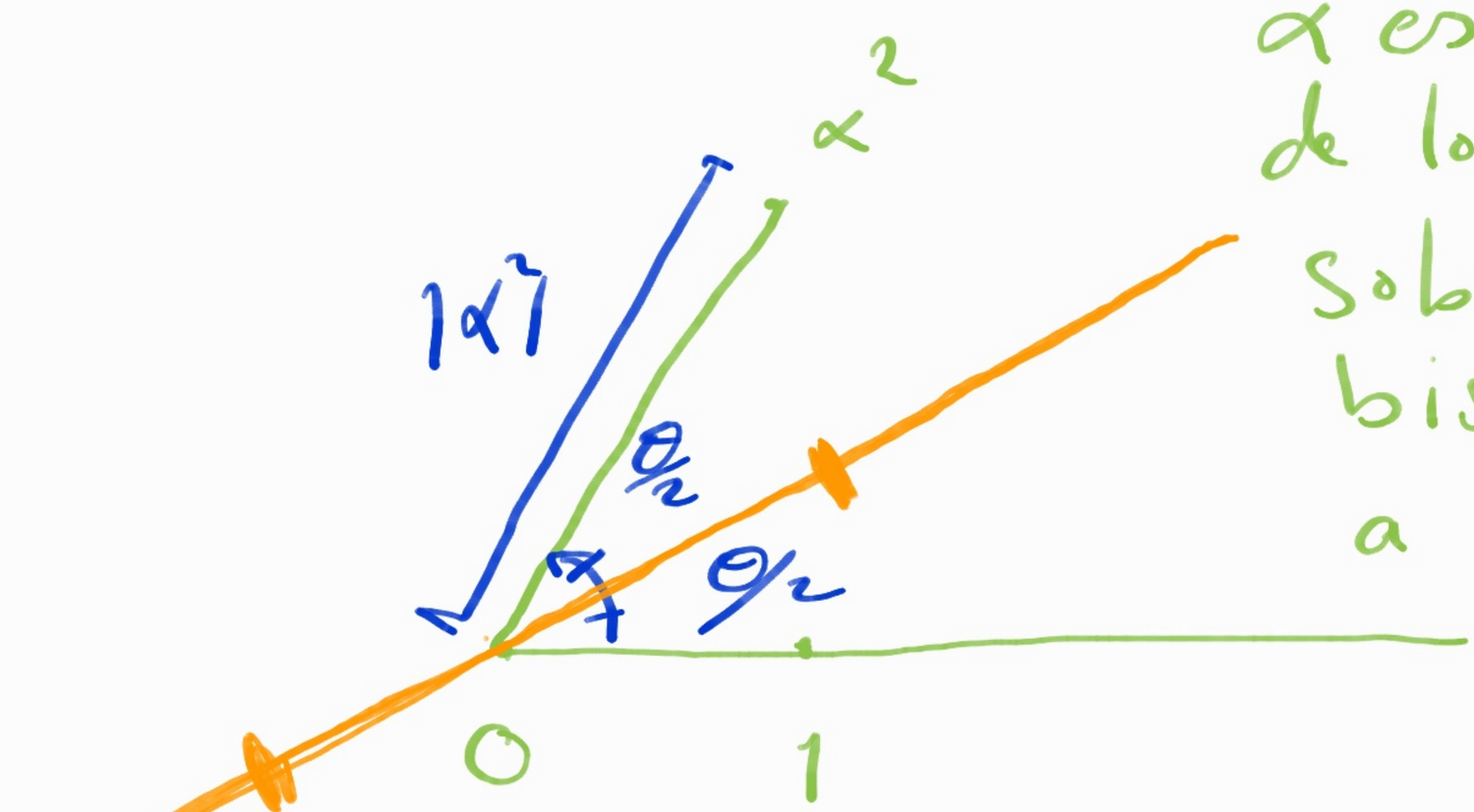
Sea $\alpha \in \mathbb{C}$ con $\alpha^2 \in K$. Entonces $\alpha \in K$.




