3/2/15

HW 4 TBA
Spring Break Mar 9-13
I'm out of town Mon Mar 16
Exam 2 Wed Mar 25.

Last time we discussed factoring the polynomial $x^n - 1$ over various rings/fields.

Over $\mathbb{C}$ we have

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1})$$

where $\omega = e^{2\pi i/n}$. Over $\mathbb{R}$ we have

$$x^n - 1 = \begin{cases} (x-1)(x+1)\prod_{k=1}^{\frac{n}{2}-1}\left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right)x + 1\right) & n \text{ even} \\ (x-1)\prod_{k=1}^{\frac{n-1}{2}}\left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right)x + 1\right) & n \text{ odd.} \end{cases}$$

Over $\mathbb{Z}$ (and also over $\mathbb{Q}$) we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

$\S$

The product is over positive integers d that divide n (we write "$d|n$" for "d divides n"). The factors $\Phi_d(x)$ are called "cyclotomic polynomials". They are irreducible over $\mathbb{Q}$, but this is not easy to prove.

[Remark: In general it is not easy to prove that a given polynomial is irreducible over a given ring.]

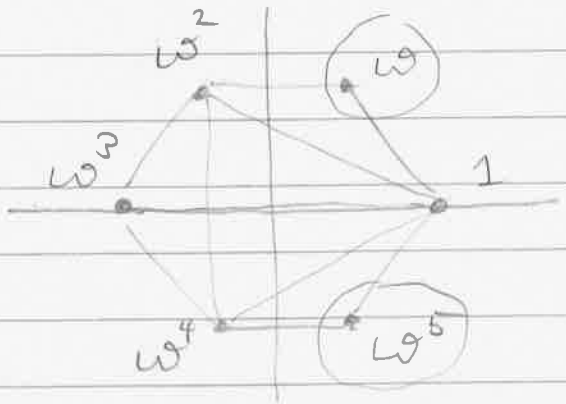
Example:

$$x^6 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)$$
$$= (x-1)(x+1)(x^2+x+1)(x^2-x+1).$$

Definition: We say that ζ is a primitive n^{th} root of unity if

- $\zeta^n - 1 = 0$, i.e., ζ is an n^{th} root of 1.
- $\zeta^m - 1 \neq 0$ for $m < n$, i.e., ζ is not an m^{th} root of 1 for any $m < n$.

Example: Let $\omega = e^{2\pi i/6}$ so the 6^{th} roots of unity form a hexagon



Which ones are primitive 6^{th} roots?

- 1 is a primitive 1st root of 1
- $\omega^3 = -1$ is a primitive 2nd root of 1
- ω^2, ω^4 are primitive 3rd roots of 1

Therefore the primitive 6^{th} roots are

$$\omega^1 \text{ & } \omega^5.$$ ///

This gives us a convenient notation for the cyclotomic polynomial.

$\wr$

Theorem: Let n be a positive integer. Then

$$\Phi_n(x) = \prod_{\zeta} (x - \zeta),$$

where the product is over primitive n^{th} roots of unity ζ.

Example: Let $\omega = e^{2\pi i/6}$, so the primitive 6^{th} roots of 1 are

$$\omega = \cos\left(\frac{2\pi}{6}\right) + i \sin\left(\frac{2\pi}{6}\right)$$

&

$$\omega^5 = \omega^{-1} = \cos\left(\frac{2\pi}{6}\right) - i \sin\left(\frac{2\pi}{6}\right).$$

Therefore the 6^{th} cyclotomic polynomial is

$$\begin{aligned}\Phi_6(x) &= (x - \omega)(x - \omega^{-1}) \\ &= (x^2 - (\omega + \omega^{-1})x + \omega\omega^{-1}) \\ &= x^2 - 2\cos\left(\frac{\pi}{3}\right)x + 1 \\ &= x^2 - x + 1.\end{aligned}$$

as we already know. //

Thinking Problem:

$$\deg(\Phi_n(x)) = ?$$

So we know how to compute the n^{th} roots of 1. Can we compute the n^{th} roots of other numbers?

Theorem: Let $u \in \mathbb{C}$ and let $\alpha \in \mathbb{C}$ be any particular n^{th} root of u. Then the n^{th} roots of u are

$$\sqrt[n]{u} = \alpha, \alpha\omega, \alpha\omega^2, \ldots, \alpha\omega^{n-1},$$

where $\omega = e^{2\pi i/n}$.

Proof: We know that

$$\begin{aligned}(\alpha\omega^k)^n &= \alpha^n(\omega^n)^k \\ &= \alpha^n 1^k \\ &= \alpha^n \\ &= u,\end{aligned}$$

hence these are all n^{th} roots of u.

