previous value because it is single-valued.

A *singular point* of the system (14) is said to be *regular* if all the solutions of the system admit at most power-law growth when approaching any singular point along any sector with vertex at the singular point (see [16], [11]). As is known, near a regular singular point every component of every solution has an entire Fuchsian singularity (see the definition in 6.1.2). The system (14) is said to be *regular* if all its singular points (including the point ∞) are regular. For a regular system (14) all single-valued functions in the field $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ are rational functions.

Theorem 6.11. *For an arbitrary regular system of linear differential equations of the form* (14) *the differential field* $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ *is a Picard–Vessiot extension of the field* $\mathcal{R}$. *The Galois group of this extension is the algebraic closure of the monodromy group of the system of equations* (14).

Proof. The monodromy group acts on the differential field $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ as a group of isomorphisms, and the corresponding field of invariants is equal to $\mathcal{R}$. The field $\mathcal{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ is generated over $\mathcal{R}$ by a finite-dimensional $\mathbb{C}$-linear space that is invariant under the action of the monodromy group, namely, by the linear space spanned by all the components of all the solutions of (14). The theorem follows now from Corollary 4.5.

Theorem 6.12. *Each component of each solution of a regular system of linear differential equations can be expressed by quadratures* (*by k-quadratures*, *by generalized quadratures*) *if and only if the monodromy group of the system is solvable* (*k-solvable*, *almost solvable*, *respectively*).

The proof follows from Theorem 4.12 (the Picard–Vessiot theorem) and from the previous theorem. As in the case of a Fuchsian equation, the 'positive' part of the theorem relating to the solvability of the system is proved mainly by means of linear algebra (see 4.7). The negative part of the theorem can be strengthened significantly by the topological version of Galois theory (see 6.2.4).

6.2. Galois theory for systems of Fuchsian linear differential equations with small coefficients. It turns out that the solvability conditions become absolutely explicit for systems of Fuchsian equations with sufficiently small coefficients [15].

6.2.1. *Systems of Fuchsian equations.* Among the systems of regular linear differential equations one can distinguish the systems of Fuchsian linear differential equations. This is an equation of the form $\mathbf{y}' = \mathbf{A}(x)\mathbf{y}$, where the matrix $\mathbf{A}(x)$ has no multiple poles and vanishes at infinity. In other words, this is an equation of the form

$$\mathbf{y}' = \sum_{p=1}^{k} \frac{A_p}{x - a_p}\mathbf{y},$$

where A_p is a complex $n \times n$ matrix for any p and $\mathbf{y} = (y_1, \dots, y_n)$ is a vector in $\mathbb{C}^n$. The points a_p are called the *poles* and the matrices A_p are called the *residue matrices* of the system of Fuchsian equations.

For systems of Fuchsian equations, as well as for other regular systems of differential equations, *the algebraic closure of the monodromy group coincides with the Galois group of the corresponding Picard–Vessiot extension* (*generated by the system of equations*) *of the field of rational functions* (see 6.1.3).

Lappo-Danilevskii developed the theory of analytic functions of matrices and applied this theory to differential equations [29]. We need some of his results relating to systems of Fuchsian equations; we use these results in the form of a corollary presented at the end of this subsection.

Let us take a non-singular point $x_0 \neq a_p$. We choose k curves $\gamma_1, \dots, \gamma_k$ in such a way that the curve γ_p starts at the point x_0, approaches the pole a_p, goes around this pole, and returns back to x_0. Corresponding to the curves $\gamma_1, \dots, \gamma_k$ are monodromy matrices $M_1, \dots, M_k$. Obviously, the matrices $M_1, \dots, M_k$ generate the monodromy group. If one fixes the curves, then the monodromy matrices depend only on the residue matrices. This dependence was studied by Lappo-Danilevskii.

First, he showed that the monodromy matrices M_p are entire functions of the residue matrices A_j. To be more exact, *there are special series with complex coefficients*

$$M_p = E + 2\pi i A_p + \sum_{1 \leqslant i,j \leqslant k} c_{i,j} A_i A_j + \cdots \tag{15}$$

in the matrices $A_1, \dots, A_k$ that express the monodromy matrices M_p and are convergent for any matrices $A_1, \dots, A_k$.

