TOPOLOGICAL GALOIS THEORY

ZHENYE QIAN

Abstract. This lecture note is typed by Zhenye Qian, thanks to instructor Jianfeng Lin in Yau Mathematical Sciences Center, Tsinghua University.

Contents

Date: February 17, 2025.

We give a schedule of following lectures:

Lecture 1 Introduction of modern Algebra and Topology.

Lecture 2 the Fundamental group of topological spaces and the topological proof of the fundamental theorem of Algebra.

Lecture 3 Solvable groups and uniformization group of multivalued functions.

Lecture 4 Topological Galois theory, proof of Abel-Ruffini theorem and Hilbert 13th problem.

1. Lecture 1: Introduction of Modern algebra and topology

1.1. **Introduction.**

¶ Classical Algebraic equations. First we recall the solution of **Quadratic** equation

$$x^2 + px + q = 0 \tag{1}$$

Via completing the square, we have

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2 - 4q}{4}$$

then the solution will be represented by

$$x = \frac{-p \pm \sqrt{p^2 - 4q}}{2} \tag{2}$$

and we denote the right term by Δ, that is $\Delta := \frac{p^2-4q}{4}$. Thus

(1) $\Delta > 0$, the equation 1 has **TWO** different solutions;
(2) $\Delta = 0$, the equation 1 has the ONLY solution;
(3) $\Delta < 0$, the equation 1 has complex[1] solutions.

Furthermore, we can be more focus on the **Cubic** equation

$$X^3 + bX^2 + cX + d = 0$$

Use a well-known transformation $X = x - \frac{b}{3}$, we can delete the quadratic term in the polynomial above and get the following eqution

$$x^3 + px + q = 0 \tag{3}$$

Then we let $x = u + v$, and obtain that

$$x^3 - 3uvx - (u^3 + v^3) = 0$$

compared with the equation 1, we have

$$\begin{cases} \frac{-p^3}{27} = u^3 \cdot v^3 \\ -q = u^3 + v^3 \end{cases}$$

and use the **Vièta theorem**, the eqations above will be regarded as the following Quadratic equation

$$\square^2 + q\square - \frac{p^3}{27} = 0$$

[1] If you have learned complex number, which is defined by following form:

$$z = \alpha + i\beta, \quad \alpha, \beta \in \mathbb{R}$$

where $\mathbb{R}$ is the real number field.

where $\square$ is the variable. Via equation 2, it is no hard to let

$$\begin{cases} u^3 = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} \\ v^3 = \frac{-q \mp \sqrt{q^2 + \frac{4p^3}{27}}}{2} \end{cases}$$

Thus the solution will be

$$x = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} \mp \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

which is called the **Cardano formula**. Similarly, let

$$\Delta := \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$$

A natural question is that: If $\Delta < 0$, if which means the equation 3 has no real solutions? In fact, the equation

$$x^3 - 6x - 4 = 0$$

where $\Delta = -4 < 0$, but the solutions will be

$$x_1 = -2, \quad x_2 = 1 + \sqrt{3}, \quad x_3 = 1 - \sqrt{3}$$

Another interesting example is

$$4x^3 - 3x - \frac{1}{2} = 0$$

where $\Delta = -\frac{3}{256} < 0$. But use the formula of Triple Angles, that is

$$4\cos^3\theta - 3\cos\theta - \frac{1}{2} = 0$$

the equation above has three real solutions ! that is

$$x_1 = \cos\frac{2\pi}{9}, \quad x_1 = \cos\frac{8\pi}{9}, \quad x_1 = \cos\frac{14\pi}{9}$$

However, via Galois theory, these numbers won't be calculate by finite $+, -, \times, \div$ or rooting arbitary number odd times or rooting non-negative number even times !

¶ Complex number. Thus we must extend the number category to rooting negative numbers, which is called the complex number, we have introduce it above, and recall some operations:

$$(a + ib) + (c + id) := (a + c) + i(b + d)$$

$$(a + ib) \cdot (c + id) := (ac - bd) + i(ad + bc)$$

where i means the imaginary unit, and $i^2 = -1$. And it is easy to verify all complex numbers (denoted by $\mathbb{C}$) become a **field**.

definition 1.1. Let $\mathbb{F}$ and two operations $+, \times$[2], we call $\mathbb{F}$ a **field**, if $+, \times$ satisfy

(1) **communative law**: $a+b=b+a,\ ab=ba, \quad \forall a,b\in\mathbb{F}$.
(2) **associative law**: $a+(b+c)=(a+b)+c,\ a(bc)=(ab)c, \quad \forall a,b,c\in\mathbb{F}$.
(3) **distribution law**: $(a+b)c=ac+bc, \quad \forall a,b,c\in\mathbb{F}$.
(4) **unit** there is $0,1\in\mathbb{F}$, such that $0+a=a,\ 1a=a, \quad \forall a\in\mathbb{F}$.
(5) **Inverse** For all elements $0\neq a\in\mathbb{F}$, there are $-a, 1/a\in\mathbb{F}$, such that $-a+a=0,\ 1/a\times a=1$.

After we recall the gemetry representation of complex numbers. Such the

(1) **norm** $|z|:=\sqrt{\alpha^2+\beta^2}, z=\alpha+i\beta$;
(2) **Angle** $\mathrm{Arg}(z)=\theta+2k\pi,\ k\in\mathbb{Z}$, where $-\pi<\tan\theta=\frac{\beta}{\alpha}\leq\pi$ and $\mathbb{Z}$ denoted by integers.

Use the observation (called **polar** representation of complex number)

$$z=r(\cos\theta+i\sin\theta), \quad r=|z| \tag{4}$$

It is easy to verify:

lemma 1.1. $|zw|=|z|\cdot|w|,\ \mathrm{Arg}(zw)=\mathrm{Arg}(z)+\mathrm{Arg}(w), \quad z,w\in\mathbb{C}$.

More useful formula is called **Euler formula**.

theorem 1.1 (Euler, 1748)**.**

$$e^{i\theta}=\cos\theta+i\sin\theta \tag{5}$$

where $e=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$, and we define

$$e^z=1+\frac{z}{1!}+\frac{z^2}{2!}+\cdots+\frac{z^n}{n!}+\cdots, \quad z\in\mathbb{C}$$

Particularly, we have $e^{i\pi}+1=0$.
¶ development of modern Algebra. Now, we can rooting any negative numbers, generally, for any complex number $z=re^{i\theta}$, where $r=|z|$ and θ is the angle of z, the form $\sqrt[n]{z}$ has actually n elements:

$$\sqrt[n]{z}:=\left\{r^{1/n}e^{i\frac{\theta+2k\pi}{n}}:k=0,1,\cdots,n-1\right\}$$

Back to the problem above,

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{\Delta}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\Delta}}, \quad \Delta=\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3$$

We can calculate this formula although $\Delta<0$. Therefore, we claim that any 3 degree polynomial with complex coefficients can calculate

[2]where we ignore the simbol $\times$.

all roots via Cardano formula. Furthermore, Ferrari found the formula of **Quartic** equation.

In fact, Gauss has proved a well-known theorem of n degree polynomials, which is called the **fundamental theorem of Algebra**

theorem 1.2 (Gauss, 1799)**.** Any n degree polynomial with complex coefficients has exactly n roots.

