Lecture 23, December 3

THE MAIN THEOREM

Let us formulate and prove the main theorem of the topological Galois theory.

Theorem 1. *A class of $\mathcal{S}$-functions $\hat{\mathcal{M}}$ consisting of $\mathcal{S}$-functions whose closed monodromy pairs lie in some complete class $\mathcal{M}$ of pairs, is stable under the differentiation, composition and meromorphic operations.*

Furthermore, if the class $\mathcal{M}$ contains

1. *the additive group $\mathbb{C}$ of complex numbers, then the class $\hat{\mathcal{M}}$ is stable under the integration,*
2. *the permutation group $S(k)$ of k elements, then the class $\hat{\mathcal{M}}$ is stable under solving algebraic equations of degrees at most k.*

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

Lemma 2 (on derivatives)**.** *For every $\mathcal{S}$-function f, the following inclusion holds*

$$[f'] \in \mathcal{M}\langle [f] \rangle.$$

Proof. Let A be the singular point set of the $\mathcal{S}$-function f, and f_a a germ of the function f at a nonsingular point a.

Let Γ denote the fundamental group $\pi_1(S^2 \setminus A, a)$, let Γ_1 and Γ_2 denote the stabilizers of the germs f_a and f'_a.

The group Γ_1 is contained in the group Γ_2. Indeed, under continuation along a path $\gamma \in \Gamma_1$, the germ f_a remains unchanged, and hence its derivative is also unchanged.

From the definition of a complete class of pairs it follows that

$$[\Gamma, \Gamma_2] \in \mathcal{M}\langle [\Gamma, \Gamma_1] \rangle.$$

Using Proposition 5.7 we obtain that $[f'] \in \mathcal{M}\langle [f] \rangle$. □ □

Lemma 3 (on compositions)**.** *For every $\mathcal{S}$-functions f and g, the following inclusion holds* $[g \circ f] \in \mathcal{M}\langle [f], [g] \rangle$.

Proof. Let A and B be the singular point sets of functions f and g. Let $f^{-1}(B)$ be the full preimage of the set B under the multivalued function f. Set

$$Q = A \bigcup f^{-1}(B).$$

Let f_a be any germ of the function f at a point $a \notin Q$, and g_b any germ of the function g at the point $b = f(a)$. The set Q is forbidden for the germ $g_b \circ f_a$. Let Γ denote the fundamental group $\Gamma = \pi_1(S^2 \setminus Q, a)$, let Γ_1 and Γ_2 denote the stabilizers of the germs f_a and $g_b \circ f_a$.

We will write G for the fundamental group $\pi_1(S^2 \setminus B, b)$ and G_0 for the stabilizer of the germ g_b.

We now define a homomorphism $\tau : \Gamma_1 \to G$. To each path γ, whose homotopy class belongs to Γ_1 (abusing notation, we will sometimes write $\gamma \in \Gamma_1$), we assign the path $\tau(\gamma)(t) = f_{\gamma(t)}(\gamma(t))$, where $f_{\gamma(t)}$ is the germ obtained by continuation of the germ f_a along the path γ up to the point t.

The paths $\tau(\gamma)$ are closed, since under continuation along γ, the germ f_a remains unchanged. A homotopy of the path γ in the set $S^2 \setminus Q$ gives rise to a homotopy of the path $\tau \circ \gamma$ in the set $S^2 \setminus B$, since $f^{-1}(B) \subseteq Q$.

Therefore, the homomorphism is well defined.

The germ $g_b \circ f_a$ is unchanged under continuation along the paths from the group $\tau^{-1}(G_0)$ or, in other words, $\tau^{-1}(G_0) \subseteq \Gamma_2$. The lemma now follows.

Indeed, we obtain the inclusions

$$\Gamma \supseteq \Gamma_2 \supseteq \tau^{-1}(G \subseteq \tau^{-1}(G) = \Gamma_1 \subseteq \Gamma,$$

that imply that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle [G, G_0], [\Gamma, \Gamma_1]\rangle$.

From Proposition proved above, we obtain that $[g \circ f] \in \mathcal{M}\langle [f], [g]\rangle$.

