Polynomials that no one can solve!

Supriya Pisolkar

IISER Pune

April 16, 2017

What are polynomials?

What are polynomials?

$$X + 1$$

What are polynomials?

$$X + 1$$

$$X^2 + 2$$

What are polynomials?

$$X + 1$$

$$X^2 + 2$$

$$3X^3 + 2X^2 - 5$$

What are polynomials?

$$X + 1$$

$$X^2 + 2$$

$$3X^3 + 2X^2 - 5$$

In general a polynomial can be expressed as

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

What are polynomials?

$$X+1$$

$$X^2+2$$

$$3X^3+2X^2-5$$

In general a polynomial can be expressed as

$$a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$$

where a_i are some numbers.

What are polynomials?

$$X + 1$$

$$X^2 + 2$$

$$3X^3 + 2X^2 - 5$$

In general a polynomial can be expressed as

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

where a_i are some numbers.

Degree of a polynomial

The highest integer power n appearing in

$$a_n X^n + a_{n-1} X^{n-1} \cdots + a_2 X^2 + a_1 X + a_0$$

is called the degree of a polynomial.

Degree of a polynomial

The highest integer power n appearing in

$$a_n X^n + a_{n-1} X^{n-1} \cdots + a_2 X^2 + a_1 X + a_0$$

is called the degree of a polynomial.

Type	Example	Degree
Linear	$X + 1$	1
Quadratic	$X^2 + 2X + 1$	2
Cubic	$X^3 + 2X$	3
Quartic	$2X^4 + x^3 + 2$	4
Quintic	$X^5 + 1$	5

History of polynomials

History of polynomials

Egyptians and Babylonians ($\sim$ 4000 years ago) :

History of polynomials

Egyptians and Babylonians ($\sim$ 4000 years ago) :

Problem: Given a specific area, they were unable to calculate lengths of the sides of certain shapes, and without these lengths they were unable to design floor plan for their kingdom.

Solving polynomials

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero.

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

  If we put $X = -1$,

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

  If we put $X = -1$,

  $p(-1) = (-1) + 1 = 0$

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

  If we put $X = -1$,

  $p(-1) = (-1) + 1 = 0$

  So -1 is a root of $X + 1$.

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

  If we put $X = -1$,

  $p(-1) = (-1) + 1 = 0$

  So -1 is a root of $X + 1$.
- Let $p(X) = (X - 5)^2 = (X - 5) \cdot (X - 5)$,

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

  If we put $X = -1$,

  $p(-1) = (-1) + 1 = 0$

  So -1 is a root of $X + 1$.
- Let $p(X) = (X - 5)^2 = (X - 5) \cdot (X - 5)$,

  Substitute, $X = 5$

Solving polynomials

Solving a polynomial $p(X)$ means finding numbers which when substituted in place of X give zero. This is also called finding **roots of a polynomial** $p(X)$.

- $p(X) = X + 1$,

  If we put $X = -1$,

  $p(-1) = (-1) + 1 = 0$

  So -1 is a root of $X + 1$.
- Let $p(X) = (X - 5)^2 = (X - 5) \cdot (X - 5)$,

  Substitute, $X = 5$

  $p(5) = (5 - 5)^2 = 0$,

  So, 5 is a root of $(X - 5)^2$.

Square root of a number

Square root of a number

For a positive integer a, there are two numbers $\sqrt{a}$ and $-\sqrt{a}$ such that

$$(\sqrt{a})^2 = a \quad \text{and} \quad (-\sqrt{a})^2 = a$$

Square root of a number

For a positive integer a, there are two numbers $\sqrt{a}$ and $-\sqrt{a}$ such that

$$(\sqrt{a})^2 = a \quad \text{and} \quad (-\sqrt{a})^2 = a$$

So, these two numbers are roots of the polynomial

$$X^2 = a$$

Square root of a number

For a positive integer a, there are two numbers $\sqrt{a}$ and $-\sqrt{a}$ such that

$$(\sqrt{a})^2 = a \quad \text{and} \quad (-\sqrt{a})^2 = a$$

So, these two numbers are roots of the polynomial

$$X^2 = a$$

They are called **square roots** of a.

