ÍNDICE GENERAL

CAPÍTULO 1

LOS TRES PROBLEMAS

Jamás, que yo sepa, una línea curva puramente
geométrica ha sido igualada
por los geómetras, a una recta dada.
Pierre de Fermat.

Usando solamente la regla y el compás, se pueden construir segmentos de distintos tamaños, cuyas longitudes representan números positivos. Esta relación entre el concepto abstracto de número, por una parte, y la geometría, fue bastante explotada por los matemáticos de la antigua Grecia.

Mediante unos métodos sencillos , a partir de un segmento unitario, se pueden construir todos los demás números enteros positivos. También es posible construir todos los racionales. Usando el Teorema de Pitágoras, se puede construir el número irracional $\sqrt{2}$. Este método de construcción tan poderoso hizo pensar a los griegos, que todos los números eran construibles.

Sabemos que algunos polígonos regulares, como por ejemplo el hexágono se puede construir con regla y compás de manera bastante simple. Basta trazar un círculo, con radio la unidad. Con el compás, manteniendo la misma apertura de sus lados, se llevan ambos lados sobre la circunsferencia y se marcan dos puuntos sobre ella. Entonces el segmento rectilíneo cuyos extremos son esos dos puntos, nos proporciona el lado del hexágono.

Mediante un procedimiento con regla y compás, algo más complejo, es posible también construir el lado de un pentágono regular. Sin embargo, despúés de muchos intentos infructuosos, los geómetras no pudieron hallar método alguno para el lado del heptágono regular. Este tipo de dificultades y otras parecidas, dieron origen a los tres famosos problemas matemáticos de construcción con regla y compás, de la antigüedad. Estos son

- Construir un heptágono regular.
- Duplicar un cubo.

- Trisectar un ángulo de 60^0.

Junto a estos tres acertijos, hay que mencionar el famoso problema de la cuadratura del círculo, de gran importancia en el desarrollo de la matemática y que se relaciona de manera directa con el número π. El enunciado del mismo es bastante simple: dado un circulo de radio 1, hallar un cuadrado que contenga la misma área.

Ejercicios

1. Construir la fracción $\frac{3}{5}$ con regla y compás
2. Construir un octógono regular.
3. Construir un pentágono regular

1.1. Números Racionales. Cuerpos

Definición 1.1 *Se llama* ***Número Racional*** *a toda fracción de la forma*

$$\frac{a}{b}$$

con a y b enteros, siendo b distinto de cero.

Los enteros a y b se llaman, respectivamente, el **Numerador** y el **Denominador** de la fracción.

En el conjunto de los números racionales tenemos definidas un par de operaciones que son la suma y el producto. Ellas satisfacen una serie de propiedades que presentamos a continuación, dentro de un contexto más general de la estructura de cuerpo.

Definición 1.2 *Un* **cuerpo** *es un conjunto $\mathbb{R}$, diferente del vacío, con dos operaciones llamadas suma y producto, denotadas por $+$ y $\cdot$ tales que verifican*

1) Para todo a, b en $\mathbb{R}$, se tiene:

$$a + b \in \mathbb{R} \quad y \quad a \cdot b \in \mathbb{R}$$

2) Para todos a, b, c en $\mathbb{R}$

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}$$

3) Para todo a, b en $\mathbb{R}$ se tiene

$$a + b = b + a \quad y \quad a \cdot b = b \cdot a$$

4) Existen elementos 0 y 1 en $\mathbb{R}$ llamados cero y uno, tales que para todo a en $\mathbb{R}$

$$\begin{aligned} a + 0 &= 0 + a = a, \\ a \cdot 1 &= 1 \cdot a = a \end{aligned}$$

5) Para todo a en $\mathbb{R}$, existe un elemento $-a$ llamado el opuesto de a tal que

$$a + (-a) = (-a) + a = 0$$

6) Si a es diferente de cero, existe un elemento a^{-1} en $\mathbb{R}$ llamado el inverso de a, tal que

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

7) Para todos a, b, c en $\mathbb{R}$

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

De ahora en adelante, las propiedades 1)- 7) serán llamadas **Axiomas de Cuerpo**
También se definen sobre un cuerpo K los

Axiomas de Orden

O1. Existe un subconjunto P de K, cuyos elementos serán llamados **números positivos**, tal que
Si a y b están en P, entonces $a+b$ y ab están en P.

O2. El número 1 es positivo

O3. (Ley de Tricotomía)
Si a es un elemento de K, entonces se cumple una y sólo una de las siguientes condiciones

1. a es positivo
2. $-a$ es positivo
3. a es igual a cero.

Gracias a estos axiomas, podemos definir una relación dentro de K de la forma siguiente:
Relación de Orden
Dados dos elementos a y b en K, diremos que a es menor o igual a b, y se denota

$$a \leq b$$

sí y sólo si $b-a$ es positivo o cero.

El lector puede probar que dicha relación satisface las tres condiciones de una relación de orden para conjuntos en general

1. (Reflexiva) Para todo a en K se cumple $a \leq a$
2. (Ansimétrica). Si $a \leq b$ y $b \leq a$, para lgunos a y b en K, entonces debe ser $a = b$.
3. (Transitiva) Si para tres elementos a, b y c en K se satisface $a \leq b$ y $b \leq c$, entonces se cumple $a \leq c$.

Observación Todo cuerpo K contiene al número 1. De igual manera todas las sumas $1+1, 1+1+1, 1+1+1+1, \ldots$ etc. Si para algún entero n se tiene que

$$\overbrace{1+1+\ldots+1}^{n\ veces} = 0$$

entonces habrá un entero mínimo k con tal propiedad. Se dice entonces que el cuerpo K tiene **Característica k**. Si tal entero no existe, diremos que K tiene **Característica 0**.

Ejemplo 1.1 *Los racionales forman un cuerpo ordenado de carcaterística 0*

Observación Todo cuerpo de carcaterística cero (como es el caso de Q) contiene una copia de los Números Enteros.

Finalmente daremos una propiedad importante de los números racionales.

Teorema 1.1 ***Propiedad Arquimedeana*** *Dados dos números racionales $0 < a < b$, eiste un entero positivo n tal que*

$$na \geq b$$

Demostración Sean $a = x/y$ y $b = z/u$, con x, y, zy u enteros positivos. Se tiene entonces

$$\frac{x}{y} < \frac{z}{u}$$

Igualando los denominadores tendremos

$$\frac{xu}{yu} < \frac{zy}{uy},$$

o bien

$$\frac{xu - zy}{yu} < 0$$

Como $yu > 0$ se debe tener $xu < zy$. Si tomamos $n = zy$, obtenemos

$$n(xu) \geq zy$$

y de aquí se sigue

$$n\,\frac{x}{y} \geq \frac{z}{u}$$

o sea

$$na \geq b.$$

Corolario 1.1 *Si a es un número racional cualquiera, entonces existe un número entero n, tal que*

$$(n-1) < a \leq n$$

Demostarción

Si a en sí mismo es un número entero, entonces basta tomar $n = a$. Si a no es entero, podemos suponer sin pérdida de generalidad que $1 < a$. Entonces por el Teorema anterior, existe un entero n , tal que

$$n = n \cdot 1 \geq a \tag{1.1}$$

Por el Axioma del elemento mínimo para los números enteros, podemos suponer, que n es el mínimo con la propiedad 1.1 Entonces debemos tener $(n-1) < a \leq n$. Con esto se da fin a la prueba.

El entero $n-1$ se llama la **Parte Entera** de a y se denota por $[a]$. Así pues $[13/2] = 6$. Como consecuencia del corolario anterior se tiene

Corolario 1.2 *Todo número racional r se expresa como un entero más otro racional menor que uno. Esto es*

$$r = [r] + r_1,$$

donde $0 \leq r_1 < 1$.

Definición 1.3 *Se llama* ***Cuerpo Arquimedeano*** *a un cuerpo ordenado K de característica cero, que cumple lo siguiente. Para todo par de elementos a y b en K, con $a < b$, existe un entero n tal que $na \geq b$.*

Ejemplo 1.2 *Los Números Racionales son un cuerpo arquimediano.*

Ejercicios

1. Demuestre que la suma y el producto de dos números racionales es un número racional.
2. Demuestre que entre dos números racionales, siempre existe otro número racional.
3. Si a y b son enteros positivos con $a > b$, demustre que $\frac{a}{b} > 1$.
4. Demuestre que todo número racional en la forma decimal se escribe como un número entero positivo seguido por un número finito de dígitos o bien una inifinitud pero con un bloque de ellos que se repiten.
5. Valor Absoluto de un número racional. Si a es un número racional cualquiera se define

$$| a |= \begin{cases} a & \text{si } a > 0 \ , \\ -a & \text{si } a < 0 \ , \\ 0, & \text{si } a = 0. \end{cases}$$

   Demuestre que para x e y racionales se verifican cada una de las siguientes propiedades

   a) $| x | \geq 0$
   b) $| x | = 0 \iff x = 0$
   c) $-| x | \leq x \leq | x |$
   d) $| z | \leq x, \iff -x \leq z \leq x$
   e) Desigualdad Triangular. $| x + y | \leq x + | y |$
   f) $| | x | - | y | | \leq | x - y |$
   g) $| xy | = | x | | y |$
   h) $\left| \frac{x}{y} \right| = \frac{|x|}{|y|}$

1.2. Números Irracionales

Definición 1.4 *Se llama* ***Número Irracional*** *a todo aquel que no sea racional*

Es un hecho bien conocido que $\sqrt{2}$ no puede escribirse como una fracción, con lo cual tenemos nuestro primer ejemplo de número irracional. La demostración es una maravilla de ingenio y simplicidad que pone en alto el poder de la matemática desarrollada por los griegos. Utiliza propiedades de los números enteros, como se verá a continuación

Teorema 1.2 *$\sqrt{2}$ no es racional*

Demostración

Supongamos por el contrario, que $\sqrt{2}$ si es racional. Esto es, existen enteros a y b tales que

$$\sqrt{2} = \frac{a}{b}$$

Podemos suponer además que la fracción ha sido simplificada al máximo, de tal forma que a y b no tengan factores primos en común. Dicho de otra manera, asumiramos que los enteros a y b son primos relativos.