But Abel and Ruffini proved a more surprising consequence.

theorem 1.3 (Abel, 1824, Ruffini, 1813)**.** There are no radical solution for general polynomial equation with at least 5 degree.

where **radical solution** means a formula with finite $+, -, \times, \div$ and rooting for the coefficients of equation.

But Galois estabished the Group theory and Field theory to solve this problem by more elegant methods, which develop the modern Algebra. We show the theorem of him.

theorem 1.4 (Galois, 1830)**.** The polynomial equation has radical solution iff its Galois group is solvable.

For example the equations

$$x^5 - x - 1 = 0, \quad x^5 + x - 1 = 0$$

the left has no radical solution, but the right one does.

The Goal of this lecture and followings is to prove the fundamental theorem of Algebra via topology methods such fundamental groups, and introduce the **Topological Galois theory** developed by Arnold in 20th centary and prove the extention of Abel-Ruffini theorem.

1.2. **Topology and topological space.**

¶ Introduction of Topology. First we recall the concept of continuous mappings. Consider the distance of any two point in Eucldean space $\mathbb{R}^n$, for

$$x = (x_1, \cdots, x_n),\ y = (y_1, \cdots, y_n)$$

we have the distance

$$|x - y| := \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

Then for mapping $f : \mathbb{R}^m \to \mathbb{R}^n$, we call f is **continuous** at $x_0 \in \mathbb{R}^m$, if for all $\epsilon > 0$, there is a $\delta > 0$ such that

$$|f(x) - f(x_0)| < \epsilon, \quad |x - x_0| < \delta$$

We can abstract the essential property of concepts above, we call $U(\subset \mathbb{R}^n)$ an **open set**, if for all $x \in U$, there a open ball $B_r(x) \subset U$, where

$$B_r(x) := \{y \in \mathbb{R}^n : |x - y| < r\}$$

thus we can define the continuous of mapping $f : \mathbb{R}^m \to \mathbb{R}^n$ by following language:

"We call f continuous on $\mathbb{R}^m$, if for all open sets $U \subset \mathbb{R}^n$, the preimage $f^{-1}(U)$ is open in $\mathbb{R}^m$, where $f^{-1}(U) : \{x \in \mathbb{R}^m : f(x) \in U\}$."

Then we can define the general topological space.

definition 1.2. Let X be a set, $\tau(\subset \mathcal{P}(X))$ (where $\mathcal{P}(X)$ is the power set of X) is called a **topology** of X, if

(1) $\emptyset, X \in \tau$;
(2) For any two $U, V \in \tau$, $U \cap V \subset \tau$;
(3) For $\{U_i\}_{i\in I} \subset \tau$, $\bigcup_{i\in I} U_i \in \tau$, where I is index set.

We call (X, τ) a **topological space** and the elements in τ are **open**.

definition 1.3. Given two topological space $(X, \tau), (Y, \xi)$, we call mapping $f : X \to Y$ is **continutous**, if for all $U \in \xi$, we have $f^{-1}(U) \in \tau$. furthermore, we call f is a **homeomorphism** if f^{-1} exists and f^{-1} is also continuous, denoted by $X \cong Y$.

A unual example is Euclidean space $\mathbb{R}^n$ with open sets like $B_r(x),\ x \in \mathbb{R}^n$.

definition 1.4. Given a topological space (X, τ), and subset $A(\subset X)$, we define the **subspace topology** on A by

$$\tau_A := \{U \cap A : U \in \tau\}$$

and call (A, τ_A) a subspace of (X, τ).

¶ Quotient topology. First we recall the **equivalent relation** $\sim$ on any set X, which means

(1) $x \sim x,\ \forall x \in X$;
(2) If $x \sim y$ then $y \sim x$, where $x, y \in X$;
(3) If $x \sim y$ and $y \sim z$, then $x \sim z$, where $x, y, z \in X$.

and the **equivalent class** denoted by

$$[x] := \{y \in X : x \sim y\ \}$$

then the set of all equivalent classes is called the **quotient set**, denoted by $X/\sim$. Then we have a natural **quotient mapping**

$$q : X \to X/\sim$$

by $x \to [x]$ where is the equivalent class of x.

definition 1.5. Given a topological space (X, τ) and a equivalent relation $\sim$ on X, then

$$\tau_{X/\sim} := \{U \subset X/\sim : q^{-1}(U) \in \tau\}$$

become a topology on $X/\sim$, we call $(X/\sim, \tau_{X/\sim})$ a **quotient space** of X.

Some examples are interesting.

example 1.1. We denote D^{n+1} be **closed disk** in $\mathbb{R}^{n+1}$:

$$D^{n+1} := \{x \in \mathbb{R}^{n+1} : |x| \leq 1\}$$

and S^n be a sphere:

$$S^n := \{x \in \mathbb{R}^n : |x = 1|\}$$

they are all subspaces of $\mathbb{R}^{n+1}$. And we have a intuitive claim:

$$D^{n+1}/S^n \cong S^{n+1}$$

example 1.2. Consider the subspaces of plane $\mathbb{R}^2$ and $I := [0, 1]$.

(1) **flat ring** $A := I^2/(0, x) \sim (1, x)$.
(2) **Möbius band** $M := I^2/(0, x) \sim (1, 1 - x)$.
(3) **torus** $T^2 := I^2/(0, x) \sim (1, x),\ (x, 0) \sim (x, 1)$.
(4) **Klein bottle** $K := I^2/(0, x) \sim (1, x),\ (x, 0) \sim (1 - x, 1)$.

In fact the spaces are not homeomorphic with each other, but we need to establish some of invariants under homeomorphism. and in the following lectures we will introduce them.

2. Lecture 2: the Fundamental group of topological spaces

2.1. **Group theory.**

¶ Review of Groups. First we recall the concepts of groups. First we give some of examples. Consider a set

$$S_n := \{f : \{1, \cdots, n\} \to \{1, \cdots, n\} : f\text{is bijectioin}\}$$

We can equip it with operation called multiplicaiton

$$fg := g \circ f : S_n \times S_n \to S_n$$

where $g \circ f = g(f(x)),\ x \in \{1, \cdots, n\}$. This operation satisfies associative law, that is

$$f(gh) = (fg)h, \quad \forall f, g, h \in S_n$$

and all elements $f \in S_n$ has inverse f^{-1} such that

$$f^{-1}f = ff^{-1} = \mathrm{id} \in S_n$$

where id is identity. But in this example may **NOT** have $fg = gf$.

definition 2.1. Let G be a set, and a operation $\cdot : G \times G \to G$ (we always ignore $\cdot$). We call G be a **group**, if

(1) **associative law** $a(bc) = (ab)c, \quad \forall a, b, c \in G$;
(2) **unit** There is an element $e \in G$, such that $ea = ae = a, \quad \forall a \in G$;
(3) **inverse** Forall $a \in G$, there is an element $a^{-1} \in G$ such that $a^{-1}a = aa^{-1} = e$.

furthermore, we call G **Abelian** if satisfies communative law, that is

$$ab = ba, \quad \forall a, b \in G$$

example 2.1. $(\mathbb{Z}, +)$ is a Abelian group.

example 2.2. $(\mathbb{Z}_n, +)$ is a Abelian group, where $\mathbb{Z}_n := \mathbb{Z}/\sim$. Where the relation $\sim$ is defined by

$$x \sim y \Longleftrightarrow x \equiv y \mod n$$

example 2.3. $(S_n, \circ)$ is a group, we call **Symmetry Group**.

example 2.4. $(\mathbb{C}^*, \times)$ is a Abelian group, where $\mathbb{C}^* := \mathbb{C} - \{0\}$.

example 2.5. Let $\square^n$ be **Regular polygon** with n edges. And we consider all operations on it as follows:

- **rotation** anti-clockwise with angle $\frac{2k\pi}{n},\ 0 \le k \le n-1$ and denoted rotation of $\frac{2\pi}{n}$ by ρ, and other will be $\rho^k := \rho \circ \cdots \circ \rho$.
- **reflection** along **axis** of symmetry, denoted by r.

