Take up HW 5 solutions

+ Fixed Field Theorem (pg. 487)

Let K be a field, $H \leq \mathrm{Aut}(K)$, $|H| = n < \infty$

Then

$$K^H := \{\alpha \in K : \mu(\alpha) = \alpha \ \forall \mu \in H\}$$

is a subfield with $[K : K^H] = |H|$.

Proof: Given any $\beta_1 \in K$, let $\{\beta_1, \beta_2, \dots, \beta_r\}$ be its H-orbit. Then

$$g(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r) \in K[x].$$

has coefficients fixed by H (since H permutes $\{\beta_1, \dots, \beta_r\}$) $\Rightarrow g(x) \in K^H[x]$

Furthermore, minpoly β_1 / K^H has degree dividing $\deg(g) = |\text{orbit}(\beta_1)|$ which divides $|H|$ by orbit-stabilizer.

Since $K^H \leq K$ is algebraic and every elt. of K has degree $\leq |H|$, $[K : K^H]$ is finite.

Steinitz
$\Longrightarrow$ $\exists\ \gamma \in K$ with $K = K^H(\gamma)$.

Let $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_r$ be the H-orbit $Orb_H(\gamma)$.
If $\mu \in Stab_H(\gamma)$ i.e. $\mu(\gamma) = \gamma$ then
$\mu(\alpha) = \alpha \ \forall\ \alpha \in K^H(\gamma) \Longrightarrow \mu = id \in H$.

$\Longrightarrow |Orb_H(\gamma)| = |H| / |Stab_H(\gamma)|$

$= |H| / 1 = |H| = r$

Claim: $h(x) = (x-\gamma_1)\cdots(x-\gamma_r)$
is the minpoly of γ / K^H.

$\Longrightarrow [K : K^H] = \deg(h) = |H|$ ☐

why irreducible?

sp. $f(x) \in K^H[x]$ satisfies $f(\gamma) = 0$.
Then $\forall\ \mu \in H$,

$0 = \mu(0) = \mu(f(\alpha)) = f(\mu(\alpha))$.

$\Longrightarrow f(\gamma_i) = 0\ \forall\ i \Longrightarrow h_2(x) \mid f(x)$.

HW 6 due Mon Apr 23

Exam 3 Fri Apr 27

Grad Prelim Fri June 1

Today: The Climax

Let $(\mathbb{Q} \subseteq) F \subseteq K$ be a finite (hence algebraic) field extension with Galois group $G = Gal(K/F)$.

Theorem. T.F.A.E.

(1) K is a splitting field over F (i.e. for some $f(x) \in F[x]$)

(2) The fixed field K^G equals F ($K^G = \{\alpha \in K : \mu(\alpha) = \alpha \ \forall \mu \in G\}$).

(3) $|G| = [K : F]$

Definition: If an extension K/F satisfies any of (1), (2), (3) we say it is "normal" (or "Galois").

Finally, TFTOGT:

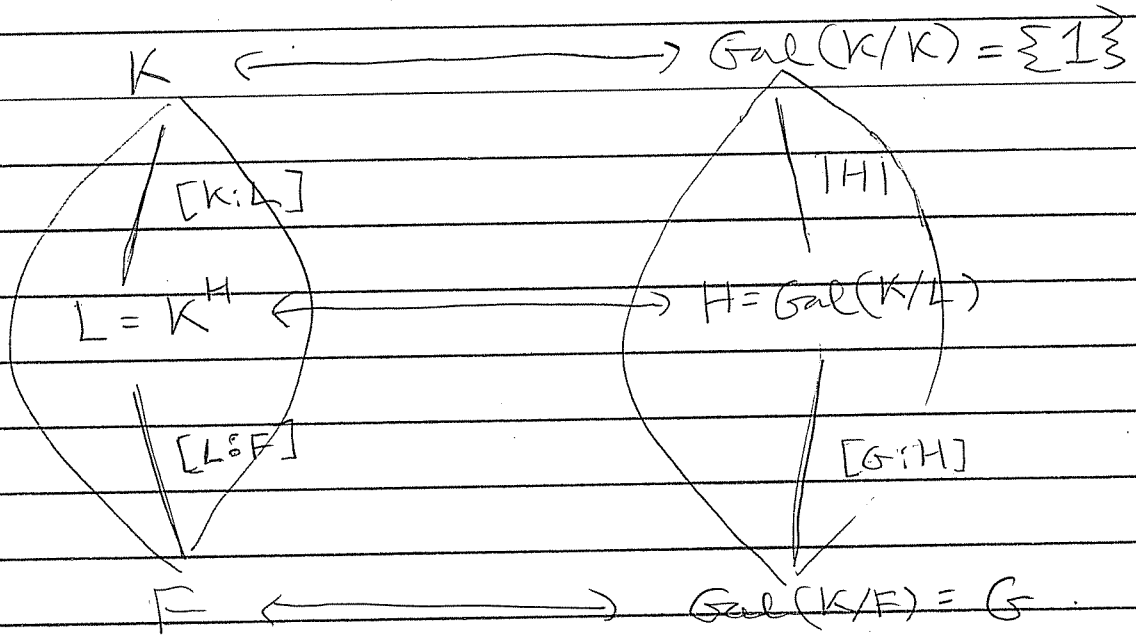
The Fundamental Theorem of Galois Theory

Let K/F be a normal field extension.
Let $\mathcal{L}(K/F)$ = the lattice of intermediate fields $= \{L : F \subseteq L \subseteq K\}$.
Let $G = Gal(K/F)$ and let $\mathcal{L}(G)$ = lattice of subgroups of $G = \{H \leq G\}$.