Elevando al cuadrado ambos miembros de la ecuación anterior se obtiene

$$2b^2 = a^2$$

Se sigue entonces que a^2 es un número par. Por lo tanto, a debe ser par y podemos hacer $a = 2t$ donde t es un número entero. Luego

$$2b^2 = 4t^2$$

Cancelando el factor 2 en ambos miembros se llega a la conclusión de que b^2 es par y por lo tanto b debe ser par. Luego hemos demostrado que tanto a como b son pares. Esto contradice la hipótesis de que son enteros primos relativos. Si llegamos a una contradicción es por haber partido de hipótesis falsas. Luego $\sqrt{2}$ es irracional.

Usando argumentos similares se puede demostrar la generalización de lo anterior.

Teorema 1.3 *Si p es un número primo, entonces $\sqrt{p}$ es un número irracional*

Demostración (Ejercicio).

El teorema anterior proporciona una infinitud de números irracionales $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, ... que se pueden formar con las raices cuadradas de los números enteros. ¿ Habrán más números irracionales, aparte de estos? Una posibilidad sería hacer combinaciones de sumas y productos de ellos.

Desafortunadamente, los irracionales no forman un conjunto cerrado bajo las operaciones habituales de suma y producto. Por ejemplo $\sqrt{2} - \sqrt{2} = 0$ es un racional. Igualmente $\sqrt{2}\sqrt{2} = 2$ es racional.

Teorema 1.4 *Si α es un número iracional y r es un racional, entonces los siguientes números son irracionales*

1. $\alpha \pm r$
2. $\alpha.r$
3. $\dfrac{1}{\alpha}$
4. $\dfrac{\alpha}{r}$
5. $\sqrt{\alpha}$

Demostración(Ejercicio)

Seguidamente daremos un método para hallar números irracionales, como raices de polinomios

Definición 1.5 *Un **Polinomio con coeficientes enteros** o Polinomio Entero, es una expresión del tipo*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \tag{1.2}$$

*donde los a_i son números enteros, llamados los **Coeficientes**.*

Una **raiz** de un polinomio $P(x)$ es un número α, tal que

$$P(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0$$

Teorema 1.5 *Si $r = \dfrac{a}{b}$ es una raíz racional del polinomio 2.9 entonces a es un divisor de a_0 y b es un divisor de a_n.*

Demostración

En primer lugar supondrems que a y b bo tienen factores primos en común. Se tiene la relación

$$\alpha\left(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1\right) = -a_0$$

Podemos hacer todos los términos enteros en la ecuación de arriba multiplicando por b^n, se tiene entonces que

$$a \cdot k = -a_0 b^n,$$

donde k es un número entero.
Luego a es un divisor de a_0.

Por otro lado

$$a_n\alpha^n = -(a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0)$$

multiplicando esta exprsión por b^n nos da

$$a_n a^n = -b(s),$$

donde s es un número entero. Luego b divide a a_n.

Sabemos que todo número racional, al escribirlo en la forma decimal, los digitos a la derecha de la coma son finitos o bien infinitos periódicos. Es decir hay un bloque de números que se repiten infinitamente.

Una carcaterización importante de los números irracionales es la siguiente: Al escribir su representación decimal, después de la coma vendrá una sucesión infinita sin ningún patrón de repetición.

Por ejemplo el número que se me acaba de ocurrir

$$\alpha = 23,34101001000100000100000010000000 1.....$$

es irracional, pues a medidas que nos alejamos hacia la derecha el número de ceros aumenta. Añadimos un cero en cada paso. ¿ Puede Ud. cosntruir otro irracional usando patrones no periódicos?

Definición 1.6 *El conjunto de los* ***números Reales****, denotado por* $\mathbf{R}$*, es igual al conjunto de los irracionales, unido al conjunto de los irracionales*

En este conjunto se definen dos operaciones de suma y producto, de manera axiomática, que satisfacen los axiomas de cuerpo. También tendremos en R los axiomas de orden . Además R contiene a Q como subcuerpo.

Por los momentos, la forma de construir los números reales, deja mucho que desear, pues lo que hemos hecho es unir dos conjuntos de números de naturaleza distinta; racionales e irracionales. Más adelante se verá una conexión más armónica y lógica entre ellos. Para llegar a tal punto necesitamos el concepto de límite d euna sucesión de números irracionales. También es necesario incorporar un nuevo axioma, el Axioma del Supremo que establece

Axioma del Supremo
Todo conjunto de números reales distinto del vacío, acotado superiormente posee un supremo.

1.3. Aproximación de irracionales

Los números irracionales se pueen aproximar por racionales con un grado de precisión tan grande como se desee. Por ejemplo

$$\sqrt{2} \simeq 1{,}41421356237....$$

lo podemos aproximar por los racionales

$$\begin{aligned} r_1 &= 1 \\ r_2 &= \frac{14}{10} \\ r_3 &= \frac{141}{100} \\ r_4 &= \frac{1414}{1000} \\ r_5 &= \frac{14141}{10000} \\ &\vdots \end{aligned}$$

POdemos preguntarnos entonces: ¿Cuán cerca estarán estos valores aproximados de $\sqrt{2}$ al valor verdadero? El lector puede observar que la diferencia entre el racional r_n y $\sqrt{2}$, se hace más pequeña a medida que n aumenta de tamaño. Concretamente, se tienen las acotaciones

$$\begin{aligned} |\alpha - r_1| &< 1 \\ |\alpha - r_2| &< 0{,}1 \\ |\alpha - r_3| &< 0{,}01 \\ |\alpha - r_4| &< 0{,}001 \\ |\alpha - r_5| &< 0{,}0001 \\ &\vdots \end{aligned}$$

Este tipo de fracciones con denominador de la forma 10^n son bastante grandes y algo incómodas de manejar. Es posible elegir fracciones con un denominador predeterminado, como veremos en el siguiente

Teorema 1.6 *Sea α un irracional y $n > 0$ un entero. Entonces existe un entero $m > 0$ tal que*

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{2n}$$

Demostración

Por la propiedad Arquimedeana de los números reales, existe un entero $m > 0$ tal que

$$(m-1) < n\alpha < m$$

Entonces afirmamos que la distancia desde $n\alpha$ a alguno de los dos enteros consecutivos $m-1$ y m debe ser menor que $1/2$. En efecto, si suponemos que las dos distancias son mayores que $1/2$, tendremos

$$1 = (m - n\alpha) + (n\alpha - (m-1)) > \frac{1}{2} + \frac{1}{2} = 1$$

lo cual es imposible. Luego podemso asumir que $n\alpha$ está más cercano a m y por lo tanto se tiene

$$|m - n\alpha| < \frac{1}{2} \tag{1.3}$$

Nótese que en esta discusión hemos descartado los casos

$$|m - n\alpha| = \frac{1}{2} \quad y \quad |n\alpha - (m-1)| = \frac{1}{2}$$

pues $n\alpha$ es un irracional.

Finalmente, podemos dividir entre m en la ecuación 1.3 para obtener el resultado buscado, cual es

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{2n}.$$

Estudiamos ahora con cierto detalle a otra aproximación a $\sqrt{2}$ siguiendo un método completamente distinto, proveniente de la Teoría de Números. A fin de comparar la potencia de este método , se pueden pisar un par de teclas en una calculadora para obtener su expresión decimal, la cual siempre será aproximada. Así pues

$$\sqrt{2} \simeq 1{,}41421356237....$$

Para calcular estas aproximaciones usaremos el **Método de las Fracciones Continuas**, que nos permitira obtener una sucesión de fracciones que se aproximan a $\sqrt{2}$, con tanta precisión como se desee.

Comenzamos por observar que

$$\begin{aligned} \sqrt{2} &= 1 + (\sqrt{2} - 1) \\ &= 1 + \frac{1}{1 + \sqrt{2}} \end{aligned}$$

Esta relación permite calcular los valores aproximados de $\sqrt{2}$ mediante un método iterativo. Iremos aproximándonos mediate una sucesión de racionales $r_1, r_2, r_3, \ldots$ que se van generando de manera recursiva. La primera aproximación será tomar la parte entera de $\sqrt{2}$ y por lo tanto el primer término de esta sucesión será $r_1 = 1$. Para elegir el siguiente usamos la fórmula recursiva

$$r_{n+1} = 1 + \frac{1}{1 + r_n} = \frac{2 + r_n}{1 + r_n} \tag{1.4}$$

Hagamos

$$r_n = \frac{p_n}{q_n} \tag{1.5}$$

con p_n y q_n números enteros, una sucesión de racionales. Tendremos la fórmula de iteración

$$\frac{p_{n+1}}{q_{n+1}} = \frac{2 + p_n/q_n}{1 + p_n/q_n} = \frac{2q_n + p_n}{q_n + p_n} \tag{1.6}$$

Comenzamos con los valores iniciales $p_1 = 1$, $q_1 = 1$. Este valor inicial de $r_1 = 1$, se introduce en la fórmula de arriba para calcular r_2, el cual nos da la aproximación $r_2 = 3/2$.

Podemos calcular los primeros diez términos para r_i, en la siguiente tabla

n	p_n	q_n	p_n/q_n	α_n
1	1	1	1	1
2	3	2	3/2	1.5
3	7	5	7/5	1.4
4	17	12	17/12	1.416666
5	41	29	41/29	1.413793103
6	99	70	99/70	1.414285714
7	239	169	239/169	1.4142o1183
8	577	408	577/408	1.4142156862
9	1393	985	1393/985	1,41421319
10	3363	2378	3363/2378	1.4142139797

Se puede deducir de la tabla, de manera empírica, que la sucesión $\{r_n\}$ converge a $\sqrt{2}$. Sin embargo es necesario dar una demostración formal de este hecho.
La demsotración la dividimos en dos partes. En primer lugar demostramos que la sucesión es convergente y que por lo tanto el límite

$$\lim_{x \to \infty} r_n$$

existe.
En segundo lugar probaremos que el límite es exactamente $\sqrt{2}$, esto es

$$\lim_{x \to \infty} r_n = \sqrt[n]{2}$$

.

Para demostrar la existencia del límite nos apoyamos en el siguiente resultado teórico, el cual se basa en la completitud de los números reales:

Teorema 1.7 *(Cauchy)*

- *Toda sucesión de números reales monótona creciente y acotada superiormente posee un límite*
- *Toda sucesión de números reales monótona decreciente y acotada inferiormente posee un límite*

Demostraremos que r_n es acotada tanto inferiormente como superiormente. Para todo entero n se tiene que $p_n > 1$ y $q_n > 1$, por lo tanto

$$1 < \frac{2q_n + p_n}{p_n + q_n} < 2$$

y luego $1 < r_n < 2$, para todo $n \geq 1$.

