Topological **M**ethods in **N**onlinear **A**nalysis
Journal of the Juliusz Schauder Center
Volume 19, 2002, 237–256

NOTE ON THE DECK TRANSFORMATIONS GROUP AND THE MONODROMY GROUP

Henryk Żołądek

Abstract. For a ramified covering between Riemann surfaces the groups Deck of deck transformations and Mon of monodromy permutations are introduced. We associate with them groups of automorphisms of certain extensions of function fields. We study relations between these objects.

1. Introduction

The idea of Riemann surface (introduced by Riemann [11]) is one of the most classical and most fruitful in mathematics (see [4], [14]). For example, the conformal field theory and the quantum cohomology theory (see [2]) grew out of this idea.

Nevertheless some notions associated with Riemann surfaces seem to be not well established; in different sources they appear under different names and are studied from specific points of view. The author had encountered this state of affairs when working on the topological proof of the theorem of Abel and Ruffini (in [16]) and in studying the monodromy groups of first integrals of polynomial vector fields (in [15]). (The proof in [16] constitutes a reconstruction of some ideas from the book of Dubrovin, Novikov and Fomenko [3] and from the lectures of Arnold for talented high school students, written by one of the listeners in [1]).

2000 *Mathematics Subject Classification.* 14H30, 14H05, 30F20.

Key words and phrases. Riemann surfaces, monodromy group, Galois group, deck transformations group.

Supported by Polish KBN Grant No 2/P03A/041/15.

In both situations the main tool is the monodromy group Mon of the Riemann surface of the corresponding algebraic function, or of the first integral.

In classical books, like the Forster's [4], the notion of the group of deck transformations Deck plays dominant role. Also the notion of Galois covering (with few examples) is introduced there. In [4] there is no example of a covering which is not Galois.

The ramified coverings are intensively studied in hyperbolic geometry. (Here we shall use mainly the book of Kruskal, Apanasov and Gusevski ([8]) with many examples, but the reader is also referred to the book of Maskit ([9]).) There the Galois coverings appear under the name regular coverings and suitable examples are provided.

The group Deck is interpreted as an automorphism group of an algebraic extension of fields of rational functions on Riemann surfaces. The case of Galois covering corresponds to the case of Galois extension of fields.

It turns out that the group Mon also admits an algebraic interpretation. It serves as the automorphism of the extension of the field of rational functions on the target space by means of all branches of the corresponding algebraic function (see Theorem 1 below). The monodromy group of a general multi-valued holomorphic function was introduced by Khovanskiĭ ([7]). There the covering is infinite, but one assumes that the set of singular points is at most countable. One can introduce here also the notion of the group of deck transformations; moreover, the dimension of manifolds can be greater than 1. In [15] it was proven that Mon = Deck for the functions defining the liouvillian first integrals of polynomial differential systems.

One aim of this paper is to clarify the relation between the groups Mon and Deck. Usually Deck is smaller than Mon, but there is no natural inclusion. Only the equality Mon = Deck takes place in the case of Galois covering. We give necessary conditions for a finite covering to be a Galois covering. Other aim is to interpret of some algebraic notions (like primitive element, normal extension, Galois group) in terms of Riemann surfaces and their ramified coverings. At the end of this note we discuss multi-dimensional and infinite degree generalizations of the above theory created for algebraic functions.

2. A ramified covering associated with an algebraic function

By an *algebraic function* $y = f(x)$ on a Riemann surface N we mean a function defined by an equation

$$F(x,y) = y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x) = 0, \tag{1}$$

where $a_j(x) \in \mathbb{C}(N)$ are rational functions on N. (When $N = \mathbb{C}P^1$, then the equation (1) defines an algebraic function in usual sense, as a multi-valued function on $\mathbb{C}$. In the case of positive genus $g = g(N)$ of N we can treat N as an algebraic curve in some projective space $\mathbb{C}P^K$; the equation (1) holds in the affine variety $(N \cap \mathbb{C}^K) \times \mathbb{C} \subset \mathbb{C}P^{K+1}$ and N has several points at infinity.) We assume that the polynomial F is irreducible, $F \neq F_1 F_2$.

Take a generic point $a \in N$. Then the equation (1) with $x = a$ has n isolated solutions $y = b_1, \dots, b_n$. In a neighbourhood U_a of a there are well defined single-valued branches $f_1(x), \dots, f_n(x)$ of solutions to (1). The pairs (f_j, U_a) form *analytic elements* of the algebraic function $f(x)$. We prolong these elements along curves $\gamma \subset N \setminus \{x'_1, \dots, x'_r\}$ which starts at a and end at points $c \in N$; (the points x'_i are singular points of f, where two or more branches are glued together). We begin with an analytic element (f_a, U_a) and end-up with an analytic element (f_c, U_c). The union of analytic elements forms an open surface M^0 with a natural projection $p^0\colon M^0 \to N \setminus \{x'_1, \dots, x'_r\}$. M^0 is a part of the algebraic curve $\Gamma \subset \mathbb{C}P^{K+1}$ whose affine part is defined by (1). By irreducibility of F the surface M^0 is connected.

Next we complete M^0 to a closed surface M (in the topology defined by analytic elements, see [4]). Then the intersections of local branches are separated and the cusps are smoothed. M is a compact, connected and smooth surface equipped with a holomorphic map $p\colon M \to N$ which is a *ramified covering*. This means that for any *critical point* $y_j \in M$ of p with a *critical value* $x_i \in N$ we have $p(\xi) = \xi^v$ for some holomorphic charts centered at y_j and at x_i; the exponent v is the *ramification index* of y_j. We can identify the surface M with the normalization of the projective curve $\Gamma \subset \mathbb{C}P^{K+1}$; it is the strict transform for resolution of singularities of Γ. We call M the *Riemann surface associated with the algebraic function* $f(x)$. The multi-valued function $f\colon N \to \mathbb{C}$ is replaced by the single-valued function $\widetilde{f}\colon M \to \mathbb{C}$ (or, better, by a holomorphic map $\widetilde{f}\colon M \to \mathbb{C}P^1$) such that $\widetilde{f} = f \circ p$. The set $\{x_1, \dots, x_m\}$ of critical values of the projection constitutes the set of all singular (branching) points of f; (it is a subset of the set $\{x'_1, \dots, x'_r\}$ introduced above). The integer $n = \deg_y F$ is the *degree* of the covering, $n = \deg p$. We put $N' \stackrel{\text{def}}{=} N \setminus \{x_1, \dots, x_m\}$, $M' \stackrel{\text{def}}{=} p^{-1}(N')$ and $p' = p|_{M'}\colon M' \to N'$; p' is an non-ramified covering.

DEFINITION 1. The *monodromy group* $\mathrm{Mon} = \mathrm{Mon}(f) = \mathrm{Mon}(M \to N)$ associated with the ramified covering $M \to N$ (or with an algebraic function f) is a subgroup of permutations $S(p^{-1}(a)) = S(n)$ of the set $p^{-1}(a) = \{b_1, \dots, b_n\}$, defined as follows. With any loop γ, which represents an element of the fundamental group $\pi_1(N', a)$, we associate the permutation $\Delta_\gamma\colon p^{-1}(a) \to p^{-1}(a)$ such that each $\Delta_\gamma(b_i)$ is the result of analytic prolongation of the analytic element (f_i, U_a) along γ. By definition, $\mathrm{Mon} = \{\Delta_\gamma \in S(n) : \gamma \in \pi_1(N', a)\}$. We treat also elements of Mon as permutations of the branches $f_1(x), \dots, f_n(x)$ over U_a.

Theorem 1. *Consider the fields* $\mathbb{K} = \mathbb{C}(N)$ *and* $\mathbb{L}_1 = \mathbb{K}(f_1, \dots, f_n)$ *(adjoining the branches* $f_j(x)$*); we treat these fields as fields of functions on* U_a*. Then we have*

$$\mathrm{Mon}(f) \simeq \mathrm{Aut}(\mathbb{K} \subset \mathbb{L}_1).$$

Proof. Elements from the group Mon act on the functions from $\mathbb{L}_1$ by means of analytic continuation. Any element from $\mathbb{L}_1$ represents an algebraic function on $\mathbb{C}$ with finite number of singular points ($\subset \{x_1, \dots, x_m\}$) and there is no problem with continuation. The continuation is compatible with algebraic operations and therefore induces an automorphism of $\mathbb{L}_1$. This automorphism is generated by a permutation of the branches f_i. Of course, the continuation acts trivially on rational functions on N. All this leads to the inclusion Mon $\subset$ $\mathrm{Aut}(\mathbb{K} \subset \mathbb{L}_1)$.