$\alpha$ es cualquiera de los dos putos sobre la bisectriz de $\theta$ a distancia $\sqrt{|\alpha^2|}$

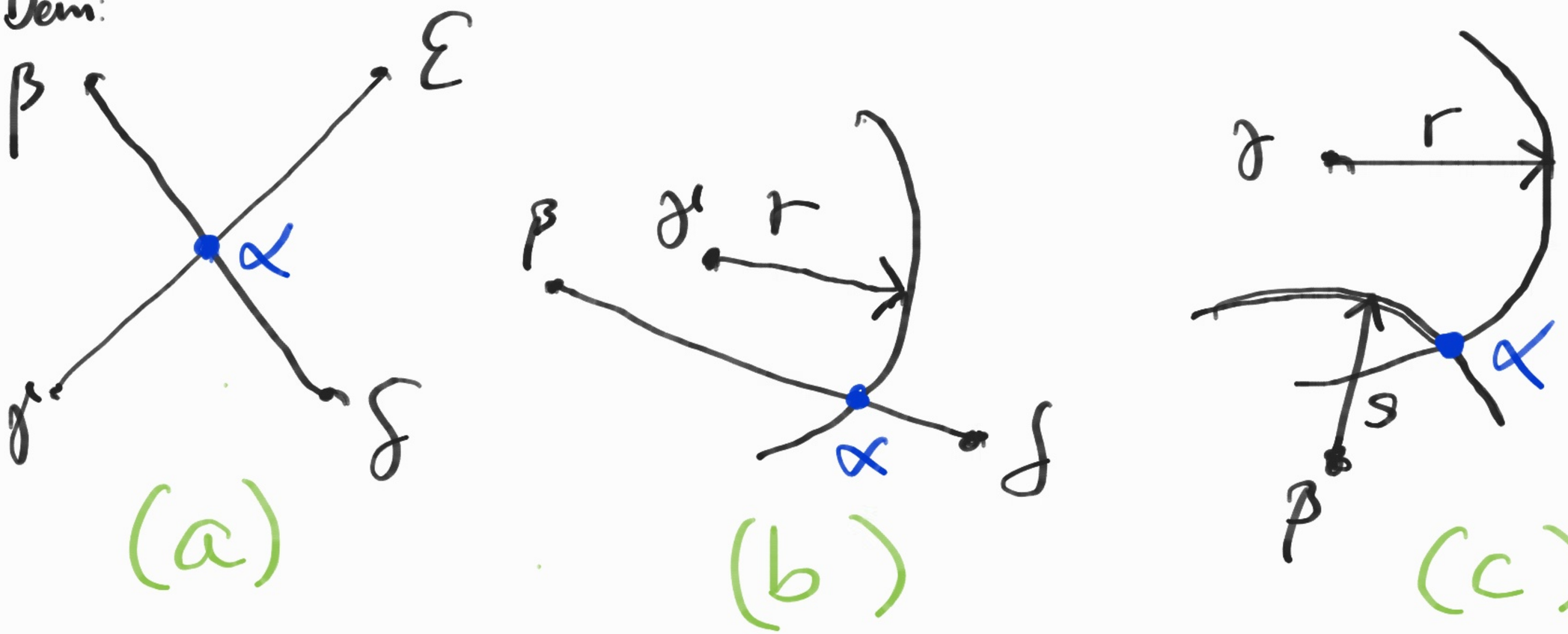
$$\alpha = r(\cos\varphi + i\,\mathrm{sen}\,\varphi) \qquad r = \sqrt{r^2}$$

$$\alpha^2 = r^2(\cos 2\varphi + i\,\mathrm{sen}\,2\varphi) \qquad \varphi = \frac{\theta}{2}$$

$\theta$ $\qquad$ $\theta$

Lema Sea $E \supseteq \mathbb{Q}$ cerrado bajo conjugación compleja y sea $\alpha \in \mathbb{C}$ construible en un paso a partir de los puntos de $E$. Entonces $[E[\alpha] : E] \leq 2$.

Dem:




Si tomamos la distancia entre dos puntos de $E$, digamos $\alpha$ y $\beta$, está distanticia está dada por $r = |\alpha - \beta|$. Entonces $r^2 = (\alpha - \beta)\overline{(\alpha - \beta)}$. Como $E$ es cerrado bajo conjugacion compleja, entonces $r^2 \in E$.