Although the monodromy matrix M_p depends on all the residue matrices A_j, its eigenvalues are determined only by the eigenvalues of the residue matrix A_p.

Theorem 6.13 ([16], [11]). *Let $\{\mu_m\}$ be the set of eigenvalues of the matrix A_p. Then $\{e^{2\pi i \mu_m}\}$ is the set of eigenvalues of the matrix M_p.*

The famous Riemann–Hilbert problem is the question of the solvability of the inverse problem, that is, the existence problem for a Fuchsian equation with a given family of monodromy matrices. The Riemann–Hilbert problem is solvable for almost every set of monodromy matrices. It was traditionally assumed that this classical result can be extended to arbitrary sets of monodromy matrices. However, as was discovered by Bolibrukh [10], [11], this is not the case. He gave an example of a set of monodromy matrices for which the Riemann–Hilbert problem is unsolvable.

Lappo-Danilevskii showed that if the residue matrices A_j are small, then they are single-valued analytic functions of the monodromy matrices M_p. Namely, he showed that if one confines oneself to Fuchsian equations with sufficiently small residue matrices $\|A_j\| < \varepsilon$, $\varepsilon = \varepsilon(n, a_1, \dots, a_k)$, then the Riemann–Hilbert problem has a unique solution for monodromy matrices M_p sufficiently close to E, that is, for $\|M_p - E\| < \varepsilon$. Moreover, *there are special series*

$$A_p = -\frac{1}{2\pi i}E + \frac{1}{2\pi i}M_p + \sum_{1 \leqslant i,j \leqslant k} b_{ij} M_i M_j + \cdots \tag{16}$$

with complex coefficients in the matrices $M_1, \dots, M_k$ that express the residue matrices A_p and converge for $\|M_p - E\| < \varepsilon$.

The series (16) are obtained by inverting the series (15). This result is a kind of implicit function theorem (for analytic maps with non-commutative variables).

We shall use the Lappo-Danilevskii theory in the form of the following assertion.

Corollary 6.14. *The monodromy matrices belong to the algebra (with identity) generated by the residue matrices. Conversely, if the residue matrices are sufficiently small and the monodromy matrices are sufficiently close to E, then the residue matrices belong to the algebra (with identity) generated by the monodromy matrices.*

6.2.2. *Groups generated by matrices close to the identity matrix.* In this subsection we prove an analogue of the Lie theorem for matrix groups generated by matrices close to the identity matrix. Let us recall the formulation of the Jordan theorem.

Theorem 6.15 (Jordan). *A finite group G of linear transformations of an n-dimensional space has a diagonal normal subgroup G_d of bounded index, that is,* $\operatorname{ind}(G, G_d) \leqslant J(n)$.

Diverse explicit upper bounds for the numbers $J(n)$ are known. (For instance, Schur showed that $J(n) \leqslant (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}$; see [37].)

Proposition 6.16. *There is an integer $T(n)$ such that a subgroup G in $GL(n)$ has a solvable normal subgroup of finite index if and only if it has a triangular normal subgroup of index $\leqslant T(n)$.*

Proof. Suppose that G' is a solvable normal subgroup of G of finite index. The Lie theorem ensures that the group G has a triangular normal subgroup G_l of finite index. Indeed, it suffices to take $G_l = G' \cap \overline{G}_0$, where $\overline{G}_0$ is the connected component of the identity of the algebraic closure $\overline{G}$ of G. However, the index of G_l can be arbitrarily large. For instance, for the group $\mathbb{Z}_k$ of kth roots of unity this index is equal to k for $n = 1$. We enlarge the normal subgroup G_l but keep it triangular. It suffices to prove the existence of a triangular subgroup of bounded index, because a subgroup of index k contains a normal subgroup of index $\leqslant k!$. Let us carry out the proof by induction on the dimension n. If the group G admits an invariant space V^k of dimension k, $0 < k < n$, then we can make an induction step. Indeed, in this case the group G acts both on the space V^k of dimension k and on the quotient space V^n/V^k of dimension $(n-k)$. By induction, one can

assume that G admits a normal subgroup of index $\leqslant T(k)T(n-k)$, and that this subgroup is triangular both in V^k and in V^n/V^k, that is, it is triangular in V^n.

