3/27/15

No HW5 yet.
I'll return Exam 2 on Monday.

Where were we?

Recall: We defined two fields of numbers.

$\mathbb{F}_{const}$ = x-coordinates of points constructible with straightedge and compass, starting from (0,0) and (1,0)

$\mathbb{F}_{sqrt}$ = numbers that can be obtained from 1 using the operations $+, -, \times, \div, \sqrt{}$.

and then we proved

☆ Theorem: $\mathbb{F}_{const} = \mathbb{F}_{sqrt}$. ///

This successfully transfers the problem of constructibility into the realm of ALGEBRA.

↓

Our next goal is to prove that

$$\sqrt[3]{2}, \ \cos\left(\frac{\pi}{9}\right), \ \cos\left(\frac{\pi}{7}\right) \notin \mathbb{F}_{\text{const}}.$$

By the theorem, it is enough to prove

$$\sqrt[3]{2}, \ \cos\left(\frac{\pi}{9}\right), \ \cos\left(\frac{\pi}{7}\right) \notin \mathbb{F}_{\text{sqrt}}.$$

And for this we need a better understanding of fields.

Recall the construction of the complex numbers $\mathbb{C}$ from the real numbers $\mathbb{R}$. We define

$$\mathbb{C} := \{ a + ib : a, b \in \mathbb{R} \}$$

where $i \in \mathbb{C}$ is some symbol such that $i \notin \mathbb{R}$ but $i^2 = -1 \in \mathbb{R}$.

This $\mathbb{C}$ is certainly a ring because we can add/subtract and multiply.

$\downarrow$

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

$(a+ib)(c+id) = (ac-bd) + i(ad+bc)$.

The 0 and 1 elements are inherited from $\mathbb{R}$.

Jargon: We say that $\mathbb{R}$ is a <u>subring</u> of $\mathbb{C}$.

$$\mathbb{R} \subseteq \mathbb{C}.$$

More surisingly, $\mathbb{C}$ is a <u>field</u>.
The trick of "rationalizing the denominator" allows us to divide:

$$\frac{1}{a+ib} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib}$$

$$= \frac{a-ib}{a^2+b^2}$$

$$= \left(\frac{a}{a^2+b^2}\right) + i\left(\frac{-b}{a^2+b^2}\right)$$

This trick suggests that we should define a function

$$* : \mathbb{C} \longrightarrow \mathbb{C}$$
$$a+ib \longmapsto a-ib$$

We will call this function "conjugation".

You proved on HW3 Problem 3 that conjugation is a "field automorphism". That is, for all $u, v \in \mathbb{C}$ we have

- $(u+v)^* = u^* + v^*$
- $(uv)^* = u^* v^*$

As a consequence of this we have a little Lemma.

☆ Lemma: For all $u \in \mathbb{C}$ we have

$$uu^* \in \mathbb{R} \quad \text{and} \quad u + u^* \in \mathbb{R}$$

Proof: For all $z \in \mathbb{C}$ note that

$$z \in \mathbb{R} \iff z^* = z.$$

Then for any $u \in \mathbb{C}$ we have

$$\begin{aligned}(uu^*)^* &= u^*(u^*)^* \\ &= u^*u \\ &= uu^*\end{aligned}$$

and hence $uu^* \in \mathbb{R}$. ///

[This is exactly why "rationalizing the denominator" works!]

Similarly, we have

$$\begin{aligned}(u+u^*)^* &= u^* + (u^*)^* \\ &= u^* + u \\ &= u + u^*\end{aligned}$$

and hence $u + u^* \in \mathbb{R}$. ///

Finally, on HW3 Problem 5 you proved a useful little theorem.

☆ Useful Little Theorem:

Let $f(x) \in \mathbb{R}[x]$ have degree 3. If $f(x)$ has a root in $\mathbb{C}$ then it must have a root in $\mathbb{R}$.

Proof: Suppose $f(u) = 0$ with $u \in \mathbb{C}$. Then we also have

$$f(u^*) = f(u)^* = 0^* = 0.$$

[Recall HW3 Problem 4.]

