Construcciones con regla y compás

Juan Sabia

1 Introducción

La idea de esta clase es ver qué construcciones geométricas pueden hacerse con el uso de una regla no graduada (sin marcas), de un compás, de un lápiz y una hoja. Esta forma de construir figuras geométricas la heredamos de los griegos, que relacionaban la geometría con la perfección y la religión. Todos estamos acostumbrados a que en el colegio primario se enseñe a trazar la bisectriz de un ángulo, la mediatriz de un segmento y a construir triángulos con regla y compás. La pregunta es qué otras construcciones se pueden hacer.

Los griegos ya tenan planteadas tres preguntas (que hoy se consideran clásicas):

- ¿Se puede trisecar un ángulo usando sólo regla y compás?
- ¿Se puede duplicar un cubo usando sólo regla y compás? (es decir, si tenemos un modelo plano de seis cuadrados para construir un cubo de volumen v, ¿se puede construir un modelo plano para construir un cubo de volumen $2v$ sólo usando regla y compás?)
- ¿Se puede cuadrar un círculo con regla y compás? (es decir, dado un círculo, ¿se puede dibujar un cuadrado de su misma superficie usando sólo regla y compás?)

Otra pregunta que puede formularse es:

- ¿Cuáles polígonos regulares pueden construirse usando regla y compás?

Vamos a intentar dar respuesta a algunas de estas preguntas (otras se escapan al contenido del curso).

2 Reglas y ejemplo

Lo primero que vamos a fijar son las reglas para dibujar con regla y compás. Partimos de un conjunto dado de puntos en el plano. Las construcciones que pueden hacerse son:

- Se puede dibujar la recta que pasa por dos puntos dados.
- Se puede trazar la circunferencia que tiene centro en un punto dado y cuyo radio sea la distancia entre dos puntos dados.

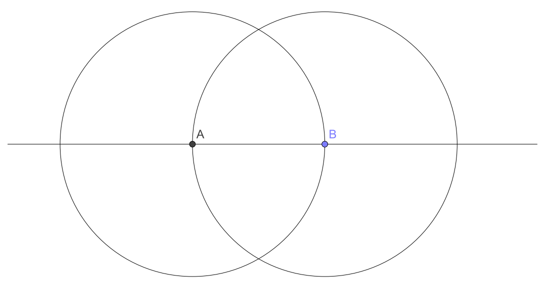
- Las intersecciones de rectas o circunferencias que se puedan dibujar se consideran puntos que pueden usarse para seguir dibujando.

En general, para simplificar la cuestión, vamos a considerar que partimos de sólo dos puntos. Un punto se dirá *construible* si se puede construir en un número finito de pasos a partir de estos dos puntos.

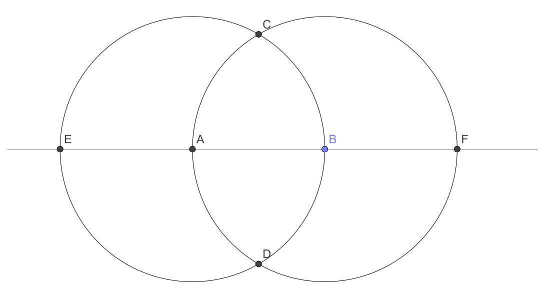
Ejemplo:

Marcamos primero los dos puntos A y B en el plano:

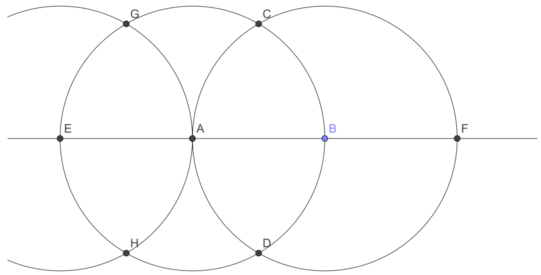
Podemos trazar la recta que une los dos puntos marcados, o cualquier circunferencia que tenga por centro uno de los puntos y radio la distancia entre dos puntos marcados. Todas las construcciones posibles serían:



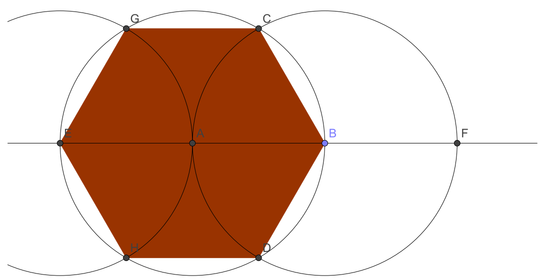
Con nuestra construcción aparecieron cuatro nuevos puntos (C, D, E y F) que podemos usar para seguir dibujando:



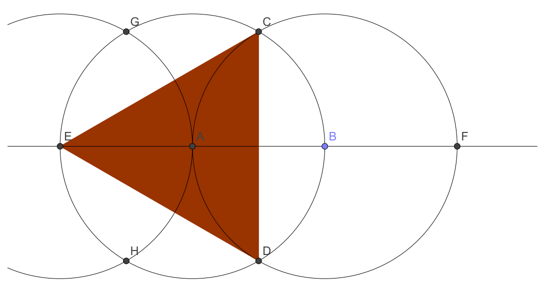
Por ejemplo, podemos trazar la circunferencia con centro E y radio igual a la distancia entre A y E, y obtenemos los puntos G y H:



De paso demostramos que algunos polígonos regulares son construibles con regla y compás: el hexágono



y el triángulo

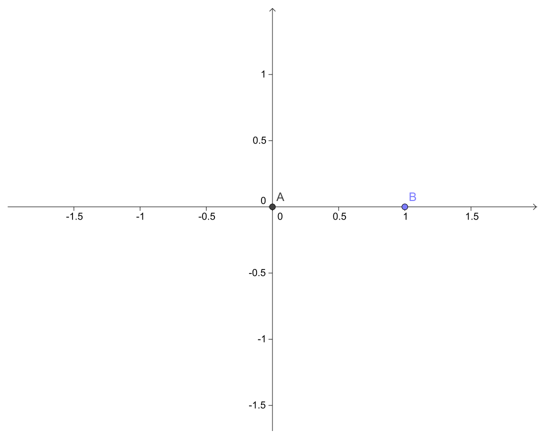


y como sabemos bisecar ángulos, podemos construir cualquier polígono regular que tenga $2^n.3$ lados para n natural.

