CONSTRUCCIONES CON REGLA Y COMPÁS: UNA INTRODUCCIÓN A LA TEORÍA DE CUERPOS

Rudy Rosas[1]

Octubre, 2008

Resumen

El presente artículo es una exposición concisa y autocontenida sobre los tres grandes problemas de la antigüedad y sus soluciones. La intención es introducir el concepto abstracto de cuerpo y algunas estructuras matemáticas subyacentes.

Clasificación AMS 2000: 12-10

Palabras Clave: *Cuerpos, regla y compás, extensiones algebraicas.*

1. *Sección Matemáticas, Departamento de Ciencias, PUCP.*

1. Introducción

Una construcción con regla y compás es el trazado de puntos, rectas o círculos usando solamente una regla y un compás ideales. Las normas de utilización de "la regla" y "el compás" fueron establecidas por los griegos, quienes fueron los que plantearon así algunos de los problemas más famosos de la historia:

La Cuadratura del Círculo:

Este problema consiste en construir un cuadrado con área igual a la de un círculo dado. Se comienza a partir de un círculo del cual se conocen su centro y alguno de los puntos de su circunferencia. Para resolver el problema basta construir un segmento de longitud igual a la del cuadrado que tiene la misma área que la del círculo dado.

La Duplicación del Cubo:

Aquí se propone la construcción de un cubo cuyo volumen sea el doble del volumen de un cubo dado. En este caso basta construir a partir de un segmento dado de longitud l, un segmento cuya longitud sea igual a $\sqrt[3]{2}l$.

La Trisección del Ángulo:

Dado un cierto ángulo, se plantea construir dos rectas que lo dividan en tres ángulos de igual medida. Este problema es resoluble para algunos ángulos particulares.

Estos problemas, a pesar de los esfuerzos de muchas generaciones de matemáticos, permanecieron sin solución por más de 2000 años. Fue recién en el siglo XIX que fue demostrada la imposibilidad de estas construcciones. Más allá de la apariencia geométrica de estos problemas. La solución de éstos sólo fue posible con el desarrollo del álgebra abstracta y el estudio de ciertos conjuntos de números llamados cuerpos. Un cuerpo

es una estructura abstracta que encuentra sus más ricos ejemplos en algunos conjuntos de números reales o complejos. Antes de enunciar de una forma matemáticamente precisa las reglas de las construcciones con regla y compás, estudiaremos la definición de Cuerpo y daremos algunos ejemplos.

2. Cuerpos

Diremos que un conjunto $F \subset \mathbb{C}$ es un cuerpo de números complejos, si satisface las propiedades siguientes:

1. F es cerrado para la suma y el producto. Dicho precisamente: para cualesquiera $a, b \in F$ se tiene $a + b \in F$ y $ab \in F$.
2. $1 \in F$.
3. Si $a \in F$, entonces $-a \in F$.
4. Si $a \in F$ y $a \neq 0$, entonces $a^{-1} \in F$.

Las siguientes propiedades de un cuerpo de números complejos se deducen fácilmente de las anteriores:

- $0 \in F$: de 2 y 3 deducimos que 1 y -1 son elementos de F. Luego por 1 tendremos que $0 = 1 + (-1) \in F$.
- Si $a, b \in F$, entonces $a - b \in F$: por 3 tenemos que $(-b) \in F$, luego $a - b = a + (-b) \in F$.
- Si $a, b \in F$ y $b \neq 0$, entonces $a/b \in F$: por 4 tenemos que $b^{-1} \in F$, luego por 1 tendremos $a/b = a(b^{-1}) \in F$
- La suma o el producto de cualquier número (finito) de elementos de F, es también un elemento de F: basta aplicar sucesivamente la propiedad 1.

A partir de ahora escribiremos simplemente cuerpo en lugar de cuerpo de números complejos.

Ejercicio. *Compruebe que* $\mathbb{Q}$, $\mathbb{R}$ *y* $\mathbb{C}$ *son cuerpos y que* $\mathbb{N}$ *y* $\mathbb{Z}$ *no lo son.*

Observe que, por definición, un cuerpo es un conjunto no vacio ($1 \in F$). Veremos ahora que, de hecho, un cuerpo (de números complejos) debe tener infinitos elementos.

Proposición. *Si* $F \subset \mathbb{C}$ *es un cuerpo, entonces* F *contiene a todos los números racionales.*

Demostración. Como $1 \in F$ y F es cerrado por la suma tendremos que $2 = 1 + 1 \in F$. Ahora, ya que $1, 2 \in F$, vemos que $3 = 1 + 2 \in F$, luego $4 = 3 + 1 \in F$ y si seguimos con este argumento podremos probar que todo número natural tiene que pertenecer a F. Además, por la propiedad 3, F contendrá también a los opuestos aditivos de todos los números naturales. Entonces $\mathbb{Z} \subset F$. Dado cualquier número racional q, sabemos que $q = a/b$ para ciertos números $a, b \in \mathbb{Z}$ con $b \neq 0$. Así, como $\mathbb{Z} \subset F$, tendremos $a, b \in F$ y consecuentemente $q = a/b$ debe pertenecer a F. □

3. Puntos Constructibles I

Ahora que ya tenemos la noción de cuerpo, trataremos de hacer precisa la noción de constructibilidad de puntos. Dado un conjunto P de puntos del plano, sean:

1. R_P el conjunto de las rectas del plano que pasan por 2 puntos distintos de P
2. C_P el conjunto de los círculos centrados en un punto de P que pasan por algún otro punto de P.

Un punto del plano es contructible en un paso a partir de P si es un punto de intersección entre dos elementos de $R_P \cup C_P$. O sea, un punto z será constructible en un paso a partir de P si:

1. z es la intersección entre las rectas determinadas por dos pares de puntos de P,

2. z es un punto de intersección entre una recta y un círculo determinados por dos pares de puntos de P, o

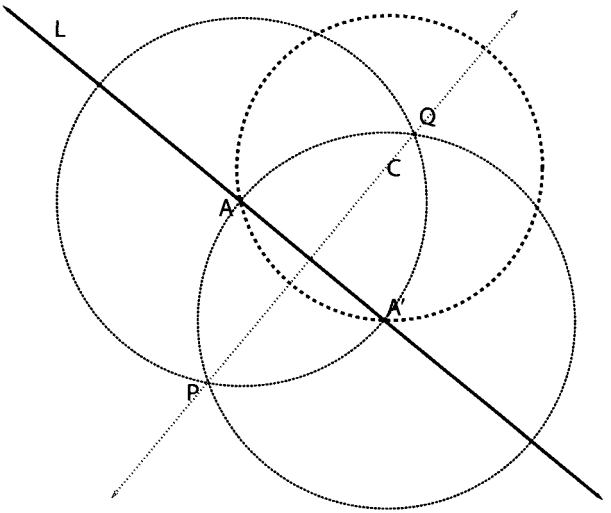
3. z es un punto de intersección entre los círculos determinados por dos pares de puntos de P.

Un punto z del plano es contructible en n pasos a partir de P, si existen puntos $z_1, \ldots, z_n$ con $z_n = z$ y tales que: z_1 es constructible en un paso a partir de P, z_2 es constructible en un paso a partir de $P \cup \{z_1\}, \ldots, z_n$ es constructible en un paso a partir de $P \cup \{z_1, \ldots, z_{n-1}\}$. Un punto del plano es constructible a partir de P si es constructible en n pasos a partir de P para algún $n \in \mathbb{N}$. Pues bien, ya que estamos interesados en estudiar los tres problemas de la antigüedad, a partir de ahora abordaremos la cuestión siguiente: Inicialmente comenzaremos con dos puntos dados (ya construidos) O y A en el plano y nos plantearemos el problema de caracterizar los puntos del plano que pueden ser construidos a partir de $\{O, A\}$. Para hacer más preciso el problema, introducimos coordenadas cartesianas en el plano de manera que $O = (0,0)$ y $A = (1,0)$. Entonces diremos que un punto del plano es constructible si éste es constructible a partir de $\{O, A\}$. Diremos también que una recta es constructible si pasa por un par de puntos constructibles. En el caso de un círculo, diremos que éste es constructible si su centro y algun punto de su circunferencia son constructibles. Es fácil ver que las intersecciones entre rectas y/o círculos constructibles son puntos constructibles. Frecuentemente identificaremos nuestro plano cartesiano con el conjunto $\mathbb{C}$ de los números complejos. Así, diremos que el número complejo $x + iy$ es constructible si el punto (x, y) es constructible.

