ALGEBRA III (Doble grado Informática-Matemáticas)

6. Construcciones con Regla y Compás

En esta sección vamos a abordar diversos problemas clásicos de matemática griega.

6.1. Planteamiento del problema.

Sea Π un plano Euclídeo dado (nuestro folio). Una **regla** es una herramienta nos permite trazar la linea recta que pasa por dos puntos dados del plano y un **compás** es una herramienta que nos permite trazar la circunferencia de centro un punto dado y de radio el segmento de extremos otros dos puntos dados.

Si $S = \{P_0, \ldots, P_n\} \leq \Pi$ es un conjunto finito de puntos del plano, se nos define una sucesión de subconjuntos

$$S = C_1(S) \subseteq C_2(S) \subseteq \cdots \subseteq C_m(S) \subseteq \cdots$$

donde $C_1(S) = S$ y, recursivamente, $C_{m+1}(S)$ es la unión de $C_m(S)$ y el conjunto de todos los puntos tales que

(1) son intersecciones de rectas que pasan por dos puntos de $C_m(S)$,
(2) son intersecciones de rectas que pasan por puntos de $C_m(S)$ con circunferencias de centro un punto de $C_m(S)$ y radio el segmento con extremos dos puntos de $C_m(S)$,
(3) son intersecciones de dos circunferencias cuyos centros son puntos de $C_m(S)$ y radios segmentos con extremos puntos de $C_m(S)$.

Definimos entonces el conjunto

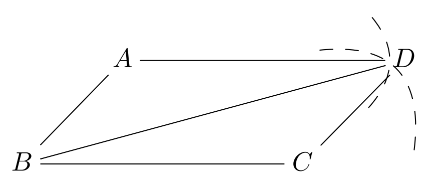
$$C(S) = \bigcup_{m \geq 1} C_m(S) \ ,$$

al que nos referimos como **el conjunto de puntos construibles (con regla y compás) desde los puntos** $S = \{P_0, \ldots, P_n\}$.

Los llamados *problemas clásicos de construcciones con regla y compás* son aquellos que se traducen en conocer si un determinado punto P es construible desde un conjunto dado de puntos $\{P_0, \ldots, P_n\}$, esto es, saber si $P \in \mathbb{C}(P_0, \ldots, P_n)$.

Ejemplo 1. *Dados tres puntos A, B, C, no alineados, ¿es construible el punto D, de tal manera los que A, B, C y D son los vértices de un paralelogramo uno de cuyos lados es el segmento de vértices A y B y el otro el de vértices B y C?*

Solución: En efecto, podemos construir el punto D como el punto de intersección de la circunferencia de centro A y radio el segmento de extremos B y C con la circunferencia de centro C y radio el segmento de extremos A y B.

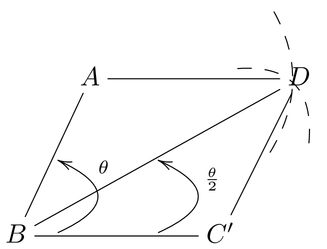


Observemos que la anterior simple construcción nos permite dar respuesta positiva a los siguientes dos problemas

Ejemplo 2. *Dados tres puntos distintos A, B, C, no alineados, ¿es construible un punto D tal que la recta que pasa por A y D es paralela a la que pasa por los puntos B y C?*

Ejemplo 3 (Bisección de ángulos)**.** *Dados tres puntos A, B, C, no alineados, ¿es construible un punto D tal que la recta que pasa por A y D es la bisectriz del ángulo $\widehat{ABC}$?*

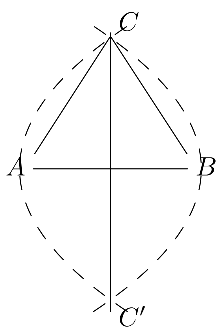
Solución: Construimos primero el punto C' intersección de la recta que pasa por B y C con la circunferencia centrada en B y de radio el segmento que une B con A, de manera que el segmento que une B con C' es de igual distancia que el que une B con A. Construimos entonces, como antes el vértice D del paralelogramo, que nos resulta un rombo, que resuelve el problema:



Otros ejemplos elementales de respuesta positiva son los siguientes

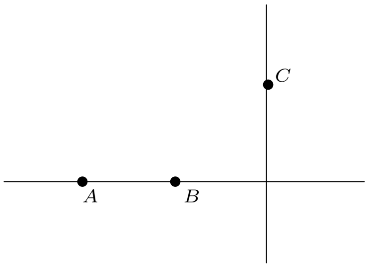
Ejemplo 4. *Dados dos puntos A, B, ¿Es posible construir un punto C tal que el triángulo de vertices A, B y C sea equilátero?, ¿Es posible construir puntos C y C' tal que la recta que pasa por ellos es la mediatriz del segmento de extremos A y B?, ¿es posible construir el punto medio del segmento AB?*

Solución: Para el primer problema encontramos dos soluciones, C y C', que son las intersecciones de las circunferencias de radio el segmento de extremos A y B y cuyos centros respectivos son estos mismos puntos.