Hay dos construcciones básicas que sabemos hacer con regla y compás que vamos a usar y no vamos a detallar:

- Dados tres puntos A, B, y C, trazar la perpendicular por C a la recta que pasa por A y B.
- Dados tres puntos A, B, y C, trazar la paralela por C a la recta que pasa por A y B.

Dados A y B, podemos pensarlos como los puntos $(0,0)$ y $(1,0)$ del plano y, por las construcciones básicas anteriores, podemos trazar los ejes cartesianos utilizando sólamente regla y compás.



3 Coordenadas

La noción de punto construible ahora significará "construible a partir del $(0,0)$ y del $(1,0)$". Por ejemplo, en la sección anterior, vimos que los puntos $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$, $(-1,0)$, $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$ y $(\frac{1}{2}, -\frac{\sqrt{3}}{2})$ (que, junto al $(1,0)$ son los vértices del hexágono regular inscripto en la circunferencia de centro $(0,0)$ y radio 1) son construibles.

Lema: Un punto (x,y) es construible si y sólo si los puntos $(x,0)$ e $(y,0)$ son construibles.

Demostración:
$\Rightarrow$) Si el punto (x,y) es construible, proyectándolo sobre los ejes, obtenemos $(x,0)$ y $(0,y)$. Con el compás, a partir del $(0,y)$ construimos el $(y,0)$.
$\Leftarrow$) Si $(x,0)$ e $(y,0)$ son construibles, utilizando el compás, podemos construir el $(0,y)$. Trazamos la recta paralela al eje de las abscisas que pasa por $(0,y)$ y la recta paralela al eje de las ordenadas que pasa por $(x,0)$. El punto de intersección de estas dos rectas es el (x,y). $\square$

Esta traducción a coordenadas puede ayudarnos a hacer algunos dibujos.

Ejemplo: Construcción del pentágono regular.

Consideremos el pentágono regular inscripto en la circunferencia de centro $(0,0)$ y radio 1 con vértice en el $(1,0)$. Las coordenadas del vértice en el primer cuadrante son $(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5})$. Si lo pensamos como número complejo, es el número $\xi = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$, que por la fórmula de De Moivre, satisface $\xi^5 = 1$ (recordar que De Moivre dice que para multiplicar complejos deben multiplicarse los módulos y sumarse los argumentos). Por lo tanto tenemos que ξ es raíz del polinomio

$$X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$$

y como $\xi \neq 1$ resulta que satisface

$$\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0.$$

Sacando ξ^2 factor común, se tiene que

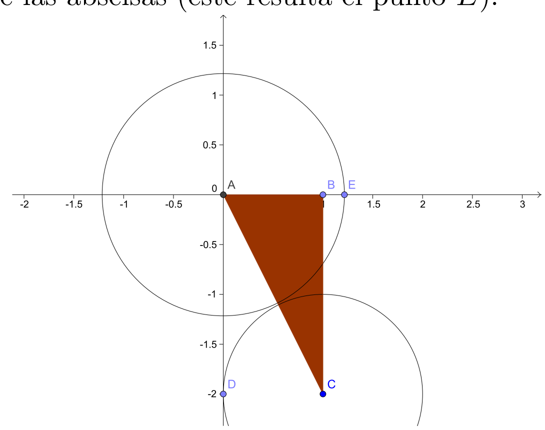
$$\xi^2 + \xi + 1 + \xi^{-1} + \xi^{-2} = (\xi + \xi^{-1})^2 + (\xi + \xi^{-1}) - 1 = 0.$$

Pero

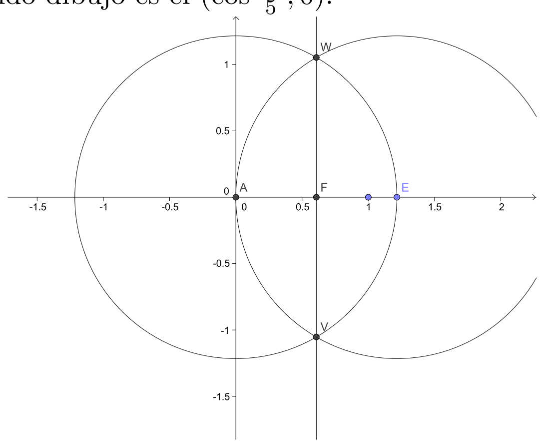
$$(\xi + \xi^{-1}) = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} + \cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5} = 2\cos\frac{2\pi}{5},$$

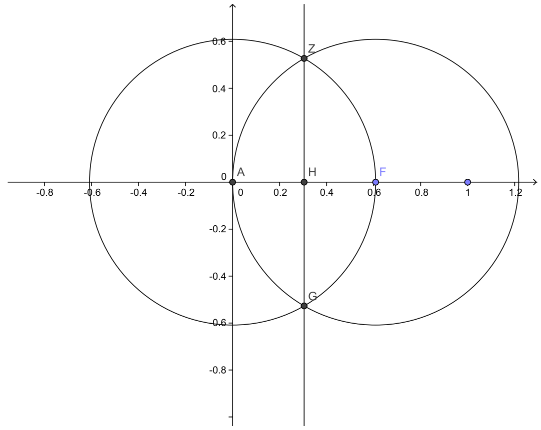
con lo que $2\cos\frac{2\pi}{5}$ resulta ser la raíz positiva del polinomio $x^2 + x - 1$, y entonces es igual a $\frac{-1+\sqrt{5}}{2}$.