Then

(1) The maps $H \rightsquigarrow K^H$ and $L \rightsquigarrow Gal(K/L)$ are inverse and provide an (anti-) isomorphis of lattices

$$\boxed{\mathcal{L}(K/L) \overset{\sim}{\longleftrightarrow} \mathcal{L}(G).}$$



(2) Given $F \subseteq L \subseteq K$ and $H = Gal(K/L) \leq G$, the extension K/L is normal, hence

$$[K:L] = |H| \quad \text{and} \quad [L:F] = [G:H]$$

(Tower Law: $[K:F] = [K:L] \cdot [L:F]$
Lagrange: $|G| = |H| \cdot [G:H]$)

(3) H is normal ($H \triangleleft G$) $\iff$ L/F is a normal extension, in which case.

$$Gal(L/F) \cong \frac{Gal(K/F)}{Gal(K/L)} = \frac{G}{H}.$$

(mnemonic: $L/F = \frac{K/F}{K/L}$)

//

HW 6 due Mon Apr 23

Exam Fri Apr 27

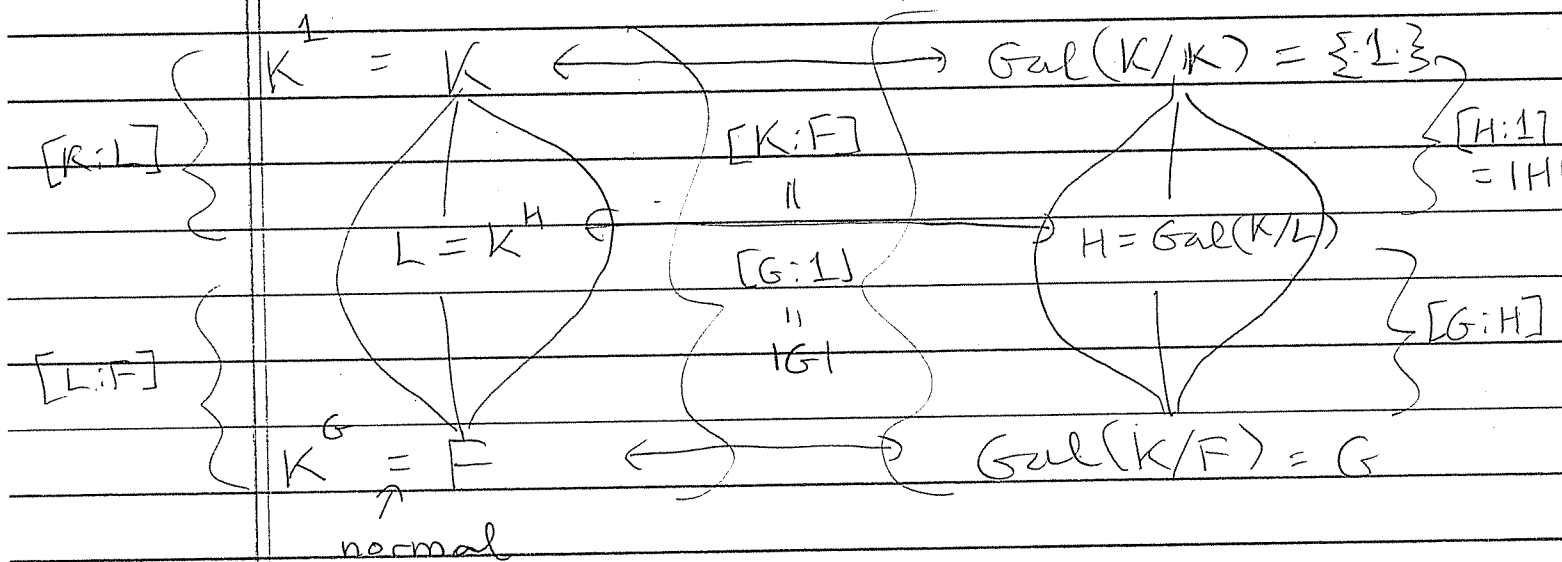
Grad Prelim Fri June 1

Today: Downhill ☺

Recall: TFTOGT

Let K/F be "normal". Then

$$\mathcal{L}(K/F) \xleftrightarrow[\text{anti}]{\sim} \mathcal{L}(\mathrm{Gal}(K/F))$$



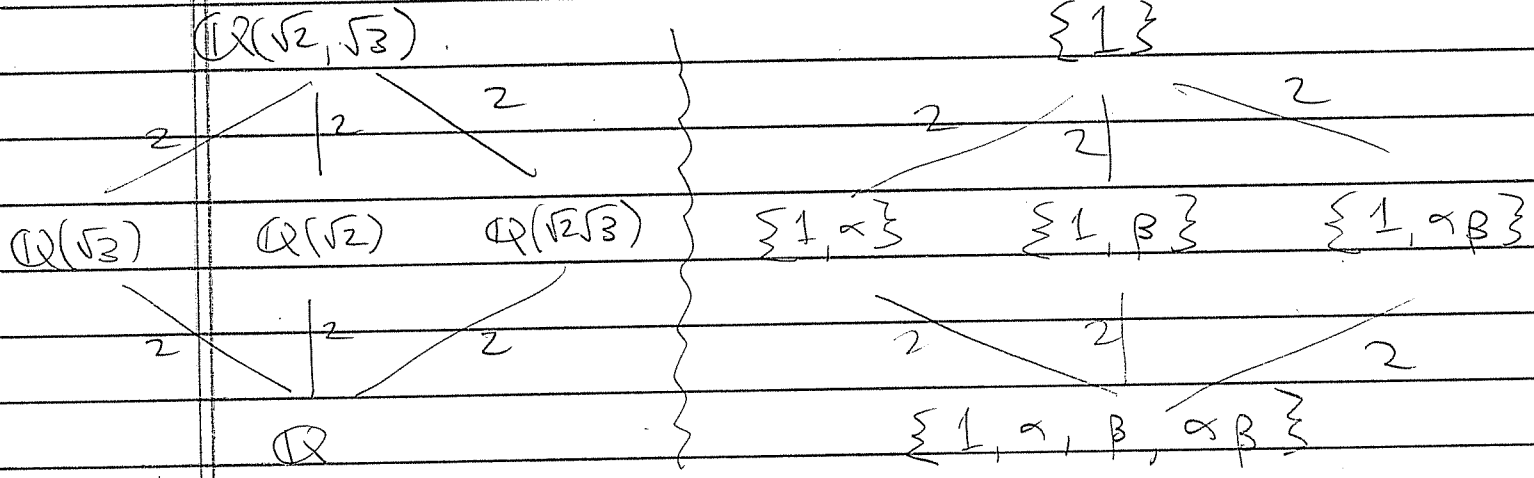
- Tower Law = Lagrange:
  $[K:L] = |H|$ & $[L:F] = [G:H]$