Then the operations with **composition** become a group, called **Dihedral Group**, denoted by D_n. This group is not a Abelian group, in fact for D_5, we consider

$$r \circ \rho \circ r^{-1} = \rho^{-1}$$

thus which is not Abelian.

¶ Homomorphism.

definition 2.2. Given two groups G, H, we call mapping $f : G \to H$ is a **homomorphism** if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G$$

furthermore we call f a **isomorphism**, if f is also a bijection.

example 2.6. recall example 2.3 and example 2.5, we can establish a isomorphism

$$f : D_3 \to S_3$$

where $f(g)$ is a **permutation** of vertex of $\square^3$. And recall example 2.2, we have another homomorphism

$$g : D_3 \to \mathbb{Z}_2$$

by $g(\rho) = [1],\ g(r) = [0]$.

2.2. **the Fundamental Group of topological space.**
¶ Path and path-connected. We recall γ a **path** in a topological space X, where

$$\gamma : I = [0, 1] \to X$$

is continuous and $\gamma(0), \gamma(1)$ are starting and endting. Particularly, we call γ **closed**, if $\gamma(0) = \gamma(1)$, thus we can regard closed path (we also called a **loop**) as

$$\gamma : S^1 \to X$$

We call topological X is **path-connected**, if for all points $x, y \in X$, there is a path link them, that is there is

$$\gamma : I \to X$$

such that $\gamma(0) = x,\ \gamma(1) = y$. Use this concept we can prove $\mathbb{R}$ is not homeomorphic to $\mathbb{C}$, indeed $\mathbb{R} - \{0\}$ is not path-connected but $\mathbb{C} - \{0\}$ does.

definition 2.3. Given two path γ, η in X. We define following operations:

(1) **inverse** $\gamma^- : I \to X := \gamma(1 - t)$.

(2) **composition** $\gamma \circ \eta : I \to X$ is denoted by

$$(\gamma \circ \eta)(t) := \begin{cases} \gamma(2t), & t \in [0, 1/2] \\ \eta(2t-1), & t \in (1/2, 1] \end{cases}$$

if $\gamma(0) = \eta(1)$.

¶ Homotopy between paths and Fundamental Group.

definition 2.4. Given two path γ, η in X with same fixed starting x and ending y . Define **homotopy** between γ and η, if there is a continuous mapping $H : I \times I \to X$ such that

(1) $H(t, 0) = \gamma(t),\ H(t, 1) = \eta(t)$;
(2) $H(0, s) = x,\ H(1, s) = y$.

denoted by $\gamma \simeq \eta$.

A simple fact is $\gamma \circ \gamma^- \simeq c$, where c is constant path, such as

$$c(t) = x \in X, \quad \forall t \in I$$

Now we can establish the Fundamental Group of topological spaces. Consider space X, and choose a **base point** x_0, and the following set

$$\Omega(X, x_0) := \{\gamma : S^1 \to X : \gamma(0) = \gamma(1) = x_0\}$$

and we define a equivalent relation $\sim$ on $\Omega(X, x_0)$, that is

$$\gamma \sim \eta \Longleftrightarrow \gamma \simeq \eta$$

Let $\pi(X, x_0) := \Omega(X, x_0)/\sim$ and define the operation

$$\cdot : \pi(X, x_0) \times \pi(X, x_0) \to \pi(X, x_0)$$

by

$$[\gamma] \cdot [\eta] = [\gamma \circ \eta]$$

theorem 2.1. $(\pi(X, x_0), \cdot)$is a group, called the **fundamental group** of X with base point x_0. Furthermore, we can ignore the base point x_0 if X is path-connected.

definition 2.5. We call space X is **simple-connected**, if $\pi(x) = 0$.

example 2.7. Let C be a **convex** subspace in $\mathbb{R}^n$, that is if $x, y \in C$, the line link x and y is also in C. Then C is simple-connected, indeed for all loops γ are homotopic to constant mapping c,consider

$$H(t, s) := (1 - s)\gamma(t) + s \cdot c$$

example 2.8. $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is **NOT** simple-connected, in fact we have

$$\pi(S^1) = \mathbb{Z}, \quad \gamma : S^1 \to S^1,\ \gamma(t) = e^{2\pi i t} \text{is } \textbf{generator}$$

and proved it later. Another example is $\pi(\mathbb{C}^*) = \mathbb{Z}$.

2.3. **the Fundamental group of S^1.** Now we want to calculate the fundamental group of S^1. Where we need the technique of covering spaces.

¶ Convering space.

definition 2.6. Consider continuous mapping $f : \overline{X} \to X$, we call f a covering mapping, if for all $x \in X$, there are open sets $U(\subset X)$ contains x such that $f^{-1}(U) = \bigsqcup_{i\in I} U_i$, where U_i is open in $\overline{X}$, $f : U_i \to U$ is homeomorphism. Where $\bigsqcup$ is **dijoint** union. And we call $\overline{X}$ a **covering space** of X. Futhermore, we call f a n **covering mapping**, if any $x \in X$ has n preimages.

example 2.9. The mapping $f : \mathbb{R} \to S^1$ by $f(\theta) = e^{2\pi i\theta}$ is a covering mapping.

Proof. We quickly verify f above is covering mapping. In fact for all $z = e^{2\pi i\theta_0} \in S^1$ has a simple neiborhood $U := \{e^{2\pi i\theta} : \theta \in (\theta_0 - 1/4, \theta_0 + 1/4)\}$, the preimages are

$$U_k = \{\theta + 2k\pi : \theta \in (\theta_0 - 1/4, \theta_0 + 1/4)\}$$

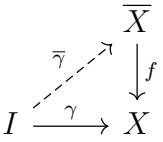
each of them are disjoint, and we have a natural homeomorphism between U_k and U. □

example 2.10. The mapping $f : \mathbb{C}^* \to \mathbb{C}^*$ by $f(z) = z^n$ is a n covering mapping.

¶ Lift property of paths.

definition 2.7. Let $f : \overline{X} \to X$ be covering mapping, and $\gamma : I \to X$ be a path in X, we call $\overline{\gamma}$ a **lift** of γ, if

$$f \circ \overline{\gamma} = \gamma$$



theorem 2.2 (Lift property of paths)**.** Given a covering mapping $f : \overline{X} \to X$, and path $\gamma : I \to X$. For any point $x \in f^{-1}(\gamma(0))$, we have

(1) there is a unique lift $\overline{\gamma} : I \to \overline{X}$ with x as starting;
(2) Suppose $\eta : I \to X$ satisfies $\eta \simeq \gamma$ and let $\overline{\eta} : I \to \overline{X}$ with x as starting, then there is $\overline{\eta} \simeq \overline{\gamma}$. Particularly, $\overline{\eta}(1) = \overline{\gamma}(1)$.

