Aplicaciones a construcciones geométricas

Facultad de Ciencias UNAM

Introducción

Antes de empezar, un poquito de terminología:

- Decimos que **podemos construir el cubo** $\mathcal{K}$
  dibujo
  si $a \in \mathbb{R}$ es un numero construible y definimos

$$\text{vol}(\mathcal{K}) := a^3.$$

- Decimos que $\theta \in \mathbb{R}$ es un **ángulo construible** si existe un triángulo ABC construible[1] en donde θ es uno de los ángulos de ABC
  dibujo

[1] Es decir, existen tres puntos construibles A, B, y C no colineales.

En esta sección demostraremos que los siguientes tres problemas (planteados por los griegos) no tienen solución con regla y compás.

(I) **Duplicar el cubo:** Si $\mathcal{K}$ es un cubo, entonces podemos construir un cubo $\mathcal{K}'$ tal que $\text{vol}(\mathcal{K}') = 2 \cdot \text{vol}(\mathcal{K})$.

(II) **Trisectar el ángulo:** Si θ es un ángulo construible, entonces $\theta/3$ también es un ángulo construible.

(III) **Cuadrar el circulo:** Dado un circulo podemos construir un cuadrado con la misma área que este circulo.

En el camino que tomaremos, resulta muy útil la siguiente definición.

F-rectas y F-circunferencias

Definición

Supongamos que F es un subcampo de $\mathbb{R}$.

- Una F**-recta** es una recta en $\mathbb{R}^2$ que contiene a 2 puntos de $F \times F$.
- Una F**-circunferencia** es una circunferencia en $\mathbb{R}^2$ cuyo centro es un punto de $F \times F$ y cuyo radio es un elemento de F.

En lo que sigue, F siempre denota un subcampo de $\mathbb{R}$. En particular, notemos que $\text{ch}(F) = 0$.

Ecuaciones para F-rectas

Proposición 1

Si ℓ es una F-recta, entonces existen $a, b, c \in F$ tales que

$$\ell = \{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\}.$$

Demostración. Antes de empezar, recuerda que si ℓ es una recta en $\mathbb{R}^2$ con pendiente m y $(0, s) \in \ell$ (recuerda que toda recta intersecta exactamente una vez al eje Y), entonces

$$\ell = \{(x, y) \in \mathbb{R}^2 \mid y = mx + s\}.$$

Con esto en mente, procedamos a la demostración.

Supongamos que ℓ es una F-recta. Por definición, existen $(x_1, y_1), (x_2, y_2) \in F \times F$ que pertenecen a ℓ. Entonces,

$$\frac{y_1 - y_2}{x_1 - x_2} \in F$$

es la pendiente de ℓ y por lo anterior, existe $s \in \mathbb{R}$ tal que $(x, y) \in \ell$ si y solo si

$$y = \frac{y_1 - y_2}{x_1 - x_2} x + s.$$

Como $(x_1, y_1) \in \ell$, podemos sustituir $x = x_1$ y $y = y_1$ para obtener

$$y_1 = \frac{y_1 - y_2}{x_1 - x_2} x_1 + s.$$

Despejando s en esta ecuación vemos que $s \in F$. Definiendo

$$a := \frac{y_1 - y_2}{x_1 - x_2}, \quad b := -1, \quad c := s = y_1 - \frac{y_1 - y_2}{x_1 - x_2} x_1$$

obtenemos lo deseado. $\square$

Ecuaciones para F-circunferencias

Proposición 2

Si $\mathcal{C}$ es una F-circunferencia, entonces existen $d, e, f \in F$ tales que

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + dx + ey + f = 0\}.$$

Demostración. Antes de empezar, recuerda que si $\mathcal{C}$ es una circunferencia en $\mathbb{R}^2$ con centro (x_0, y_0) y radio $r > 0$, entonces

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid (x - x_0)^2 + (y - y_0)^2 = r^2\}.$$

Con esto en mente, procedamos a la demostración.