- L/F normal $\iff H \lhd G$, in which case
  $\mathrm{Gal}(L/F) \cong \dfrac{\mathrm{Gal}(K/F)}{\mathrm{Gal}(K/L)}$ //

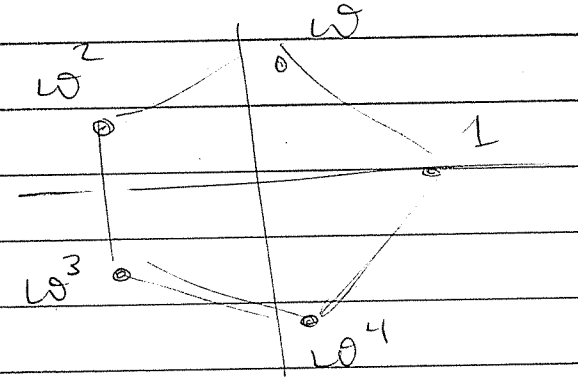
Examples:

(1) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is normal with Galois group

	1	α	β	$\alpha\beta$	
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	



(2) The splitting field of $x^4+x^3+x^2+x+1 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/5}$.



$x^5-1 = (x-1)\cdot(x^4+x^3+x^2+x+1)$.

roots $\omega, \omega^2, \omega^3, \omega^4$

The Galois group.

	1	α	α^2	α^3	$\alpha^4=1$	$\cong \mathbb{Z}/(4)$
ω	ω	ω^2	ω^4	$\omega^8=\omega^3$	$\omega^6=\omega$	

$\mathbb{Q}(\omega)$	$\{1\}$
2 |	| 2
$\mathbb{Q}(\omega)^{\{1,\alpha^2\}}$	$\{1,\alpha^2\}$
2 |	| 2
$\mathbb{Q}$	$\{1,\alpha,\alpha^2,\alpha^4\}$

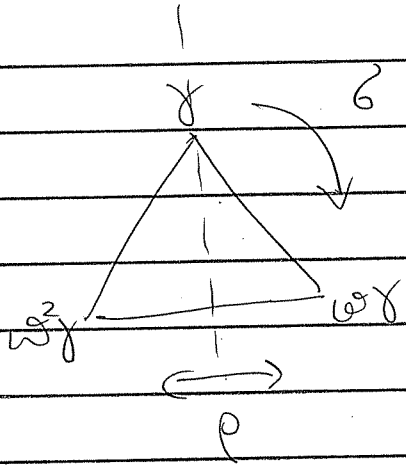
Fact: $\mathbb{Q}(\omega)^{\{1,\alpha^2\}} = \mathbb{Q}(\omega+\omega^4) = \mathbb{Q}\left(\frac{\sqrt{5}-1}{2}\right)$

$= \mathbb{Q}\left(\frac{1+\sqrt{5}}{2}\right) = \mathbb{Q}(\text{golden ratio}) \subseteq \mathbb{R}$.