Combinando las anteriores es claro que podemos dar respuesta positiva al siguiente problema

Ejemplo 5. *Dados tres puntos no alineados A, B, C ¿es construible un punto D tal que la recta que pasa por C y D es perpendicular a la que pasa por A y B?*

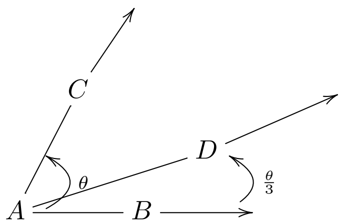


Otro ejemplo sería este

Ejemplo 6. *Dados dos puntos A y B, ¿podemos construir los vértices C y D del cuadrado del que el segmento que une A y B es uno de los lados?*

Otros problemas tienen dificultades, por ejemplo

Ejemplo 7 (Trisección de ángulos)**.** *Consideremos el problema de trisecar un ángulo θ. Aquí tenemos tres puntos, el vértice A y dos puntos B y C de forma que las rectas que determinan con A forman un ángulo θ, entonces ¿es posible construir un punto D tal que la rectas que pasan por A y B y por A yD respectivamente formen el ángulo $\theta/3$?*



Ejemplo 8 (Cuadratura del círculo)**.** *Dados dos puntos A y B ¿es posible construir puntos A' y B' tal que el cuadrado de lado el segmento de extremos A' y B' tenga igual area que el círculo de centro A y radio el segmento de extremos A y B?*

Ejemplo 9 (Duplicación de cubo)**.** *Dados dos puntos A y B ¿es posible construir puntos A' y B' tal que el cubo de lado el segmento de extremos A' y B' tenga doble volumen que el cubo de lado el segmento de extremos A y B?.*

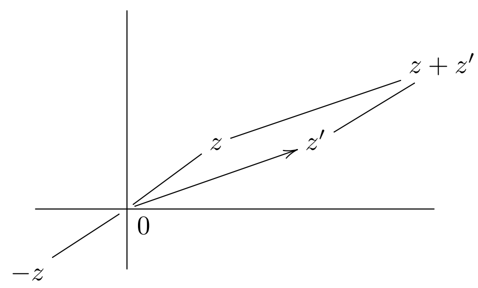
6.2. Algebraización del problema.

A continuación, en orden a algebraizar el problema, vamos a manejar coordenadas cartesianas para los puntos del plano. Notemos que, dado el conjunto de puntos datos $S = \{P_0, P_1, \ldots, P_n\} \subset \Pi$, es evidente que si $S = \emptyset$ entonces $C(S) = \emptyset$, y si $S = \{P_0\}$, entonces $C(S) = S = \{P_0\}$. Por tanto, para que haya un problema de construcción con regla y compás significativo el conjunto de puntos datos tendrá al menos dos puntos, P_0 y P_1, que nosotros utilizaremos para introducir coordenadas cartesianas: tomaremos P_0 como centro del sistema de ejes cartesianos, por tanto $P_0 = O = (0, 0)$; la recta $\overline{P_0P_1}$ como uno de los ejes, digamos el *eje de abscisas (las $x's$)*, y su perpendicular que pasa por P_0 (que podemos construir) como el otro eje, el *eje de las ordenadas (las $y's$)*; finalmente, tomaremos la distancia $|P_0P_1|$ como unidad de medida, así que será $P_1 = (1, 0)$.

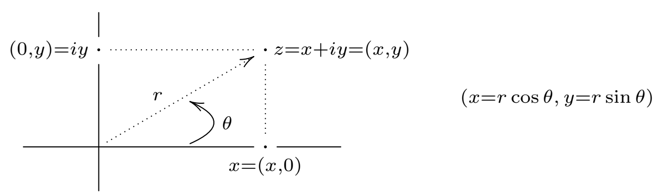
Vamos también a pensar en los puntos del plano como representación geométrica de los números complejos, así que vamos a asociar cada punto P del plano de coordenadas cartesianas (x, y) con el número complejo $z = x + iy$ y, de esta forma, identificamos los puntos del plano con los números complejos. El conjunto de puntos dados $S = \{P_0, \ldots, P_n\}$ lo tendremos identificado con el correspondiente conjunto de complejos $S = \{z_0, \ldots, z_n\}$, donde $z_0 = 0$ y $z_1 = 1$, y el conjunto $C(S) = C(P_0, \ldots, P_n)$ de puntos construibles con un correspondiente conjunto de números complejos, que denotaremos $C(S) = C(z_0, z_1, \ldots, z_n)$ y al que nos referiremos como **el conjunto de números complejos construibles (con regla y compás) desde** $z_0, \ldots, z_n$. De manera que el punto $(x, y) \in \Pi$ es construible desde $P_0, \ldots, P_n$ si y solo si el complejo $x + iy$ es construible desde $z_0, \ldots, z_n$. Queremos ahora probar la siguiente caracterización de $C(S) = C(z_0, z_1, \ldots, z_n)$:

Teorema 10. * *$C(S)$ es el menor subcuerpo de $\mathbb{C}$ conteniendo a $z_0, z_1, \ldots, z_n$ y cerrado para raíces cuadradas y conjugación.*

Demostración: Vemos primero que $C(S)$ es un subcuerpo de $\mathbb{C}$ cerrado para raíces cuadradas y conjugación. Supongamos que $z = x + iy$ y $z' = x' + iy' \in C(S)$. Entonces $z + z' = (x + x') + i(y + y')$ puede ser construido por el ya mencionado método del paralelogramo