Square root of a number

For a positive integer a, there are two numbers $\sqrt{a}$ and $-\sqrt{a}$ such that

$$(\sqrt{a})^2 = a \quad \text{and} \quad (-\sqrt{a})^2 = a$$

So, these two numbers are roots of the polynomial

$$X^2 = a$$

They are called **square roots** of a.

$$(4)^2 = 16 \text{ so, we write } \sqrt{16} = 4.$$

The sign $\sqrt{\cdot}$ is called a **radical sign**.

Solving a general Quadratic polynomials

Solving a general Quadratic polynomials

Consider a simple quadratic polynomial $p(X) = X^2 + 5X + 6$.

Solving a general Quadratic polynomials

Consider a simple quadratic polynomial $p(X) = X^2 + 5X + 6$.

How to find a root of this equation?

Solving a general Quadratic polynomials

Consider a simple quadratic polynomial $p(X) = X^2 + 5X + 6$.

How to find a root of this equation?

Nearly 1400 years ago Brahmagupta, an Indian mathematician, gave the first explicit root of $p(X)$.

BRAHMAGUPTA

Brahmagupta was an Indian mathematician and astronomer who wrote two important works on mathematics: the Brahmasphutasiddhanta and the Khandakhadyaka and he was the first mathematician to use the concept of the zero. But right now people don't know where Brahmagupta's mathematics are derivated from.

Solving a general Quadratic polynomials

Consider a simple quadratic polynomial $p(X) = X^2 + 5X + 6$.

How to find a root of this equation?

Nearly 1400 years ago Brahmagupta, an Indian mathematician, gave the first explicit root of $p(X)$.

BRAHMAGUPTA

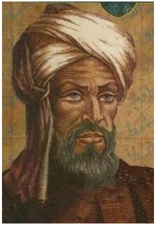
Brahmagupta was an Indian mathematician and astronomer who wrote two important works on mathematics: the Brahmasphutasiddhanta and the Khandakhadyaka and he was the first mathematician to use the concept of the zero. But right now people don't know where Brahmagupta's mathematics are derivated from.

Roots of a quadratic polynomials

In general, for a quadratic equation $aX^2 + bX + c$, there are two roots;

Roots of a quadratic polynomials

In general, for a quadratic equation $aX^2 + bX + c$, there are two roots; Muhammad ibn Musa al-Khwarizmi (Baghdad, 1100 years ago), inspired by Brahmagupta, developed a set of formulas that worked for



$$x = \frac{-b + (\sqrt{b^2 - 4ac})}{2a}, \qquad x = \frac{-b - (\sqrt{b^2 - 4ac})}{2a}$$

Solving Cubic polynomials

Solving Cubic polynomials

Gerolamo Cardano (Italy, 600 years ago) first published the formula for roots of cubic polynomials

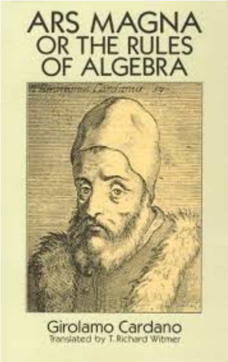


Figure: Gerolamo Cardano (1501-1576)

Solving Cubic polynomials

Solving Cubic polynomials

Consider a cubic equation

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

Formula for a root of this polynomial is given by

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

Quartic polynomial

Quartic polynomial

What happens to quartic polynomials?

Quartic polynomial

What happens to quartic polynomials?

There is a analogous formula for finding roots given by **Lodovico Ferrari** (1545), a student of Cardano but it is much worse and I won't even try to write it down here!!

Mysterious Quintic polynomials

Mysterious Quintic polynomials

For next nearly 400 years people tried to solve quintic polynomials!