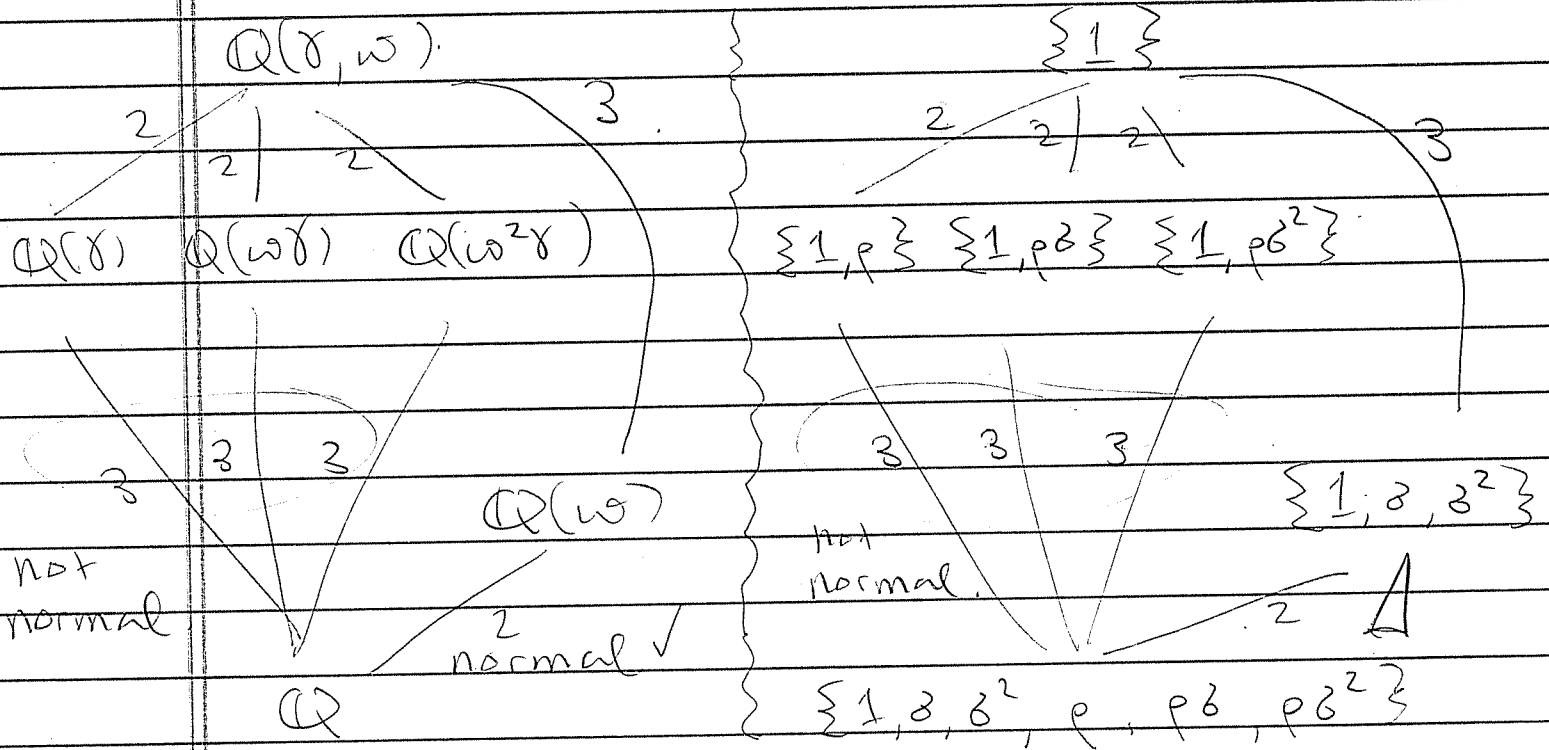
---

(3) Let $\gamma = \sqrt[3]{2} \in \mathbb{R}$, $\omega = e^{2\pi i/3} \in \mathbb{C}$. Then $x^3-2 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\gamma,\omega)$ and Galois group

	1	σ	σ^2	ρ	$\rho\sigma$	$\rho\sigma^2$	
γ	γ	$\omega\gamma$	$\omega^2\gamma$	γ	$\omega^2\gamma$	$\omega\gamma$	$\cong D_3$.
ω	ω	ω	ω	ω^2	ω^2	ω^2	



Symmetries of equilateral triangle.



$\mathbb{Q}(\gamma)/\mathbb{Q}$ is not normal because

$\mathrm{Gal}(\mathbb{Q}(\gamma,\omega)/\mathbb{Q}(\gamma)) \not\trianglelefteq \mathrm{Gal}(\mathbb{Q}(\gamma,\omega)/\mathbb{Q})$.

Also $[\mathbb{Q}(\gamma):\mathbb{Q}] = 3$

But $|\mathrm{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q})| = 1$.

$1 \neq 3$.

HW 6 due Mon Apr 23

Exam 3 Fri Apr 27

Grad Prelim Fri June 1

Today: Straightedge & Compass

The Beginning

Pythagoras: "All is number"

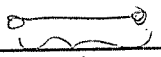
The Crisis: $\sqrt{2}$ is not a number ($\sqrt{2} \notin \mathbb{Q}$).

Resolution: Replace

"number" $\leftarrow$ "length of line segment"

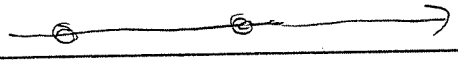
Greek math founded on

lines & circles $\longleftrightarrow$ straightedge & compass

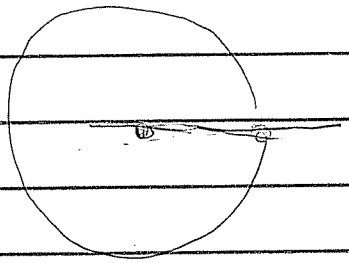
Axioms: Start from 

We can

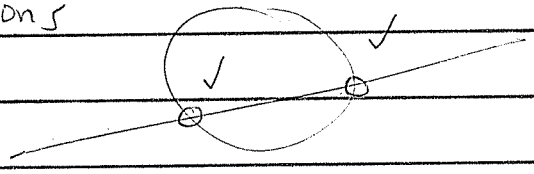
① Draw lines (indefinitely)



(2) Draw circle on radius



(3) Find intersections



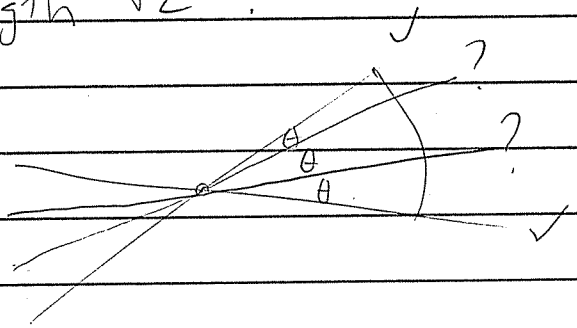
///.

☆ Goal: Prove/Construct every true thing.

Problems emerged:

(1) ∃? line segment length $\sqrt[3]{2}$?

(2) Trisect an angle?



(3) Draw regular 7-gon?

(4) ∃? line segment length π ?

STUCK!

Enter Descartes (1637):

point = ordered pair of numbers.

DEF: Say $\alpha \in \mathbb{R}$ is constructible $\iff$ point $(\alpha, 0)$ is constructible with edge & compass.

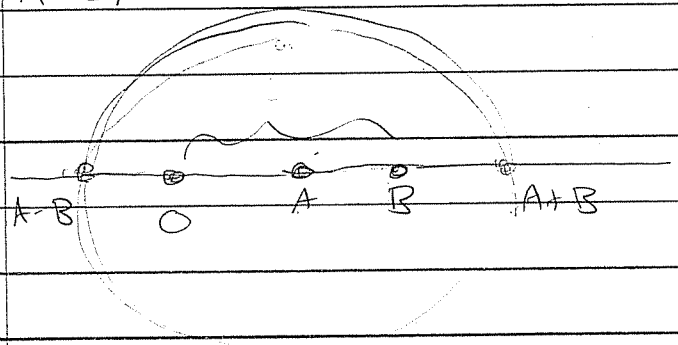
Axiom: 0 & 1 are constructible.

