Abel's Theorem

by Sophia Breslavets, Igor Goldanskii and Denys Honcharov

Mentor: Elizaveta Nesterova

Abel's Theorem

Theorem (Abel's Theorem). *For* $n \geq 5$ *the general algebraic equation of degree* n

$$a_0 w^n + a_1 w^{n-1} + \cdots + a_{n-1} w + a_n = 0$$

is not solvable by radicals.

Basics

Let's get acquainted with some basic concepts and theorems

Groups and Isomorphisms

Definition. *G with a binary operation on it is a **group** if:*

1) $\forall a, b, c \in G$ *we have* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

2) $\exists e \in G$ *such that* $\forall a \in G$ *we have* $a \cdot e = e \cdot a = a$;

3) $\forall a \in G \ \exists a^{-1} \in G$ *such that* $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition. *A map* $f\colon G \to G'$ *is a **homomorphism** if* $\forall a, b \in G$ *we have* $f(a \cdot b) = f(a) \cdot f(b)$.

Definition. *Let* $\phi\colon G \to G'$ *be a homomorphism. The set of the elements* $g\colon \phi(g) = e_{G'}$ *is called the **kernel of the homomorphism** ϕ.*

Definition. *A homomorphism* $f\colon G \to G'$ *is an **isomorphism** if there is another homomorphism* $g\colon G \to G'$ *such that* $f \circ g = Id_{G'}$ *and* $f \circ g = Id_G$.

Subgroups. Normal Subgroups

Definition. *A subset H of a group G is called a subgroup if it forms a group itself under the same binary operation.*

Theorem. *If H is a subgroup of a group G, the unit elements in G and H coincide.*

Theorem. *The order of a subgroup H of a group G divides the order of G.*

Definition. *A subgroup N of a group G is called a* ***normal subgroup of G*** *if $\forall a \in N$ and $\forall g \in G$ the element $gag^{-1} \in N$.*

Commutative Groups and Commutants

Definition. *Two elements a and b of a group are said to* ***commute*** *if $ab = ba$.*

Definition. *If in a group any two elements commute, the group is called* ***commutative****.*

Definition. *The element $aba^{-1}b^{-1}$ is called the* ***commutator*** *of the elements a and b.*

Definition. *The set of all possible products of a finite number of commutators of a group G is called the* ***commutant*** *of the group G and is denoted by $K(G)$.*

Theorem. *The commutant is a normal subgroup.*

Theorem. *The commutant coincides with the unit element if and only if the group is commutative.*

Soluble Groups

Definition. *A group G is said to be soluble if the sequence $G, K(G), K_2(G), K_3(G)$ ends with a unit group, i.e. $G = \{e\}$ or $\exists n \in G\colon\ K_n(G) = \{e\}$.*

Theorem. *If a group G is not commutative and has no normal subgroups other than $\{e\}$ and G, it is not soluble.*

Theorem. *Every subgroup of a soluble group is soluble.*

Abel's Theorem Proof

Let's now prove Abel's Theorem!

Abel's Theorem Proof: Part 1

Permutations and Symmetric Groups

Definition. *The group of all permutations of degree n with the usual operation of multiplication of permutations is called the* ***symmetric group of degree n*** *and is denoted by* S_n.

Definition. *The* ***cyclic permutation*** *(or a* ***cycle****) is a permutation which maps some elements to each other in a cyclic fashion, while fixing all others.*

Theorem. *Every permutation can be uniquely represented (up to different ordering of factors) by a product of independent cycles.*

Definition. *The permutation* $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ *is called even or odd according to the parity of the number of inversions in the lower row.*

Alternating Groups of Degree n

Definition. *The group of all even permutations of degree n is called the* ***alternating group of degree n*** *and is denoted by* A_n.

Theorem. *For* $n \geq 4$ A_n *is not commutative.*

$$(1 \quad 2 \quad 3) \cdot (3 \quad 4 \quad 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$(3 \quad 4 \quad 5) \cdot (1 \quad 2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$$

S_n Solubility

Theorem. *For $n \geq 5$ the symmetric group S_n is not soluble.*

Proof plan:

1) The symmetric group S_n for $n \geq 5$ contains a subgroup isomorphic to A_5;
2) A_5 is not soluble;
3) Every subgroup of a soluble group is soluble *(see before)*, then S_n can't be soluble for $n \geq 5$.

