Final Algebra Lecture:

Thm: L/K field ext^n, $\alpha_1, \dots, \alpha_n$ alg. $/K$.
Then $K(\alpha_1, \dots, \alpha_n)$ is a finite alg. ext^n $/K$.

Pf: α_i alg. $/K \Rightarrow \alpha_i$ alg. $/K(\alpha_1, \dots, \alpha_{i-1})$

$\Rightarrow [K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})] < \infty$

$\Rightarrow \Rightarrow [K[\alpha_1, \dots, \alpha_n] : K] < \infty \Rightarrow K(\alpha_1, \dots, \alpha_n)/K$ alg. (apply Thm to all elts)

(last: Induct. on degree)

Cor: L/K. The set of alg. elts is a field.

Pf: $\alpha, \beta \in L$ alg $/K \Rightarrow K(\alpha, \beta)/K$ alg.
$\Rightarrow$ this ext^n contains $\alpha \pm \beta, \alpha\beta, \alpha^{-1} (\alpha \neq 0)$, all alg. elts $/K$.

Ex: $\sqrt{2} + \sqrt[3]{2}$ is alg. $/\mathbb{Q}$.

$\exists$ subfield $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ of all alg. elts.
$[\overline{\mathbb{Q}} : \mathbb{Q}]$ is countably ∞.

Cor: L/K finite $\iff$ L gen. by finitely many alg elts.

Th: alg./alg. = alg.

L
|
K
|
F.

Pf: $x \in L$ alg. /K.

$\Rightarrow \exists$ rel^n $a_0 + \cdots + a_n x^n = 0$, $a_i \in K$.

Let $E := F(a_0, \ldots, a_n)$.

E/F is f.g. and alg. $\Rightarrow [E:F] < \infty$

$E(x)/E$ is simple + alg. $\rightsquigarrow$ also finite

$E(x)$
| $< \infty$ $\Rightarrow$ $E(x)/F$ finite
E
| $< \infty$ $\Rightarrow$ x contained in finite ext^n of F
F $\Rightarrow$ $E(x)/F$ alg. $\Rightarrow$ x alg. /F ☐

Straight edge + compass constructions:

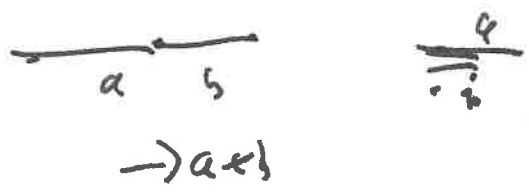
What can you do? Turn into a pf. problem

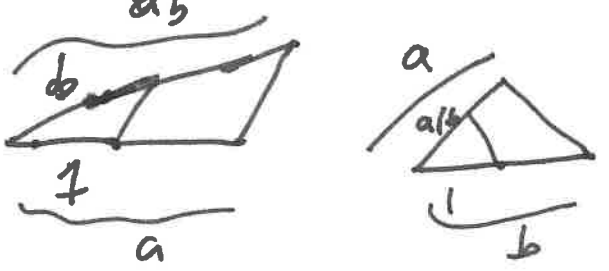
Pick unit distance. A # is constructible

if can construct line of that length,

(also include negatives)

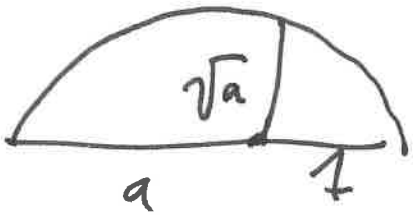
Possibilities:





$\rightsquigarrow$ Set is a subfield of $\mathbb{R}$.

Can intersect lines + circles: solve quadratic eqns



$\rightsquigarrow$ take square roots.

$\rightsquigarrow$ Prop: A real # x is constructible
finite.
$\Leftrightarrow$ iff lives in a tower of quad. ext'ns / $\mathbb{Q}$

In particular, $[\mathbb{Q}(x):\mathbb{Q}] = 2^n$, some n.