Suppose that Mon $\neq \mathrm{Aut}(\mathbb{K} \subset \mathbb{L}_1)$. By the fundamental theorem of Galois theory (see Theorem 6 below) the group Mon is associated with an intermediary field $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}_1$, such that $\mathrm{Aut}(\mathbb{M} \subset \mathbb{L}_1) = \mathrm{Mon}$ and $\mathbb{M} = \mathbb{L}^{\mathrm{Mon}} = \{h \in \mathbb{L}_1 : \mathrm{Mon}\,(h) = \{h\}\}$. The field $\mathbb{M}$ consists of those functions which are invariant with respect to the analytic continuation (monodromy). Therefore they are single-valued functions. Their singularities are regular (of power type), also at infinity. From this it is easy to deduce that they are rational (by Riemann's theorem about removable singularities). This means that $\mathbb{M} = \mathbb{K}$ (a contradiction). $\square$

Definition 2. The *deck transformations group* of the algebraic function f (or of the covering $M \to N$) consists of homeomorphisms $\Phi' \colon M' \to M'$ (where $M' = p^{-1}(N \setminus \textit{singularities})$ which preserve fibers, i.e. $\Phi' \circ p' = p'$. (Of course, any such Φ' is analytic). This group is denoted by

$$\mathrm{Deck} = \mathrm{Deck}(f) = \mathrm{Deck}(M \to N).$$

Theorem 2.

(a) *Any* $\Phi' \in \mathrm{Deck}$ *is prolonged in an uniquely way to a holomorphic diffeomorphism* Φ *of the complete surface* M*.*

(b) *Let* $\mathbb{K} = \mathbb{C}(N)$ *(as above) and* $\mathbb{L}_2 = \mathbb{C}(M)$*. We embed* $\mathbb{C}(N)$ *into* $\mathbb{C}(M)$ *using the induction homomorphism* p^**. Then we have*

$$\mathrm{Deck}(M \to N) \simeq \mathrm{Aut}(\mathbb{K} \subset \mathbb{L}_2).$$

Proof. The point (a) follows from the Riemann's theorem about removable singularities.

(The point (b) is proven also in [4]). The embeddings of p^* is obvious: $h \circ p \equiv 0 \ \Rightarrow \ h \equiv 0$. Of course, any $\Phi \in \mathrm{Deck}$ defines the automorphism Φ^* of $\mathbb{C}(M)$, which is trivial on functions which are constant on fibers of p; thus

$\mathrm{Deck}(f) \subset \mathrm{Aut}(\mathbb{K} \subset \mathbb{L}_2)$. Consider an automorphism $\sigma \in \mathrm{Aut}(\mathbb{K} \subset \mathbb{L}_2)$. We apply it to the function $\widetilde{f}: M \to \mathbb{C}$, which defines the algebraic function f by $\widetilde{f} = f \circ p$. Then $(\sigma f) \circ p: N \to \mathbb{C}$ is a multi-valued function on N with algebraic singularities and defines a Riemann surface M_1. The surface M_1 is associated with the same algebraic equation (1) as M, i.e. $F(x, y) = 0$; (we can treat the latter as $F(T) = 0,\ F \in \mathbb{K}[T]$). But the Riemann surface M is unique up to a fiber isomorphism. This shows that M_1 is fiber isomorphic to M. That in order defines a deck transformation $\Phi: M \to M$. $\square$

Theorem 3.

(a) *We have the representations*

$$\mathrm{Mon} \simeq \pi_1(N', a) \Big/ \bigcap_j \mathrm{Stab}(b_j) = \pi_1(N', a) \Big/ \bigcap_{\gamma \in \pi_1(N', a)} \gamma \cdot p_* \pi_1(M', b_1) \cdot \gamma^{-1} \tag{2}$$

and

$$\mathrm{Deck} \simeq \mathrm{Norm}(p_* \pi_1(M', b_1))/p_* \pi_1(M', b_1) \tag{3}$$

where $\mathrm{Stab}(b_j) = \{\gamma \in \pi_1(N', a) : \Delta_\gamma b_j = b_j\}$ *is the stabilizer of* b_j *and the normalizer of* $p_* \pi_1(M', b_1)$ *in* $\pi_1(N', a)$, $\mathrm{Norm}(p_* \pi_1(M', b_1))$ *is equal* $\{\gamma \in \pi_1(N', a) : \gamma \cdot p_* \pi_1(M', b_1) \cdot \gamma^{-1} = p_* \pi_1(M', b_1)\}$.

(b) *In particular, the equality*

$$\mathrm{Deck} = \mathrm{Mon}$$

holds if and only if $p_* \pi_1(M', b_1)$ *is a normal subgroup of* $\pi_1(N', a)$.

Proof. (The formula (2) an be found in [3] and in [7]. The formula (3) is well known, see [8] and [9].)

(a) The homomorphism $\Delta: \pi_1(N', a) \to \mathrm{Mon} \subset S(p^{-1}(a))$ is given by the action of $\pi_1(N', a)$ on the fiber $p^{-1}(a) = \{b_1, \ldots, b_n\}$. This action is transitive, i.e. for any $b_i \neq b_j$ there exists a monodromy map Δ_γ such that $\Delta_\gamma(b_i) = b_j$. This follows from connectivity of M' (the points b_i and b_j are connected by a path $\delta \subset M'$ whose projection is the loop γ). Next, Mon is uniquely determined by the actions of $\pi_1(N', a)$ on each element b_i; the trivial element from Mon arises from the intersection of all stabilizers of the points b_i. This gives the identity $\mathrm{Mon} \simeq \pi_1 / \bigcap$stabilizers. The stabilizer of b_i equals $p_* \pi_1(M', b_i)$; (it consists of those loops in N' which ale lifted to closed loops through b_i). By transitivity any two stabilizers (e.g. of b_i and b_j) are conjugated (by means of the above loop γ). Thus we get the formula (2).

Let Φ be a deck transformation. It is uniquely defined by its restriction to any open subset of M'. Take such a subset in the form V_{b_1} = *component of* $p^{-1}(U_a)$ *containing* b_1. Let $V_{b_j} = \Phi(V_{b_i})$. We choose a monodromy map Δ_γ such that $\Delta_{\gamma_0}(b_i) = b_j$ which we prolong fiberwise to the neighbourhood V_{b_1}. Of course, $\Phi|V_{b_1} = \Delta_{\gamma_0}|V_{b_1}$. Thus $\Delta_{\gamma_0}|V_{b_1}$ can be prolonged to a fiber diffeomorphism of M.

In order to show the identity (3), we must:

(i) distinguish those monodromy maps Δ_{γ_0} which can be prolonged from V_{b_1} to deck transformations, and

(ii) notice that the loops δ from $\pi_1(M', b_1)$ are projected to loops $\gamma = p(\delta)$ such that $\Delta_\gamma|V_{b_1} \equiv \mathrm{id}$ (they are prolonged to trivial elements in Deck).

Suppose that a monodromy map $\Delta_{\gamma_0}|V_{b_1}$ can be prolonged to a fiber diffeomorphism of M. We prolong Δ_{γ_0} along paths $\delta \subset M'$ which start at b_1. In particular, if $\delta \in \pi_1(M', b_1)$ with $p(\delta) = \gamma \in p_*\pi_1(M', b_1)$, then the prolongation gives a new diffeomorphism $\Delta_{\gamma^{-1}\gamma_0\gamma}|V_{b_1} = \Delta_{\gamma^{-1}}|V_{b_j} \circ \Delta_{\gamma_0}|V_{b_1} \circ \Delta_\gamma|V_{b_1}$. The latter should coincide with $\Delta_{\gamma_0}\colon V_{b_1} \to V_{b_j}$. Thus $\Delta_{\gamma^{-1}}|V_{b_j} = \mathrm{id}\colon V_{b_j} \to V_{b_j}$, $\Delta_{\gamma_0\gamma}|V_{b_1} = \Delta_{\gamma\gamma_0}|V_{b_1}$ and hence $\Delta_{\gamma_0^{-1}\gamma\gamma_0}|V_{b_1} = \Delta_\gamma|V_{b_1} = \mathrm{id}$. This means that $\gamma_0\gamma\gamma_0^{-1} \in p_*\pi_1(M', b_1)$. So $\gamma_0 \in \mathrm{Norm}(p_*\pi_1(M', b_1))$.