S_n Solubility: Part 1

Lemma. The symmetric group S_n for $n \geq 5$ contains a subgroup isomorphic to A_5.

Proof:

It's easy to see that the subgroup of S_n containing all permutations of type

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & n \\ i_1 & i_2 & i_3 & i_4 & i_5 & 6 & \dots & n \end{pmatrix}$$

with an even number of inversions in i_1, i_2, i_3, i_4, i_5 is isomorphic to A_5.

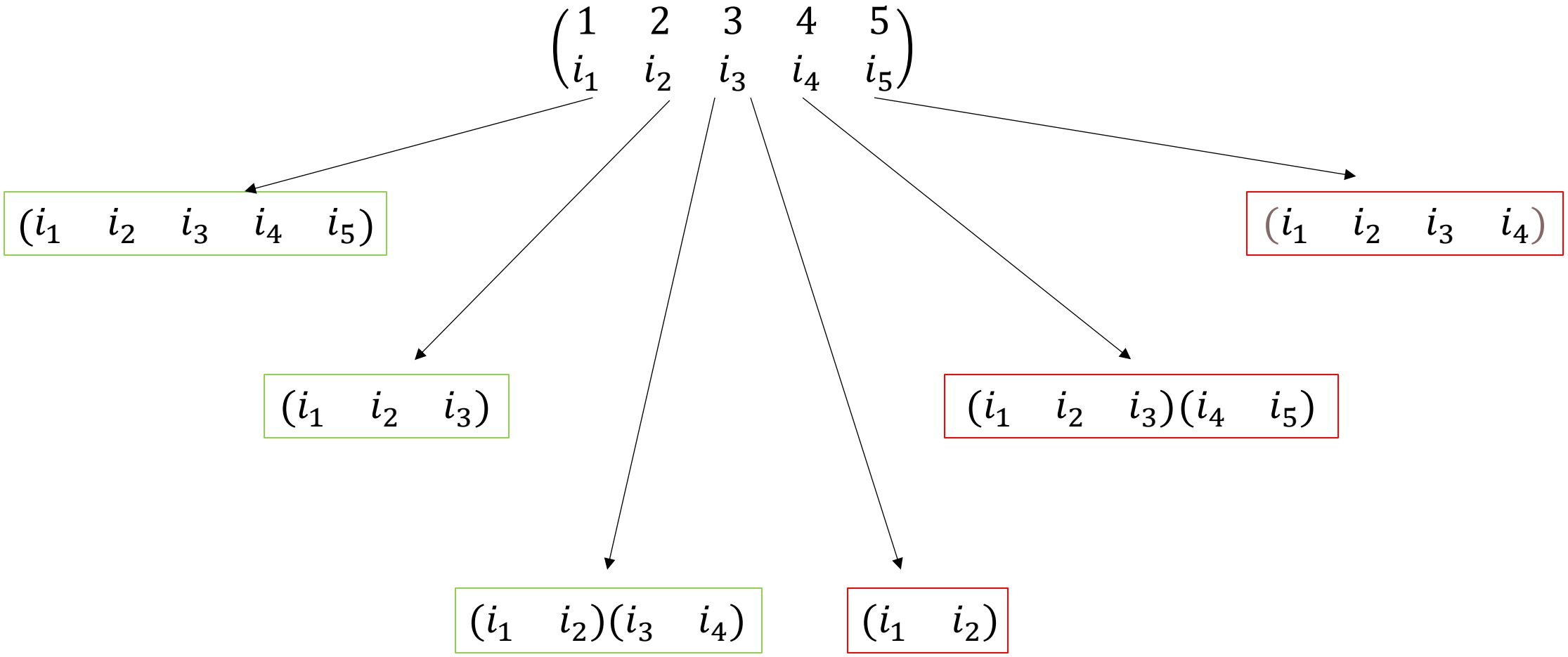
S_n Solubility: Part 2

Lemma. A_5 is not soluble.

Proof plan:

1) Every even permutation of degree 5, different from the identity, can be decomposed into independent cycles in just one of the following ways: $(i_1 \quad i_2 \quad i_3 \quad i_4 \quad i_5)$, $(i_1 \quad i_2 \quad i_3)$, $(i_1 \quad i_2)(i_3 \quad i_4)$;
2) Let N be a normal subgroup of A_5. Then if N contains a permutation which splits into independent cycles in one of the ways above, N contains all the permutations splitting into independent cycles in this way;
3) The group A_5 doesn't contain normal subgroups except the identity and the whole group;
4) As A_5 is not commutative and has no normal subgroups except the identity and the whole group, it is not soluble.