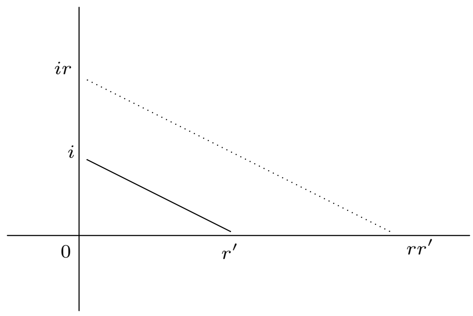
También es claro que $-z = -x + i(-y)$ es construible (es el otro punto de intersección de la recta que pasa por 0 y z con la circunferencia de centro 0 y radio $|z|$ = longitud del segmento de extremos 0 y z. De esta manera concluimos que $C(z_0, z_1, \ldots, z_n)$ es un subgrupo del grupo aditivo del cuerpo $\mathbb{C}$ de los números complejos. Para ver que $C(S)$ es cerrado para multiplicación, inversos, y raíces cuadradas es cómodo usar la expresión de los complejos en su forma polar $z = re^{i\theta}$, donde, si $z = x + iy$, entonces $r = |z| = \sqrt{x^2 + y^2}$ es la longitud del segmento de extremos 0 y z, $\theta \in \mathbb{R}$ es la amplitud en radianes del ángulo desde el eje de abscisas a la recta que pasa por 0 y z, y $e^{i\theta} = \cos\theta + i \sin\theta$.



y es fácil ver que z es construible si y solo si r y $e^{i\theta}$ son construibles: Si z lo es, entonces r es la intersección de la circunferencia de centro el origen de coordenadas 0 y radio $r = |z|$ con el semieje positivo de abscisas y $e^{i\theta}$ la intersección de la circunferencia centrada en el origen y radio 1 con la semirecta que pasa por 0 y z. Si r y $e^{i\theta}$ son construibles, entonces

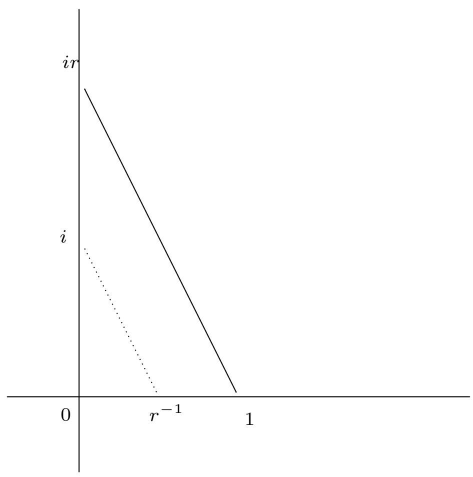
z es la intersección de la semirecta que pasa por 0 y $e^{i\theta}$ con la circunferencia de centro 0 y radio r.

Si $z = re^{i\theta}$ y $z' = r'e^{i\theta'}$ son construibles, entonces $zz' = rr'e^{i(\theta+\theta')}$ tiene valor absoluto rr' igual al producto de los valores absolutos de z y z', y su amplitud es la suma de las dos amplitudes dadas. La construcción de rr' es indicada en la figura



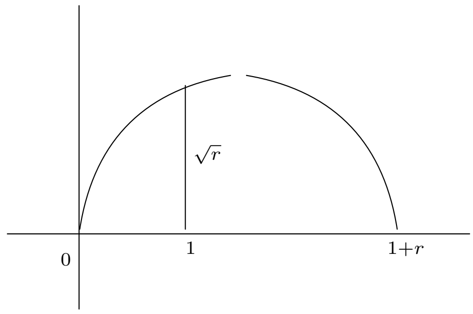
Aquí, la recta que pasa por ir y rr' es paralela a la recta que pasa por i y r' (Usar el Teorema de Thales). Por otra parte, la construcción de $e^{i(\theta+\theta')}$ es fácil: es el nuevo punto de intersección de la circunferencia de centro 0 y radio 1 con la circunferencia de centro $e^{i\theta}$ y radio el segmento que lo une con $e^{i\theta'}$.

Si $z \neq 0$, entonces $z^{-1} = \frac{1}{r}e^{-i\theta}$. La construcción de $\frac{1}{r}$ es indicada en la figura



y $e^{-i\theta}$ lo construimos como el nuevo punto de intersección de la circunferencia de centro 0 y radio 1 con la circunferencia de centro 1 y radio el segmento que une 1 con $e^{i\theta}$. Puesto que el conjugado es $\bar{z} = re^{-i\theta}$, es claro ya que este es construible. Por otro lado, $\sqrt{z} = \sqrt{r}e^{i\theta/2}$. Ya conocemos como bisecar ángulos, por tanto como construir $e^{i\theta/2}$. La construcción de $\sqrt{r}$

es indicada en la siguiente figura



donde el punto $(1, \sqrt{r})$ es obtenido intersectando la circunferencia centrada en $(\frac{1+r}{2}, 0)$ y radio $\frac{1+r}{2}$ con la recta paralela al eje de ordenadas que pasa por el $(1,0)$. En efecto, si llamamos $(1,x)$ a ese punto, a a la longitud del segmento que une $(0,0)$ con $(1,x)$ y b a la del segmento que une $(1,x)$ con $(1+r,0)$, por el Teorema de Pitágoras, tenemos las igualdades $a^2 = x^2+1$, $b^2 = x^2+r^2$ y $(1+r)^2 = a^2+b^2$. De donde $r^2+2r+1 = 2x^2+r^2+1$ y $x^2 = r$; o sea que $x = \sqrt{r}$.