La sucesión r_n no es monótona reciente ni decreciente. Sin embargo ella está formada por dos sucesiones monótonas: la de los términos pares es decreciente y la de los pares es creciente, como se verá a continuación. Pero antes necesitamos un resultado intermedio

Teorema 1.8 *Para todo $n \geq 1$ se tiene*

$$p_{n+2}q_n - q_{n+2}p_n = 2 \cdot (-1)^{n+1}$$

Demostración

Haremos la prueba por inducción sobre n. Para n = 1 el resultado es cierto, pues $p_3q_1 - q_3p_1 = 7 - 5 = 2$. Supongamos que para $n-1$ el resultado sea cierto y probaremos que se cumple para n. Entonces

$$\begin{aligned}
p_{n+2}q_n - q_{n+2}p_n &= (2q_{n+1}p_{n+1})(q_{n-1} + p_{n-1}) - (p_{n+1} + q_{n+1})(2q_{n-1} + p_{n-1}) \\
&= 2q_{n+1}q_{n-1} + 2q_{n+1}p_{n-1} + p_{n+1}q_{n-1} + p_{n+1}p_{n-1} \\
&\quad -2p_{n+1}q_{n-1} - p_{n+1}p_{n-1} - 2q_{n+1}q_{n-1} - q_{n+1}p_{n-1} \\
&= q_{n+1}p_{n-1} - p_{n+1}q_{n-1} \\
&= (-1)({}_{n+1}q_{n-1} - q_{n+1}p_{n-1}) \\
&= (-1)2(-1)^n \\
&= 2(-1)^{n+1}
\end{aligned}$$

Dividiendo entre $q_{n+2}q_n$ en la relación anterior, tendremos

$$r_{n+2} - r_n = \frac{2(-1)^n}{q_{n+2}q_n}$$

Luego la sucesión de los términos impares escreciente y la sucesión de los términos pares es decreciente. Ambas sucesiones están acotadas, como ya ha sido verificado. Por el Teorema de Cauchy las dos sucesiones convergen a un límite. POdemos hallar el valor de este límite, independientemente de cual sucesión estemos cosiderando. . Sea

$$L = \lim_{x \to \infty} r_n$$

Usando la relación.2.11 se obtiene

$$L = \frac{2 + L}{1 + L}$$

o sea

$$L^2 + L = 2 + L$$

y por lo tanto

$$L = \sqrt{2}$$

Ejercicios

1. Demuestre que toda sucesión de números reales monótona creciente y acotada superiormente posee un límite
2. Demuestre que entre dos números irracionales, existe siempre un número racional.
3. Hallar una sucesión de fracciones que converja hacia π
4. Generalize la técnica de aproximación a $\sqrt{2}$, para el caso $\sqrt{p}$, donde p es cualquier entero positivo que no sea un cuadrado perfecto. Comience tomando el primer término $r_1 = [\sqrt{p}]$, la Parte Entera del número.

1.4. Números algebraicos

Definición 1.7 *Un cuerpo F se dice una* **extensión** *de un cuerpo K, si $K \subseteq F$ y además K es un subcuerpo de F.*

Definición 1.8 *Sea F una extensión de K. Un elemento $\alpha \in F$ se dice* **algebraico sobre** *K si α satisface una ecuación polinomial*

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0 \tag{1.7}$$

con $a_i \in K$.

Observación Si α es algebraico sobre K, entonces α puede ser raíz de muchos polinomios con coeficientes en K, y entonces el polinomio f en la definición anterior no es único.

Sin embargo hay un polinomio especial, entre los polinomios que anulan a α, que merece particular antención.

Definición 1.9 *Sea α algebraico sobre K. Entonces el* **polinomo minimal de** *α, es el polinomio mónico, de grado mínimo que anula a α.*

Observación Si $f(x)$ es el polinomio minimal de α, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$. Si $f(x)$ es reducible entonces $f(x) = p(x)q(x)$, y entonces ambos polinomios $p(x)$ y $q(x)$ son mónicos. Además alguno de ellos anula a α y esto contradice la minimalidad de $f(x)$.

Ejemplo 1.3 *Sea $\alpha = 1+\sqrt{2}$, el cual es algebraico sobre $\mathbb{Q}$. El polinomio minimal de α viene dado por:*

$$f(x) = x^2 - 2x - 1$$

Definición 1.10 *Sea α algebraico sobre K. Entonces diremos que α es* **algebraico de grado** *n, si el grado del polinomio minimal de α es n.*

Ejemplo 1.4 *El número irracional $\alpha = 1 + \sqrt{2}$ es algebraico de grado 2.*

Veremos ahora, a partir de un ejemplo concreto, cómo se puede construir un nuevo cuerpo, usando el cuerpo base Q y un elemento algebraico α.

Consideremos el número irracional $\sqrt{2}$, el cual no pertenece al conjunto de los Racionales Q. Ciertamente, $\sqrt{2}$ es un número algebraico sobre Q, de grado dos, con polinomio minimal

$$p(x) = x^2 - 2$$

Definimos ahora

$$Q(\sqrt{2}) = \{a + b\sqrt{2} \mid \quad a\,y\,b \text{ son racionales}\}$$

Dentro de este conjunto se definen dos operaciones, suma y producto de la forma siguiente:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

y

$$(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$$

Entonces el lector puede verificar facilmente que este par de operaciones son cerradas y satisfacen las leyes conmutativas, asociativas y distributivas. Además $0 = 0+0\sqrt{2}$ y $1 = 1+0\sqrt{2}$ y son los elementos neutros para la suma y el producto, respectivamente. Por otro lado, el opuesto de $a+b\sqrt{2}$ es el elemento $-a-b\sqrt{2}$, el cual pertenece a $Q(\sqrt{2})$. Finalmente, proaremos que todo eelemento no nulo de $Q(\sqrt{2})$ posee inverso bajo el producto. En efecto si $a+b\sqrt{2} \neq 0$, entonces tenemos la relación

$$(a+b\sqrt{2})\cdot(a-b\sqrt{2}) = a^2-2b^2 \tag{1.8}$$

Nótese que el número racional en el lado derecho de la ecuación es distinto de cero. Caso contrario se tendría $a^2 = 2b^2$, con lo cual $a/b = \sqrt{2}$, siendo esto es una contradicción.

Podemos entonces dividir el segundo factor en la ecuación 1.8 y se tendrá

$$(a+b\sqrt{2})\cdot\frac{1}{a^2-2b^2}(a-b\sqrt{2}) = 1$$

Hemos entonces probado que el conjunto $Q(\sqrt{2})$ satisface todas las propiedades de un cuerpo. Este se llama el **Cuerpo Cuadrático** generado por $\sqrt{2}$ sobre los racionales.

Son fáciles de verificar un par de hechos

1. $Q(\sqrt{2})$ contiene a Q como subcuerpo.
2. $Q(\sqrt{2})$ es un espacio vectorial sobre Q de dimensión 2.

Definición 1.11 *Sea F una extensión de K. La dimensión de F como espacio vectorial sobre K, se denomina* **grado de la extensión** *de F sobre K, y se denota por $[F:K]$.*

Si el grado de la extensión F sobre K es finito, diremos que F es una **extensión** finita de K.

Teorema 1.9 *Sea α algebraico sobre K de grado n. Entonces el grado de $K(\alpha)$ sobre K es n.*

Demostración Sea $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ el polinomio minimal de α, el cual es irreducible, y consideremos el Dominio de Integridad $K[\alpha]$, formado por todas las expresiones del tipo:

$$b_m\alpha^m + \cdots + b_1\alpha + b_0$$

donde $b_i \in K$.

Notemos que α satisface el polinomio $f(x)$ y por lo tanto

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

Esta última expresión, nos permite reducir toda potencia de α de grado n o superior, a una combinación lineal de los elementos $\alpha^{n-1}, \ldots, \alpha, 1$. Luego

$$K[\alpha] = \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \cdot 1 \mid b_i \in K\}$$

Afirmamos además que $K[\alpha]$ es un cuerpo, para lo cual probaremos que todos los inversos de los elementos de $K[\alpha]$ están en $K[\alpha]$.

En efecto, sea $t = b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0$ un elemento en $K[\alpha]$ distinto de cero. Entonces el polinomio $g(x) = b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ es primo relativo con $f(x)$, pues $f(x)$ es irreducible y $f(x)$ no divide a $g(x)$. Luego existen polinomios $q(x)$ y $s(x)$ en $\mathbb{Q}[x]$, tales que

$$f(x)q(x) + g(x)s(x) = 1$$

Sustituyendo esta expresión en el valor de $x = \alpha$, tenemos

$$f(\alpha)q(\alpha) + g(\alpha)s(\alpha) = 1$$

Teniendo en cuenta que $f(\alpha) = 0$, se deduce

$$g(\alpha)s(\alpha) = 1$$

o sea

$$t \cdot s(\alpha) = 1$$

lo cual implica que $t^{-1} = s(\alpha) \in K[\alpha]$.

Por lo tanto, hemos probado que $k[\alpha]$ es un cuerpo y su cuerpo de cocientes es igual a si mismo. Por lo tanto $K(\alpha) = K[\alpha]$.

Para finalizar mostraremos que los elementos $1, \alpha, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)$ sobre K. Para probar esto, sólo nos falta verificar que estos elementos son linealmente independientes.

Supongamos que

$$C_{n-1}\alpha^{n-1} + \cdots + C_1\alpha + C_0 \cdot 1 = 0$$

para algunos elementos $C_i \in K$.

Luego el polinomio $f'(x) = C_{n-1}x^{n-1} + \cdots + C_1x + C_0$ es de grado menor que el grado de $f(x)$ y además anula a α. Esto contradice la minimalidad de $f(x)$ y por lo tanto $C_{n-1} = C_{n-2} = \cdots = C_1 = C_0 = 0$.

Los elementos $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forman una base de $K(\alpha)$ sobre K y por lo tanto

$$[K(\alpha) : K] = n$$

Con esto se da fin a la prueba.