¶ Proof of $\pi(S^1) = \mathbb{Z}$. Now we use the Lift property of loops to prove $\pi(S^1) = \mathbb{Z}$.

proof of $\pi(S^1) = \mathbb{Z}$. We have following steps.

Step 1 Consider covering mapping $f : \mathbb{R} \to S^1$. And consider the decomposition $S^1 = U \cup V$, where

$$U := \{e^{2\pi i\theta}\theta \in (0, 3/4)\}, \quad V := \{e^{2\pi i\theta}\theta \in (1/4, 5/4)\}$$

Then $f^{-1}(U) = \bigsqcup_{k\in\mathbb{Z}} U_k$, where $U_k = (k, k+3/4)$ and $f : U_k \to U$ is a homeomorphism, so does V.

Step 2 Consider $\gamma : I \to X$, then $I = \gamma^{-1}(u) \cup \gamma^{-1}(v)$ and $\gamma^{-1}(U)$, $\gamma^{-1}(V)$ are open sets in I. Use the well-known Lebesgue lemma, we can let

$$0 = t_0 < t_1 < \cdots < t_N = 1$$

such that for all $0 \leq i \leq N-1$, we have

$$[t_i, t_{i+1}] \subset \gamma^{-1}(U) \quad \text{or} \quad [t_i, t_{i+1}] \subset \gamma^{-1}(V)$$

Step 3 Suppose $[0, t_1] \subset \gamma^{-1}(U)$, choose i such that $x \in U_i$, and define the lift $\overline{\gamma}$ on $[0, t_1]$ be

$$[0, t_1] \xrightarrow{\gamma} U \xrightarrow{(f|_{U_i})^{-1}} \overline{X}$$

Similarly, we can define $\overline{\gamma}$ totally. The uniqueness can be verify in every interval $[t_i, t_{i+1}]$.

Step 4 Finally, suppose there is a homotopy between another loop η and γ, called H. Similarly we can divide $I \times I$ into several cubes, and every cubes in $H^{-1}(U)$ and $H^{-1}(V)$, then lift H to $\overline{H} : I \times I \to \overline{X}$ and which is homotopy between $\overline{\eta}$ and $\overline{\gamma}$.

Step 5 Now given a loop $\gamma : S^1 \to S^1$, then lift it along f to $\overline{\gamma} : I \to \mathbb{R}$ (One may pay attention to the lift of loops may **NOT** be closed !) However, we have

$$f(\overline{\gamma}(1)) = \gamma(1) = \gamma(0) = f(\overline{\gamma}(0))$$

Thus $\overline{\gamma}(1) - \overline{\gamma}(0) \in \mathbb{Z}$, we define this integer be **linking number** of loop γ, denoted by $\mathrm{rot}(\gamma)$. For example, consider $\gamma_n : S^1 \to S^1$ by $\gamma_n(t) = e^{2\pi int}$, then $\overline{\gamma}_n(t) = nt$, then $\mathrm{rot}(\gamma) = \overline{\gamma}(1) - \overline{\gamma}(0) = n$.

Step 6 Via lift property of loops, we can verify if $\gamma \simeq \eta$, then $\mathrm{rot}(\gamma) = \mathrm{rot}(\eta)$. And if loops γ and η have the same starting and ending, we can choose the lift $\overline{\gamma}$ and $\overline{\eta}$ such that $\mathrm{rot}(\gamma) = \mathrm{rot}(\eta)$, since $\mathrm{rot}(\gamma) = \mathrm{rot}(\eta)$, then $\overline{\gamma}(1) = \overline{\eta}(1)$. Thus $\overline{\gamma}$ and $\overline{\eta}$ can be homotopied by

$$\overline{H} : I \times I \to \mathbb{R}, \quad \overline{H}(t, s) := (1-s)\overline{\gamma}(t) + s \cdot \overline{\eta}(t)$$

then $f \circ \overline{H}$ gives a homotopy between $\gamma \simeq \eta$. And

$$\mathrm{rot} : \pi(S^1) \to \mathbb{Z}$$

a well-defined homomorphism.

□

Then we can extend the consequence above to $\mathbb{C}^*$. consider loop

$$\gamma : S^1 \to \mathbb{C}^*$$

can we can define **link number** of γ be

$$\mathrm{rot}(\gamma) := \mathrm{rot}\left(S^1 \to S^1,\ t \mapsto \frac{\gamma(t)}{|\gamma(t)|}\right)$$

For example, $\gamma_n : S^1 \to \mathbb{C}^*$, by $\gamma(z) = z^n$, we have $\mathrm{rot}(\gamma_n) = n$.
¶ the fundamental theorem of Algebra: Proof. Now we use the technique of fundamental group to prove the fundamental theorem of Algebra.

Suppose the polynomial

$$f(z) := a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

has no complex root, it's no hard to let $a_n = 1$. For all $R \geq 0$, consider loop

$$\gamma_R : S^1 \to \mathbb{C}^*, \quad \gamma_R(z) = f(Rz)$$

We have following three claims:

- For all $R' > R$, the mapping $f|_{\{z : R' \leq |z| \leq R\}}$ is a homotopy between $\gamma_{R'}$ and γ_R, then $\mathrm{rot}(\gamma_{R'}) = \mathrm{rot}(\gamma_R)$.
- $\gamma_0 = f(0)$ is constant mapping and $\mathrm{rot}(\gamma_0) = 0$.
- Let $R > |a_{n-1}| + \cdots + |a_0| + 1$, consider $\eta_R : S^1 \to \mathbb{C}^*$, defined by $\eta_R(z) := (Rz)^n$. Then there is a homotopy between γ_R and η_R be

$$H(z,s) := (1-s)\gamma(z) + s\eta(z) = (Rz)^n + s\left(\sum_{k=1}^{n-1} a_k (Rz)^k\right) \neq 0$$

Therefore,

$$0 = \mathrm{rot}(\gamma_R) = \mathrm{rot}(\eta_R) = n$$

conflict !

3. Lecture 3: Solvable groups and Uniformization group

3.1. **Solvable Groups.**

¶ Subgroup and Normal subgroup. Here we review the definition of subgroups, we call $H(\subset G)$ is a **subgroup** of group G, if

- $ab \in H$, when$a, b \in H$;
- $a^{-1} \in H$, when$a \in H$

And we call $a, b \in G$ are **conjugate**, if there is $g \in G$ such that

$$gag^{-1} = b$$

it is easy to verify conjugate induces a equivalent relation on G, and the equivalent class is called **conjugate class**. Obviously, every conjugate class just has **ONE** element when G is Abelian.

definition 3.1. Given group G and subgroup H, we call H a **normal subgroup** of G, if for all $a \in H$, we have

$$gag^{-1} \in H, \quad \forall g \in G$$

Particularly, we call G a **simple group**, if the normal subgroup just are G and $\{e\}$.

example 3.1. Recall example 2.5, and consider D_5. In fact we have

$$D_5 = \{e,\ \rho, \cdots, \rho^4\} \cup \{r_1, \cdots, r_5\}$$

where r_i is the reflection along ith axis of symmetry. D_5 has 4 conjugate classes, they are

$$\{e\},\ \{\rho,\ \rho^4\},\ \{\rho^2,\ \rho^3\},\ \{r_1, \cdots, r_5\}$$

¶ Example: Dodecahedron. Now we consider a **Dodecahedron** $\mathbf{D}_{12}$, one can see it in figure 1. Which has

- 20 vertices;
- 30 edges;
- 12 faces.

