Lecture 15–16, October 29, November 3

INTRODUCTION TO TOPOLOGICAL GALOIS THEORY

ON REPRESENTABILITY OF ALGEBRAIC FUNCTIONS BY RADICALS (CONTINUATION)

The field of rational functions of

$$x_1, \dots, x_N$$

is isomorphic to the field

$$\mathcal{R}$$

of germs of rational functions at the point

$$x_0 \in \mathbb{C}^N \setminus \Sigma.$$

Consider the field extension

$$\mathcal{R}\langle y_1, \dots, y_n \rangle$$

of $\mathcal{R}$ by the germs $y_1, \dots y_n$ at x_0 satisfying the equation (1) from previous lecture:

$$P_n y^n + P_{n-1} y^{n-1} + \cdots + P_0 = 0, \tag{1}$$

Lemma 1. *Every permutation S_γ from the monodromy group can be uniquely extended to an automorphism of the field*

$$\mathcal{R}\{y_1, \dots, y_n\}$$

over the field $\mathcal{R}$.

Proof. Every element

$$f \in \mathcal{R}\langle y_1, \dots, y_n \rangle$$

is a rational function of

$$x, y_1, \dots, y_n.$$

It can be continued meromorphically along the curve

$$\gamma \in \pi_1(\mathbb{C}^m \setminus \Sigma, x_0)$$

together with

$$y_1, \dots, y_n.$$

This continuation gives the required automorphism, because the continuation preserves the arithmetical operations and every rational function returns back to its original values (since it is a single-valued valued function).

The automorphism is unique because the extension is generated by

$$y_1, \dots, y_n.$$

□

By definition the *Galois group* of the equation (1) is the group of all automorphisms of the field

$$\mathcal{R}\{y_1, \ldots, y_n\}$$

over the field $\mathcal{R}$.

According to Lemma 1 the monodromy group of the equation (1) can be considered as a subgroup of its Galois group.

Recall that by definition a multivalued function $y(x)$ is *algebraic* if all its meramorphic germs satisfy the same algebraic equation over the field of rational functions.

Theorem 2. *A germ*

$$f \in \mathcal{R}\langle y_1, \ldots, y_n \rangle$$

is fixed under the monodromy action if and only if $f \in \mathcal{R}$.

Proof. A germ
$$f \in \mathcal{R}\langle y_1, \dots, y_n \rangle$$
is fixed under the monodromy action if and only if f is a germ of a single valued function. The field $\mathcal{R}\langle y_1, \dots, y_n \rangle$ contains only germs of algebraic functions. Any single valued algebraic function is a rational function. □

According to the Galois theory Theorem 2 can be formulated in the following way.

Theorem 3. *The monodromy group of the equation (1) is isomorphic to the Galois group of the equation (1) over the field $\mathcal{R}$.*

Below we will not rely on Galois theory. Instead we will use Theorem 3 directly.

Lemma 4. *The monodromy group acts on the set*

$$Y_{x_0}$$

transitively if and only if the equation (1) is irreducible over the field of rational functions.

Proof. Assume that there is a proper subset

$$\{y_1, y_2, \dots y_k\}$$

of Y_{x_0} invariant under the monodromy action. Then the elementary symmetric functions

$$r_1 = y_1 + \cdots + y_k, \quad r_2 = \sum_{i<j} y_i y_j, \dots,$$

$$r_k = y_1 \cdot \dots \cdot y_k$$

belong to the field $\mathcal{R}$.

Thus

$$y_1, y_2, \dots y_k$$

are solutions of the degree $k < n$ equation

$$y^k - r_1 y^{k-1} t + \dots (-1)^k r_k = 0.$$

So equation (1) is reducible.

On the other hand if the equation (1) can be represented as a product of two equations over $\mathcal{R}$ then their roots belong to two complementary subsets of Y_{x_0} which are invariant under the monodromy action. $\square$

Corollary 5. *An irreducible equation (1) defines a multivalued algebraic function $y(x)$ whose set of germs at $x_0 \in \mathbb{C}^N \setminus \Sigma$ is the set*

Y_{x_0} and whose monodromy group coincides with the monodromy group of the equation (1).

