Construcciones con regla y compás.

Rafael Potrie

15 de noviembre de 2006

1. Introducción

Mi intención es presentar de forma casi autocontenida[1] la demostración de que no se puede trisecar el ángulo de 60º ni se puede duplicar el volumen de un cubo con regla y compás (la demostración también sirve para probar que no se puede hallar la cuadratura de un círculo, si se asume la trasendencia del número π). Estos problemas de construcción de magnitudes mediante el uso de regla y compás se remontan a la época de los griegos (quienes no llegaron a conocer la respuesta) que consideraban que las únicas magnitudes existentes eran las que podían ser construidas.

Lo más sorprendente es la sencillez de la prueba, que la hace una de las demostraciones más bellas que conozco en matemáticas[2].

La idea de la prueba es tan buena que parece que los problemas de trisección de un ángulo y duplicación del volúmen de un cubo fueron pensados una vez conocida la respuesta (cosa que como fue comentado no fue así).

El resultado que permite probar estos resultados es el siguiente:

Teorema 1. *Las magnitudes constructibles son las que son raíz de un polinomio irreducible con coeficientes en $\mathbb{Q}$ de grado 2^n.*

Decimos que un polinomio es irreducible en $\mathbb{Q}$ si no se puede escribir como producto de dos polinomios con coeficientes en $\mathbb{Q}$ de grado mayor o igual a 1. Ejemplos de polinomios irreducibles en $\mathbb{Q}$ son, por ejemplo, los polinomios de grado 1 (si multiplicamos dos polinomios de grado mayor o igual a 1 el resultado será un polinomio de grado mayor o igual a 2). Otro ejemplo puede ser $x^2 - 2$ que sabemos que se escribe como $(x - \sqrt{2})(x + \sqrt{2})$ por lo que no sería irreducible en $\mathbb{R}$, pero si lo es en $\mathbb{Q}$ pues $\sqrt{2} \notin \mathbb{Q}$ y como las raices de $x^2 - 2$ son efectivamente $\pm\sqrt{2}$ no puede ser escrito como producto de dos polinomios de grado 1 con coeficientes en $\mathbb{Q}$ (observar que los polinomios de grado 1 en $\mathbb{Q}$ tienen raices en $\mathbb{Q}$).

Vamos a ver como este teorema implica los resultados mencionados. Para eso, vamos a utilizar un resultado de Álgebra que nos dice que dado un número (llamemosle u) que es raíz de un polinomio irreducible en $\mathbb{Q}$ de grado n entonces todo polinomio irreducible que se anula en u , tiene grado n. Eso se puede ver considerando el conjunto de todos los polinomios con coeficientes en $\mathbb{Q}$ que se anulan en dicho número y tomando uno de grado mínimo (digamos f). Este será irreducible (pues si se escribiese como producto de dos, uno de ellos tendría que anularse en u y tendría grado menor) y además cualquier otro polinomio (llamemosle g) que se anule en u que no sea del mismo grado no podrá ser irreducible (pues podriamos escribir utilizando el algoritmo de división de Euclides a $g = qf + r$ con r polinomio de grado menor que f, pero como f y g se anulan en u, r también debería anularse y por lo tanto, como f era de grado mínimo, $r = 0$)[3].

1.0.1. Duplicación del volumen de un cubo

Este problema consiste en hallar la arista de un cubo cuyo volumen sea el doble de uno cuya arista es conocida (y puede ser construida). En particular, podemos considerar el problema de construir la arista de un cubo con volumen 2([4]). Recordemos que el volúmen de un cubo es a^3 donde a es la longitud de la arista. Por lo tanto, buscamos que $a^3 = 2$ por lo que la arista que buscamos construir ha de ser raiz del polinomio $a^3 - 2$ que es irreducible en $\mathbb{Q}$ pues tiene como raices $\sqrt[3]{2}$ y dos complejas conjugadas que ninguna está en $\mathbb{Q}$ por lo tanto, como la forma de escribir un polinomio de grado 3 como producto de dos con grado mayor o igual a 1 es que uno tenga grado 2 y otro grado 1, no puede ser reducido ya que el de grado 1 tendría una raíz en $\mathbb{Q}$.

