Lecturer: Jiahui (Kent) Huang

Date: 20251026

Insolvability of quintics.

1. Quadratics

Get roots using coefficients:

If $ax^2+bx+c=0$

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

<u>Proof</u>: Complete the square.

Get coefficients using roots:

If r_1, r_2 are two roots of a (monic) quadratic f

then $f=(x-r_1)(x-r_2)=x^2-\boxed{(r_1+r_2)}x+\boxed{r_1 r_2}$

2. Symmetric polynomials.

Let $f\in\mathbb{C}[x,y]$, then f is symmetric if

$f(x,y)=f(y,x)$.

Let $f\in\mathbb{C}[x_1,\dots,x_n]$ then f is symmetric if

$f(x_1,\dots,x_n)=f(\text{a permutation of } x_1,\dots,x_n)$

for any permutation.

Ex elementary symmetric polynomials.

$e_1=x_1+\cdots+x_n$

$$e_2 = x_1x_2 + x_1x_3 + \dots + x_1x_n$$
$$+ x_2x_3 + \dots + x_2x_n$$
$$+ \dots$$
$$+ \dots + x_{n-1}x_n$$

$$e_j = \sum_{1 \le i_1 < i_2 < \dots < i_j \le n} x_{i_1} \cdots x_{i_j}$$ degree j.

for $1 \le j \le n$.

Theorem Fundamental theorem of symmetric polynomials

Let $f \in \mathbb{C}[x_1, \dots, x_n]$ be symmetric. Then

- $\exists\, g \in \mathbb{C}[e_1, \dots, e_n]$
- such that

$$f(x_1, \dots, x_n) = g(e_1(x_1, \dots, x_n), \dots, e_n(x_1, \dots, x_n))$$

i.e. any sym. poly is a polynomial combination of the elem. sym. poly.

Proof Observation:

If f has a term x_1

then it must have $x_1, x_2, \dots, x_n$ by symmetry.

The set $\{x_1, \dots, x_n\}$ is called the orbit of permutations of the x_1 term.

x_1 is called a representative of this orbit.

The polynomial f is the sum of finitely many orbits.

If S is an orbit.

we can order monomials in S by lexicographic order and take the first item to be the representative s.

e.g. $\{acb^2, cba^2, c^2ab\}$
$= \{\underbrace{a^2bc}_{\text{representative}}, ab^2c, abc^2\}$.

If $s = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is a representative for some $a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$.

then let $b_n = a_n$, $b_{n-1} = a_{n-1} - a_n$, $b_{n-2} = a_{n-2} - a_{n-1}, \dots, b_1 = a_1 - a_2$

Consider $\tilde{s} = e_1^{b_1} e_2^{b_2} \cdots e_n^{b_n}$

e.g. $a^2bc \rightsquigarrow a_1 = 2, a_2 = 1, a_3 = 1$
$\rightsquigarrow b_1 = 1, b_2 = 0, b_3 = 1$

$e_1^{b_1} e_2^{b_2} e_3^{b_3} = (a+b+c)abc = a^2bc + ab^2c + abc^2$.

Say the coefficient of s in f is a, and we take s to be the rep. of the orbit with highest lex. order. then all terms of $f - a\tilde{s}$ has lower lex. order than s.

Finally, note that $\tilde{s}$ is a poly. expression of $e_1, \dots, e_n$ so it suffices to repeat the process for $f - a\tilde{s}$.

Question What do you use to "repeat the process"?
Why does the process terminate?