Usemos esto para construir el pentágono regular con regla y compás:
Primero construimos un segmento $\overline{AC}$ de longitud $\sqrt{5}$ usando Pitágoras, le restamos 1 y lo ubicamos en el eje de las abscisas (éste resulta el punto E):

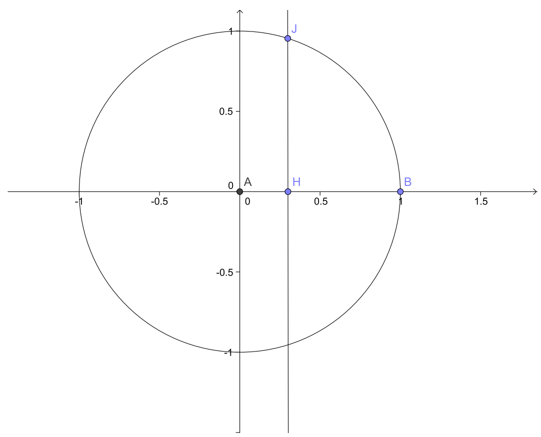


Ahora, en dos pasos, dividimos el segmento $\overline{AE}$ en cuatro partes iguales, y el punto H que aparece en el segundo dibujo es el $(\cos\frac{2\pi}{5}, 0)$:

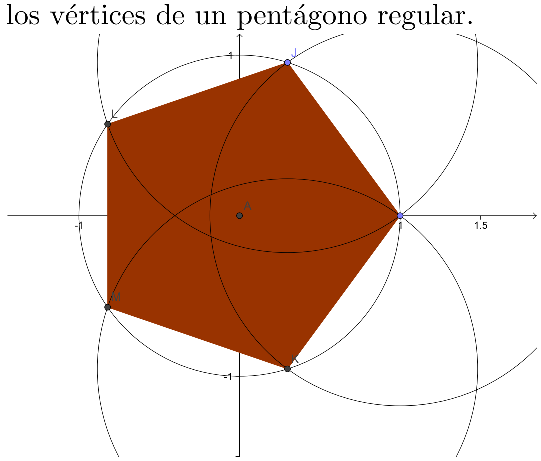




Ahora que ya tenemos el punto $(\cos\frac{2\pi}{5}, 0)$ podemos construir un ángulo $\widehat{JAH}$ de medida $\frac{2\pi}{5}$ que es lo que necesitamos para construir el pentágono regular (el punto J resulta ser $(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5})$):



Trasladando la medida del ángulo por la circunferencia obtenemos los puntos J, L, M y K que con el $(1, 0)$ son los vértices de un pentágono regular.



Como antes, como sabemos bisecar ángulos, podemos construir cualquier polígono regular de $2^n.5$ lados para cualquier valor natural de n.

Como comentario, se sabe que

$$\cos(\frac{2\pi}{17}) = -\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

por lo que la construcción del polígono regular de 17 lados queda como inquietud para el que tenga mucha paciencia (vamos a justificar por qué es posible construirlo un poco más adelante).

4 De la geometría al álgebra

Los problemas planteados por los griegos no tuvieron respuesta por más de 2000 años, hasta que tuvieron una formulación algebraica.

Definición: Un número real se dice *construible* si es primera o segunda coordenada de un punto construible a partir del $(0,0)$ y del $(1,0)$.

Ya vimos ejemplos de puntos construibles por lo tanto sus coordenadas son números construibles (por ejemplo, $\frac{1}{2}$, $\frac{\sqrt{3}}{2}$). Es fácil ver a partir del lema anterior que un número x es construible si y sólo si $(x,0)$ es un punto construible si y sólo si $(0,x)$ es un punto construible.

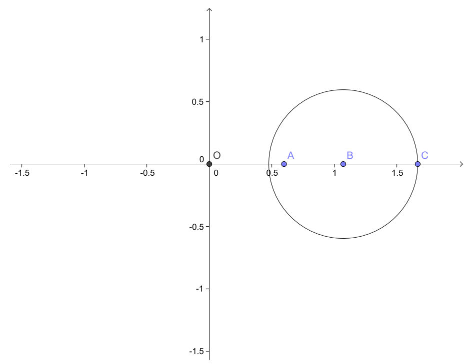
La propiedad algebraica importante que cumplen los números construibles es que forman un cuerpo con las operaciones usuales de los números reales:

Teorema: El conjunto $\mathcal{C} = \{x \in \mathbb{R} \mid x \text{ es un número construible}\}$ es un cuerpo con las operaciones usuales de los números reales. Además, si $x > 0$ es construible, entonces $\sqrt{x}$ también es construible (es decir, $\mathcal{C}$ es un cuerpo cerrado para raíces cuadradas de elementos positivos).

Demostración:
Para ver esto basta ver que $\mathcal{C}$ es cerrado para la suma y el producto, que es cerrado para el opuesto aditivo y el inverso multiplicativo, que tiene al 0 y al 1 (ya que las propiedades conmutativas, asociativas y distributivas se heredan de los números reales).

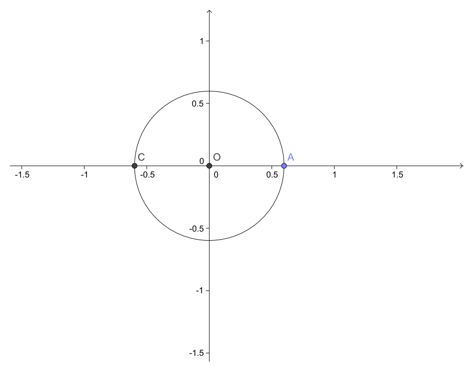
- $\mathcal{C}$ es cerrado para la suma:

  Supongamos que x e y están en $\mathcal{C}$. Esto quiere decir que $A = (x,0)$ $B = (y,0)$ son construibles. Pero trazando una circunferencia de radio $|\overline{AO}|$ con centro en B tendremos el punto $C = (x+y,0)$ sobre el eje de las abscisas (la figura muestra como hacerlo en el caso en que los dos sean positivos, pero es claro que se puede hacer en cualquier caso):