[1] En principio los requisitos para entender la prueba son: Polinomios, Teorema de Thales, Numeros Complejos y Espacios vectoriales. Un estudiante que haya finalizado el primer semestre de la carrera de Matemáticas o Ingeniería debería estar en condiciones de comprender la demostración. Por sugerencias mandenme un mail a rpotrie@fing.edu.uy .

[2] Lamentablemente no se a quien se debe la prueba. Me han dicho (aunque no lo puedo asegurar) que le pertenece a Galois.

[3] Gracias al Sambita por esta prueba.

[4] Claramente las unidades son arbitrarias, pero una vez fijado que la arista de uno vale 1 debemos de ser coherentes con esta elección

Esto implica que no podemos construir $\sqrt[3]{2}$ ya que no anula un polinomio irreducible de grado 2^n (recordar que el grado del polinomio irreducible que un número anula está bien definido y es único).

1.0.2. Trisección de un ángulo

Está claro que con regla y compaz es posible construir un ángulo de 60^o (basta construir un triángulo equilatero para obtener dicho ángulo). Vamos a probar que no es posible construir uno de 20^o lo que imposibilita trisecar el ángulo de 60^o.

Si pudiesemos construir el ángulo de 20^o, podriamos construir la magnitud $\cos(20^o)$ (basta construir el ángulo de 20^o como en la figura 1, tomar una logitud de 1 en la "hipotenuza" y luego construir un segmento AB como se ve en la figura, el punto medio distará $\cos(20^o)$ del vértice del ángulo [5]).

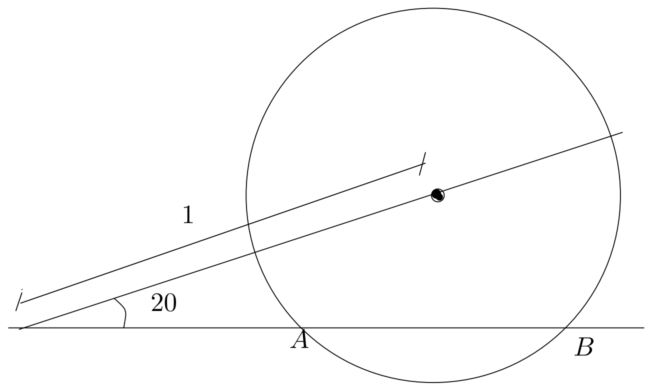

Figura 1: Construir $cos(20^o)$.

Para ver que no se puede construir $\cos(20^o)$ observemos que vale lo siguiente para un ángulo α cualquiera [6]:

$$\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$$

Tomando $\alpha = 20^o$, tenemos $\cos(3\alpha) = \cos(60^o) = \frac{1}{2}$ y por lo tanto se cumple que $\cos(20^o)$ es raíz de

$$\frac{1}{2} = 4x^3 - 3x$$

y como el polinomio $8x^3 - 6x - 1$ es irreducible [7] concluimos que no se puede trisecar el ángulo de 60^o.

1.0.3. Cuadratura del círculo

Este problema consiste en hallar un cuadrado cuyo perimetro sea el misma que el de un círculo dado. Por lo tanto, es equivalente a construir un lado a que verifique que $4a = 2\pi R$ donde R es el radio del círculo. Considerando el círculo de radio 1 tenemos que a tiene que verificar $a = \frac{\pi}{2}$. Es fácil ver que esto no puede ser construido pues no existe ningún polinomio con coeficientes en $\mathbb{Q}$ que se anule en $\frac{\pi}{2}$ [8].

2. Demostración del Teorema

La demostración se divide en dos pasos muy simples.

Primero, utilizando el teorema de Thales se puede probar que el conjunto de puntos que se pueden construir en el plano es un subcuerpo de los complejos $\mathbb{C}$. Esto quiere decir que, con las operaciones de los complejos, este conjunto es cerrado. Esto es equivalente a decir que si tomamos dos puntos constructibles u, v entonces, podemos construir los puntos $u - v$ y $\frac{u}{v}$.

[5] Se puede construir la mediatriz del segmento AB y se tendrá un triángulo rectángulo con un ángulo de 20^o e hipotenuza de longitud 1, por lo tanto, uno de los catetos medirá $\cos(20^o)$.