S_n Solubility: Part 2.1



S_n Solubility: Part 2.2

Let N contain a permutation a of type $(i_1 \quad i_2 \quad i_3 \quad i_4 \quad i_5)$.

Suppose that $a = (1 \quad 2 \quad 3 \quad 4 \quad 5)$. Let's prove that $(i_1 \quad i_2 \quad i_3 \quad i_4 \quad i_5) \in N$.

- The row i_1, i_2, i_3, i_4, i_5 has an even number of inversions:

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$ is even, then N contains $gag^{-1} = (i_1 \quad i_2 \quad i_3 \quad i_4 \quad i_5)$;

- The row i_1, i_2, i_3, i_4, i_5 has an odd number of inversions:

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_4 & i_2 & i_5 & i_3 \end{pmatrix}$ is even, then N contains $gag^{-1} = (i_1 \quad i_4 \quad i_2 \quad i_5 \quad i_3)$ and $(gag^{-1})^2 = (i_1 \quad i_2 \quad i_3 \quad i_4 \quad i_5)$.

S_n Solubility: Part 2.2

Let N contain a permutation a of type $(i_1 \quad i_2 \quad i_3)$.

Suppose that $a = (1 \quad 2 \quad 3)$. Let's prove that $(i_1 \quad i_2 \quad i_3) \in N$.

- The row i_1, i_2, i_3, i_4, i_5 has an even number of inversions:

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$ is even, then N contains $gag^{-1} = (i_1 \quad i_2 \quad i_3)$;

- The row i_1, i_2, i_3, i_4, i_5 has an odd number of inversions:

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_5 & i_4 \end{pmatrix}$ is even, then N contains $gag^{-1} = (i_1 \quad i_2 \quad i_3)$.

S_n Solubility: Part 2.2

Let N contain a permutation a of type $(i_1 \quad i_2)(i_3 \quad i_4)$.

Suppose that $a = (1 \quad 2 \quad 3)$. Let's prove that $(i_1 \quad i_2)(i_3 \quad i_4) \in N$.

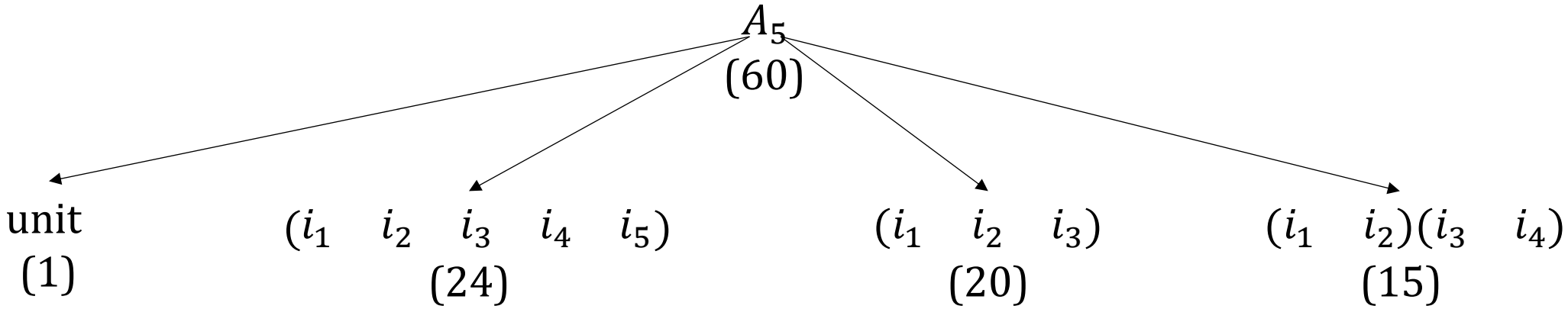
- The row i_1, i_2, i_3, i_4, i_5 has an even number of inversions:

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$ is even, then N contains $gag^{-1} = (i_1 \quad i_2)(i_3 \quad i_4)$;

- The row i_1, i_2, i_3, i_4, i_5 has an odd number of inversions:

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_2 & i_1 & i_3 & i_4 & i_5 \end{pmatrix}$ is even, then N contains $gag^{-1} = (i_1 \quad i_2)(i_3 \quad i_4)$.

