CONSTRUCCIONES CON REGLA Y COMPAS

Enzo R. Gentile

Sea $\mathbb{R}^2$ el plano de la geometría analítica, consideraremos ciertas operaciones sobre $\mathbb{R}^2$:

a) dados dos puntos distintos de $\mathbb{R}^2$ podemos trazar una recta que los una.

b) dada una recta podemos marcar dos puntos sobre la misma y considerar el segmento por ellos determinado.

c) dado un punto podemos construir una circunferencia de centro en ese punto y radio determinado según (b).

d) determinar puntos como intersecciones de: a) dos rectas, b) rectas y circunferencia, c) dos circunferencias.

Fijados a), b), c) y d) veamos algunos tipos de construcciones que podemos hacer.

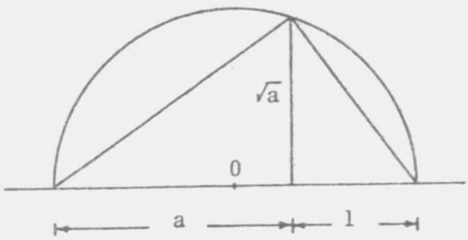
i) Dado una recta r y un punto A, podemos trazar una recta r' perpendicular a r por A. En efecto, con centro en A trazamos una circunferencia de radio suficientemente grande. Esta corta a r en B y B'. Haciendo centro en B trazamos una circunferencia de radio BB' y haciendo centro en B' trazamos una circunferencia de radio también BB'. Las mismas se intersectan en C y C'. La recta determinada por C y C' tiene las propiedades pedidas.

ii) Dada una recta y un punto exterior a la misma, podemos trazar una paralela a la misma que pase por ese punto. Dejamos su construcción a cargo del lector.

iii) Podemos trisecar el ángulo recto.

Consideramos a $\mathbb{R}^2$ como la totalidad de pares ordenados (a,b) de números reales. Diremos que un número *real* a es *construible* (siempre debe entenderse con regla y compás) si el punto $(a,0)$ es construible, a partir de segmentos construibles. Por ejemplo, el segmento $(0,0)(1,0)$ es construible, por definición. Por lo tanto, el punto $(1,0)$ es construible. A partir de él lo serán $(2,0)$, $(3,0)$, ..., $(-1,0)$, $(-2,0)$, ... es decir, un conjunto equivalente a los enteros. En efecto, con centro en $(1,0)$ y radio igual al segmento $(0,0)(1,0)$ trazo una circunferencia. La misma intersecta a la recta $(x,0)$, $x \in \mathbb{R}$ en los puntos $(0,0)$ y $(2,0)$. Así queda construido $(2,0)$. Análogamente consideramos los puntos construibles de la forma $(0,b)$. En general, el punto (a,b) es construible si y sólo si $(a,0)$ y $(0,b)$ son construibles.

Identificando a $\mathbb{R}^2$ con el cuerpo complejo podemos referirnos a números complejos construibles con regla y compás. En general, si a y b son números complejos construibles, entonces $a+b$ y $a-b$ son también construibles. Utilizando el teorema de Thales de la geometría elemental, se puede probar que si a y b son números reales construibles, entonces $a.b$ y a/b $(b \neq 0)$ son construibles (para más detalles véase el artículo de Elsa Malisani en este número). En definitiva el conjunto de números complejos construibles es, con respecto a la suma y el producto ordinarios un cuerpo K, el *cuerpo de los números construibles*. Este cuerpo K, tiene una propiedad importante, a saber: si $u \in K$, entonces $\sqrt{u} \in K$. Es decir, K es cerrado respecto de tomar raíces cuadradas. En efecto, esto está probado en la construcción siguiente, cuya justificación se deja a cargo del lector.



Un número complejo $a+bi$ es construible, si así lo es el punto (a,b) de $\mathbb{R}^2$. La teoría de Galois permitió resolver casi simultáneamente varios problemas famosos de geometría. Por ejemplo, los referentes a:

i) Duplicación del cubo (construir un cubo de volumen doble a un cubo dado, por ejemplo dado un cubo de lado 1, construir un cubo de volumen igual a 2. Esto equivale a poder construir con regla y compás el número real $\sqrt[3]{2}$, que es una solución de la ecuación $X^3 - 2 = 0$).

ii) Trisección del ángulo, con regla y compás.

iii) Construcción con regla y compás del polígono regular de n lados.

Veamos en qué propiedades algebraicas se traduce la propiedad de ser construible con regla y compás. La ecuación de una recta en $\mathbb{R}^2$ es,

$$aX + bY + c = 0$$

y la ecuación de la circunferencia de centro (a_1,b_1) y que pasa por (a_2,b_2) es,

$$(X-a_1)^2 + (Y-b_1)^2 = (a_2-a_1)^2 + (b_2-b_1)^2 = r^2$$

o también

$$X^2 + Y^2 - 2a_1X - 2b_1Y + c_1 = 0$$

si $c_1 = a_1^2 + b_1^2 - r^2$.