[6] Esto se demuestra utilizando las exponenciales complejas.

[7] Es fácil ver que las raices no pueden ser racionales recordando que las raices racionales de un polinomio tienen que ser de la forma $\frac{a}{b}$ con a dividiendo al término independiente y b dividiendo al coeficiente de mayor grado. En este caso, las posibles raices racionales serían $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ que no verifican.

[8] Una prueba de que π es trascendente se puede encontrar en el libro *Álgebra* de S.Lang.

Una vez conseguido esto, se observa que todo punto constructible es intersección de rectas y circunferencias, por lo tanto, solución de un polinomio de grado 2 con coeficientes en el cuerpo de los puntos que se pueden construir. Como el proceso de construcción es finito, se llega a la conclusión.

El primer paso requiere únicamente conocer la definición de cuerpo y recordar el Teorema de Thales. La segunda, sin embargo, hace uso de la noción de espacio vectorial[9].

2.0.4. Los constructibles son un cuerpo

Primero veamos un poco que elementos podemos construir.

Recordemos que siempre podemos construir la recta perpendicular a una recta dada (r) por un punto cualquiera (p). Para hacer eso, basta tomar una circunferencia centrada en p que corte la recta r en 2 puntos, A y B. La mediatriz[10] y del segmento $\overline{AB}$ será efectivamente una recta perpendicular a r (pues $\overline{AB} \subset r$) y pasará por p pues equidista de A y B. Vease la figura 2.

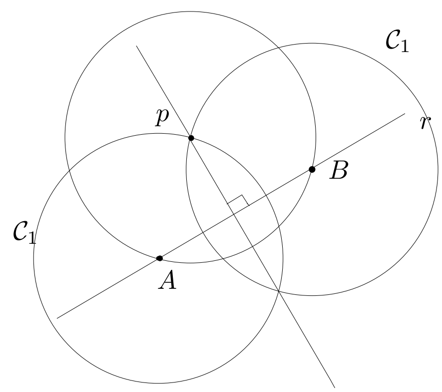

Figura 2: Construcción de la perpendicular a una recta por un punto.

Está claro que esta construcción nos permite entre otras cosas, trazar la paralela a una recta r dada por un punto p que no pertenezca a ella (primero se traza la perpendicular s por el punto p y luego la perpendicular a s por el punto p será una paralela a r por p).

Veamos a que nos referimos por puntos constructibles. Primero, consideramos dos puntos cualesquiera en el plano. Les llamaremos 0 y 1. Tracemos ahora la recta por ellos. Esta representará la recta real.

Antes de mostrar que los constructibles son un subcuerpo de $\mathbb{C}$ veamos que podemos construir todos los racionales[11].

Es fácil ver que podemos construir los enteros, pues tomamos el compás, lo apoyamos en el 0 y lo abrimos hasta llegar al 1. Ahora, manteniendolo abierto, lo apoyamos en el 1 y trazamos la circunferencia de centro 1 y radio 1. Esta intersectará al eje real en el punto 0 (ya lo teníamos) y en el punto 2. Continuando este proceso (ahora apoyamos el compás en el punto 2 la circunferencia cortará en 1 y 3) podemos construir todos los números enteros positivos. De igual manera construimos los negativos (nos paramos en 0 hacemos la circunferencia de radio uno y corta en 1 y -1).

Nos estaría faltando poder hacer las fracciones, para eso es que utilizaremos el Teorema de Thales. Recordemos que decía que frente a una situación como la de la figura 3 se cumple que

$$\frac{b}{a} = \frac{d}{c}$$

Entonces, para construir el número $\frac{n}{m}$ procedemos como en la figura 4. Trazamos una recta auxiliar que pase por el 0. Tomamos en ella los valores m y 1. Unimos el punto m en la recta auxiliar con el punto n en la recta real por medio de una recta r y luego trazamos la paralela a la recta r por el punto 1 de la recta auxiliar. Esta paralela, utilizando el Teorema de Thales, intersectará el eje real en $\frac{n}{m}$.