Let $F \subseteq \mathbb{R}$ be the sub set of c'ble numbers.

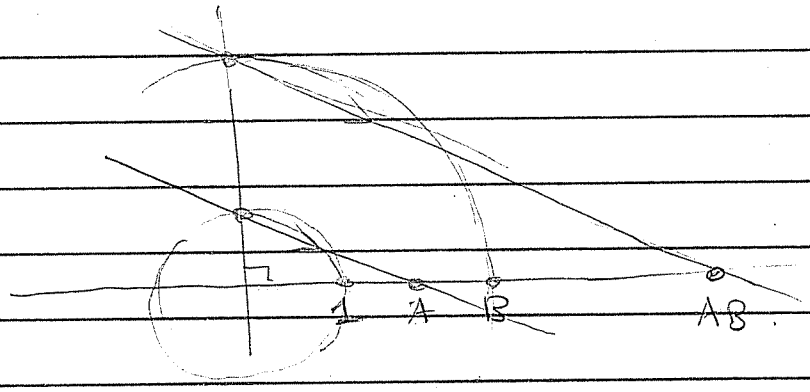
Theorem: $F \subseteq \mathbb{R}$ is a subfield

Given $A, B \in F$:

ADD/SUBTRACT. Draw circle center = A
radius = B.

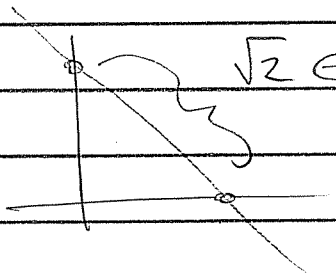


MULTIPLY/
DIVIDE.



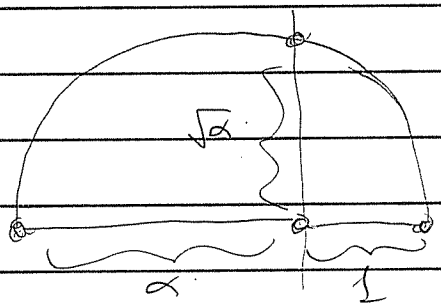
Corollary: $\mathbb{Q} \subseteq F \subseteq \mathbb{R}$.

Idea: $\mathbb{Q} = F$? NO.



In general, $\alpha \in F$, $\alpha > 0 \Rightarrow \sqrt{\alpha} \in F$.

Proof:



So F is closed under $+, -, \times, \div$, $\sqrt{}$
(field; more)

Is that all? Yes.

Theorem: $\alpha \in \mathbb{R}$ is c'ble $\iff$
$\exists$ chain of degree 2 field extensions

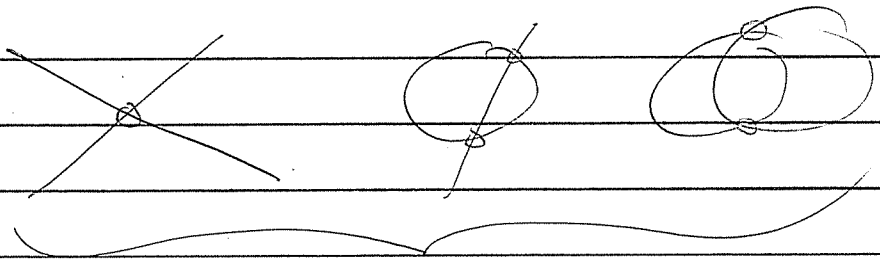
$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = \mathbb{Q}(\alpha) \left(\subseteq \mathbb{R}\right)$$

with $\alpha \in F_n$.

Lose nothing by taking $\subseteq$ instead.

Proof: $\Leftarrow$ done.

$\Rightarrow$: Where do new points come from?



Quadratic equations with constructible coefficients

Use Quadratic formula ∎

Corollary: α constructible $\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] =$ power of 2

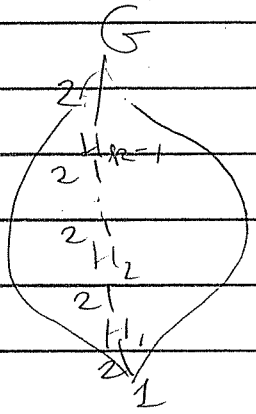
Remark: If $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal then

α c'ble $\Leftrightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k$, $k \in \mathbb{N}$.

Proof uses Galois & group theory.

$|Gal(\mathbb{Q}(\alpha)/\mathbb{Q})| = 2^k$

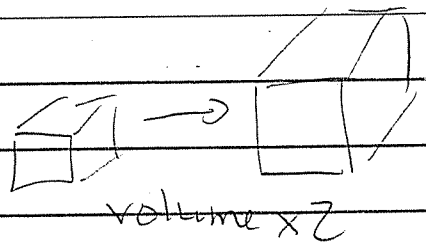
Find a chain of normal subgroups of index 2.



∎

Corollary: Classical problems (1), (2), (3) are impossible.

(1) If we can double a cube



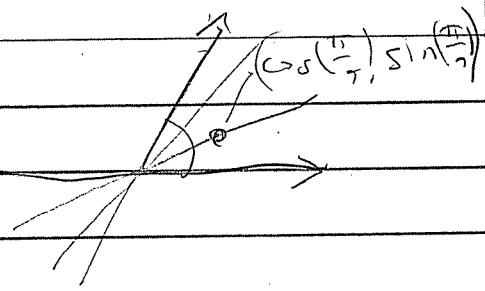
Then $\sqrt[3]{2}$ is constructible

$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2^k$

But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

(minpoly $x^3 - 2$).