Supongamos que $\mathcal{C}$ es una F-circunferencia con centro $(x_0, y_0) \in F \times F$ y radio $r \in F$. Por lo mencionado anteriormente,

$$\begin{aligned}(x, y) \in \mathcal{C} &\iff (x - x_0)^2 + (y - y_0)^2 = r^2 \\ &\iff x^2 - 2xx_0 + x_0^2 + y^2 - 2yy_0 + y_0^2 = r^2.\end{aligned}$$

Definiendo

$$d := -2x_0, \quad e := -2y_0, \quad f := x_0^2 + y_0^2 - r_0^2$$

y observando que cada uno de estos elementos pertenece a F (pues $(x_0, y_0) \in F \times F$ y $r \in F$), obtenemos lo deseado. $\square$

La intersección de dos F-rectas vive en $F \times F$

Proposición 3

Si ℓ y ℓ' son dos F-rectas que se intersectan en (u, v), entonces $(u, v) \in F \times F$.

Demostración. Por la proposición anterior, existen $a, b, c, a', b', c' \in F$ tales que

$$\ell = \{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\} \quad \text{y}$$
$$\ell' = \{(x, y) \in \mathbb{R}^2 \mid a'x + b'y + c' = 0\}.$$

Como $(u, v) \in \ell \cap \ell'$, entonces

$$au + bv + c = 0 \quad \text{y} \quad a'u + b'v + c' = 0$$

Despejando u y v en términos de $a, b, c, a', b', c' \in F$ obtenemos lo deseado. $\square$

Las coordenadas de las intersecciones de una F-recta con una F-circunferencia viven (en el peor de los casos) en una F-extensión cuadrática

Proposición 4

Supongamos que ℓ es una F-recta y que $\mathcal{C}$ es una F-circunferencia. Si $(u, v) \in \ell \cap \mathcal{C}$, entonces existe $\alpha \in F$ tal que $u, v \in F(\sqrt{\alpha})$.

Demostración. Por la proposición 2, existen $a, b, c, d, e, f \in F$ tales que

$$\ell = \{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\} \quad \text{y}$$
$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + dx + ey + f = 0\}.$$

Como $(u, v) \in \ell \cap \mathcal{C}$, entonces

$$au + bv + c = 0 \tag{1}$$
$$\text{y} \quad u^2 + v^2 + du + ev + f = 0. \tag{2}$$

Despejemos a u y v. Para esto, recordemos que como ℓ es una recta, entonces $a \neq 0$ o $b \neq 0$ (si ambos fueran 0, la ecuación que determina a ℓ seria $c = 0$).

Veamos el caso $b \neq 0$. El caso $a \neq 0$ es análogo.

Despejando a v en (1) obtenemos

$$v = -\frac{au + c}{b}. \tag{3}$$

Sustituyendo esto en (2) obtenemos

$$u^2 + \left(-\frac{au + c}{b}\right)^2 + du + e\left(-\frac{au + c}{b}\right) + f = 0.$$

Esto es una ecuación cuadrática en u con coeficientes en un campo con característica distinta de 2 (como $F \subset \mathbb{R}$, $\mathrm{ch}(F) = 0$).

Recuerda que en el corolario 2.6.9 vimos que toda solución a una extensión cuadrática vive en una extensión de la forma $F(\sqrt{\alpha})$ con $\alpha \in F$.

Por lo tanto $u \in F(\sqrt{\alpha})$ y por (3), esto implica que también $v \in F(\sqrt{\alpha})$. $\square$

Las coordenadas de las intersecciones de dos F-circunferencias viven (en el peor de los casos) en una F-extensión cuadrática

Proposición 5

Supongamos que $\mathcal{C}$ y $\mathcal{C}'$ son dos F-circunferencias. Si $(u, v) \in \mathcal{C} \cap \mathcal{C}'$, entonces existe $\alpha \in F$ tal que $u, v \in F(\sqrt{\alpha})$.

Demostración. Supongamos que $\mathcal{C}$ y $\mathcal{C}'$ son dos F-circunferencias. Por la proposición 2, existen $d, e, f, d', e', f' \in F$ tales que

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + dx + ey + f = 0\} \quad \text{y}$$
$$\mathcal{C}' = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + d'x + e'y + f' = 0\}.$$

Si $(u, v) \in \mathcal{C} \cap \mathcal{C}'$, entonces

$$u^2 + v^2 + du + ev + f = 0 \quad \text{y} \quad u^2 + v^2 + d'u + e'v + f' = 0.$$

Restando estas dos ecuaciones obtenemos

$$(d - d')u + (e - e')v + (f - f') = 0.$$

Sea

$$\ell := \{(x, y) \in \mathbb{R}^2 \mid (d - d')x + (e - e')y + (f - f') = 0\}.$$

Entonces ℓ es una F-recta y $(u, v) \in \ell \cap \mathcal{C}$. Usando la proposición anterior, obtenemos lo deseado. □

En lo que sigue, demostraremos el resultado que nos permitirá demostrar la falsedad de los problemas (I), (II), y (III). Para esto, necesitamos el siguiente lema.