Supongamos ahora que $F \leq \mathbb{C}$ es cualquier subcuerpo conteniendo a los z_i, $1 \leq i \leq n$, y cerrado bajo raíces cuadradas y conjugación. Si tenemos en cuenta la definición de $C(S)$ como $\bigcup C_m(S)$ vemos que, en orden a probar que $F \supseteq C(z_0, z_1, \ldots, z_n)$, es suficiente probar F es cerrado para las construcciones con regla y compás. Esto es, que la intersección de dos rectas determinadas por complejos de F, o de tal una recta con una circunferencia de centro un complejo de F y radio la distancia entre complejos de F, o de dos tales circunferencias, están todos en F. Notamos primero que el hecho de que F es cerrado para conjugación y contiene a $i = \sqrt{-1}$ implica que si $z = x+iy \in F$, x, y reales, entonces $x, y \in F$ (y recíprocamente). Se sigue de este hecho que la ecuación de cualquier recta que pasa por dos puntos distintos de F tiene la forma $ax+by+c = 0$, donde a, b, c son números reales en F: un punto $x+iy$ pertenece a la recta que pasa por x_0+iy_0 y x_1+iy_1 si y solo si se satisface la ecuación

$$(y_1-y_0)(x-x_0)+(x_0-x_1)(y-y_0) = 0$$

o, equivalentemente,

$$(y_1-y_0)x+(x_0-x_1)y+(y_0-y_1)x_0+(x_1-x_0)y_0 = 0.$$

Similármente, la ecuación de la circunferencia con centro un punto F y radio igual a la longitud de un segmento con extremos puntos de F es de la forma $x^2+y^2+dx+ey+f = 0$ donde d, e, f son números reales en F: un punto $x+iy$ pertenece a la circunferencia de centro x_0+iy_0 y radio la distancia entre x_1+iy_1 y x_2+iy_2 si y solo si se satisface la ecuación

$$(x-x_0)^2+(y-y_0)^2-(x_2-x_1)^2+(y_2-y_1)^2 = 0.$$

Ahora, las coordenadas de un punto $x+iy$ que sea intersección de dos rectas no paralelas $ax+by+c = 0$ y $a'x+b'y+c' = 0$, donde $a, b, c, a', b', c' \in F$, pueden ser determinadas por la regla de Cramer como

$$x = \frac{\begin{vmatrix} -c & b \\ -c' & b' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} = \frac{-cb'+c'b'}{ab'-a'b}, \quad y = \frac{\begin{vmatrix} -c & a \\ -c' & a' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} = \frac{-ca'+ca'}{ab'-a'b},$$

y vemos así que $x + iy \in F$. Las abscisas de los puntos de intersección de los de una recta de ecuación $y = ax + b$ con los de la circunferencia $x^2 + y^2 + dx + ey + f = 0$ se obtienen resolviendo la ecuación de 2º grado $x^2 + (ax + b)^2 + dx + e(ax + b) + f = 0$. Usando la conocida fórmula cuadrática, vemos que las soluciones están en F si a, b, d, e, f están en F. Manejamos similármente el caso de la intersección de una recta $x = c$ con una circunferencia $x^2+y^2+dx+ey+f = 0$. Finalmente, el caso restante se sigue de que los puntos de intersección de dos circunferencia $x^2 + y^2 + dx + ey + f = 0$ y $x^2 + y^2 + d'x + e'y + f' = 0$ son los mismos que los puntos de intersección de los puntos de la circunferencia $x^2 + y^2 + dx + ey + f = 0$ con la recta $(d - d')x + (e - e')x + f - f' = 0$. $\square$

Nota 11. *Observar que $C(S)$ contiene a todos los números complejos $a + bi$ donde a, b son racionales, y que este es un subconjunto denso en $\mathbb{C}$.*

Para el siguiente criterio, digamos que por una **extensión radical cuadrática** de un cuerpo de números $K \leq \mathbb{C}$ se entiende una extensión simple de este cuerpo que es generada por la raíz cuadrada de algún número $a \in K$, esto es, una extensión E/K tal que $E = K(\sqrt{a})$, para algún $a \in K$. Una torre de extensiones de cuerpos numéricos $K_0 \leq K_1 \leq \cdots \leq K_r$ es llamada una tal torre se llama una **torre radical cuadrática** si cada extensión K_{i+1}/K_i es radical cuadrática.

Lema 12. *Si $K = F_0 \leq F_1 \leq \cdots \leq F_r$ es una torre radical cuadrática que comienza en un cuerpo K, entonces existe una otra torre radical cuadrática que también comienza en K, $K = E_0 \leq E_1 \leq \cdots \leq E_s$, tal que $F_r \leq E_s$ y E_s/K es normal.*

Demostración. Procedemos inductivamente en r.

Caso $r = 1$. Tenemos $K \leq F_1$, donde $F_1 = K(\sqrt{a})$, para algún $a \in K$. Pero esta extensión es siempre normal, pues F_1 es el cuerpo de descomposición sobre K del polinomio $x^2 - a$ (sus raíces son $\pm\sqrt{a}$).

Caso $r > 1$. Por hipótesis de inducción, existe una torre radical $K = E_0 \leq E_1 \leq \cdots \leq E_t$, tal que $F_{r-1} \leq E_t$ y E_t/K es normal. Supongamos que su grupo de Galois es $G(E_t/K) = \{\sigma_1 = id, \sigma_2, \ldots, \sigma_m\}$.