Ejercicios

1. Demuestre que $Q(3+5\sqrt{2}) = Q(\sqrt{2})$
2. Demuestre que $Q(\sqrt{3} \neq Q(\sqrt{2}$
3. Si α es una raíz quinta de la unidad, demuestre que el grado de $Q(\alpha)$ sobre Q es igual a 4.

1.5. Extensiones de Cuerpos

El caso típico de una extensión del cuerpo $\mathbb{Q}$, consiste en un cuerpo de la forma $\mathbb{Q}(\alpha)$, donde α es raíz de un polinomio $p(x)$ irreducible en $\mathbb{Q}[x]$. Dichas extensiones son cuerpos que están dentro del cuerpo de los números complejos, y contienen a $\mathbb{Q}$ como subcuerpos. La forma de construirlos, depende del polinomio $p(x)$ y de la raíz α

Ejemplo 1.5 *El cuerpo $\mathbb{C}$ de los números complejos es una extensión finita del cuerpo $\mathbb{R}$ de los números reales.*

Definición 1.12 *Sea K un cuerpo y α un elemento en una extensión de K. Entonces el* **cuerpo engendrado por α sobre K,** *denotado por $K(\alpha)$, es igual a la intersección de todas las extensiones de K que contienen a α.*

Observación Es claro que la definición de arriba tiene sentido, pues si α está en una extensión F, se tiene que $K(\alpha) \subseteq F$.

Por otro lado, es fácil probar que la intersección de cualquier número de cuerpos es un cuerpo.

Si K es un cuerpo, F una extensión de K y $\alpha \in F$, sea $K[\alpha]$ el subanillo de F formado por todas las expresiones polinomiales en K.

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 \tag{1.9}$$

donde $a_i \in K$.

Entonces $K[\alpha]$ es un Dominio de Integridad que contiene a K y al elemento α.

El cuerpo de cociente de este Dominio de Integridad, formado por los cocientes de las expresiones del tipo (1.9), lo denotamos por U_α.

Es claro entonces que U_α es una extensión de K que contiene a α, y por lo tanto está contenido en $K(\alpha)$. Por otro lado, si L es una extensión de K que contiene a α, entonces debe contener todas las expresiones del tipo $a_n\alpha^n + \cdots + a_1\alpha + a_0$. Como L es un cuerpo, se tiene que L contiene todos los cocientes de dichas expresiones y por lo tanto L contiene a U_α. Luego U_α y $K(\alpha)$ son la misma cosa. Hemos demostrado entonces

Proposición 1.1 *Sea K un cuerpo y α un elemento en una extensión de K. Entonces $K(\alpha)$ consiste en todas las formas racionales*

$$\frac{f(\alpha)}{g(\alpha)}$$

donde $f(\alpha), g(\alpha)$ están en $K[\alpha]$ y $g(\alpha) \neq 0$

Teorema 1.10 *Sea K un cuerpo y $K(\alpha)$ una extensión finita de grado n. Entonces α es algebraico de grado n sobre K.*

Demostración Consideremos los elementos $1, \alpha, \alpha^2, \ldots, \alpha^n$ en $F(\alpha)$. Puesto que la dimensión del espacio $K(\alpha)$ sobre K es n, estos $(n+1)$ elementos son linealmente independientes. Luego existen elementos $a_0, a_1, \ldots, a_n$ en K, no todos nulos, tales que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 \cdot 1 = 0$$

Luego α es algebraico sobre K. El grado del polinomio minimal de α es menor o igual a n. Si suponemos que el grado de este polinomio es $m < n$, entonces por el teorema anterior se deduce $[K(\alpha) : K] = m < n$, lo cual es una contradicción. Luego α es algebraico de grado n.

Nuestro próximo paso será probar que el conjunto de los elementos algebraicos sobre un cuerpo K, es un cuerpo. Antes necesitamos el siguiente resultado.

Proposición 1.2 *Sea K un cuerpo y F una extensión finita de K. Sea L una extensión finita de F. Entonces L es una extensión finita de K y además: $[L : K] = [L : F][F : K]$.*

Demostración Sea $[F : K] = n$ y $[L : F] = m$. Sean $\{x_1, \ldots, x_n\}$ una base de F sobre K, y $\{y_1, \ldots, y_m\}$ una base de L sobre F.

Probaremos que $\{x_i y_j\}$ $1 \leq i \leq n$, $1 \leq j \leq m$, es una base de L sobre K.

Sea $l \in L$. Entonces existen elementos $l_1, \ldots, l_m$ en F, tal que

$$l = l_1y_1 + \cdots + l_my_m \tag{1.10}$$

Como los l_i están en F, para cada l_i existen elementos $k_{ij} \in K$, tales que

$$l_i = k_{i1}x_1 + \cdots + k_{in}x_n, \quad \text{para todo} \quad 1 \leq i \leq m \tag{1.11}$$

Sustituyendo estos valores de l_i en la expresión (1.10) obtenemos

$$l = k_{11}x_1y_1 + \cdots + k_{m1}x_1y_m + \cdots + k_{1n}x_ny_1 + \cdots + k_{mn}x_my_n$$

Luego los elementos $\{x_i y_j\}$ son un conjunto de generadores de L sobre K.

Supongamos que para algunos elementos a_{ij} en K, $1 \leq i \leq n$, $1 \leq j \leq m$, no todos nulos, se tiene

$$(a_{11}x_1y_1 + \cdots + a_{1m}x_1y_m) + \cdots + (a_{n1}x_ny_1 + \cdots + a_{nm}x_ny_m) = 0$$

Luego reagrupamos estos elementos para obtener

$$(a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n)y_1 + \cdots + (a_{1m}x_1 + \cdots + a_{nm}x_n)y_m = 0$$

Como $x_i \in F$ para todo $1 \leq i \leq n$ y $a_{ij} \in K \subseteq F$, se tiene que los elementos

$$C_j = a_{1j}x_1 + \cdots + a_{nj}x_n, \qquad 1 \leq j \leq m$$

están todos en F, pues F es un cuerpo.

Luego se tendrá la combinación lineal

$$C_1 y_1 + \cdots + C_m y_m = 0$$

Como los $y_1, \ldots, y_m$ son linealmente independientes sobre F, se deben anular todos los C_i. Por lo tanto

$$C_k = 0, \quad \text{para todo} \quad 1 \leq k \leq m$$

o sea

$$a_{1j} x_1 + \cdots + a_{nj} x_n = 0, \qquad 1 \leq j \leq m$$

Nótese que los a_{ij} están en K y los elementos $x_1, \ldots, x_n$ son linealmente independientes sobre K. Luego se deduce de esto que $a_{ij} = 0$ para todo $1 \leq i \leq n$, $1 \leq j \leq m$.

En conclusión hemos probado que el conjunto $\{x_i y_j\}$ constituye una base de L sobre K, la cual tiene $m.n$ elementos. Luego $[L : K] = m.n$. Con esto queda probado la proposición.

Teorema 1.11 *Sea K un cuerpo, y F una extensión de K. Entonces el conjunto de elementos de F que son algebraicos sobre K es un subcuerpo de F.*

Demostración Sea $\mathcal{A}$ el conjunto de los elementos de F que son algebraicos sobre K. Para probar que $\mathcal{A}$ es un cuerpo basta tomar un par de elementos cualquiera a y b en $\mathcal{A}$, y demostrar

i) $a \pm b$ está en $\mathcal{A}$
ii) ab está en $\mathcal{A}$
ii) a/b está en $\mathcal{A}$, si $b \neq 0$

Sea $T = K(a)$ y $L = T(b)$. Entonces $a \in L$ y $b \in L$. Por ser L un cuerpo se tiene que $a \pm b \in L$, $ab \in L$ y $a/b \in L$, si $b \neq 0$.

Luego $[K(a+b) : K] \leq [L : K] = [L : T][T : K]$

Ahora bien, como b es algebraico sobre K, de grado n, digamos, entonces b es algebraico sobre $K(a)$, de grado $\leq n$. Luego

$$[L : T] = [T(b) : K(a)] \leq n$$

Sabemos también que a es algebraico sobre K, de grado m digamos. Luego

$$[T : K] = [K(a) : K] = m$$

Por lo tanto

$$[K(a+b) : K] \leq m.n$$

Luego $K(a+b)$ es una extensión finita de K, y por el teorema 1.10, se tiene que $a+b$ es algebraico sobre K. De igual forma se prueba que los elementos $a-b$, ab y a/b son algebraicos sobre K.

1.6. Solución a los tres problemas

Desde el punto de vista del Álgebra podemos preguntarnos, si se tiene un cuerpo K ¿Cuales números son construibles partiendo de K?.

En primer lugar, medante la construcción con regla y compás, se pueden hallar puntos en el plano que resultan ser intersecciones entra rectas y circunsferencias. Estas intersecciones nos conducen a sistemas de ecuaciones lineales y cuadráticas. Con las ecuaciones lineales no podemos salir del cuerpo base K. Sin embargo, las cuadráticas permiten crear nuevas extensiones como veremos adelante.

Supongamos que tenemos a un geómetra bien sentado frente a su mesa de trabajo con suficiente papel blanco, equipado de lápices, una regla y un compás. Este hombre quiere construir el número ω con esos elementos de trabajo. Se le impone la condición de considerar como cuerpo de partida los números racionales Q. En un primer paso obtendrá un número α_1 el cual es solución de una ecuaión cuadrática

$$x^2 + b_1 x + c_1 = 0$$

Si α_1 es racional entonces no habremos salido del cuerpo base. Si por el contrario, $\alpha_1 = a + b\sqrt{s_1}$ es un irracional, entonces este número se encuentra en la extensión finita de grado dos $Q(\sqrt{s_1})$

Para el paso siguiente, nuestro hombre podrá partir del cuerpo $Q(\sqrt{s_1})$ y realizar una nueva operación de regla y compás. Entonces, posiblemente obtendrá una ecuación cuadraática, cuya solución será u irracional $\alpha_2 = a' + b'\sqrt{s_2}$ el cual puede estar fuera del cuerpo de partida. Es evidente que el grado de esta nueva estensión sobre $Q(\sqrt{s_1})$ es 2. Además, es fácil verificar que el grado de $Q(\sqrt{s_2})$ sobre Q es igual a 4.