□ □

Lemma 4 (on integrals)**.** *For every $\mathcal{S}$-function f, the following inclusion holds $[\int f(x)dx] \in \mathcal{M}\langle [f], \mathbb{C}\rangle$, where $\mathbb{C}$ is the additive group of complex numbers.*

Proof. Let A be the singular point set of the function f, and $Q = A \bigcup \{\infty\}$. Let f_a be any germ of the function f at a point $a \notin Q$, and g_a a germ of $\int f(x)dx$ at this point, $g'_a = f_a$. We can take the set Q as a forbidden set for the germs f_a and g_a.

Let Γ denote the fundamental group $\Gamma = \pi_1(S^2 \setminus Q, a)$, let Γ_1 and Γ_2 denote the stabilizers of the germs f_a and g_a.

We now define a homomorphism $\tau : \Gamma_1 \to \mathbb{C}$. To each path $\gamma \in \Gamma_1$, assign the number $\int_\gamma f_{\gamma(t)}(\gamma(t))dx$, where $f_{\gamma(t)}$ is the germ obtained by continuation of the germ f_a along the path 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 $[\Gamma, \Gamma_2] \in \mathcal{M}\langle[\Gamma, \Gamma_1], \mathbb{C}\rangle$. From Proposition proved above, we obtain that $[\int f(x)dx] \in \mathcal{M}\langle[f], \mathbb{C}\rangle$.

□ □

In the sequel, it will be convenient to use vector functions.

The definitions of a forbidden set, a $\mathcal{S}$-function, and the monodromy group carry over automatically to vector functions.

Lemma 5 (on vector functions)**.** *For every vector $\mathcal{S}$-function $\mathbf{f} = (f_1, \dots, f_n)$, the following equality holds:*

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

Proof. Let A_i be the singular point sets of the functions f_i. The singular point set of the vector function $\mathbf{f}$ is the set $Q = \bigcup A_i$.

Let $\mathbf{f}_a = (f_{1,a}, \ldots, f_{n,a})$ be any germ of the vector function $\mathbf{f}$ at a point $a \notin Q$.

Let Γ denote the fundamental group $\Gamma = \pi_1(S^2 \setminus Q, a)$, let Γ_i denote the stabilizer of the germ $f_{i,a}$, and Γ_0 the stabilizer of the vector germ $\mathbf{f}_a$. The stabilizer Γ_0 is exactly $\bigcap_{i=1}^{n} \Gamma_i$, which implies that $\mathcal{M}\langle[\Gamma, \Gamma_0]\rangle = \mathcal{M}\langle[\Gamma, \Gamma_1], \ldots, [\Gamma, \Gamma_n]\rangle$. Thus we obtain that $\mathcal{M}\langle[\mathbf{f}]\rangle = \mathcal{M}\langle[f_1], \ldots, [f_n]\rangle$. □ □

Lemma 6 (on meromorphic operations)**.** *For every vector $\mathcal{S}$-function $\mathbf{f} = (f_1, \ldots, f_n)$ and a meromorphic function $F(x_1, \ldots, x_n)$ such that the function $F \circ \mathbf{f}$ is defined, the following inclusion holds $[F \circ \mathbf{f}] \in \mathcal{M}\langle[\mathbf{f}]\rangle$.*

Proof. Let A be the singular point set of the function $\mathbf{f}$, and B the projection of the singular point set of the function $F\circ\mathbf{f}$ to the Riemann sphere.

We can take the set $Q=A\cup B$ as a forbidden set for the functions $F\circ\mathbf{f}$ and $\mathbf{f}$.

Let $\mathbf{f}_a$ be any germ of the function $\mathbf{f}$ at a point a, $a\notin Q$.

Let Γ denote the fundamental group $\Gamma=\pi_1(S^2\backslash Q,a)$, let Γ_1 and Γ_2 denote 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, under continuation along any path $\gamma\in\Gamma_1$, the vector function remains unchanged, and therefore the meromorphic function of it is also unchanged. From the inclusion $\Gamma_2\subseteq\Gamma_1$ it follows that $[\Gamma,\Gamma_2]\in\mathcal{M}\langle[\Gamma,\Gamma_1]\rangle$. Thus we obtain that $[F\circ\mathbf{f}]\in\mathcal{M}\langle[\mathbf{f}]\rangle$. $\square$ $\square$

Lemma 7 (on algebraic functions)**.** *For every vector $\mathcal{S}$-function $\mathbf{f}=(f_1,\dots,f_n)$ and an algebraic function y of it defined by the equation*

$$y^k + f_1 y^{k-1} + \cdots + f_k = 0, \tag{17}$$

the following inclusion holds: $[y] \in \mathcal{M}\langle [\mathbf{f}], S(k)\rangle$, *where* $S(k)$ *is the permutation group of* k *elements.*

Proof. Let A be the singular point set of the function $\mathbf{f}$, and B the projection of the set of algebraic ramification points of the function y to the Riemann sphere.

