Abel's Theorem

Mentor: Tang-Kai Lee

Rishi Gujjar, Shane Lee, Henry Stepanyants

MIT PRIMES

December 6th, 2022

Introduction

Any quadratic of the form $ax^2 + bx + c$ can be solved with the handy formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Introduction

Similarly, the formula for cubic polynomials is

$$x = \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} + \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) - \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}.$$

The quartic formula is too large to fit on a slide.

Introduction

Abel's Impossibility Theorem: There is no general solution in radicals to polynomial equations of degree five or higher with arbitrary coefficients.

Group Theory

Definition of a Group

A *group* consists of a set and a well-defined binary operation.

We can denote groups as $(G, \cdot)$.

We can also denote groups as simply G.

Properties of a Group

Every group $(G, \cdot)$ has the following properties:

- **Identity:** There exists an identity element e such that for any element $g \in G$, $e \cdot g = g \cdot e = g$.
- **Inverse:** For every element $g \in G$, there exists an inverse element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.
- **Associativity:** For any three elements $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Closure:** For any two elements $a \cdot b \in G$, $a \cdot b$ is also contained in G.

These properties are sufficient and necessary to define a group.

Basic Example of a Group

One of the simplest examples of a group is $(\mathbb{Z}, +)$, or the group of integers under addition.

- **Identity:** 0 is an identity element because for any integer a, $a + 0 = 0 + a = a$.
- **Inverse:** For any integer a, its additive inverse is $-a$.
- **Associativity:** For any three integers a, b, c, $(a + b) + c = a + (b + c)$.
- **Closure:** The sum of any two integers is also an integer.

Some Definitions

Subgroup: A *subgroup* is a group H contained within another group G.

Order: The *order* of a group is the number of elements.

Permutations

Permutation of degree n: A *permutation of degree n* is a permutation of the integers $1, 2, \ldots, n$.

Every permutation of degree n can be written in the form

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

where i_m is the image of the element m under the permutation.

Permutations *cont.*

For example, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

maps 1 to 3, 3 to 4, 4 to 1, and 2 and 5 to themselves.

1, 3, and 4 are permuted cyclicly. We call such permutations *cyclic permutations*, which have their own notation. This particular permutation can be written as (134).

Permutations *cont.*

All non-trivial permutations can be decomposed into a unique product of independent cyclic permutations. For example, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

can be written as $(134) \cdot (25)$.

Permutations *cont.*

Permutations can be composed together.

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

This provides us with a group operation.

Symmetric Group: The group of all permutations of degree n is called the *symmetric group of degree n* and is denoted by S_n.

Transpositions

Transposition: A *transposition* is a cycle consisting of two elements.

Lemma

Every cycle can be written as a product of transpositions.

As an example,

$$(14325) = (1 \cdot 5)(1 \cdot 2)(1 \cdot 3)(1 \cdot 4).$$

Therefore, all permutations can be written as a product of transpositions.

$$\text{Permutations} \longrightarrow \text{Cycles} \longrightarrow \text{Transpositions}$$

Parity and Alternating Group

We call a permutation *even* or *odd* based on the parity of the number of transpositions in any decomposition of that permutation.

$$\text{even permutation} \cdot \text{even permutation} = \text{even permutation}$$

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

Normal Groups and the Commutant

Normal Subgroup: A *normal subgroup* is a subgroup H of G such that for any element $g \in G$ and $h \in H$, $ghg^{-1} \in H$.

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

Commutant: The *commutant* of a group G, denoted by $K(G)$, is the set of all possible products of commutators of G.

Lemma

$K(G)$ is a **normal** subgroup of G.

Soluble Groups

Soluble: A group G is *soluble* if the sequence of groups G, $K(G)$, $K_2(G)$, $K_3(G)$, ... ends, for a finite n, with the unit group $\{e\}$.

As an example,

$$K(S_3) = \{e, (123), (132)\},$$

and

$$K(\{e, (123), (132)\}) = \{e\},$$

so S_3 is soluble.

Soluble Groups *cont.*

Lemma

Every subgroup of a soluble group is soluble.

Lemma

Suppose that a group G is not commutative and has no normal subgroups other than $\{e\}$ and G. Then G is not soluble.

Alternating Group of Degree 5

We now show that A_5, the alternating group of degree 5, is not soluble.

We do this by using the previous lemma with the fact that A_5 has no normal subgroups besides itself and $\{e\}$.