But we know that u has at most n n^{th} roots (by Descartes' Theorem). Hence we have all of them. ///

Example: Compute the 4th roots of -4.

Step 1: Find one solution $\alpha^4 = -4$.

In polar form we have $\alpha = re^{i\theta}$,

$$\alpha^4 = -4$$
$$(re^{i\theta})^4 = 4e^{i\pi}$$
$$r^4 e^{i4\theta} = 4e^{i\pi}$$

$$\Rightarrow \quad r^4 = 4$$
$$r = +\sqrt[4]{4} = +\sqrt{2}.$$

$$\Rightarrow \quad 4\theta - \pi = 2\pi k$$
$$\theta = \frac{2\pi k + \pi}{4}, \quad k \in \mathbb{Z}.$$

We only need one solution so take $k = 0$ to get

$$\theta = \frac{\pi}{4}.$$

Then

$$\alpha = \sqrt{2}\, e^{i\pi/4} = \sqrt{2}\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = 1 + i .$$

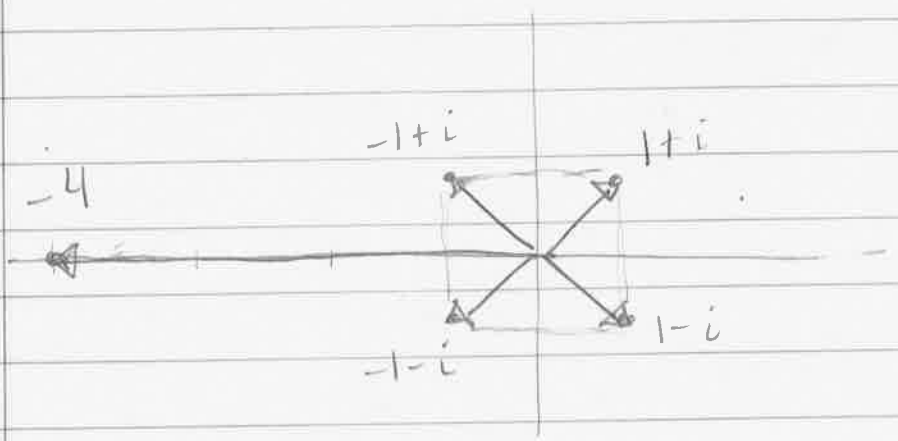
Step 2: The other solutions are

$$\alpha,\ \alpha\omega,\ \alpha\omega^2,\ \alpha\omega^3 .$$

Since $\omega = e^{2\pi i/4} = i$, we get

$$\alpha,\ i\alpha,\ -\alpha,\ -i\alpha .$$

The 4th roots of -4 are: $\pm 1 \pm i$.



Note that they form a square!

3/4/15

HW 4 TBA by this Friday
- due Fri Mar 20.

Spring Break Mar 9 - 13.

NO CLASS Mon Mar 16
- I'm out of town.

Exam 2 Wed Mar 25.

Let ζ be any complex number of length 1.

$$|\zeta| = 1.$$

Then we have

$$\zeta \zeta^* = |\zeta|^2 = 1$$

and hence

$$\zeta^* = \zeta^{-1}.$$

In Polar Form: $\zeta = e^{it}$, $t \in \mathbb{R}$

$$(e^{it})^* = (e^{it})^{-1}$$
$$= e^{-it}.$$

Q: When is $\zeta^n = 1$?

$$(e^{it})^n = e^{int} = 1$$

$$\Longleftrightarrow \quad nt = 2\pi k$$
$$t = 2\pi k/n \quad \text{for some } k \in \mathbb{Z}.$$

Then

$$\zeta = e^{i2\pi k/n} = \left(e^{i2\pi/n}\right)^k.$$

These are the n^{th} roots of unity.

If $\omega := e^{i2\pi/n}$, note that

$$\omega + \omega^{-1} = \omega + \omega^* = 2\cos\left(\frac{2\pi}{n}\right).$$

$$\Longrightarrow \quad \cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}\left[\omega + \omega^{-1}\right]$$

That turns out to be useful.

//

Problem: For which integers n does

$$\cos\left(\frac{\pi}{n}\right)$$

have a "nice" formula?