Thm: It is impossible to double a cube.

$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3 \neq 2^n$. —

↑ not power of 2.

Can't trisect an angle! Can't construct $\cos(\theta/3)$ given $\cos(\theta)$ (take $\theta = 60°$; $\cos(\theta) = 1/2$).

triple angle: $\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3$

$\beta := \cos(20^\circ)$ satisfies $4\beta^3 - 3\beta - 1/2 = 0$

or $8\beta^3 - 6\beta - 1 = 0$.

rational root theorem

Set $\alpha = 2\beta \rightsquigarrow \alpha$ satisfies $\alpha^3 - 3\alpha - 1 = 0$.

$\rightsquigarrow [\mathbb{Q}(\alpha) : \mathbb{Q}) = 3 \Rightarrow$ not constructible.

Can ☐ the circle: $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$

So not constructible.

Regular n-gon:

bisect angles

Constructible $\iff n = 2^k \cdot p_1 \cdots p_t$ $k \geq 0$.

p_i Fermat primes of shape $2^m + 1$

(necessarily of shape $2^{2^n} + 1$)

Only known ones: $3, 5, 17, 257, 65537$.

Ex: Can construct squares, hexagons, Δ, Pentagon, hexagon, 17-gon ← Gauss

Why those: need: $[\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = 2^k$. Prove!

ζ_n = primitive n^{th} root of 1 ~~order~~ r.o.u. Cyclotomic field

$\zeta_n^2 - 2x\zeta_n + 1 = 0$; $x = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$

deg. = $\varphi(n)$

$\mathbb{Q}(\zeta_n)$

| 2 (find quad. eqn), or Galois

$\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(2\pi/n))$

|

$\mathbb{Q}$

$\mathbb{Q}(\zeta_n)$.

↗

min poly = cyclotomic poly

$\rightsquigarrow$ ~~$\mathbb{Q}(\zeta_n+\zeta_n^{-1})$~~ $\left[\mathbb{Q}(\cos 2\pi/n):\mathbb{Q}\right] \le \varphi(n)/2$.

need $\varphi(n) = 2^k$.

φ is mult. $\Rightarrow$ if $n = p_1^{a_1} \cdots p_t^{a_t}$

$\varphi(n) = \prod \varphi(p_i^{a_i})$ $\Rightarrow$ each $\varphi(p_i)$ a power of 2

$\Rightarrow$ $p=2$ good

$p>2$! ~~$p_i^{a_i} \cdots p_t^{a_t}$~~ $p_i^{a_i-1}(p_i-1) = 2^k$

$\Rightarrow a_i = 1 \Rightarrow p_i - 1 = 2^k$

$\Rightarrow p_i$ Fermat prime ✓

(need Galois for converse)

~~power of 2 # #~~

~~means deg $(\cos(2\pi/n)) = 2^k$~~.

$\mathbb{Q}(\zeta_n)$

|

$\mathbb{Q}(\zeta_n+\zeta_n^{-1})$

$/2^k$

$\mathbb{Q}$

Galois theory says: Gal gp.

size power of 2 ...

$\rightsquigarrow$ group theory —

chain of descending subgps

of index 2

$\rightsquigarrow$ Galois $\rightarrow$ chain of ext. of deg 2.

extensions, built

quadratic

7-gon

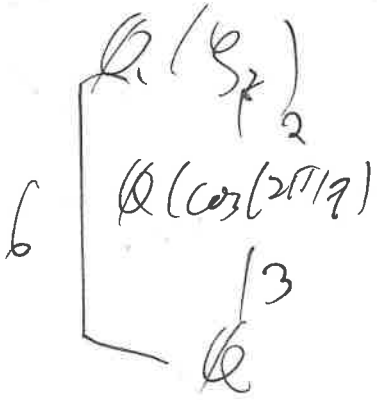
Ex: Can't do heptagon.

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1)$$

min poly of ζ_7

we saw was red by Eisenstein

$\rightsquigarrow$



Existence! Org ass'n

Solve cubics too!