Math-123: Solving the cubic polynomial

Sebastien Vasey

Harvard University

April 29, 2020

Recall

We saw last time that polynomials of degree at most 4 have a formula for their roots, in terms of sums, products, and root extraction.

Recall

We saw last time that polynomials of degree at most 4 have a formula for their roots, in terms of sums, products, and root extraction.

What is this formula?

Recall

We saw last time that polynomials of degree at most 4 have a formula for their roots, in terms of sums, products, and root extraction.

What is this formula?

For degree 1 and 2, it is well known...

Recall

We saw last time that polynomials of degree at most 4 have a formula for their roots, in terms of sums, products, and root extraction.

What is this formula?

For degree 1 and 2, it is well known...

Today we look at degree 3 (degree 4 can be reduced to degree 3).

Recall

We saw last time that polynomials of degree at most 4 have a formula for their roots, in terms of sums, products, and root extraction.

What is this formula?

For degree 1 and 2, it is well known...

Today we look at degree 3 (degree 4 can be reduced to degree 3).

Disclaimer: If you ever have to do this in practice, it's probably better (and easier) to just use numerical approximations...

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative...

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative... But Del Ferro didn't know about negative numbers!

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative... But Del Ferro didn't know about negative numbers! (while well known to everybody else, they were accepted in the West only in the 19th century!!!)

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative... But Del Ferro didn't know about negative numbers! (while well known to everybody else, they were accepted in the West only in the 19th century!!!)

He keeps his achievement secret until his death (1526), when he tells his student Antonio Fior.

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative... But Del Ferro didn't know about negative numbers! (while well known to everybody else, they were accepted in the West only in the 19th century!!!)

He keeps his achievement secret until his death (1526), when he tells his student Antonio Fior.

1530: Tartaglia announces he can solve some cubics. This leads to a contest between Fior and Tartaglia!

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative... But Del Ferro didn't know about negative numbers! (while well known to everybody else, they were accepted in the West only in the 19th century!!!)

He keeps his achievement secret until his death (1526), when he tells his student Antonio Fior.

1530: Tartaglia announces he can solve some cubics. This leads to a contest between Fior and Tartaglia!

Tartaglia gets asked about $x^3 + mx = n$, for which he had worked out the method.

Some (very partial and Western-centric) history

Contributions from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and *Italians*...

Early 16th century: Del Ferro solves $x^3 + mx = n$.

This is in fact the general case if one allows m and n to be negative... But Del Ferro didn't know about negative numbers! (while well known to everybody else, they were accepted in the West only in the 19th century!!!)

He keeps his achievement secret until his death (1526), when he tells his student Antonio Fior.

1530: Tartaglia announces he can solve some cubics. This leads to a contest between Fior and Tartaglia!

Tartaglia gets asked about $x^3 + mx = n$, for which he had worked out the method.

Fior gets asked about $x^3 + mx^2 = n$, and cannot do it!

History continued

In 1539, Cardano persuades Tartaglia to reveal his method (as a poem!). He has to promise he will never himself reveal it (or at least give time to Tartaglia to reveal it first).

History continued

In 1539, Cardano persuades Tartaglia to reveal his method (as a poem!). He has to promise he will never himself reveal it (or at least give time to Tartaglia to reveal it first).

Cardano gets around the promise by publishing the method in 1545 as the work of Del Ferro...

History continued

In 1539, Cardano persuades Tartaglia to reveal his method (as a poem!). He has to promise he will never himself reveal it (or at least give time to Tartaglia to reveal it first).

Cardano gets around the promise by publishing the method in 1545 as the work of Del Ferro...

Tartaglia challenges Cardano to a competition, etc.

History continued

In 1539, Cardano persuades Tartaglia to reveal his method (as a poem!). He has to promise he will never himself reveal it (or at least give time to Tartaglia to reveal it first).

Cardano gets around the promise by publishing the method in 1545 as the work of Del Ferro...

Tartaglia challenges Cardano to a competition, etc.