- $\mathcal{C}$ es cerrado para el opuesto aditivo:

  Si $A = (x, 0)$ es construible, $C = (-x, 0)$ es construible en un paso usando el compás:

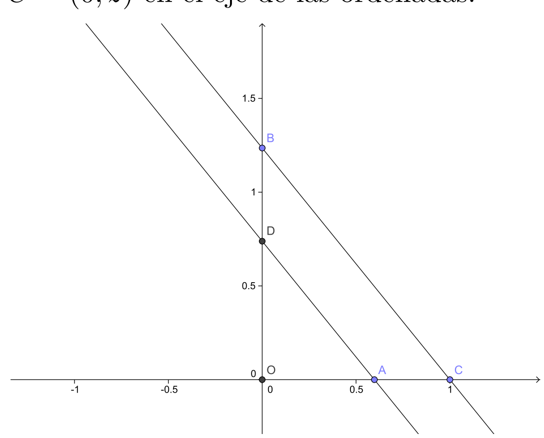


- $0 \in \mathcal{C}$:

  Trivial ya que el $(0, 0)$ es construible.

- $\mathcal{C}$ es cerrado para el producto:

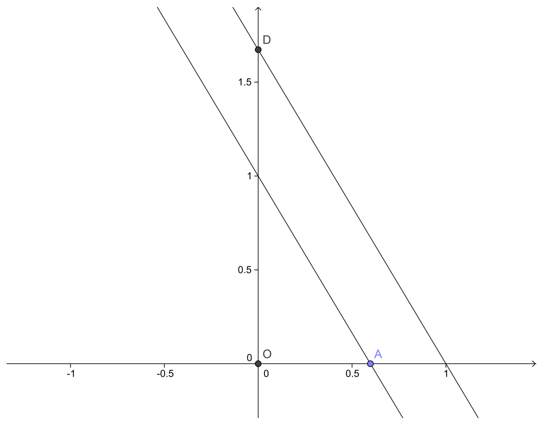
  Si x e y son construibles, $A = (x, 0)$ y $B = (0, y)$ son construibles. Los ubicamos en el plano. Unimos el punto B con el $(1, 0)$ y trazamos la paralela a esta recta por A obteniendo el punto $C = (0, z)$ en el eje de las ordenadas:



  Por semejanza de triángulos, se tiene que $\frac{y}{1} = \frac{z}{x}$ y por lo tanto, el número construible z es $x.y$

- $\mathcal{C}$ es cerrado para el inverso multiplicativo:

  Sea x un número construible no nulo, y sea $A = (x, 0)$. Unimos A con el punto $(0, 1)$ y trazamos la paralela a esta recta por el $(1, 0)$. Esta recta corta al eje de las ordenadas en el punto $D = (0, w)$.

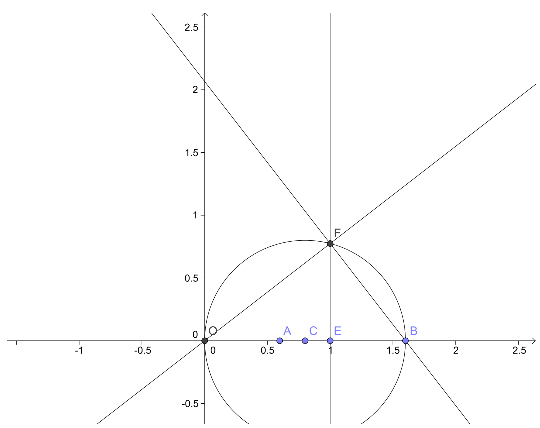
  De nuevo por semejanza de triángulos, $\frac{w}{1} = \frac{1}{x}$, es decir $w = x^{-1}$ es construible.

- $1 \in \mathcal{C}$:

  Trivial ya que el $(1, 0)$ es construible.

- $\mathcal{C}$ es cerrado para la raíz cuadrada:

  Sea x un número positivo construible. Entonces el punto $A = (x, 0)$ es construible. También por los ítems anteriores podemos construir $B = (x + 1, 0)$ y $C = (\frac{x+1}{2}, 0)$. Con centro en C trazamos la circunferencia de radio $\frac{x+1}{2}$. Trazamos la recta perpendicular al eje de las abscisas que pasa por el punto $E = (1, 0)$ y la intersección de esta recta con la circunferencia la llamamos $F = (1, z)$. La construcción obtenida es la siguiente:

  Usando Pitágoras tenemos que:

$$|\overline{FE}|^2 + |\overline{EO}|^2 = |\overline{FO}|^2 \qquad |\overline{FE}|^2 + |\overline{EB}|^2 = |\overline{FB}|^2$$

y sumando ambas identidades y volviendo a usar Pitgoras (notar que el ángulo $\widehat{OFE}$ es recto) tenemos que

$$2|\overline{FE}|^2 + |\overline{EO}|^2 + |\overline{EB}|^2 = (|\overline{EO}| + |\overline{EB}|)^2$$

con lo que

$$|\overline{FE}|^2 = |\overline{EO}|.|\overline{EB}|.$$

Usando que $|\overline{EO}| = 1$ y que $|\overline{EB}| = x$, tenemos
$z^2 = x$ y por lo tanto $z = \sqrt{x}$ es un número construible. □

Observaciones:

- Como 1 es construible y el conjunto de construibles es un cuerpo, cualquier elemento de $\mathbb{Q}$ es construible (sumando, restando, multiplicando y dividiendo, que son operaciones cerradas para los construibles).
- Cualquier raíz cuadrada de un elemento positivo de $\mathbb{Q}$ es construible.
- El número $\cos(\frac{2\pi}{17})$ antes mencionado es construible, ya que se obtiene a partir de números racionales y operaciones que son cerradas en $\mathcal{C}$. Por lo tanto, el polígono regular de 17 lados es construible con regla y compás, y también los de $2^n.17$ lados, para cualquier n natural.
- Un cuerpo ordenado que cumple que es cerrado para la raíz cuadrada de sus elementos positivos se llama *pitagórico* (por el hecho de que, si el cuerpo está incluido en $\mathbb{R}$, cualquier triángulo rectángulo que uno pueda construir con catetos con medidas en el cuerpo, la longitud de la hipotenusa también está en el cuerpo). Notar que $\mathbb{Q}$ no es pitagórico pero $\mathbb{R}$ y $\mathcal{C}$ sí lo son. Vamos a ver que estos dos cuerpos son distintos (una posible demostración para los que saben algo de cardinalidad se basa en que $\mathcal{C}$ es numerable y $\mathbb{R}$ no lo es) con lo cual se prueba que hay números reales no costruibles con regla y compás.