S_n Solubility: Part 2.2



Abel's Theorem Proof: Part 2

Introducing the Loops

We will be introducing the groups of monodromy through the loops. First, we should prove that the loops form a group. In order to do that, let us go over some definitions first.

Definition. *A **loop of a point x_0 in a space X** is a path $C\colon I \to X, t \to C(t)$ such that $C(0) = C(1) = x_0$.*

Definition. *Two loops C and C' are called **homotopic** (noted as $\varphi \sim \varphi'$) if there's such a homotopy $C_s\colon I \to X$ such that $C_0 = C$, $C_1 = C'$, $C_s(0) = C_s(1) = x_0$ and $0 \leqslant s \leqslant 1$ (the last condition makes sure that the homotopy is continuous at the ends of the pathways).*

Definition. *The **product** $C_1 \cdot C_2$ of two loops C_1 and C_2 is a loop C such that $C(t) = C_1(2t)$ with $0 \leqslant t \leqslant \frac{1}{2}$ and $C(t) = C_2(2t)$ when $\frac{1}{2} \leqslant t \leqslant 1$. In other words, the product of two loops is a loop made of two connected loops that are being passed consequentially (with double speed).*

Why the Loops Form a Group

Loops are a group only if the next three conditions are true:

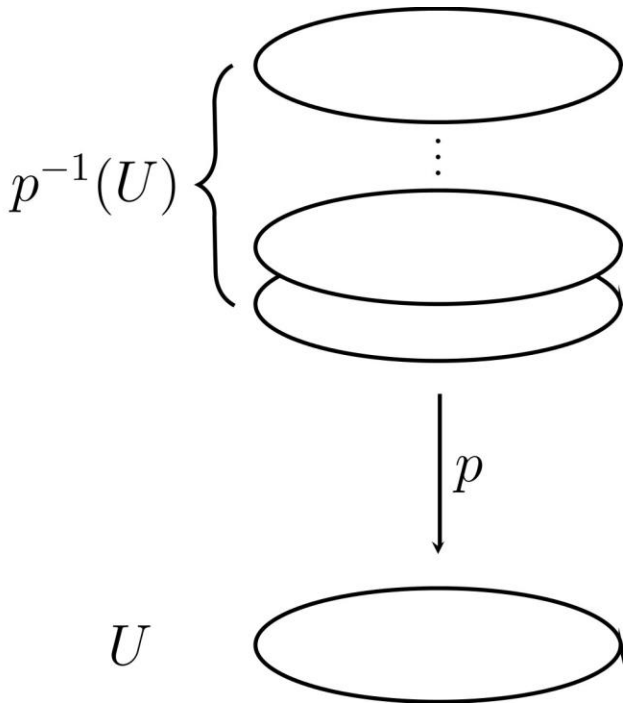
1) Associativity: $(C_1 \cdot C_2) \cdot C_3 = C_1 \cdot (C_2 \cdot C_3)$
2) Existence of unit element: There's such a loop e, so that $C \cdot e = e \cdot C = C$
3) Existence of inverse element: For every loop C there's such a loop C^{-1}, so that $C \cdot C^{-1} = e$

We're not going to go into the details of the proof right now, since we don't have enough time to do that, but turns out that all of the above are true.

Loops (we think that two loops stick together if there is a homotopy between them) form a group. This group is usually noted as $\pi(X, x_0)$, where X is a space and x_0 is a chosen point.

Coverings

Definition. *A finite (of degree n) covering of a topological space X is a continuous surjective map $f: Y \to X$, such that $\forall x \in X$ there is an open neighborhood U_x such that $f^{-1}(U_x) \cong \coprod_{i=1}^{n} V^{(i)}$ where $f \left| V^{(i)} : V^{(i)} \to U_x \right.$ is a homomorphism.*



Turns out that we can lift any path (or loop) from the space X onto Y. That is because the paths are compact, we can easily cover them with the finite amount of liftable neighborhoods.

Relation of the Groups of the Loops and the Monodromy Groups

Loops are operating on the set of the preimages of the point x_0. We can associate them with branches (*branches – images of the biggest liftable neighborhoods). Loops permute the branches.