(2) If we can trisect $\pi/3$



$\Rightarrow \cos(\frac{\pi}{9})$ c'ble

$\Rightarrow 2\cos(\frac{\pi}{9})$ c'ble

$\Rightarrow [\mathbb{Q}(2\cos(\frac{\pi}{9})) : \mathbb{Q}] = 2^k$

But $[\mathbb{Q}(2\cos(\frac{\pi}{9})) : \mathbb{Q}] = 3$

(minpoly $x^3 - 3x - 1$).

(3) If we can construct regular 7-gon

then $\cos(\frac{\pi}{7})$ is c'ble.

$2\cos(\frac{\pi}{7})$ has minpoly $x^3 + x^2 - 2x - 1$

HW 6 due Mon Apr 23

Exam 3 Fri Apr 27

Grad Prelim Fri June 1

Today: Regular Polygons (Roots of unity).

$\mathbb{C}$

$\mathbb{R}$

Recall: $\alpha \in \mathbb{R}_{\geq 0}$ is constructible (with straightedge & compass)

$\Updownarrow$

$\exists$ chain of quadratic extensions

$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = \mathbb{Q}(\alpha)$.

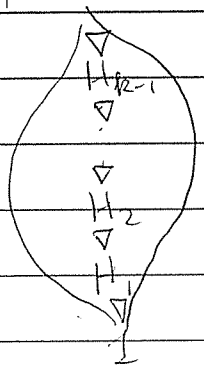
Cor: α c'ble $\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k$

Partial Converse: If $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k \Rightarrow \alpha$ c'ble.

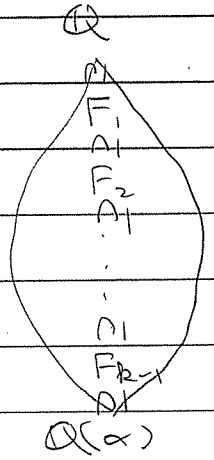
NON TRIVIAL!

Proof: $|Gal(\mathbb{Q}(\alpha)/\mathbb{Q})| = 2^k$

$\exists$ chain by group theory.

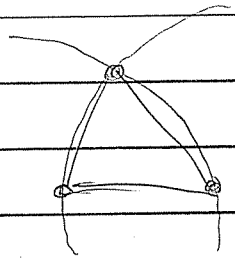


$\exists$ chain of field extensions by Galois connection



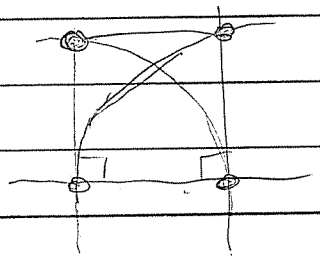
Q: For which n is regular n-gon c'ble?

$n=3$



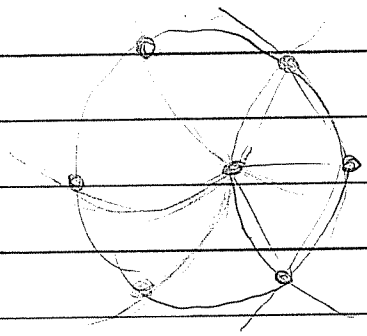
✓ $2^k \cdot 3$

$n=4$



✓ 2^k

$n=6$



✓

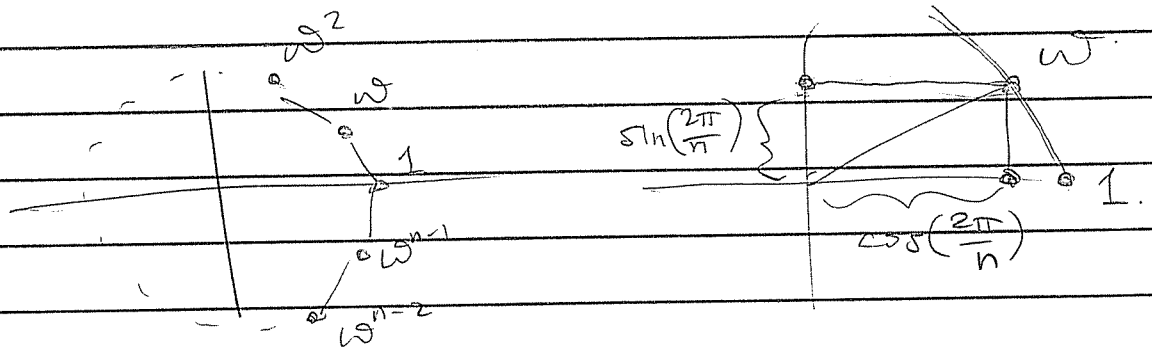
Fact n-gon c'ble $\Rightarrow$ $2^k n$-gon c'ble.

Q: $n=5$? $n=7$?

Let $\omega_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$.

So $\sqrt[n]{1} = \{1, \omega_n, \omega_n^2, \cdots, \omega_n^{n-1}\}$

= vertices of regular n-gon



Theorem: regular n-gon c'ble

$\Updownarrow$

$\cos\left(\frac{2\pi}{n}\right)$ c'ble.

$\Updownarrow$

ω_n c'ble.

$\Updownarrow$

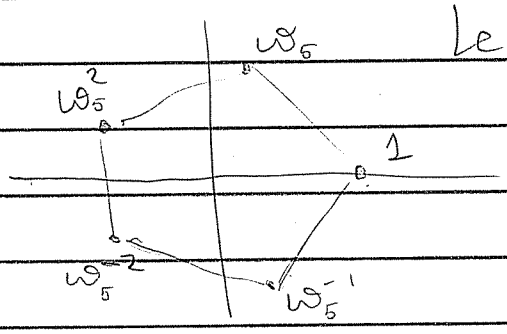
$[\mathbb{Q}(\omega_n) : \mathbb{Q}] = 2^k$.