The normal subgroup G_l can be reduced to triangular form, and hence it admits a non-zero maximal eigenspace V^k. Two cases can occur: $V^k \subset V^n$ and $V^k = V^n$. Consider the first case, that is, $V^k \subset V^n$. We denote by $\widetilde{G}_l$ the subgroup of G consisting of all transformations under which the subspace V^k is invariant (we thus enlarge the normal subgroup G_l). Let us prove that $\operatorname{ind}(G, \widetilde{G}_l) \leqslant n$. Indeed, the group of permutations given by G permutes the maximal eigenspaces of each normal subgroup of G and, in particular, permutes these spaces for G_l. However, there can be at most n maximal eigenspaces. This implies the desired relation $\operatorname{ind}(G, \widetilde{G}_l) \leqslant n$. To complete the proof, it suffices to apply the induction step to the group $\widetilde{G}_l$. Consider the other case, that is, let $V^k = V^n$, in which case the subgroup G_l consists of the matrices λE. One can assume that G consists of matrices with unit determinant. Indeed, otherwise one can consider the group formed by the matrices $(\det A)^{-1}A$. Under this assumption, the normal subgroup G_l is finite (because $\lambda^n = 1$). The group G is also finite, because $\operatorname{ind}(G, G_l) < \infty$. To complete the proof, it suffices to use the Jordan theorem.

Proposition 6.16′. *There is an integer $D(n)$ such that any subgroup G of $GL(n)$ has a diagonal normal subgroup of finite index if and only if it has a diagonal normal subgroup of index $\leqslant D(n)$.*

The proof of Proposition 6.16′ is similar to that of Proposition 6.16, and we do not dwell on this proof. The numbers $T(n)$ and $D(n)$ also admit an explicit upper bound (cf. [37]).

Lemma 6.17. *The equation $X^N = A$, where $\|A - E\| < \varepsilon$, $\|X - E\| < \varepsilon$, and X and A are complex $n \times n$ matrices close to E, has a unique solution if $\varepsilon = \varepsilon(n, N)$ is sufficiently small. Moreover, every invariant space V of the matrix A is also X-invariant.*

Proof. Let us write $B = A - E$ and

$$X = E + \frac{1}{N}B + \frac{1}{2}\frac{1}{N}\left(\frac{1}{N} - 1\right)B^2 + \cdots .$$

If $\|B\| < 1$, then the series is convergent and $X^N = A$. We now take the number $\varepsilon = \varepsilon(n, N)$ to be so small that the implicit function theorem ensure the uniqueness of the solution. The space V is invariant under $B = A - E$, and hence under X.

Lemma 6.18. *Let the Nth powers of all the matrices in a matrix group G belong to some algebraic group L. Then the index of the group $G \cap L$ in the group G is finite.*

Proof. Consider the algebraic closure $\overline{G}$ of the group G. One can readily see that if $X \in \overline{G}$, then $X^N \in L$. We denote by $\overline{G}_0$ and L_0 the connected components of the identity in the groups $\overline{G}$ and L, respectively. If A belongs to L_0 and $A = e^M$, then the equation $X^N = A$ has a solution in the same group. Indeed, it suffices to set $X = e^{\frac{M}{N}}$. However, the equation $X^N = A$ has a unique solution if the matrices A and X are close to E. This implies that $\overline{G}_0 \subseteq L_0 \subseteq L$. The lemma now follows from the condition $\operatorname{ind}(\overline{G}, \overline{G}_0) < \infty$.

Remark. If $L = e$, then Lemma 6.18 becomes a theorem of Burnside: *a matrix group satisfying the identity $X^N = e$ is finite.*

Proposition 6.19. *There is an integer $N(n)$ such that a subgroup G of $GL(n)$ has a solvable normal subgroup of finite index if and only if all the matrices $A^{N(n)}$, $A \in G$, can simultaneously be reduced to triangular form.*

Proof. In one direction, Proposition 6.19 follows from Proposition 6.16 if we set $N(n) = T(n)!$. To prove it in the other direction, one must apply Lemma 6.18 to the group G and the group L of triangular matrices.