If $u \in \mathbb{R}$ we're done. Otherwise, suppose that $u \notin \mathbb{R}$, i.e., $u^* \neq u$. Then by Descartes' Factor Theorem we have

$$f(x) = (x-u)(x-u^*)\, g(x)$$

where $g(x) \in \mathbb{C}[x]$ has degree 1, say $g(x) = ax + b$ with $a, b \in \mathbb{C}$, $a \neq 0$. Note that $g(-b/a) = 0$ and hence

$$f(-b/a) = 0.$$

We're done if we can prove that $-b/a \in \mathbb{C}$ is real. There are a few ways to do this. Perhaps the least slick but most convincing way is to expand the polynomial:

$$f(x) = (x-u)(x-u^*)(ax+b)$$

$$= ax^3 + \text{something} \cdot x^2 + \text{something} \cdot x + uu^*b$$

Since $f(x) \in \mathbb{R}[x]$ we conclude that $a \in \mathbb{R}$ and $uu^*b \in \mathbb{R}$, and since $uu^* \in \mathbb{R}$ this implies $b \in \mathbb{R}$.

Hence $-b/a \in \mathbb{R}$.

$\blacksquare$

You might say this is not interesting because we already know (via the Intermediate Value Theorem) that every real cubic has a real root.

You're right. But the theorem is still interesting because it applies in a more general situation.

What situation?

Suppose we have two fields

$$\mathbb{F} \subseteq \mathbb{E}$$

and an element $\alpha \in \mathbb{E}$ such that $\alpha \notin \mathbb{F}$ but $\alpha^2 \in \mathbb{F}$. Then we define

$$\mathbb{F}[\alpha] := \{ a + \alpha b \; : \; a, b \in \mathbb{F} \}.$$

It turns out that $\mathbb{F}[\alpha]$ is a field, via the same trick of "rationalizing the denominator".

Jargon: We call the pair $\mathbb{F} \subseteq \mathbb{F}[\alpha]$ a

Quadratic Field Extension (Q.F.E.).

Almost everything we know about $\mathbb{R} \subseteq \mathbb{C}$ holds in general for Q.F.E.s.

Math Club Today.

3/30/15

Exam 2 Statistics.

Total: 25
Average: 20.4
Quartiles: 18, 21, 24
St. Dev.: 4.4

Very Approximate Grade Ranges

A $\approx$ 23 – 25
B $\approx$ 21 – 23
C $\approx$ 8 – 19

with the scores so close together, these are not very accurate. My Fault!

I will distribute Exam 2 solutions and new HW 5 on Wednesday.
HW 5 will be due Fri April 10.

Last time we reviewed what we know about the "field extension" from real numbers to complex numbers:

$$\mathbb{R} \subseteq \mathbb{C}.$$

We decided that most of what we know holds in more general settings, such as

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}].$$

Definition: Consider a pair of fields

$$\mathbb{F} \subseteq \mathbb{E}$$

and consider an element $\alpha \in \mathbb{E}$ such that $\alpha \notin \mathbb{F}$ but $\alpha^2 \in \mathbb{F}$. Then we define the set

$$\mathbb{F}[\alpha] := \{ a + \alpha b : a, b \in \mathbb{F} \}.$$

Observe that this is a subring of $\mathbb{E}$ containing $\mathbb{F}$:

$$\mathbb{F} \subseteq \mathbb{F}[\alpha] \subseteq \mathbb{E}.$$

But more is true. Define the conjugation map

$$\begin{aligned} * : \mathbb{F}[\alpha] &\longrightarrow \mathbb{F}[\alpha] \\ a + \alpha b &\longmapsto a - \alpha b \end{aligned}$$

and observe that it is a ring automorphism, i.e., for all $u, v \in \mathbb{F}[\alpha]$ we have

- $(u+v)^* = u^* + v^*$
- $(uv)^* = u^* v^*$. ///

We can use this to prove that for all $u \in \mathbb{F}[\alpha]$ we have

$$uu^* \in \mathbb{F} \quad \text{and} \quad u + u^* \in \mathbb{F}.$$

Now we can observe that $\mathbb{F}[\alpha]$ is actually a field via the trick of "rationalizing the denominator":

$$\frac{1}{u} = \frac{1}{u} \cdot \frac{u^*}{u^*} = \frac{u^*}{uu^*}$$

If $u = a + \alpha b$ this is

$$\frac{1}{a+\alpha b} = \frac{1}{a+\alpha b} \cdot \frac{a - \alpha b}{a - \alpha b} = \frac{a - \alpha b}{a^2 - \alpha^2 b^2}$$

$$= \left(\frac{a}{a^2 - \alpha^2 b^2} \right) + \alpha \left(\frac{-b}{a^2 - \alpha^2 b^2} \right).$$

[This only works because $a^2 - \alpha^2 b^2 \in \mathbb{F}$.]