(b) The property (b) easily follows from the formulas (2) and (3). □

REMARK 1. The proof of the formula (3) does not suggest that the group Deck can be included into the group Mon. We have associated to a $\Phi \in$ Deck a map $\Delta_{\gamma_0}|V_{b_1}$, but we have not shown that $\Phi|V_{b_i} = \Delta_{\gamma_0}|V_{b_i}$ when b_i is not in the same orbit of Deck as b_1.

DEFINITION 3. A ramified covering $M \xrightarrow{p} N$ is called the *Galois covering* if the group Deck acts transitively on the noncritical fiber $p^{-1}(a)$. Galois coverings are sometimes called the normal coverings (see [4]), or regular coverings (see [8] and [3]).

PROPOSITION 1. *The following conditions:*

(a) *the group* $p_*\pi_1(M', b_1)$ *is a normal subgroup of* $\pi_1(N', a)$, *i.e.* Deck = Mon,

(b) $|\mathrm{Deck}| = n = \deg p$,

are equivalent to the condition that a covering $M \xrightarrow{p} N$ *is a Galois covering.*

PROOF. (a) The group $p_*\pi_1(M', b_1)$ is a normal subgroup of $\pi_1(N', a)$ if and only if all the stabilizers of points b_j in $\pi_1(N', a)$ (i.e. $p_*\pi_1(M', b_j)$) are equal. Then the normalizer of $p_*\pi_1(M', b_1)$ is equal to $\pi_1(N', a)$.

If $p_*\pi_1(M', b_1)$ is a normal subgroup of $\pi_1(N', a)$, then by (2) and (3) Mon = Deck; hence the group Deck acts transitively on the distinguished fiber.

Assume that $p_*\pi_1(M', b_1)$ is not normal in $\pi_1(N', a)$. Then there are two different stabilizers $p_*\pi_1(M', b_1) \neq p_*\pi_1(M', b_j)$. Suppose that Deck acts transitively on the set $\{b_1, \dots, b_n\}$; in particular b_1 and b_j are in one orbit of the action of Deck, $b_j = \Phi(b_1)$. Let $\Phi|V_{b_1} = \Delta_{\gamma_0}|V_{b_1}$ (like in the proof of the formula (3) from Theorem 3). Then the formulas $\Delta_{\gamma^{-1}\gamma_0\gamma}|V_{b_1} = \Delta_{\gamma_0}|V_{b_1}$ and $\Delta_\gamma|V_{b_j} = \mathrm{id}$ for $\gamma \in p_*\pi_1(M', b_1)$ show that the stabilizers of b_1 and b_j coincide, a contradiction.

(b) Because any transformation from Deck is defined by its value on b_1 and there are at most n of them, then $|\mathrm{Deck}| \leq n$. The equality $|\mathrm{Deck}| = n$ holds only in the case of transitivity of Deck. (Note also that for Galois coverings we have the equalities $|\mathrm{Mon}| = |\pi_1(N')/p_*\pi_1(M')| = |p^{-1}(a)|$.) $\square$

It would be nice if one had a direct criterion of Galois property for ramified coverings. Such criterion should be expressed in local terms of the algebraic curve $F(x, y) = 0$.

Definition 4 ([8]). We say that a ramified covering $p: M \to N$ is *of regular type* if for any critical value $x_i \in N$ all the critical points y_j in the fiber $p^{-1}(x_i)$ have the same ramification index, i.e. we have $p(\xi_j) - x_i = \xi_j^v$ for some local charts ξ_j in M with center at y_j.

Theorem 4.

(a) *If a covering $p: M \to N$ is Galois, then it is of regular type.*

(b) *If N is simply connected (i.e. $N = \mathbb{C}P^1$), then $p: M \to N$ is Galois if and only if it is of regular type.*

Proof. (The point (a) of this theorem can be found in [8] and the point (b) was proven by Greenberg in [5]).

(a) Assume that the group Deck acts transitively on any non-critical fiber. Let x_i be a critical value of the map p and let $y_1 \in p^{-1}(x_i)$ has the ramification index v_1. Thus $p(\xi_1) = x_i + \xi^{v_1}$ for a local chart $\xi_1: W_1 \to \mathbb{C}$, $\xi_1(y_1) = 0$. We choose the base point $a \in N$ from the neighbourhood $Z = p(W_1)$ of x_i. Then the set $p^{-1}(a) \cap W_1$ contains v_1 points $b_k = (a - x_i)^{1/v_1} e^{2\pi i k/v_1}$, $k = 1, \dots, v_1$. By transitivity of Deck there exists a transformation $\Phi_1: M \to M$ such that $\Phi_1(b_1) = b_2$, of course, $\Phi_1 = \Delta_{\gamma_i}$ where γ_i is the loop around x_i.

Suppose that $p^{-1}(x_i)$ contains another critical point $y_2 \neq y_1$ with the ramification index v_2 and the local chart ξ_2 in a neighbourhood W_2.

Let $b_{v_1+1}, \dots, b_{v_1+v_2}$ be the points from $p^{-1}(a)$ near y_2. There exists $\Psi \in$ Deck such that $\Psi(b_{v_1+1}) = b_1$. Consider the map $\Phi_2 = \Psi^{-1} \circ \Phi_1 \circ \Psi \in \mathrm{Deck}$. It defines a cyclic permutation τ of the set $\{b_{v_1+1}, \dots, b_{v_1+v_2}\}$. We have $\tau^{v_1} = \mathrm{id}$, what implies that v_2 divides v_1, $v_2|v_1$. By changing the roles of y_1 and y_2 we get $v_1|v_2$. Hence $v_1 = v_2$.

(b) If $\pi_1(N, a) = 0$, then $\pi_1(N', a)$ is generated by the loops γ_i around the critical values x_i, $i = 1, \dots, m$. Therefore it is enough to show that the monodromy maps Δ_{γ_j} can be prolonged to fiber automorphisms of M. For this it is enough to prove the following.

Let $y_1, y_2 \in p^{-1}(x_i)$ (with local charts $\xi_{1,2}: W_{1,2} \to \mathbb{C}$ and with the base point $a \in Z = p(W_{1,2})$) and let δ be a path in M joining y_2 with y_1 and omitting critical points on the way. Thus $\gamma = p(\delta)$ is a loop in $\pi_1(N\backslash\{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m\}, x_i)$ which induces a map $\Delta_\gamma: W_2 \to W_1$. What we need is the identity

$$\Delta_\gamma^{-1} \circ \Delta_{\gamma_i} \circ \Delta_\gamma|_{W_2} = \Delta_{\gamma_i}|_{W_2}. \tag{4}$$

But this is obvious, as the both maps in (4) are rotations by the same angle $2\pi/v_1 = 2\pi/v_2$ in the chart ξ_2. □

The notion of Galois covering takes its origin from algebra. In the next section we present some elements of the theory of fields and their extensions.

3. Algebraic Galois theory

In this paper we assume that all fields have characteristic zero. In fact they are fields of functions on complex varietes. All the below algebraic results are taken from the book of Waerden ([13]).

DEFINITION 5. An extension $\mathbb{K} \subset \mathbb{L}$ of algebraic fields is called *normal* if for any element $\beta \in \mathbb{L}$ with its minimal polynomial $g(T) = (T-\beta_1)(T-\beta_2)\dots(T-\beta_r) \in \mathbb{K}[T]$, $\beta_1 = \beta$ (where β_j belong to the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$) all the roots β_j also belong to $\mathbb{L}$. Equivalently, $\mathbb{K} \subset \mathbb{L}$ is normal if and only if $\mathbb{L}$ is obtained from $\mathbb{K}$ by adjoining all roots of finite number of polynomials from $\mathbb{K}[T]$; if the extension is finite, then one polynomial is sufficient.