One can prove the following proposition similarly.

Proposition 6.19′. *There is an integer $N(n)$ such that a subgroup G of $GL(n)$ has a diagonal normal subgroup of finite index if and only if all the matrices $A^{N(n)}$, $A \in G$, can simultaneously be reduced to diagonal form.*

Theorem 6.20. *There is a number $\varepsilon(n) > 0$ such that the subgroup G of $GL(n)$ generated by matrices A_α that are close to the identity matrix, $\|E - A_\alpha\| < \varepsilon(n)$, has a solvable normal subgroup of finite index if and only if all the matrices A_α can simultaneously be reduced to triangular form.*

Proof. Let us take a number $\varepsilon(n) > 0$ small enough that the equation

$$X^{N(n)} = A,$$

where $\|E - X\| < \varepsilon(n)$, satisfies the conditions of Lemma 6.17. By Proposition 6.19, all the matrices $A_\alpha^{N(n)}$ can be reduced to triangular form. However, by Lemma 6.17, the invariant subspaces of the matrices $A_\alpha^{N(n)}$ and A_α coincide. Therefore, the matrices A_α can also be reduced to triangular form.

The proof of the next proposition is similar.

Proposition 6.21. *There is a positive number $\varepsilon(n) > 0$ such that any subgroup G of $GL(n)$ generated by matrices A_α close to the identity matrix, $\|E - A_\alpha\| < \varepsilon(n)$, has a diagonal normal subgroup of finite index if and only if all the matrices A_α can simultaneously be reduced to diagonal form.*

Remark. Both in Theorem 6.20 and in Proposition 6.21 one can weaken the condition that the matrices A_α be close to the identity matrix. It suffices to restrict ourselves to closeness in the Zariski topology. We say that a matrix A is k-resonant if it has distinct eigenvalues λ_1 and λ_2 related by the condition $\lambda_1 = \varepsilon_k \lambda_2$, where $\varepsilon_k^k = 1$, $\varepsilon_k \neq 1$. All k-resonant matrices form an algebraic set not containing the identity matrix. It suffices to assume that the matrices A_α are not $N(n)$-resonant.

6.2.3. *Explicit solvability criteria.* We proceed to an explicit solvability criterion, beginning with two simple lemmas.

Lemma 6.22. *A Fuchsian system of order n of the form*

$$\dot{\mathbf{y}} = \sum_{i=1}^{k} \frac{A_i}{x - a_i} \mathbf{y}$$

with sufficiently small coefficients $\|A_i\| < \varepsilon = \varepsilon(n, a_1, \dots, a_k)$ *is solvable by generalized quadratures if and only if its monodromy matrices* M_i *are triangular.*

Proof. The monodromy group of the system is generated by the monodromy matrices M_i. If the residue matrices A_i are small, $\|A_i\| < \varepsilon$, then the matrices M_i are close to E. Let us choose a number $\varepsilon = \varepsilon(n, a_1, \dots, a_k)$ small enough that the monodromy matrices $M_1, \dots, M_k$ satisfy the conditions of Theorem 6.20. By this theorem, the monodromy group has a solvable normal subgroup of finite index if and only if the matrices $M_1, \dots, M_k$ are triangular. It remains to use Theorem 6.12.

Lemma 6.23. *The triangularity and the diagonality of the Galois group for a Fuchsian system are equivalent to the same condition on the monodromy matrices* $M_1, \dots, M_k$.

Proof. The monodromy group is generated by the monodromy matrices $M_1, \dots, M_k$ and is triangular or diagonal whenever they are. The lemma now follows from the fact that for a Fuchsian equation the Galois group coincides with the algebraic closure of the monodromy group (see 6.1.3).