Mysterious Quintic polynomials

For next nearly 400 years people tried to solve quintic polynomials!
Then came Evariste Galois (who was only 20 years old at that time), and proved that a general quintic polynomial need not have a root that can be expressed by radicals.

Mysterious Quintic polynomials

For next nearly 400 years people tried to solve quintic polynomials!
Then came Evariste Galois (who was only 20 years old at that time), and proved that a general quintic polynomial need not have a root that can be expressed by radicals.

Allegedly he was in love with a woman engaged to an artillery officer. Galois challenged the officer in order to win her affection. In the nights leading up to the duel, he did write many letters to his friends/colleagues. The most significant of these had the ideas which are foundation of Galois Theory which brought to light non-solvability of a general quintic.

Who am ‘i’ ?

Who am 'i' ?

Question

Is it true that every polynomial will always have a solution somewhere?

Who am 'i' ?

Question

Is it true that every polynomial will always have a solution somewhere?

A root of $X^2 = 1$ which is $i = \sqrt{-1}$ does not belong to the set of real numbers.

Who am 'i' ?

Question

Is it true that every polynomial will always have a solution somewhere?

A root of $X^2 = 1$ which is $i = \sqrt{-1}$ does not belong to the set of real numbers.

Thus we need to extend the set of real numbers by introducing, or 'adjoining', i.

Who am 'i' ?

Question

Is it true that every polynomial will always have a solution somewhere?

A root of $X^2 = 1$ which is $i = \sqrt{-1}$ does not belong to the set of real numbers.

Thus we need to extend the set of real numbers by introducing, or 'adjoining', i.

Complex Numbers $\mathbb{C}$

Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

$$\mathbb{R}(i) := \{a + bi\} \text{ where } a, b \text{ are real numbers and } i = \sqrt{-1}.$$

Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

$$\mathbb{R}(i) := \{a + bi\} \text{ where } a, b \text{ are real numbers and } i = \sqrt{-1}.$$

This is called the set set of complex numbers.

Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

$$\mathbb{R}(i) := \{a + bi\} \text{ where } a, b \text{ are real numbers and } i = \sqrt{-1}.$$

This is called the set set of complex numbers.

Example: $-1 + 3i$,

Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

$$\mathbb{R}(i) := \{a + bi\} \text{ where } a, b \text{ are real numbers and } i = \sqrt{-1}.$$

This is called the set set of complex numbers.

Example: $-1 + 3i$, $2 + i$, $-3i$

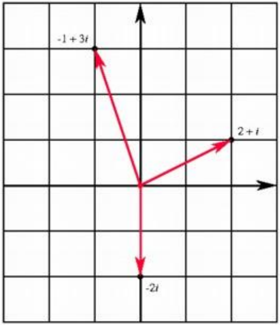
Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

$$\mathbb{R}(i) := \{a + bi\} \text{ where } a, b \text{ are real numbers and } i = \sqrt{-1}.$$

This is called the set set of complex numbers.

Example: $-1 + 3i$, $2 + i$, $-3i$



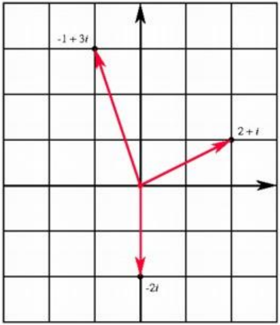
Complex Numbers $\mathbb{C}$

Now lets 'adjoin' $i = \sqrt{-1}$ to the set of reals.

$$\mathbb{R}(i) := \{a + bi\} \text{ where } a, b \text{ are real numbers and } i = \sqrt{-1}.$$

This is called the set set of complex numbers.

Example: $-1 + 3i$, $2 + i$, $-3i$



Fundamental theorem of Algebra

Fundamental theorem of Algebra

By using complex numbers, Carl Friedrich Gauss(Germany), proved a following remarkable result.