Puesto que F_r/F_{r-1} es radical, será $F_r = F_{r-1}(\sqrt{a})$, para algún $a \in F_{r-1}$. Construimos entonces la torre radical cuadrática

$$\begin{aligned} K = E_0 \leq E_1 \leq \cdots \leq E_t \leq E_t(\sqrt{\sigma_1(a)}) \leq E_t(\sqrt{\sigma_1(a)}, \sqrt{\sigma_2(a)}) \leq \cdots \\ \leq \ldots \leq E_t\big(\sqrt{\sigma_1(a)}, \sqrt{\sigma_2(a)}, \ldots, \sqrt{\sigma_n(a)}\big) = E_s\,. \end{aligned}$$

puesto que cada $\sigma_i(a) \in E_t$, es claro que se trata efectivamente de una torre radical cuadrática y, claramente, $F_r \leq E_s$. Bastará por tanto argumentar que E_s/K es normal:

Supongamos que E_t el cuerpo de descomposición sobre K de un polinomio $f \in K[x]$; esto es, $E_t = K(\alpha_1, \ldots, \alpha_k)$ donde $\alpha_1, \ldots, \alpha_k$ son las diferentes raíces de ese f. Consideremos el polinomio $g = \prod_{i=1}^{n} (x^2 - \sigma_i(a)) \in E_t[x]$. Para cualquier $\sigma \in G(E_t/K)$, la lista $\sigma\sigma_1, \ldots, \sigma\sigma_n$ es una permutación de la lista $\sigma_1, \ldots, \sigma_n$, y por consiguiente

$$g^\sigma(x) = \prod_{i=1}^{n}(x^2 - \sigma\sigma_i(a)) = \prod_{i=1}^{n}(x^2 - \sigma_i(a)) = g(x);$$

esto es, los coeficientes de g están en el cuerpo fijo $E_t^{G(E_t/K)} = K$. Así que $g \in K[x]$. El cuerpo de descomposición sobre K del polinomio producto fg es justamente

$$K\big(\alpha_1, \ldots \alpha_k, \sqrt{\sigma_1(a)}, \ldots, \sqrt{\sigma_n(a)}\,\big) = E_t(\sqrt{\sigma_1(a)}, \ldots, \sqrt{\sigma_n(a)}\,) = E_s\,,$$

y concluimos que la extensión E_s/K es normal. □

Teorema 13. *Sea $S = \{z_0 = 0, z_1 = 1, \ldots, z_n\} \subseteq \mathbb{C}$ un conjunto de números. Pongamos*
$$\mathbb{Q}_S = \mathbb{Q}(z_0, z_1, \ldots, z_n, \overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1).$$
Entonces, un complejo $z \in C(S)$ si y solo si existe una torre radical cuadrática
$$\mathbb{Q}_S = K_0 \leq K_1 \leq \cdots \leq K_r$$
tal que $z \in K_r$.

Demostración. Si $\mathbb{Q}_S = K_0 \leq K_1 \leq \cdots \leq K_r$ es una torre radical cuadrática, vemos, por inducción, que $K_r \leq C(S)$: Puesto que $C(S)$ es cerrado para conjugación y cada $z_i \in C(S)$, también cada $\bar{z}_i \in C(S)$, y resulta claro que $K_0 = \mathbb{Q}_S \leq C(S)$. Supongamos demostrado que que $K_{r-1} \leq C(S)$. Como $K_r = K_{r-1}(\sqrt{d})$, para algún $d \in K_{r-1}$, y $C(S)$ es cerrado para raíces cuadradas, se sigue que $\sqrt{d} \in C(S)$ y, entonces, que $K_r \leq C(S)$.

Sea $F \leq \mathbb{C}$ el conjunto de todos los números complejos que pertenecen al extremo de una torre radical cuadrática que comienza en $\mathbb{Q}_s$. F es un subcuerpo: Sean $z, z' \in F$. Existirán torres radicales cuadráticas $\mathbb{Q}_s = K_0 \leq K_1 \leq \cdots \leq K_r$ y $\mathbb{Q}_S = K'_0 \leq K'_1 \leq \cdots \leq K'_s$ tal que $z \in K_r$ y $z' \in K'_s$. Supongamos que $K'_{i+1} = K'_i(\sqrt{d_{i+1}})$, $i = 0, \ldots, r' - 1$, con $d_{i+1} \in K'_i$. Construyamos la torre de extensiones

(1) $$\mathbb{Q}_S = K_0 \leq \cdots \leq K_r \leq K_r(\sqrt{d_1}) \leq K_r(\sqrt{d_1}, \sqrt{d_2}) \leq \cdots \leq K_r(\sqrt{d_1}, \ldots, \sqrt{d_s}).$$

Por inducción, vemos fácilmente que $K'_i \subseteq K_r(\sqrt{d_1}, \ldots, \sqrt{d_i})$:
- $K'_1 = K'_0(\sqrt{d_1}) \leq K_r(\sqrt{d_1})$
- $K'_{i+1} = K'_i(\sqrt{d_{i+1}}) \leq K_r(\sqrt{d_1}, \ldots, \sqrt{d_{i+1}})$.

y, entonces, cada $d_{i+1} \in K_r(\sqrt{d_1}, \ldots, \sqrt{d_i})$. Así que (1) es una torre radical cuadrática. Puesto que $z, z' \in K_r(\sqrt{d_1}, \ldots, \sqrt{d_s})$, entonces también $-z$, $z + z'$, zz', y z^{-1} si $z \neq 0$, están en el extremo de la torre. Luego también en F. Así que F es un subcuerpo.

Claramente F es cerrado para raíces cuadradas.