Solvability criterion. *For a set of poles* $a_1, \dots, a_k$ *and a positive integer* n *there is a number* $\varepsilon(n, a_1, \dots, a_k)$ *such that the solvability conditions for Fuchsian systems of order* n,

$$\dot{\mathbf{y}} = \sum_{i=1}^{k} \frac{A_i}{x - a_i}\mathbf{y},$$

with small coefficients, $\|A_i\| < \varepsilon(n, a_1, \dots, a_k)$, *acquire an explicit form.*

Namely, the system is solvable:

1) *by quadratures or by generalized quadratures*[3] *if and only if the matrices* A_i *are triangular* (*in some basis*);
2) *by integrals and algebraic functions or by integrals and radicals*[3] *if and only if the matrices* A_i *are triangular and their eigenvalues are rational*;
3) *by integrals if and only if the matrices* A_i *are triangular and their eigenvalues are equal to zero*;
4) *by exponentials of integrals and by algebraic functions or by exponentials of integrals*[3] *if and only if the matrices* A_i *are diagonal*;
5) *by algebraic functions or by radicals*[3] *if and only if the matrices* A_i *are diagonal and their eigenvalues are rational*;
6) *by rational functions if and only if all the matrices* A_i *are zero.*

Proof. Let $\varepsilon(n, a_1, \dots, a_k)$ be a number small enough that the conditions of Lemma 6.23 are valid and the residue matrices are expressible in terms of the monodromy matrices (see 6.2.1).

Each of the forms of solvability implies solvability by generalized quadratures. Under our assumptions, solvability by generalized quadratures implies a triangular form of the monodromy matrices (Lemma 6.22), and hence the triangular form of the Galois group (Lemma 6.23). Therefore, we can apply the criterion presented at the end of 4.8. We must transform the conditions on the Galois group in this criterion into conditions on the residue matrices A_i.

[3]These forms of solvability differ if the values of the coefficients are not subjected to the above restriction.

The conditions on the Galois group in the criterion in 4.8 are equivalent to the same conditions on the monodromy matrices $M_1, \dots, M_k$. This fact was partially verified in Lemma 6.23. The remaining verification is also not complicated.

Under the assumptions of our theorem, the condition that the monodromy matrices $M_1, \dots, M_k$ belong to some algebra with identity, for example, to the algebra of triangular matrices or diagonal matrices, is equivalent to the same condition on the residue matrices $A_1, \dots, A_k$ (Corollary 6.14).

The eigenvalues of the matrices M_i are roots of unity or 1s if and only if the eigenvalues of the matrices A_i are rationals or integers, respectively (see 6.2.1).

Our criterion follows now from the criterion in 4.8.

Remark. At the conference dedicated to the 100th birthday of A. N. Kolmogorov, Andrei Bolibrukh told me that in the solvability criterion one can weaken the requirement that the matrices A_i be small. *It suffices to assume that the eigenvalues of these matrices are small.* This was my last conversation with Andrei.

6.2.4. *Strong unsolvability of equations.* The topological version of Galois theory enables one to strengthen the classical results on unsolvability of equations in explicit form.

The monodromy group of an algebraic function coincides with the Galois group of the corresponding Galois extension of the field of rational functions (see 5.1.2). Therefore, by Galois theory, 1) *an algebraic function can be expressed by radicals if and only if its monodromy group is solvable*; 2) *an algebraic function can be expressed in terms of rational functions by using radicals and solutions of algebraic equations of degree k if and only if the monodromy group of this function is k-solvable.*

Our results (see 5.5.2) imply the following assertion.

Corollary 6.24. 1) *If the monodromy group of an algebraic equation over the field of rational functions is not solvable, then the solution of this equation does not belong to the class of functions representable by single-valued $\mathcal{S}$-functions and quadratures.*

2) *If the monodromy group of an algebraic equation is not k-solvable, then the solution of this equation does not belong to the class of functions representable by single-valued $\mathcal{S}$-functions and k-quadratures.*

One can similarly strengthen the results on unsolvability in explicit form presented in 6.1.1, 6.1.3, and 6.2.3.

Corollary 6.25. *If the monodromy group of a linear differential equation over the field of rational functions is not solvable* (*not k-solvable, not almost solvable*), *then a generic solution of the equation does not belong to the class of functions representable by single-valued $\mathcal{S}$-functions and quadratures* (*k-quadratures, generalized quadratures, respectively*).