Fundamental theorem of Algebra

By using complex numbers, Carl Friedrich Gauss(Germany), proved a following remarkable result.

Figure: Carl Friedrich Gauss (1777-1855)

Fundamental theorem of Algebra

By using complex numbers, Carl Friedrich Gauss(Germany), proved a following remarkable result.

Figure: Carl Friedrich Gauss (1777-1855)

'Every polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ of degree $n > 0$ where $a_i's$ are complex numbers, has a root in complex numbers'.

Sets

Sets

Consider the set of integers : $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$

Sets

Consider the set of integers : $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$

Take two integers m and n, then $m + n$ is again a integer.

Sets

Consider the set of integers : $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$

Take two integers m and n, then $m + n$ is again a integer.

There is a **special element** called **zero** 0 such that $m + 0 = m$.

Sets

Consider the set of integers : $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$

Take two integers m and n, then $m + n$ is again a integer.

There is a **special element** called **zero** 0 such that $m + 0 = m$.

Also, there is an integer $-m$ such that $m + (-m) = 0$.

Groups

A **group** is a set G, with an operation $+$, such that:

Groups

A **group** is a set G, with an operation $+$, such that:

(1) a, b are in G then $a + b$ is in G.

Groups

A **group** is a set G, with an operation $+$, such that:

(1) a, b are in G then $a + b$ is in G.
(2) G contains a special element called identity e.

Groups

A **group** is a set G, with an operation $+$, such that:

(1) a, b are in G then $a + b$ is in G.
(2) G contains a special element called identity e.
(3) G contains inverses i.e. if a is in G then there is an element $-a$ in G such that $a + (-a) = e$.

Groups

A **group** is a set G, with an operation $+$, such that:

(1) a, b are in G then $a + b$ is in G.
(2) G contains a special element called identity e.
(3) G contains inverses i.e. if a is in G then there is an element $-a$ in G such that $a + (-a) = e$.

Example: the set of integer numbers

Fields

Fields

The set of rational numbers,

$$\mathbb{Q} := \{\frac{m}{n} \text{ where } m \text{ and } n(\neq 0) \text{ are integers}\}$$

Fields

The set of rational numbers,

$$\mathbb{Q} := \{\frac{m}{n} \text{ where } m \text{ and } n (\neq 0) \text{ are integers}\}$$

Then $\mathbb{Q}$ is a group.

Fields

The set of rational numbers,

$$\mathbb{Q} := \{\frac{m}{n} \text{ where } m \text{ and } n(\neq 0) \text{ are integers}\}$$

Then $\mathbb{Q}$ is a group.

There is one more operation on $\mathbb{Q}$ which is multiplication. Also, every non-zero rational number has a inverse.

Fields

The set of rational numbers,

$$\mathbb{Q} := \{\frac{m}{n} \text{ where } m \text{ and } n(\neq 0) \text{ are integers}\}$$

Then $\mathbb{Q}$ is a group.

There is one more operation on $\mathbb{Q}$ which is multiplication. Also, every non-zero rational number has a inverse.

A set with two operations $+$ and '$\cdot$' where every non-zero element has a inverse is called a **field**.

Fields

The set of rational numbers,

$$\mathbb{Q} := \{\frac{m}{n} \text{ where } m \text{ and } n(\neq 0) \text{ are integers}\}$$

Then $\mathbb{Q}$ is a group.

There is one more operation on $\mathbb{Q}$ which is multiplication. Also, every non-zero rational number has a inverse.

A set with two operations $+$ and '$\cdot$' where every non-zero element has a inverse is called a **field**.
Example: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Polynomials and groups

Polynomials and groups

Consider a polynomial $p(X)$ which has no roots in $\mathbb{Q}$.

Polynomials and groups

Consider a polynomial $p(X)$ which has no roots in $\mathbb{Q}$.

Example: $X^2 + 1$ has no root in $\mathbb{Q}$.