In the end, the solution is known as *Cardano's formula.*

History continued

In 1539, Cardano persuades Tartaglia to reveal his method (as a poem!). He has to promise he will never himself reveal it (or at least give time to Tartaglia to reveal it first).

Cardano gets around the promise by publishing the method in 1545 as the work of Del Ferro...

Tartaglia challenges Cardano to a competition, etc.

In the end, the solution is known as *Cardano's formula.*

For more about the solution and poem, see `https://www.maa.org/press/periodicals/convergence/how-tartaglia-solved-the-cubic-equation-cubic-equations`.

There is also a recent book (I haven't read): *The secret formula*, by Toscano.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

We get $g(y) = y^3 + py + q$, where $p = \frac{1}{3}(3b - a^2)$, $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

We get $g(y) = y^3 + py + q$, where $p = \frac{1}{3}(3b - a^2)$, $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

The splitting field for f and g are the same.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

We get $g(y) = y^3 + py + q$, where $p = \frac{1}{3}(3b - a^2)$, $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

The splitting field for f and g are the same.

Recall the *discriminant* of a polynomial is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$, for roots α_1, ..., α_n. In our case, the difference between the roots of $f(x)$ and the roots of $g(x)$ is the same, so they have the same discriminant.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

We get $g(y) = y^3 + py + q$, where $p = \frac{1}{3}(3b - a^2)$, $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

The splitting field for f and g are the same.

Recall the *discriminant* of a polynomial is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$, for roots α_1, ..., α_n. In our case, the difference between the roots of $f(x)$ and the roots of $g(x)$ is the same, so they have the same discriminant.

Let α, β, γ be the roots of $g(y)$. Let's try to compute a simple expression for D, in terms of p and q.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

We get $g(y) = y^3 + py + q$, where $p = \frac{1}{3}(3b - a^2)$, $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

The splitting field for f and g are the same.

Recall the *discriminant* of a polynomial is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$, for roots α_1, ..., α_n. In our case, the difference between the roots of $f(x)$ and the roots of $g(x)$ is the same, so they have the same discriminant.

Let α, β, γ be the roots of $g(y)$. Let's try to compute a simple expression for D, in terms of p and q.

We have $g(y) = (y - \alpha)(y - \beta)(y - \gamma)$. It follows that $g'(\alpha) = (\alpha - \beta)(\alpha - \gamma)$, $g'(\beta) = (\beta - \alpha)(\beta - \gamma)$, $g'(\gamma) = (\gamma - \alpha)(\gamma - \beta)$.

Cubic: beginning of the solution

Consider $f(x) = x^3 + ax^2 + bx + c$. Make the substitution $x = y - a/3$.

We get $g(y) = y^3 + py + q$, where $p = \frac{1}{3}(3b - a^2)$, $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

The splitting field for f and g are the same.

Recall the *discriminant* of a polynomial is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$, for roots α_1, ..., α_n. In our case, the difference between the roots of $f(x)$ and the roots of $g(x)$ is the same, so they have the same discriminant.

Let α, β, γ be the roots of $g(y)$. Let's try to compute a simple expression for D, in terms of p and q.

We have $g(y) = (y - \alpha)(y - \beta)(y - \gamma)$. It follows that $g'(\alpha) = (\alpha - \beta)(\alpha - \gamma)$, $g'(\beta) = (\beta - \alpha)(\beta - \gamma)$, $g'(\gamma) = (\gamma - \alpha)(\gamma - \beta)$.

So $D = -g'(\alpha)g'(\beta)g'(\gamma)$.

We have: $D = -g'(\alpha)g'(\beta)g'(\gamma)$, $g(y) = y^3 + py + q$.

We have: $D = -g'(\alpha)g'(\beta)g'(\gamma)$, $g(y) = y^3 + py + q$.

Since $g'(y) = 3y^2 + p$, we have:

$-D = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)$.

We have: $D = -g'(\alpha)g'(\beta)g'(\gamma)$, $g(y) = y^3 + py + q$.

Since $g'(y) = 3y^2 + p$, we have:

$-D = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)$.