Continuando de esta manera, si nuestro geómetra termina exitosamente su trabajo y nos da una construcción con regla y compás de ω, se habrá generado una torre de extensiones de grado 2^n de Q.

$$Q \subset Q(\alpha_1) \subset Q(\alpha_1, \alpha_2) \subset \ldots \subset Q(\alpha_1, \alpha_2, \ldots \alpha_n)$$

donde $w \in Q(\alpha_1, \alpha_2, \ldots \alpha_n)$

Observación La extensión $Q(\alpha_1, \alpha_2, \ldots \alpha_n)$ es una extensión finita de Q de grado 2^n . Esto implica que ω satisface un polinomio de grado 2^n con coeficientes en Q.

Hemos demostrado entonces el siguiente

Teorema 1.12 *Todo número construible es algebraico. Más precisamente: Si el número ω es construible sobre Q entonces es algebraico sobre Q y además satisface*

$$[Q(\omega) : Q] = 2^n$$

para algún $n > 0$.

La pregunta natural que podemos formular ahora es la siguiente: ¿ Habrán números alebraicos que no sean construibles? La respuesta es Si.

Ejemplo 1.6 *El número $\alpha = cos20^\circ$ es un número algebraico el cual no es construible.*

Para demostrar este hecho, notemos la identidad trigonométrica

$$cos3\theta = 4cos^3\theta - 3cos\theta$$

Poniendo $\theta = 20^\circ$ y sabiendo que $Cos60^\circ = 1/2$ tendremos la ecuación para α,

$$4\alpha^3 - 3\alpha = 1/2,$$

Por lo tanto α es una raíz de la ecuación polinomial cúbica

$$8x^3 - 6x - 1 = 0$$

y por lo tanto es algebraico sobre Q.

Sin embargo este polinomio es irreducible sobre el cuerpo de los números Racionales (Ejercicio). Por lo tanto el grado de la extensión de $Q(\alpha)$ es 3, el cual no es una potencia de dos. De acuerdo al teorema anterior, α no puede ser construible.

Este ejemplo demuestra la imposibilidad de dividir el ángulo de 60° en tres partes iguales usando regla y compás, uno de los tres problemas famosos de la antiguedad.

CAPÍTULO 2

MÉTODOS ANALÍTICOS

2.1. El Número de Euler

En otra de las caras de la Pirámide de Samarkanda los arqueólogos encontraron los versos de arriba. Había uno entre ellos bastante sagaz, especie de Indiana Jones, que se destacaba por su habilidad para descifrar códigos secretos. Construyóun número algo extraño, contando las letras de cada palabra y colocando un punto después del primer número. El resultado fue algo familiar

$$e \cong 2{,}7182818284...$$

Este es el Número de Euler, considerado por algunos como el más importante de toda la matemática. En estas notas contaremos algunas de sus propiedades, pues se llevaría un volumen completo escribir todo lo que se sabe sobre él.

Comenzamos nuestra aproximación desde el campo de las funciones reales.

Definimos la **Función Exponencial** como la serie de potencias

$$e^x = \sum_{k=0}^{\infty} \frac{(x)^k}{k!} \tag{2.1}$$

Para probar que dicha función está bien definida, debemos probar en primer lugar que la serie de arriba converge, para todo valor de x.

Recordemos la definición de convergencia de series.

Definición 2.1 *Se dice que la serie de números reales*

$$\sum_{n=1}^{\infty} a_n$$

es convergente, si a partir de un valor de n grande, la suma de los últimos términos se va haciendo arbitrariamente pequeña. Esto es

$$\lim_{k \longrightarrow \infty} \sum_{n=k}^{\infty} a_n = 0.$$

Probar la convergencia o no de una serie, usando directamente la definición, puede ser muy complicado. Por eso existen criterios de convergencia, que facilitan este trabajo.

Recordemos el Criterio de Convergencia del Cociente

Teorema 2.1 *Sea la serie*

$$\sum_{n=1}^{\infty} a_n$$

con $a_n > 0$ *y supongamos que*

$$\lim_{n \longrightarrow \infty} \frac{a_{n+1}}{a_n} = r$$

Si $r < 1$ *la serie converge.*

Teorema 2.2 *Si x es un número real , entonces la serie*

$$e^x = \sum_{k=0}^{\infty} \frac{(x)^k}{k!}$$

converge.

Demostración Se tiene en primer lugar el caso especial $x = 0$ en le cual la serie es convergente a 1. Sea ahora $x > 1$. Entonces

$$\begin{aligned} \lim_{n \longrightarrow \infty} \frac{a_{n+1}}{a_n} &= \lim_{n \longrightarrow \infty} \frac{\dfrac{(x)^{k+1}}{(k+1)!}}{\dfrac{x^k}{k!}} \\ &= \lim_{n \longrightarrow \infty} \frac{x}{(k+1)} \\ &= 0 \end{aligned}$$

Entonces basta aplicar el criterio anterior para demostrar la convergencia.

Si una serie es convergente, entonces la sucesión de sus términos, necesariamente converge a cero. Luego tenemos un resultado importante

Corolario 2.1 *Si x es un número real positivo*

$$\lim_{n\longrightarrow\infty} a_n = \lim_{n\longrightarrow\infty} \frac{x^n}{n!} = 0$$

Si $x < 0$ entonces en la serie 2.9 se alternan los términos positivos y negativos. Esto es

$$e^x = \sum_{k=0}^{\infty} \frac{(-1)^k (y)^k}{k!}$$

con $y = -x$.

Daremos ahora otro criterio de convergencia, para series de términos con signos alternados

Teorema 2.3 *Criterio de Leibniz.*

Si la sucesión a_n es monótona decreciente y además

$$\lim_{n\longrightarrow\infty} a_n = 0$$

Entonces la serie

$$\sum_{k=0}^{\infty} (-1)^{n+1} a_n$$

es convergente

Estamos ahora en posición favorable para dar la segunda parte de la desmotarción del teorema. En efecto, si x es número real negativo, hacemos $x = -y$ con $y > 0$. Por la propiedad Arquimedeana de los números reales existe un entero postivo n, tal que $y < n + 1$. Entonces tenemos

$$a_{n+1} = \frac{y^{n+1}}{(n+1!} = \frac{y}{(n+1)} \frac{y^n}{n!} < \frac{y^n}{n!} = a_n$$

Luego se tendrá

$$e^x = \sum_{k=0}^{\infty} \frac{(x)^k}{k!} = \sum_{k=0}^{n} \frac{(x)^k}{k!} + \sum_{k=n+1}^{\infty} \frac{(-1)^{k+1} (y)^k}{k!}$$

El primer sumando del lado derecho es una suma finita y por lo tanto representa un número real. El segundo sumando es una serie infinita,la cual es convergente por el criterio de Leibniz.

Con esto damos fin a la demostración del Teorema 1.2.

Seguidamente pasamos a revisar una serie de propiedades interesantes de la función exponencial $f(x) = e^x$, que se derivan de su desarrollo en serie.

1. $e^0 = 1$

2. El Número de Euler, el cual es la base de los logaritmos Neperianos satisface

$$f(1) = e$$

3. La función exponencial $f(x)$ posee derivadas de todos los órdenes.

4. $f'(0) = 1$

5. Como $\frac{d}{dx}e^x = e^x$. La función exponencial satisface la ecuación diferencial

$$\frac{d}{dx}f(x) = f(x).$$

6. Para x e y números reales $e^{x+y} = e^x \dot{e}^y$

Ella es la única función de variable real con estas propiedades.

Para la segunda propiedad podemos calcular el valor aproximado del número e, usando las sumas parciales de la serie.

$$e = \sum_{k=0}^{\infty} \frac{1}{n!}$$

Hagamos

$$S_n = 1 + 1 + 1/2 + 1/6 + \ldots + 1/n!,$$

para $n \geq 0$.

Calculamos los primeros 8 valores de S_n y los organizamos en una tabla. Nótese la buena velocidad con la cual los términos de la serie convergen al valor real.

n	S_n
1	2
2	2.5
3	2.66666
4	$2{,}708\overline{3}$
5	$2{,}71\overline{6}$
6	$2{,}7180\overline{5}$
7	2.71825396
8	2. 71827876

La propiedad 5 nos dice que la función exponencial transforma sumas en productos, comportándose como una potencia de un número real con exponente entero.

Teorema 2.4 *Si x e y son númers reales, entonces*

$$e^{x+y} = e^x \cdot e^y$$

Demostración

Desarrollaremos en serie ambas expresiones. Es claro que el producto de dos series de número reales es otra serie de números reales. Para demostrar la igualdad de arriba, probaremos que las dos coinciden en en término enésimo. Esto es, si se tiene

$$e^{x+y} = \sum_{k=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{k=0}^{\infty} \alpha_n,$$

y

$$e^x e^y = \left(\sum_{k=0}^{\infty} \frac{(x)^n}{n!} \right) \left(\sum_{k=0}^{\infty} \frac{(x)^n}{n!} \right) = \sum_{k=0}^{\infty} \beta_n,$$

entonces debemos demostrar $\alpha_n = \beta_n$. Pero esto es cierto, pues

$$\begin{aligned} \alpha_n &= \frac{(x+y)^n}{n!} \\ &= \frac{x^n + \binom{n}{1} x^{n-1} y + \ldots + \binom{n}{k} x^{n-k} y^k + \ldots + y^n}{n!} \\ &= \frac{x^n}{n!} \cdot 1 + \frac{x^{n-1}}{(n-1)!} \cdot y + \ldots \frac{x^{n-k} y^k}{(n-k)! k!} \ldots 1 \cdot \frac{y^n}{n!} \\ &= \beta_n \end{aligned}$$

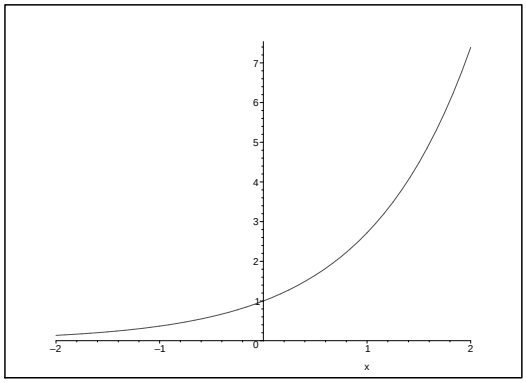

Figura 2.1: La función $f(x) = e^x$

Esta constante e aparece en conexión con los números complejos, mediante la relación maravillosa

$$e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta \tag{2.2}$$

donde el lado derecho representa un número complejo en el círculo unitario de ángulo θ. Dicha fórmula se conoce con el nombre de *Fórmula de Euler* en honor a Leonhard Euler, quien la descubrió cerca de 1740.