We can take the set $Q = A \cup B$ as a forbidden set for the functions y and $\mathbf{f}$. Let y_a and $\mathbf{f}_a$ be any germs of the functions y and $\mathbf{f}$ at a point $a \notin Q$ that are related by the equality

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

Let Γ denote the fundamental group $\Gamma = \pi_1(S^2 \setminus Q, a)$, let Γ_1 and Γ_2 denote the stabilizers of the germs $\mathbf{f}_a$ and y_a.

Under continuation along any path $\gamma \in \Gamma_1$, the coefficients of equation (17) are unchanged, therefore, under continuation along the path γ, the roots of equation (17) are permuted.

Thus we have a homomorphism τ of the group Γ_1 to the group $S(k)$, $\tau : \Gamma_1 \to S(k)$.

The group Γ_2 is contained in the kernel of the homomorphism τ, which implies that $[\Gamma, \Gamma_2] \in \mathcal{M}\langle[\Gamma, \Gamma_1], S(k)\rangle$. From Proposition 5.7, we obtain that $[y] \in \mathcal{M}\langle[f], S(k)\rangle$. $\square$ $\square$

This concludes the proof of the main theorem.

GROUP-THEORETIC OBSTRUCTIONS TO REPRESENTABILITY BY QUADRATURES

We compute the classes of group pairs that appear in the main theorem, and formulate a necessary condition of the representability of functions by quadratures, k-quadratures and generalized quadratures.

COMPUTATION OF SOME CLASSES OF GROUP PAIRS

The main theorem motivates the following problems: describe the minimal class of group pairs containing the additive group $\mathbb{C}$ of complex numbers; describe the minimal classes of group pairs containing, respectively, the group $\mathbb{C}$ and all finite groups, or, the group $\mathbb{C}$ and the group $S(k)$. We give solutions of these problems.

Proposition 1. *The minimal complete class of pairs $\mathcal{M}\langle\mathcal{L}_\alpha\rangle$ containing given almost complete classes of pairs $\mathcal{L}_\alpha$, consists of the group pairs $[\Gamma, \Gamma_0]$ that admit a chain of subgroups*

$$\Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$$

such that for any i, $1 \leq i \leq m-1$, the group pair $[\Gamma_i, \Gamma_{i+1}]$ is contained in some almost complete class $\mathcal{L}_{\alpha(i)}$.

To prove this, it suffices to verify that the group pairs $[\Gamma, \Gamma_0]$ satisfying the conditions of the proposition, firstly, belong to the complete class $\mathcal{M}\langle \mathcal{L}_\alpha \rangle$ and, secondly, form a complete class of pairs. Both statements follow immediately from definitions. It is also easy to verify the following propositions.

Proposition 2. *The collection of group pairs* $[\Gamma, \Gamma_0]$ *such that* Γ_0 *is a normal subgroup of the group* Γ, *and the group* Γ/Γ_0 *is commutative, is the minimal almost complete class of pairs* $\mathcal{L}\langle \mathcal{A} \rangle$ *containing the class* $\mathcal{A}$ *of all Abelian groups.*

Proposition 3. *The collection of group pairs* $[\Gamma, \Gamma_0]$ *such that* Γ_0 *is a normal subgroup of the group* Γ, *and the group* Γ/Γ_0 *is finite, is the minimal almost complete class of pairs* $\mathcal{L}\langle \mathcal{K} \rangle$ *containing the class* $\mathcal{K}$ *of all finite groups.*

Proposition 4. *The collection of group pairs* $[\Gamma, \Gamma_0]$ *such that* $\operatorname{ind}(\Gamma, \Gamma_0) \leq k$, *is an almost complete class of group pairs.*

The class of group pairs from Proposition 4 will be denoted by $\mathcal{L}\langle \operatorname{ind} \leq k\rangle$. Proposition 4 is of interest to us in connection with the characteristic property of subgroups in the group $S(k)$, Lemma 3.13.