Un punto $(x,y) \in \mathbb{R}^2$ será construible si y sólo si es solución de algunos de los sistemas siguientes:

$$\text{(I)} \quad \begin{aligned} a_1X + b_1Y + c_1 &= 0 \\ a_2X + b_2Y + c_2 &= 0 \end{aligned}$$

$$\text{(II)} \quad \begin{aligned} a_1X + b_1Y + c_1 &= 0 \\ X^2 + Y^2 - 2a_2X - 2b_2Y + c_2 &= 0 \end{aligned}$$

$$\text{(III)} \quad \begin{aligned} X^2 + Y^2 - 2a_1X - 2b_1Y + c_1 &= 0 \\ X^2 + Y^2 - 2a_2X - 2b_2Y + c_2 &= 0 \end{aligned}$$

donde los coeficientes $a_1, b_1, c_1, \ldots$ son números reales construibles. En efecto, nuestra afirmación es equivalente a determinar un punto en R^2 como intersección de dos rectas o de recta y circunferencia o de dos circunferencias. En cualquiera de los casos se trata de resolver ecuaciones en *una indeterminada de grado a lo sumo* 2. En el caso (I), si las rectas no son paralelas (único caso que interesa) es $d = a_1b_2 - a_2b_1 \neq 0$ y por lo tanto la solución es (x,y) con,

$$x = (b_2c_1 - b_1c_2)/d \quad , \quad y = (a_2c_1 - a_1c_2)/d \quad .$$

En el caso (II), si (por ejemplo) $a_1 \neq 0$ despejando formalmente X en la primera ecuación y reemplazando en la segunda ecuación se obtiene una ecuación de segundo grado en Y, cuyas soluciones y_1, y_2 (reales o imaginarias) reemplazadas en la primera ecuación, darán soluciones

x_1, x_2 respectivamente. En el caso (III), "restando" las ecuaciones resulta

$$(*) \qquad 2(a_2 - a_1)X - 2(b_2 - b_1)Y + c_1 - c_2 = 0$$

que es la ecuación de la recta que une los puntos de intersección de las dos circunferencias, supuesto que dichas circunferencias son distintas y tienen intersección no vacía (único caso que geométricamente interesa). Resolviendo el sistema formado por (*) y una de las ecuaciones de (III), se obtiene la solución de (III).

En resumen: *un número real es construible con regla y compás si y sólo si es solución de una ecuación algebraica con coeficientes construibles, de grado a lo sumo 2.*

Un número complejo será construible con regla y compás si y sólo si sus componentes (real e imaginaria) son construibles.

Las construcciones geométricas traducidas al lenguaje analítico o algebraico equivalen a determinar números a partir de los números racionales, por las operaciones racionales y la extracción de raíces cuadradas. Podemos definir entonces para cada número construible, el *número mínimo* de ecuaciones cuadráticas *irreducibles* necesarias para obtener al mismo a partir del cuerpo Q o también, el *número mínimo* de raíces cuadradas que son suficientes para obtener el número. Se debe entender que las raíces cuadradas que se consideran son propias, no consideramos raíces cuadradas del tipo $\sqrt{a^2} = \pm a$. Cuando hablamos de ecuaciones irreducibles $f(X) = 0$, con $f(X)$ un polinomio, entendemos que el polinomio $f(X)$ es irreducible sobre el cuerpo en cuestión.

Llamaremos grado de un número construible al número que acabamos de definir. Así, si $\alpha \in Q$ diremos que α tiene grado 0. Si α es solución de una ecuación $X^2 + rX + s = 0$ irreducible, con r y s racionales, entonces α es de grado 1. En general, un número α tiene grado $n > 1$ si y sólo si es solución de una ecuación cuadrática irreducible $X^2 + rX + s = 0$ donde r y s son números construibles de grado menor que n, pero uno al menos tiene grado $n-1$.

Nota: Para el lector conocedor de un poco de la Teoría de Cuerpos un número α tiene grado n si y sólo si α pertenece a un cuerpo extensión de Q obtenido efectuando n adjunciones de raíces cuadradas,

$$Q = K_0 \subset K_1 = K_0(\sqrt{a_1}) \subset K_2 = K_1(\sqrt{a_2}) \subset \ldots \subset K_n = K_{n-1}(\sqrt{a_n})$$

con $\alpha \in K_n$ y $\alpha \notin K_j$, $j < n$. Cada adjunción $K(\sqrt{a})$, donde $\sqrt{a} \notin K$, significa formar la totalidad,

$$(*) \qquad K(\sqrt{a}) = \{r + s\sqrt{a} : r,s \in K\} \quad .$$

El valor $\sqrt{a}$ debe entenderse una raíz cuadrada en $\mathbb{C}$, del número a. En la situación (*), $K(\sqrt{a})$ es un cuerpo, *la extensión cuadrática* de K obtenida adjuntando $\sqrt{a}$. Observar que si α es un número construible de grado n entonces $-\alpha$ y $1/\alpha$ son construibles y tienen también grado n.