3. Monodromy

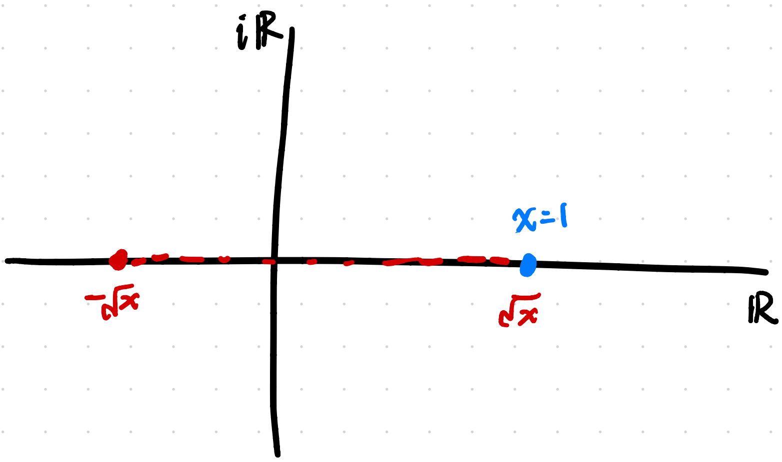
Consider $x^3 + a_1 x^2 + a_2 x + a_3 = 0$.
Say with roots r_1, r_2, r_3.

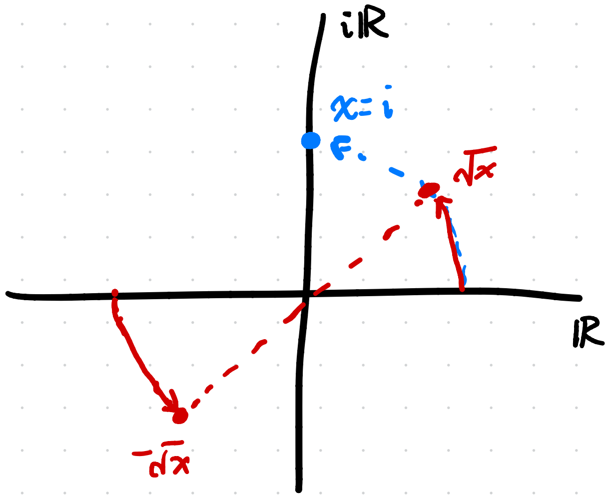
Then a_1, a_2, a_3 are symmetric polynomials of r_1, r_2, r_3
as seen before.

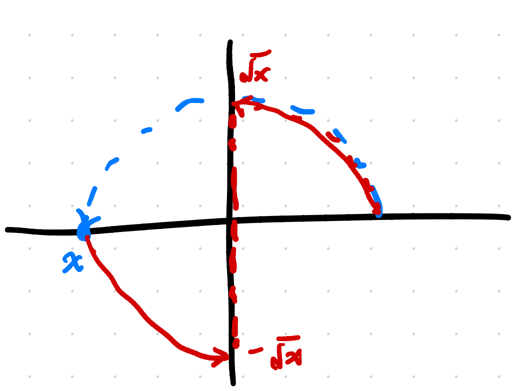
$\Rightarrow$ You can never distinguish r_1, r_2, r_3 by
just taking polynomials in a_1, a_2, a_3.

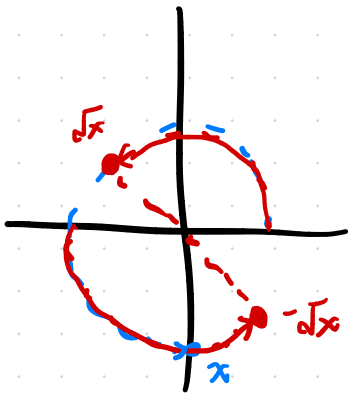
How did we resolve this for quadratics?