A chain of subgroups

$$\Gamma_i, i = 1, \ldots, m, \Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$$

is called a *normal tower of the group pair* $[\Gamma, \Gamma_0]$ if the group Γ_{i+1} is a normal subgroup of the group Γ_i for every $i = 1, \ldots, m-1$. The collection of quotient groups Γ_i/Γ_{i+1} is called the *collection of divisors with respect to the normal tower.*

Theorem 8 (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 group pair* $[\Gamma, \Gamma_0]$ *belongs to the minimal complete class* $\mathcal{M}\langle \mathcal{A}, \mathcal{K}\rangle$ *containing all finite groups and commutative groups if and only if it has a normal tower such that each divisor in this tower is either a finite group or a commutative group.*

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

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

Proof. The first claim of the theorem follows from the description of the classes $\mathcal{L}\langle\mathcal{A}\rangle$ and $\mathcal{L}\langle\mathcal{K}\rangle$ given in Propositions 7.2 and 7.3, and from Proposition 7.1.

To prove the second claim, consider the minimal complete class of group pairs containing the classes $\mathcal{L}\langle\mathcal{A}\rangle$ and $\mathcal{L}\langle\text{ind} \leq k\rangle$. This class consists of group pairs $[\Gamma, \Gamma_0]$ that admit a chain of subgroups

$$\Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$$

such that, for every i, $1 \leq i \leq m-1$, either the group Γ_i/Γ_{i+1} is commutative, or we have $\text{ind}(\Gamma_i, \Gamma_{i+1}) \leq k$ (see Propositions 7.3, 7.4 and Proposition 7.1). The class of group pairs just described contains the group $S(k)$ (see Lemma 3.13) together with all commutative groups, and it is obviously the minimal complete class of pairs possessing these properties. It only remains to reformulate the answer. We can gradually transform the chain of subgroups

$$\Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$$

into a normal tower for the pair $[\Gamma, \Gamma_0]$. Suppose that, for $j < i$, the group Γ_{j+1} is a normal subgroup of the group

$$\Gamma_j, \quad \text{and} \quad \mathrm{ind}(\Gamma_i, \Gamma_{i+1}) \le k,$$

Let $\overline{\Gamma}_{i+1}$ denote the maximal normal subgroup of the group Γ_i contained in the group Γ_{i+1}. It is clear that the quotient group $\Gamma_i/\overline{\Gamma}_{i+1}$ is a subgroup of the group $S(k)$. Instead of the initial chain of subgroups, consider the chain

$$\Gamma = G_1 \supseteq \cdots \supseteq G_m = \Gamma_0$$

such that $G_j = \Gamma_j$ for $j \le i$ and

$$G_j = \Gamma_j \bigcap \overline{\Gamma}_{i+1} \quad \text{for} \quad j > i.$$

Continuing this process (for at most m steps), we will pass from the initial chain of subgroups to a normal tower, thus obtaining a description of the class $\mathcal{M}\langle \mathcal{A}, S(k)\rangle$ in the desired terms.

We now prove claim 3. According to Propositions 7.2 and 7.3, the group pair $[\Gamma, \Gamma_0]$ belongs to the class $\mathcal{M}\langle\mathcal{A}\rangle$ if and only if there exists a chain

$$\Gamma = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m \subseteq \Gamma_0$$

such that Γ_i/Γ_{i+1} are commutative groups. Consider a chain of groups

$$\Gamma = G^1 \supseteq \cdots \supseteq G^m$$

such that the group G^{i+1} is the commutator of the group G^i for $i = 1, \ldots, m-1$. Every automorphism of the group Γ takes the chain of groups G^i to itself, hence each group G^i is a normal subgroup of the group Γ. Induction by i shows 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 $G^m \subseteq \Gamma_0$, we have

$$G^m \subseteq \bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}.$$

By 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 statement (a pair of groups with a solvable monodromy group lies in the class $\mathcal{M}\langle\mathcal{A}\rangle$) is obvious. □ □

Proposition 5. *Every commutative group* Γ, *whose cardinality is at most the cardinality of the continuum belongs to the class* $\mathcal{L}\langle\mathbb{C}\rangle$.