Lema 1. *Si la recta L y el punto C son constructibles, entonces la recta perpendicular a L que pasa por el punto C es constructible.*

Demostración. Por definición, la recta L contiene al menos dos puntos constructibles, así que podemos escoger en L un punto constructible A distinto de C. Supongamos que la recta AC no es perpendicular a L, caso contrario no habría nada que probar. Entonces el círculo centrado

en C que pasa por A intersecta a L en un punto $A' \neq A$, asi que el círculo centrado en A que pasa por A' y el círculo centrado en A' que pasa por A se intersectan en dos puntos constructibles P y Q. finalmente es fácil ver que la recta PQ es la recta buscada. □

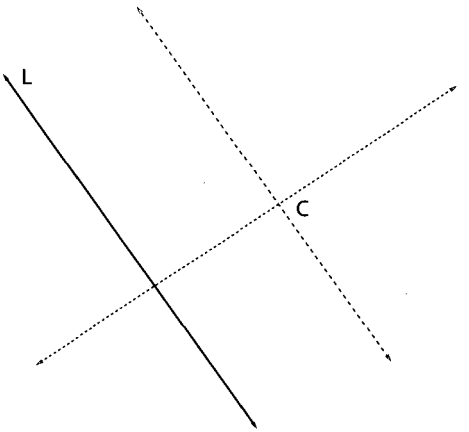


Lema 2. *Si la recta L y el punto C son constructibles, entonces la recta paralela a L que pasa por C es constructible.*

Demostración. Construimos primero la recta L^t perpendicular a L que pasa por C. Luego construimos la recta perpendicular a L^t que pasa por C. □

Proposición 3. *El número $x + iy \in \mathbb{C}$ es constructible si y sólo si x e y son números (en $\mathbb{C}$) constructibles.*

Demostración. Supongamos que $x + iy$ es constructible. El punto $(x, 0)$ es la intersección entre el eje X y la recta paralela al eje Y que pasa



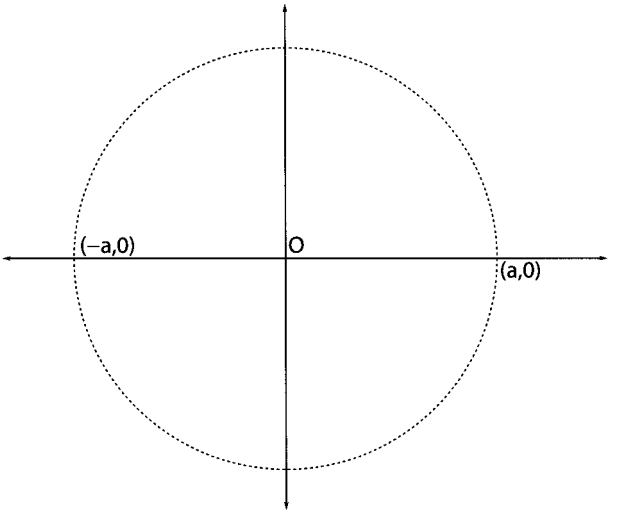
por el punto constructible (x, y). Luego $(x, 0)$ es constructible. Análogamente podemos probar que $(0, y)$ es constructible. Luego $(y, 0)$ será constructible, ya que es un punto de intersección entre el eje X y el círculo centrado en O que pasa por $(0, y)$. Supongamos ahora que $(x, 0)$ y $(y, 0)$ son constructibles. Procediendo como antes, podemos "construir" el punto $(0, y)$ y las rectas perpendiculares al eje X y al eje Y que pasan por $(x, 0)$ y $(0, y)$ respectivamente. Entonces el punto (x, y), siendo la intersección de estas dos rectas, será un punto constructible. □

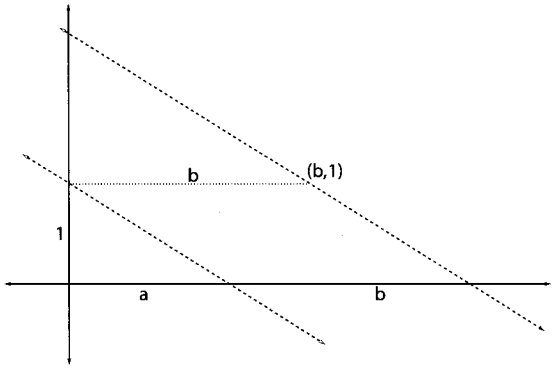
Teorema 4. *El conjunto de los números reales constructibles es un cuerpo.*

Demostración. Sean a y b números reales constructibles.

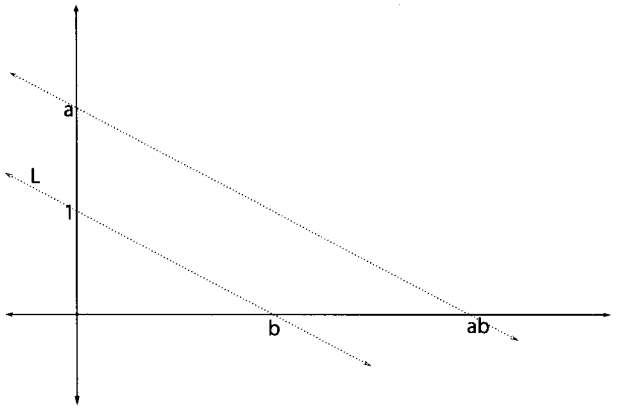
1. $-a$ es constructible: El punto $(-a, 0)$ es un punto de intersección de el eje X con el círculo centrado en O que pasa por $(a, 0)$.

2. $a+b$ es constructible: Claramente el número $1 \in \mathbb{C}$ es constructible, así que por la proposición 3 el punto $(b, 1)$ es constructible. Sea L la recta que pasa por $(0, 1)$ y $(a, 0)$. Es fácil ver que el punto $(a+b, 0)$ es el punto de intersección entre el eje X y la recta paralela a L que pasa por $(b, 1)$. Entonces $a + b$ es constructible.


(−a,0)
O
(a,0)


b
(b,1)
1
a
b

3. ab es constructible: Sea L la recta que pasa por los puntos constructibles $(b,0)$ y $(0,1)$. Es fácil probar (es sólo una semejanza de triángulos) que la recta paralela a L que pasa por el punto constructible $(0,a)$ intersecta al eje X en el punto $(ab,0)$. Entonces ab es constructible.

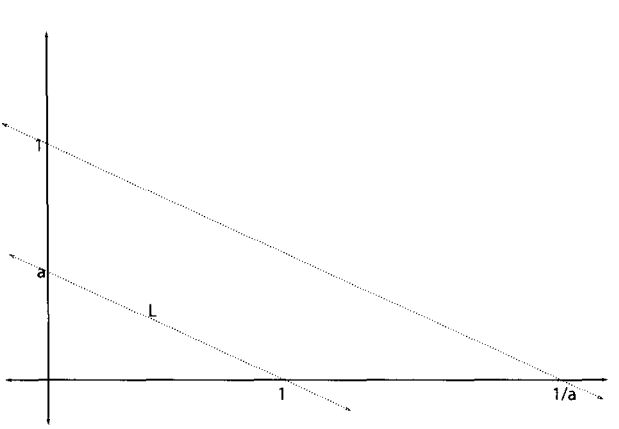


4. Si $a \neq 0$, entonces a^{-1} es constructible: Sea L la recta que pasa por los puntos constructibles $(0,a)$ y $(1,0)$. Entonces el punto $(a^{-1},0)$ será constructible, ya que es la intersección entre el eje X y la recta paralela a L que pasa por $(0,1)$.