Theorem 3, Corollary 5 and the Galois theory immediately imply the following result.

Theorem 6. *An algebraic function whose monodromy group is solvable can be represent by rational functions using the arithmetic operations and radicals.*

As we know from previous lectures A stronger version of Theorem 6 can be proven using linear algebra. Let us recall the needed result (in its statement we replaced a commutative algebra V containing all roots of unity by a commutative $\mathbb{C}$-algebra).

Theorem 7. *Let G be a finite solvable group of order n acting by automorphisms on a $\mathbb{C}$-algebra V. Then every element x of* *the algebra V can be obtained from the elements of the invariant subalgebra V_0 by takings n-th roots and summing.*

Theorem 8. *An algebraic function whose monodromy is solvable can be represented by rational functions by root extractions and summations.*

Proof. One can prove Theorem 8 by applying Theorem 7 to the monodromy action by automorphisms on the extension

$$\mathcal{R}\langle y_1, \ldots, y_n \rangle$$

with the field of invariants $\mathcal{R}$. □

PROPERTIES OF SOLVABLE GROUPS

Problem 1. *We say that* G_0 *is a characteristic subgroup of a group* G *if for any automorphism*

$$\sigma : G \to G$$

the image $\sigma(G_0)$ *of the subgroup* G_0 *is equal to* G_0.

1) Show that any characteristic subgroup of G *is a normal subgroup of* G.

2) Assume that $G_1 \subset G_0 \subset G$ *is a chain of subgroups such that* G_1 *is a characteristic subgroup of* G_0, *and* G_0 *is a characteristic subgroup of* G *then* G_1 *is a characteristic subgroup of* G.

3) Assume that $G_1 \subset G_0 \subset G$ *is a chain of subgroups such that* G_1 *is a characteristic subgroup of* G_0, *and* G_0 *is a normal subgroup of* G *then* G_1 *is a normal subgroup of* G.

Definition 1. *The (first) commutator* $G^{(1)}$ *of a group* G *is a subgroup of* G *generated by all elements of the form*

$$xyx^{-1}y^{-1}$$

where x, y *are any elements of* G*.*

The k*-th commutator* $G^{(k)}$ *of a group* g *is a commutator of the* k_1*-th commutator of* G*.*

Problem 2. *Show that the commutator of a group* g *is a characteristic subgroup of* G*. Consider the decreasing chain of commutators*

$$G \supset G^{(1)} \supset \cdots \supset G^{(k)}.$$

Show that for any $1 \leq i \leq k$ *the group* $G^{(i)}$ *is a normal subgroup of* G*.*

Definition 2. *A group G is solvable in k-steps if there is a normal chain*

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = e$$

if for any $0 \leq i < k$ the factor group G_i/G_{i+1} is commutative and e is the the trivial group.

Problem 3. *1) Show that the commutator is the smallest normal divisor in G such that the corresponding factor group is commutative, i.e. $G'h$ is commutative if and only if H is a normal divisor of G and $H \supset G^{(1)}$.*

2) A group G is solvable in k-steps if and only if $G^{(k)} = e$.

Problem 4. *1) Let $\tau : G \to F$ be a onto homomorphism. Show that for any $k \geq 1$ the image $\tau(G^{(k)}$ is equal to $F^{(k)}$.*

2) Let $\tau : G \to F$ be a homomorphism. Show that for any $k \geq 1$ the inclusion $\tau^{-1}F^{(k)} \subset G^{(k)}$ holds.

TOPOLOGICAL OBSTRUCTION TO REPRESENTABILITY BY RADICALS

Let us introduce some notation.

By G^m we denote the m-th commutator subgroup of the group G. For any $m \geq$ the group G^m is a normal subgroup in G.

By $F(D, x_0)$ we denote the fundamental group of the domain $U = \mathbb{C}^N \setminus D$ with the base point $x_0 \in U$, where D is an algebraic hypersurface in $\mathbb{C}^N$.

Let $H(D, m)$ be the covering space of the domain $\mathbb{C}^N \setminus D$ corresponding to the subgroup $F^m(D, x_0)$ of the fundamental group $F(D, x_0)$.