Lema 6

Supongamos que F es un subcampo de $\mathbb{R}$. Si $\alpha_1,\ldots,\alpha_n \in F$, entonces $F(\sqrt{\alpha_1})$ es una F-extensión de grado ≤ 2 y en general, $F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_i})$ es una $F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})$-extensión de grado ≤ 2 para toda $i \in \{2,\ldots,n\}$.

Demostración. Supongamos que $\alpha_1,\ldots,\alpha_n \in F$.

Caso 1. $\sqrt{\alpha_i} \in F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})$.
Entonces $F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_i}) = F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})$ y por lo tanto, $F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_i})$ es una $F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})$-extensión de grado 1.

Caso 2. $\sqrt{\alpha_i} \notin F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})$.
Entonces el polinomio $x^2 - \alpha_i$ es irreducible en $F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})$ porque no tiene raíces ahí. Por lo tanto,

$$[F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_i}) : F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})] = \deg_{F(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{i-1}})} \sqrt{\alpha_i} = 2.$$

□

Las coordenadas de un punto construible pertenecen a una $\mathbb{Q}$-extensión de grado 2^m para alguna $m \in \mathbb{Z}_{\geq 0}$

Proposición 7

Si $(u, v) \in \mathbb{R}$ es construible, entonces existen $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ tales que

- $u, v \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ y
- $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ es una $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$-extensión de grado ≤ 2 para toda i.

En particular,

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] = 2^m \text{ para alguna } m \in \mathbb{Z}_{\geq 0}.$$

Demostración. Como (i) nuestras únicas herramientas son la regla y el compás y (ii) por definición, todas las construcciones empiezan desde el dibujo que solo tiene a O y A, entonces todas las construcciones tienen el siguiente "formato":

(En la siguiente diapositiva justificamos la existencia del paso 4.)

1. Construyes los puntos de $\mathbb{Q} \times \mathbb{Q}$ y los números de $\mathbb{Q}$ que vas a necesitar en el resto de la construcción.
2. Construyes ciertas $\mathbb{Q}$-rectas y/o $\mathbb{Q}$-circunferencias (usando los puntos de $\mathbb{Q} \times \mathbb{Q}$ y los números de $\mathbb{Q}$ que construiste en el paso anterior).
3. Demuestras que (gracias a la construcción en el paso anterior) tienes "nuevos" puntos y/o números construibles, digamos $(u_1, v_1), \ldots, (u_k, v_k)$ y $\beta_1, \ldots, \beta_l$.
4. Observas que existen $\alpha_1, \ldots, \alpha_{n_1} \in \mathbb{R}$ tales que
   - $u_1, v_1, \ldots, u_k, v_k \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{n_1})$ y
   - $\mathbb{Q}(\alpha_1, \ldots, \alpha_j)$ es una $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$-extensión de grado ≤ 2 para toda j.

1'. Construyes todos los puntos de $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n_1}) \times \mathbb{Q}(\alpha_1, \ldots, \alpha_{n_1})$ y los números de $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n_1})$ que vas a necesitar en el resto de la construcción.

$\vdots$

Para ver porque siempre tenemos un paso 4, primero recordemos que todos los puntos "nuevos" son intersecciones de $\mathbb{Q}$-circunferencias con $\mathbb{Q}$-rectas o intersecciones de dos $\mathbb{Q}$-circunferencias. En cualquier caso, las proposiciones 4 y 5 implican que existe $\gamma_i \in \mathbb{Q}$ tal que $u_i, v_i \in \mathbb{Q}(\sqrt{\gamma_i})$.

Usando la notación del paso 3, definimos

$$\alpha_i = \begin{cases} \sqrt{\gamma_i} & \text{si } i \in \{1, \ldots, k\} \\ \beta_{i-k} & \text{si } i \in \{k+1, \ldots, k+l\} \end{cases}$$

Claramente, $u_1, v_1, \ldots, u_k, v_k \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{n_1})$.