From the class on symmetric functions: if we have a "general" polynomial $x^3 - s_1x^2 + s_2x - s_3 = (x - \alpha)(x - \beta)(x - \gamma)$, then $s_1 = \alpha + \beta + \gamma$, $s_2 = \alpha\beta + \alpha\gamma + \beta\gamma$, $s_3 = \alpha\beta\gamma$. Here, $s_1 = 0$, $s_2 = p$, $s_3 = -q$.

We have: $D = -g'(\alpha)g'(\beta)g'(\gamma)$, $g(y) = y^3 + py + q$.

Since $g'(y) = 3y^2 + p$, we have:

$-D = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)$.

From the class on symmetric functions: if we have a "general" polynomial $x^3 - s_1x^2 + s_2x - s_3 = (x - \alpha)(x - \beta)(x - \gamma)$, then $s_1 = \alpha + \beta + \gamma$, $s_2 = \alpha\beta + \alpha\gamma + \beta\gamma$, $s_3 = \alpha\beta\gamma$. Here, $s_1 = 0$, $s_2 = p$, $s_3 = -q$.

Expanding D, get:

$$-D = 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3$$

We have: $D = -g'(\alpha)g'(\beta)g'(\gamma)$, $g(y) = y^3 + py + q$.

Since $g'(y) = 3y^2 + p$, we have:

$-D = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)$.

From the class on symmetric functions: if we have a "general" polynomial $x^3 - s_1x^2 + s_2x - s_3 = (x-\alpha)(x-\beta)(x-\gamma)$, then $s_1 = \alpha + \beta + \gamma$, $s_2 = \alpha\beta + \alpha\gamma + \beta\gamma$, $s_3 = \alpha\beta\gamma$. Here, $s_1 = 0$, $s_2 = p$, $s_3 = -q$.

Expanding D, get:

$$-D = 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3$$

Expressing this in terms of s_1, s_2, s_3, this simplifies to $-D = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3$.

We have: $D = -g'(\alpha)g'(\beta)g'(\gamma)$, $g(y) = y^3 + py + q$.

Since $g'(y) = 3y^2 + p$, we have:

$-D = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)$.

From the class on symmetric functions: if we have a "general" polynomial $x^3 - s_1x^2 + s_2x - s_3 = (x-\alpha)(x-\beta)(x-\gamma)$, then $s_1 = \alpha+\beta+\gamma$, $s_2 = \alpha\beta + \alpha\gamma + \beta\gamma$, $s_3 = \alpha\beta\gamma$. Here, $s_1 = 0$, $s_2 = p$, $s_3 = -q$.

Expanding D, get:

$$-D = 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3$$

Expressing this in terms of s_1, s_2, s_3, this simplifies to $-D = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3$.

So $D = -4p^3 - 27q^2$.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Recall $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Recall $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$.

We know $g(y)$ has at least one real root. Say it is α. If β and γ are not real, then they are conjugates.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Recall $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$.

We know $g(y)$ has at least one real root. Say it is α. If β and γ are not real, then they are conjugates.

In this case, $\alpha - \beta$ and $\alpha - \gamma$ are conjugates too, so $(\alpha - \beta)^2(\alpha - \gamma)^2$ is real, and $\beta - \gamma$ is purely imaginary, so $D < 0$.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Recall $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$.

We know $g(y)$ has at least one real root. Say it is α. If β and γ are not real, then they are conjugates.

In this case, $\alpha - \beta$ and $\alpha - \gamma$ are conjugates too, so $(\alpha - \beta)^2(\alpha - \gamma)^2$ is real, and $\beta - \gamma$ is purely imaginary, so $D < 0$.

Conversely, if $D < 0$, then $g(y)$ has non-real roots.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Recall $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$.

We know $g(y)$ has at least one real root. Say it is α. If β and γ are not real, then they are conjugates.

In this case, $\alpha - \beta$ and $\alpha - \gamma$ are conjugates too, so $(\alpha - \beta)^2(\alpha - \gamma)^2$ is real, and $\beta - \gamma$ is purely imaginary, so $D < 0$.

Conversely, if $D < 0$, then $g(y)$ has non-real roots.

So the roots are all real if and only if $D \geq 0$. If $D = 0$, some roots repeat and if $D > 0$ they are all distinct.