Alternating Group of Degree 5 *cont.*

Each of the possible even permutations of degree 5 belong in one of these categories:

1. (), the identity. 1 such element exists.
2. (abc), a cycle of size three. $\binom{5}{3} \cdot 2 = 20$ such elements exist.
3. $(abcde)$, a cycle of size five. $4! = 24$ such elements exist.
4. $(ab)(cd)$, two cycles of size two. $\binom{5}{2} \cdot \binom{3}{2}/2 = 15$ such elements exist.

Alternating Group of Degree 5 *cont.*

Lemma

If any normal subgroup of A_5 contains at least one element of a certain category, it contains all elements of that category.

Every normal subgroup of A_5 must therefore contain a category entirely, or not contain it at all. The identity is contained by default. The sizes of categories 2, 3, 4 are 20, 15, 24.

Sizes of Possible Combinations				
	Neither 2 nor 3	2	3	2 & 3
No 4	1	21	16	36
4	25	45	40	60

Alternating Group of Degree 5 *cont.*

Theorem

The order of a subgroup divides the order of the whole group (Lagrange's Theorem).

The order of A_5 is 60.

The only two possible combinations of categories that had a size that divides 60 are just category 1 and categories 1, 2, 3, and 4. These combinations correspond with $\{e\}$ and A_5.

Therefore, the only normal subgroups of A_5 are A_5 and $\{e\}$.

Therefore, A_5 is not soluble.

Complex Analysis

Definition of a Complex Number

We define the complex numbers $\mathbb{C}$ by adjoining $i = \sqrt{-1}$ to the real numbers. Under this consideration, the elements of the complex numbers are of the form $a + bi$ where $a, b \in \mathbb{R}$ with the well-defined operations,

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

Properties of $\mathbb{C}$

We note the following,

- Both $(\mathbb{C}, +)$ and $(\mathbb{C} - \{0\}, \cdot)$ form groups.
- The operations, $+, \cdot$ are commutative.
- They follow the distributive law: for any $a, b, c \in \mathbb{C}$,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Under these considerations we say that $\mathbb{C}$ is a *field*.

Fundamental Theorem of Algebra

$\mathbb{C}$ is *algebraically closed*: the roots of all non-constant polynomials with coefficients in $\mathbb{C}$ are also in $\mathbb{C}$.

Continuity

Definition

We say a function $f(z)$ is *continuous* at z_0 if for any $\epsilon > 0$ there exists a δ such that

$$|z - z_0| < \delta \implies |f(z) - f(z_0)| < \epsilon$$

where $|\cdot|$ is the standard Euclidean metric on $\mathbb{C}$.

If a function is continuous for every point on its domain, we say the function itself is continuous.

Continuous Functions

Examples

Some trivial examples of continuous functions are the constant function $f(z) = c$ and the identity function $g(z) = z$.

Lemma

The sum and product of continuous functions in $\mathbb{C}$ are also continuous. Thus, we can say that all polynomials are continuous.

Parametric Curves

We can also express functions in terms of a parameter t as shown.

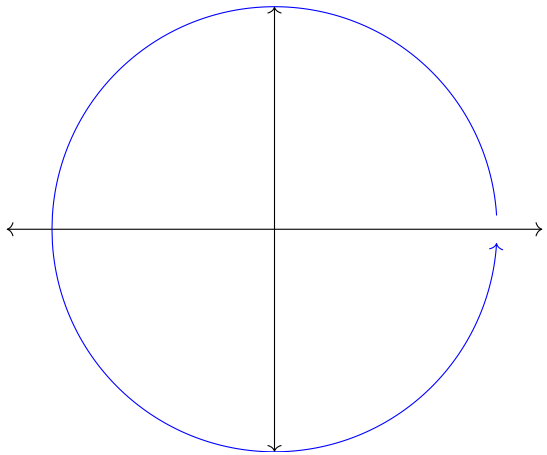


Figure: A parameterized unit circle, $f(t) = cos(2\pi t) + isin(2\pi t)$ where $t \in [0, 1]$.

Variation of Argument

Variation of Argument

For a continuous curve $f(t) : [0, 1] \to \mathbb{C} - \{0\}$, we define the variation of the argument $\varphi(t)$ to be the continuous function describing the argument.