□

Corolario 5. *El conjunto K de los números complejos constructibles es un cuerpo.*

Demostración. Sean $z = a + ib$ y $w = c + id$ números complejos constructibles. Entonces por la proposición 3 a, b, c y d son constructibles. Luego, por la proposición 4 los números $-a$, $-b$, $(a+c)$, $(b+d)$, $(ac-bd)$, $(ad+bc)$ son constructibles y, de nuevo por la proposición 3, los números $-z$, $z+w$ y zw serán constructibles. Además, si $z \neq 0$ tendremos también



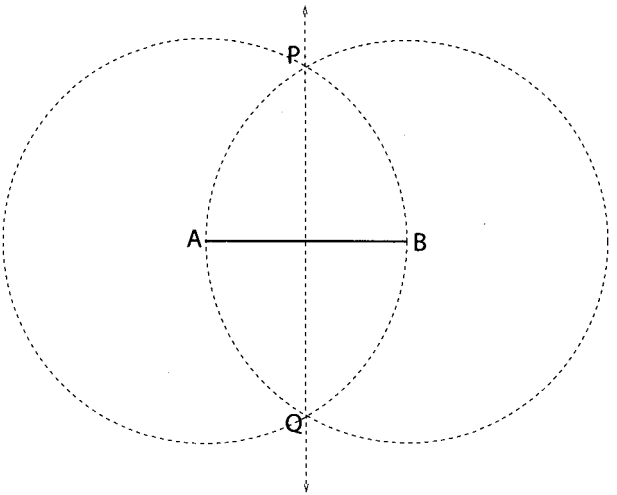
que $\frac{a}{a^2+b^2}$ y $\frac{-b}{a^2+b^2}$ son constructibles y por consiguiente lo mismo ocurrirá con z^{-1}. □

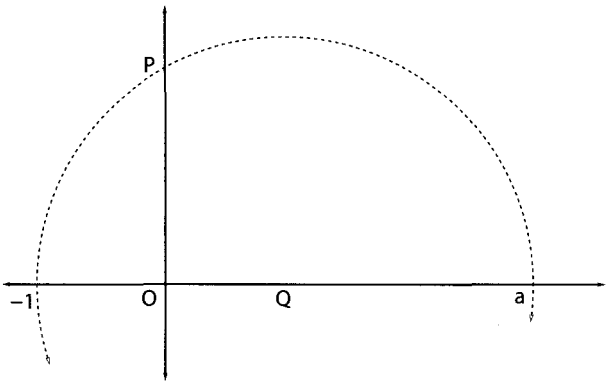
Lema 6. *Si A y B son constructibles, entonces el punto medio del segmento AB es también constructible.*

Demostración. El círculo centrado en A que pasa por B y el círculo centrado en B que pasa por A se intersectan en los puntos P y Q. La recta PQ intersecta al segmento AB en su punto medio. □

Proposición 7. *Si $a > 0$ es un número real constructible, entonces $\sqrt{a}$ es también constructible.*

Demostración. Los puntos $(-1, 0)$ y $(a, 0)$ son constructibles, así que el punto medio del segmento que definen es constructible. Sea Q este punto medio y construyamos el círculo centrado en este punto que pasa por $(a, 0)$. Este círculo intersecta la parte positiva del eje y en un punto P. Se deduce de la semejanza entre los triángulos $(-1, 0)OP$ y $PO(a, 0)$ que la longitud de OP es igual a $\sqrt{a}$. entonces $P = (0, \sqrt{a})$ y por lo tanto $\sqrt{a}$ es constructible. □


P
A
B
Q


P
−1
O
Q
a

4. Polinomios en una Variable

Desde la escuela estamos familiarizados con resolver problemas que conducen a ecuaciones simples, por ejemplo, expresiones del tipo $5x + 2 = 12$ ó $x^2 + x - 6 = 2$. Ya en esta epoca desarrollamos métodos para encontrar todas las soluciones a estas ecuaciones. Sabíamos así que la ecuación general $ax^2 + bx + c = 0$ $(a \neq 0)$ posee dos soluciones (o sólo una) dadas por las fórmulas

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a}, \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Sabemos también resolver fácilmente ecuaciones de "mayor grado" en algunos casos especiales, por ejemplo, las ecuaciones $x^3 - x = 0$ ó $x^4 - 2 = 0$. Así, es intuitivamente claro lo que significa "resolver" una ecuación del tipo

$$a_0 + a_1 x + \ldots + a_n x^n = 0.$$

La expresión $a_0 + a_1 x + \ldots + a_n x^n$ es conocida por todos nosotros como polinomio. Un polinomio se puede interpretar como una función desde el punto de vista del análisis, precisamente, la función real $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $x \in \mathbb{R}$. Luego la ecuación de arriba propone el problema de encontrar los puntos de la recta real donde la función f toma el valor 0. Por otro lado, un polinomio puede entenderse, desde el punto de vista algebraico, simplemente como una expresión (o símbolo) del tipo $a_0 + a_1 x + \ldots + a_n x^n$, donde n es cualquier número entero no negativo y $a_0, \ldots, a_n$ son números complejos. El término $a_j x^j$ $(j = 0, \ldots, n)$ se llama "término de grado j" del polinomio (aquí convenimos que $a_0 x^0 = a_0$) y el número a_j es el coeficiente de dicho término. Para todo $j > n$ decimos que el coeficiente del término de grado j es nulo. Por supuesto y como es natural no nos interesa diferenciar (por ejemplo) los polinomios $1 + x^2$ de $1 + 0x + x^2 + 0x^3$. Entonces diremos que dos polinomios son iguales (idénticos) si para todo $j \in \mathbb{Z}_{\geq 0}$, los coeficientes de los términos de grado j de ambos polinomios, son iguales. Denotaremos por 0 al polinomio que tiene todos sus coeficientes iguales a cero. Claramente, si

el polinomio $f(x)$ es diferente del polinomio nulo, entonces $f(x)$ admite una expresión de la forma $a_0 + a_1x + \ldots + a_nx^n$ con $n \in \mathbb{Z}_{\geq 0}$ y $a_n \neq 0$. En este caso decimos que el polinomio $f(x)$ tiene grado igual a n y escribiremos $\partial(f) = n$ [1] . El coeficiente a_n se llama coeficiente principal del polinomio y cuando $a_n = 1$ diremos que el polinomio es mónico. Observe que los polinomios de grado cero son expresiones de la forma a_0 con $a_0 \in \mathbb{C}\backslash\{0\}$. A todos estos polinomios, incluyendo además al polinomio nulo, les llamaremos constantes (o polinomios constantes).

A continuacion definimos la suma y el producto de polinomios. Dados los polinomios $f(x) = a_0 + a_1x + \ldots + a_nx^n$ y $g(x) = b_0 + b_1x + \ldots + b_mx^m$ (supongamos $n \geq m$), definimos la suma $f(x) + g(x)$ como siendo el polinomio

$$c_0 + c_1x + \ldots + c_nx^n,$$

donde $c_j = a_j + b_j$ para todo $j \leq n$ (naturalmente aqui hacemos $b_j = 0$ para todo $j > m$). El producto $f(x)g(x)$ será por definición el polinomio

$$d_0 + d_1x + \ldots + d_{n+m}x^{n+m},$$

donde $d_k = \sum_{i+j=k} a_ib_j = a_0b_k + a_1b_{k-1} + \ldots a_kb_0$ para todo $k = 0, 1 \ldots, n+m$. En particular tenemos $c_{n+m} = a_nb_m$. Asi, si a_n y b_m son distintos de cero, también c_{n+m} será distinto de cero y tendremos por lo tanto la siguiente propiedad.

Proposición 8. *Si $f(x)$ y $g(x)$ son polinomios no nulos, entonces el grado del producto $f(x)g(x)$ es igual a las suma de los grados de $f(x)$ y $g(x)$. En particular, el producto de dos polinomios no nulos es también no nulo.*

Por otro lado, es fácil ver a partir de la definición que el producto de cualquier polinomio por el polinomio nulo es igual al polinomio nulo.

[1] Observe que no se define el grado del polinomio nulo.

Si $F \subset \mathbb{C}$ es un cuerpo, denotaremos por $F[x]$ al conjunto de los polinomios con coeficientes en F. Dados $f(x), g(x) \in F[x]$, observe que los coeficientes de $f+g$ y fg se obtienen por operaciones sucesivas de suma y multiplicación a partir de los coeficientes de f y g. Esto garantiza que los coeficientes de $f+g$ y fg pertenecen a F, es decir, $f+g, fg \in F[x]$. Asi, las operaciones suma y producto de polinomios están bien definidas y son cerradas en $F[x]$ y tenemos las siguientes propiedades:

1. La suma y el producto en $F[x]$ son operaciones conmutativas y asociativas.

2. Existe $1 \in F[x]$ (polinomio constante 1) tal que para todo $f \in F[x]$ se tiene $1 \cdot f = f \cdot 1 = f$.

3. Existe $0 \in F[x]$ (polinomio nulo) tal que $0 + f = f + 0$ para todo $f \in F[x]$.

Decimos que el polinomio $f(x)$ divide al polinomio $g(x)$, si existe un polinomio $h(x)$ tal que $g(x) = f(x)h(x)$. En este caso escribiremos $f(x)|g(x)$. Se deduce fácilmente que si $f|g$ y $g|h$, entonces $f|h$.