5 Un poco de teoría de cuerpos

Vamos a aprovechar que el conjunto $\mathcal{C}$ es un cuerpo para caracterizar de alguna forma los números construibles. Para eso, vamos a necesitar algunos resultados sobre cuerpos en general. Todos los cuerpos con los que vamos a trabajar incluyen a $\mathbb{Q}$ y están incluidos en $\mathbb{R}$. Sus operaciones son la suma y el producto que heredan de los números reales.

Definición Si K es un cuerpo, $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ y $\alpha \in \mathbb{R}$, se define el *cuerpo generado por* α *sobre* K y se nota $K(\alpha)$ al conjunto

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f,\ g \in K[X], g(\alpha) \neq 0 \right\}.$$

Es decir, tomamos todas las fracciones racionales a coeficientes en K y las evaluamos en α (siempre que el denominador no se anule en α). Este conjunto de números reales resulta ser un cuerpo con la suma y el producto usuales de $\mathbb{R}$.

Ejemplo
Supongamos que el cuerpo K es el de los números racionales y $\alpha = \sqrt{2}$. Entonces cualquier elemento de $\mathbb{Q}(\sqrt{2})$ es un cociente de polinomios a coeficientes en $\mathbb{Q}$ evaluado en $\sqrt{2}$:

$$\frac{a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + \cdots + a_n(\sqrt{2})^n}{b_0 + b_1\sqrt{2} + b_2(\sqrt{2})^2 + \cdots + b_m(\sqrt{2})^m}$$

pero teniendo en cuenta que $(\sqrt{2})^2 = 2$, podemos reagrupar los términos de potencia par y de potencia impar y obtenemos que el elemento es de la forma

$$\frac{c_0 + c_1\sqrt{2}}{d_0 + d_1\sqrt{2}}$$

con c_0, c_1, d_0 y d_1 racionales. Como el denominador es no nulo, podemos racionalizar y nos queda que

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a,\ b \in \mathbb{Q}\}$$

(comparar con los anillos que trabajamos en la primera parte del curso).

La notación $K(\alpha_0, \alpha_1, \ldots, \alpha_r)$ significará $K(\alpha_0)(\alpha_1)(\ldots)(\alpha_r)$, es decir, al cuerpo K primero le agregamos α_0, al cuerpo obtenido le agregamos α_1 y así sucesivamente.

En la situación que consideramos, si $\mathbb{Q} \subseteq K \subseteq E \subseteq \mathbb{R}$ y K y E son cuerpos con las operaciones que heredan de $\mathbb{R}$, E puede considerarse un espacio vectorial sobre K (tenemos la suma de elementos de E, sabemos multiplicar elementos de E por elementos de K y se cumplen todas las propiedades de espacio vectorial). A la dimensión de E como K-espacio vectorial la notaremos $\dim_K E$ para dejar claro sobre que cuerpo la estamos considerando.

Una propiedad de las dimensiones que vamos a usar es que, en cierto sentido, son multiplicativas:

Proposición 1. Si $K \subseteq E \subseteq F$ son tres cuerpos cuyas operaciones coinciden (es decir, K y E heredan sus operaciones de F) y $\dim_K E$ y $\dim_E F$ son finitas, entonces

$$\dim_K F = \dim_K E.\dim_E F.$$

Demostración: Lo que vamos a hacer es construirnos una base de F como K-espacio vectorial a partir de una base de F como E-espacio vectorial y de una base de E como K-espacio vectorial.

Supongamos que $B_1 = \{f_1, \ldots, f_n\}$ es una base de F como E-espacio vectorial (con lo cual, $\dim_E F = n$) y que $B_2 = \{e_1, \ldots, e_m\}$ es una base de E como K-espacio vectorial (con lo que $\dim_K E = m$). Veamos que el conjunto $B = \{f_i.e_j\}_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$ resulta ser una base (es decir, un sistema de generadores linealmente independiente) de F como K-espacio vectorial y, como su cardinal es $n.m$, la proposición quedaría probada.

Para esto vamos a ver primero que B es un sistema de generadores de F como K-espacio vectorial:

Sea $f \in F$. Como B_1 es base de F como E-espacio vectorial, en particular es un sistema de generadores y, por lo tanto, existen elementos $a_1, \ldots, a_n$ en E tales que $f = a_1.f_1 + \cdots + a_n.f_n$. Como cada a_i está en E (para $1 \leq i \leq n$) y B_2 es una base de E como K-espacio vectorial (en particular es un sistema de generadores) para cada a_i, existen $k_{i1}, \ldots, k_{im}$ tales que $a_i = k_{i1}e_1 + \cdots + k_{im}e_m$. Por lo tanto

$$f = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} k_{ij} e_j \right) f_i$$

que reagrupando y distribuyendo da

$$f = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} k_{ij}.(e_j.f_i)$$

con lo que cualquier elemento $f \in F$ se escribe como combinación lineal de B con coeficientes en K y, por lo tanto B resulta un sistema de generadores de F como K-espacio vectorial.

