Thm $\alpha \in \mathbb{C}$ iff $\exists\, \mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n \subseteq \mathbb{C}$ s.t. $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ for $1 \le i \le n$.

Pf ($\Leftarrow$) Have $F_i = F_{i-1}(\sqrt{\alpha_i})$ for some $\alpha_i \in F_{i-1}$. $F_0 = \mathbb{Q} \subseteq \mathbb{C}$. Suppose $F_{i-1} \subseteq \mathbb{C}$. Then $\alpha_i \in \mathbb{C} \Rightarrow \sqrt{\alpha_i} \in \mathbb{C}$ so $F_i \subseteq \mathbb{C}$. ✓

($\Rightarrow$) We show $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ s.t. F_n contains $\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)$ and $[F_i : F_{i-1}] = 2$. Then $\alpha \in F_n(i)$, so done.

Proceed by induction on N, number of times P1, P2, P3 used in construction of α. For $N = 0$, $\alpha = 0$ or 1 so $F_n = F_0 = \mathbb{Q}$. Now suppose α constructed in $N > 1$ steps, where the last step uses P1, intersection of distinct lines ℓ_1, ℓ_2. Then ℓ_1 constructed from α_1, β_1 by C1, ℓ_2 from α_2, β_2 by C1. By ind hypothesis, $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ with $[F_i : F_{i-1}] = 2$ and $F_n \ni$ Re, Im of $\alpha_1, \beta_1, \alpha_2, \beta_2$. Use linear algebra, line intersection formula, to show $\mathrm{Re}(\alpha), \mathrm{Im}(\alpha) \in F_n$.

Next suppose last step in construction of α uses P2, intersection of line ℓ, circle C. Then ℓ built from $\alpha_1 \neq \beta_1$, C1 and C built from $\alpha_2 \neq \beta_2$ and γ_2, all coming from earlier stages of construction. Thus $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ with $[F_i : F_{i-1}] = 2$ and F_n containing Re, Im of $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_2$. Line/circle intersection is a quadratic cond'n and get $\alpha \in F_n$ or quad extn of F_n.

Re, Im ( )

Sim for two circle intersections (P3) constructing α. □

Cor $\mathbb{C}$ is the smallest subfield of $\mathbb{C}$ that is closed under the operation of taking square roots.

Pf Already showed $\alpha \in \mathbb{C} \Rightarrow \sqrt{\alpha} \in \mathbb{C}$. Take $F \subseteq \mathbb{C}$ closed under $\sqrt{\ }$ and take $\alpha \in \mathbb{C}$. Then $\exists\, \mathbb{Q} = F_0 \subseteq_2 F_1 \subseteq_2 \cdots \subseteq_2 F_n \subseteq \mathbb{C}$ $\alpha \in F_n$

Same induction as before with F in place of $\mathbb{C}$ shows $F_n \subseteq F$ ✓

Cor If $\alpha \in \mathbb{C}$, then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^m$ for some $m \in \mathbb{N}$. Thus all $\alpha \in \mathbb{C}$ are alg/$\mathbb{Q}$ with minimal poly/$\mathbb{Q}$ of degree 2^m.

e.g. You can't trisect a 120° angle b/c $\zeta_9 \notin \mathbb{C}$. (HW)

e.g. Given a cube with volume 1, can we construct one with volume 2 ("duplication of the cube")?

Requires construction of $\sqrt[3]{2}$, but $\sqrt[3]{2}$ has min'l polynomial x^3-2 over $\mathbb{Q}$, so is not in $\mathbb{C}$.

e.g. Given a radius 1 circle, can we construct a square of same area ("squaring the circle")?

Requires $\sqrt{\pi} \in \mathbb{C} \Rightarrow (\sqrt{\pi})^2 = \pi \in \mathbb{C} \Rightarrow \pi$ alg/$\mathbb{Q}$ $\mathbb{Q}$.

Thm Let $\alpha \in \mathbb{C}$ be alg/$\mathbb{Q}$ and let L be the splitting field of $m_{\alpha,\mathbb{Q}}$. Then α is constructible iff $[L:\mathbb{Q}]$ is a power of 2.

Note $L \neq \mathbb{Q}(\alpha)$ in general!

Pf Reading ☐

Regular polygons and roots of unity:

Defn An odd prime p is a Fermat prime if $p = 2^{2^m}+1$ for some $m \geq 0$.

Thm Let $n > 2$ be an integer. Then a regular n-gon can be constructed by straightedge & compass (i.e. $\zeta_n \in \mathbb{C}$) iff $n = 2^s p_1 \cdots p_r$ where $s \geq 0$ is an integer and $p_1, \ldots, p_r$ are distinct Fermat primes. ($r > 0$).

Pf We have $\zeta_n \in \mathbb{C}$ iff $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ is a power of 2, and $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$, so $\zeta_n \in \mathbb{C}$ iff $\phi(n)$ is a power of 2.

Suppose $n = 2^s p_1 \cdots p_r$, p_i Fermat primes. Then

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \begin{cases} 2^{s-1}(p_1 - 1)\cdots(p_r - 1) & \text{if } s > 0 \\ (p_1 - 1)\cdots(p_r - 1) & s = 0 \end{cases}.$$

This is a power of 2 since each p_i is a Fermat prime.

Now suppose $\phi(n)$ is a power of 2 and $n = q_1^{a_1} \cdots q_s^{a_s}$ prime fact'n.

Then $\phi(n) = q_1^{a_1 - 1}(q_1 - 1) \cdots q_s^{a_s - 1}(q_s - 1)$

If q_i is odd, then $a_i = 1$ since $\phi(n)$ is a power of 2, and also $q_i - 1$ is a power of 2.

But if $q = 2^k + 1$ is prime, then k is a power of 2 (HW).

So the odd q_i are Fermat primes and have $a_i = 1$. □

Note $F_n = 2^{2^n} + 1$ is prime for $n = 0, \ldots, 4$, composite for $5 \le n \le 32$, unknown in gen'l.

n	F_n
0	3
1	5
2	17
3	257
4	65537