En los diagramas (a), (b) y (c), tenemos que $\beta, \gamma, \delta, \varepsilon$ y $r^2, s^2$ son elementos de $E$.

El hecho de que $\alpha$ esté sobre la linea determinada por $\beta$ y $\delta$, implica que $\frac{\alpha-\beta}{\delta-\beta} \in \mathbb{R}$. Así

$$\overline{\alpha} = \overline{\beta} + \frac{\alpha-\beta}{\delta-\beta}(\overline{\delta}-\overline{\beta})$$

Lo mismo podemos hacer por $\gamma$ y $\varepsilon$ Así

$$\overline{\beta} + \frac{\alpha-\beta}{\delta-\beta}(\overline{\delta}-\overline{\beta}) = \overline{\gamma} + \frac{\alpha-\gamma}{\varepsilon-\gamma}(\overline{\varepsilon}-\overline{\gamma})$$

Si esta expresión, no una identidad para todos los valores posibles de $\alpha$

entonces despejamos $\alpha$. los que nos dice $\alpha \in E$
Si la expresion es una identidad para toda $\alpha$
ponemos $\alpha = \beta$, y así

$\overline{\beta} = \bar{\gamma} + \frac{\beta - \gamma}{\varepsilon - \gamma}(\bar{\varepsilon} - \bar{\gamma})$ esto forza a $\beta$ a estar en la linea $\overline{\gamma\varepsilon}$ y $\alpha = \beta \in E$ $\therefore [E[\alpha]:E] = 1$.

Del hecho de que $\alpha$ está a distancia $r$ de $\gamma$ (casos (b) y (c)) se puede escribir como $(\alpha - \gamma)\overline{(\alpha - \gamma)} = r^2$ y esto da

$$\overline{\alpha} = \overline{\gamma} + \frac{r^2}{\alpha - \gamma}$$

Para el caso (b), esta expresión la podemos igualar con la expresión primera de $\bar{z}$. Multiplicando por $\alpha - \gamma$, obtenemos

$$(\alpha-\gamma)\left[\bar{\beta}+\frac{\alpha-\beta}{\delta-\beta}(\bar{\delta}-\bar{\beta})\right]=\bar{\gamma}(\alpha-\gamma)+r^2$$

que es una expresión cuadratica en $\alpha$ con coeficientes en $E$. Esta igualdad no es una identidad ya que al sustituir $\gamma$ en $\alpha$ queda $0=r^2\nabla$

Esto me dice que $[E[\alpha]:E]\leq 2$ °

Finalmente, en el caso (c), $\alpha$ está a distancia $s$ de $\beta$. Podemos obtener una expresión como la anterior para $\mathcal{L}$ i.e., $\overline{\alpha} = \overline{\beta} + \dfrac{s^2}{\alpha - \beta}$

Multiplicando por $(\alpha-\gamma)(\alpha-\beta)$ obtenemos

$$\overline{\gamma}(\alpha-\gamma)(\alpha-\beta) + r^2(\alpha-\beta) = \overline{\beta}(\alpha-\gamma)(\alpha-\beta) + s^2(\alpha-\gamma)$$

que no es una identidad ya que al poner $\gamma$ en vez de $\alpha$, nos da que $\beta = \gamma$ ↯

Así que $\alpha$ satisface una expresión cuadrática con coeficientes en $E$ ∴ $[E[\alpha]:E] \leq 2$.

Teorema: Sea $\alpha \in \mathbb{C}$. Las siguientes condiciones son equivalentes:

(i) $\alpha$ es construible.

(ii) $\alpha$ está en un subcampo de $\mathbb{C}$ que es normal y de grado una potencia de 2 so sobre $\mathbb{Q}$.

(iii) Existen campos $E_i \subseteq \mathbb{C}$ con:

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r$$

tales que $\alpha \in E_r$ y $[E_i : E_{i-1}] = 2$ para $1 \leq i \leq r$.