Ahora veamos que B es un conjunto linealmente independiente si tomamos coeficientes en K:

Supongamos que tenemos una combinación lineal de los elementos de B igualada a 0, es decir, $\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} k_{ij}.(e_j.f_i) = 0$ con $k_{ij} \in K$. Reordenando los términos y sacando factor común, $\sum_{1 \leq i \leq n} \left(\sum_{1 \leq j \leq m} k_{ij}.e_j \right).f_i = 0$. Como las sumas entre paréntesis son elementos en E y B_1 es una base de F como E-espacio vectorial (en particular es un conjunto linealmente independiente), entonces los elementos $\sum_{1 \leq j \leq m} k_{ij}.e_j$ deben dar 0 para cualquier índice i. Pero ahora usamos que B_2 es una base de E como K-espacio vectorial, y entonces cualquier combinación lineal de sus elementos a coeficientes en K igualada a 0 debe tener coeficientes nulos, con lo que $k_{ij} = 0 \; \forall i, j$, que es lo que queríamos probar. $\square$

Un último resultado de teoría de cuerpos que vamos a demostrar antes de volver a las construcciones con regla y compás es el siguiente:

Proposición 2. Sea $K \subseteq \mathbb{R}$ un cuerpo y sea $\alpha \in \mathbb{R}$ un elemento que es raíz de un polinomio mónico irreducible f sobre K de grado n. Entonces $\dim_K K(\alpha) = n$.

Demostración: Para probar este resultado sobre dimensión vamos a ver que el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ como K-espacio vectorial.

Veamos primero que es un sistema de generadores: Si $z \in K(\alpha)$, resulta que existen polinomios g y h en $K[X]$ tales que $h(\alpha) \neq 0$ y $z = \frac{g(\alpha)}{h(\alpha)}$.

Estudiemos un poco lo que pasa con el polinomio h: el máximo común divisor entre f y h debe ser un divisor mónico de f, que como es irreducible, sus únicos divisores mónicos son 1 y f. Si f dividiese a h, $h(\alpha)$ sería 0 (pues $f(\alpha) = 0$) y esto es un absurdo. Luego el máximo común divisor entre f y h es 1.
Usando el algoritmo de Euclides, 1 se escribe como combinación lineal de f y h, es decir, existen $u, v \in K[X]$ tales que $1 = u(X).f(X) + v(X).h(X)$. Si evaluamos esta igualdad en α, tenemos que $1 = v(\alpha).h(\alpha)$.

Por lo tanto, el elemento z que teníamos cumple

$$z = \frac{g(\alpha)}{h(\alpha)} = \frac{g(\alpha).v(\alpha)}{h(\alpha).v(\alpha)} = (g.v)(\alpha),$$

es decir, es un polinomio a coeficientes en $K[X]$ evaluado en α.
Tomemos ese polinomio y dividámoslo por f. Obtenemos un cociente q y un resto r, que es el polinomio nulo o tiene grado menor o igual que $n-1$ tales que

$$(g.v)(X) = f(X).q(X) + r(X)$$

y, si evaluamos esta identidad en α, obtenemos que

$$z = (g.v)(\alpha) = r(\alpha) = a_0.1 + a_1.\alpha + a_2.(\alpha)^2 + \cdots + a_{n-1}.(\alpha)^{n-1}$$

con $a_0, a_1, a_2 \ldots, a_{n-1} \in K$ con lo que probamos que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es un conjunto de generadores de $K[\alpha]$ como K-espacio vectorial.

Veamos ahora que este conjunto es linealmente independiente: Supongamos que

$$a_0.1 + a_1.\alpha + a_2.(\alpha)^2 + \cdots + a_{n-1}.(\alpha)^{n-1} = 0.$$

Entonces los polinomios f y $p = a_0.1 + a_1.X + a_2.(X)^2 + \cdots + a_{n-1}.(X)^{n-1}$ tienen a α como raíz común y, por lo tanto, α es raíz del máximo común divisor entre f y p, que no puede ser 1. Resulta entonces que este máximo común divisor es f, con lo cual f divide a p y, por una cuestión de grado, esto sólo puede pasar si p es el polinomio nulo. Esto demuestra que $a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0$ y, entonces, el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ resulta ser lineamente independiente, y por lo tanto, es una base de $K[\alpha]$ como K-espacio vectorial, como queríamos demostrar. $\square$

Ejemplo importante: Si tomamos $K = \mathbb{Q}$ y $\alpha = \sqrt[3]{2}$, resulta que α es raíz del polinomio $X^3 - 2$, que es irreducible en $\mathbb{Q}[X]$ por Einsestein. Por lo tanto $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$.

6 Los cuerpos y las construcciones

El paso fundamental para relacionar el álgebra con las construcciones con regla y compás es calcular las posibles dimensiones de los cuerpos que generan los números construibles:

Teorema. Sean $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ puntos construibles a partir del $(0, 0)$ y del $(0, 1)$ y sea (x, y) un punto construible en un paso a partir de ellos. Entonces

$$\dim_{\mathbb{Q}(x_1,y_1,x_2,y_2,\ldots,x_n,y_n)} \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)(x, y) \leq 2.$$

Demostración: El punto (x, y) se obtiene a partir de la intersección de dos rectas, una recta y una circunferencia o de dos circunferencias construibles a partir de los puntos dados.

- Intesección de dos rectas:

  Esto quiere decir que el punto (x, y) es solución de un sistema de ecuaciones

  $$\begin{cases} (y_i - y_j)(x - x_j) = (y - y_j)(x_i - x_j) \\ (y_k - y_\ell)(x - x_\ell) = (y - y_\ell)(x_k - x_\ell) \end{cases}$$

  pero entonces, resolviendo el sistema mediante despejes, x e y se obtienen sumando, restando, multiplicando y dividiendo elementos que ya están en el cuerpo, así que ellos ya están en $\mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$ y la dimensión que queremos calcular es 1 (recordar que la dimensión de un cuerpo sobre sí mismo es 1 pues el conjunto $\{1\}$ es una base).