[$\mathbb{Q}(\omega_n)$ is called the nth cyclotomic field]

angle	$2\pi/3$	$2\pi/4$	$2\pi/5$	$2\pi/6$	$2\pi/7$
cosine	$-1/2$	0	$\frac{1}{4}(\sqrt{5}-1)$	$1/2$	
c'ble?	✓	✓	✓	✓	✗

$$\cos\left(\frac{2\pi}{7}\right) = \frac{1}{6}\left[\sqrt[3]{\frac{7+21\sqrt{-3}}{2}} + \sqrt[3]{\frac{7-21\sqrt{-3}}{2}} - 1\right]$$

Pentagon: $\omega_5 = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$.



Let $u = \omega_5 + \omega_5^{-1} = 2\cos\left(\frac{2\pi}{5}\right)$.

Note: $\omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} = 0$

Because

$$x^5 - 1 = (x-\omega^2)(x-\omega)(x-1)(x-\omega^{-1})(x-\omega^{-2})$$
$$= x^5 - (\omega^2 + \cdots + \omega^{-2})x^4 + \cdots$$
$$0.$$

Then $u^2 = (\omega + \omega^{-1})^2 = \omega^2 + 2\omega\omega^{-1} + \omega^{-2}$.

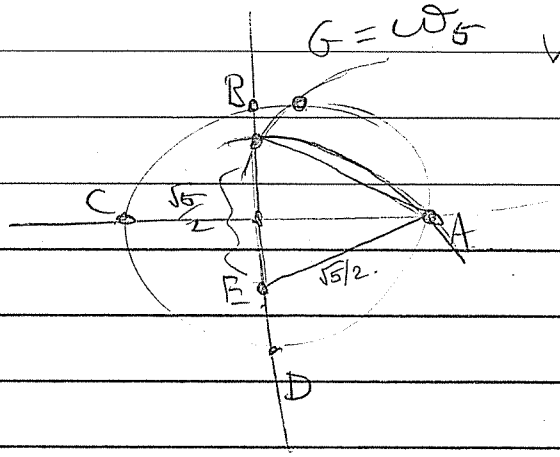
$$= \omega^2 + \omega^{-2} + 2.$$
$$= (\omega^2 + \omega^1 + 1 + \omega^{-1} + \omega^{-2}) - (\omega + \omega^{-1}) + 1$$
$$= 0 - u + 1.$$

$\Rightarrow u^2 + u - 1 = 0$, $(u > 0)$.

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

$\Rightarrow \cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{2}$ c'ble!

Construction:



It was possible because.

$$\mathbb{Q}(\omega_5) \supseteq_2 \mathbb{Q}(\sqrt{5}) \supseteq_2 \mathbb{Q}.$$

Q: For which n is $[\mathbb{Q}(\omega_n) : \mathbb{Q}] = 2^k$?

Minpoly of $\omega_n / \mathbb{Q}$? Factor $x^n - 1$.

$x^2 - 1 = (x-1)(x+1)$

$x^3 - 1 = (x-1)(x^2+x+1)$

$x^4 - 1 = (x-1)(x+1)(x^2+1)$

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

$x^6 - 1 = (x^3-1)(x^3+1)$.

$= \underset{1}{(x-1)} \underset{3}{(x^2+x+1)} \underset{2}{(x+1)} \underset{6}{(x^2-x+1)}$

Define $\Phi_n(x) = \prod_{k,n \text{ coprime}} (x - \omega_n^k)$.

So $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$

and. $\deg(\Phi_n(x)) = \varphi(n)$

Euler's totient.

Theorem (Gauss):

$\Phi_n(x) \in \mathbb{Z}[x]$ and is irreducible.

Cor: $[\mathbb{Q}(\omega_n) : \mathbb{Q}] = \varphi(n)$.

So when is $\varphi(n) = 2^k$?

Theorem (Gauss-Wantzel):

regular n-gon is c'ble

$\Updownarrow$

$\varphi(n) = 2^k$ for some k

$\Updownarrow$

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

where $p_1, \ldots, p_m$ are distinct "Fermat" primes i.e. $p_i = 2^{2^i} + 1$ for some i.

$7 \neq 2^{2^i} + 1$ NOT Fermat.

$17 = 2^{2^2} + 1$ Yes ✓

(Q: $\exists$ ∞ many fermat primes?)

HW 6 due NOW.

Today: The End.

Wed: Review

Fri: Exam 3

Let $\sqrt{\mathbb{Q}} = \{\alpha \in \mathbb{R} : \alpha \text{ is constructible with straightedge and compass}\}$

Theorem: $\alpha \in \sqrt{\mathbb{Q}} \iff \exists$ chain of quadratic field extensions $\mathbb{Q} : F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n = \mathbb{Q}(\alpha)$

~500 BC

Theorem (Pythagoreans): $\mathbb{Q} \subsetneq \sqrt{\mathbb{Q}}$

Greeks seemed to believe $\sqrt{\mathbb{Q}} = \mathbb{R}$.

1637

Theorem (Descartes): $\sqrt{\mathbb{Q}} \subsetneq \mathbb{R}$

Theorem (Gauss-Wantzel):

$$\cos\left(\frac{\pi}{n}\right) \in \sqrt{\mathbb{Q}}$$

$$\Updownarrow$$

$$n = 2^{\alpha} \cdot p_{i_1} \cdot p_{i_2} \cdots p_{i_k}$$

distinct Fermat primes.

So now what? Take higher roots!

DEF: Let $\sqrt[\infty]{\mathbb{Q}} := \{\alpha \in \mathbb{R} : \alpha$ has a formula in terms of $\mathbb{Q}$, field operations and arbitrary roots.

$\sqrt[\infty]{\mathbb{Q}}$ = "radical numbers" $\supseteq \sqrt{\mathbb{Q}}$

Q: $\sqrt[\infty]{\mathbb{Q}} = \mathbb{R}$?

Theorem (Cardano, 1545):
Given $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$,
Let

$$p = \frac{-b}{3a}, \quad q = p^3 + \frac{bc - 3ad}{6a^2}, \quad r = \frac{c}{3a}$$

Then $f(x) = 0$ has solution

$$x = \sqrt[3]{q + \sqrt{q^2 + (r-p^3)^3}} + \sqrt[3]{q - \sqrt{q^2 + (r-p^3)^3}} + p.$$

- Ferrari gave a similar formula for the quartic.