Discriminant and behavior of roots

The discriminant of $g(y) = y^3 + py + q$ is $D = -4p^3 - 27q^2$.

Recall $D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$.

We know $g(y)$ has at least one real root. Say it is α. If β and γ are not real, then they are conjugates.

In this case, $\alpha - \beta$ and $\alpha - \gamma$ are conjugates too, so $(\alpha - \beta)^2(\alpha - \gamma)^2$ is real, and $\beta - \gamma$ is purely imaginary, so $D < 0$.

Conversely, if $D < 0$, then $g(y)$ has non-real roots.

So the roots are all real if and only if $D \geq 0$. If $D = 0$, some roots repeat and if $D > 0$ they are all distinct.

Example: We can check that $x^3 + x^2 - 2x - 1$ has discriminant $D = 35721 > 0$, so has three distinct roots.

Galois group of a cubic

Let $g(y) = y^3 + py + q \in \mathbb{Q}[x]$.

Galois group of a cubic

Let $g(y) = y^3 + py + q \in \mathbb{Q}[x]$.

If $g(y)$ is reducible, it factors either as a linear term times a quadratic, or as the product of three linear factors. The Galois group is either Z_2 or 1.

Galois group of a cubic

Let $g(y) = y^3 + py + q \in \mathbb{Q}[x]$.

If $g(y)$ is reducible, it factors either as a linear term times a quadratic, or as the product of three linear factors. The Galois group is either Z_2 or 1.

If $g(y)$ is irreducible, the Galois group is a subgroup of S_3 of order divisible by 3. Thus it is either $A_3 = Z_3$ or S_3.

Galois group of a cubic

Let $g(y) = y^3 + py + q \in \mathbb{Q}[x]$.

If $g(y)$ is reducible, it factors either as a linear term times a quadratic, or as the product of three linear factors. The Galois group is either Z_2 or 1.

If $g(y)$ is irreducible, the Galois group is a subgroup of S_3 of order divisible by 3. Thus it is either $A_3 = Z_3$ or S_3.

If it is Z_3, the splitting field has degree 3 so is obtained by adding any root.

Galois group of a cubic

Let $g(y) = y^3 + py + q \in \mathbb{Q}[x]$.

If $g(y)$ is reducible, it factors either as a linear term times a quadratic, or as the product of three linear factors. The Galois group is either Z_2 or 1.

If $g(y)$ is irreducible, the Galois group is a subgroup of S_3 of order divisible by 3. Thus it is either $A_3 = Z_3$ or S_3.

If it is Z_3, the splitting field has degree 3 so is obtained by adding any root.

If it is S_3, we saw that $\sqrt{D} \notin \mathbb{Q}$. The splitting field has degree 6, so is obtained by adding any root and $\sqrt{D}$.

Cardano's formula

It would take too long to derive it, and the derivation is not super interesting anyway.

Cardano's formula

It would take too long to derive it, and the derivation is not super interesting anyway. So here it is!

Let $A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$.

Let $B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}}$.

Then a root of $g(y) = y^3 + py + q$ is given by $\alpha = \frac{A+B}{3}$.

Cardano's formula

It would take too long to derive it, and the derivation is not super interesting anyway. So here it is!

Let $A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$.

Let $B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}}$.

Then a root of $g(y) = y^3 + py + q$ is given by $\alpha = \frac{A+B}{3}$.

The other roots are:

$\beta = \frac{\rho^2 A + \rho B}{3}$.

$\gamma = \frac{\rho A + \rho^2 B}{3}$.

Where $\rho = e^{2\pi i/3}$.

Cardano's formula

It would take too long to derive it, and the derivation is not super interesting anyway. So here it is!

Let $A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$.

Let $B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}}$.

Then a root of $g(y) = y^3 + py + q$ is given by $\alpha = \frac{A+B}{3}$.

The other roots are:

$\beta = \frac{\rho^2 A + \rho B}{3}$.

$\gamma = \frac{\rho A + \rho^2 B}{3}$.

Where $\rho = e^{2\pi i/3}$.