An extension $\mathbb{K} \subset \mathbb{L}$ is called the *Galois extension* if it is normal and separated; (the latter means that $g'(\beta) \neq 0$ for the minimal polynomial $g(T)$ of any $\beta \in \mathbb{L}$). Because in the characteristic zero all extensions are separated, the notions of normal extension and Galois extension are the same.

The automorphism group of a Galois extension is called the *Galois group* and is denoted by $\mathrm{Gal} = \mathrm{Gal}(\mathbb{K} \subset \mathbb{L})$ (or $\mathrm{Gal}_{\mathbb{K}}\mathbb{L}$, or $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$).

For an extension $\mathbb{K} \subset \mathbb{L}$ an element $\alpha \in \mathbb{L}$ is called *primitive* if $\mathbb{L} = \mathbb{K}(\alpha)$. If a primitive element exists, then the extension is called *simple*.

THEOREM 5.

(a) *Any extension of the form $\mathbb{L} = \mathbb{K}(\beta_1, \dots, \beta_r)$ is simple. In particular, any finite Galois extension is of the form $\mathbb{L} = \mathbb{K}(\alpha)$.*

(b) *Let $\mathbb{L} = \mathbb{K}(\alpha)$. Then any element σ of the group* $\mathrm{Aut}(\mathbb{K} \subset \mathbb{L})$ *is uniquely defined by the value $\sigma(\alpha) = \alpha_i$, where α_i is a root of the minimal polynomial $g(T)$ for α which lies in $\mathbb{L}$. Therefore*

$$|\mathrm{Aut}(\mathbb{K} \subset \mathbb{L})| \leq [\mathbb{L} : \mathbb{K}] \stackrel{\mathrm{def}}{=} \dim_{\mathbb{K}} \mathbb{L}$$

and the equality holds only when the extension is Galois. In the latter case the group Gal *acts transitively on the roots of the minimal polynomial* $g(T)$*.*

(c) *If* $\mathbb{K} \subset L$ *is Galois, then* $\mathbb{L}^{\mathrm{Gal}} \stackrel{\mathrm{def}}{=} \{\beta \in \mathbb{L} : \mathrm{Gal}(\beta) = \{\beta\}\} = \mathbb{K}$*.*

Proof. It is enough to prove the point (a) for $r = 2$; next we use induction. So, assume that $\mathbb{L} = \mathbb{K}(\beta, \gamma)$ and let $\beta_1 = \beta, \beta_2, \dots, \beta_k$ and $\gamma_1 = \gamma, \gamma_2, \dots, \gamma_l$ be the conjugate elements (in the algebraic closure of $\mathbb{K}$), the roots of the minimal polynomials $f(T)$ and $g(T)$, respectively. We put the primitive element in the form $\alpha = \beta + a\gamma$, where $a \in \mathbb{K}$ is such that $\beta_i + a\gamma_j \neq \beta + a\gamma$ for all i and $j \neq 1$. We have to show that $\gamma \in \mathbb{K}(\alpha)$.

The element γ is a common root of the two polynomials $g(T)$ and $f(\alpha - aT)$, both from $\mathbb{K}(\alpha)[T]$. By the above assumption it is unique such common root, and the greatest common divisor of these polynomials is just $T - \gamma$. Because $\gcd(g(T), f(\alpha - aT)) \in \mathbb{K}(\alpha)[T]$, the coefficient $\gamma \in \mathbb{K}(\alpha)$.

(b) Let $g(T) = (T - \alpha_1) \dots (T - \alpha_n) \in \mathbb{K}[T]$ be the minimal polynomial for the primitive element $\alpha = \alpha_1$. The vector space $\mathbb{L} = \mathbb{K}(\alpha) = K[T]/(g(T))$ over $\mathbb{K}$ has the basis $1, \alpha, \dots, \alpha^{n-1}$. Therefore any automorphism σ of $\mathbb{L}$ over $\mathbb{K}$ is determined by its value on α. Of course, $\sigma(\alpha) = \alpha_i$ for some i and it extends to an isomorphism $\mathbb{K}(\alpha_1) \to \mathbb{K}(\alpha_i)$. However, we can take only those σ for which $\alpha_i \in \mathbb{L}$; thus the inequality $|\mathrm{Aut}| \leq n$. The equality holds when all $\alpha_i \in \mathbb{L}$, what means normality; of course, then $\mathrm{Aut} = \mathit{Gal}$ acts transitively on the roots.

(c) follows from (b). □

Corollary. *A ramified extension* $p: M \to N$ *is Galois if and only if the extension* $\mathbb{K} = \mathbb{C}(N) \subset \mathbb{C}(M) = \mathbb{L}_1$ *is Galois.*

Proof. By Proposition 1(b) and Theorem 2 p is Galois if and only if

$$|\mathrm{Aut}(\mathbb{C}(N) \subset \mathbb{C}(M))| = |\mathrm{Deck}| = n = \deg p.$$

But the extension $\mathbb{K} \subset \mathbb{L}_2$ is simple, $\mathbb{L}_2 = \mathbb{K}(T)/g(T) = \mathbb{K}(f)$, and $[\mathbb{C}(M) : \mathbb{C}(N)] = n$. Now it is enough to apply Theorem 5(b). □

Theorem 6 (Fundamental theorem of Galois theory). *Let* $\mathbb{K} \subset \mathbb{L}$ *be a Galois extension. There exists a one-to-one correspondence between the intermediary fields* $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$ *and the subgroups* $H \subset G = \mathrm{Gal}(\mathbb{K} \subset \mathbb{L})$ *given by the maps*

$$M \to H = \mathrm{Gal}(\mathbb{M} \subset \mathbb{L}), \quad H \to \mathbb{M} = \mathbb{L}^H.$$

Proof. We have to show that the compositions

$$\mathbb{M} \to H \to \mathbb{L}^H \quad \text{and} \quad H \to \mathbb{M} \to \mathrm{Gal}(\mathbb{M} \subset \mathbb{L})$$

are identities. Note that above the extensions $\mathbb{M} \subset \mathbb{L} = \mathbb{K}(\alpha) = \mathbb{M}(\alpha)$ are also Galois.

The inclusions $\mathbb{M} \subset \mathbb{L}^H$ and $H \subset \mathrm{Gal}(\mathbb{M} \subset \mathbb{L})$ are obvious. The equality $\mathbb{L}^H = \mathbb{M}$ follows from Theorem 5(c). Finally, suppose $H \neq H_1 = \mathrm{Gal}(\mathbb{L}^H \subset \mathbb{L})$; then $[G : H_1] = [\mathbb{L} : \mathbb{L}^H]$. But the equality $\mathbb{M} = \mathbb{L}^{\mathrm{Gal}(\mathbb{M} \subset \mathbb{L})}$ for $\mathbb{M} = \mathbb{L}^H$ implies that $\mathbb{L}^{H_1} = \mathbb{L}^H$. Thus $[G : H_1] = [G : H]$ and the inclusion $H \subset H_1$ gives $H = H_1$. $\square$

In Theorem 1 we have considered the extension

$$\mathbb{K} = \mathbb{C}(N) \subset \mathbb{L}_1 = \mathbb{K}(f_1, \dots, f_n)$$

associated with any covering, Galois or not. Recall also that $\mathbb{L}_2 = \mathbb{C}(M)$. The branches f_j are all the roots of the polynomial $g(T) = F(x, T) \in \mathbb{K}[T]$. This and Theorem 6 give the following proposition; (for the point (b) one uses the identity Deck = Mon for Galois coverings).

Proposition 2.

(a) *The extension* $\mathbb{K} \subset \mathbb{L}_1$ *is Galois.*

(b) *The equality* $\mathbb{L}_2 = \mathbb{L}_1$ *holds only for Galois coverings.*

Remark 2. Although the field $\mathbb{L}_2 = \mathbb{C}(M)$ is clearly smaller that $\mathbb{L}_1$, we do not have any inclusion. The reason is that elements of $\mathbb{C}(M)$, e.g. $\widetilde{f}$, cannot be treated as multivalued functions on some open subset, e.g. on U_a. We cannot decide which of the (generally) non-equivalent branches to choose. In the case of Galois covering all the branches appear at equivalent footing. Compare also Remark 1.

