4/12

Friday, April 12, 2019 11:29

If K/F is a p-extension ($K \subseteq E$ s.t. E/F is Galois & $|Gal(E/F)| = p^r$), then K is a tower of simple Galois extensions of degree p.

<u>Proof</u>: $G = Gal(E/F)$ is a p-group.

Let $H = Gal(E/K)$. Then $\exists$ subnormal series

$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_r = G \text{ with } H_{i+1}/H_i \cong \mathbb{Z}_p \ \forall i.$$

(by Sylow & something else).

Then let $L_i = Fix(H_i)$ $\forall i$, and then

$K = L_0 \supseteq L_1 \supseteq L_2 \supseteq \cdots \supseteq L_r = F$ s.t. L_i/L_{i+1} are galois

with $Gal(L_i/L_{i+1}) \cong H_{i+1}/H_i \cong \mathbb{Z}_p$. $\square$

<u>Theorem</u> α is constructible over F iff $\alpha \in$ 2-extension of F.

(F - field generated by $S \subseteq \mathbb{R}$).

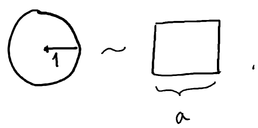
<u>Def</u> $\alpha \in \mathbb{C}$ is constructible iff $Re\,\alpha$ and $Im\,\alpha$ are constructible.

<u>Lemma</u> $\underset{a+bi}{\underset{\parallel}{\alpha}} \in$ 2-extension of $F \subseteq \mathbb{R}$ iff $a, b \in$ 2-extensions of F.

proof If $a \in K_1$, $b \in K_2$ where K_1, K_2 are towers of quadratic extensions, then K_1K_2/F is also a tower of quadratic extensions, and $K_1K_2(i)/F$ is also good, and $\alpha \in K_1K_2(i)$.

Conversely, if $\alpha \in K$ which is a tower of quadratic extensions, then $\bar{\alpha} \in \bar{K}$, and $\bar{K}$ is also a tower of quadratic extensions. Then $\frac{\alpha+\bar{\alpha}}{2} = \operatorname{Re} \alpha \in K\bar{K}$, $\frac{\alpha-\bar{\alpha}}{2i} \in K\bar{K}(i)$, and $K\bar{K}$ and $K\bar{K}(i)$ are 2-extensions $\square$

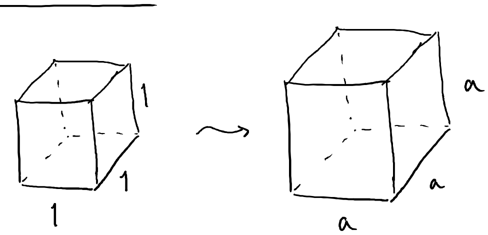
Squaring a Circle



Construct a s.t. $a^2 = \pi$.

Unsolvable since π is transcendental.

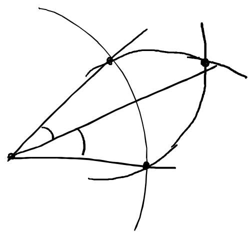
Doubling a Cube



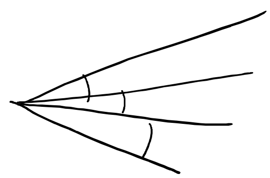
construct a s.t. $a^3 = 2$

Impossible bc x^3-2 is irreducible, $\sqrt[3]{2}$ has degree 3: it's not in a tower of quadratic extns.