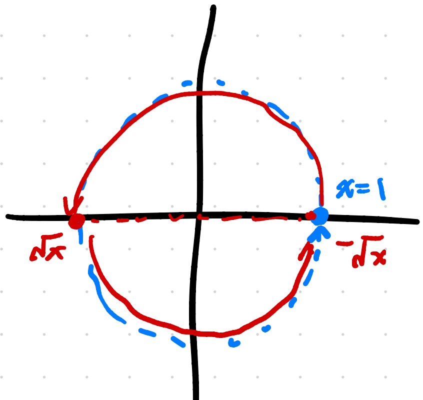
Consider $\pm\sqrt{x}$ (bad notation)







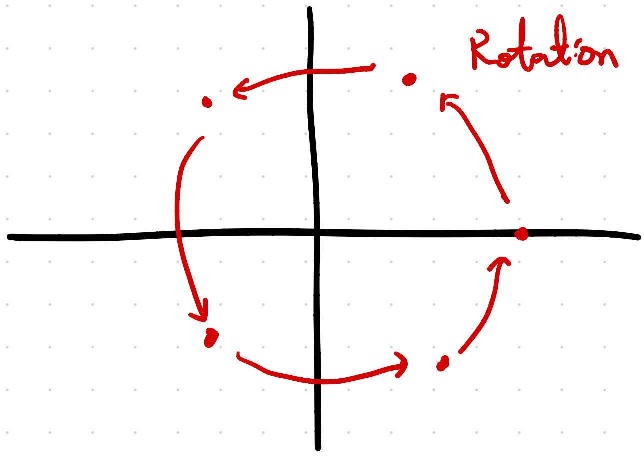


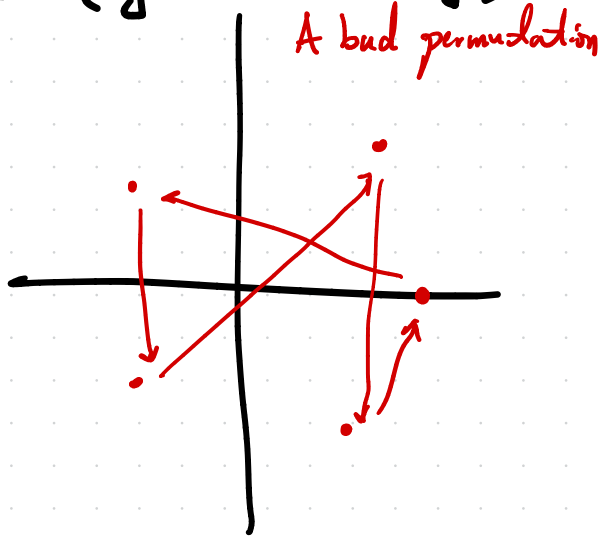


0 is a ==ramified point== for square roots.

- only one square root.
- If you loop a non-zero value around 0, the two square roots get swapped.

For $\sqrt[m]{\cdot}$ the m-th root, wrapping around 0 rotates the roots (cyclic monodromy)





not all permutations can be achieved by this.

The permutations achieved are called ==monodromy action==

4 Monodromy of quintics.

We saw $x \longmapsto \{m\text{-th roots of } x\}$
has a monodromy of rotation when x loops around the origin

Now consider

$$(a_0, a_1, a_2, a_3, a_4) \longmapsto$$

$$\{\text{the 5 roots of } x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0\}$$

In general, the RHS has 5 roots.

but for some $(a_0, a_1, \ldots, a_4) \in \mathbb{C}^5$

there are repeated roots.

Such points are ramification points.

Ex let $f = (x-1)^2 (x-2)(x-3)(x-4)$.

The coefficients give a ramified pt.

because 1 is a repeated root.

Wrapping around a collection of ramified points

will induce a $\underbrace{\text{permutation}}_{\text{monodromy}}$ on the 5 roots

like before.

Ex Wrapping around f will swap two roots.

Fact • All permutations of 5 roots can be achieved as monodromy.

• Not all permutations can be "achieved" by cyclic monodromy.

More precisely: permutation group S_5 is not solvable.

If we have a formula of roots in term of coefficients

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2}$$ quadratic, monodromy $= S_2$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \cdots$$ cubic monodromy $= S_3$

$x =$ crazy expression quartic monodromy $= S_4$

$x =$? quintic monodromy $=$?

Since S_5 can not be built up by cyclic monodromy, there can not exist a quintic formula involving only coefficients and taking m-th roots.