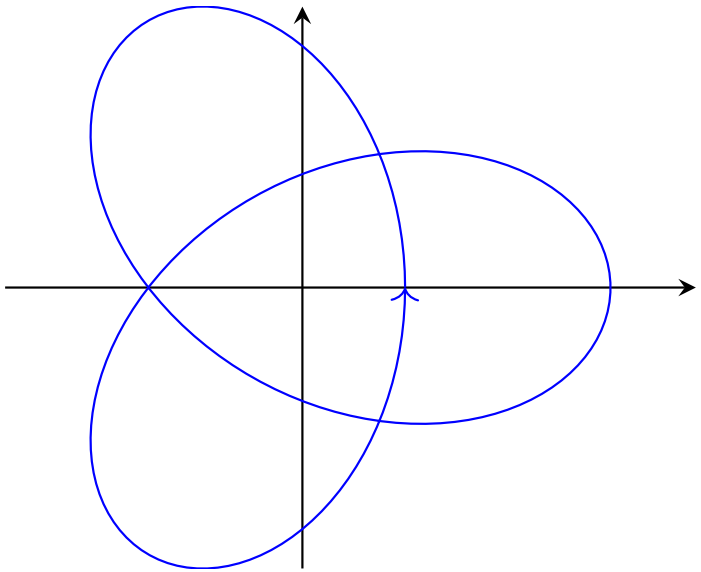


Figure: Trefoil, $f(t) = 2\text{cis}(2\pi t) - \text{cis}(4\pi t)$ where $t \in [0, 1]$.

Riemann Surfaces

So far, we have dealt with curves that have a single unique image. What about multi-valued functions like $\sqrt{z}$ where there are two complex solutions $\pm\omega_0$?
We create a branch cut on the complex plane from 0 to $-\infty$ twice. For the first cut, we take the root with a positive real component:

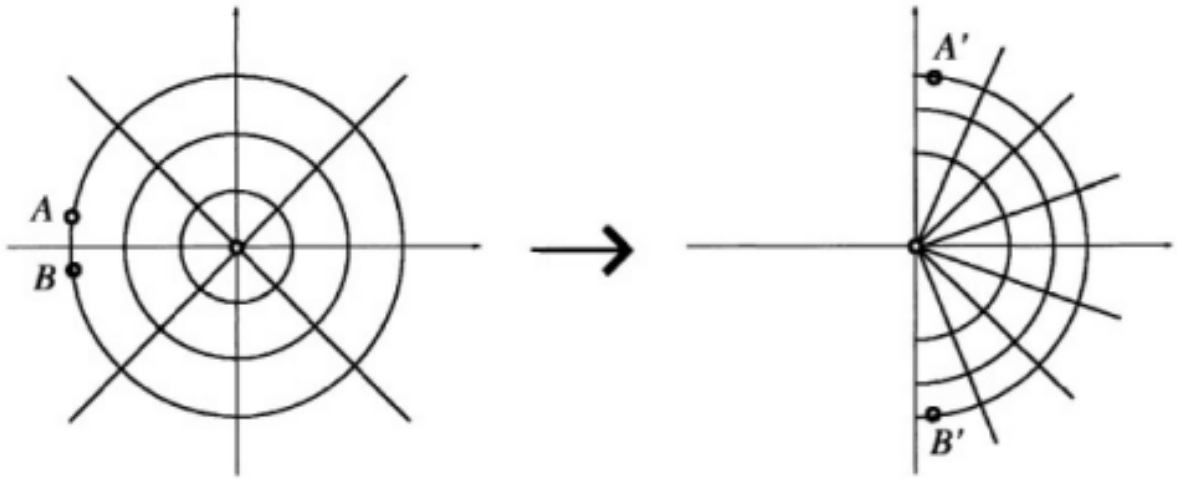


Figure: Riemann Sheet 1 of $\sqrt{z}$ (Abel's Theorem in Problems and Solutions by V.B. Alekseev)

Riemann Surfaces *cont.*

Then, for the second cut, we take the the root with a negative real component:

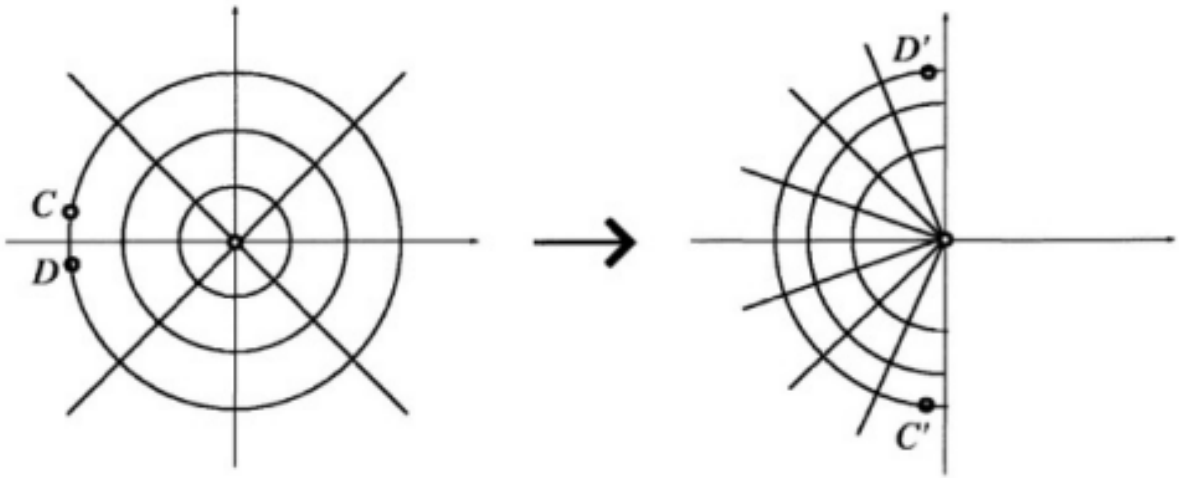


Figure: Riemann Sheet 2 of $\sqrt{z}$ (Abel's Theorem in Problems and Solutions by V.B. Alekseev)

Riemann Surfaces *cont.*

Stitching together these two Riemann "sheets" give us a Riemann surface that adequately describes $\sqrt{z}$:

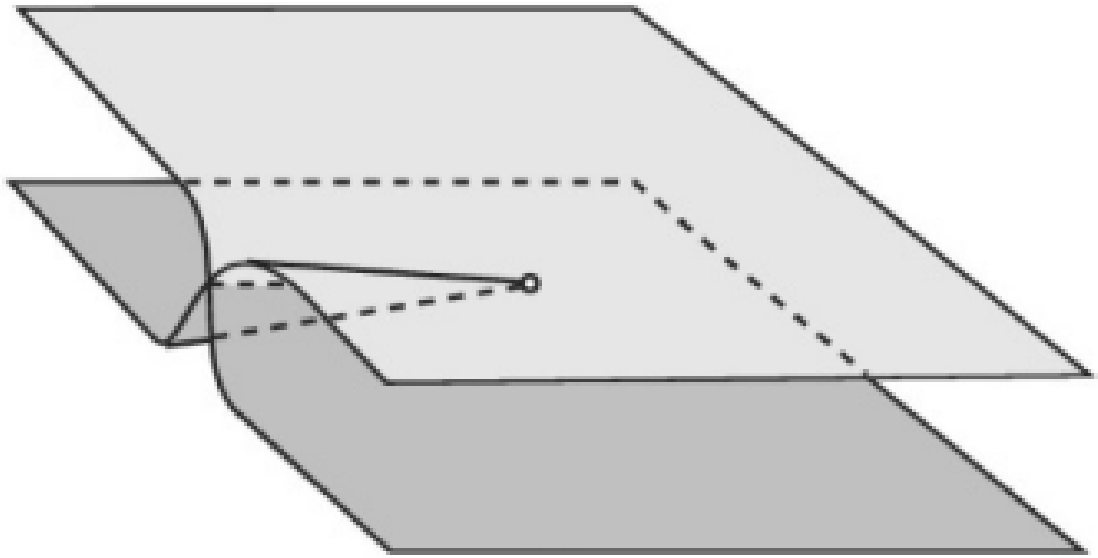


Figure: Riemann Surface of $\sqrt{z}$ (Abel's Theorem in Problems and Solutions by V.B. Alekseev)

Branch Points and Non-uniqueness Points

Definition

We say point z_0 is a *non-uniqueness* point if when a curve intersects it, then the uniqueness of the Riemann sheet of its image determined by continuity is lost.

Definition

We say point z_0 is a *branch* point if it is a non-uniqueness point such that for any curve a turn about z_0 will change the Riemann sheet of its image.