You already know

$$\cos(\pi/2) = \sqrt{0}/2 = 0$$
$$\cos(\pi/3) = \sqrt{1}/2 = 1/2$$
$$\cos(\pi/4) = \sqrt{2}/2 = 1/\sqrt{2}$$
$$\cos(\pi/6) = \sqrt{3}/2 = \sqrt{3}/2$$
$$\cos(\pi/+\infty) = \sqrt{4}/2 = 1$$

Do you know any others? On HW3.1 we saw that

$$\cos(\theta/2) = \frac{1}{2}\sqrt{2+2\cos\theta}$$

So if we have a formula for $\cos(\pi/n)$ we also get a formula for

$$\cos\left(\frac{\pi}{2^k \cdot n}\right) \quad \text{for any } k \in \mathbb{Z}.$$

Example:

$$\cos\left(\frac{\pi}{12}\right) = \frac{1}{2}\sqrt{2+2\cos\left(\frac{\pi}{6}\right)}$$

$$= \frac{1}{2}\sqrt{2+2\frac{\sqrt{3}}{2}}$$

$$= \frac{1}{2}\sqrt{2+\sqrt{3}}\,.$$

So which angles don't we know yet?

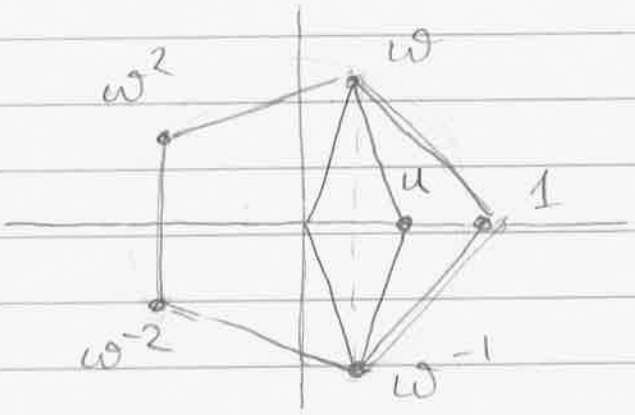
$\frac{\pi}{3}, \frac{\pi}{4}, \left(\frac{\pi}{5}\right), \frac{\pi}{6}, \frac{\pi}{7}, \frac{\pi}{8}, \frac{\pi}{9}, \frac{\pi}{10}$

$$\cos\left(\frac{\pi}{5}\right) = ?$$

How could we compute this? We need some kind of equation that we can solve....

Let $\omega := e^{2\pi i/5}$ and consider the 5th roots of unity.

$$1, \omega, \omega^2, \omega^{-2}, \omega^{-1}.$$



Here are two important facts:

(1) $\omega + \omega^{-1} = 2\cos(2\pi/5)$

(2) $\omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} = 0$. [Why?]

We will turn these into a formula for $\cos(\pi/5)$. First let $u := \omega + \omega^{-1}$ try to find a formula for u. Note that

$$\begin{aligned} u &= (\omega + \omega^{-1})^2 \\ &= \omega^2 + 2\omega\omega^{-1} + \omega^{-2} \\ &= \omega^2 + 2 + \omega^{-2}. \end{aligned}$$

Great. So that means

$$\begin{array}{rr} u^2 & \omega^2 + 0 + 2 + 0 + \omega^{-2} \\ + u & + \quad \omega + 0 + \omega^{-1} \\ - 1 & - \quad 1 \\ \hline 0 & \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} = 0 \end{array}$$

We get an equation

$$u^2 + u - 1 = 0$$

$$\Longrightarrow \quad u = \frac{-1 + \sqrt{5}}{2} \approx 0.618$$

We conclude that

$$2\cos(2\pi/5) = \frac{-1+\sqrt{5}}{2}$$

$$\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}$$

How about $\cos(\pi/5)$?

$$\cos(\pi/5) = \frac{1}{2}\sqrt{2 + 2\cos(2\pi/5)}$$

$$= \frac{1}{2}\sqrt{2 + \frac{-1+\sqrt{5}}{2}}$$

$$= \frac{1}{2}\sqrt{\frac{3+\sqrt{5}}{2}}$$

OK, Good Job.

$$\cos\left(\frac{\pi}{5}\right) = \frac{1}{2}\sqrt{\frac{3+\sqrt{5}}{2}}$$

Does this simplify any further? Yes, it sort of accidentally does. Check that

$$\cos\left(\frac{\pi}{5}\right) = \frac{1+\sqrt{5}}{4}.$$

In any case, the formula is "nice".

Thinking Problem:

What about $\cos\left(\frac{\pi}{7}\right)$ & $\cos\left(\frac{\pi}{9}\right)$?

Are they "nice"?

3/6/15

HW 4 due Fri Mar 20

NO CLASS:
- Mar 9, 11, 13 (Spring Break)
- Mar 16 (I'm out of town).

Exam 3 Wed Mar 25

Last time I asked the question:

For which n does $\cos(\pi/n)$ have a "nice" formula?

What do I mean by "nice"?

Historical Context:

The Pythagoreans (c. 500 BC) believed that "all is number", where "number" means "ratio of whole numbers".

The Crisis: $\sqrt{2}$ is not a "number".