Therefore, we can map the group $\pi(X, x_0)$ onto the group S_n (the symmetric group or the group of permutations).

Monodromy group will be the image of this mapping. Monodromy groups act on branches.

Monodromy Property

The property of the coverings stated in the last paragraph of the previous slide helps us prove a fact that is called monodromy property.

Monodromy property. *If there are two homotopic loops C_1 and C_2 that join the points z_0 and z_1 on the plane z, then the value $w(z_1)$ of the function w is uniquely defined by continuity along the loops C_1 and C_2 (when a value $w_0 = w(z_0)$ is chosen).*

Loop could be lifted in n different paths with the initial point in every preimage of x_0. When the loop is lifted it could either stay the loop or be deformed into an interval.

Therefore, any loop of X is operating on the preimages of x_0.

Monodromy property makes a conclusion, that homotopic loops are acting the same way.

Riemann Surfaces

Definition. *If more than one value of* w *corresponds to each value of* z *we call* $w(z)$ *a* ***multivalued function****.*

Define another multivalued function F: $z \to (z, w(z))$

$$C \to C \times C$$

Let's take projection from $Im(F)$ to the first coordinate. Obviously, it's surjective.

For certain good functions this is going to be a covering without some finite amount of points in C.

$Im(F)$ without the images of the points that were not included in covering is a RS.

Scheme of RS is a way to show how monodromy group operates on the covering.

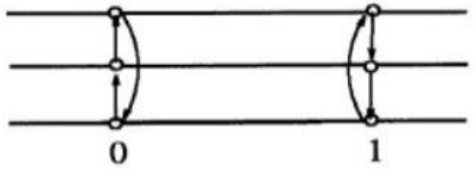


Fig. The scheme of RS of function $\sqrt[3]{z(z-1)^2}$

Abel's Theorem Proof: Part 3

Monodromy Groups of Functions Representable by Radicals

Theorem. *If the multi-valued function $h(z)$ is representable by radicals its monodromy group is soluble.*

Theorem 1. *The first theorem helps to build the schemes of the Riemann surfaces of the functions $h(z) = f(z) + g(z)$, $h(z) = f(z) - g(z)$, $h(z) = f(z) \cdot g(z)$, $h(z) = \frac{f(z)}{g(z)}$ starting from the schemes of the Riemann surfaces of the functions $f(z)$ and $g(z)$ with the same cuts.*

Theorem 2. *The second theorem helps to build the scheme of the Riemann surface of the function $h(z) = \big(f(z)\big)^n$ starting from the scheme of the Riemann surface of function $f(z)$ defined by the same cuts.*

Theorem 3. *The third theorem helps to build the scheme of the Riemann surface of the function $h(z) = \sqrt[n]{f(z)}$ starting from the scheme of the Riemann surface of the function $f(z)$ defined by the same cuts.*

What We Can Do by Using the Theorem 1

Definition. *The **direct product** $G \times F$ of groups G and H is the set of all the ordered pairs (g, h), where $g \in G$ and $h \in H$, with the binary operation: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$, where $g_1 g_2$ is taken in G, and $h_1 h_2$ in H.*

Prove that if F and G are the permutation groups of the initial schemes (of functions $f(z)$, $g(z)$), then the permutation group of the scheme built by the formal method is isomorphic to a subgroup of the direct product $G \times F$.

Let H_1 and H_2 be the permutation groups of the scheme built by the formal method and of the real scheme of the Riemann surface of the function $h(z)$ correspondingly. We can prove that there exists a surjective homomorphism of H_1 onto H_2.

Then we obtain the final statement that will help us to prove the main theorem:

Statement 1. *Suppose the monodromy groups of the functions $f(z)$ and $g(z)$ be soluble. Then the monodromy groups of the function $h(z)$ are soluble as well.*

What We Can Do by Using the Theorem 2

Statement 2. *Suppose the monodromy group of the function* $f(z)$ *be soluble. Then the monodromy group of the function* $h(z) = \big(f(z)\big)^n$ *is also soluble.*

To prove this theorem, we need to use the second of the auxiliary theorems and also the second problem from the last block.

What We Can Do by Using the Theorem 3

Let H be the permutation group of a scheme of the function $h(z) = \sqrt[n]{f(z)}$ and F the permutation group of a scheme of the function $f(z)$ made with the same cuts. Define a surjective homomorphism of the group H onto the group F.