Construcción del polígono regular de n lados.

Se trata de hallar todas las soluciones de la ecuación $X^n - 1 = 0$, mediante las operaciones racionales y la extracción de raíces cuadradas. El problema se reduce a considerar sólo los valores de n que son primos positivos (por qué?). Sea pues $n = p$ primo positivo. Dado que,

$$X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

es suficiente construir una solución de la ecuación

$$X^{p-1} + \ldots + X + 1 = 0 .$$

El polinomio $\theta_p(X) = X^{p-1} + \ldots + X + 1$ se denomina, *polinomio ciclotómico* de orden p y es bien sabido que es *irreducible* sobre Q (*Ciclotomía* significa partición de la circunferencia). Para que la solución sea factible con regla y compás debemos hallarla, como ya se dijo, por sucesivas resoluciones de ecuaciones cuadráticas. Veamos algunos ejemplos,

1. Construcción del triángulo equilátero $(p = 3)$.

Debemos considerar la ecuación $X^2 + X + 1 = 0$. La solución es bien conocida, $(-1 + i\sqrt{3})/2$ y $(-1 - i\sqrt{3})/2$. Geométricamente se construye con regla y compás un segmento de longitud $-1/2$ sobre el eje horizontal, otro de longitud $\sqrt{3}/2$ sobre el eje vertical. El punto del plano con esas coordenadas es un vértice del triángulo equilátero. En forma análoga se obtiene el otro, que junto con 1 nos da los tres vértices buscados.

2. Pentágono Regular $(p = 5)$.

Debemos considerar la ecuación,

$$\theta_5(X) = X^4 + X^3 + X^2 + X + 1 = 0 .$$

Operando algebraicamente se obtiene

$$\theta_5(X) = X^2(X^2 + X + 1 + X^{-1} + X^{-2}) = X^2[(X + X^{-1})^2 + (X + X^{-1}) - 1]$$

y llamando $Y = X + X^{-1}$ se obtiene la ecuación cuadrática

$$Y^2 + Y + 1 = 0$$

cuyas soluciones son

$$a_1 = (-1 + \sqrt{5})/2 \qquad y \qquad a_2 = (-1 - \sqrt{5})/2 \ .$$

Escribiendo $a_1 = X + X^{-1}$ resulta la ecuación cuadrática

$$X^2 - a_1X + 1 = 0$$

con coeficientes "construibles", resultando soluciones

$$(a_1 + \sqrt{a_1^2 - 4})/2 \qquad y \qquad (a_1 - \sqrt{a_1^2 - 4})/2 \ .$$

Utilizando a_2 se obtienen otras dos soluciones que junto con 1 dan los cinco vértices buscados. Véase el artículo de Elsa Malisani en este número para más detalles sobre la construcción del pentágono y decágono regular.

3. Construcción del Heptágono regular (p = 7).

Se trata de resolver por "cuadraturas" la ecuación $\theta_7(X) = 0$. Podemos proceder en forma análoga y escribir,

$$\theta_7(X) = X^3(X^3 + X^2 + X + 1 + X^{-1} + X^{-2} + X^{-3})$$

y llamando $Y = X + X^{-1}$ habrá que proceder a resolver la ecuación $Y^3 + Y^2 - 2Y - 1 = 0$. Notemos que el polinomio en Y hallado es irreducible sobre Q . En efecto, tratándose de un polinomio de tercer grado es suficiente investigar la existencia de raíces en Q. Por el Teorema de Gauss las posibles raíces son los enteros que dividen a 1 , o sea 1 ó -1 . Como ninguno de estos valores es raíz, queda probada la irreducibilidad de $Y^3 + Y^2 - 2Y - 1$. Siendo este polinomio irreducible estamos bloqueados por esta vía a los fines de la construcción con regla y compás que, como sabemos, involucra sólo ecuaciones de grado 1 ó 2 y no irreducibles de mayor grado.

