Teoremas Fundamentales

Jesús Pérez Sánchez

Marzo 2008

Introducción

Esta monografía, en realidad, es un viaje, o paseo, por algunos espacios maravillosos de la Matemática. Nos toparemos con teoremas fundamentales de la Matemática y algunas aplicaciones de los mismos.

Para mi ha sido placentero este deambular por la Aritmética, el Álgebra y el Análisis.

Con la esperanza de que este sencillo material sea de utilidad, sobre todo a los alumnos de nuestra Licenciatura, sólo les pido que observaciones y sugerencias, sean enviadas a : jesusp@ula.ve

Mérida, marzo de 2008.

Índice general

1. Teorema Fundamental de la Aritmética. **1**

2. El Teorema Fundamental del Álgebra. **21**

3. El Teorema Fundamental del Cálculo **31**

4. El Teorema de Baire. **43**

Capítulo 1

Teorema Fundamental de la Aritmética.

Al hacer una presentación formal del conjunto de los números naturales, $\mathbb{N} = \{0, 1, 2, 3 \ldots\}$, debemos recurrir a los **axiomas de Peano** (matemático italiano, 1858-1932):

(P_1) El objeto 0 (cero) pertenece al conjunto $\mathbb{N}$, $0 \in \mathbb{N}$.

(P_2) Si $x \in \mathbb{N}$, existe (y es único) $s(x) \in \mathbb{N}$ (el sucesor de x).

(P_3) Para todo $x \in \mathbb{N}$, es $s(x) \neq 0$ (0 no es sucesor de otro número natural).

(P_4) Si $s(x) = s(y)$, entonces, $x = y$ (un número natural no puede ser sucesor de dos naturales distintos).

(P_5) Si A es un subconjunto de $\mathbb{N}$, tal que:

i) $0 \in A$.

ii) $a \in A$ implica que $s(a) \in A$,

entonces, $A = \mathbb{N}$.

Nota 1.1: Después de definir la suma (+) y el producto (.), en $\mathbb{N}$, se demuestra que: $s(x) = x + 1$, para todo $x \in \mathbb{N}$ (ver [1], pág. 33)

A partir de (P_5), podemos deducir el

Primer Principio de Inducción Completa:

Sea n_0 un número natural, y supongamos que para cada natural $\mathbf{n} \geq n_0$, hay asociada una afirmación A_n. Admitamos que sea posible probar que:

i) A_{n_0} es verdadera

ii) Para cada natural $k \geq k_0$, **si** A_k es verdadera, **entonces** A_{k+1} **también** es verdadera.

En estas condiciones, $\mathbf{A_n}$ **es verdadera, para todo** $\mathbf{n \geq n_0}$**.**

Demostración:

Sea $S = \{\mathbf{n} \in \mathbb{N}$: $A_{n_0+\mathbf{n}}$ es verdadera $\}$. Tenemos que, según i), $0 \in S$.

Supongamos que $k \in S$.

Luego, A_{n_0+k} es verdadera.

Ahora, en virtud de ii), resulta que A_{n_0+k+1} también es verdadera; de modo que: $k+1 \in S$.

Así, S satisface las condiciones del axioma (P_5).

Conclusión: $S = \mathbb{N}$. ∎

Ejemplo 1.1:

a) Demostrar que $2^{4n} - 1$ es múltiplo de 15, para todo número natural $n \geq 1$.

b) Demostrar que $2^n > 2n + 1$, para todo número natural $n \geq 3$.

Solución:

a) En este caso, $A_{\mathbf{n}}$ significa:

$$2^{\mathbf{4n}} - 1 \quad \text{es múltiplo de15.}$$

Luego, $A_{\mathbf{1}}$ es la afirmación:

$$2^{4\times\mathbf{1}} - 1 \quad \text{es múltiplo de 15, la cual es verdadera.}$$

Supongamos ahora que:

$$2^{\mathbf{4k}} - 1 \quad \text{es múltiplo de 15, con} \quad k \geq 1. \tag{1.1}$$

Queremos ver si, **entonces**, $2^{\mathbf{4(k+1)}} - 1$ también es múltiplo de 15.

Pero,

$$2^{4(\mathbf{k+1})} - 1 = 2^{4k}.\mathbf{2}^4 - 1 = 2^{4k}\mathbf{(15+1)} - 1 = \mathbf{2}^{4k}.\mathbf{15} + \mathbf{2}^{4k}\mathbf{-1} \tag{1.2}$$

En (1.2), el primer sumando, obviamente es múltiplo de 15, y el segundo también lo es, en virtud de (1.1).