Polynomials and groups

Consider a polynomial $p(X)$ which has no roots in $\mathbb{Q}$.

Example: $X^2 + 1$ has no root in $\mathbb{Q}$.

One constructs a field $\mathbb{Q}(\alpha)$ which contains a root α of $p(X)$

Polynomials and groups

Consider a polynomial $p(X)$ which has no roots in $\mathbb{Q}$.

Example: $X^2 + 1$ has no root in $\mathbb{Q}$.

One constructs a field $\mathbb{Q}(\alpha)$ which contains a root α of $p(X)$

Example: $\mathbb{Q}(i)$ contains a root i of $X^2 + 1$.

Polynomials and groups

Consider a polynomial $p(X)$ which has no roots in $\mathbb{Q}$.

Example: $X^2 + 1$ has no root in $\mathbb{Q}$.

One constructs a field $\mathbb{Q}(\alpha)$ which contains a root α of $p(X)$

Example: $\mathbb{Q}(i)$ contains a root i of $X^2 + 1$.

When we 'adjoin' all roots of $p(X)$ to $\mathbb{Q}$, then that 'bigger' field is called the **splitting field** of that polynomial.

Polynomials and groups

Consider a polynomial $p(X)$ which has no roots in $\mathbb{Q}$.

Example: $X^2 + 1$ has no root in $\mathbb{Q}$.

One constructs a field $\mathbb{Q}(\alpha)$ which contains a root α of $p(X)$

Example: $\mathbb{Q}(i)$ contains a root i of $X^2 + 1$.

When we 'adjoin' all roots of $p(X)$ to $\mathbb{Q}$, then that 'bigger' field is called the **splitting field** of that polynomial.

Galois theory

Galois showed that, for a polynomial $p(X)$, there is a way to associate;

$$p(X) \to \text{ splitting field } \to \text{ Galois group}$$

Galois theory

Galois showed that, for a polynomial $p(X)$, there is a way to associate;

$$p(X) \rightarrow \text{ splitting field } \rightarrow \text{ Galois group}$$

The association is such that to study roots of a polynomial it is enough to study the corresponding group and vice-versa.

Galois theory

Galois showed that, for a polynomial $p(X)$, there is a way to associate;

$$p(X) \to \text{ splitting field } \to \text{ Galois group}$$

The association is such that to study roots of a polynomial it is enough to study the corresponding group and vice-versa.

He proved that roots of a general quintic polynomial can not be expressed in terms of radicals whenever the associated group is 'non-solvable'.

Summary

Summary

There are some mysterious polynomials of degree 5 and higher whose solutions can not be expressed by using radicals i.e. $\sqrt{\cdot}, \sqrt[3]{\cdot}, \sqrt[4]{\cdot}$

Summary

There are some mysterious polynomials of degree 5 and higher whose solutions can not be expressed by using radicals i.e. $\sqrt{\cdot}, \sqrt[3]{\cdot}, \sqrt[4]{\cdot}$

You can think of it as if, some of the functions are missing from your calculator.!

Summary

There are some mysterious polynomials of degree 5 and higher whose solutions can not be expressed by using radicals i.e. $\sqrt{\cdot}, \sqrt[3]{\cdot}, \sqrt[4]{\cdot}$

You can think of it as if, some of the functions are missing from your calculator.!

One such polynomial is $X^5 - 4X + 2$.

Timeline

3700 years ago	Egyptians made a table.
3600 years ago	Pythagoras worked with integers and rational numbers.
2500 years ago	Babylonians solved some quadratic equations.
1100 years ago	Al-Khwarizmi proved a formula for roots of a quadratic.
600 years ago	Cardano gave a formula for finding roots of a cubic.
600 year ago	Ferrari proved a formula for roots of quartic polynomials.
217 years ago	Gauss proved Fundamental theorem of Algebra.
200 years ago	Galois proved non-solvability of some quintic polynomials.

Thank You!