There appears the natural question about realization of the field $\mathbb{L}_1$ as a field of rational functions on some surface S covered over N. One wants to get S as a Riemann surface of an algebraic function $h(x)$. We should have $\mathbb{L}_1 = \mathbb{K}(h)$, i.e. h should be a primitive element. The choice of primitive element is dictated by the proof of Theorem 5(a). Namely one puts

$$h(x) = f_1(x) + b_2(x) f_2(x) + \ldots + b_n(x) f_n(x) \tag{5}$$

for some rational functions $b_j(x) \in \mathbb{C}(N)$. The function $z = h(x)$ satisfies an algebraic equation $H(x, z) = 0$ of degree $|\mathrm{Mon}(M \to N)|$ with respect to z and the covering $S \to N$ is a Galois covering. In the next section we present this construction in an example (Example 3).

4. Examples

Here we present examples illustrating the theoretical statements and constructions from the previous two sections.

Example 1 (Generic algebraic function). Let the polynomial $F(x,y)$, which defines an algebraic function $y = f(x)$, be typical. Then the projective curve $\Gamma \subset \mathbb{C}P^2$ defined by $F = 0$ is smooth (hence connected and irreducible) and the restriction of the projection $(x,y) \to x$ to $\Gamma \cap \mathbb{C}^2$ has only non-degenerate (Morse) critical points with different critical values.

The group Mon is generated by transpositions (of two branches glued at critical points) and is transitive. This implies that Mon $= S(n)$ (see [16]). (This fact, together with non-solvability of $S(n)$, $n \geq 5$ and solvability of the monodromy group of functions expressed by radicals, gives the topological proof of the Abel–Ruffini theorem; see [1] and [16].)

On the other hand, the corresponding covering is manifestly not of regular type (there is only one critical point in each critical fiber). Thus $M \to N$ is not Galois (Theorem 4(a)). We have Deck $= \{e\}$, in fact.

(We see here that the group Deck is not very useful in applications.)

Example 2. The cubic equation

$$y^3 - 3y - 2x = 0, \tag{6}$$

although gives a singular curve (cusp at infinity), has all the features of the general algebraic equation from Example 1. Here we are able to provide suitable formulas.

Using the Cardano formula

$$y = \left(-\frac{q}{2} + \left(\frac{q^2}{4} + \frac{p^3}{27} \right)^{1/2} \right)^{1/3} + \left(-\frac{q}{2} - \left(\frac{q^2}{4} + \frac{p^3}{27} \right)^{1/2} \right)^{1/3}$$

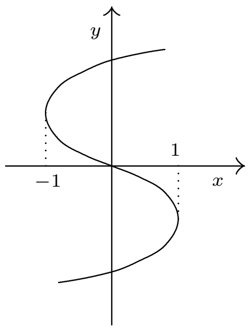
(with 36 branches) we get three solutions which, for x real and close to 0, take the form

$$f_{0,1,2}(x) = -i[\zeta_{0,1,2}(\sqrt{1-x^2} - ix)^{1/3} - \bar{\zeta}_{0,1,2}(\sqrt{1-x^2} + ix)^{1/3}] \tag{7}$$

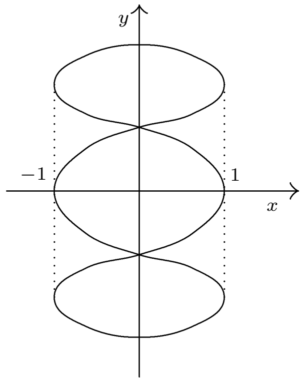
where $\zeta_0 = 1$, $\zeta_{1,2} = -1/2 \pm i\sqrt{3}/2$ are the cubic roots of unity and all the square and cubic roots in (7) are positive for $x = 0$. We have $f_0 = -2/3x + \dots$, $f_{1,2} = \pm\sqrt{3} + \dots$ for $x \to 0$, as expected from (6).

The curve (6) is presented at Figure 1(a). There are two finite critical points of the projection: $(x,y) = \pm(1,-1)$. Both are ramification points of the covering of index 2. There is one more ramification point at infinity, of index 3. Because $p^{-1}(\pm 1)$ contains regular point and ramification point, the covering is not of regular type; hence not Galois.

Therefore, the extension $\mathbb{K} \subset \mathbb{L}_2$ is not Galois. Here the both surfaces M and N are rational; M is parametrized by y. Thus $\mathbb{L}_2 = \mathbb{C}(y)$ and $\mathbb{K} = \mathbb{C}(x) \simeq \mathbb{C}(y^3 - 3y) \subset \mathbb{C}(y)$. Any automorphism σ of the field $\mathbb{C}(y)$ is the change $y \to (ay+b)/(cy+d)$ induced by a Möbius transformation Φ of $M = \mathbb{C}P^1$. The



(a)



(b)

Figure 1

fact that σ is trivial on the subfield $\mathbb{C}(y^3-3y)$ means that Φ is constant on the fibers of p. Φ must keep fixed the three ramification points $y=\pm1,\infty$ (they are unique in the critical fibers). Only $\Phi=\mathrm{id}$ satisfies this condition. In this way we confirm the triviality of the group of deck transformations, $\mathrm{Deck}=\{e\}$. On the other hand, we know that $\mathrm{Mon}=S(3)$.

Here we can see why $\mathrm{Deck}\not\subset\mathrm{Mon}$ and $\mathbb{L}_2\not\subset\mathbb{L}_1$. If it were so, then we would have $\mathbb{L}_2=\mathbb{L}_1^{\mathrm{Deck}}=\mathbb{L}_1$ with $\mathrm{Aut}(\mathbb{K}\subset\mathbb{L}_2)=\mathrm{Mon}$.

As we know, the extension $\mathbb{K}\subset\mathbb{L}_1=\mathbb{K}(f_1,\dots,f_n)$ associated with Example 1 (or Example 2) is normal (we adjoin all the roots of the polynomial $F(x,T)\in\mathbb{K}[T]$). Theorem 5(a) says that $\mathbb{L}_1=\mathbb{K}(h)$ for a primitive element $h\in\mathbb{L}_1$. This element represents an algebraic function $z=h(x)$ on N and satisfies an algebraic equation $G(x,z)=z^d+b_{d-1}(x)z+\dots+b_0(x)=(z-h_1(x))\dots(z-h_d(x))=0$, $h_1=h$. The degree $d=|\mathrm{Gal}(\mathbb{K}\subset\mathbb{L}_1)|$. We associate with $z=h(x)$ its Riemann surface $S=M(h)$ with a covering $q{:}\,S\to N$. We have a single-valued function $\widetilde{h}{:}\,S\to\mathbb{C}$ such that $\widetilde{h}=h\circ q$. Of course, $\widetilde{h}\in\mathbb{C}(S)$, where the latter field is isomorphic to $\mathbb{L}_1$. We have $\mathrm{Deck}(S\to N)=\mathrm{Aut}(\mathbb{K}\subset\mathbb{C}(S))=\mathrm{Aut}(\mathbb{K}\subset\mathbb{L}_1)\simeq\mathrm{Mon}(S\to N)$ and the covering $S\to N$ is Galois. The element h should be chosen in the form $h(x)=f_1(x)+c_2(x)f_2(x)+\dots+c_n(x)f_n(x)$, $c_j\in\mathbb{K}(N)$ (see (5)).