Q: The quintic?

Theorem (Lagrange-Ruffini-Abel, 1824):

$\exists$ quintic $f(x) \in \mathbb{Q}[x]$ with NO roots in $\sqrt[\infty]{\mathbb{Q}}$.

Since every quintic has a real root, this implies

$$\sqrt[\infty]{\mathbb{Q}} \subsetneq \mathbb{R}.$$

So now what?

DEF: Let $\mathbb{Q}^{alg} := \{ \alpha \in \mathbb{R} : f(\alpha) = 0 \text{ for some } f(x) \in \mathbb{Q}[x] \}$.

HW4: $\mathbb{Q}^{alg}$ is a field.
(the alg. closure of $\mathbb{Q}$ in $\mathbb{R}$)

Re-Phrase Abel: $\sqrt[\infty]{\mathbb{Q}} \subsetneq \mathbb{Q}^{alg}$.

But maybe... $\mathbb{Q}^{alg} = \mathbb{R}$?

Theorem (Liouville, 1844):
$\exists$ transcendental numbers

i.e. $\mathbb{Q}^{alg} \subsetneq \mathbb{R}$.

Summary:

$$\mathbb{Q} \subsetneq \sqrt{\mathbb{Q}} \subsetneq {}^{\infty}\sqrt{\mathbb{Q}} \subsetneq \mathbb{Q}^{alg} \subsetneq \mathbb{R}$$

↑ Pythagoras ↑ Descartes ↑ Abel ↑ Liouville

So now what? We need new tools.

Idea (Galois)

FUNCTOR

Field extension $\hookrightarrow$ Group

K/F $\quad$ $Gal(K/F)$

(numbers) $\quad$ (geometry?)

In this spirit...

Theorem: $\alpha \in {}^{\infty}\sqrt{\mathbb{Q}} \iff \exists$ chain of extensions

$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = \mathbb{Q}(\alpha)$

such that $\forall\, i$, F_{i+1}/F_i is a splitting field for some $x^{k_i} - \alpha_i \in F_i[x]$. ///

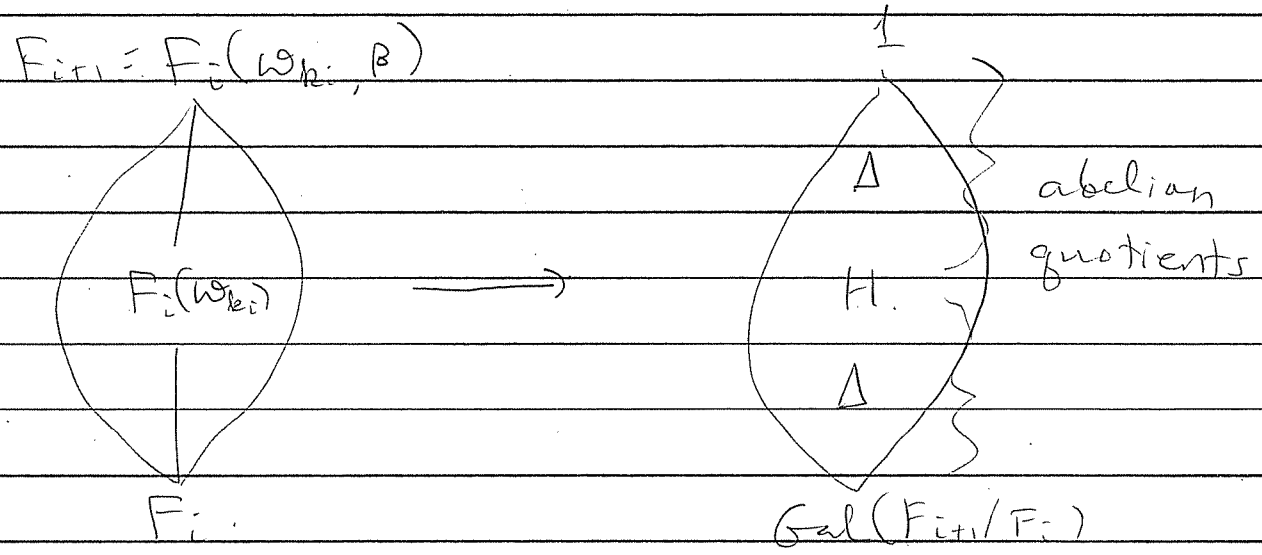
↓

"$\mathbb{Q}(\sqrt[3]{2}, \omega_3)$"

Look closer: $F_{i+1} = F_i(\beta, \omega_{k_i})$

where β is some root of $x^{k_i} - a_i$

and $\omega_{k_i} = e^{2\pi i/k_i}$



⇝ Galois' Theorem: Given $f(x) \in \mathbb{Q}[x]$ with split. field $K/\mathbb{Q}$ Then $f(x)$ is "solvable" (by radicals) $\Leftrightarrow \exists$ chain of normal extensions

$\mathbb{Q} = F_0 \leq F_1 \leq \cdots \leq F_n = K$

with $Gal(F_{i+1}/F_i)$ abelian $\forall i$.

↓

Translation to groups: $\exists$ chain of normal subgroups.

$$1 = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = \mathrm{Gal}(K/\mathbb{Q})$$

with G_{i+1}/G_i abelian $\forall i$.
(say $\mathrm{Gal}(K/\mathbb{Q})$ is a "solvable" group).

Finally, the quintic.

Most quintics have $\mathrm{Gal}(K/\mathbb{Q}) \tilde{\simeq} S_5$.

$$S_5 \overset{2}{\triangleright} I \quad \text{(now what?)} \quad \overset{1}{\triangleright} 1$$

$\uparrow$
icosahedron

I is simple |