{

Assume that $\sqrt{2}$ is a fraction of whole numbers. Then we can write it in lowest terms $\sqrt{2} = a/b$ where a & b are relatively prime. Then

$$2 = a^2/b^2$$
$$2b^2 = a^2$$

Since a^2 is even, a must also be even, say $a = 2k$ for some $k \in \mathbb{Z}$. Then

$$2b^2 = a^2 = 4k^2$$
$$b^2 = 2k^2.$$

Since b^2 is even, b must also be even, say $b = 2k$.

Now a & b are both even, which contradicts the fact that they are relatively prime.

Because of this the Greeks became distrustful of "number" and instead founded their mathematics on "geometry", in particular, on constructions with

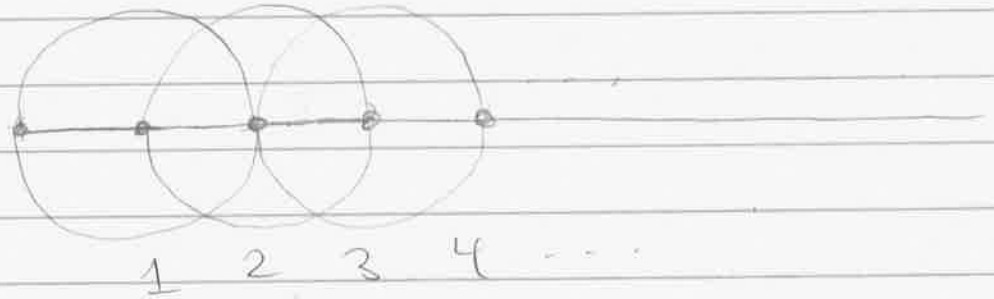
straightedge & compass
(lines & circles)

Starting from a given line segment

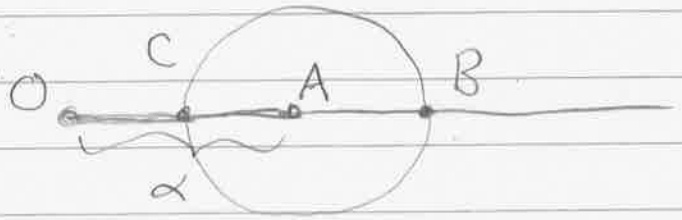
unit length = "1"

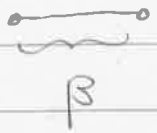
What lengths can we construct ?

Integers ✓



Given lengths α, β we can add and subtract them :

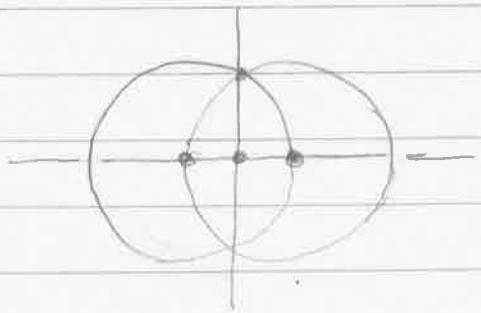


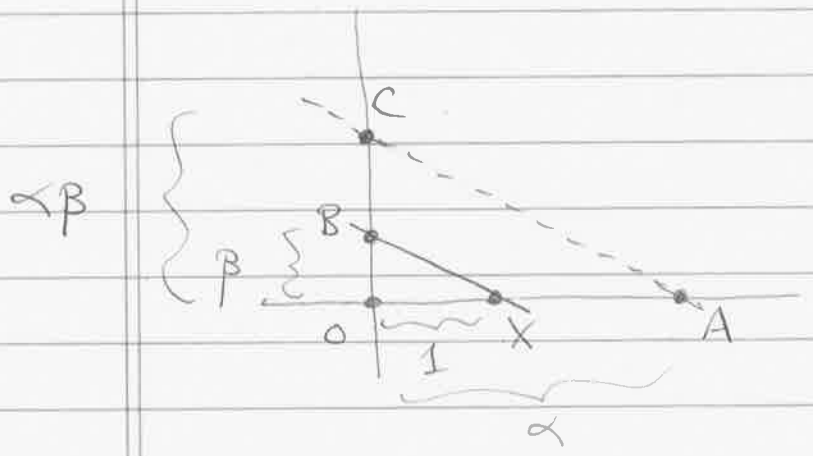


Proof: Given line segment OA of length α and another segment of length β, Euclid I.2 allows us to draw a circle of radius β around A. The segment OB has length $\alpha+\beta$ and the segment OC has length $\alpha-\beta$ (assuming that $\alpha > \beta$).