Example 3 (Example 2 revisited). Because $f_0(x)+f_1(x)+f_2(x)=0$ in (6) and (7), we have $\mathbb{L}_1=\mathbb{K}(f_1,f_2)=\mathbb{C}(x,f_1(x),f_2(x))$. We choose

$$h(x)=f_1(x)-f_2(x).$$

Using the formulas $f_1+f_2=-f_0$, $f_1f_2+f_0(f_1+f_2)=-3$, i.e. $f_1f_2=f_0^2-3$, we express the functions h^2, h^4, h^6 in terms of x and f_0. They turn out to be dependent; namely, $z = h(x)$ satisfies the equation

$$G(x,z) = z^2(z^2-9)^2 + 108(x^2-1) = 0.$$

The curve $G(x,z)=0$ is drawn at Figure 1(b). We see that above $x=\pm 1$ there are three ramification points (with index 2). Above $x=0$ the curve $G=0$ is singular. But these singularities are the simple double points; the two local components are separated in the Riemann surface S. There are also ramification points above $x=\infty$. We have there two local components $z^3 \pm i\sqrt{108}x + \ldots = 0$, each containing a ramification point with index 3. We see that the covering $S \to N = \mathbb{C}P^1$ is of regular type, hence Galois (by Theorem 4(b)). Moreover, the Riemann–Hurwitz formula $d\cdot\chi(N) = \chi(S) + \sum_{z\in S}(v(z)-1)$ shows that $\chi(S)=2$; i.e. $S=\mathbb{C}P^1$.

We shall construct explicitly the deck transformations generating the group $\mathrm{Deck}(S\to N)\simeq S(3)$. For this we need certain parametrization of $S=\mathbb{C}P^1$. We use the formula

$$f_2^2 + f_1 f_2 + {f_1}^2 = 3$$

(following from $(f_1+f_2)^2 = f_0^2$, $f_1 f_2 = f_0^2 - 3$). We have $(f_2-\zeta f_1)(f_2-\overline{\zeta} f_1) = 3$, $\zeta = -1/2 + i\sqrt{3}/2$ and we put $f_2 - \zeta f_1 = -i\sqrt{3}t$, $f_2 - \overline{\zeta} f_1 = i\sqrt{3}t^{-1}$. This gives

$$f_1 = t + t^{-1}, \quad f_2 = \overline{\zeta}t + \zeta t^{-1}, \quad f_0 = \zeta t + \overline{\zeta} t^{-1}.$$

and the desired parametrization of the surface S

$$z = f_1 - f_2 = (1-\overline{\zeta})t + (1-\zeta)t^{-1}, \quad x = \frac{1}{2} f_0(t) f_1(t) f_2(t).$$

The algebraic function $z = h(x)$ has 6 branches

$$\begin{aligned} h_1 &= f_1 - f_2, & h_2 &= f_2 - f_1, & h_3 &= f_0 - f_2, \\ h_4 &= f_2 - f_0, & h_5 &= f_1 - f_0, & h_6 &= f_0 - f_1. \end{aligned}$$

The monodromy map Δ_{γ_1}, corresponding to the loop γ_1 around the point x_1, acts as the transposition $\sigma_1 = (f_0 f_1) \in S(\{f_0, f_1, f_2\})$ of branches of the surface M. In the surface S we get the permutation

$$\tau_1 = (h_1 h_3)(h_2 h_4)(h_5 h_6) \in S(\{h_1, \ldots, h_6\}).$$

The latter permutation is given by the changes

$$\begin{aligned} (1-\overline{\zeta})t + (1-\zeta)t^{-1} &\to (\overline{\zeta}-\zeta)t + (\overline{\zeta}-\zeta)t^{-1}, \\ (1-\zeta)t + (1-\overline{\zeta})t^{-1} &\to (\zeta-1)t + (\overline{\zeta}-1)t^{-1}, \end{aligned}$$

which are induced by one transformation $\Phi_1 \colon t \to \overline{\zeta} t^{-1}$.

The monodromy Δ_{γ_2}, corresponding to the loop γ_2 around $x=-1$, gives the permutations $\sigma_2=(f_0 f_2)$ and

$$\tau_2=(h_1h_5)(h_2h_6)(h_3h_4)$$

where the latter is extended to the transformation $\Phi_2\colon t\to t^{-1}$. The involutions Φ_1 and Φ_2 generate the group $\mathrm{Deck}(S\to N)$.

EXAMPLE 4 (Galois coverings). Large class of Galois coverings is given by algebraic functions of the form

$$f(x)=R_1(x)^{\mu_1}+R_2(x)^{\mu_2}+\ldots+R_s(x)^{\mu_s}$$

where μ_j are positive rational numbers and the functions $R_j(x)$ are rational and such that their divisors of zeroes and poles (including those at infinity) are disjoint. For example,

$$f=\sqrt{x}+\sqrt[3]{(x-1)/(x+1)}.$$

If μ_j are irreducible ratios p_j/q_j and R_j are not powers, then we have

$$\mathrm{Mon}=\mathrm{Deck}=\mathbb{Z}_{q_1}\oplus\ldots\oplus\mathbb{Z}_{q_s}.$$

This follows directly from the construction of the Riemann surface of the function f by taking $q_1\cdot\ldots\cdot q_s$ copies of the complex plane, cut along radii from singularities of the summand functions and glued in a suitable way.

EXAMPLE 5 (The canonical map). Consider a hyperelliptic curve

$$y^2=P(x^2)$$

where the polynomial P has isolated zeroes different from $x^2=0$. It defines a Riemann surface M of genus $g=\deg P-1$.

Consider the *canonical map* $\iota\colon M\to\mathbb{C}P^{g-1}$, defined as follows (see [6]). Let

$$\omega_0=\frac{dx}{y},\quad \omega_1=\frac{x\,dx}{y},\quad \omega_{g-1}=\frac{x^{g-1}\,dx}{y}$$

be the basis of the space $H^{1,0}(M)=H^0(M,\Omega^1)\simeq\mathbb{C}^g$ of holomorphic 1-forms on M. We put

$$\iota(z)=(\omega_0(z):\omega_1(z):\ldots:\omega_{g-1}(z)),\quad z\in M$$

with the values in the projectivization of $H^{1,0}$. The map $\iota\colon M\to\iota(M)$ is the same as the 2-fold covering $p\colon M\to\mathbb{C}P^1$ associated with the algebraic function $\sqrt{P(x^2)}$.

The curve M admits two symmetries: $\Theta_1\colon(x,y)\to(x,-y)$ and $\Theta_2\colon(x,y)\to(-x,y)$. Because $\Theta_1^*\omega_j=-\omega_j$, we see that $\iota(z)=\iota(\Theta_1(z))$. The covering $\iota\colon M\to\iota(M)$ is the quotient map $M\to M/\Theta_1$.

Consider the family M_t of curves defined by

$$H(x,y) = t, \quad H = y^2 - P(x^2).$$

Take the meromorphic forms

$$\eta_1 = \frac{x\,dx}{y}, \quad \eta_2 = \frac{d\eta_1}{dH} = \frac{x\,dx}{2y^3}, \quad \eta_3 = \frac{d\eta_2}{dH}, \dots$$

Here the form $\nu = d\eta/dH$ is the *Gelfand–Leray form* on the curve $H = t$ such that $d\eta = \nu \wedge dH$. If $\delta(t)$ is a family of integer cycles in the Riemann surfaces $H = t$ and $I(t) = \int_{\delta(t)} \eta_1$ is an Abelian integral, then we have $d^j I/dt^j = \int_{\delta(t)} \eta_j$.

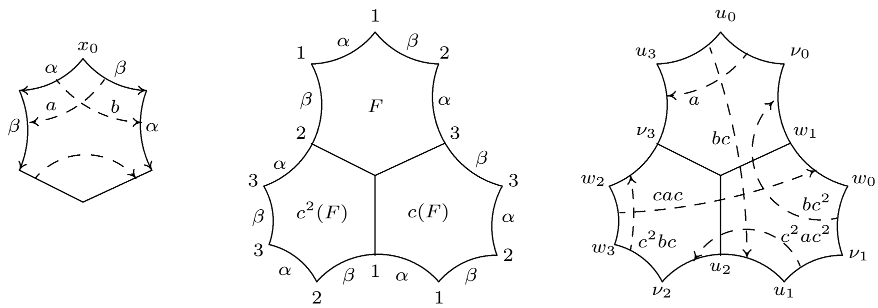
For any $k \geq 3$ the map

$$\rho\colon z \to (\eta_1(z) : \dots : \eta_k(z))$$

defines a ramified covering over a surface $N = \rho(M) \subset \mathbb{C}P^{k-1}$. Because $\Theta_1^* \eta_j = -\eta_j$ and $\Theta_2^* \eta_j = \eta_j$, the map ρ is constant on orbits of action of the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ generated by the two involutions. In fact, here $\mathrm{Deck}(\rho) = \mathrm{Mon}(\rho) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the covering is Galois.