Jargon: We call $\mathbb{F} \subseteq \mathbb{F}[\alpha]$ a "Quadratic Field Extension" (QFE).

We call $\mathbb{F}[\alpha]$ "$\mathbb{F}$ adjoin α".

Finally, we have a useful little theorem:

☆ Given $f(x) \in \mathbb{F}[x]$ with degree 3, <u>if</u> f has a root in $\mathbb{F}[\alpha]$, <u>then</u> it has a root in $\mathbb{F}$.

<u>Proof</u>: Same as for the QFE $\mathbb{R} \subseteq \mathbb{C}$. ///

So what?

We are trying to prove that

$$\sqrt[3]{2},\ \cos\left(\frac{\pi}{9}\right),\ \cos\left(\frac{\pi}{7}\right) \notin \mathbb{F}_{sqrt}$$

Recall that

$\mathbb{F}_{sqrt}$ = numbers that can be formed from 1 using the operations $+, -, \times, \div, \sqrt{\ }$.

This can be written in a "more complicated but actually more useful" way.

Observation: If $\alpha \in \mathbb{F}_{sqrt}$ then there exists a chain of Quadratic Field Extensions

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \mathbb{F}_3 \subseteq \cdots \subseteq \mathbb{F}_k$$

such that $\alpha \in \mathbb{F}_k$.

Example: Consider $1 + \sqrt{1+\sqrt{2}} \in \mathbb{F}_{sqrt}$.

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq (\mathbb{Q}[\sqrt{2}])[\sqrt{1+\sqrt{2}}]$$

$1+\sqrt{2}$ is in here

$1+\sqrt{1+\sqrt{2}}$ is in here.

The idea is: Every time we take a square root of something that doesn't have a square root, this bumps us up by a QFE.

If you believe that, then we can now prove a Big Theorem.

☆ Theorem: It is impossible to "double the cube" using straightedge and compass.

<u>Proof</u>: By previous discussions, "doubling the cube" is equivalent to constructing a line segment with length $\sqrt[3]{2}$.

We must show that $\sqrt[3]{2} \notin \mathbb{F}_{const}$, or equivalently, $\sqrt[3]{2} \notin \mathbb{F}_{sqrt}$.

Assume for contradiction that $\sqrt[3]{2} \in \mathbb{F}_{sqrt}$. Then there exists a chain of QFE's

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_k \subseteq \cdots \subseteq \mathbb{F}_{sqrt}$$

such that $\sqrt[3]{2} \in \mathbb{F}_k$.

Now observe that $\sqrt[3]{2}$ is a root of the degree 3 polynomial $f(x) := x^3 - 2 \in \mathbb{Q}[x]$.

Since $\mathbb{Q} \subseteq \mathbb{F}_{k-1}$ we can say that $f(x) \in \mathbb{F}_{k-1}[x]$. Then since $f(x)$ has a root in $\mathbb{F}_k$ (namely, $\sqrt[3]{2}$) the useful little theorem says $f(x)$ has a root in $\mathbb{F}_{k-1}$. Call it $c_{k-1} \in \mathbb{F}_{k-1}$.

Now since $\mathbb{Q} \subseteq \mathbb{F}_{k-2}$ we can say that $f(x) \in \mathbb{F}_{k-2}[x]$. Then since $f(x)$ has a root in $\mathbb{F}_{k-1}$ (namely, c_{k-1}) the useful little theorem says that $f(x)$ has a root in $\mathbb{F}_{k-2}$ (call it c_{k-2}).

Continuing in this way by induction, we conclude that $f(x)$ has a root in $\mathbb{Q}$. Call it $c \in \mathbb{Q}$.

But does $f(x) = x^3 - 2$ have a root in $\mathbb{Q}$?

RAN OUT OF TIME :(

4/1/15

HW 5 is due Fri Apr 10
HW 6 will come after
Exam 3 is on Fri Apr 24.

Today we will prove a big Theorem.

Recall the useful little theorem.