Teorema 9. *(Algoritmo de la división con resto) Dados $f(x), p(x) \in F[x]$ con $\partial(p) = d$, entonces*

$$f(x) = p(x)q(x) + r(x),$$

para ciertos polinomios $q(x), r(x) \in F[x]$ con $r(x) = 0$ o $\partial(r) < d$. Además los polinomios $q(x)$ y $r(x)$ son únicos.

Demostración. Sean $f(x) = ax^n + \ldots$ y $p(x) = bx^d + \ldots$ con $b \neq 0$. Si $n \geq d$, como $b \neq 0$ podemos definir el polinomio $\frac{a}{b}x^{n-d}p(x) = ax^n + \ldots$, cuyo término de mayor grado es igual al término de mayor grado de $f(x)$. Así que si restamos $\frac{a}{b}x^{n-d}p(x)$ de $f(x)$ obtendremos un polinomio en $F[x]$ cuyo término de mayor grado tiene como máximo grado $n-1$ (podría ser nulo), es decir

$$f_1(x) = f(x) - (\frac{a}{b})x^{n-d}p(x) = a_1x^{n-1} + \ldots,$$

Si $n-1 \geq d$, esta vez restamos $\frac{a_1}{b}x^{n-d-1}p(x)$ de $f_1(x)$ para anular el termino a_1x^{n-1} y obtendremos el polinomio

$$f_2(x) = f(x) - \frac{a}{b}x^{n-d}p(x) - \frac{a_1}{b}x^{n-d-1}p(x) = a_2x^{n-2} + \ldots,$$

el cual, o es nulo, o tiene grado $\leq n-2$.

Entonces, si seguimos con este proceso, después de un número finito de pasos obtendremos un polinomio $f_k(x) \in F[x]$, o bien nulo, o bien de grado estrictamente menor que d expresado en la forma

$$f_k(x) = f(x) - \frac{a}{b}x^{n-d}p(x) - \frac{a_1}{b}x^{n-d-1}p(x) - \ldots - \frac{a_{k-1}}{b}x^{n-d-k}p(x).$$

entonces $f(x) = p(x)(\frac{a}{b}x^{n-d} + \frac{a_1}{b}x^{n-d-1} + \ldots + \frac{a_{k-1}}{b}x^{n-d-k}) + f_k(x)$ y finalmente sólo tenemos que hacer $q(x) = \frac{a}{b}x^{n-d} + \frac{a_1}{b}x^{n-d-1} + \ldots + \frac{a_{k-1}}{b}x^{n-d-k}$ y $r(x) = f_k(x)$. Si $f = pq' + r'$ es otra división con resto de f, restando las ecuaciones tendremos $p(q-q') = r'-r$. Entonces, como $r'-r$ es nulo o tiene grado menor que el grado de p, se deduce de la proposición 8 que $q-q' = 0$ y de ahi sigue la unicidad. □

Dados $f(x), g(x) \in F[x]$, decimos que un polinomio $d(x) \in F[x]$ es un máximo común divisor de f y g sobre F si:

1. $d(x)$ es divisor común de $f(x)$ y $g(x)$,
2. Si $u(x)$ es divisor común de $f(x)$ y $g(x)$, entonces $u(x)$ divide a $d(x)$,
3. $d(x)$ es mónico.

Teorema 10. *Dado un cuerpo F y dados $f(x)$, $g(x)$ en $F[x]$, existe un único máximo común divisor $d(x)$ de f y g sobre F. Además este polinomio se expresa en la forma:*

$$d(x) = a(x)f(x) + b(x)g(x),$$

para ciertos polinomios $a, b \in F[x]$.

Demostración. Sea

$$I = \{a(x)f(x) + b(x)d(x) : a(x), b(x) \in F[x]\}.$$

Como el conjunto de los grados de los polinomios no nulos de I es un subconjunto de $\mathbb{Z}_{\geq 0}$, existe un polinomio $d(x) \in I$ tal que $\partial(d(x)) \leq \partial(u(x))$ para todo $u(x) \in I$. Es fácil ver que cualquier múltiplo de $d(x)$ es también un elemento de I, así que multiplicando $d(x)$ por el inverso de su coeficiente principal si es necesario, podemos asumir que $d(x)$ es mónico. Afirmación: $d(x)$ divide a $f(x)$ y $g(x)$. Para esto, como (evidentemente) $f, g \in I$, es suficiente mostrar que $d(x)$ divide a todo elemento de I. Sea $u(x) \in I$. Por el algoritmo de la división $u(x) = q(x)d(x) + r(x)$ donde $r(x)$ es el polinomio nulo o tiene grado menor que el de $d(x)$. Es fácil ver que $r = u - qd$ es también un elemento de I, así que $r(x)$ no puede tener grado menor que el de $d(x)$ (por la definición de d). Entonces $r = 0$ y $d(x)$ divide a $u(x)$. Sea ahora $d'(x)$ cualquier divisor común de $f(x)$ y $g(x)$. Entonces existen polinomios f' y g' tales que $f = d'f'$ y $g = d'g'$. Como $d \in I$, existen $a, b \in F[x]$ tales que $d = af + bg$. Entonces $d = ad'f' + bd'g' = d'(af' + bg')$, es decir, d'divide a d. Por lo tanto $d(x)$ es un máximo común divisor de $f(x)$ y $g(x)$. Suponga que $d'(x)$ es otro máximo común divisor $f(x)$ y $g(x)$. Entonces sigue de la definición de máximo común divisor que $d|d'$ y $d'|d$. Se deduce de la proposición 8 que si $P(x)$ divide a $Q(x) \neq 0$, entonces $\partial(P) \leq \partial(Q)$. Por esto y lo anterior tendremos que los grados de $d(x)$ y $d'(x)$ son iguales. Luego, como $d = d'c$, de nuevo por la proposición 8 el grado de c debe ser cero, es decir, c es una constante. Como d y d' son ambos mónicos, concluimos que $c = 1$ y por lo tanto $d = d'$. □

Denotamos el máximo común divisor de $f(x)$ y $g(x)$ por $(f(x), g(x))$. Decimos que un polinomio $p(x) \in F[x]$ de grado mayor que cero, es irreductible sobre F, si no existen polinomios $f(x), g(x) \in F[x]$ de grado mayor que cero tales que $p(x) = f(x)g(x)$. Dicho de otra forma: Un polinomio $p(x)$ de grado mayor que cero es irreductible si $p(x) = f(x)g(x)$ implica que f o g es una constante diferente de cero.

Ejemplo 11. Los polinomios lineales, es decir, los polinomios de la forma $f(x) = ax + b$ $(a \neq 0)$, son irreductibles. Un polinomio cuadrático $f(x) = ax^2 + bx + c$ $(a \neq 0)$, es irreductible sobre F si y sólo si no tiene raíces en F.

Ejercicio 12. Pruebe que el polinomio $f(x) = 8x^3 - 6x - 1$ es irreductible sobre $\mathbb{Q}$. (Sugerencia: si f fuera el producto de dos factores no constantes, entonces uno de estos sería lineal y en consecuencia f tendría una raíz racional. Pruebe entonces que f no tiene raíces racionales.)

Proposición 13. *Si $p(x), f(x) \in F[x]$ y $p(x)$ es irreductible, entonces: o $p(x)$ divide a $f(x)$, o $(p(x), f(x)) = 1$.*

Demostración. Sea $d(x) = (p(x), f(x))$. Como $d(x)$ divide a $p(x)$, entonces $p(x) = d(x)c(x)$. Luego, o $d(x)$ es una constante y por lo tanto igual a 1, o $c(x) = c$ es una constante diferente de cero. La segunda posibilidad implica que $p(x) = cd(x)$ divide a $f(x)$, ya que $d(x)|f(x)$. □

Cuando $(f(x), g(x)) = 1$, decimos que los polinomios $f(x)$ y $g(x)$ son primos entre si.

4.1. Raíces de un Polinomio

Decimos que $\alpha \in \mathbb{C}$ es una raíz del polinomio $f(x) = a_0 + a_1 x + \ldots, a_n x^n$ si $f(a) := a_0 + a_1\alpha + \ldots a_n\alpha^n$ es igual a cero. En este caso decimos también que el polinomio $f(x)$ se anula en α.