Example of a Riemann Surface

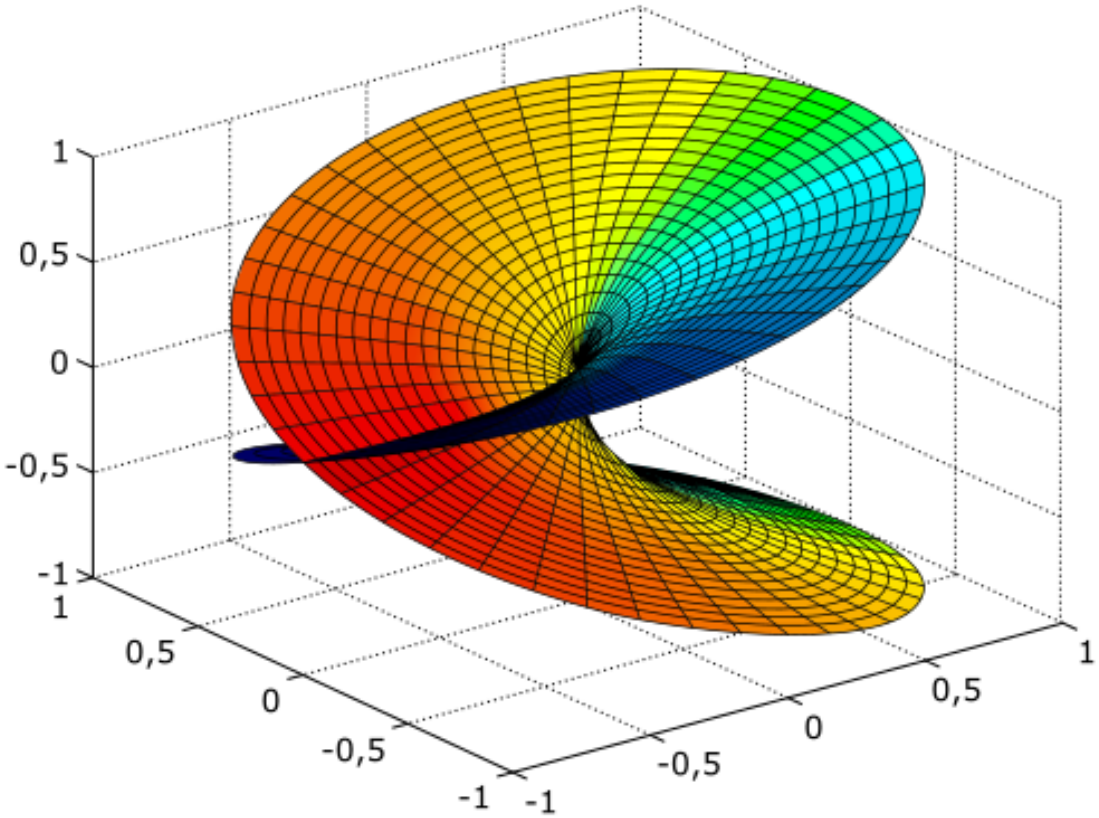


Figure: Riemann Surface of $\sqrt{z}$ (Wikipedia Commons)

Monodromy property

Definition

Suppose for two curves C_1 and C_2 from z_0 to z_1 such that they do not pass through any non-uniqueness points and C_1 can be continuously deformed to C_2. If the value of a function $w(z_1)$ when defined by continuity along C_1 and C_2 is always the same, then we say $w(z)$ has the monodromy property.

Monodromy group

Definition

We define the *monodromy group* of a function $f(z)$ as the group generated the permutation of sheets upon a turn of a branch point.

Example of a Monodromy group

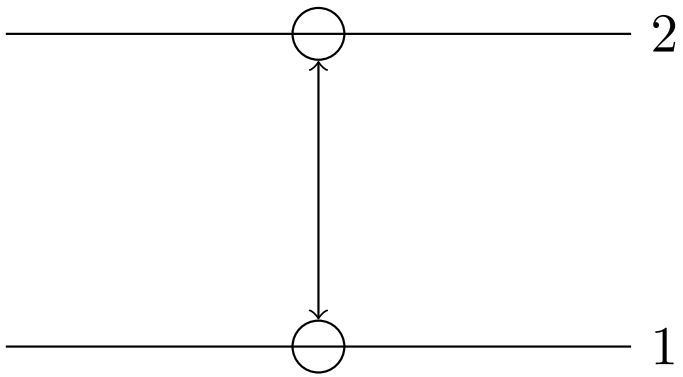


Figure: The monodromy group of $\sqrt{z}$ is S_2.