- Intersección de una recta y de una circunferencia:

  Esto quiere decir que el punto (x, y) es solución de un sistema de ecuaciones

  $$\begin{cases} (y_i - y_j)(x - x_j) = (y - y_j)(x_i - x_j) \\ (y - y_\ell)^2 + (x - x_\ell)^2 = r^2 \end{cases}$$

  donde r^2 es un elemento de $\mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$ ya que es el cuadrado de la distancia entre dos puntos (x_h, y_h) y (x_k, y_k). Despejamos una variable de la ecuación de la recta (la que se pueda) y la reemplazamos en la de la circunferencia. Tenemos entonces que la otra variable satisface un polinomio de grado 2 con coeficientes en $\mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$ y la variable despejada está en el cuerpo generado por la otra sobre $\mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$. Luego, la dimensión que queremos calcular es, por la Proposición 2, a lo sumo dos.

- Intersección de dos circunferencias: reemplazando la ecuación de una circunferencia por la resta de las dos ecuaciones, tenemos la ecuación de una circunferencia y la de una recta, y entonces este caso se reduce al caso anterior. $\square$

Corolario 1. Sea $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ es una cadena de puntos construibles a partir del $(0, 0)$ y del $(1, 0)$ tales que (x_1, y_1) se construye en un paso a partir de ellos, (x_2, y_2) se construye en un paso a partir del $(0, 0)$, el $(1, 0)$ y el (x_1, y_1) y así sucesivamente. Entonces $\dim_{\mathbb{Q}} \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$ es una potencia de 2.

Demostración. Usando la Proposición 1 sobre la multiplicatividad de la dimensión, tenemos que

$$\dim_{\mathbb{Q}} \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n) =$$

$$= \dim_{\mathbb{Q}} \mathbb{Q}(x_1, y_1). \dim_{\mathbb{Q}(x_1,y_1)} \mathbb{Q}(x_1, y_1, x_2, y_2) \ldots \dim_{\mathbb{Q}(x_1,y_1,\ldots,x_{n-1},y_{n-1})} \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n)$$

y por el Teorema, cada uno de estos números es 1 ó 2, por lo que el producto es una potencia de 2. □

Corolario 2. Si x es un número construible $\dim_{\mathbb{Q}} \mathbb{Q}(x)$ es una potencia de 2.

Demostración. Si x es un número construible, $(x, 0)$ es un punto construible en un número finito de pasos, por lo que existen puntos $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, todos construibles en un paso a partir de los anteriores de forma tal que $(x, 0)$ se construye en un paso a partir de ellos. Luego, por el Corolario 1, $\dim_{\mathbb{Q}} \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n, x)$ es una potencia de 2. Ahora bien, usando nuevamente la multiplicatividad de la dimensión

$$\dim_{\mathbb{Q}} \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n, x) = \dim_{\mathbb{Q}} \mathbb{Q}(x). \dim_{\mathbb{Q}(x)} \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n, x)$$

por lo que $\dim_{\mathbb{Q}} \mathbb{Q}(x)$ es un divisor de una potencia de 2 y, por lo tanto, es una potencia de 2. □

7 Algunas respuestas

- **Resultado 1.** El cubo no puede duplicarse con regla y compás.

  Solución: Si tenemos un cubo cuyos lados miden 1 (el segmento que une el $(0, 0)$ y el $(1, 0)$, por ejemplo) y se pudiese duplicar su volumen, podríamos construir un lado de longitud $\sqrt[3]{2}$ y, por lo tanto, este número sería construible. Sin embargo, ya vimos que $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$ que no es una potencia de 2.

- **Resultado 2.** No se puede trisecar cualquier ángulo con regla y compás.

  Solución: Utilizando las fórmulas del coseno y del seno de la suma, se prueba fácilmente que
  $$\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha).$$
  Reemplazando $\alpha = \frac{\pi}{9}$, tenemos que
  $$4\cos^3(\frac{\pi}{9}) - 3\cos(\frac{\pi}{9}) - \frac{1}{2} = 0,$$
  es decir que el coseno del ángulo de $\frac{\pi}{9}$ es raíz del polinomio $f(X) = X^3 - \frac{3}{4}X - \frac{1}{8}$. Este polinomio es irreducible en $\mathbb{Q}[X]$ ya que tiene grado 3 y se puede ver que no tiene raíces en $\mathbb{Q}$ usando Gauss con el polinomio $8.f$. Si el ángulo de $\frac{\pi}{3}$ (que ya construimos cuando dibujamos el hexágono regular) se pudiese trisecar, podríamos dibujar el punto $(\cos(\frac{\pi}{9}), \sin(\frac{\pi}{9}))$ y el número $\cos(\frac{\pi}{9})$ sería construible, pero como es raíz de un polinomio irreducible de grado 3, resulta que $\dim_{\mathbb{Q}} \mathbb{Q}(\cos(\frac{\pi}{9})) = 3$ que no es una potencia de 2, lo que es un absurdo. Luego, el ángulo $\frac{\pi}{3}$ no se puede trisecar. (Notar que esto implica que no se puede construir un polígono regular de 18 lados con regla y compás.)

- **Resultado 3.** No se puede cuadrar un círculo con regla y compás.

  Solución: Si se pudiese cuadrar un círculo de radio 1, tendríamos que poder construir un cuadrado con un lado de longitud $\sqrt{\pi}$ y, por lo tanto, π sería construible. Si esto fuese cierto, $\dim_{\mathbb{Q}} \mathbb{Q}(\pi)$ sería una potencia de 2. Sin embargo, Lindemann probó en 1882 que $\dim_{\mathbb{Q}} \mathbb{Q}(\pi) = \infty$ o, lo que es lo mismo, que π es trascendente (esta demostración se escapa al contenido del curso).

- **Resultado 4** El heptágono regular no se puede construir con regla y compás.

  Solución: Vamos a proceder en forma similar a como lo hicimos con el pentágono regular.