Proposición 14. *$\alpha \in \mathbb{C}$ es raíz de $f(x)$ si y sólo si $(x - \alpha)$ divide a $f(x)$.*

Demostración. Supongamos que α es raíz de $f(x)$. Por el algoritmo de la división podemos escribir $f(x) = q(x)(x - \alpha) + r(x)$, donde $r(x) = 0$ o $\partial(r) < \partial(x - \alpha) = 1$. Luego $r(x) = r_0$ es una constante. Por otro lado, si evaluamos en α cada uno de los miembros de la igualdad anterior obtenemos $0 = f(\alpha) = r(\alpha) = r_0$. Entonces $f(x) = q(x)(x - \alpha)$. Recíprocamente, si $(x-\alpha)|f(x)$, entonces $f(x) = (x-\alpha)h(x)$, para algún polinomio h, lo que muestra que $f(\alpha) = 0$. □

Proposición 15. *Si $f(x)$ es un polinomio de grado n, entonces $f(x)$ tiene como máximo n raíces complejas.*

Demostración. Razonemos por inducción en n. Es fácil ver que todo polinomio de grado 1 admite exactamente una una raíz ($a_0 + a_1 x = 0$ si y solamente si $x = -a_0/a_1$). Supongamos que todo polinomio de grado $k < n$ tiene como máximo k raíces complejas y sea $f(x)$ un polinomio de grado n. Si $f(x)$ no tiene raíces no habría nada que probar, así que podemos asumir que $f(x)$ tiene alguna raíz $\alpha \in \mathbb{C}$. Entonces $(x - \alpha)$ divide a $f(x)$ y tendremos $f(x) = (x - \alpha)h(x)$. Si $\theta \neq \alpha$ es raíz de $f(x)$, entonces $f(\theta) = (\theta - \alpha)h(\alpha)$, de donde deducimos que $h(\theta) = 0$; es decir, toda raíz de f diferente de α tiene que ser raíz de $h(x)$. Como $f(x)$ no es nulo, necesariamente $h(x) \neq 0$ y tendremos por la proposición 8 que $\partial(h) = n - 1 < n$. Entonces, por la hipótesis de inducción, el polinomio $h(x)$ tiene como máximo $n - 1$ raíces y por lo tanto, $f(x)$ tendrá como máximo n raíces. □

El siguiente Teorema, cuya prueba omitimos, es fundamental para el estudio de los polinomios y sus propiedades

Teorema. *(Teorema Fundamental del Álgebra) Todo polinomio no constante con coeficientes complejos tiene al menos una raíz compleja.*

Corolario 16. *Si $f(x) \in \mathbb{C}[x]$ tiene grado $n \geq 1$, entonces existen $c, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tales que $f(x) = c(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$.*

Demostración. Procedemos por inducción en n. El corolario es obvio para $n = 1$. Supongamos que el resultado vale para $n = k \geq 1$. Sea $f(x)$ un polinomio de grado $k + 1$. Por el Teorema Fundamental del Álgebra $f(x)$ tiene una raíz $\alpha \in \mathbb{C}$. Entonces existe $h(x) \in \mathbb{C}[x]$ tal que $f(x) = (x - \alpha)h(x)$. Entonces $h(x)$ tiene grado k y por la hipótesis inductiva existen $c, \alpha_1, \ldots, \alpha_k \in \mathbb{C}$ tales que $h(x) = c(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_k)$. Luego $f(x) = c(x - \alpha)(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k)$ y el corolario vale también para $n = k + 1$. □

5. Espacios Vectoriales

Decimos que V es un espacio vectorial sobre el cuerpo F, si existen (sobre V) una operación suma, que a todo par de elementos $x, y \in V$ asocia un elemento $x + y \in V$, y una operación producto que a todo "escalar" $a \in F$ y todo $x \in V$ les hace corresponder un elemento ax en V, con las siguientes propiedades:

1. La suma $+$ hace de V un grupo conmutativo:

   a) $\forall x, y, z \in V$ se cumple que $x + y = y + x$ y $(x + y) + z = x + (y + z)$ (propiedades conmutativa y asociativa).

   b) Existe un elemento $0 \in V$ tal que $0 + x = x$ para todo $x \in V$.

   c) Para todo $x \in V$ existe un elemento en V denotado por $-x$ tal que $x + (-x) = 0$.

2. $\forall a, b \in F, x \in V$ se tiene
   $a(bx) = (ab)x$ (propiedad asociativa mixta)

3. $\forall a, b \in F, x, y \in V$ se cumple que
   $a(x+y) = ax+ay$ y $(a+b)x = ax+by$ (propiedades distributivas).

4. Si 1 es la unidad en F, entonces $1 \cdot x = x$ para todo $x \in V$.

A partir de estas propiedades se deducen otras como:

1. Si 0 es elemento nulo en F, entonces $0x = 0$ para todo $x \in V$.

2. $(-1)x = -x$.

3. $a(x - y) = ax - ay$ y $(a - b)x = ax + by$.

Si V es un espacio vectorial sobre F decimos también que V es un F-espacio vectorial. Si $F = \mathbb{R}$ o $\mathbb{C}$ decimos que V es un espacio vectorial real o complejo, respectivamente.

5.1. Base de un espacio vectorial

Sea V un F-espacio vectorial. Decimos que un conjunto finito $\{v_1, \ldots, v_n\} \subset V$ es linealmente independiente si la igualdad $a_1v_1 + \ldots + a_nv_n = 0$ sólo es posible cuando $a_1 = \ldots = a_n = 0$. Un conjunto $\{v_1, \ldots, v_n\} \subset V$ es una base de V si es linealmente independiente y todo elemento de V se expresa como una combinación lineal con coeficientes en F de los elementos $\nu_1, \ldots, \nu_n$, es decir:

$$V \subset \{a_1\nu_1 + \ldots + a_n\nu_n : a_1, \ldots, a_n\}.$$

Utilizaremos el siguiente teorema de Álgebra Lineal, que aceptaremos sin prueba:

Teorema. *Si $\{v_1, \ldots, v_n\}$ y $\{u_1, \ldots, u_m\}$ son bases de V, entonces $n = m$.*

Luego, si un espacio vectorial V tiene alguna base finita, el número de elementos de esta base es un número que depende sólo del espacio vectorial y es, por definición, la dimensión de V.

6. Extensiones de Cuerpos y Números Algebraicos

Decimos que el cuerpo E es una extensión de F si $F \subset E$. En este caso escribiremos $E|F$.

Ejercicio 17. Verifique que, si $E|F$, la suma en E y el producto usual entre un elemento de F y un elemento de E hacen de E un F-espacio vectorial.

Si E tiene dimensión finita igual a n, decimos que la extensión $E|F$ es finita de grado n. En este caso denotamos $n = [E : F]$.

Ejemplo. Considere la extensión $\mathbb{C}|\mathbb{R}$. Probemos que el conjunto $B = \{1, i\}$ es una base de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial. Si $a, b \in \mathbb{R}$ y $a(1) + bi =$

0, entonces claramente debemos tener $a = b = 0$, asi que B es linealmente independiente. Por otro lado sabemos que $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, asi que B genera $\mathbb{C}$ y es por lo tanto una base. En particular tenemos que $[\mathbb{C} : \mathbb{R}] = 2$.