Solubility of Monodromy group

Definition

We say a function is *representable by radicals* if it can be expressed in terms of $f(z) = c$ and $g(z) = z$ through finite operations of addition, subtraction, multiplication, division, and taking the nth root where n is an integer.

Lemma

All functions that are representable by radicals have soluble monodromy groups.

The solubility of the monodromy group is an invariant under the aforementioned operations!

Abel's Theorem

Statement of Abel's Theorem

Abel's Theorem

The solutions of a general polynomial equation of degree $n \geq 5$ are not *representable by radicals* through its coefficients.

In other words, there isn't a good formula we can use to find the roots of a polynomial of the form

$$a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$$

or any general polynomial of greater degree.

Repeated roots

Consider the equation $w^5 - 5w + z = 0$, where w is a function of z. To find the values of z that lead to double roots of w, we can take its derivative and set it to 0:

$$5w^4 - 5 = 0 \rightarrow w = -1, 1, -i, i$$

Plugging these back into our original equation, we find that the corresponding values of z are $z = -4, 4, -4i, 4i$, respectively. Each polynomial using one of these values will have a double root for w.

Finding Branch Points

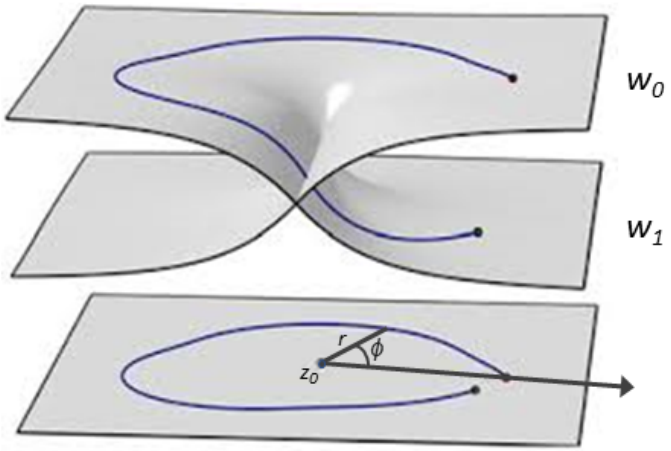


Figure: Riemann surface construction (Abel's Theorem in Problems and Solutions by V.B. Alekseev)

Assume r is very small. We can express any z as $z = z_0 + re^{i\phi}$, where $\phi \in [0, 2\pi)$. Consider $z_0 = 4$ and its corresponding double root $w_0 = 1$. We can rewrite our equation as

$$(w-1)^2(w^3 + 2w^2 + 3w + 4) = -re^{i\phi}.$$

Finding Branch Points *cont.*

For w very close to 1,

$$(w-1)^2 \approx -\frac{r}{10}e^{i\phi} = \frac{r}{10}e^{i(\phi+\pi)}.$$

Thus we have

$$w \approx 1 + \sqrt{\frac{r}{10}}e^{i(\frac{\phi+\pi}{2}+n\pi)},$$

where $n = 0, 1$. This is a multi-valued function that can only be represented by 2 sheets, with a branch point at $z_0 = 4$.
In general, a fifth-order equation like the one we have will need five Riemann sheets to be represented, as it has four branch points, $z = -4, 4, -4i, 4i$.

