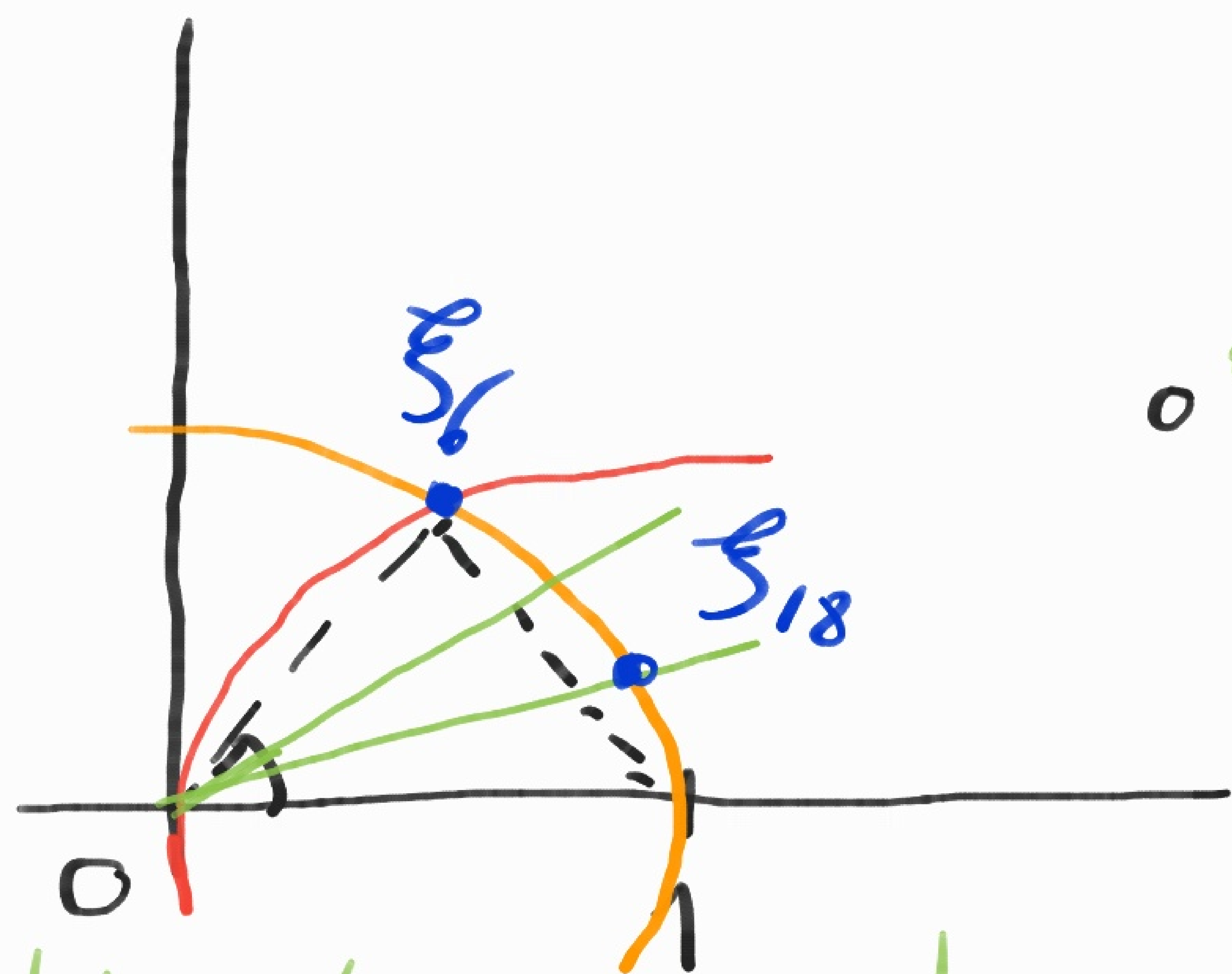
Cor. Si $\alpha \in \mathbb{C}$ es construible, entonces α es algebraico sobre $\mathbb{Q}$ y $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ es una potencia de 2.

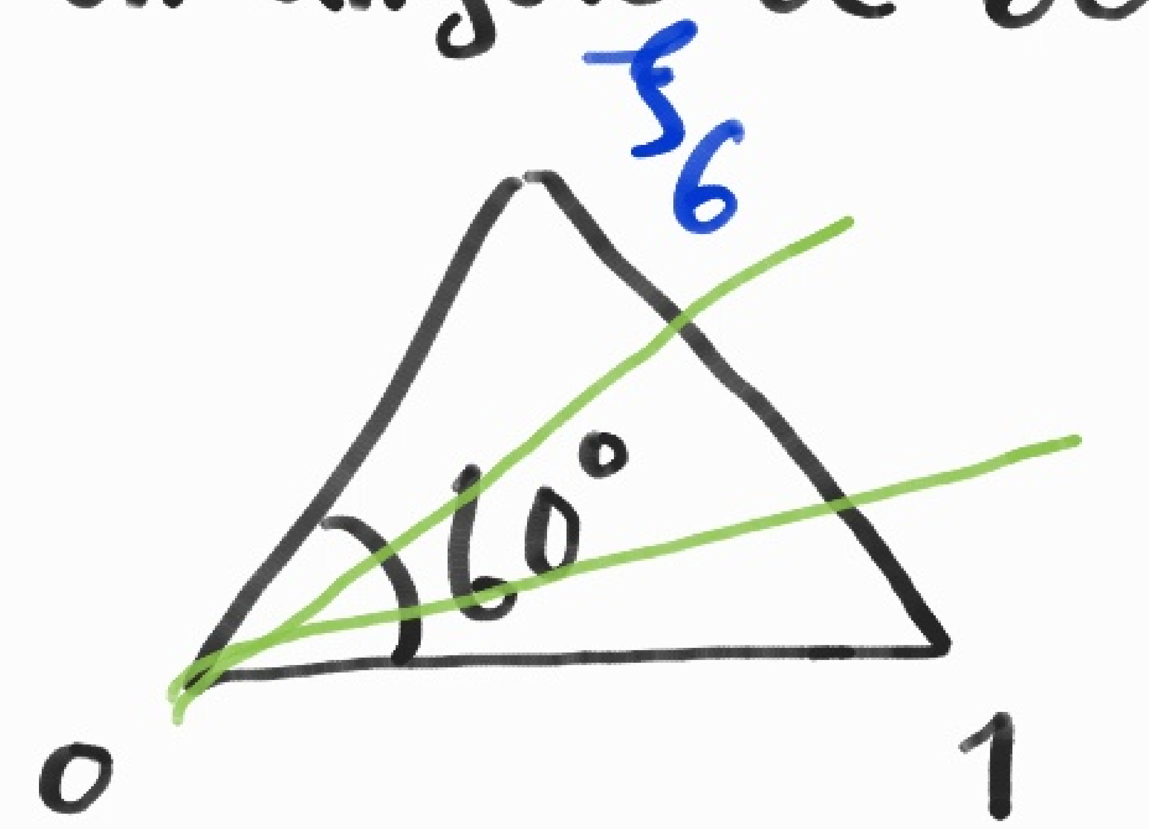
Cor. Usando regla y compas no se puede cuadrar el circulo.