Teorema 18. *Si $E|F$ y $K|E$ son extensiones finitas, entonces $[K : F] = [K : E][E : F]$. En particular $K|F$ es también finita.*

Demostración. Sean $\{u_1, \ldots, u_m\}$ y $\{v_1, \ldots, v_n\}$ bases de E y K como F-espacio vectorial y E-espacio vectorial respectivamente ($m = [E : F]$, $n = [K : E]$). Bastará probar que el conjunto de mn elementos $\{u_i v_j : i = 1, \ldots, n, j = 1, \ldots, m\}$ es una base de K como F-espacio vectorial. Suponga que $\sum_{i,j} a_{ij}(u_i v_j) = 0$ para $a_{ij} \in F$. Entonces $(\sum_i a_{ij} u_i) v_j = 0$ y como $(\sum_i a_{ij} u_i) \in E$ y $\{v_j\}$ es base de K como E-espacio vectorial, tendremos que $(\sum_i a_{ij} u_i) = 0$ para cada $j = 1, \ldots, m$. Luego, como $\{u_i\}$ es base de E como F-espacio vectorial, concluimos que $a_{ij} = 0$ para todo i y todo j y por lo tanto $\{u_{ij}\}$ es linealmente independiente. Dado $\theta \in K$, existen $b_1, \ldots, b_m \in E$ tales que $\theta = \sum_j b_j v_j$. Por otro lado, para cada j, existen $a_{1j}, \ldots, a_{nj} \in F$ tales que $b_j = \sum_i a_{ij} u_i$. Entonces $\theta = \sum_{i,j} a_{ij} u_i v_j$ y por lo tanto $\{u_i v_j\}$ es base. □

6.1. Números Algebraicos sobre un Cuerpo F

Decimos que un número $\alpha \in \mathbb{C}$ es algebraico sobre F, si α es raíz de algún polinomio no nulo con coeficientes en F. Asi por ejemplo, i, $\sqrt{2}$ y $\sqrt[3]{2}$ son números algebraicos sobre $\mathbb{Q}$, ya que son raices de los polinomios $x^2 + 1$, $x^2 - 2$ y $x^3 - 2$ en $\mathbb{Q}[x]$, respectivamente.

Proposición 19. *Si la extensión $E|F$ es finita, entonces todo $\alpha \in E$ es algebraico sobre F.*

Demostración. Sea $n = [E : F]$. Como la dimensión del F-espacio vectorial E es igual a n, el conjunto $\{1, \alpha, \ldots, \alpha^n\}$ debe ser linealmente dependiente, así que existen números $a_0, \ldots, a_n \in F$ no todos nulos tales que $a_0 + a_1\alpha \ldots, a_n\alpha^n = 0$, es decir, α es raíz del polinomio $a_0 + a_1x + \ldots a_nx^n$ en $F[x]$. □

Dado α algebraico sobre F, sea C el conjunto (no vacío por definición) de los polinomios no nulos con coeficientes en F que se anulan en α. Sea $N = \{\partial(f) : f \in C\}$. Como N es un conjunto no vacío de números naturales, éste tendrá un elemento mínimo, digamos $d \in N$. Decimos que este número d es el grado de α sobre F. O sea, el grado de α es el grado mínimo entre los grados de los polinomios que se anulan en α. Sea $p(x) \in C$ algún polinomio de grado d. Dividiendo $p(x)$ por su coeficiente principal si es necesario, podemos asumir que $p(x)$ es mónico.

Teorema 20. *Sea α algebraico de grado d sobre F. Entonces:*

1. *Existe un único polinomio mónico $p(x) \in F[x]$ de grado d que se anula en α.*
2. *El polinomio $p(x)$ es irreducible sobre F*
3. *$p(x)$ es el único polinomio mónico e irreducible sobre F se anula en α.*
4. *Si el polinomio $f(x) \in F[x]$ se anula en α, entonces $p(x)$ lo divide.*

El polinomio $p(x)$ se llama polinomio mínimal o irreducible de α sobre F.

Demostración. (1) Sean $p(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0$ y $q(x) = x^d + b_{d-1}x^{d-1} \ldots + b_0$ polinomios mónicos de grado d en $F[x]$, que se anulan en α. Entonces $p(x) - q(x) = (a_{d-1} - b_{d-1})x^{d-1} + \ldots$ es un polinomio que se anula en α. Entonces, o $p - q \in F[x]$ es el polinomio nulo, o entonces el grado de $p - q$ es menor que d. La última posibilidad no es factible por la definición de d, así que necesariamente $p(x) = q(x)$.

(2) Suponga que $p(x) = h(x)q(x)$ para ciertos polinomios $h, q \in F[x]$. Como $h(\alpha)q(\alpha) = p(\alpha) = 0$, tendremos $h(\alpha) = 0$ ó $q(\alpha) = 0$, digamos $h(\alpha) = 0$. Luego, ya que claramente $h(x) \neq 0$, tendremos $\partial(h) \geq d$ por la definición de d. Entonces, usando la proposición 8 deducimos que $\partial(h) = d$ y $\partial(q) = 0$, y q es por lo tanto una constante.

(4) Por el algoritmo de la división tenemos $f(x) = q(x)p(x) + r(x)$, donde $r(x) = 0$ ó $\partial(r) < \partial(p) = d$. Pero $r(x) = f(x) - q(x)p(x)$ se anula en α, así que $r(x) = 0$ ó entonces $\partial(r) \geq d$ (por la definición de d). Deducimos de aquí que $r(x) = 0$ y luego $p|f$.

(3) Sea $q(x)$ un polinomio mónico e irreductible que se anula en α. Por (4) tenemos que p divide a q, es decir, $q(x) = p(x)h(x)$, para algún polinomio con coeficientes racionales. Entonces, como q es irreducible y p no es constante, tendremos que $h(x) = a_0$ es una constante. Así que $q(x) = a_0 p(x)$ y como p y q son ambos mónicos concluimos que $a_0 = 1$ y $q(x) = p(x)$.

□

6.1.1. Números Algebraicos

Diremos que un número es algebraico cuando es algebraico sobre $\mathbb{Q}$. Llamaremos $\mathcal{A}$ al conjunto de todos los números algebraicos. Este conjunto es claramente infinito, ya que contiene a $\mathbb{Q}$, pero es mayor que $\mathbb{Q}$ puesto que contiene números no racionales como $\sqrt{2}$. Diremos que un número es trascendente si éste no es algebraico. Fue Liouville en 1884 quien mostró explícitamente el primer número trascendente:

$$\xi = \sum_{n=1}^{\infty} 10^{-n!} = 0,110001000000000000000001000\ldots$$

Hermite en 1873 demostró que el número e, la base de los logaritmos naturales, es un número trascendente. Hasta este momento los números algebraicos, aunque su existencia era irrefutable, eran aparentemente

"raros", y fue Cantor quien probó en 1874 que de hecho, en cierto sentido, los números trascendentes representan la "mayoría" de los números reales. Como dato interesante (aunque no es relevante para el resto de la exposición) haremos preciso el resultado de Cantor. Decimos que un conjunto es numerable cuando es finito o puede ponerse en biyección con el conjunto de los números naturales.

Proposición 21. *El conjunto $\mathcal{A}$ de los números algebraicos es un conjunto numerable.*

Demostración. El conjunto $P_n = \{a_0 + a_1x + \ldots + a_nx^n : a_j \in \mathbb{Q}\}$ de los polinomios de grado n se puede poner en biyeccion con un subconjunto de $\mathbb{Q}^n$ mediante la correspondencia

$$a_0 + a_1x + \ldots + a_nx^n \mapsto (a_0, \ldots, a_n) \in \mathbb{Q}^n.$$

Entonces P_n es un conjunto numerable. Luego, el conjunto $P_1 \cup P_2 \cup \ldots$ de todos los polinomios no nulos con coeficientes racionales es un conjunto numerable. Sea $f_1, f_2, \ldots$ una numeración de todos los polinomios no nulos con coeficientes racionales y sea R_j el conjunto (finito, por 15) de las raíces del polinomio f_j. Entonces $\mathcal{A} = R_1 \cup R_2 \cup \ldots$ es un conjunto numerable, ya que es la unión de una cantidad numerable de conjuntos finitos.

Un teorema clásico de Cantor establece que el conjunto de los números reales es no numerable. Luego, la proposición anterior implica que el conjunto $\mathbb{R}\backslash\mathcal{A}$ de los números trascendentes es un conjunto infinito no numerable. □

6.2. Extensiones Simples

El caso más importante de extensiones que trataremos aquí es el de extensiones simples. Sea F un cuerpo y $\theta \in \mathbb{C}$. Denotamos por $F(\theta)$ al conjunto:

$$\{\frac{P(\theta)}{Q(\theta)} : P, Q \in F[x], Q(\theta) \neq 0\}.$$

Proposición 22. *El conjunto $F(\theta)$ es un cuerpo que contiene a F y a θ. Además, si E es un cuerpo que contiene a F y a θ, entonces $F(\theta) \subset E$.*

Demostración. Dado $\alpha \in$ F, tomando P igual al polinomio constante α y Q igual al polinomio constante 1 vemos que $\alpha \in F(\theta)$, luego $F \subset F(\theta)$. en particular $1 \in F(\theta)$. Por otro lado, tomando $P(x) = x$ y $Q = 1$ vemos que $\theta \in F(\theta)$. Dados $a, b \in F(\theta)$, es rutinario probar que $a + b$, ab, $-a$ y a^{-1}(si $a \neq 0$) son elementos de $F(\theta)$. Entonces $F(\theta)$ es un cuerpo. Sea E un cuerpo que contiene a F y a θ y sea $a \in F(\theta)$. Entonces $a = \frac{P(\theta)}{Q(\theta)}$, donde P y Q son polinomios con coeficientes en F. $P(\theta)$ es una sucesión finita de operaciones de suma y multiplicación usando elementos de E. Luego $P(\theta) \in E$. Análogamente $Q(\theta) \in E$ y como este elemento es diferente de cero, también tendremos $a = \frac{P(\theta)}{Q(\theta)} \in E$. □

El cuerpo $F(\theta)$ es llamado "cuerpo generado por la adjunción de θ a F" o "cuerpo generado por F y θ" y es, en el sentido de la proposición anterior, "el menor cuerpo que contiene a F y a θ".