We will say that an algebraic function is an *R-function* if it becomes a single-valued function on some covering $H(D, m)$.

Lemma 9. *If*

$$m_1 \geq m_2 \quad \textit{and} \quad D_1 \supset D_2$$

then there is a natural projection

$$\rho : H(D_1, m_1) \to H(D_2, m_2).$$

Thus if a function y becomes a single-valued function on

$$H(D_2, m_2)$$

then it certainly becomes a single-valued function on

$$H(D_1, m_1).$$

Proof. Let

$$p_* : F(D_1, x_0) \to F(D_2, x_0)$$

be the homomorphism induced by the embedding

$$p : \mathbb{C}^N \setminus D_1 \to \mathbb{C}^N \setminus D_2.$$

Lemma 9 follows from the following obvious inclusions:

$$p_*^{-1}[F^{m_2}(D_2, x_0)] \subset F^{m_2}(D_1, x_0)$$

and

$$F^{m_2}(D_1, x_0) \subset F^{m_1}(D_1, x_0).$$

□

Lemma 10. *If* y_1 *and* y_2 *are R-function then*

$$y_1 + y_2, \quad y_1 - y_2, \quad y_1 \cdot y_2, \quad y_1/y_2$$

also are R-functions.

Proof. Assume that R-functions y_1 and y_2 become single-valued functions on the coverings

$$H(D_1, m_1) \quad and \quad H(D_2, m_2).$$

By Lemma 9 the functions y_1,y_2 become single-valued on the covering

$$H(D, m) \quad where \quad D = D_1 \bigcup D_2 \quad and$$

$$m = \max(m_1, m_2).$$

Thus the functions $y_1 + y_2$, $y_1 - y_2$, $y_1 \cdot y_2$ and y_1/y_2 also become single-valued on on the covering $H(D, m)$. The proof is completed since

$$y_1 + y_2, \quad y_1 - y_2, \quad y_1 \cdot y_2 \quad and \quad y_1/y_2$$

are algebraic functions. □

Lemma 11. *Composition of an R-function with the degree q radical is an R-function.*

Proof. Assume that the function y defined by (1) is R-function which becomes a single-valued function on the covering

$$H(D_1, m).$$

Let

$$D_2 \subset \mathbb{C}^N$$

be the hypersurface, defined by the equation

$$P_n P_0 = 0,$$

where

$$P_n \quad and \quad P_0$$

are the leading coefficient and the constant term of the equation (1).

According to Lemma 9 the function y becomes a single-valued function on the covering

$$H(D,m) \quad where \quad D = D_1 \bigcup D_2.$$

Let

$$h_0 \in H(D,m)$$

be a point whose image under the natural projection

$$\rho : H(D,m) \to \mathbb{C}^N \setminus D$$

is the point x_0. One can identify the fundamental groups

$$\pi_1(H(D,m), h_0) \quad and \quad F^m(D, x_0).$$

By definition of D_2
the function y never equals to zero or to infinity on $H(D,m)$.

Hence y defines a map

$$y : H(D,m) \to \mathbb{C} \setminus \{0\}.$$

Let

$$y_* : \pi_1(H(D,m), h_0) \to \pi_1(\mathbb{C} \setminus \{0\}, y(h_0))$$

be the induced homomorphism of the fundamental groups.

The group

$$\pi_1(H(D,m), h_0)$$

is identified with the group $F^m(D, x_0)$

and the group

$$\pi_1(\mathbb{C} \setminus \{0\}, y(h_0))$$

is isomorphic to $\mathbb{Z}$.

So

$$\ker y_* \subset F^{m+1}(D, x_0).$$

Thus all loops from the group

$$y_*(F^{m+1}(D, x_0))$$

do not wind around the origin $0 \in \mathbb{C}$.

Hence any germ of $y^{1/q}$ does not change its value after continuation along a loop from the group

$$F^{m+1}(D, x_0).$$

So $y^{1/q}$ is a single-valued function on $H(D, m+1)$. The proof is completed since $y^{1/q}$ is an algebraic function. $\square$