Las series de potencia de $\mathrm{sen}\,\theta$ y $\cos\theta$, se pueden obtener por medio del Teorema de Taylor del cálculo diferencial. Tenemos también la posibilidad de calcular estas series, trabajando de manera formal. Sobre las funciones seno y coseno, apenas conocemos los valores para $\theta = 0$. Así pues

$$\begin{aligned} \mathrm{sen}(0) &= 0 \\ \cos(0) &= 1 \end{aligned}$$

Luego las series de potencias respectivas serán

$$\mathrm{sen}\,\theta = a_1\theta + a_2\theta^2 + \cdots + a_n\theta^n + \cdots \tag{2.3}$$
$$\cos\theta = 1 + b_1\theta + b_2\theta^2 + \cdots + b_n\theta^n + \cdots \tag{2.4}$$

Recordemos que la función seno es impar, es decir $\mathrm{sen}(-\theta) = -\,\mathrm{sen}\,\theta$, luego podemos igualar sus series respectivas y comparar los coeficientes para obtener

$$\begin{aligned} a_1 &= a_1 \\ a_2 &= -a_2 \\ a_3 &= a_3 \\ a_4 &= -a_4 \\ &\vdots \end{aligned}$$

De aquí se deduce que todos los coeficientes de las potencias pares son cero. Luego (2.3) se puede escribir

$$\mathrm{sen}\,\theta = a_1\theta + a_3\theta^3 + a_5\theta^5 + \cdots + a_{2n+1}\theta^{2n+1} + \cdots \tag{2.5}$$

También, la función coseno es par, es decir $\cos\theta = \cos(-\theta)$ y por lo tanto los coeficientes de las potencias impares son todas nulas. Luego se tiene el desarrollo en serie para el coseno

$$\cos\theta = 1 + b_2\theta^2 + b_4\theta^4 + \cdots + b_{2n}\theta^{2n} + \cdots \tag{2.6}$$

Para calcular el valor de los coeficientes a_i en (2.5), derivamos la serie del seno y la igualamos a la del coseno pues $\dfrac{d}{d\theta}\,\mathrm{sen}\,\theta = \cos\theta$.

De aquí obtenemos que $a_1 = 1$.

Una segunda derivación de la serie (2.5) produce

$$\frac{d^2}{d\theta^2}\operatorname{sen}\theta = -\operatorname{sen}\theta$$

Luego

$$\begin{aligned}\frac{d^2}{d\theta^2}\operatorname{sen}\theta &= 2\cdot 3a_3\theta + 5\cdot 4a_5\theta^3 + \cdots + (2k+1)2ka_{2k+1}\theta^{k-1} + \cdots \\ &= -a_1\theta - a_3\theta^3 - \cdots - a_{2k-1}\theta^{k-1} - \cdots\end{aligned}$$

Igualando los coeficientes de las potencias del mismo orden nos da

$$\begin{aligned}a_3 &= \frac{-a_1}{2\cdot 3} \\ a_5 &= \frac{-a_3}{5\cdot 4} \\ &\vdots \\ a_{2k+1} &= \frac{-a_{2k-1}}{(2k+1)\cdot 2k} \\ &\vdots\end{aligned}$$

Esta sucesión de recurrencia nos da los valores:

$$a_3 = \frac{-1}{3!}, \quad a_5 = \frac{1}{5!}, \quad a_{2k+1} = \frac{(-1)^k}{(k+1)!}, \quad \cdots$$

Luego la serie del seno de θ es

$$\operatorname{sen}\theta = \theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots \tag{2.7}$$

Haciendo el mismo tipo de análisis para la serie del coseno nos da

$$\cos\theta = 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots$$

Volvamos ahora al desarrollo en serie de potencias de e^{kx}, y pongamos $k = i,\ x = \theta$. Luego nos queda

$$\begin{aligned}e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \cdots + \frac{(i\theta)^n}{n!} + \cdots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \cdots\end{aligned}$$

Olvidando por los momentos el problema de la convergencia, podemos hacer un reordenamiento de esta última serie para obtener

$$e^{i\theta} = \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} + \cdots\right) + i\left(\theta + \frac{\theta^3}{3!} - \frac{\theta^5}{5!} + \cdots\right) = \cos\theta + i\,\mathrm{sen}\,\theta$$

Al menos heurísticamente, hemos probado la fórmula de Euler. Bastaría dar un toque final de rigurosidad a nuestros métodos, probando la convergencia de ambas series para cualquier θ número real.

La fórmula de Euler permite usar una notación más corta para expresar los números complejos. Si z es cualquier complejo, se tiene la representación polar

$$z = |z|(\cos\theta + i\,\mathrm{sen}\,\theta)$$

luego podemos hacer

$$z = |z|e^{i\theta}$$

Ejemplo 2.1 *Supongamos que queremos calcular* $\mathrm{sen}\,3\theta$ *y* $\cos 3\theta$*.*

Tenemos entonces

$$\begin{aligned}\cos 3\theta + i\,\mathrm{sen}\,3\theta &= e^{i3\theta} = \left(e^{i\theta}\right)^3 = (\cos\theta + i\,\mathrm{sen}\,\theta)^3 \\ &= \cos^3\theta + 3\cos^2\theta i\,\mathrm{sen}\,\theta + 3\cos\theta i^2\,\mathrm{sen}^2\,\theta + i^3\,\mathrm{sen}^3\,\theta \\ &= (\cos^3\theta - 3\cos\theta\,\mathrm{sen}^2\,\theta) + i(3\cos^2\theta\,\mathrm{sen}\,\theta - \mathrm{sen}^3\,\theta)\end{aligned}$$

Igualando partes reales e imaginarias nos quedan las fórmulas

$$\begin{aligned}\cos 3\theta &= \cos^3\theta - 3\cos\theta\,\mathrm{sen}^2\,\theta \\ \mathrm{sen}\,3\theta &= 3\cos^2\theta\,\mathrm{sen}\,\theta - \mathrm{sen}^3\,\theta\end{aligned}$$

2.2. El poder del Análisis

El estudio profundo de la naturaleza
es la fuente más abundante
para los descubrimientos matem áticos.
Joseph Fourier

Jean Baptiste Joseph Fourier (1768- 1830) fue un científico natural, cuya área principal de investigación fue la Teoría del Calor. En sus estudios d elas ecuaciones diferenciales, Furier hace uso d elas series trigonométricas, que habían sido estudiadas por L. Euler y D. Bernoulli.Desarrolló un método para demostrar que todas las funciones continuas se pudene expresar como una serie d etérminos trigonométricos, las llamadas Series de Fourier.
Usando métodos del Análisis demostró algunos hechos importantes sobre los números reales.

Teorema 2.5 *(Fourier (1815)) El número e es irracional*

Demostración

Recordemos que la función exponencial posee un desarrollo en serie de potencias convergente

$$e^x = \sum_{k=0}^{\infty} \frac{(x)^k}{k!}$$

Probaremos que e es irracional. Supongamos por el absurdo que

$$e = \sum_{k=0}^{\infty} \frac{(1)^k}{k!} = \frac{a}{b},$$

con a y b enteros distintos de cero. Sea $e = \sigma_n + \rho_n$, donde

$$\sigma_n = \sum_{k=0}^{n} \frac{1}{k!}$$

y

$$\rho_n = \sum_{k=n+1}^{\infty} \frac{1}{k!}$$

Luego

$$n!be = n!a$$

El lado derecho de esta ecuación es un número entero. En el lado izquierdo tenemos

$$n!be = n!b\sigma_n + n!b\rho_n,$$

siendo el primer sumando un número entero.

Afirmamos que el segundo sumando es un racional menor que uno. Pues

$$n!b\rho_n = b(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \ldots)$$

Sin embargo, esta serie la podemos acotar usando la serie geométrica. Esto es

$$\begin{aligned} \frac{1}{n+1} &< \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \ldots \\ &< \frac{1}{n+1)} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \ldots = \frac{1}{n} \end{aligned}$$

Por lo tanto

$$n!b\rho_n$$

no puede ser un entero, lo cual es una cotradicción.

El matemático francés Laplace (1749- 1827) fue uno de los grandes fundadores de la Teoría de las porbabilidades: a partir de 1774 escribió una gran cantidada de ensayos sobre este tema. El fue el primero en demostrar que el área bajo la curva de probabilidad es igual a la raíz cuadrada de Pi. En su trabajo *Essai philosophique des probabilités* demuestra la fórmula

$$\int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi}$$

Es decir, $\sqrt{\pi}$ se puede interpretar como el área debajo de la gráfica de la función positiva $f(e^{-x^2}$ (Ver la figura)

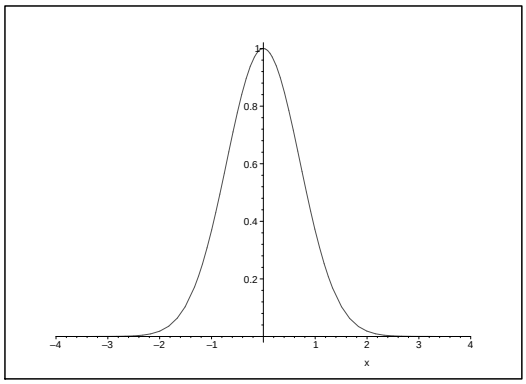

Figura 2.2: la función $f(x) = exp(-x^2)$

Laplace también fue el inventor del método de las transformadas (que llevan su nombre) para resolver ecuaciones difereniales. Nos interesa estudiar la Transformada de laplace de un polinomio

$$I(t) = \int_0^t e^{t-u} f(u) du$$

donde t es un número complejo y $f(u)$ un polinomio con coeficientes complejos.

Integrando por partes, tantas veces como sea necesario, en la ecuación de arriba nos da

$$\begin{aligned} I(t) &= e^t \sum_{j=0}^{\infty} f^{(j)}(0) - \sum_{j=0}^{\infty} f^{(j)}(t) \\ &= e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t) \end{aligned}$$

donde n es el grado de $f(x)$.