Ahora, veamos que $\mathbb{Q}(\alpha_1, \ldots, \alpha_j)$ es una $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$-extensión de grado ≤ 2 para toda j.

Nota que como β_j es una distancia entre dos elementos de $\mathbb{Q} \times \mathbb{Q}$, entonces β_j en realidad es de la forma $\sqrt{\delta_j}$ para alguna $\delta_j \in \mathbb{Q}$. Usando el lema anterior obtenemos lo deseado.

Finalmente, notemos que como siempre acabamos en un paso 4, entonces, siempre acabamos en un campo de la forma

$$\mathbb{Q}\left(\alpha_1, \ldots, \alpha_{n_1}, \alpha_{n_1+1}, \ldots, \alpha_{n_2}, \ldots, \alpha_{n_k}, \ldots, \alpha_n\right).$$

que satisface

- $u, v \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ y
- $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ es una $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$-extensión de grado ≤ 2 para toda i.

□

$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2 si α es construible

Lema 8

Si $\alpha \in \mathbb{R}$ es construible, entonces

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k \text{ para alguna } k \in \mathbb{Z}_{\geq 0}.$$

Demostración. Supongamos que $\alpha \in \mathbb{R}$ es construible. Equivalentemente $(0, \alpha)$ también es construible y por la proposición anterior existen $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ tales que $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ y

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] = 2^m \text{ para alguna } m \in \mathbb{Z}_{\geq 0}.$$

Como $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, entonces $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ y por lo tanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide a

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] = 2^m.$$

De donde, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ para alguna $k \in \mathbb{Z}_{\geq 0}$. $\square$

No se puede duplicar cualquier cubo

Teorema 9

La siguiente afirmación es falsa:

> ***Duplicar el cubo:*** *Si $\mathcal{K}$ es un cubo, entonces podemos construir un cubo $\mathcal{K}'$ tal que $vol(K') = 2vol(K)$.*

Demostración. Supongamos lo contrario. Sea $\mathcal{K}$ un cubo con volumen 1. Entonces existe un cubo $\mathcal{K}'$ con volumen 2. Por definición de volumen de un cubo, esto implica que $\mathcal{K}'$ tiene lados de longitud $\sqrt[3]{2}$. Sin embargo, esto es imposible pues $\sqrt[3]{2}$ no es construible:

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^k.$$

□

Un lema para demostrar que no se puede trisectar cualquier ángulo

Lema 10

Para todo $x \in \mathbb{R}$

$$\cos 3x = 4\cos^2 x - 3\cos x. \tag{4}$$

Antes de ver la demostración, recordemos que los griegos siempre consideraban los argumentos de cos y sin como ángulos. Por lo tanto, dentro de nuestros axiomas, la formula (4) sera valida para x un ángulo construible.

La demostración que damos para (4) es valida para toda $x \in \mathbb{R}$ y en particular, también sera valida para todo x ángulo construible.

Demostración. Asumimos las siguientes formulas trigonométricas.

$$\cos^2 x + \sin^2 y = 1 \tag{5}$$

$$\cos(x+y) = \cos x \cos y - \sin x \sin y \tag{6}$$

$$\cos(2x) = 2\cos^2 x - 1 \tag{7}$$

$$\sin(2y) = 2\cos x \sin x \tag{8}$$

Entonces

$$\begin{aligned}
\cos 3x &= \cos(2x + x) \\
&= \cos 2x \cos x - \sin 2x \sin x && \text{(por (6))} \\
&= (2\cos^2 x - 1)\cos x - (2\cos x \sin x)\sin x && \text{(por (7) y (8))} \\
&= (2\cos^2 x - 1)\cos x - 2\cos x \sin^2 x \\
&= (2\cos^2 x - 1)\cos x - 2\cos(1 - \cos^2 x) && \text{(por (5))} \\
&= 4\cos^3 x - 3\cos x.
\end{aligned}$$

Otro lema para ver que no se puede trisectar el ángulo

Lema 11

El polinomio $8x^3 - 6x - 1 \in \mathbb{Q}[x]$ es irreducible en $\mathbb{Q}[x]$. En particular, si α es una raíz de $8x^3 - 6x - 1$, entonces

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

Demostración. Antes que nada, recordemos que en la proposición 1.26.1 vimos que si $p(x) \in \mathbb{Z}[x]$ es primitivo[2], entonces

$$p(x) \text{ es irreducible en } \mathbb{Z}[x] \iff p(x) \text{ es irreducible en } \mathbb{Q}[x].$$

Por lo tanto (como $8x^3 - 6x - 1$ es primitivo), basta probar que $8x^3 - 6x - 1$ es irreducible en $\mathbb{Z}[x]$.