Corollary 6.26. *If the monodromy group of a system of linear differential equations over the field of rational functions is not solvable* (*not k-solvable, not almost solvable*), *then at least one component of almost every solution does not belong to the class of functions representable by single-valued $\mathcal{S}$-functions and quadratures* (*k-quadratures, generalized quadratures, respectively*).

Corollary 6.27. *If a system of Fuchsian differential equations with small coefficients is not triangular, then at least one of the components of almost every solution does not belong to the class of functions representable by single-valued $\mathcal{S}$-functions and quadratures* (*k-quadratures*, *generalized quadratures*, *respectively*).

Bibliography

[1] V. B. Alekseev, *Abel's theorem in problems and solutions*, MCCME, Moscow 2001. (Russian)

[2] V. I. Arnol'd, "Algebraic unsolvability of the problem of Ljapunov stability and the problem of the topological classification of the singular points of an analytic system of differential equations", *Funktsional. Anal. i Prilozhen.* **4**:3 (1970), 1–9; English transl., *Funct. Anal. Appl.* **4** (1970), 173–180.

[3] V. I. Arnol'd, "Superpositions", Selected Works of A. N. Kolmogorov, vol. I: Mathematics and Mechanics, Nauka, Moscow, 1985, pp. 444–451; English transl., Kluwer, Dordrecht, 1991, pp. 519–527.

[4] V. I. Arnol'd, "Topological proof of the transcendence of the Abelian integrals in Newton's *Principia*", *Istor.-Mat. Issled.* **31** (1989), 7–17. (Russian)

[5] V. I. Arnol'd, "Problèmes résolubles et problèmes irrésolubles analytiques et géométriques", Passion des Formes. Dynamique Qualitative Sémiophysique et Intelligibilité. Dédié à R. Thom, ENS Éditions, Fontenay–St Cloud 1994, pp. 411–417.

[6] V. I. Arnol'd, "Sur quelques problèmes de la théorie des systèmes dynamiques", *Topol. Methods Nonlinear Anal.* **4**:2 (1994), 209–225; Russian transl., Vladimir Igorevich Arnol'd. Selected Works–60, Fazis, Moscow 1997, pp. 533–551.

[7] V. I. Arnol'd, "I. G. Petrovskii, Hilbert's topological problems, and modern mathematics", *Uspekhi Mat. Nauk* **57**:4 (2002), 197–207; English transl., *Russian Math. Surveys* **57** (2002), 833–845.

[8] V. I. Arnol'd and O. A. Oleinik, "Topology of real algebraic varieties", *Vestnik Moskov. Univ. Ser.* I *Mat. Mekh.* **6** (1979), 7–17; English transl., *Moscow Univ. Math. Bull.* **34** (1979), 5–17.

[9] V. I. Arnol'd and V. A. Vassil'ev, "Newton's *Principia* read 300 years later", *Notices Amer. Math. Soc.* **36** (1989), 1148–1154; addendum, *Notices Amer. Math. Soc.* **37** (1990), 144.

[10] A. A. Bolibrukh, "The monodromy inverse problems of the analytic theory of differential equations", Mathematical Events of the 20th Century, Fazis, Moscow, 2003, pp. 53–79; English transl., Springer-Verlag, Berlin (to appear).

[11] A. A. Bolibrukh, *Fuchsian differential equations and holomorphic bundles*, MCCME, Moscow 2000. (Russian)

[12] D. B. Fuks, A. T. Fomenko, and V. L. Gutenmakher, *Homotopic topology*, Moscow State Univ., Moscow 1969; English transl., Publ. House of the Hungarian Academy of Sciences, Budapest 1986.

[13] V. V. Golubev, *Lectures on the analytic theory of differential equations*, 2nd ed., Gostekhizdat, Moscow–Leningrad 1950. (Russian)

[14] A. Hurwitz and R. Courant, *Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen*, 4th rev. aug. ed., Springer-Verlag, Berlin 1964; Russian transl., *Theory of functions*, Nauka, Moscow 1968.

[15] Yu. S. Il'yashenko and A. G. Khovanskii, *Galois theory of systems of Fuchsian differential equations with small coefficients*, preprint no. 117, Keldysh Institute of Applied Mathematics, Moscow 1974. (Russian)

[16] E. L. Ince, *Ordinary differential equations*, Longmans, London 1926; Russian transl., Gostekhizdat, Khar'kov 1939.