This example is in fact a special case of Example 4; namely for $g(u) = \sqrt{P(u)} + \sqrt{u}$. The function g on M is equal to $x + y$ for $x = \sqrt{u}$.

Due to the symmetries $\Theta_{1,2}$ we have $\int_{\delta(t)} \eta_1 \equiv 0$, when the cycle $\delta(t)$ is represented by a real oval of the curve $H = t$ symmetric around the origin. Note that the form η_1 is not exact on the surface $H = t$ (because integrals over non-symmetric cycles do not vanish). We expect that always, whenever $\int_{\delta(t)} \eta \equiv 0$ for a non-exact η, the curves $H = t$ should reveal some symmetry.



(a) (b) (c)

Figure 2

Example 6 (Covering of regular type, but not Galois)). We use the Example 14 from the book [8]. There one constructs a 3-fold covering $p\colon M \to E$ over an elliptic curve E (torus) with only one critical point with ramification index 3 and one critical value x_1. M has genus 2. Of course, the covering is of regular type; $p^{-1}(x_1)$ is one point.

In order to proceed further, we need more information about the construction of this covering. Firstly, one realizes the curve E with distinguished point x_1 as an *orbifold*; this means that a small disc around x_1 is identified with $\{|z| < \varepsilon\}/\mathbb{Z}_3$. One puts $E = \mathbf{D}/\Gamma$ where $\mathbf{D} = \{|z| < 1\}$ is the simply connected hyperbolic surface and Γ is a Fuchsian group of isometries of $\mathbf{D}$ with generators a, b, c satisfying the relations

$$aba^{-1}b^{-1}c = c^3 = e. \tag{8}$$

(By a *Fuchsian group* Γ we mean the subgroup of index 2 in a group of isometries of $\mathbf{D}$ generated by inversions with respect to several circles orthogonal to the *absolute* $\partial\mathbf{D}$. This subgroup consists of maps which are compositions of even number of inversions and are Möbius maps preserving $\mathbf{D}$. Moreover, the Fuchsian group acts on $\mathbf{D}$ discontinously, i.e. the stabilizers of points are finite and isolated.

The (infinite) "universal" covering $\mathbf{D} \to \mathbf{D}/\Gamma$ is an example of Galois covering.)

The *fundamental domain* $F \subset \mathbf{D}$ of Γ with the action of the maps a, b, c is presented at Figure 2(a). The elliptic vertex x_1 with angle $2\pi/3$ is situated at the origin $x = 0$.

The relations (8) are responsible for the discreetness of Γ. This can be explained in terms of the images $g(F)$, $g \in \Gamma$ of the fundamental domain. These sets should meet only along their boundaries (no overlapping); they form a partition of $\mathbf{D}$. The relation $c^3 = e$ is responsible for partition of a neighbourhood the vertex $x_1 = 0$; the relation $aba^{-1}b^{-1}c = e$ responds for regular partition near the vertex x_0 in Figure 2(a). (Poincaré has shown that if any elliptic transformation g, which arises from a composition $g_l \dots g_1 \in \Gamma$ such that $v_0 \xrightarrow{g_1} v_1 \xrightarrow{g_1} \dots \longrightarrow v_l = v_0$ for a subset $\{v_0, \dots, v_l\}$ of vertices of the fundamental domain, has angle $2\pi/k$ at the fixed point v_0, then the group Γ is discrete).

In Figure 2(b) we see the fundamental domain $F' = F \cup c(F) \cup c^2(F) = F_1 \cup F_2 \cup F_3$ of the subgroup $\Gamma' \subset \Gamma$ corresponding to the Riemann surface $M = \mathbf{D}/\Gamma'$. Here Γ and Γ' play the roles of fundamental groups for orbifolds. All theorems from Section 2 hold in the case when the fundamental groups $\pi_1(E')$ and $\pi_1(M')$ are replaced by Γ' and Γ. In particular,

$$\mathrm{Deck}(M \to E) = \mathrm{Norm}(\Gamma')/\Gamma'$$

In Figure 2(c) we present the generators of the group Γ'; they are a, cac, c^2ac^2, bc^2, cb, c^2bc. By the Poincaré theorem the group Γ' is Fuchsian. We see that the vertices of the domain F' are divided into three groups $\{u_0, u_1, u_2, u_3\}$,

$\{v_0, v_1, v_2, v_3\}$, $\{w_0, w_1, w_2, w_3\}$. Each group represents one point in M (above $x_0 \in E$); in Figure 2(b) they are labelled by 1, 2, 3, respectively.

From Figure 2(b) one can calculate the group $\mathrm{Mon}(M \to E)$. The punctured torus $E' = E \setminus (\textit{critical value}) = E \setminus x_1$ has the loops α and β generating its fundamental group $\pi_1(E', x_0)$ (see Figure 2(a)). We have $\Delta_\alpha = (23)$ and $\Delta_\beta = (12)$. Thus $\mathrm{Mon} = S(3)$.

We define the homomorphism $\Delta\colon \Gamma \to S(3) = \mathrm{Mon}$ by

$$\Delta(a) = (23), \quad \Delta(b) = (12), \quad \Delta(c) = (132).$$

It turns out that $\Gamma' = \Delta^{-1}(G')$, where $G' = \{e, (12)\} \subset S(3)$ is a subgroup which keeps 1 at place. Therefore

$$\mathrm{Deck} = \mathrm{Norm}(\Gamma')/\Gamma' = \mathrm{Norm}(G')/G' = \{e\}.$$

In [8] the authors do not provide the formulas for the maps a, b, c. Below we show how to find them. We firstly find corresponding automorphisms of the upper half-plane $\mathbf{H} = \{\mathrm{Im}\,\zeta > 0\}$; they will belong to the group $\mathrm{PSL}(2,\mathbb{R})$. We shall find two matrices $A, B \in \mathrm{SL}(2,\mathbb{R})$, which induce the corresponding Möbius transformations γ_A, γ_B such that $\gamma_{C^{-1}}$, $C^{-1} = ABA^{-1}B^{-1}$ is elliptic of order 3. We put

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then

$$C^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -\lambda^2 b \\ -\lambda^{-2} c & a \end{pmatrix} = \begin{pmatrix} ad - \lambda^{-2} bc & (1-\lambda^2)ab \\ (1-\lambda^{-2})cd & ad - \lambda^2 bc \end{pmatrix}.$$

The condition that the transformation γ_C^{-1} is conjugated to the rotation by $2\pi/3$ means that the eigenvalues of C^{-1} are $e^{\pm i/3}$, or that $\mathrm{Tr}\, C^{-1} = 1$. So we put $a = 13$, $b = c = 2/3$, $d = 1/9$, $\lambda = 2$. Then γ_A, γ_B become hyperbolic transformations and $C^{-1} = \left(\begin{smallmatrix} 4/3 & -26 \\ 1/18 & -1/3 \end{smallmatrix}\right)$, with the eigenvectors $\left(\begin{smallmatrix} \zeta_{1,2} \\ 0 \end{smallmatrix}\right)$, $\zeta_{1,2} = 3(5 \pm \sqrt{27}i) \in \pm\mathbf{H}$. In the chart $x = (\zeta - \zeta_1)/(\zeta - \zeta_2)$ the map γ_C^{-1} is the needed rotation.

Let $D = \left(\begin{smallmatrix} 1 & -\zeta_1 \\ 1 & -\zeta_2 \end{smallmatrix}\right)$. Then $a = \gamma_{DAD^{-1}}$, $b = \gamma_{DBD^{-1}}$, $c = \gamma_{DCD^{-1}}$.

5. Generalizations

The multi-valued functions $\ln x$, $x^{\sqrt{2}}$, $\sqrt{1 - x^{\sqrt{2}}}$, $\sqrt{1-(1-x^i)^i}$ are elementary, but take infinite number of values, and the fourth function has singularities in a dense subset of the complex plane. The classical theory of Riemann surfaces learns us how to deal with functions which have isolated singularities. The corresponding theory for functions with at most countable set of singularities (the so-called S-functions) was created by Khovanskiĭ in [7].