Si $f(x) = \sum_{j=0}^{n} a_j x^j$, hagamos

$$\overline{f}(x) = \sum_{j=0}^{n} \mid a_j \mid x^j$$

Entonces

$$\begin{aligned} I(t) &\leq \left| \int_0^t e^{t-u} f(u) du \right| \\ &\leq t \quad max \left\{ \left| e^{t-u} \right| \right\} max|f(u)| \\ &\leq |t||e^t|\overline{f}(t). \end{aligned}$$

Hemos demostrado entonces el siguiente

Teorema 2.6 *Sea*

$$f(x) = \sum_{m=0}^{n} a_m x^m$$

y

$$F(x) = \sum_{k=0}^{m} f^k(x),$$

y hagamos

$$F(0)e^x - F(x) = Q(x).$$

Entonces

$$\mid Q(x) \mid \leq e^{|x|} \sum_{m=0}^{n} \mid a_m \mid\mid x^m \mid .$$

Demostración (Ejercicio)

Observación

Este resultado es fundamental para la demostración que dió Hermite, sobre la transcendencia de e, la cual será abordada en la próxima sección

2.3. Números Transcendentes.

El primero demostrar que hay números transcendentes fue el matemático francés J. Louiville (1809-1892). Su demostración es de tipo constructiva, exhibiendo unos números algo extraños que no son algebraicos.

Louville demostró que los irracionales algebraicos, son aquellos que no pueden ser aproximados con un alto grado de precisión, mediante fracciones. Más precisamente

Teorema 2.7 *(Louiville) Sea α un número algebraico irracional con polinomio minimal*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

y $\dfrac{p}{q}$ una aproximación racional de α, con q suficientemente grande. Entonces se debe tener

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{n+1}} \tag{2.8}$$

Demostración En primer lugar probaremos que

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}$$

En efecto, calculando $f(p/q)$ y colocando q^n en todos los denominadores tendremos

$$\begin{aligned}\left|f\left(\frac{p}{q}\right)\right| &= \frac{p^n}{q^n} + \frac{q}{q}\frac{p^{n-1}}{q^{n-1}} + \ldots + \frac{q^{n-1}}{q^{n-1}}\frac{p}{q} + \frac{q^n a_0}{q^n} \\ &= \frac{|p^n + qp^{n-1} + \ldots + q^{n-1}p + q^n a_0|}{|q^n|} \\ &\geq \frac{1}{|q^n|}\end{aligned}$$

Por el Teorema del Valor Medio,existe un número real ξ entre α tal que

$$f(\alpha) - f(x) = f'(\xi)(\alpha - x)$$

Sea $M = \text{máx}\,|f'(z)|$, con $|z - \alpha| < 1$. Luego

$$|f(\alpha) - f(x)| \leq M \cdot |\alpha - x|$$

Recordemos que $f(\alpha) = 0$. Luego, si existe una fracción $x = p/q$, tal que $|\frac{p}{q} - \alpha| < 1|$ se tendrá

$$\left|f\left(\frac{p}{q}\right)\right| \leq M\left|\alpha - \frac{p}{q}\right|$$

Por lo tanto, escoginedo a q suficientemente grande se obtiene

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{n+1}}$$

El teorema anterior se puede expresar en palabras: Si α es un irracional algebraico de grado n, entonces no existe una aproximación racional de grado $n+1$.
Con este resultado se pueden construi números reales que no satisfagan la condición de arriba, tal como lo hizo el genio de Louiville.

Teorema 2.8 *El número*

$$\alpha = \sum_{m=1}^{\infty} \frac{1}{10^{m!}}$$

es transcendente.

Demostración

En primer lugar, la serie de arriba es convergente, pues es dominada por la serie geométrica

$$\sum_{m=1}^{\infty} \frac{1}{10^{m}}$$

Tomamos ahora la sucesión de racionales

$$\frac{p^n}{q^n} = \sum_{m=1}^{n} \frac{1}{10^{m}}$$

con $p^n > 1$, $q^n > 1$ y $(p^n, q^n) = 1$. Es claro que la sucesión $\left\{\frac{p^n}{q^n}\right\}$ converge a α.

Note que q^n es un divisor de $10^{n!}$, lo cual implica que $q_n \leq 10^{n!}$. Entonces tendremos

$$\begin{aligned} 0 &< \alpha - \frac{p^n}{q^n} = \sum_{m>n} \frac{1}{10^{m}} \\ &= \frac{1}{10^{(n+1)!}} \left(1 + \frac{1}{10^{n+2}} + \frac{1}{10^{(n+2)(n+3)}} + \dots\right) \\ &< \frac{2}{10^{(n+1)!}} = \frac{2}{(10^{n!})^{n+1}} \\ &< \frac{1}{q_n^{n+1}} \end{aligned}$$

En consecuenia, hemos demostardo la desigualdad

$$\left|\alpha - \frac{p^n}{q^n}\right| < \frac{1}{q_n^{n+1}}$$

lo cual nos dice que α no puede ser algebraico

Teorema 2.9 *(Hermite)(1873) El número* **e** *es trascendente.*

Demostración Supongamos que e un cero de $P(x)$, donde

$$P(x) = \sum_{k=0}^{m} g_k x^k, \quad g_0 \neq 0, \quad m > 0$$

y los g_h son enteros. Sea p un número primo mayor que $max(m, |g_0|)$ y sea

$$f(x) = \frac{1}{(p-1)!} x^{p-1}(1-x)^p(2-x)^p \cdots (m-x)^p = \sum_{k=0}^{n} a_k x^k$$

o bien

$$f(x) = \frac{s(x)}{(p+1)!},$$

donde

$$s(x) = x^{p-1}(1-x)^p(2-x)^p \cdots (m-x)^p$$

Este polinomio $f(x)$, es el **Polinomio de Hermite de orden m**, cuyas raices son $0, 1, 2, \ldots, m$, todas ellas de orden p, salvo el 0 de orden $p-1$.

Podemos escribir la expansión de $s(x)$

$$s(x) = (m!)^p x^{p-1} + A_p x^p + \cdots$$

con A_i enteros.

También podemos hallar la expasión de Taylor en serie de potencias alrededor de h, para cada $h = 0, 1, 2, \ldots m$

$$s(x) = B_{p,h}(x-h)p + B_{p+1,h}(x-h)^{p+1} + \cdots$$

donde los $B_{i,h}$ son enteros.

Podemos ahora construir los términos $F(x)$ y $Q(x)$ del Teorema anterior, usando el polinomio $f(x)$. Tenemos entonces

$$0 = F(0)P(e) = F(0)\sum_{h=0}^{m} g_h e^h = \sum_{h=0}^{m} g_h F(h) + \sum_{h=0}^{m} g_h Q(h) \tag{2.9}$$

Tenemos entonces

$$\begin{aligned} \sum_{h=0}^{m} g_h F(h) &= g_0 \sum_{k=0}^{n} f^k(0) + \sum_{h=1}^{m} g_h \sum_{k=0}^{n} f^k(h) \\ &= g_0((m!)^p + pA_p + \ldots) + \sum_{h=1}^{m} g_h(pB_{p,h} + p(p+1)B_{p+1,h} + \ldots) \end{aligned}$$

Esta expresión es un entero. Además, como $p \nmid g_0(m!)^p$ y los restantes términos son enteros divisibles por p se tiene

$$| \sum_{h=0}^{m} g_k F(h) | \geq 1.$$

Si podemos probar que existe un primo $p > max(m, |g_0|)$, tal que

$$| \sum_{h=0}^{m} g_h Q(h) | < 1$$

entonces se obtiene una contradicción a partir d e la ecuación (2.9). Por el Teorema anterior, será suficiente probar que para cualquier x fijo, tendremos

$$\sum_{k=0}^{n} | a_k | | x |^k \longrightarrow 0, \quad cuando \quad p \longrightarrow \infty$$

Sin embargo, esto se cumple, pues, cuando $p \longrightarrow \infty$

$$\sum_{k=0}^{n} | a_k | | x |^k \leq \frac{|x|^{p-1} \prod_{h=1}^{m} (h + |x|)^p}{(p-1)!} \longrightarrow 0$$

2.4. Una serie famosa para Π

Usted puede dudar de la existencia de Dios.
Pero como un buen matemático
Ud. debe creer en la existencia de El LIbro.
Un Libro que guarda Dios en donde están
las más bellas demostraciones matemáticas.
Paul Erdös

Antes de probar la transcendencia del número π. Daremos una serie famosa para calcularlo, obtenida por Leonhard Euler

Teorema 2.10

$$\sum_{n\geq 1}\frac{1}{n^2}=\frac{\pi^2}{6}$$

Demostración

Esta serie nos da el valor de la Función de Riemann $\xi(2)$. La demostración que daremos aquí es de Le Veque del año 1956. Sin embargo Euler probó un resultado más general que esto en 1734.

Evaluaremos de dos maneras distintas la integral doble

$$I=\int_0^1\int_0^1\frac{1}{1-xy}\quad dxdy$$

En primer lugar, descomponemos en serie de potencias, la función que aparece dentro de la integral. Por lo tanto

$$\begin{aligned}
I &= \int_0^1\int_0^1\sum_{n\geq 0}(xy)^n\quad dxdy\\
&= \sum_{n\geq 0}\int_0^1\int_0^1 x^n y^n\quad dxdy\\
&= \sum_{n\geq 0}\left(\int_0^1 x^n\quad dx\right)\left(\int_0^1 y^n\quad dy\right)\\
&= \sum_{n\geq 0}\frac{1}{n+1}\frac{1}{n+1}=\sum_{n\geq 0}\frac{1}{(n+1)^2}=\sum_{n\geq 0}\frac{1}{n^2}
\end{aligned}$$

Podemos evaluar a I de otra forma, haciendo un cambio de coordenadas $T(x,y)=(u,v)$, donde

$$u=\frac{x+y}{2},\quad v=\frac{y-x}{2}$$

El determinante Jacobiano de esta transformación viene dado por

$$J = \frac{\partial(x,y)}{\partial(u,v)} = \begin{vmatrix} \frac{dx}{du} & \frac{dx}{dv} \\ \frac{dy}{du} & \frac{dy}{dv} \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$$

$u = v$

R

$T(R)$

$x = 0$ $x = 1$

$v = 1 - u$

Haciendo $x = u - v$, e $y = u + v$, la integral se transforma en

$$I = \iint_{T(R)} \frac{dv}{1 - u^2 + v^2} \quad 2dv$$

Notese que por la simetría con respecto al eje u de la función

$$f(u,v) = \frac{1}{1 - u^2 + v^2}$$

basta calcular la integral por sobre el eje u y luego duplicar este valor. Esto es

$$I = 4\int_0^{1/2} \left(\int_0^u \frac{dv}{1 - u^2 + v^2} \right) du + 4\int_{1/2}^1 \left(\int_0^{1-u} \frac{dv}{1 - u^2 + v^2} \right) du$$

Usamos ahora la fórmula de integración

$$\int \frac{dx}{a^2 + x^2} = \frac{1}{a}\, arctan\left(\frac{x}{a}\right) + C,$$

luego

$$\int_0^u \frac{dv}{1-u^2+v^2} = \frac{1}{\sqrt{1-u^2}}\, arctan\left(\frac{u}{\sqrt{1-u^2}}\right) - 0$$

y por lo tanto

$$I = I_1 + I_2,$$

donde

$$I_1 = 4\int_0^{1/2} \frac{1}{\sqrt{1-u^2}}\, arctan\left(\frac{u}{\sqrt{1-u^2}}\right) du$$

e

$$I_2 = 4\int_{1/2}^1 \frac{1}{\sqrt{1-u^2}}\, arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right) du$$

Haciendo las sustituciones $u = sen\theta$, $u = cos\theta$, en la primera y segunda integral, respectivamente, se pueden simplificar y calcular las dos. Sin embargo utilizaremos otro camino más corto.