La extensión $E|F$ es simple si existe $\theta \in F$ tal que $E = F(\theta)$, es decir si E es generado por la adjunción a F de un único elemento.

Proposición 23. *Si α es algebraico de grado d sobre F, entonces la extensión $F(\alpha)|F$ es finita de grado d.*

Demostración. Probemos que $B = \{1, \alpha, \ldots, \alpha^{d-1}\}$ es una base de $F(\alpha)$ como F-espacio vectorial. Si $a_0(1) + a_1(\alpha) + \ldots a_{d-1}(\alpha^{d-1}) = 0$ entonces α es raíz del polinomio $f(x) = a_0 + a_1 x + \ldots a_{d-1}x^{d-1}$. Pero por la definición de d el número α no es raíz de ningún polinomio no nulo de grado menor que d. Entonces $a_0 = \ldots = a_{d-1} = 0$ y B es por lo tanto linealmente independiente. Queda ahora probar que todo elemento de $F(\alpha)$ se expresa como una combinación lineal con coeficientes en F de los elementos de B. Sea $a = P(\theta)/Q(\theta)$ un elemento arbitrario de $F(\theta)$. Sea $p(x)$ el polinomio irreductible de α. Entonces $p(x)$ tiene grado d. Como $Q(\theta) \neq 0$, el polinomio $p(x)$ no divide a $Q(x)$ y 13 implica que $(p(x), Q(x)) = 1$. Luego, por el Teorema 10 existen polinomios $a(x), b(x) \in F[x]$ tales que $1 = a(x)p(x) + b(x)Q(x)$ y, como $p(\alpha) = 0$,

tendremos $Q(\alpha)b(\alpha) = 1$. Entonces $a = P(\theta)/Q(\theta) = P(\theta)b(\theta)$. Por el algoritmo de la división $P(x)b(x) = q(x)p(x)+r(x)$, donde el polinomio r es nulo o tiene grado menor que d, es decir $r(x) = r_0+r_1x+\ldots r_{d-1}x^{d-1}$. Entonces finalmente tenemos:

$$a = P(\alpha)b(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha) = r_0 + r_1\alpha + \ldots + r_{d-1}x^{d-1}.$$

□

Teorema 24. *El conjunto de los números algebraicos sobre un cuerpo F es un cuerpo.*

Demostración. Sea A el conjunto de los números algebraicos sobre F y considere dos elementos $\alpha, \beta \in A$. Como β es algebraico sobre F, claramente será también algebraico sobre $F(\alpha)$. Por la proposición 23 las extensiones $F(\alpha)|F$ y $F(\alpha,\beta)|F(\alpha)$ son finitas, así que (proposición 18) $F(\alpha,\beta)|F$ es finita y por la proposisión 19 todo número en $F(\alpha,\beta)$ será algebraico sobre F. En particular, los números $\alpha+\beta$, $\alpha.\beta$ y α/β (si $\beta \neq 0$) son algebraicos sobre F. Por lo tanto A es un cuerpo. □

7. Puntos Constructibles II

Como antes, identificaremos el plano bidimensional con el cuerpo de los números complejos.

Proposición 25. *Sea $\zeta = a+bi$ constructible en un paso a partir de un cierto conjunto $P \subset \mathbb{C}$. Suponga que los puntos de P tienen coordenadas en un cuerpo $F \subset \mathbb{R}$. Entonces: o $F(a,b) = F$ o la extensión $F(a,b)|F$ tiene grado 2.*

Demostración. La recta que pasa por los puntos (a_1,b_1) y (a_2,b_2) tiene como ecuación:

$$(a_2-a_1)(y-b_1) = (b_2-b_1)(x-a_1).$$

El círculo centrado en (a_1, b_1) que pasa por (a_2, b_2) es definido por la ecuación:

$$(x - a_1)^2 + (y - b_1)^2 = (a_2 - a_1)^2 + (b_2 - b_1)^2.$$

Si ζ es el punto de intersección de dos rectas que pasan por puntos de P, vemos que las coordenadas de ζ se obtienen resolviendo un par de ecuaciones lineales con coeficientes en F. Es fácil ver de ahí que estas coordenadas pertenecerán al cuerpo F. Si ζ es un punto de intersección entre una recta y un círculo determinados por puntos de P, las coordenadas de P se obtienen resolviendo un sistema donde una ecuación es lineal, y la otra es cuadrática. De la ecuación lineal podemos expresar $y = qx + l$ $(q, l \in F)$ y reemplazar esto en la ecuación cuadrática. Obtenemos así una ecuación cuadrática con coeficientes en F en la variable x. Esto muestra que a será raíz de un polinomio cuadrático con coeficientes en F, de donde (usando la fórmula) tenemos $a = r + s\sqrt{d}$ con $r, s, d \in F$. Luego $b = q(r + s\sqrt{d}) + l$. Es fácil probar que $F(a, b) = F(\sqrt{d})$. Luego $F(a, b) = F$ si $\sqrt{d} \in F$ o $[F(a, b) : F] = 2$ si $\sqrt{d} \notin F$. Finalmente, suponga que ζ se obtiene por la intersección de dos círculos. Podemos restar ambas ecuaciones y anular los terminos cuadráticos. Así obtenemos una relación lineal entre x e y y procedemos como en el caso anterior. □

Teorema 26. Si $\zeta = a + ib$ es constructible, entonces existe una cadena finita cuerpos:

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbb{R}$$

tales que $a, b \in K_m$ y $[K_j : K_{j-1}] = 2$ para todo $j \in \{1, \ldots, m\}$. Luego: las coordenadas de un punto contructible son números algebraicos cuyos grados son potencias de 2.

Demostración. Sean $\zeta_1, \ldots, \zeta_n = \zeta$ tales que $\zeta_1 = a_1 + b_1 i$ es constructible en un paso a partir de $C = \{O = (0, 0), A = (1, 0)\}$, $\zeta_2 = a_2 + b_2$ es constructible en un paso a partir de $C \cup \{\zeta_1\}$, ... , $\zeta_n = a_n + b_n$ es constructible en un paso a partir de $C \cup \{\zeta_1, \ldots, \zeta_{n-1}\}$. Sean $F_0 = \mathbb{Q}$, $F_1 = \mathbb{Q}(a_1, b_1)$, ... , $F_n = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$. Las coordenadas de C

estan en $F_0 = \mathbb{Q}$, así que por la proposición 25 tenemos $F_1 = F_0$ o $[F_1 : F_0] = 2$. Las coordenadas de $C \cup \{\zeta_1\}$ están en $F_1 = \mathbb{Q}(a_1, b_1)$, así que nuevamente por 25 tenemos $F_2 = F_1$ o $[F_2 : F_1] = 2$. Así, después de aplicar 25 un número finito de veces, concluimos que $F_k = F_{k-1}$ o $[F_k : F_{k-1}] = 2$ para todo $k = 1, \ldots, n$. Eliminando de la lista $F_0 \subset \ldots \subset F_n$ los cuerpos que sean iguales a su sucesor obtenemos una cadena $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbb{R}$ que claramente prueba la primera parte de la proposición. Aplicando sucesivamente el Teorema 18 obtenemos

$$[K_m : K_0] = [K_m : K_{m-1}] \cdot \ldots \cdot [K_1 : K_0] = 2^m.$$

Recuerde que el grado de a es igual a $[\mathbb{Q}(a) : \mathbb{Q}]$. Como $\mathbb{Q} \subset \mathbb{Q}(a) \subset K_m$, aplicando nuevamente 18 tenemos $[K_m : \mathbb{Q}] = [K_m : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}]$. Entonces $[\mathbb{Q}(a) : \mathbb{Q}]$ divide 2^m y será por lo tanto una potencia de 2. Análogamente se procede con b. □

Corolario 27. *Si $\zeta \in \mathbb{C}$ es constructible, entonces existe una cadena finita de cuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_m \subset \mathbb{C}$$

tal que $\zeta \in K_m$ y $[K_j : K_{j-1}] = 2$ para todo $j \in \{1, \ldots, m\}$. Luego: Todo número complejo constructible es un número algebraico cuyo grado es una potencia de 2.