Proof. The set of complex numbers $\mathbb{C}$ is a vector space over the rational numbers, whose dimension is the cardinality of the continuum.

Let $\{e_\alpha\}$ be a basis of this space. The subgroup $\tilde{\mathbb{C}}$ of the group $\mathbb{C}$ spanned by the numbers $\{e_\alpha\}$, is a free Abelian group with the number of generators equal to the cardinality of the continuum.

Every commutative group Γ, whose cardinality is at most the cardinality of the continuum is a quotient group of the group $\tilde{\mathbb{C}}$, and, therefore, $\Gamma \in \mathcal{L}\langle\mathbb{C}\rangle$. □ □

From Proposition 7.6 and from the computation of the classes

$$\mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle, \mathcal{M}\langle S(n)\rangle \text{ and } \quad \mathcal{M}\langle\mathcal{A}\rangle,$$

it follows that a pair of groups $[\Gamma, \Gamma_0]$, for which the cardinality of Γ is at most the cardinality of the continuum belongs to the classes

$$\mathcal{M}\langle\mathbb{C},\mathcal{K}\rangle, \mathcal{M}\langle\mathbb{C}, S(n)\rangle, \quad \text{and} \quad \mathcal{M}\langle\mathbb{C}\rangle$$

if and only if it belongs to the classes

$$\mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle, \mathcal{M}\langle\mathcal{A}, S(n)\rangle \quad \text{and} \quad \mathcal{M}\langle\mathcal{A}\rangle.$$

This result suffices for our purposes, since the permutation group of the branches of a function has at most cardinality of the continuum.

Lemma 9. *A free noncommutative group* Λ *does not belong to the class* $\mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle$*.*

Proof. Suppose that $\Lambda \in \mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle$, i.e. Λ has a normal tower

$$\Lambda = \Gamma_1 \supseteq \cdots \supseteq \Gamma_m = e$$

such that each divisor in this tower is a finite group or a commutative group. Each group Γ_i is free as a subgroup of a free group. The group $\Gamma_m = e$ is commutative. Let Γ_{i+1} be the commutative group with the smallest index.

For any elements a, $b \in \Gamma_i$, there exists a nontrivial relation: if Γ_i/Γ_{i+1} is commutative, then, for example, elements

$$aba^{-1}b^{-1} \quad \text{and} \quad ab^2a^{-1}b^{-2}$$

commute; if Γ_i/Γ_{i+1} is finite, then some powers a^p, b^p of the elements a, b commute. Therefore, the group Γ_i has at most one generator, and it is therefore commutative. The contradiction proves that $\Lambda \notin \mathcal{M}\langle\mathcal{A},\mathcal{K}\rangle$. □ □

Lemma 10. *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 $A(k)$ is simple and noncommutative. For this group, the criterion of being in the class

$$\mathcal{M}\langle\mathbb{C}, S(k-1)\rangle$$

obviously fails. Therefore, the symmetric group $S(k)$ for $k > 4$ does not belong to the class

$$\mathcal{M}\langle\mathbb{C}, S(k-1)\rangle.$$

□ □

Lemma 11. *The only transitive permutation group of k elements generated by transpositions is the symmetric group $S(k)$.*

Proof. Let a group Γ be a transitive permutation group generated by transpositions of the set M with k elements.

A subset $M_0 \subseteq M$ is said to be *complete* if every permutation of the set M_0 extends to some permutation of the set M from the group Γ. Complete subsets exist.

For example, two elements of the set M that are interchanged by a basis transposition, form a complete subset. Take a complete subset M_0 of the maximal cardinality. Suppose that $M_0 \neq M$.

Then, by the induction hypothesis, the restriction of Γ to M_0 coincides with $S(M_0)$. Since the group Γ is transitive, there exists a basis transposition μ interchanging some elements

$$a \notin M_0 \quad \text{and} \quad b \in M_0.$$

The permutation group 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. The obtained contradiction proves that the group Γ is the group $S(M)$. $\square$ $\square$