Dem:

Sea $\alpha \in K$, el campo de numeros construibles. Entonces $\alpha$ puede ser construido en un número finito $m$ de pasos a partir de $0, 1 \in K$ (que están dados). Por inducción sobre $m$ probaremos que existe una extensión normal $L \supseteq \mathbb{Q}$ en $\mathbb{C}$ de grado una potencia de 2 y tal que $\alpha$ y todos los puntos intermedios usados

en la construcción de $\alpha$, están en $L$.

Si $m=0$, entonces $\alpha \in \mathbb{Q}$ ✓

Sup. $m>0$ y por hipotesis de inducción hay una extension normal $E \supseteq \mathbb{Q}$ de gra
grado una potencia de 2 y que contiene a todos los puntos usados en la
construcción de $\alpha$. Como $E$ es normal, $E$ es cerrada
bajo conjugacion compleja y así aplica el
lema anterior. Por lo tanto $[E[\alpha]:E] \leq 2$.
Podemos asumir que $[E[\alpha]:E]=2$ y si no
tomamos $L=E$.

Sea $f = \min_E(\alpha)$ y denotemos $g$ al producto de las distintas imagenes de $f$ bajo $Gal(E/\mathbb{Q})$. Sea $L$ el campo de descomposición de $g$ sobre $E$ en $\mathbb{C}$.

Si $\beta$ es cualquier raiz de $g$ en $L$, entonces $gr(\min_E(\beta)) = 2$

Así al adjuntar $\beta$ a $E$, obtenemos una extension de grado 2. Como $L$ se obtiene al ir adjuntando las distintas raices de $g$ tenemos que $[L:E]$ es de grado una potencia de 2.

Para ver que $L$ es normal sobre $\mathbb{Q}$, notemos que $E \supseteq \mathbb{Q}$ es de Galois y que $g$ es invariante bajo $Gal(E/\mathbb{Q})$, así que $g(x) \in \mathbb{Q}[x]$. También $E$ es el campo de descomposición de un polinomio $h(x) \in \mathbb{Q}[x]$. Se sigue que $L$ es el campo de descomposición de $gh \in \mathbb{Q}[x]$. Lo que implica que $L$ es normal sobre $\mathbb{Q}$. Por lo tanto tenemos (ii).

Ahora supongamos (ii). Entonces tenemos una extension normal $E \supseteq \mathbb{Q}$ de grado una potencia de 2 y con $\alpha \in E$. Como $E \supseteq \mathbb{Q}$ es de Galois el orden de $Gal(E/\mathbb{Q})$ es una potencia de 2 es decir, $Gal(E/\mathbb{Q})$ es un 2-grupo. Entonces existe una cadena de subgrupos

$$\{e\} \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_r = Gal(E/\mathbb{Q})$$

con $[G_i : G_{i-1}] = 2$.

Por el TFG, los campos fijos de estos subgrupos dan una torre $\mathbb{Q} = E_0 \subseteq \dots \subseteq E_r = E$

con $[F_i : F_{i-1}] = 2$.

(iii)⇒(i). Tenemos la cadena de campos $\mathbb{Q} = E_0 \subseteq \cdots \subseteq E_r$ con $\alpha \in E_r$ y $[E_i : E_{i-1}] = 2$. Por inducción sobre r, mostraremos que $E_r \subseteq K$. Sabemos que $E_0 = \mathbb{Q} \subseteq K$ y esto es la base de inducción. Es suficiente mostrar que si $U \subseteq V \subseteq \mathbb{C}$ campos con $U \subseteq K$ y $[V:U] = 2$ entonces $V \subseteq K$. Tenemos $V = U[\gamma]$ con $\gamma$ raiz de un polinomio cuadratico con coeficientes en $U$, digamos $f(x) = ax^2 + bx + c$

Ent $\gamma = \dfrac{-b + \sqrt{b^2 - 4ac}}{2}$. Así $\delta = 2\gamma + b = \sqrt{b^2 - 4ac}$

Entonces $V = U[\delta]$ con $\delta^2 \in U \subseteq K$

Por un lema anterior, $\delta \in K$. Por lo tanto $V \subseteq K$.

Así que si $E_{r-1} \subseteq K$, como $[E_r : E_{r-1}] = 2$, se tiene que $\alpha \in E_r \subseteq K$.