Para ver que F es cerrado por conjugación, notemos primero que si calculamos la imagen de $\mathbb{Q}_S$ por el automorfismo de conjugación obtenemos que
$$\overline{\mathbb{Q}_S} = \overline{\mathbb{Q}(z_0, z_1, \ldots, z_n, \overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1)} = \mathbb{Q}(\overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1, z_0, z_1, \ldots, z_n) = \mathbb{Q}_S$$
Además, si E/F es una extensión radical cuadrática, entonces la extensión de los cuerpos conjugados $\bar{E}/\bar{F}$ es también radical cuadrática: Si $E = F(\sqrt{a})$ con $a \in F$, entonces
$$\bar{E} = \bar{F}(\overline{\sqrt{a}}) = \bar{F}(\sqrt{\bar{a}}),$$
pues $(\overline{\sqrt{a}})^2 = \bar{a}$ y, por tanto, $\overline{\sqrt{a}} = \pm\sqrt{\bar{a}}$, donde $\bar{a} \in \bar{F}$. Entonces, si $z \in F$ y pertenece al extremo de la torre de extensiones cuadráticas $\mathbb{Q}_S = K_0 \leq K_1 \leq \cdots \leq K_r$, entonces su conjugado $\bar{z}$ pertenece al extremo de la torre de extensiones cuadráticas $\mathbb{Q}_S = \bar{K}_0 \leq \bar{K}_1 \leq \cdots \leq \bar{K}_r$, y concluimos que $\bar{z} \in F$.

Luego, por el anterior teorema, $F \supseteq C(S)$. □

Lema 14. *Toda extension de cuerpos de números E/K con $[E : K] = 2$ es radical cuadrática.*

Demostración. Escojamos un $\alpha \in E$ tal que $\alpha \notin K$. Tenemos la torre $K \leq K(\alpha) \leq E$, y la igualdad $2 = [E : K] = [E : K(\alpha)][K(\alpha) : K]$ obliga a que $[E : K(\alpha)] = 1$ y $[K(\alpha) : K] = 2$, ya que $K \neq K(\alpha)$ y no puede ser $[K(\alpha) : K] = 1$. Entonces $E = K(\alpha)$ y $Irr(\alpha, K)$ es de grado 2. Supongamos $Irr(\alpha, K) = x^2 + bx + c$. Entonces $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ y $E = K(\alpha) = K(\sqrt{b^2 - 4c})$ es una extensión radical cuadrática de K. □

Teorema 15. * *Sea $S = \{z_0 = 0, z_1 = 1, \ldots, z_n\} \subseteq \mathbb{C}$ un conjunto de números. Pongamos*

$$\mathbb{Q}_S = \mathbb{Q}(z_0, z_1, \ldots, z_n, \overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1).$$

Las siguientes propiedades, para un complejo $z \in C$, son equivalentes:

(1) $z \in C(S)$.
(2) *z es algebraico sobre $\mathbb{Q}_S$ y si $f = Irr(z, \mathbb{Q}_S)$ entonces $[\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$, para algún entero $m \geq 2$.*
(3) *z es algebraico sobre $\mathbb{Q}_S$ y si $f = Irr(z, \mathbb{Q}_S)$ entonces $G(f/\mathbb{Q}_S)$ es un 2-grupo.*

Demostración. Las propiedades (2) y (3) son equivalentes, pues

$$[\mathbb{Q}_S(f) : \mathbb{Q}_S] = |G(\mathbb{Q}_S(f)/\mathbb{Q}_S) = |G(f/\mathbb{Q}_S)|.$$

Supongamos $z \in C(S)$. Existirá una torre radical cuadrática $\mathbb{Q}_S = K_0 \leq \cdots \leq K_r$ con $z \in K_r$ y $K_r/\mathbb{Q}_S$ normal. Puesto que cada extensión K_i/K_{i-1} es radical cuadrática, será $K_i = K_{i-1}(\sqrt{a_i})$ para algún $a_i \in K_{i-1}$. Si $\sqrt{a_i} \in K_{i-1}$, entonces $K_i = K_{i-1}$ y $[K_i : K_{i-1}] = 1$. Si $\sqrt{a_i} \notin K_{i-1}$, entonces $Irr(\sqrt{a_i}, K_{i-1}) = x^2 - a_i$ y $[K_i : K_{i-1}] = 2$. Entonces $[K_r : \mathbb{Q}_S] = \prod_1^r [K_i : K_{i-1}] = 2^k$ para algún entero $k \geq 0$.

Puesto que la extension $K_r/\mathbb{Q}_S$ es finita, por tanto algebraica, y $z \in K_r$, resulta que z es algebraico sobre $\mathbb{Q}_S$. Sea $f = Irr(z, \mathbb{Q}_S)$. Como $K_r/\mathbb{Q}_S$ es normal, todas las raíces f estarán en K_r y será $\mathbb{Q}_S(f) \leq K_r$. Considerando la torre $\mathbb{Q}_S \leq \mathbb{Q}_S(f) \leq K_r$, tendremos que $2^k = [K_r : \mathbb{Q}_S] = [K_r : \mathbb{Q}_S(f)]\,[\mathbb{Q}_S(f) : \mathbb{Q}_S]$, de donde concluimos que $[\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$ para algún $m \leq k$.