[17] I. Kaplansky, *An introduction to differential algebra*, Hermann, Paris 1957; Russian transl., Mir, Moscow 1959.

[18] A. G. Khovanskii, "The representability of algebroidal functions as compositions of analytic functions and one-variable algebroidal functions", *Funktsional. Anal. i Prilozhen.* **4**:2 (1970), 74–79; English transl., *Funct. Anal. Appl.* **4** (1970), 152–156.

[19] A. G. Khovanskii, "Compositions of holomorphic functions with radicals", *Uspekhi Mat. Nauk* **26**:2 (1971), 213–214. (Russian)

[20] A. G. Khovanskii, "The representability of functions by quadratures", *Uspekhi Mat. Nauk* **26**:4 (1971), 251–252. (Russian)
[21] A. G. Khovanskii, "The representability of functions by quadratures", Candidate (PhD) dissertation, Steklov Mathematical Institute, Moscow, 1973. (Russian)
[22] A. Khovanskij, "Topological obstructions for representability of functions by quadratures", *J. Dynam. Control Systems* **1**:1 (1995), 91–123.
[23] A. G. Khovanskii, "On the continuability of multivalued analytic functions to an analytic subset", *Funktsional. Anal. i Prilozhen.* **35**:1 (2001), 62–73; English transl., *Funct. Anal. Appl.* **35** (2001), 51–59.
[24] A. G. Khovanskii, "On the monodromy of a multivalued function along its ramification locus", *Funktsional. Anal. i Prilozhen.* **37**:2 (2003), 65–74; English transl., *Funct. Anal. Appl.* **37** (2003), 134–141.
[25] A. G. Khovanskii, "Multidimensional results on the nonrepresentability of functions by quadratures", *Funktsional. Anal. i Prilozhen.* **37**:4 (2003), 74–85; English transl., *Funct. Anal. Appl.* **37** (2003), 302–310.
[26] E. R. Kolchin, "Algebraic matric groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations", *Ann. of Math.* (2) **49** (1948), 1–42.
[27] E. R. Kolchin, "Galois theory of differential fields", *Amer. J. Math.* **75** (1953), 753–824.
[28] A. G. Kurosh, *Lectures in general algebra*, Fizmatgiz, Moscow 1962; English transl., (Pure Appl. Math., vol. 70) Pergamon Press, Oxford–Edinburgh–New York 1965.
[29] I. A. Lappo-Danilevskii, *Application of matrix functions to the theory of linear systems of ordinary differential equations*, Gostekhizdat, Moscow 1957. (Russian)
[30] J. Liouville, "Sur la détermination des intégrales dont la valeur est algébrique", *J. École Polytech. Paris* **14** (1833), 124–193.
[31] J. Liouville, "Mémoire sur l'intégration d'une classe de fonctions transcendentes", *J. Reine Angew. Math.* **13**:2 (1835), 93–118.
[32] J. Liouville, "Mémoire sur l'intégration d'une classe d'équations différentielles du second ordre en quantités finies explicites", *J. Math. Pures Appl. Sér.* I **4** (1839), 423–456.
[33] J. F. Ritt, *Integration in finite terms. Liouville's theory of elementary methods*, Columbia Univ. Press, New York 1948.
[34] M. Rosenlicht, "Liouville's theorem on functions with elementary integrals", *Pacific J. Math.* **24** (1968), 153–161.
[35] M. Rosenlicht, "On Liouville's theory of elementary functions", *Pacific J. Math.* **65** (1976), 485–492.
[36] M. F. Singer, "Formal solutions of differential equations", *J. Symbolic Comput.* **10**:1 (1990), 59–94.
[37] M. F. Singer, "Liouvillian solutions of nth order homogeneous linear differential equations", *Amer. J. Math.* **103** (1981), 661–682.

University of Toronto,
Moscow Independent University,
Institute for Systems Analysis, Russian Academy of Sciences,
E-mail: askold@math.toronto.edu

Received 30/MAR/04
Translated by IPS(DoM)