Prove that the kernel of the homomorphism defined by the solution of the preceding problem is commutative.

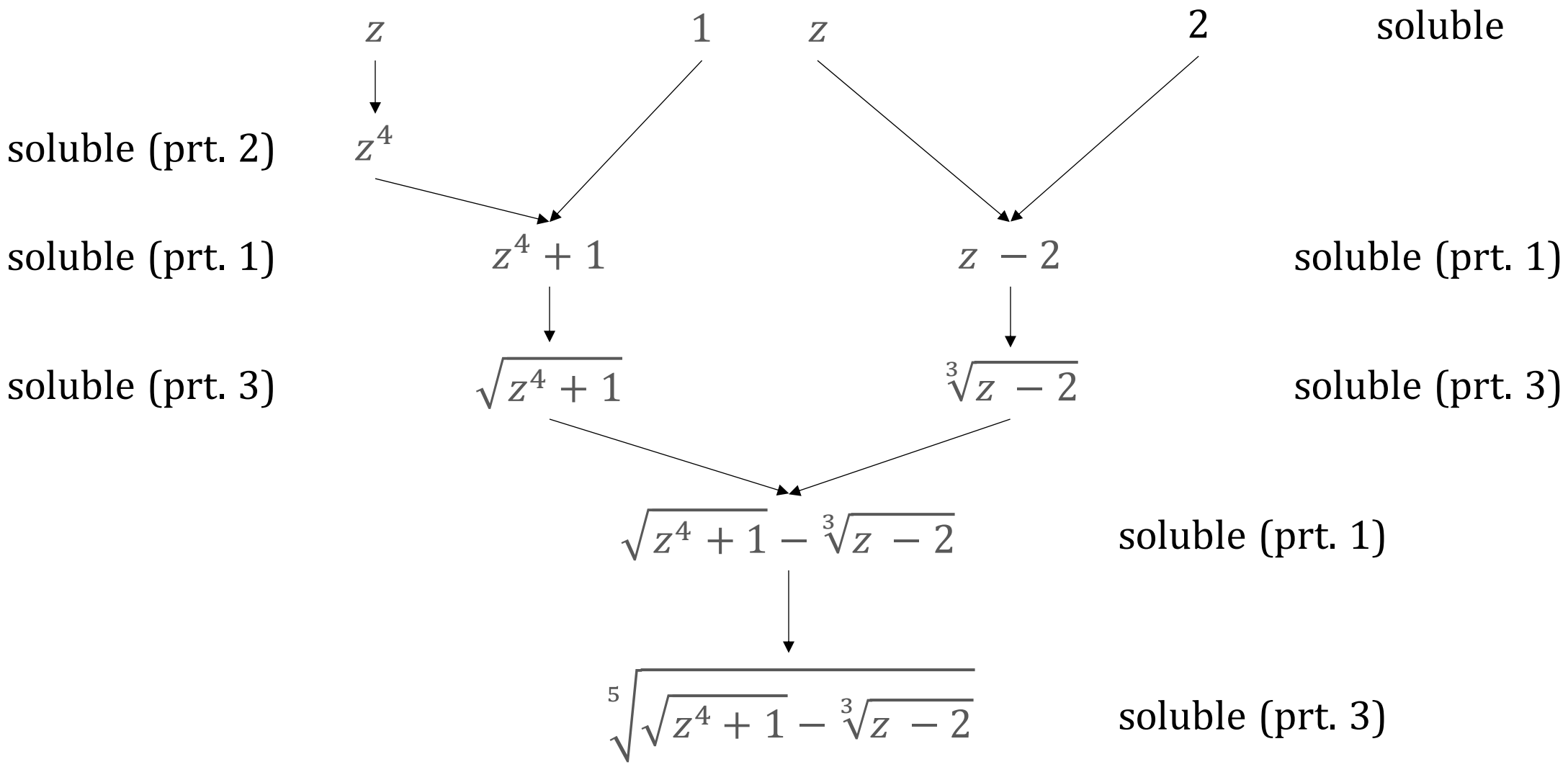
Then we obtain the final statement that will help us to prove the main theorem:

Statement 3. *Suppose the monodromy group F of the function $f(z)$ be soluble. Then the monodromy group H of the function $h(z) = \sqrt[n]{f(z)}$ is also soluble.*