Recíprocamente, supongamos estamos en las hipótesis (2) = (3). Como $G(\mathbb{Q}_S(f)/\mathbb{Q}_S) = G(f/\mathbb{Q}_S)$ es un 2-grupo (y todo p-grupo es resoluble) tendrá una serie con factores cíclicos de orden 2, esto es, de la forma

$$G(\mathbb{Q}_S(f)/\mathbb{Q}_S) = G_0 \geq G_1 \geq \cdots G_i \geq G_{i+1} \geq \cdots \geq G_k = 1,$$

donde cada G_{i+1} es normal en el G_i y cada cociente G_i/G_{i+1} es cíclico de orden 2. Por la correspondencia de Galois, tendremos una correspondiente torre de subextensiones

$$(2) \qquad \mathbb{Q}_S = \mathbb{Q}_S(f)^{G_0} \leq \cdots \mathbb{Q}_S(f)^{G_i} \leq \mathbb{Q}_S(f)^{G_{i+1}} \leq \cdots \mathbb{Q}_S(f)^{G_1} \leq \mathbb{Q}_S(f)^{G_k} = \mathbb{Q}_S(f).$$

Como cada $G_i = G(\mathbb{Q}_S(f)/\mathbb{Q}_S(f)^{G_i})$ y es $G_{i+1} \trianglelefteq G_i$, el Teorema Fundamental de la Teoría de Galois, aplicado a la torre $\mathbb{Q}_S(f)^{G_i} \leq \mathbb{Q}_S(f)^{G_i+1} \leq \mathbb{Q}_S(f)$, nos garantiza que cada extensión $\mathbb{Q}_S(f)^{G_{i+1}}/\mathbb{Q}_S(f)^{G_i}$ es normal con grupo de Galois

$$G\big(\mathbb{Q}_S(f)^{G_{i+1}}/\mathbb{Q}_S(f)^{G_i}\big) \cong G_i/G_{i+1},$$

que cíclico de orden 2. En particular, $[\mathbb{Q}_S(f)^{G_{i+1}} : \mathbb{Q}_S(f)^{G_i}] = 2$ y, por el lema anterior la torre de extensiones (2) es radical cuadrática. Como en su extremo $\mathbb{Q}_S(f)$ está obviamente z, el anterior teorema nos garantiza que $z \in C(S)$. $\square$

Corolario 16. *Sea $S = \{z_0 = 0, z_1 = 1, \ldots, z_n\} \subseteq \mathbb{C}$ un conjunto de números. Si un complejo $z \in C(S)$ entonces z es algebraico sobre $\mathbb{Q}_S$ y su polinomio irreducible $Irr(z, \mathbb{Q}_S)$ es de grado 2^k, para algún entero $k \geq 0$.*

Demostración. Si $z \in C(S)$, ya sabemos que z es algebraico sobre $\mathbb{Q}_S$ y que, si $f = Irr(z, \mathbb{Q}_S)$ entonces $[\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$ para un cierto entero $m \geq 0$. Puesto que $\mathbb{Q}_S \leq \mathbb{Q}_S(z) \leq \mathbb{Q}_S(f)$, de la igualdad $[\mathbb{Q}_S(z) : \mathbb{Q}_S][\mathbb{Q}_S(f) : \mathbb{Q}_S(z)] = [\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$ se deduce que $[\mathbb{Q}_S(z) : \mathbb{Q}_S] = gr(Irr(z, \mathbb{Q}_S))$ es también una potencia de 2. $\square$

Ejemplo 17 (*Trisección de ángulos)*. No todo ángulo se puede trisecar con regla y compás. En particular el de $60°$ $(=\frac{\pi}{3}$ radianes) no se puede trisecar. En este caso, tenemos tres puntos datos: el vértice $P_0 = (0,0)$, el punto $P_1 = (1,0)$ y el punto $P_2 = (\cos 60°, \sin 60°) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$. La cuestión es saber si el punto $P = (\cos 20°, \sin 20°)$ es construible con regla y compás desde esos puntos. Claramente esto es equivalente a que lo sea el punto $(\cos 20°, 0)$.

Vamos a aplicar el criterio del teorema anterior. En el caso presente, tenemos el conjunto complejos dato

$$S = \{z_0 = 0, z_1 = 1, z_2 = e^{i\pi/3} = \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\},$$

y el cuerpo $\mathbb{Q}_S = \mathbb{Q}(z_0, z_1, z_2, \bar{z}_0, \bar{z}_1, \bar{z}_2) = \mathbb{Q}(i\sqrt{3})$. Por el teorema anterior, la trisección del ángulo de $60°$ requiere que $\cos 20°$ sea algebraico y su irreducible sobre $\mathbb{Q}(i\sqrt{3})$ sea de grado una potencia de 2, o sea que $[\mathbb{Q}(i\sqrt{3}, \cos 20^o) : \mathbb{Q}(i\sqrt{3})]$ ha de ser una potencia de dos. Como $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$, por la torre $\mathbb{Q} \leq \mathbb{Q}(i\sqrt{3}) \leq \mathbb{Q}(i\sqrt{3}, \cos 20^o)$, deducimos que sería también $[\mathbb{Q}(i\sqrt{3}, \cos 20^o) : \mathbb{Q}]$ una potencia de dos. Y por la torre $\mathbb{Q} \leq \mathbb{Q}(\cos 20^o) \leq \mathbb{Q}(i\sqrt{3}, \cos 20^o)$ también lo sería $[\mathbb{Q}(\cos 20^o) : \mathbb{Q}]$. Esto es, sería $Irr(\cos 20, \mathbb{Q})$ un polinomio de grado una potencia de dos.