Este procedimiento es sumamente general ya que si tenemos dos puntos cualesquiera del eje real (constructibles) que deseamos dividir, llamemosles a y b los podemos sustituir por n y m en el argumento consiguiendo dividirlos. En particular, también podemos multiplicar reales (pues $ab = a/(1/b)$ y podemos dividir 1 entre b pues 1 es constructible).

[9]En algún momento intentaré eliminar este prerequisito, ya sea agregando un apéndice con lo necesario para seguir la prueba si no se está familiarizado con espacios vectoriales o buscando una prueba que no los requiera (que debe existir ya que el Teorema fue probado antes de existir los espacios vectoriales como objeto de estudio).

[10]La mediatriz se construía considerando dos círcunferencias $\mathcal{C}_1$ y $\mathcal{C}_2$ de igual radio (por ejemplo que pasen por p) y uniendo con una recta los puntos de intersección.

[11]La idea de mostrar que es un subcuerpo es la misma, pero puede resultar más natural empezar por construir los racionales.

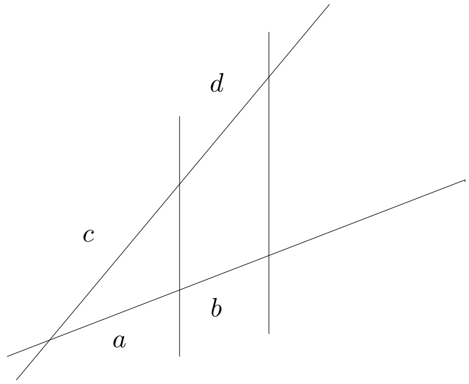

Figura 3: Teorema de Thales.

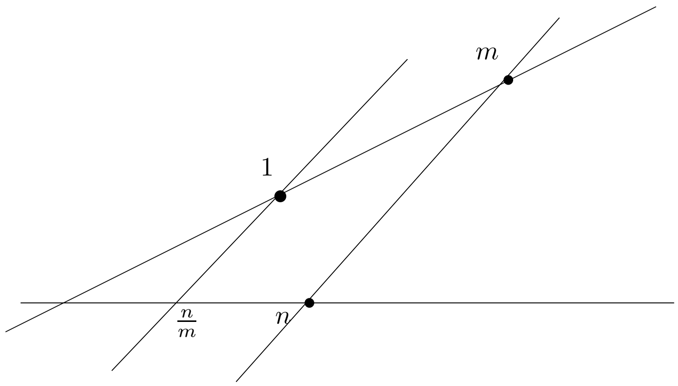

Figura 4: Construyendo $\frac{n}{m}$.

Más fácil aún es sumar y restar magnitudes reales ya que consiste únicamente en tomar la medida desde el 0 a un punto, trasladarla hasta el otro punto y trazar la circunferencia. Dicho esto, vemos que el conjunto de los puntos constructibles es un subcuerpo de los complejos ya que la suma y el producto complejo consiste en realizar operaciones entre sus partes reales e imaginarias y dado que sabemos trazar paralelas y perpendiculares, podemos conseguir la parte real e imaginaria de los complejos, operar con ellas y luego volver a construir el complejo resultante[12].

2.1. Los constructibles como raices de polinomios en $\mathbb{Q}$

La idea es la siguiente: Como los puntos constructibles son intersecciones de rectas y circunferencias, estos resultan ser raices de polinomios de grado 2. Mediante un simple argumento de extensiones de cuerpos, se puede ver que todo punto pertenence a una extensión de $\mathbb{Q}$ de dimensión 2^n ([13]). Esto implica inmediatamente que el elemento es algebraico de grado 2^k concluyendo el teorema. En lo que sigue intentaremos dar una prueba más elemental utilizando las mismas ideas pero deshuasandolas más y explicando los conceptos necesarios.

TERMINAR ALGÚN DÍA!!!!!!!!!!

[12]Obviamente no es la forma óptima de construir los puntos en mención, pero funciona.

[13]Para construir un elemento se realiza una cantidad finita de operaciones de intersectar rectas y circunferencias, por ende, podemos partir de $\mathbb{Q}$ y el primer corte implicará una extensión algebraica de grado 2 o 1. Ahora, razonamos de igual forma pero en el nuevo cuerpo, esto nos da que todo elemento se encuentra en una extensión de dimensión 2^n pues la dimensión es el producto de las dimensiones.