One can see it in the figure 1. And let $G = \mathrm{Iso}(\mathbf{D}_{12})$, which called the **rotation group** of $\mathbf{D}_{12}$. Where every elements in G are rotations of $\mathbf{D}_{12}$ around some axis l of symmetry. We have three different cases:

Case 1 rotation around a vertex: the angle is $\theta = \pm\frac{2\pi}{3}$;
Case 2 rotation around the center of edge: the angle is $\theta = \pi$;
Case 3 rotation around the center of face: the angle is $\theta = \pm\frac{2\pi}{5}$ or $\pm\frac{4\pi}{5}$;

We denote such three rotations subsets by B_V, B_E, B_F, then

$$G = \{e\} \sqcup B_V \sqcup B_E \sqcup B_F$$

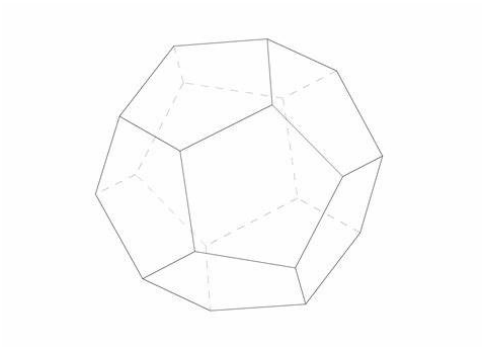


FIGURE 1. Dodecahedron

thus

$$|B_V| = \frac{20}{2} \times 2,\ |B_E| = \frac{30}{2} \times 1,\ |B_V| = \frac{12}{2} \times 4$$

where $|-|$ denotes the number of elment in a set. Therefore,

$$|G| = 1 + |B_V| + |B_E| + |B_F| = 1 + 20 + 15 + 24 = 60$$

Then we consider the conjugate classes in G. First we obtain following communative diagram:

$$\begin{array}{ccc} \mathbf{D}_{12} & \xrightarrow{\rho_1} & \mathbf{D}_{12} \\ \downarrow g & & \downarrow g \\ \mathbf{D}_{12} & \xrightarrow{\rho_2} & \mathbf{D}_{12} \end{array}$$

where ρ_1, ρ_2 is rotation around some axis l by some angle, and g is any element in G, and indeed

$$\rho_1 = \rho(l, \theta),\ \rho_1 = \rho(g(l), \theta)$$

Thus

$$\rho(l, \theta) = g \cdot \rho(g(l), \theta) \cdot g^{-1}$$

Which means G is "totally" smmetric:

- Any two vertices V, V', there is $g \in G$, such that $g(V) = V'$.
- Any two edges E, E', there is $g \in G$, such that $g(E) = E'$.
- Any two faces F, F', there is $g \in G$, such that $g(F) = F'$.

Therefore, there are 5 conjugate classes of G:

(1) $\{e\}$, just one element.
(2) All rotations around vertices, there are 20 emelents.
(3) All rotations around center of edges, there are 15 emelents.
(4) All $\pm\frac{2\pi}{5}$ rotations around center of faces, there are 12 emelents.
(5) All $\pm\frac{4\pi}{5}$ rotations around center of faces, there are 12 emelents.

Use a fact that the number of elements in subgroup $H(\subset G)$ (the **order**) can divide the order of G, and observe that all numbers above plus 1 can **NOT** divide 60, then we get a more useful consequence:

theorem 3.1. The rotation group of Dodecahedron is a simple group.

¶ Permutation and Solvable groups. We have know that for a set B, the symmetry group of it (denoted by $S_B = \{B \to B \text{ a bijection}\}$), and denoted $S_n := S_B$ if $|B| = n$. For $g \in S_n$, define the **count inversion** of g by

$$\tau(g) := \{(i,j) \in \{1,\cdots,n\} \times \{1,\cdots,n\} : i < j,\ \tau(j) < \tau(i)\}$$

And we say g a **even permutation**, if $|\tau(g)|$ is an even; say **odd permutation**, if $|\tau(g)|$ is an odd.

Then we quickly review the representatioin of permutations, for example, $g \in S_5$, we may write

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

which means that g map 1 to 2, 2 to 3, 3 to 4 and 4 to 1, and map 5 to 5. Sometimes we represent g by

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

And a useful ovservation os that

$$|\tau(g \circ h)| \text{ and } |\tau(g)| + |\tau(h)| \text{ like parity.}$$

Let A_n be all even permutations in S_n, which is the normal subgroup of S_n, and $|A_n| = n!/2$. We now want to show

$$\mathrm{Iso}(\mathbf{D}_{12}) \cong A_5$$

To prove it, we firstly define the **distance** of all vertices in $\mathbf{D}_{12}$ by

$$d(V_1, V_2) := \{\text{the least number of edges linking } V_1, V_2\}$$

then we can divide all vertices into 5 classes (with 4 vertices in one class), and in every class, the distance between each vertex is 4. Thus every 4 vertices in one class generate a **tetrahedron**, denoted by $\Delta_k,\ k = 1,\cdots,5$. And we claim:

(1) $g(\in \mathrm{Iso}(\mathbf{D}_{12}))$ induces an even permutation of $\{\Delta_1,\cdots,\Delta_5\}$.
(2) (1) induces a homomorphism $\mathrm{Iso}(\mathbf{D}_{12}) \to A_5$, and we can prove which is a suijection as well.

Therefore, we have

corollary 3.1. A_5 is a simple group.

Now we introduce the solvable groups. We call all forms in G

$$aba^{-1}b^{-1}$$

are **commutators**, and all communatators in one group G become a group, called **communatator subgroup**, denoted by $[G, G]$, which is actually a normal subgroup.

definition 3.2. Given a group G, let $G^{(0)} := G$, and define $G^{(k)}$ be k**th communator subgroup** of G by induction:

$$G^{(0)} := G, \quad G^{(k)} := [G^{(k-1)}, G^{(k-1)}]$$

and define the **length** of G be

$$l(G) := \min\{k : G^{(k)} = \{e\}\} \in \mathbb{N}$$

We call G a **solvable group**, if $l(G) < \infty$.

A immediate fact is

$$l(G) = 1 \Longleftrightarrow G \neq \{e\} \text{ and } [G, G] = \{e\} \Longleftrightarrow$$
$$G \text{ is a nontrivial Abelian group}$$

example 3.2. Let $G = S_2 \cong \mathbb{Z}_2$, then $l(S_2) = 1$.

example 3.3. Let $G = S_3 \cong D_3$, then $l(S_3) = 1 frm{-}e$.

example 3.4. Let $G = S_4$, then $G^{(1)} = A_4 \cong$ Iso(tetrahedron). Observed that

Iso(tetrahedron) = $\{e\} \cup \{\text{rotation around edges}\} \cup \{\text{rotation around vertices}\}$

Then $G^{(2)} = \{e\} \cup \{\text{rotation around edges}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, which is called **Klein group**, then $G^{(3)} = \{3\}$. Therefore, $l(S_4) = 3$.