Ahora, tenemos la identidad trigonométrica

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

que nos da la igualdad

$$4(\cos 20°)^3 - 3\cos 20° - \frac{1}{2} = 0.$$

Así que $\cos 20°$ es raíz del polinomio $x^3 - \frac{3}{4}x - \frac{1}{8}$. Pero ocurre que este polinomio es irreducible sobre $\mathbb{Q}$, ya que es de grado 3 y no tiene raíces (sus posibles raíces es $\mathbb{Q}$ son las mismas que las del polinomio $8x^3 - 6x - 1 \in \mathbb{Z}[x]$, cuyas únicas posibles raíces son $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$, y comprobamos directamente que ninguno de estos racionales lo es). Entonces $Irr(\cos 20°, \mathbb{Q}) = x^3 - \frac{3}{4}x - \frac{1}{8}$, que es de grado 3, y no una potencia de 2.

Alternativamente: Si $z = e^{\frac{\pi i}{9}}$, entonces $z + \bar{z} = 2\cos 20^o$ es raíz de $x^3 - 3x - 1$, pues

$$(z+\bar{z})^3 - 3(z+\bar{z}) - 1 = z^3 + \bar{z}^3 + 3z + 3\bar{z} - 3z - 3\bar{z} - 1 = 2\cos\frac{\pi}{3} - 1 = 1 - 1 = 0.$$

Como $x^3 - 3x - 1$ no tiene raíces en $\mathbb{Q}$, es irreducible, así que $Irr(2\cos 20^o, \mathbb{Q}) = x^3 - 3x - 1$ y $[[\mathbb{Q}(\cos 20^o) : \mathbb{Q}] = [\mathbb{Q}(2\cos 20^o) : \mathbb{Q}] = 3$. □

Ejemplo 18 (*Duplicación del cubo)*. En este caso, tenemos dos puntos datos, $P_0 = (0,0)$ y $P_1 = (1,0)$, que son una de las aristas de un cubo, y la cuestión es saber si es construible con regla y compás desde esos puntos el punto $P = (a, 0)$ tal que el cubo del cual el segmento de extremos P_0 y P es una de sus aristas tenga volumen doble. Claramente esto es equivalente a que lo sea el punto $(\sqrt[3]{2}, 0)$, y por el teorema anterior, habría de ser $Irr(\sqrt[3]{2}, \mathbb{Q})$ de grado una potencia de 2 (en este caso $\mathbb{Q}_S = \mathbb{Q}$). Pero $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ que es de grado 3.

Ejemplo 19 (*Cuadratura del círculo)*. En este caso, tenemos dos puntos datos, $P_0 = (0,0)$ y $P_1 = (1,0)$, que determinan un círculo de centro P_0 y radio 1, y la cuestión es saber si es construible el punto $P = (a, 0)$ tal que el cuadrado del cual el segmento de extremos P_0 y P es uno de sus lados tenga igual area que el círculo dado. Claramente esto requiere que $a = \sqrt{\pi}$ y que a sea algebraico sobre $\mathbb{Q}$. Pero esto implicaría que π es algebraico sobre $\mathbb{Q}$, lo que contradice el Teorema de Lindemann, que nos asegura que π, y entonces también $\sqrt{\pi}$, es trascendente.

6.3. **Poligonos regulares.**

En este caso, tenemos dos puntos datos, P_0 y P_1, que determinan un círculo de centro P_0 y radio la amplitud del segmento que los une, y la cuestión es saber si son construibles los n vértices de un polígono regular inscrito en la circunferencia de centro P_0 y radio el segmento de extremos P_0 y P_1, uno de los cuales es P_1. Tomando $P_0 = (0.0)$ y $P_1 = (1, 0)$, la cuestión reduce claramente a saber si el punto $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ es, o no, construible desde P_0 y P_1.

Definición 20. *Un primo $p \geq 2$ de $\mathbb{Z}$ se dice que p* **de Fermat** *si es de la forma $p = 2^k + 1$ para algún entero $k \geq 1$.*

Por ejemplo, los primos 3, 5, 17, 257 y 65537 son primos de Fermat.

Teorema 21. * *El polígono regular de n lados es construible si y solo si n factoriza en la forma*

$$n = 2^m p_1 p_2 \cdots p_r,$$

donde $m \geq 0$, cada p_i es un primo de Fermat, y $p_i \neq p_j$ si $i \neq j$.

DEMOSTRACIÓN. Algebraizando el problema, tenemos $S = \{0, 1\}$ y $\mathbb{Q}_S = \mathbb{Q}$. Puesto que ya sabemos que $z_n = e^{\frac{2\pi i}{n}}$ es algebraico sobre $\mathbb{Q}$, que $Irr(z_n, \mathbb{Q}) = \Phi_n$, y que $\mathbb{Q}(\Phi_n) = \mathbb{Q}(z_n)$. El teorema nos asegura que z_n es construible si y solo si $gr(\Phi_n)$ es una potencia de dos, esto es , si y solo si $\varphi(n)$ es una potencia de dos.

Supongamos que la factorización en primos distintos de n es

$$n = 2^m p_1^{m_1} \cdots p_r^{m_r},$$

donde $m \geq 0$, cada $m_i \geq 1$, y cada $p_i \geq 3$. Entonces

$$\varphi(n) = 2^{e-1}(p_1 - 1)p_1^{m_1 - 1} \cdots (p_r - 1)p_r^{m_r - 1}.$$

Es claro que, $\varphi(n)$ es una potencia de 2 si y solo si cada $m_i = 1$ y cada $p_i = 1 + 2^{k_i}$ para algún $k_i \geq 2$. $\square$