Final Step

In order to prove the main theorem, the main statements of each of the three parts should be combined. Let's prove, for example, that the monodromy group of the function $\sqrt[5]{\sqrt{z^4+1}-\sqrt[3]{z-2}}$ is soluble:

Final Step


z
1
z
2
soluble
soluble (prt. 2)
z^4
soluble (prt. 1)
$z^4 + 1$
$z - 2$
soluble (prt. 1)
soluble (prt. 3)
$\sqrt{z^4 + 1}$
$\sqrt[3]{z - 2}$
soluble (prt. 3)
$\sqrt{z^4 + 1} - \sqrt[3]{z - 2}$
soluble (prt. 1)
$\sqrt[5]{\sqrt{z^4 + 1} - \sqrt[3]{z - 2}}$
soluble (prt. 3)

Monodromy group of some polynomial function

Consider $P_z(w) = a_5w^5 + a_4w^4 + a_3w^3 + a_2w^2 + a_1w + z$.

Let z_0: $P_{z_0}(w)$ has 5 roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Then $\forall\epsilon > 0\ \ \exists\rho > 0$: $\forall z_0'\ |z_0 - z_0'| < \rho$. For any $i = 1, 2, 3, 4, 5$ there exist β_i: β_i is a root of the $P_z(w)$ and $|\alpha_i - \beta_i| < \varepsilon$.

Observation 1. *For some polynomials*

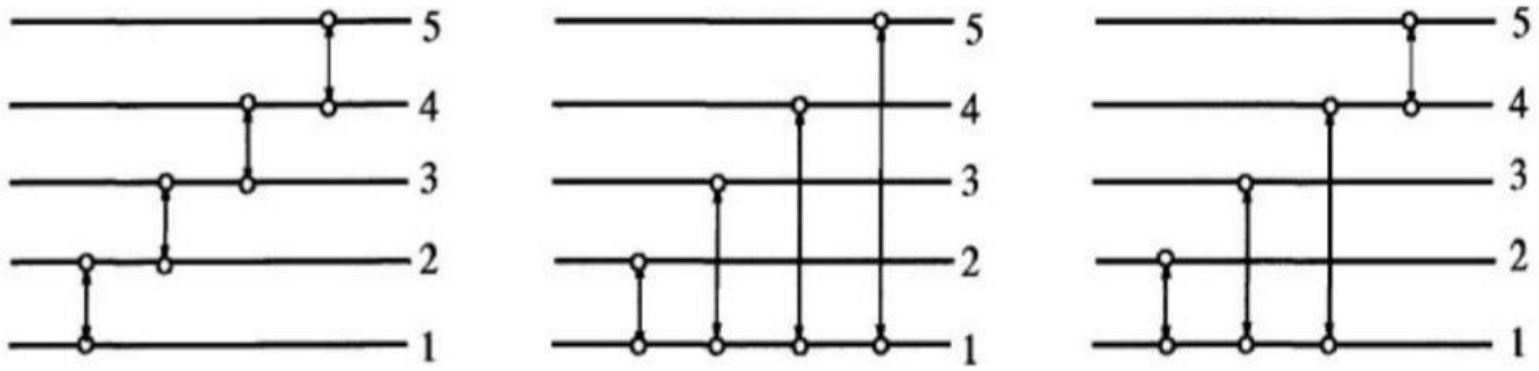
$$P_z'(w) = 5a_5(w - w_1)(w - w_2)(w - w_3)(w - w_4),$$

where w_1, w_2, w_3, w_4 *are different.*

Schemes of such groups

Observation 2. *z_i is a branch point.*

Due to observations and how these polynomials work at branch points we can travel only between 2 branches and other remain the same, so schemes are look like this:



Final statement

Statement. *In any possibility that 4 transpositions generate all* S_5.

Observation. *If the roots of polynomial* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ *are representable by radicals, then it is still true for any choice of* a_n, a_{n-1}, …, a_0 *if* $a_n \neq 0$.

Finally, combining the Observation, the existence of polynomials with insoluble monodromy groups and the Theorem, we get the **Abel's Theorem**.

Thank You!

- The organizers of Yulia's Dream program
- Our mentor Elizaveta
- Our parents and friends
- And **you all for your attention!**