This works for any D (if $D = 0$, then $A = B$ so $\beta = \gamma$).

Cardano's formula

It would take too long to derive it, and the derivation is not super interesting anyway. So here it is!

Let $A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$.

Let $B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}}$.

Then a root of $g(y) = y^3 + py + q$ is given by $\alpha = \frac{A+B}{3}$.

The other roots are:

$\beta = \frac{\rho^2 A + \rho B}{3}$.

$\gamma = \frac{\rho A + \rho^2 B}{3}$.

Where $\rho = e^{2\pi i/3}$.

This works for any D (if $D = 0$, then $A = B$ so $\beta = \gamma$).

Cardano was puzzled by the case $D > 0$ ("Casus irreducibilis") because of the complex number $\sqrt{-3D}$. He could manage it without really understanding.

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Can complex numbers be avoided?

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Can complex numbers be avoided? The answer is no!

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Can complex numbers be avoided? The answer is no!

Suppose we had an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with three distinct real roots, and we could express one of these roots by radicals involving just reals.

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Can complex numbers be avoided? The answer is no!

Suppose we had an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with three distinct real roots, and we could express one of these roots by radicals involving just reals.

Then the splitting field of $f(x)$ is contained in a root extension $\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$.

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Can complex numbers be avoided? The answer is no!

Suppose we had an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with three distinct real roots, and we could express one of these roots by radicals involving just reals.

Then the splitting field of $f(x)$ is contained in a root extension $\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$.

where K_{i+1}/K_i is a simple radical extension.

Complex numbers are unavoidable

If $D > 0$ (as with $x^3 + x^2 - 2x - 1$), then there are three distinct real roots. Still, Cardano's formula requires going through complex numbers.

Can complex numbers be avoided? The answer is no!

Suppose we had an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with three distinct real roots, and we could express one of these roots by radicals involving just reals.

Then the splitting field of $f(x)$ is contained in a root extension
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$.

where K_{i+1}/K_i is a simple radical extension.

Note $s \geq 2$, since the splitting field of $f(x)$ has degree divisible by 3, and $\mathbb{Q}(\sqrt{D})$ has degree 2.

We will prove this is not possible.

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

Without loss of generality, $n_i = p_i$ is prime: otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$. It follows the degree is 1 or p_i:

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

Without loss of generality, $n_i = p_i$ is prime: otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$. It follows the degree is 1 or p_i:

Lemma

If F is a subfield of $\mathbb{R}$, $a \in F$, and p is a prime, then $d := [F(\sqrt[p]{a}) : F]$ is either 1 or p.

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

Without loss of generality, $n_i = p_i$ is prime: otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$. It follows the degree is 1 or p_i:

Lemma

If F is a subfield of $\mathbb{R}$, $a \in F$, and p is a prime, then $d := [F(\sqrt[p]{a}) : F]$ is either 1 or p.

Proof.

The minimal polynomial for $\alpha = \sqrt[p]{a}$ is $\prod_{\sigma \in \mathrm{Aut}(L/F)}(x - \sigma(\alpha))$, where L is the Galois closure of $F(\sqrt[p]{a})/F$.

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

Without loss of generality, $n_i = p_i$ is prime: otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$. It follows the degree is 1 or p_i:

Lemma

If F is a subfield of $\mathbb{R}$, $a \in F$, and p is a prime, then $d := [F(\sqrt[p]{a}) : F]$ is either 1 or p.

Proof.

The minimal polynomial for $\alpha = \sqrt[p]{a}$ is $\prod_{\sigma \in \mathrm{Aut}(L/F)}(x - \sigma(\alpha))$, where L is the Galois closure of $F(\sqrt[p]{a})/F$.
So the constant term of the minimal poly is $\alpha^d \zeta$, ζ a pth root of unity.

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

Without loss of generality, $n_i = p_i$ is prime: otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$. It follows the degree is 1 or p_i:

Lemma

If F is a subfield of $\mathbb{R}$, $a \in F$, and p is a prime, then $d := [F(\sqrt[p]{a}) : F]$ is either 1 or p.

Proof.