Para esto, supongamos lo contrario. Es decir, supongamos que existen $a(x), b(x) \in \mathbb{Z}[x]$ de grado ≥ 1 tales que

$$8x^3 - 6x - 1 = a(x)b(x). \tag{9}$$

[2]Los coeficientes son primos relativos.

Como $\deg a(x), \deg b(x) \geq 1$, la igualdad $8x^3 - 6x - 1 = a(x)b(x)$ implica que uno de los factores tiene grado 2 y el otro tiene grado 1. Sin perdida de generalidad, supongamos que

$$a(x) = a_1 x + a_0 \quad \text{y} \quad b(x) = b_2 x^2 + b_1 x + b_0 \tag{10}$$

Mas aun, es fácil verificar que podemos pedir sin perdida de generalidad que $a_1 \geq 0$. Sustituyendo (10) en (9) obtenemos

$$\begin{aligned} 8x^3 - 6x - 1 &= (a_1 x + a_0)(b_2 x^2 + b_1 x + b_0) \\ &= a_1 b_2 x^3 + a_1 b_1 x^2 + a_1 b_0 x + a_0 b_2 x^2 + a_0 b_1 x + a_0 b_0 \end{aligned}$$

Usando esto, obtenemos que $a_1 | 8$ y $a_0 | 1$. Por lo tanto, $a(x)$ debe ser alguno de los siguientes polinomios

$$(8x \pm 1), \ \ (4x \pm 1), \ \ (2x \pm 1), \ \ (x \pm 1)$$

Sin embargo, se puede verificar directamente que ninguna de las raíces de estos polinomios es raíz de $8x^3 - 6x - 1$. Una contradicción. $\square$

No se puede trisectar cualquier ángulo

Teorema 12

La siguiente afirmación es falsa:

> ***Trisectar el ángulo:*** *Si θ es un ángulo construible, entonces $\theta/3$ también es un ángulo construible.*

Demostración. Veamos que $\theta = \pi/3$ es el contraejemplo buscado.

Primero veamos que $\pi/3$ es un ángulo construible.

Recuerda que en la introducción a la sección anterior vimos que podemos construir un triángulo equilátero. Usando que

- todos los ángulos de un triángulo equilátero valen lo mismo y que
- la suma de los ángulos de un triángulo es π,

obtenemos lo deseado.

Ahora, veamos por contradicción que $\left(\pi/3\right)/3 = \pi/9$ no es un ángulo construible. Si lo fuera, entonces por el lema 10 tendríamos la primera de las siguientes igualdades

$$4\left(\cos(\pi/9)\right)^3 - 3\cos(\pi/9) = \cos\left(3\pi/9\right) = \cos(\pi/3) = 1/2.$$

De donde,

$$8\left(\cos(\pi/9)\right)^3 - 6\cos(\theta/9) - 1 = 0.$$

Pero entonces por el lema 11,

$$\left[\mathbb{Q}(\cos(\pi/9)) : \mathbb{Q}\right] = 3$$

contradiciendo el lema 8. □

No se puede cuadrar el circulo

Teorema 13

La siguiente afirmación es falsa:

> ***Cuadrar el circulo:*** *Dado un circulo podemos construir un cuadrado con la misma área que este circulo.*

Demostración. Como el circulo unitario tiene área π, basta ver que no se puede construir un cuadrado con área π. Esto seria equivalente a demostrar que $\sqrt{\pi}$ es un numero construible o equivalentemente, que π es un numero construible.

Sin embargo, π no es algebraico sobre $\mathbb{Q}$ (esto es bastante difícil de probar y por eso lo omitimos). En particular, la $\mathbb{Q}$-extensión $\mathbb{Q}(\pi)$ no es finita y por lo tanto no satisface $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^k$ para alguna $k \in \mathbb{Z}_{\geq 0}$. $\square$