He considers analytic prolongations of analytic elements f_c (germs of multi-valued function $f(x)$) along paths in $\mathbb{C}\setminus A$, where A is a countable set containing singularities of f called the *prohibited set*. Thus one obtains an (open) Riemann surface M_A with a projection p_A onto $\mathbb{C}$. Analogously as in Section 2 one defines the monodromy group $\mathrm{Mon}_A \subset S(p^{-1}(a))$ of the covering p_A. Next, Khovanskiĭ takes the closure of Mon_A in the product space $(M_A)^{M_A}$, using the Tikhonov topology. The result is the *closed monodromy group* $\overline{\mathrm{Mon}}$, which does not depend on the prohibited set A.

One can define the deck transformation groups Deck_A as consisting on fiber diffeomorphisms of the covering $M_A \to \mathbb{C}$ and the *closed deck transformation group* $\overline{\mathrm{Deck}}$ as the closure of Deck_A. Again one obtains the inclusions $\mathrm{Deck}_A \subset \mathrm{Mon}_A$ and $\overline{\mathrm{Deck}} \subset \overline{\mathrm{Mon}}$. We can treat the family $\{M_A\}$ of Riemann surfaces as a virtual Riemann surface $M = M(f)$ whose monodromy group is $\overline{\mathrm{Mon}}$. Such virtual covering would be called Galois if $\overline{\mathrm{Deck}} = \overline{\mathrm{Mon}}$.

It seems that many statements and notions from Section 2 could be generalized to the case of S-functions. For example, we could try to define coverings of regular type as those for which all components (in M_A) of sets of the form $p_A^{-1}(U \setminus A)$, U – small disc, are diffeomorphic. The set of coverings of regular type over $\mathbb{C}$ should be the same as the set of Galois coverings.

We leave this subject aside, because we have no rigorous proofs of the above statements at the moment. Instead, we present some natural examples of infinite Galois coverings.

Example 7 (Liouvillian first integrals). Consider a differential equation

$$\frac{dy}{dx} = \frac{P(x,y)}{Q(x,y)}$$

where P and Q are polynomials. Singer [12] has proven that such equation has a first integral of the liouvillian type (i.e. obtained from rational functions by a series of operations like exponentiation, integration and solution of an algebraic equation) if and only if it has an integrating multiplier of the form

$$R = e^g \prod f_i^{a_i}.$$

Here $g(x,y)$ is a rational function, f_i are polynomials and $a_i \in \mathbb{C}$. Thus the first integral is a multivalued function

$$H(x,y) = \int_{(x_0,y_0)}^{(x,y)} R\omega, \quad \omega = Q\,dx - P\,dy.$$

The singularities S of H lie in the algebraic curves defined by $f_i = 0$ and in poles of g. By analytic continuation one obtains a (two-dimensional) Riemann surface $M = M(H)$ with a projection onto $\mathbb{C}^2 \setminus S$.

It turns out (see [15]) that the monodromy transformations take the form $h \to \lambda h + \mu$. Thus they are prolonged to analytic diffeomorphisms of $(\mathbb{C}^2 \setminus S) \times \mathbb{C}$

$$\Phi(x, y; h) = (x, y; \lambda h + \mu)$$

which, restricted to M, define the deck transformations. So Deck = Mon and this covering is Galois.

In [15] the monodromy group Mon(H) was extended together with certain extension of the Riemann surface $M(H)$. That construction allowed to reveal the nature of singularities of $H(x, y)$ along the poles of the exponent rational function $g(x, y)$.

Example 8 (Riccati equation). It is an equation of the form

$$\frac{dy}{dx} = \frac{A(x)y^2 + B(x)y + C(x)}{D(x)}$$

where A, B, C, D are polynomials. Any its solution $y = \varphi(x)$ defines a multi-valued holomorphic function with singularities in the set $x_1, \dots, x_m$ of zeroes of the polynomial D. The evolution operators $\{\varphi(x)\} \to \{\varphi(x')\}$ take the form of Möbius maps (because they are automorphisms of $\mathbb{C}P^1$). Therefore the monodromy maps $\Delta\colon \{\varphi(x_0)\} \to \{\varphi(x_0)\}$ are also of this form: $y \to (ay + b)/(cy + d)$. They are extended to diffeomorphisms $(x, y) \to (x, (ay + b)/(cy + d))$ of $(\mathbb{C} \setminus \{x_1, \dots, x_m\}) \times \mathbb{C}P^1$.

For example, for the equation $dy/dx = y^2/x$ with solutions $y(1) = y_0$, $y(x) = y_0/(1 - y_0 \ln x)$, the monodromy around any circle around $x = 0$ gives the deck transformation $y/(1 - 2\pi i y)$.

Also the first integral (not liouvillian, in general), which takes the form

$$H(x, y) = \frac{y\varphi_1(x) - E(x)\varphi_1'(x)}{y\varphi_2(x) - E(x)\varphi_2'(x)}$$

defines a multi-valued function and a Galois covering over $\mathbb{C}^2 \setminus \{D = 0\}$. Here also Mon $\subset$ PSL$(2, \mathbb{C})$. (In the last formula the function $E(x)$ is rational and $\varphi_{1,2}(x)$ are two independent solutions of a suitable second order linear differential equation.)

There should exist an algebraic variant of the theory of infinite coverings. The Picard–Vessiot extensions from differential Galois theory provide good theory for the case of multivalued functions defined as solutions of linear differential equations. These solutions also define Galois coverings. There the automorphism group is an algebraic Lie group. In the case of differential equations with regular singularities this Lie group forms an algebraic closure of the discrete monodromy group (see [10]).

It is widely expected that these phenomena have further generalizations. In the case of liouvillian first integrals the existence of such a generalization was confirmed in [15].

References

[1] V. B. Alexeev, *Abel Theorem in Problems and Solutions*, Nauka, Moscow, 1974. (in Russian)

[2] H. Dijkgraaf, F. C. Faber and G. van der Geer (eds.), *Moduli Spaces of Curves*, Birkhäuser, Boston, 1995.

[3] V. A. Dubrovin, S. P. Novikov and A. T. Fomenko, *Modern Geometry*, Nauka, Moscow, 1986. (in Russian)

[4] O. Forster, *Riemannsche Flächen*, Springer–Verlag, Berlin, 1977.

[5] L. Greenberg, *Maximal groups and signatures*, Discontinuous Groups and Riemann Surfaces, Princeton University Press, Princeton, 1974, pp. 207–226.

[6] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, J. Wiley Sons, New York, 1978.

[7] A. G. Khovanskiĭ, *Topological obstructions to the representability of functions by quadratures*, J. Dynam. Control Systems **1** (1995), 91–123.

[8] S. L. Krushkal, B. A. Apanasov and N. A. Gusevskiĭ, *Kleinian groups in examples and problems*, Transl. Math. Monogr. **62** (1986).

[9] B. Maskit, *Kleinian groups*, Springer–Verlag, Berlin, 1988.

[10] M. van der Put, *Recent work on differential Galois theory*, Sem. Bourbaki 1997–1998, Asterisque, 1998, pp. 341–367.

[11] B. Riemann, *OEuvres Mathématiques*, Gauthier–Villars, Paris, 1898.

[12] M. F. Singer, *Liouvillian first integrals of differential equations*, Trans. Amer. Math. Soc. **333** (1992), 673–688.

[13] B. L. van der Waerden, *Algebra I. Achte Auflage der Modernen Algebra*, Springer–Verlag, Berlin, 1971.

[14] H. Weyl, *Die Idee der Riemannsche Fläche*, 3. Aufl. Stuttgart, Teubner, 1955.

[15] H. Żołądek, *The extended monodromy group and liouvillian first integrals*, J. Dynam. Control Systems **4** (1998), 1–28.

[16] ———, *The topological proof of Abel–Ruffini theorem*, Topol. Methods Nonlinear Anal. **16** (2000), 253–265.

Manuscript received November 28, 2001

Henryk Żołądek
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warsaw, POLAND

E-mail address: zoladek@mimuw.edu.pl