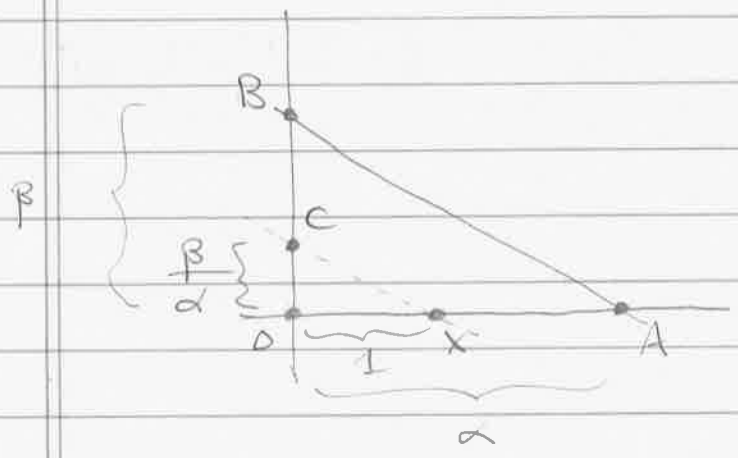
Given lengths α, β we can multiply and divide them.

Proof: Draw perpendicular axes.





To multiply: Use Euclid I.2 to construct X, A, B such that $\overline{OX} = 1$, $\overline{OA} = \alpha$, $\overline{OB}$, β. Then use Euclid I.31 to draw line through A parallel to BX. The segment OC has length $\alpha\beta$. ///

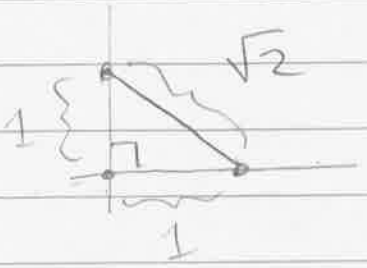


To divide: Construct X, A, B as before. Use Euclid I.31 to draw Line through X parallel to AB. Note that $\overline{OC} = \beta/\alpha$. ///

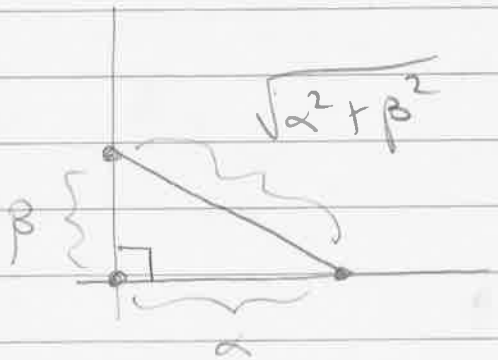
Conclusion: All positive rational lengths are constructible.

Is that all? No.

We know that $\sqrt{2}$ is irrational, but it is certainly constructible



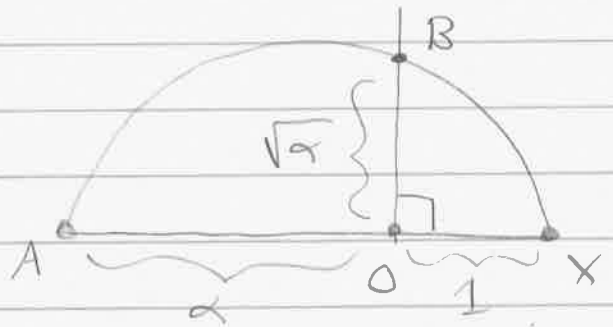
In fact, given lengths α, β we can always construct $\sqrt{\alpha^2+\beta^2}$:



Does that mean we can construct $\sqrt{\alpha}$ for every constructible α ??

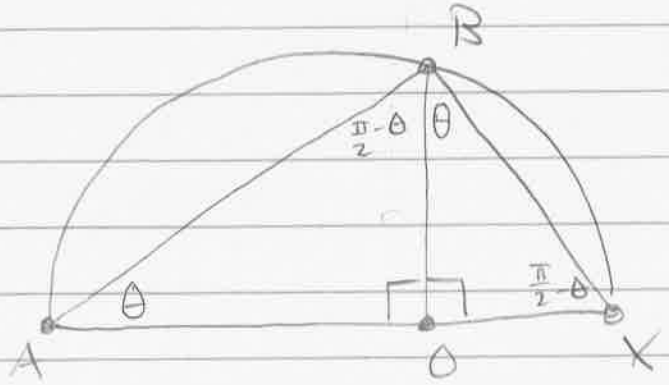
Theorem: If α is constructible then so is $\sqrt{\alpha}$.

Proof: Draw circle on a segment of length $\alpha + 1$.



Construct perpendicular bisector at O. Segment OB has length $\sqrt{\alpha}$.

Why? We'll use Thales' Theorem (Euclid III.33): angle ABX is 90°.