Notemos que las funciones

$$g(u) = arctan\left(\frac{u}{\sqrt{1-u^2}}\right),$$

y

$$h(u) = arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right)$$

tienen derivadas

$$g'(u) = \frac{1}{\sqrt{1-u^2}}, \quad y \quad h'(u) = -\frac{1}{2}\left(\frac{1}{\sqrt{1-u^2}}\right)$$

Entonces usamos la fórmula de integración

$$\int f'(x)f(x)dx = \frac{1}{2}f(x)^2 + C$$

Tenemos entonces

$$\begin{aligned} I_1 &= 4(\frac{1}{2})\left[\left(arctan\frac{1}{\sqrt{3}}\right)^2 - arctan(0)^2\right] \\ &= 2\left(\frac{\pi}{6}\right)^2 - 0^2 \end{aligned}$$

$$\begin{aligned} I_2 &= -4\left[arctan(0)^2 - \left(arctan\frac{1}{\sqrt{3}}\right)^2\right] \\ &= 4\left(\frac{\pi}{6}\right)^2 \end{aligned}$$

Por lo tanto

$$I = 2\left(\frac{\pi}{6}\right)^2 + 4\left(\frac{\pi}{6}\right)^2 = \frac{\pi^2}{6}$$

2.5. π es irracional

Hoy y ayer, o vivir cuadrando el triste ruedo
del vacío infinito.
Imposible medición, fracasada por
un mal comienzo.
R. Ocsicinarf.

El número π ha estado rodeado de leyendas, en donde se mezclan misteriosos cálculos y construcciones geométricas desde los egipcios hasta nuestros días. El problema de cuadrar el círculo, el cual consiste en hallar un cuadrado de igual área a un cîrculo dado, espoleó la imaginación de muchos matemáticos del pasado, académicos notables, taumaturgos, así como simples aficionados del noble arte de los números.

Pero ¿ Cuál es el valor exacto del número π? . No importa si no lo recordamos en este momento. Un matemático persa del sigloXII, de nombre Ocsicnarf, lo dejó grabado en uno de los muros de una pirámide en Samarkanda. Para guardar el secreto de su conocimiento y hacerlo llegar a futuras generaciones de otros *Cuadradores del círculo* y ahorrales años de investigación. Un conocimiento obtenido con gran sacrificio, después de dedicar muchos años, meses y días este acertijo. Todo quedó encriptado en un poema, que reproducimos arriba. El número de letras en cada palabra nos da la clave para obtener una aproximación de π, hasta 18 cifras, algo bastante sorprendente para su época. Luego

$$\pi \cong 3{,}141592653589793238...$$

Teorema 2.11 *El número* Π *es irracional.*

Demostración Supongamos por el contrario que $\pi = \frac{a}{b}$, donde a y b son enteros positivos. Sea

$$f(x) = \frac{x^n(a-bx)^n}{n!}$$

y

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \ldots + (-1)^n f^{(2n)}(x).$$

De acuerdo al segundo lema se sigue que $F(0)$ y $F(\pi)$ son enteros. Ahora bien

$$\frac{d}{dx}(F'(x)sen(x) - F(x)cosx) = f(x)sen(x),$$

por lo tanto

$$\int_0^\pi f(x)sen(x)dx = F(\pi) - F(0) \tag{2.10}$$

es un entero. Pero, para $0 < x < \pi$ y n suficientemente grande tendremos

$$0 < f(x)sen(x) < \frac{\pi^n a^n}{n!} < \frac{1}{n},$$

de tal forma que

$$0 < \int_0^\pi f(x)sen(x)dx < 1,$$

lo cual contradice a (2.10) como una ecuación en enteros.

2.6. Π es Transcendente

Teorema 2.12 *(Lidemann) (1882) El número* Π *es trascendente.*

Demostración

Probaremos que $i\pi$ no es algebraico. Con esto es suficiente, pues los números algebraicos forman un cuerpo y además i es algebraico, pues satisface la ecuación $x^2 + 1 = 0$.

Supongamos por el contrario que $i\pi$ satisface una ecuación de la forma

$$f(x) = ax^m + a_1x^{m-1} + \ldots = 0, \quad a > 0$$

Entonces $ai\pi$ es una solución de la ecuación

$$a^{m-1}f(\frac{x}{a}) = x^m + a_1x^{m-1} + \ldots = 0.$$

Esta suposición de que $i\pi$ es algebraico nos lleva a concluir que $ai\pi$ es algebraico. Para llegar a una contradicción probaremos que $ai\pi$ no satisface una ecuación de la forma

$$P(y) = y^m + k_{m-1}y^{m-1} + \ldots + k_0 = 0, \quad m > 0.$$

Factorizando el polinomio de arriba en el cuerpo de los números complejos nos da

$$P(y) = \prod_{h=1}^{m}(y - a\alpha_h).$$

Probaremos ahora que

$$R = \prod_{h=1}^{m}(e^0 - e^{\alpha_h}) \neq 0.$$

Este resultado será la clave para lograr la demostración del teorema. Por supuesto, esto es un absurdo, pues contradice la relación bastante conocida: $1 + e^{\pi i} = 0$.

Ahora bien, R puede escribirse como

$$R = c + \sum e^{\alpha} + \sum e^{\alpha+\alpha'} + \ldots = c + e^{\beta 1} + e^{\beta_2} + \ldots + e^{\beta_r},$$

Notemos que en la factorización de $P(y)$ aparecen algunas raíces complejas y sus conjugadas. Entonces tendremos $e^{\alpha_i}e^{-\alpha_i} = 1$ para estas parejas. Por lo tanto c es el número de unos en la factoriación de R. Por otro lado, $\beta_1, \beta_2, \ldots, \beta_r$ son términos no nulos.

Sea p un número primo mayor que max $(c, a, \prod_{h=1}^{r} a|\beta_h|)$ y consideremos

$$f(x) = \frac{(ax)^{p-1})\prod_{h=1}^{r}(ax - a\beta_h)^p}{(p-1)!} \tag{2.11}$$

desarrollando este producto nos da

$$f(x) = \Sigma_{k=0}^{n} a_k x^k \tag{2.12}$$

Repitiendo los mismos pasos que dimos en la demostración del Teorema de Hermite, tendremos

$$\begin{aligned} f(x) &= \frac{A_{p-1}x^{p-1} + A_p x^p + \ldots}{(p-1)!} \\ &= \frac{\gamma_{p,h}(x-\beta_h)^p \gamma_{p+1,h}(x-\beta_h)^{p+1} + \ldots}{(p-1)!}, \end{aligned}$$

donde los A_i son funciones simétricas de $\{a\beta_1, \ldots, a\beta_r\}$ y por lo tanto funciones simétricas de $a\alpha_1, \ldots a\alpha_h$. Por lo tanto los A_i son números racionales enteros y además A_{p-1} no es divisible por p.

Al igual que en la demostración de Hermite hacemos

$$\begin{aligned} 0 &= F(0)R \\ &= F(0)(c + \sum_{h=1}^{r} e^{\beta_h} \\ &= cF(0) + \sum_{h=1}^{r} F(\beta_h) + \sum_{h=1}^{r} Q(\beta_h) \end{aligned}$$

En primer lugar observamos que

$$cF(0) = c(a_{p-1} + pA_p + \ldots)$$

es un entero racional que no es múltiplo de p. también

$$\begin{aligned} \sum_{h=1}^{r} F(\beta_h) &= \sum_{h=1}^{r}(p\gamma_{p,h} + p(p+1)\gamma_{p+1,h} + \ldots) \\ &= p\sum_{h=1}^{r}\gamma_{p,h} + p(p+1)\sum_{h=1}^{r}\gamma_{p+1,h}\ldots \\ &= pc_p + p(p+1)c_{p+1} + \ldots, \end{aligned}$$

donde $c_p, c_{p+1}, \ldots$, por ser funciones simétricas de $a\beta_1, \ldots, a\beta_r$, resultan ser enteros.. SE sigue entonces que $\sum_{h=1}^{r} F(\beta_h)$ es un múltiplo de p y por tanto

$$\mid cF(0) + \sum_{h=1}^{r} F(\beta_h) \mid \geq 1,$$

Solo falta probar que para un p suficientemente grande

$$\mid \sum_{h=1}^{r} Q(\beta_h) \mid < 1$$

Pero, cuando $p \longrightarrow \infty$ se tiene

$$\Sigma_{k=0}^{n} \mid a_k \mid \mid x \mid^k \leq \frac{(a \mid x \mid)^{p-1}) \prod_{h=1}^{r} (a \mid x \mid -a \mid \beta_h \mid)^p}{(p-1)!} \longrightarrow 0$$

y de esto se sigue la demostración.

BIBLIOGRAFÍA

[1] J. K. Arrow, *Social Choice and Individual Values*, 2nd ed., Wiley, New York, 1963.