Si fuera posible cuadrar un circulo de radio 1, como el area de este circulo es π, entonces tendriamos un cuadrado de lado $\sqrt{\pi}$. Esto implica el numero real $\sqrt{\pi}$ es construible y por lo tanto $(\sqrt{\pi})^2 = \pi$ es construible $\triangledown$

ya que esto implicaría que π es algebraico. (π es trasendente es un teorema de Lindemann)

Cor. Usando regla y compas no se puede trisecar un angulo de $60°$.





$$\xi_6 = e^{\frac{2\pi i}{6}}$$

Si fuera posible trisecar el angulo de $60°$, entonces ξ_{18} seria construible. Pero

$[\mathbb{Q}[\xi_{18}]:\mathbb{Q}] = \varphi(18) = 6$ que no es una potencia de 2 ¡$\triangledown$!

Cor. Usando regla y compas no se puede duplicar un cubo.

Dem:

Consideremos el cubo unitario es decir, un cubo de lado 1

Supongamos que podemos duplicar este cubo. Entonces la longitud del lado de este nuevo cubo debe de ser $\sqrt[3]{2}$. Por lo tanto el número real $\sqrt[3]{2}$ es construible.

pero sabemos que el polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, es X^3-2. Lo que implica que $[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]=3$ que no es una potencia de 2 ∇

¿Cuándo es posible construir un n-ágono regular con regla y compas?

Si queremos construir un n-agono tenemos que poder construir ξ_n una raiz n-ésima primitiva de la unidad. Por otro lado $n = 2^\ell m$ con m impar. Como $\mathrm{mcd}(2^\ell, m) = 1$, ξ_n se puede obtener a partir de ξ_{2^ℓ} y ξ_m. Notemos que ξ_{2^ℓ} siempre es construible para cualquier ℓ. Así que la pregunta de arriba nos interesa para n impar. Los antiguos griegos solo tenian una respuesta afirmativa para 3, 5 y 15.

Def: Un número primo p es de Fermat si $p = 2^a + 1$ para algun $a \geq 1$.

Por ejemplo, los valores $a = 1, 2, 4, 8$ y 16 dan los primos de Fermat $3, 5, 17, 257$ y $65,537$.

Lema: Si 2^a+1 es primo con $a \geq 1$, entonces $a = 2^n$ p.a. n

Esto sugiere que el siguiente primo de Fermat es $2^{32}+1$. Pero $2^{32}+1$ no es primo ya que es divisible por 641.

Teorema (Gauss). Sea $n \geq 3$. Entonces es posible construir un n-ágono regular con regla y compas exactamente cuando $\varphi(n)$ es una potencia de 2. Esto pasa si y solo si $n = 2^e p_1 \cdots p_r$ donde $e \geq 0$ y los p_i's son primos de Fermat distintos.

Dem:

Como las n-esimas raices de la unidad

forman los vertices de un n-agono regular inscrito en un circulo de radio 1, entonces el n-agono regular es construible con regla y compas si y solo si ζ_n es construible si y solo si $[\mathbb{Q}[\zeta_n]:\mathbb{Q}] = \underline{\varphi(n)}$ es una potencia de 2.

Escribimos $n = q_1^{e_1} \cdots q_k^{e_k}$ con q_i primos y $e_i \geq 1$. Entonces $\varphi(n)$ es el producto de $\varphi(q_i^{e_i})$ $\forall\, 1 \leq i \leq k$. Así que $\varphi(n)$ es una potencia de 2 si y solo si $\varphi(q_i^{e_i})$ es una potencia de 2 para cada $1 \leq i \leq k$.

¿Para qué exponentes e, $\varphi(p^e)$ es una potencia de 2 con p primo?

Si p es primo, $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

Se sigue que $\varphi(2^e)$ siempre es

una potencia de 2.

Para un primo impar p, $\varphi(p^e)$ es una potencia de 2 si y solo si $e=1$ y p es un primo de Fermat.

Por el Teorema de Gauss es posible construir un n-agono regular con regla y compas para $n=3,5,17$ pero no para cualquier numero intermedio.