Since the triangles AOB & BOX are similar (same angles), we have

$$\frac{\overline{AO}}{\overline{OB}} = \frac{\overline{OB}}{\overline{OX}} \Rightarrow \frac{\alpha}{\overline{OB}} = \frac{\overline{OB}}{1}$$

$$\Rightarrow \alpha = \overline{OB}^2.$$

Conclusion: All numbers that can be formed from 1 using operations

$$+, -, \times, \div, \sqrt{}$$

are constructible.

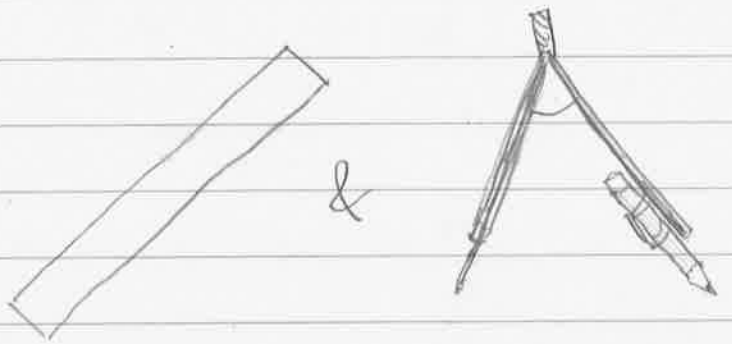
Question: Is every length constructible?

The Greeks probably assumed the answer is yes, but we will prove using modern algebra that the answer is NO!

3/18/15

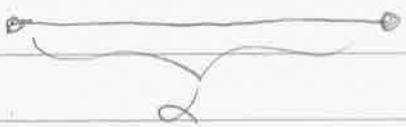
HW 4 due Friday
Review next Monday
Exam 2 next Wednesday

Recall: Last time we discussed constructions with straightedge & compass



We say that a number α is constructible if starting from a unit line segment

we can construct a segment of length α



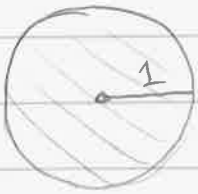
using only a straightedge and compass.

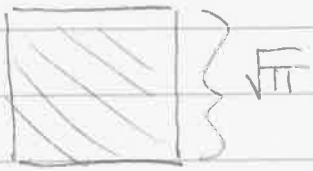
Q: Which numbers are constructible?

The Greeks probably assumed that all numbers are constructible, but they got stuck on a few famous problems

(1) Squaring the Circle.

Given a circle, construct a square with the same area.



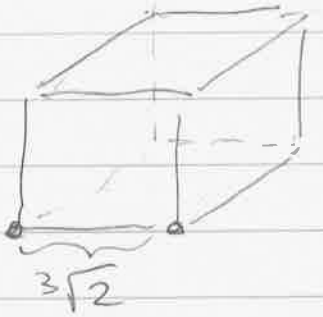


Area π Area π

Is $\sqrt{\pi}$ constructible?

(2) Doubling the Cube.

Given a cube, construct a cube with double the volume.

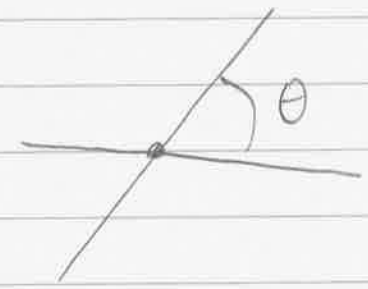


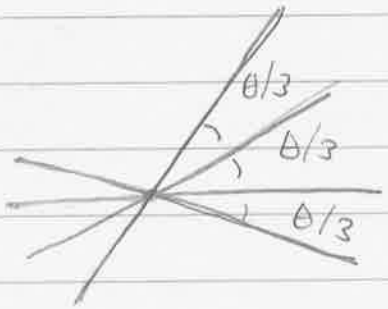
volume 1 volume 2

Is $\sqrt[3]{2}$ constructible?

(3) Trisecting the Angle.

Given the angle θ, construct angle $\frac{\theta}{3}$.



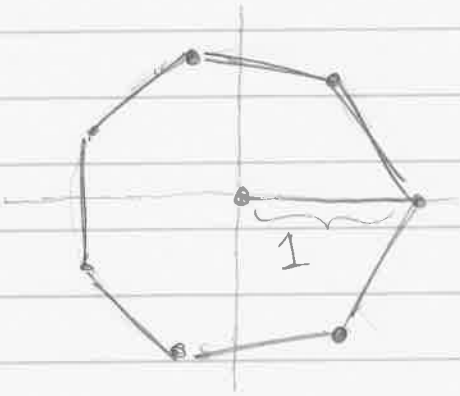


In terms of numbers: Given $\cos\theta$, can you construct $\cos(\theta/3)$?

↓

④ Constructing the Heptagon.

Construct a regular 7-sided polygon.



Is $\cos\left(\frac{\pi}{7}\right)$ constructible?