☆ Let $\mathbb{F} \subseteq \mathbb{E}$ be a QFE and let $f(x) \in \mathbb{F}[x]$ have degree 3. If f has a root in $\mathbb{E}$, then f has a root in $\mathbb{F}$.

Proof: See HW3.5. ///

☆ Big Theorem: Consider a polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 with NO rational roots. Then the roots of $f(x)$ are NOT CONSTRUCTIBLE.

Proof: Assume for contradiction that $f(\alpha) = 0$ for some constructible α. Then there exists a chain of QFE

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_k .$$

such that $\alpha \in \mathbb{F}_k$. Since $f(x) \in \mathbb{F}_{k-1}[x]$ the ULT implies that f has a root in $\mathbb{F}_{k-1}$. Then since $f(x) \in \mathbb{F}_{k-2}[x]$ the ULT implies that f has a root in $\mathbb{F}_{k-2}$.

Continuing in this way (i.e., using induction) we conclude that f has a root in $\mathbb{Q}$.

CONTRADICTION.

$\blacksquare$

That seems like a strange result, but we will now see that it is very powerful.

Theorem: It is impossible to "double the cube" using straightedge & compass.

<u>Proof</u>: This is equivalent to proving that the number $\sqrt[3]{2} \approx 1.26$ is not constructible. To do this, note that $\sqrt[3]{2}$ is a root of $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. We will show that this f has no rational roots.

$\int$

Suppose that $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with no common factor. Then

$$\left(\frac{a}{b}\right)^3 - 2 = 0$$

$$a^3 - 2b^3 = 0$$

$$a^3 = 2b^3 .$$

Since a divides $2b^3$ and since a, b are coprime we conclude that a divides 2, i.e., $a = \pm 1$ or ± 2.

Since b divides a^3 and since a, b are coprime we conclude that b divides 1, i.e., $b = \pm 1$.

Now the only possibilities for a/b are

$$\frac{a}{b} = \pm 1 \text{ or } \pm 2 .$$

But you can check that none of these is a root of f.

$\blacksquare$

Theorem: It is impossible to "trisect the angle" using straightedge & compass.

Proof: We will prove, in particular, that it is impossible to trisect the angle $\pi/3 = 60°$. To do this it is enough to show that the number $\cos(\pi/9)$ is not constructible.

Recall from HW 4.4 that

$$4\cos^3\theta - 3\cos\theta = \cos(3\theta).$$

Substitute $\theta = \pi/9$ to get

$$4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right) = \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$$

and then let $u = 2\cos(\pi/9)$ to get

$$4\left(\frac{u}{2}\right)^3 - 3\left(\frac{u}{2}\right) = \frac{1}{2}$$

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

$$u^3 - 3u - 1 = 0.$$

If we can show that $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$ has no rational root, then it will follow from the ULT that $2\cos(\pi/9)$ (and hence $\cos(\pi/9)$) is not constructible.

And you proved this on HW 4.5(b).

$\blacksquare$

Theorem: The regular 7-gon is not constructible with straightedge & compass.

<u>Proof</u>: We will prove the equivalent fact that the number $2\cos(2\pi/7)$ is not constructible.

To do this let $\omega = e^{2\pi i/7}$ and consider $u := \omega + \omega^{-1} = 2\cos(2\pi/7)$. We want to find an equation for u (hopefully an equation of degree 3 with rational coefficients).

We will use the fact that

$$\omega^3 + \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} + \omega^{-3} = 0.$$

Note that

$$u^3 = \omega^3 + 0 + 3\omega^2 + 0 + 3\omega^{-1} + 0 + \omega^{-3}$$
$$u^2 = \omega^2 + 0 + 2 + 0 + \omega^{-2}$$
$$u = \omega + 0 + \omega^{-1}$$

so that

$$u^3 + u^2 - 2u - 1 = \omega^3 + \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} + \omega^{-3}$$
$$= 0 .$$

Now let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. We will be done if we can show that $f(x)$ has no rational roots.

Suppose that $f(a/b) = 0$ for some coprime integers $a, b \in \mathbb{Z}$. By the "rational root test" [HW4.5(a)] this implies that a divides -1 (hence $a = \pm 1$) and b divides 1 (hence $b = \pm 1$). This means that $a/b = \pm 1$ and one can check that ± 1 are <u>not</u> roots of $f(x)$.

$\blacksquare$

Good work. That was a substantial piece of mathematics.