Supongamos que el problema de la construcción del heptágono regular sea posible. Es decir, podemos construir una solución de $\theta_7(X) = 0$ por cuadraturas. Se sigue que también tendremos una solución α de $Y^3 + Y^2 - 2Y - 1 = 0$ por cuadraturas. Esto nos llevará a un absurdo que implicará la imposibilidad de construir el heptágono regular con regla y compás. El número α satisface entonces dos ecuaciones

$$Y^3 + Y^2 - 2Y - 1 = 0$$

y

$$Y^2 + rY + s = 0$$

con r y s números construibles de grado menor al grado de α . Se tiene

$$\alpha^3 = -\alpha^2 + 2\alpha + 1$$

$$\alpha^3 = -r\alpha^2 - s\alpha$$

o sea

$$(1 - r)\alpha^2 - (2 + s)\alpha - 1 = 0$$

y como $1 - r \neq 0$ (por razones de grado!) resulta la ecuación,

$$\alpha^2 - \left(\frac{2+s}{1-r}\right)\alpha - \frac{1}{1-r} = 0 \quad .$$

Puesto que la ecuación $Y^2 + rY + s = 0$ es irreducible se debe verificar que,

$$r = -\frac{2+s}{1-r} \qquad y \qquad s = \frac{-1}{1-r} \quad .$$

Operando (y omitimos los detalles) resulta la siguiente ecuación satisfecha por r,

$$r^3 - 2r^2 - r + 1 = 0 \ .$$

Notemos que r es un número construible de grado menor que α. se sigue de la ecuación precedente que $-r^{-1}$ satisface la ecuación "original",

$$Y^3 + Y^2 - 2Y - 1 = 0 \ .$$

En efecto,

$$\begin{aligned} -r^{-3} + r^{-2} + 2r^{-1} - 1 &= r^{-3}(-r^3 + 2r^2 + r - 1) \\ &= -r^{-3}(r^3 - 2r^2 - r + 1) \\ &= 0 \end{aligned}$$

Hemos probado entonces que la ecuación $Y^3 + Y^2 - 2Y - 1 = 0$ admite una solución que es un número construible de grado menor al grado de α. Iterando este proceso logramos "por descenso" que la ecuación tiene finalmente solución en $\mathbf{Q}$, cosa imposible, pues esta ecuación, vimos, es irreducible sobre $\mathbf{Q}$. Hemos pues probado la imposibilidad de construir con regla y compás el heptágono regular. El mismo razonamiento prueba la imposibilidad de "duplicar el cubo", pues se trata de resolver la ecuación $X^3 - 2 = 0$, que es irreducible sobre $\mathbf{Q}$. A manera de ejercicio el lector puede mostrar la imposibilidad de trisecar el ángulo de 60 grados, o sea de construir con regla y compás un ángulo de 20 grados. En este caso se hace uso de la ecuación

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

que para $\theta = 20°$ toma la forma

$$8 \cos^3 20° - 6 \cos 20° - 1 = 0$$

y escribiendo $X = 2 \cos\theta$ resulta la ecuación,

$$X^3 - 3X - 1 = 0 .$$

Este polinomio es irreducible sobre $\mathbb{Q}$ como el lector puede probar y el razonamiento sigue las líneas trazadas en el caso del heptágono regular.

El resultado de mayor trascendencia sobre construcciones de polígonos regulares es debido a C.F. Gauss (1777-1855). Se refiere a la posibilidad de construir el polígono regular de 17 lados con regla y compás y en general, de los polígonos regulares con un número primo p de lados para los p de la forma

$$p = 2^{2^n} + 1$$

llamados primos de Fermat (P. de Fermat 1601-1665). El resultado final es el siguiente:

<u>Teorema</u>. El polígono regular de n lados es construible con regla y compás si y sólo si n es de la forma

$$n = 2^s p_1 \dots p_r$$

con s natural ó cero y los p_i son primos de Fermat, distintos dos a dos.

Nota final. Puesto que hay sólo 5 primos de Fermat conocidos hasta el presente, a saber

$$2^{2^n} + 1 \quad \text{con} \quad n = 0, 1, 2, 3, 4$$

se sigue que hay sólo 31 polígonos regulares con un número impar de lados que son construibles con regla y compás. Se ignora si existen infinitos primos de Fermat. ((Se cree que hay sólo un número finito, por un razonamiento de tipo eurístico. En efecto, si existieran infinitos primos de Fermat, significaría que Fermat habría tenido infinitos tíos. Por lo tanto su madre o su padre habría tenido infinitos hermanos. Pero para tener infinitos hermanos es necesario tener infinitas madres. Pero esto es un absurdo pues: Madre hay una sola! Otro argumento, debido a Jarvis, parece más convincente. Jarvis dice mucho más, dice que no hay primos de Fermat, pues por razones de edad estarían ya todos muertos!)).

Facultad de Ciencias Exactas y Naturales,
Ciudad Universitaria
(1428) Núñez, Buenos Aires.

Escuchado en medios de comunicación:

"Tan chico como 000000000,1".

"La política dió un giro de 360 grados".