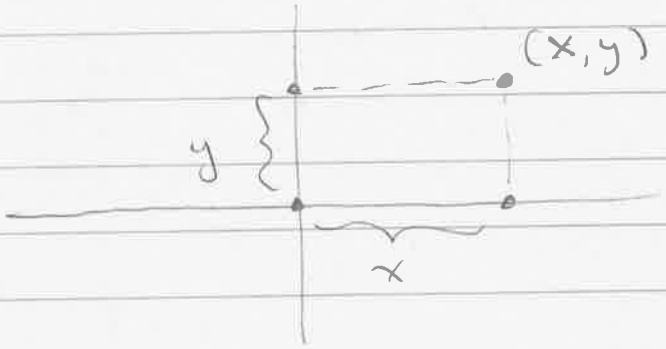
We will prove in this class that constructions ②, ③, ④ are impossible.

Construction ① is also impossible but this is harder to prove. (It was proved by Ferdinand von Lindemann in 1882.)

Q: How could we possibly prove these things?

A: We will translate the problem into ALGEBRA!

To do this we will introduce Cartesian coordinates



The point (x, y) is constructible if and only if the lengths x & y are both constructible. This will also allow us to work with "negative lengths"

This segment has a negative length.

We saw last time that if α, β are constructible then so are

$$\alpha+\beta,\ \alpha-\beta,\ \alpha\cdot\beta,\ \frac{\alpha}{\beta}\ (\text{if } \beta\neq 0),\ \sqrt{\alpha}.$$

In particular the set of constructible numbers form a <u>field</u>.

Call it $\mathbb{F}_{const}$.

Note that every rational number is constructible

$$\mathbb{Q} \subseteq \mathbb{F}_{const}$$

But many constructible numbers are not rational

e.g. $\sqrt{2} \in \mathbb{F}_{const} - \mathbb{Q}$

In order to prove that ②, ③, ④ are impossible, we will prove the following

}

(2) $\sqrt[3]{2} \notin \mathbb{F}_{const}$.

(3) $\cos\left(\frac{\pi}{3}\right) \in \mathbb{F}_{const}$ but $\cos\left(\frac{\pi}{9}\right) \notin \mathbb{F}_{const}$.

(4) $\cos\left(\frac{\pi}{7}\right) \notin \mathbb{F}_{const}$.

and in order to prove this we must obtain a better algebraic understanding of the field $\mathbb{F}_{const}$.

==

First of all, let

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

We will show that $\mathbb{F}_{const} = \mathbb{F}_{sqrt}$.

We already know that $\mathbb{F}_{sqrt} \subseteq \mathbb{F}_{const}$.

How can we show that $\mathbb{F}_{const} \subseteq \mathbb{F}_{sqrt}$?

3/20/15

HW 4 due NOW
(Solutions will be online later today).
Review Monday
Exam 2 Wednesday.

Recall: Last time we defined the field of constructible numbers.

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

We want to prove that

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

and hence the classical problems of "doubling the cube", "trisecting the angle", and "constructing the regular heptagon" are

IMPOSSIBLE.

To prove this we need a better algebraic understanding of the field $\mathbb{F}_{const}$.

As a first step we will prove that

$$\mathbb{F}_{const} = \mathbb{F}_{squrt},$$

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

We saw previously that each of these operations can be performed using compass & straightedge ($\sqrt{}$ is the hardest). Hence

$$\mathbb{F}_{sqrt} \subseteq \mathbb{F}_{const}$$

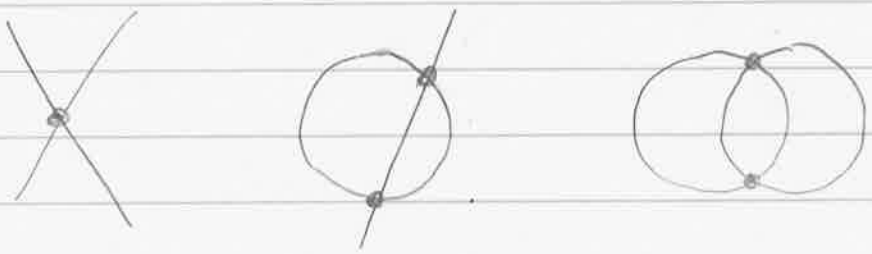
In order to prove that

$$\mathbb{F}_{const} \subseteq \mathbb{F}_{sqrt}$$

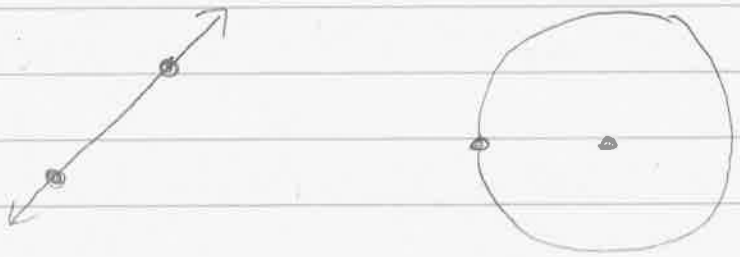
we must show that <u>every</u> constructible number can be expressed via $+, -, \times, \div, \sqrt{}$.