History: These three impossibility theorems were first rigorously proved by Pierre Wantzel in 1837. The solution had been sought for thousands of years!

The problem of "squaring the circle" still remained open until it was proved impossible by Ferdinand von Lindemann in 1882. In fact, he proved the stronger result that π is a transcendental number, i.e., it is not the root of any polynomial with rational coefficients.

Lindemann's proof was quite technical and you will be happier if I say nothing about it.

4/3/15

HW 5 due Fri Apr 10
HW 6 will come after.
I am out of town Mon Apr 20.
Exam 3 Fri Apr 24.

Last time we proved a big theorem.

☆ Theorem (Wantzel, 1837):

The following constructions are NOT POSSIBLE with straightedge & compass:

- doubling the cube
- trisecting the angle
- constructing a regular 7-gon.

This finally proved that the system of Euclidean geometry is not complete. In other words,

$$\mathbb{F}_{const} \subsetneq \mathbb{R} .$$

The ancient Greeks would have been deeply troubled by this;

it would have been a crisis similar to the Pythagorean discovery that

$$\mathbb{Q} \subsetneq \mathbb{R}$$
$$\sqrt{2}$$

Wantzel actually proved a much more general result about the constructibility of regular polygons. Here he was building on the work of Carl Friedrich Gauss (1777 – 1855).

Recall: The Greeks knew that every 2^k-gon is constructible. They also knew that if the m-gon and n-gon are constructible, with $\gcd(m,n) = 1$, then the (mn)-gon is constructible.

That is they knew that the regular

$$2^k \cdot 3\text{-gon}, \quad 2^k \cdot 5\text{-gon}, \quad \text{and } 2^k \cdot 3 \cdot 5\text{-gon}$$

are constructible for all k.

This was the state of Knowlegde for over 2000 years until Gauss shocked the world in 1796 (he was 19 years old) by showing that the regular 17-gon is constructible.

Surprisingly, he did not show <u>how</u> to construct the 17-gon but he showed it is <u>possible</u> by proving that

$$16\cos(2\pi/17) = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}$$
$$+ 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}},$$

which is a constructible number. The first explicit construction of the 17-gon was given by Johannes Erchinger in 1825.

[Gauss requested that the 17-gon be inscribed on his tombstone, but the stonemason apparently declined ☺. A 17-pointed star does appear on a modern monument to Gauss.]

Five years later Gauss proved something even more spectacular:

The regular 257-gon and 65537-gon are also constructible!

What?! This becomes more clear if we use a different language.

Definition: Let n be a positive integer. We define

$$\varphi(n) := \#\{k : 1 \leq k \leq n-1,\ \gcd(k,n) = 1\}.$$

This is called Euler's totient function (see HW 5).

Gauss proved that if $\varphi(n)$ is a power of 2 then the regular n-gon is constructible. He also claimed that this condition is necessary but didn't give a proof.

Wantzel finished the proof in 1837.

☆ Gauss - Wantzel Theorem:

The regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2.

///

You will show on HW5 that $\varphi(n)$ is a power of 2 if and only if

$$n = 2^k \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_m$$

where $p_1, p_2, \ldots, p_m$ are distinct "Fermat primes", i.e., primes of the form $2^a + 1$.

You will also show that if $2^a + 1$ is prime then a is a power of 2.

Define the nth "Fermat number" by

$$F(n) := 2^{(2^n)} + 1.$$

In 1650, Pierre Fermat conjectured that $F(n)$ is prime for all $n \geq 0$, based on the evidence that

$$F(0) = 2^1 + 1 = 3$$
$$F(1) = 2^2 + 1 = 5$$
$$F(2) = 2^4 + 1 = 17$$
$$F(3) = 2^8 + 1 = 257$$
$$F(4) = 2^{16} + 1 = 65537$$

are all prime. Leonhard Euler showed in 1732 that

$$F(5) = 2^{32} + 1 = 4294967297$$

is <u>not</u> <u>prime</u>. To this day, no other "Fermat prime" has been found, but it has not been proved that none exist.

In this sense, the problem of constructible polygons is <u>still</u> <u>open</u>.

///

4/6/15

HW 5 due Friday
HW 6 will follow
I am out of town Mon Apr 20.
Exam 3 is Fri Apr 24.