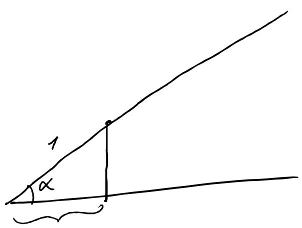
Trisecting an Angle



Bisection.



possible?



$$\underset{\substack{\parallel \\ a}}{\cos\alpha} \rightsquigarrow \text{construct } \underset{\substack{\parallel \\ b}}{\cos\left(\tfrac{\alpha}{3}\right)}.$$

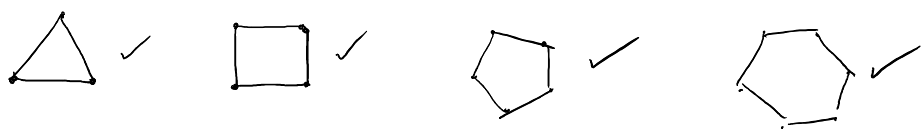
$$\cos\alpha = 4\cos^3\left(\tfrac{\alpha}{3}\right) - 3\cos\left(\tfrac{\alpha}{3}\right).$$

$a = 4b^3 - 3b \rightsquigarrow b$ is a root of $4x^3-3x-a \in \mathbb{Q}(a)$.

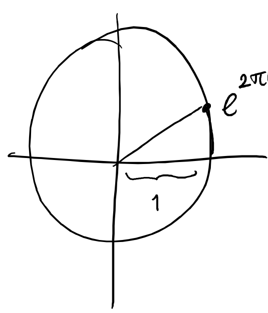
$2x \mapsto x$. $x^3 - 3x - 2a$.

for $a = \frac{1}{2}$, this is irreducible of deg. 3, So its root, b, is <u>not</u> contained in a 2-extension of $\mathbb{Q}(a)$.

Construction of regular n-gons



7-gon : not constructible.



$e^{2\pi i/n} = \omega$, root of $\Phi_n(x)$ of degree $\varphi(n)$.

$\deg \omega = \deg \Phi_n = \varphi(n)$.

if ω is constructible, then $\varphi(n) = 2^r$

If $\varphi(n) = 2^r$, then the splitting field of Φ_n (which is $\mathbb{Q}(\omega)$) <u>has degree 2^r</u>, so ω is constructible

↳ not true for general polynomial, Φ_n is special.

Regular n-gon is constructible iff $\varphi(n) = 2^r$.

3, 4, 5, 6 ok, 7 is not.

$n = 2^k p_1^{l_1} \cdots p_m^{l_m}$ $\quad \varphi(n) = 2^{k-2} \prod p_i^{l_i - 1}(p_i - 1)$,

distinct primes

$\varphi(n) =$ a power of 2 iff $l_i = 1 \; \forall i$ and each

$\underbrace{P_i = 2^{m_i} + 1}_{\text{Fermat Primes}}$ for some m_i.

<u>Lemma</u>: If $2^d + 1$ is prime, then d is a power of 2.

So any fermat prime is $p = 2^{2^k} + 1$ for some k.
$(3, 5, 17, 257, \text{etc.})$

<u>Proof</u> If $d = ml$, m is odd, then $2^d + 1 = 2^{ml} + 1$ is divisible by $2^l + 1$; $\dfrac{x^m + 1}{x + 1}$ if m is odd

If $n_1, \ldots, n_k > 0$ are square-free integers then

$\sqrt{n_1}, \ldots, \sqrt{n_k}$ are linearly independent over $\mathbb{Q}$.

eg. $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}$, etc.

Claim: if $p_1, \dots, p_k$ are distinct primes, then

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k}) : \mathbb{Q}] = 2^k,$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})/\mathbb{Q}) \cong \mathbb{Z}_2^k$$

To prove: if $p \neq p_1, \dots, p_k$, then $\sqrt{p} \notin \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})$.

Proof: if $\sqrt{p} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})$, then $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ has degree 2, and corresponds to a subgroup of $\mathbb{Z}_2^k$ of index 2:

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k}) \arrow[d, dash] \arrow[dd, dash, bend left, "2^k"] \\
\mathbb{Q}(\sqrt{p}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

there are 2^{k-1} subgroups of index 2, corresponding to all quadratic extensions of $\mathbb{Q}$ in $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})$.

So $\sqrt{p} \in \mathbb{Q}(\sqrt{p_{i_1} \cdots p_{i_j}})$ for some $i_1, \dots, i_j$.

but then $p = p_{i_1} \cdots p_{i_j}$, contradiction. $\square$