We claim that: In the examples above, when $2 \leq n \leq 4$, the radical solution need n times of composition of rootings.

Two more facts are

- The subgroups of solvable group are solvable.
- The quotient groups of solvable group are solvable.

Via corollary 3.1, we have

example 3.5. Let $G = A_5$, G is NOT solvable, then S_5 is NOT solvable, furthermore, S_n is **NOT** solvable, when $n \geq 5$!

3.2. **Uniformization group of Multivalued functions.**

¶ Multivalued function.

definition 3.3. Let X, Y be two sets, we call a mapping $X \to \mathcal{P}(Y)$ a **multivalued function**, denoted by $f : X \rightsquigarrow Y$, and define the **domain** of f by

$$D(f) := \{x \in X : f(x) \neq \emptyset\}$$

example 3.6. $\sqrt{-} : \mathbb{C} \rightsquigarrow \mathbb{C}$ is a multivalued function, when $z \neq 0$, the set $\sqrt{z}$ has two elements.

definition 3.4. Let X, Y be topological spaces, consider multivalued function $f : X \rightsquigarrow Y$. For $x \in D(f)$, we call x a **regular point** of f, if there is a open set $U(\subset X)$, such that there are a family of (disjoint with each other) open sets $\{V_i\}_{i\in I}$ of Y, and a family of continuous mappings $\{f_i : U \to V_i\}_{i\in I}$, and for all $y \in U$, we have $f(y) = \{f_i(y)\}_{i\in I}$.

We denote the set of all regular points by $R(f)$ and call $R(f)$ be **regular domain**, if $R(f)$ is open, and call $x(\in R(f) - D(f))$ **bifurcation point**.

example 3.7. Let $f = \sqrt[n]{-} : \mathbb{C} \rightsquigarrow \mathbb{C}$, then f is a multivalued functions, and $D(f) = \mathbb{C},\ R(f) = \mathbb{C}^*$.

example 3.8. $e^z : \mathbb{C} \to \mathbb{C}$ is a classical function, but the inverse of e^z is multivalued, which called **logarithmic function**, denoted by $\log z$. In fact, via Euler's formula (see theorem 1.1), we have

$$\log z = \log |z| + i\mathrm{Arg}(z)$$

then we have $D(\log) = R(\log) = \mathbb{C}^*$.

example 3.9. Consider all monicpolynomials, let $P_n := \{p(z) : z^n + a_{n-1}z^{n-1}c + \cdots + a_1 z + a_0\}$, then we have isomorphism

$$P_n \cong \mathbb{C}^n$$

We define a multivalued function

$$\Psi : P_n \to \mathbb{C}$$

by $\Psi(p) := \{\text{all roots of } p\}$. Particularly, when $n = 2$, we have

$$\Psi : (p, q) \to \frac{-p + \sqrt{p^2 - 4q}}{2}$$

by formula 2. And

$$R(\Psi) = P_n^s$$

where P_n^s is **seperable** polynomials space, that is polynomials with no multivalued roots.

¶ Lift property of regular paths. Consider multivalued function $f : X \rightsquigarrow Y$, we call path $\gamma : I \to R(f)$ a **regular path**, and $\overline{\gamma} : I \to Y$ is a **lift** of γ, if $\overline{\gamma}(t) \in f(\gamma(t))$. Similar to theorem 2.2, we have

theorem 3.2. Suppose $\gamma : I \to R(f)$ a regular path, and x_0 is starting, then

(1) there is a unique lift of γ starting from y_0, denoted by $\overline{\gamma}_{y_0} : I \to Y$.
(2) Suppose there is another regular path η which is homotopic to γ, then $\overline{\gamma}_{y_0}$ is homotopic to $\overline{\eta}_{y_0}$, particularly, they have the same ending.

definition 3.5. Given multivalued function $f : X \rightsquigarrow Y$ and regular path γ from x_0 to x_1. Define **parallel transport** $M(f, \gamma) : f(x_0) \to f(x_1)$ be a mapping $M(f, \gamma)(y_0) - \overline{\gamma}_{y_0}(1)$.

We have some observations:

- $M(f, \gamma) : f(\gamma(0)) \to f(\gamma(1))$ depends on homotopy class of γ, thus we write $M(f, [\gamma])$.
- $M(f, \gamma^-) = M(f, \gamma)^{-1}$, thus $M(f, \gamma)$ is bijective.
- When γ is a regular loop, we have a bijection
$$M(f, \gamma) : f(x_0) \to f(x_1)$$
that is $M(f, \gamma) \in S_{f(x_0)}$.

theorem 3.3. Given multivalued function $f : X \rightsquigarrow Y$, choose base point $x_0 \in R(f)$, then we have a well-defined homomorphism
$$\rho : \pi_1(R(f), x_0) \to S_{f(x_0)}, \quad \rho([\gamma]) := M(f, [\gamma])$$

Here we say ρ a **uniformization homomorphism** and the image of ρ be **uniformization group** of multivalued function f, denoted by $M(f, x_0)$. A intuitive description is that the uniformization group $M(f, x_0)$ describes how the elements permutate when parallel tranport along one loop, and which is a subgroup of S_n, where $n = |f(x_0)|$. Also, we can define the **complexity** of multivalued function f be $c(f) := \max\{l(M(f, x_0)) : x_0 \in R(f)\}$. Finally, when $R(f)$ is path-connected, we ignore the base point, similar to the fundamental groups.

example 3.10. Consider $f(z) = \sqrt[n]{z}$. Choose $x_0 = 1 \in R(f) = \mathbb{C}^*$ as base point, then
$$f(x_0) = \{1,\ \xi, \cdots,\ \xi^{n-1}\}, \quad \xi = e^{\frac{2\pi i}{n}}$$
We have known that $\pi_1(R(f), x_0) = \mathbb{Z}$, which is generated by $\gamma(t) = e^{2\pi i t}$. Observed that γ has n lifts
$$\overline{\gamma}_{\xi^k} : [0, 1] \to \mathbb{C}, \quad \overline{\gamma}_{\xi^k} = \xi^k \cdot e^{\frac{2\pi t i}{n}}$$

thus

$$M(f,\gamma)(\xi^k) = \overline{\gamma}_{\xi^k}(1) = \xi^{k+1}$$

Therefore, the image of generator $[\gamma]$ under mapping $\rho : \pi_1(R(f), x_0) \to S_{f(x_0)}$ is cyclic permutation

$$\sigma = \begin{pmatrix} 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{pmatrix}$$

which means $M(\sqrt[n]{z}) = \mathbb{Z}_n$, which generated by σ. Where $c(f) = 1$.

example 3.11. Recall example 3.9, choose base point $x_0 = p(z) = z^n - 1$, then $\Psi_n(x_0) = \{1, \cdots, \xi^{n-1}\}$, thus $x_0 \in R(\Psi_n) = P_n^s$. We claim that

$$M(\Psi, x_0) \cong S_n$$

Proof. Choose $0 \leq j < k < n$,the path from ξ^j to ξ^k, $\eta : I \to \mathbb{C}$ and another path γ from ξ^k to ξ^j, such that $\eta(0,1),\ \gamma(0,1),\ \Psi_n(x_0)$ are disjoint. For $t \in I$, consider polynomial

$$p_t(z) := \prod_{i \neq j,k,\ 0 \leq i \leq n-1} (z - \xi^i) \cdot (z - \eta(t)) \cdot (z - \gamma(t))$$

then $\gamma : I \to P_n^s,\ t \mapsto p_t(z)$, is a loop with base point x_0. And satisfies $(\xi^j, \xi^k) = M(\Psi_n, \gamma) \in M(\Psi_n)$. Since every elements in $S_{f(x_n)}$ are the product of (ξ^j, ξ^k), thus $M(\Psi_n) = S_{f(x_0)} = S_n$. □