Theorem: $\mathbb{F}_{const} \subseteq \mathbb{F}_{sqrt}$.

Proof: Recall that new points can only be constructed by the intersections of previously constructed lines & circles.



and new lines & circles can only be constructed via straightedge & compass from previously constructed points.



We will proceed by induction. We begin with the points $(0,0)$ and $(1,0)$.

Note that $0, 1 \in \mathbb{F}_{sqrt}$. ✓

The equation of the line containing (a_1, b_1) and (a_2, b_2) is

$$\frac{y - b_1}{x - a_1} = \frac{b_2 - b_1}{a_2 - a_1}$$

$$(y - b_1)(a_2 - a_1) = (x - a_1)(b_2 - b_1)$$

$$y(a_2 - a_1) + x(b_1 - b_2) + \left[b_1(a_1 - a_2) + a_1(b_2 - b_1)\right] = 0.$$

If the points had coordinates in $\mathbb{F}_{sqrt}$ then the coefficients of the equation are in $\mathbb{F}_{sqrt}$.

Similarly the circle with center (a_1, b_2) and containing (a_2, b_2) has coefficients in $\mathbb{F}_{sqrt}$. [Computation omitted.]

Finally we will show that if two lines/circles have coefficients in $\mathbb{F}_{sqrt}$ then their points of intersection have coordinates in $\mathbb{F}_{sqrt}$.

Three Cases:

1. (line – line), Given Lines

$$a_1 x + b_1 y + c_1 = 0$$
$$a_2 x + b_2 y + c_2 = 0$$

their point of intersection (if it exists) is

$$(x_0, y_0) = \left(\frac{a_2 c_1 - a_1 c_2}{a_1 b_2 - a_2 b_1}, \frac{b_1 c_2 - b_2 c_1}{a_1 b_2 - a_2 b_1} \right).$$

If $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{F}_{sqrt}$ then we also have $x_0, y_0 \in \mathbb{F}_{sqrt}$.

2. (line – circle), Given line and circle

(i) $$Ax + By + C = 0$$
(ii) $$(x-a)^2 + (y-b)^2 = r^2$$

with $A, B, C, a, b, r \in \mathbb{F}_{sqrt}$. We write (i) as

$$y = (C - Ax)/B$$

and substitute into (ii) to get a quadratic equation in x with coefficients in $\mathbb{F}_{sqrt}$. Then the Quadratic Formula gives

$$x = \frac{-\mathbb{F}_{sqrt} \pm \sqrt{\mathbb{F}_{sqrt}}}{2\mathbb{F}_{sqrt}} \in \mathbb{F}_{sqrt}.$$

(Abuse of notation. You know what I mean.)

3. (circle-circle). Given two circles

$$(x-A)^2 + (y-B)^2 = R^2$$
$$(x-a)^2 + (y-b)^2 = r^2$$

with $A, B, R, a, b, r \in \mathbb{F}_{sqrt}$. We expand to get

(i) $$x^2 - 2Ax + A^2 + y^2 - 2By + B^2 - R^2 = 0$$

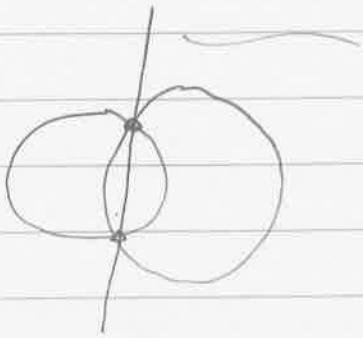
(ii) $$x^2 - 2ax + a^2 + y^2 - 2by + b^2 - r^2 = 0$$

↓

Then we subtract (i) from (ii) to get

(iii) $$x(2A-2a)+y(2B-2b)+\left(a^2+b^2-r^2-A^2-B^2+R^2\right)=0$$

This is the equation of a line.
Which line?



this one.

The points of intersection are now given by intersecting (i) & (iii) or (ii) & (iii).

In either case we are back to Case 2, so we conclude that the points of intersection have coordinates in $\mathbb{F}_{sqrt}$.

Conclusion: We start in $\mathbb{F}_{sqrt}$ and every construction keeps us in $\mathbb{F}_{sqrt}$. Hence

$$\mathbb{F}_{sqrt} \subseteq \mathbb{F}_{const}.$$