Drawing Schemes

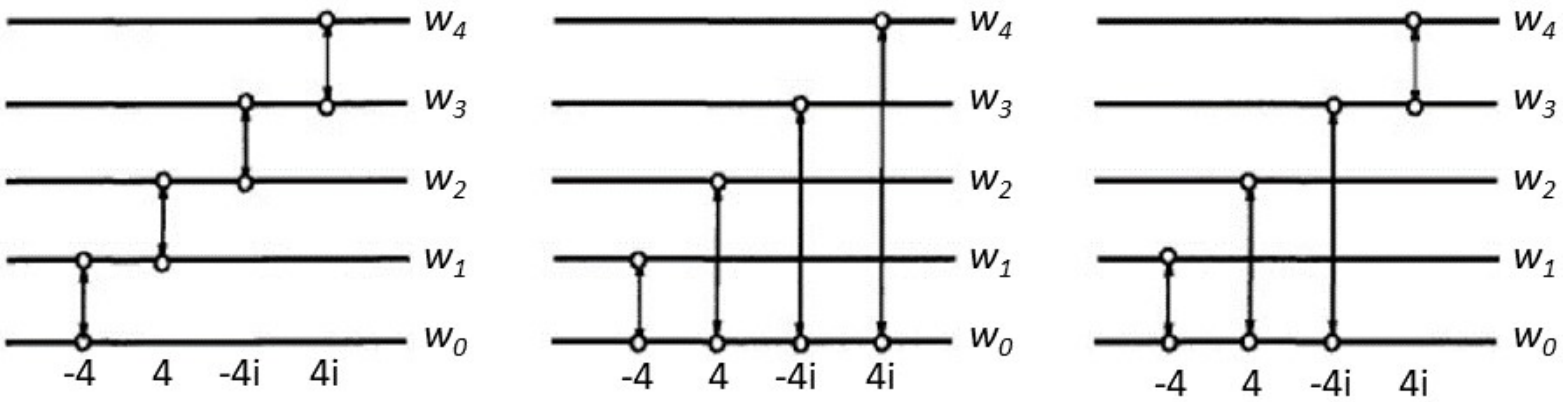
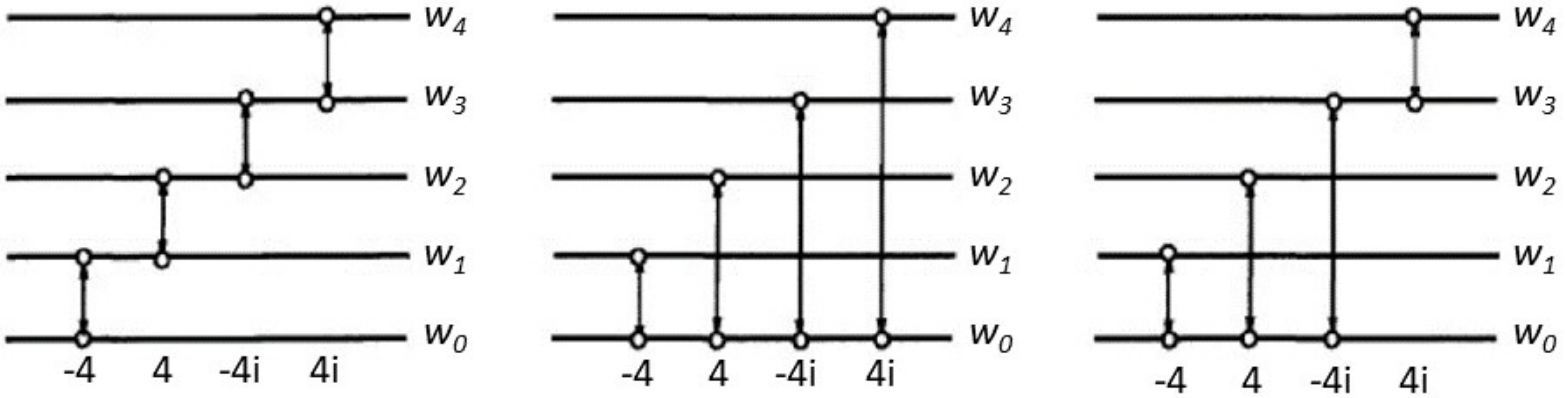


Figure: Schemes of $w^5 - 5w + z = 0$ (Abel's Theorem in Problems and Solutions by V.B. Alekseev)

These are the three ways we can connect our five sheets. None of them are the same, and there exist no other constructions that aren't identical to one of these three.

Drawing Schemes *cont.*



Definition

The transpositions (0, 1), (1, 2), (2, 3), ... are called elementary transpositions.

Lemma

If a subgroup of group S_n contains all elementary transpositions, then it coincides with the whole group S_n.

Proof of Abel's Theorem

Since the alternating group A_5 is a subgroup of S_5, by the lemma stated earlier, S_5 is not soluble. Thus, since our function w does not have a soluble monodromy group, it is not representable by radicals, so it is impossible to find the roots of a general fifth-order polynomial in this way.

Acknowledgements

We would like to thank Dr. Pavel Etingof and Dr. Slava Gerovitch for creating the MIT PRIMES program and giving us this opportunity, our mentor Tang-Kai Lee for guiding us through this material, and our parents for driving us to and from MIT every weekend.