Therefore, we have

$$c(\Psi_2) = 1,\ c(\Psi_3) = 2,\ c(\Psi_4) = 3,\ c(\Psi_5) = \infty$$

4. Lecture4: proof of Abel-Ruffini theorem and Hilbert 13th problem

4.1. **Solvable multivalued function.**

¶ Communator loops and Lift property. Sometimes the lifts of loops are not closed, we call a regular loop $\gamma : I \to R(f)$ with base point x_0 is **liftable**, if

$$\rho(\gamma) : f(x_0) \to f(x_0)$$

is identity, which is equivalent to the lifts of it are all closed, Similarly, this property is **ONLY** dependent on homotopy class of path.

Another concept is **communator loop**, we call a regular loop $\gamma : I \to R(f)$ is a **communator loop**, if there are regular loops γ_1, γ_2, such that

$$\gamma = \gamma_1\gamma_2\gamma_1^-\gamma_2^-$$

and we call k**th communator loop**, if there are $(k-1)$th communator loops, γ_1, γ_2, such that $\gamma = \gamma_1\gamma_2\gamma_1^-\gamma_2^-$.

lemma 4.1. Let multivalued function $f : X \rightsquigarrow Y$ with $c(f) = 1$, there is a regular loop which is **NOT** liftable, however, any 1st communator loop is liftable.

Proof. $M(f, \gamma) \neq \{e\}$, thus there is a loop γ, such that $\rho(\gamma) \neq e$, then γ is not liftable.

suppose $\gamma = \gamma_1\gamma_2\gamma_1^-\gamma_2^-$, we have

$$\rho(\gamma) = \rho(\gamma_1)\rho(\gamma_2)\rho(\gamma_1)^{-1}\rho(\gamma_2)^{-1} \in M(f, x_0)$$

Since $c(f) = 1$, $M(f, x_0)$ is an Abelian group, which means $\rho(\gamma) = e$, γ is ilftable. □

Similarly, we can prove the theorem as follows by induction:

theorem 4.1. Given multivalued function $f : X \rightsquigarrow Y$. Then

1. $c(f) = k < \infty$ iff all kth communator loops is liftable;
2. $c(f) = \infty$ iff for all $k > 0$, there is a kth communator loop not liftable.

¶ Complexity formula. On the other hand, we define the **composition** of multivalued functions $f : X \rightsquigarrow Y$ and $g : Y \rightsquigarrow Z$, that is

$$g \circ f : X \rightsquigarrow Z, \quad g \circ f(x) := \bigcup_{y \in f(x)} g(y)$$

We call a multivalued function $f : X \rightsquigarrow Y$ is **regular**, if $R(f) = X$.

theorem 4.2. Suppose g a regular multivalued function, then

$$c(g \circ f) \leq c(g) + c(f)$$

Proof. To simplify the proof, we suppose $c(g) = 1$. Let $c(f) = k$, and choose a $(k+1)$th communator γ with base point x_0 in $R(g \circ f)$. Here we choose $z_0 \in (g \circ f)(x_0)$, there is a point $y_0 \in f(x_0)$ such that $z_0 \in g(y_0)$, then $\gamma = \gamma_1\gamma_2\bar{\gamma_1}\bar{\gamma_2}$, where $\gamma 1, \gamma_2$ are kth communators. Since $c(f) = k$, γ_1, γ_2 can lift to the regular loops $\overline{\gamma}_1, \overline{\gamma}_2$ in Y. Thus, $\overline{\gamma} = \overline{\gamma}_1\overline{\gamma}_2\overline{\gamma}_1^{-}\overline{\gamma}_2^{-}$ is a lift of γ w.r.t. f, and is the communator loop in Y. Finally, since $c(g) = 1$, thus $\overline{\gamma}$ can lift to $\hat{\gamma}$ which is a regular loop w.r.t. g in Z, with base boint z_0, then $\hat{\gamma}$ is a lift w.r.t. $g \circ f$, and since $\hat{\gamma}$ is closed, then

$$c(g \circ f) \leq k + 1$$

□

Given two multivalued functions $f, g : X \rightsquigarrow Y$, we say f is contained in g, denoted by $f \subset g$, if for all $x \in X$, we have $f(x) \subset g(x)$. Obviously, we have

theorem 4.3. Let $f \subset g$, and $R(f) \subset R(g)$, then

$$c(f) \leq c(g)$$

In fact, we have proved the following theorem:

theorem 4.4. Suppose $f : X \rightsquigarrow Y$ is contained in

$$X \overset{f_1}{\rightsquigarrow} X_1 \overset{f_2}{\rightsquigarrow} X_2 \overset{f_3}{\rightsquigarrow} \cdots \overset{f_n}{\rightsquigarrow} X_n = Y$$

where f_i are regular, then

$$c(f) \leq \sum_{i=1}^{n} f(f_i)$$

definition 4.1. We say multivalued function $f : X \rightsquigarrow Y$ is **solvable**, if $c(f) < \infty$.

example 4.1.
(1) monodrome function f is solvable, since $c(f) = 0$.
(2) function $f = \sqrt[n]{-}$ is solvable, since $c(f) = 1$.
(3) logarithmic function and inverse trigonometric function are solvable.
(4) When $n \geq 5$, function Ψ_n is **NOT** solvable, see example 3.9

corollary 4.1. If a multivalued function is not solvable, then it can not contain finite regular solvable functions.

4.2. **topological proof of Abel' theorem.**

¶ Zariski topology.

definition 4.2. Let $A \subset \mathbb{C}^n$, we call A is a **Zariski closed** if there are finite polynomials $f_1, \cdots, f_m$ such that

$$A = \{(z_1, \cdots, z_n) : f_i(z_1, \cdots, z_n) = 0,\ i = 1, 2, \cdots, m\}$$

Similarly, we call A is **Zariski open**, if $\mathbb{C}^n - A$ is closed.

Obviously, we have

- All Zariski open sets induces a topology, we call **Zariski topology**.
- The preimage of polynomial mapping of Zariski open(closed) set is open(closed).
- The finite union of non-empty Zariski open set is non-empty.
- For $n = 1$, the Zariski open set is path-connected.

definition 4.3. Consider polynomials $f_1, \cdots, f_m;\ g_1, \cdots, g_m : \mathbb{C}^n \to \mathbb{C}$, we call

$$Q = (\frac{f_1}{g_1}, \cdots, \frac{f_m}{g_m}) : U \to \mathbb{C}^m$$

is a **rational function**. And the domain of it is

$$U = \{(z_1, \cdots, z_n) \in \mathbb{C}^n : g_i(z_1, \cdots, z_n) \neq 0\}$$

definition 4.4. Let $k_1, \cdots, K_n$ be positive integers, we call

$$f : \mathbb{C}^n \rightsquigarrow \mathbb{C}^n, \quad f(z_1, \cdots, z_n) = \{(y_1, \cdots, y_n) \in \mathbb{C}^n : y_i \in \sqrt[k_i]{z_i}\}$$

a **rooting function**. And the domain of it is

$$R(f) = \{(z_1, \cdots, z_n) : z_i \neq 0,\ k_i > 1\}$$

is Zariski open.