Last time we discussed the

☆ Gauss-Wantzel Theorem:

The regular n-gon is constructible with straight edge and compass if and only if $\varphi(n)$ is a power of 2.

Equialently, n is a power of two times a product of distinct Fermat primes, i.e., primes of the form 2^a+1 for some a.

[You will investigate these ideas on HW5]

We have now shown that

$$\mathbb{Q} \subsetneq \mathbb{Q}_{const} \subsetneq \mathbb{R}$$

$\sqrt{2}$ $\qquad$ $\sqrt[3]{2}$

$\cos(\pi/9)$

$\cos(\pi/7)$

In other words, the Pythagorean and Euclidean systems are both incomplete.

And yet, we know that the numbers

$$\sqrt[3]{2}, \quad \cos\left(\frac{\pi}{9}\right), \quad \cos\left(\frac{\pi}{7}\right)$$

all have formulas involving the operations
$+, -, \times, \div, \sqrt{\ }, \sqrt[3]{\ }$.

It is probably too much to hope that every number can be written this way, so let's include roots of all orders.

Definition: Let

$\mathbb{Q}_{rad}$:= numbers than can be formed from 1 using the operations
$+, -, \times, \div, \sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }, \sqrt[5]{\ }, \ldots$.

We will call this the field of radical numbers. Note that this is a subfield of $\mathbb{C}$, containing the constructible numbers:

$$\mathbb{Q} \subsetneq \mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad} \subseteq \mathbb{C}$$

The question now becomes:

$$\mathbb{Q}_{rad} = \mathbb{C} \quad ?$$

i.e., is <u>every</u> number "expressible by radicals" ?

It is actually not hard to prove that the answer is <u>NO</u>.

<u>Definition</u>: We define the set of <u>algebraic</u> <u>numbers</u> as follows

$$\mathbb{Q}_{alg} := \{ \alpha \in \mathbb{C} : f(\alpha) = 0 \text{ for some } f \in \mathbb{Q}[x] \}$$

It turns out that $\mathbb{Q}_{alg}$ is a <u>field</u> (the product and sum of algebraic numbers is algebraic). One can also show that every radical number is algebraic. We thus have a chain of subfields

$$\mathbb{Q} \subsetneq \mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad} \underset{?}{\subseteq} \mathbb{Q}_{alg} \underset{?}{\subseteq} \mathbb{C}.$$

Our goal for the rest of the class is to examine the inclusions

$$\mathbb{Q}_{rad} \subseteq \mathbb{Q}_{alg} \subseteq \mathbb{C}.$$

It will turn out that <u>both</u> inclusions are strict.

☆ Abel - Ruffini Theorem (1823):

$$\mathbb{Q}_{rad} \subsetneq \mathbb{Q}_{alg}.$$

i.e., there exists a polynomial whose roots are not "solvable by radicals"

☆ Liouville's Theorem (1844):

$$\mathbb{Q}_{alg} \subsetneq \mathbb{C}.$$

i.e., there exists a complex (or real) number that is not the root of any polynomial with rational coefficients.

Jargon: The elements of $\mathbb{C} - \mathbb{Q}_{alg}$ are called trans<u>cendent</u>al <u>numbers</u>.

Specifically, Liouville proved that the number

$$\frac{1}{1} + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \cdots + \frac{1}{10^{n!}} + \cdots$$

is transcendental. Thus transcendental numbers exist. You might object that Liouville's number seems artificial.

Charles Hermite proved proved in 1873 that e is transcendental and Ferdinand von Lindemann proved that π is transcendental in 1882.

In retrospect, we know that almost all complex/real numbers are transcendental because the set of complex/real numbers is uncountably infinite, whereas the set of algebraic numbers is only countably infinite.

Thus

$$\mathbb{Q} \subsetneq \mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad} \subsetneq \mathbb{Q}_{alg} \subsetneq \mathbb{C}$$

this is the BIGGEST JUMP!

That was culture. Let's get back to mathematical details.

Recall from Exam 1 Problem 4 that the equation

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

has solution given by

$$x = \sqrt[3]{4} + \sqrt[3]{2}$$

$$\approx 2.847.$$

But this only looks like <u>one</u> <u>solution</u>. Where are the other two?

By now we should have the tools to figure this out.

The problem is that Cardano's Formula is not very sophisticated about how it handles complex numbers.