Demostración. Por el teorema anterior existe una cadena finita de cuerpos: $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbb{R}$ tales que $a, b \in K_m$ y $[K_j : K_{j-1}] = 2$ para todo $j \in \{1, \ldots, m\}$. Si $i \in K_m$, entonces $\zeta = a + ib \in K_m$ y no habría nada más que probar. Caso contrario, podemos aumentar el cuerpo $K_m(i)$ a la cadena y tendremos $[K_m(i) : K_m] = 2$ y $\zeta = a + ib \in K_m(i)$. Finalmente, la prueba de que el grado de ζ es una potencia de 2 sigue como en la demostración anterior. □

7.1. La Cuadratura del Círculo

Lema 28. *La distancia entre dos puntos constructibles es un número real constructible.*

Demostración. Sean $P, Q \in \mathbb{C}$ puntos constructibles. Entonces $\zeta = P - Q$ es un número constructible. El círculo centrado en O que pasa por ζ intersecta al eje x en el punto $(|\zeta|, 0)$. Entonces el número $|\zeta|$ es constructible. □

Dado un círculo, ¿es posible construir con regla y compás un cuadrado con igual área? Suponga que el círculo en cuestión tiene como centro un punto O y pasa por un punto A (dados). Naturalmente podemos definir un sistema de coordenadas donde O sea el origen de coordenadas y $A = (1, 0)$. Con estas unidades, el área del círculo será igual a π. Si pudiéramos construir un cuadrado de área π, la distancia entre dos de sus vertices consecutivos sería igual a $\sqrt{\pi}$ y por el corolario 28 este número debería ser algebraico. Esto es absurdo ya que caso contrario $\pi = \sqrt{\pi} \cdot \sqrt{\pi}$ sería algebraico (teorema 24).

7.2. La Duplicación del Cubo

Si nuestro cubo dado tuviera lado 1, para duplicarlo, tendriamos que construir un cubo de lado $\sqrt[3]{2}$. Como antes, esto implicaría que $\sqrt[3]{2}$ sea un número constructible, lo que no es cierto ya que el polinomio irreductible de este número es $x^3 - 2$ y su grado es por lo tanto igual a 3 (no es potencia de 2).

7.3. La Trisección del Ángulo

Dado un ángulo cualquiera, es siempre posible su trisección usando regla y compás? Esto es posible en algunos casos particulares, así por ejemplo, un ángulo recto puede ser fácilmente trisecado: El círculo centrado en $O = (0, 0)$ pasando por $A = (0, 1)$ y el círculo centrado en A pasando por O se intersectan en un punto en el primer cuadrante, que llamaremos P. Claramente el triángulo OPA es equilátero, así que el ángulo $\angle POA$ es $\pi/3$. Entonces OP es una de las trisectrices del ángulo recto del primer cuadrante. Para construir la otra trisectriz basta bisecar el ángulo $\angle POA$. Sin embargo, esta construcción es muy particular y se basa

en las propiedades geométricas especiales de $\pi/3$ (como ser el ángulo de un triángulo equilátero). Veremos ahora que, de hecho, el ángulo $\angle POA$ no puede ser trisecado. Por lo visto arriba el punto P es constructible. Si fuera posible trisecar el ángulo, una de sus trisectrices intersectaría el círculo unitario en el punto $Q = e^{\frac{\pi}{9}i} = \cos(\frac{\pi}{9}) + i\text{sen}(\frac{\pi}{9})$. Entonces Q y en consecuencia su abscisa $\alpha = \cos(\frac{\pi}{9})$ serían constructibles. Igualando las partes reales en $(cos\theta + isen\theta)^3 = cos(3\theta) + isen(3\theta)$ deducimos la identidad:

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta.$$

reemplazando $\theta = \pi/9$ obtenemos la ecuación $8\alpha^3 - 6\alpha - 1 = 0$. El polinomio $8x^3 - 6x - 1$ es irreductible sobre $\mathbb{Q}$ (ejercicio 12) y será por tanto el polinomio minimal de α. Esto prueba que el grado de α es 3, lo que es una contradicción.

8. Condiciones Suficientes para la Constructibilidad

En esta sección demostraremos que las condiciones necesarias para la constructibilidad dadas en la sección 7 son también condiciones suficientes.

Lema 29. *Si* $[E : F] = 2$, *existe* $d \in F$ *tal que* $E = F(\sqrt{d})$.

Demostración. Tome $\alpha \in E \backslash F$. El polinomio minimal $p(x)$ de α sobre F debe tener grado n mayor que 1 ya que $\alpha \notin F$, y menor o igual que 2 puesto que $n = [F(\alpha) : F]$ divide a $[E : F] = 2$. Entonces $p(x)$ tiene grado 2. Además $[F(\alpha) : F] = 2 = [E : F]$ y es fácil deducir de aquí que $F(\alpha) = E$. Sea $p(x) = x^2 + bx + c$. Entonces $\alpha = -b/2 + \sqrt{d}/2$ ó $-b/2 - \sqrt{d}/2$, donde $d = b^2 - 4c \in F$. Finalmente es fácil ver que $E = F(\alpha) = F(\sqrt{d})$.

□

Teorema 30. *Si* $\zeta = a + ib$ *es tal que existe una cadena finita cuerpos:*

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbb{R}$$

con $a, b \in K_m$ *y* $[K_j : K_{j-1}] = 2$ *para todo* $j \in \{1, \ldots, m\}$, *entonces el punto* ζ *es constructible.*

Demostración. Procedemos por inducción en el número m de elementos de la cadena. Si a y b pertenecen a $K_0 = \mathbb{Q}$, entonces estos números serán constructibles ya que el conjunto de los números constructibles es un cuerpo (teorema 4) y todo cuerpo contiene a $\mathbb{Q}$. Supongamos ahora que para toda cadena de m elementos:

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbb{R}$$

con $[K_j : K_{j-1}] = 2$ vale que los elementos de K_m son constructibles. Considere ahora cualquier cadena de $m + 1$ elementos:

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_{m+1} \subset \mathbb{R}$$

con $[K_j : K_{j-1}] = 2$. Sea $d \in K_m$ tal que $K_{m+1} = K_m(\sqrt{d})$ (lema 29). Por la hipótesis de inducción todo número en K_m será constructible, en particular d es constructible. Luego, por la proposición 7 el número $\sqrt{d}$ es constructible. Entonces el conjunto de los números constructibles contiene a K_m y a $\sqrt{d}$ y por lo tanto contiene a $K_m(\sqrt{d})$ (proposición 22), es decir, todo número en K_{m+1} es constructible. □

Corolario 31. *Si* $\zeta \in \mathbb{C}$ *es tal que existe una cadena finita de cuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_m \subset \mathbb{C}$$

con $\zeta \in F_m$ *y* $[K_j : K_{j-1}] = 2$ *para todo* $j \in \{1, \ldots, m\}$, *entonces el número* ζ *es constructible.*

Demostración. Si $\zeta = a + ib \in F_m$, es fácil ver que a y b pertenecen al cuerpo $F_{m+1} = F_m(i)$. Entonces por el teorema anterior a y b son constructibles y por lo tanto ζ será constructible. □

Referencias

[1] Michael Artin: *Algebra.*

[2] Serge Lang: *Algebra.*

[3] Joseh Rotman: *Galois Theory.*

[4] I. Kaplansky: *Fields and Rings.*

Abstract

The present article is a concise and autocontained exposition on the three geometric problems of antiquity and their solutions. The intention is to introduce the abstract concept of Field and some mathematical underlying structures.

Keywords: Fields, ruler and compass, algebraic extensions

Rudy Rosas
Sección Matemáticas,
Departamento de Ciencias,
Pontificia Universidad Católica del Perú
rudy.rosas@pucp.edu.pe