  Consideremos el número complejo $\tau = \cos(\frac{2\pi}{7}) + i\sin(\frac{2\pi}{7})$. Por el mismo razonamiento que hicimos antes, tenemos que

  $$\tau^6 + \tau^5 + \tau^4 + \tau^3 + \tau^2 + \tau + 1 = 0.$$

  Sacando τ^3 factor común, tenemos que

  $$0 = \tau^3 + \tau^2 + \tau + 1 + \tau^{-1} + \tau^{-2} + \tau^{-3} = (\tau + \tau^{-1})^3 + (\tau + \tau^{-1})^2 - 2(\tau + \tau^{-1}) - 1,$$

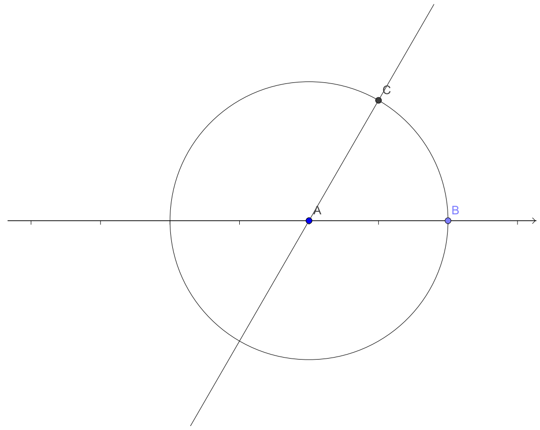
  pero $(\tau + \tau^{-1}) = 2\cos(\frac{2\pi}{7})$ resulta ser raíz del polinomio $X^3 + X^2 - 2X - 1$, que es irreducible en $\mathbb{Q}[X]$. Luego, $\dim_{\mathbb{Q}} \mathbb{Q}(2\cos(\frac{2\pi}{7})) = 3$ que no es una potencia de 2. Por lo tanto, el número $2\cos(\frac{2\pi}{7})$ no es construible con regla y compás y, entonces, $\cos(\frac{2\pi}{7})$ tampoco lo es, con lo que el heptágono regular no es construible.

Comentario: Se sabe que un polígono regular de n lados es construible con regla y compás si y sólo si la descomposiciónn en factores primos de n es de la forma $n = 2^j.p_1 \ldots p_r$, donde $j \in \mathbb{N}_0$ y cada p_i es un primo distinto de la forma $2^{2^{k_i}} + 1$ (a estos primos se los llama primos de Fermat). Una de las implicaciones de este teorema fue probada por Gauss y la otra fue demostrada por Pierre Wantzel (este último fue el primero en dar una prueba rigurosa de la imposibilidad de trisecar un ángulo y de duplicar un cubo). La demostración de este teorema se escapa a los alcances del curso.

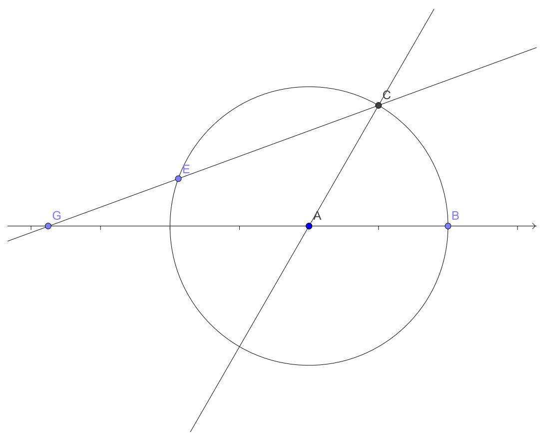
8 Como trisecar un ángulo con regla *marcada* y compás

Suponemos ahora que tenemos un compás y una regla *con una medida fija marcada*. No interesa cuánto mide el segmento marcado en la regla, sino que podamos usarlo como radio de una circunferencia o que podamos hacerlo coincidir con dos puntos. Trisequemos ahora un ángulo cualquiera.

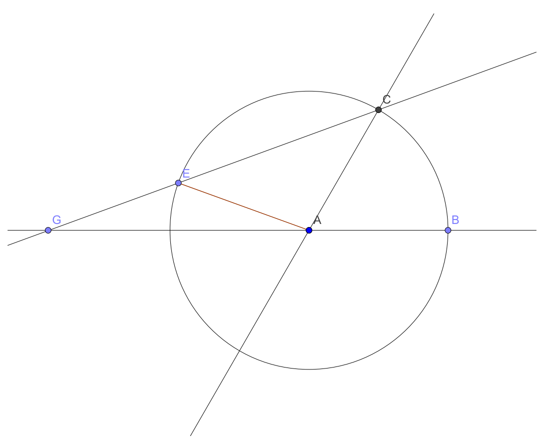
Dado el ángulo $\widehat{CAB}$, dibujemos una circunferencia con centro en el vértice y radio igual a la medida en la regla que llamaremos $r = |\overline{AB}|$.



Ahora, hacemos pasar la regla por C de forma tal que las marcas a distancia r se ubiquen una sobre la circunferencia y la otra sobre la recta $\overline{AB}$ (y así obtenemos los puntos E y G, que están a distancia r).



Unimos los vértices A y E para obtener la figura de análisis.



Notar que los triángulos AEG y EAC son isósceles, ya que cada uno tiene dos lados que miden r.
Consideremos ahora la siguiente identidad:

$$\widehat{BAC} + \widehat{CAE} + \widehat{EAG} = \pi.$$

Entonces

$$\widehat{BAC} + (\pi - 2(\widehat{CEA})) + \widehat{EAG} = \pi$$

y luego

$$\widehat{BAC} - 2(\widehat{CEA}) + \widehat{EAG} = 0.$$

Pero $\widehat{CEA} = 2(\widehat{EAG})$, con lo que

$$\widehat{BAC} - 3\widehat{EAG} = 0$$

lo que demuestra que el ángulo $\widehat{EAG}$ es exactamente un tercio del ángulo original $\widehat{BAC}$ (es decir, trisecamos el ángulo original usando compás y una regla con una medida fija marcada).