Obviously, we have $c(\text{rational function}) = 0,\ c(\text{rooting function}) = 1$.

¶ the Statement of Abel's theorem. Recall example3.9.

definition 4.5. Let U be a non-empty Zariski open set of $P_n \cong \mathbb{C}^n$, consider composition multivalued function

$$f : U \overset{f_1}{\rightsquigarrow} \mathbb{C}^{n_1} \overset{f_2}{\rightsquigarrow} \mathbb{C}^{n_2} \overset{f_3}{\rightsquigarrow} \dots \overset{f_n}{\rightsquigarrow} \mathbb{C}$$

where f_i are rational functions or rooting functions. We call f a **rooting formula** of n degree equation, if $f \subset \Psi_n|_U$.

remark 4.1.
(1) U could not be P_n, that is allow the rooting formula to fail for some special polynomials.
(2) We only require $\Psi_n|_U \subset f$, but not $\Psi_n|_U = f$, that is allow extraneous roots of rooting formula.

example 4.2. When $n = 2$, consider

$$f : P_2 \cong \mathbb{C}^2 \overset{f_1}{\to} \mathbb{C}^2 \overset{f_2}{\rightsquigarrow} \mathbb{C}^2 \overset{f_3}{\to} \mathbb{C}$$

where

- $f_1(z, w) = (z, z^2 - w)$
- $f_2(z, w) = (z, \sqrt{w})$
- $f_3(z, w) = \frac{-z+w}{2}$

then

$$f(p, q) = \frac{-p + \sqrt{p^2 - 4q}}{2}$$

is rooting formula.

theorem 4.5 (Abel theorem)**.** There is no rooting formula when $n \geq 5$.

remark 4.2. In fact, if we allow some general operations to extend the concepts of classical arithmetic, Bring have got a consequence in 1786.

theorem 4.6 (Bring, 1786)**.** There is a "general rooting formula" for 5 degree equations, which is dependent on $+, -, \times, \div, \sqrt{}, \sqrt[3]{}$, and a multivalued function

$$\Psi : \mathbb{C} \rightsquigarrow \mathbb{C}, \ \Psi(q) := \{\text{the roots of } z^5 + qz + 1 = 0\}$$

theorem 4.7 (Bring, Hamilton)**.** There is a "general rooting formula" for 6 degree equations, which is dependent on $+, -, \times, \div, \sqrt{}, \sqrt[3]{}$, and a multivalued function

$$\Psi : \mathbb{C}^2 \rightsquigarrow \mathbb{C}, \ \Psi(p, q) := \{\text{the roots of } z^6 + pz^2 + qz + 1 = 0\}$$

¶ proof of Abel's theorem. Now we start to proof theorem4.5.
Firstly, we consider a proposition:

proposition 4.1. Let $U \subset P_n$ a non-empty Zariski open set, consider $\Psi_n|_U : U \to \mathbb{C}$, then the uniformized groups

$$M(\Psi_)n|_U) \cong S_n$$

Thus, when $n \geq 5$, $\Psi_n|_U$ is **NOT** solvable.

Proof. Consider function $\sigma : \mathbb{C}^n \to P_n$ by $\sigma(z_1, \cdots, z_n) = (z - z_1)(z - z_2) \cdots (z - z_n)$. Choose polynomial $p_o \in R(\Psi_n) \cap U$, let the roots of p_0 be $r_1, \cdots, r_n$. Choose $g \in S_n$, then $\sigma(r_1, \cdots, r_n) = \sigma(r_{g(1)}, \cdots, r_{g(n)}) = p_0$. Therefore, $(r_1, \cdots, r_n), (r_{g(1)}, \cdots, r_{g(n)})$ is blong to $\sigma^{-1}(U \cap R(\Psi_n))$. $\sigma^{-1}(U \cap R(\Psi_n))$ is Zariski open in $\mathbb{C}^n$, thus there is a path γ linking $(r_1, \cdots, r_n), (r_{g(1)}, \cdots, r_{g(n)})$, then $\sigma \circ \gamma : [0, 1] \to U \cap R(\Psi_n)$ is a regular loop of $\Psi_n|_U$ with base point p_0. Parallel transport g along $\sigma \circ \gamma$, we have $g \in M(\Psi_n|_U)$. □

Proof of theorem4.5. Let $n \geq 5$, suppose there is a rooting formula

$$\Psi_n|_U \subset f : U \xrightarrow{f_1} \mathbb{C}^{n_1} \overset{f_2}{\rightsquigarrow} \mathbb{C}^{n_2} \rightsquigarrow \cdots \rightsquigarrow \mathbb{C}^{n_k} \overset{f_k}{\rightsquigarrow} \mathbb{C}$$

Let $V_i = R(f_i)$, since f_i are rational functions or rooting functions, V_i are non-empty Zariski open. And let $U_k = V_k$, define $U_i = f_i^{-1}(U_{i+1}) \cap V_i$, then U_i is non-empty Zariski open.

Now we consider the new comppsition

$$\Psi_n|_{U_i} \subset f|_{U_1} : U_1 \overset{f_1|_{U_1}}{\rightsquigarrow} U_2 \overset{f_2|_{U_2}}{\rightsquigarrow} U_3 \rightsquigarrow \cdots \rightsquigarrow U_k \overset{f_k|_{U_k}}{\rightsquigarrow} \mathbb{C}$$

Since $U_i \subset R(f_i)$, $f_i|_{U_i}$ are regular solvable functions. And since $\Psi_n|_{U_1}$ is contained in some composition of regular solvable functions, $\Psi_n|_{U_1}$ is solvable, which is in contradiction with proposition above, so we complete the proof ! □

4.3. **Hilbert 13th problem.**

¶ the Statement of Hilbert 13th problem. Recall the statement of Abel's theorem and consequences of Bring and Hamilton. Hilbert posed a problem in ICM at 1900, which is called the **Hilbert's 13 problem** and **NOT** be solved up to now.

conjecture (Hilbert's 13 problem)**.** 7 degree equation

$$z^7 + pz^3 + qz^2 + rz + 1 = 0$$

can **NOT** be solved by a algebraic function with two variables.

¶ Kolmogorov-Arnold representation theorem.

theorem 4.8 (Kolmogorov, Arnold)**.** Every continuous functions with several variables on bounded domain, can be written by several continuous functions with ONE variable and composition of plus $+$. Specifically, for all continuous functions with several variables $f : [0,1]^n \to \mathbb{R}$, there is a continuous functions with one variable $\varphi_{p,q}, \Phi_q$, such that

$$f(x_1, \cdots, x_n) = \sum_{q=1}^{2n+1} \Phi_q \left(\sum_{p=1}^{n} \varphi_{p,q}(x_p) \right)$$

Which means that the plus

$$+ : \mathbb{R}^2 \to \mathbb{R}, \quad (x, y) \mapsto x + y$$

is the unique continuous functions with several variables, for example,

$$xy = e^{\log x + \log y}$$

can be written by the composition of $e^-, \log(-), +$. Therefore, this theorem means that the conjecture of Hilbert is fail for continuous functions.