The minimal polynomial for $\alpha = \sqrt[p]{a}$ is $\prod_{\sigma \in \mathrm{Aut}(L/F)}(x - \sigma(\alpha))$, where L is the Galois closure of $F(\sqrt[p]{a})/F$.
So the constant term of the minimal poly is $\alpha^d \zeta$, ζ a pth root of unity.
Since α is a real number and $\alpha^d \zeta \in F$ is real, ζ is real, so $\zeta = \pm 1$.

$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with K_{i+1}/K_i is a simple radical extension: $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$.

Without loss of generality, $n_i = p_i$ is prime: otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$. It follows the degree is 1 or p_i:

Lemma

If F is a subfield of $\mathbb{R}$, $a \in F$, and p is a prime, then $d := [F(\sqrt[p]{a}) : F]$ is either 1 or p.

Proof.

The minimal polynomial for $\alpha = \sqrt[p]{a}$ is $\prod_{\sigma \in \mathrm{Aut}(L/F)}(x - \sigma(\alpha))$, where L is the Galois closure of $F(\sqrt[p]{a})/F$.
So the constant term of the minimal poly is $\alpha^d \zeta$, ζ a pth root of unity.
Since α is a real number and $\alpha^d \zeta \in F$ is real, ζ is real, so $\zeta = \pm 1$.
Thus $\alpha^d \in F$ and $\alpha^p = a \in F$ too. If $d \neq p$, then can write $1 = ad + bp$ and get $\alpha \in F$, so $d = 1$. □

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We saw any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality K_{s-1} does not contain a root of $f(x)$ (otherwise it could replace K_s).

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We saw any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality K_{s-1} does not contain a root of $f(x)$ (otherwise it could replace K_s).

In particular, $f(x)$ is irreducible over K_{s-1}. So K_s/K_{s-1} has degree divisible by 3.

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We saw any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality K_{s-1} does not contain a root of $f(x)$ (otherwise it could replace K_s).

In particular, $f(x)$ is irreducible over K_{s-1}. So K_s/K_{s-1} has degree divisible by 3.

Since the degree is prime, it must be exactly 3.

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We saw any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality K_{s-1} does not contain a root of $f(x)$ (otherwise it could replace K_s).

In particular, $f(x)$ is irreducible over K_{s-1}. So K_s/K_{s-1} has degree divisible by 3.

Since the degree is prime, it must be exactly 3.

K_s is a splitting field of $f(x)$ over K_{s-1}, so is Galois.

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We saw any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality K_{s-1} does not contain a root of $f(x)$ (otherwise it could replace K_s).

In particular, $f(x)$ is irreducible over K_{s-1}. So K_s/K_{s-1} has degree divisible by 3.

Since the degree is prime, it must be exactly 3.

K_s is a splitting field of $f(x)$ over K_{s-1}, so is Galois.

Since $K_s = K_{s-1}(\sqrt[3]{a_{s-1}})$, it contains the other cube roots of a_{s-1}.

We have so far: $f(x)$ is irreducible, has three distinct real roots, so $D > 0$, and its splitting field is contained in
$\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt{D}) \subseteq \ldots \subseteq K_s = K \subseteq \mathbb{R}$, with
$K_{i+1} = K_i(\sqrt[p_i]{a_i})$, $a_i \in K_i$, $[K_{i+1} : K_i] = p_i$

We saw any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality K_{s-1} does not contain a root of $f(x)$ (otherwise it could replace K_s).

In particular, $f(x)$ is irreducible over K_{s-1}. So K_s/K_{s-1} has degree divisible by 3.

Since the degree is prime, it must be exactly 3.

K_s is a splitting field of $f(x)$ over K_{s-1}, so is Galois.

Since $K_s = K_{s-1}(\sqrt[3]{a_{s-1}})$, it contains the other cube roots of a_{s-1}.

In particular, K_s contains the cube roots of unity, so cannot be contained in the reals.

The End!

- The last exam will be on the course webpage soon: click on "Last exam" in the last row of the table, or use the "File" menu in Canvas. *Good luck!*
- I hope you enjoyed the class.