Así, $2^{4(\mathbf{k+1})} - 1$ queda expresado como suma de dos múltiplos de 15, por lo cual, también es múltiplo de 15, como queríamos probar.

b) Tenemos que, $A_{\mathbf{n}}$ quiere decir:

$$2^{\mathbf{n}} > 2\mathbf{n} + 1, \quad \text{para} \quad n \geq 3$$

Así, A_3 nos dice:

$$2^{\mathbf{3}} > 2.\mathbf{3} + 1, \text{lo cual es verdadero.}$$

Supongamos que A_k es cierto, para $k \geq 3$, o sea,

$$2^{\mathbf{k}} > 2\mathbf{k} + 1, \qquad k \geq 3 \tag{1.3}$$

Queremos saber si (1.3) implica que

$$2^{\mathbf{k+1}} > 2(\mathbf{k+1}) + 1, \qquad \text{para} \quad k \geq 3$$

Ahora bien, multiplicando ambos miembros de (1.3) por 2, llegamos a:

$$2^{k+1} > \mathbf{4k} + 2$$

O sea,

$$2^{k+1} > \mathbf{2k}+\mathbf{2k} + 2 \tag{1.4}$$

Pero, como $k \geq 3$, resulta que $2k + 2 > 3$. Usando este último resultado en (1.4), llegamos a:

$$2^{k+1} > 2k + 3 = \mathbf{2(k+1)+1}, \qquad \text{como queriamos.}$$

■

Ahora, a partir del Primer Principio de Inducción completa, obtendremos un notable resultado, conocido como **Principio de Buena Ordenación** (que abreviaremos como P.B.O):

Todo subconjunto $\mathbf{A \subseteq N}$, no vacio, posee un elemento mínimo.

Demostración: Sea X el conjunto de todos los números naturales n, tales que $\{0, 1, 2, ..., n\} \subseteq \mathbb{N} - A$.

Así, $0 \in X$ significa: $0 \notin A$; y si n_0 es tal que $n_0 \in X$, entonces, $n_0 \notin A$, y $0, 1, 2, ..., n_0 - 1$ tampoco pertenecen a A.

No olvidemos que queremos probar que A tiene un elemento mínimo.

Si $0 \in A$, no tenemos más nada que probar, (0 sería el elemento mínimo de A).

Supongamos, entonces que $0 \notin A$, luego, $0 \in X$.

También resulta que $X \neq \mathbb{N}$, pues $X \subseteq \mathbb{N} - A$ y $A \neq \emptyset$.

Así, en virtud de (P_5), concluimos que: existe un número natural m_0 tal que, $m_0 \in X \quad$ y $\quad s(m_0) = m_0 + 1 \notin X$.

De modo que,

$$m_0 + 1 \in A \qquad \text{y} \qquad \{0, 1, 2, \ldots, m_0\} \subseteq \mathbb{N} - A.$$

En otras palabras, $m_0 + 1$ es el elemento mínimo de A. ∎

Veamos a continuación, que el **P.B.O** implica el Primer Principio de inducción completa.

En efecto, sea $\mathcal{P}$ una propiedad, referida a los números naturales.

Supongamos que:

$$\begin{aligned} &\bullet \quad n_0 \quad \text{tiene la propiedad} \quad \mathcal{P}. \\ &\bullet \quad \text{Si} \quad n \geq n_0 \quad \text{verifica la propiedad} \quad \mathcal{P}, \text{ entonces,} \\ &\qquad n + 1, \quad \text{a su vez, cumple con dicha propiedad.} \end{aligned} \tag{1.5}$$

Consideremos

$$Y = \{n \in \mathbb{N}, n \geq n_0 : n \text{ no cumple} \quad \mathcal{P}\}$$

Supongamos que $Y \neq \emptyset$.

Aplicando el **P.B.O**, deducimos que Y posee un elemento mínimo (llamémoslo m_0). ¿Que podemos decir acerca de m_0?

$$m_0 \in Y \tag{1.6}$$

(O sea: $m_0 \geq n_0$ y m_0 **no** cumple $\mathcal{P}$)

Así que, más precisamente, $m_0 > n_0$. Luego, $m_o - 1$ es un número natural, tal que $m_o - 1 \geq n_o$ y, además, $m_0 - 1 \notin Y$ (ya que m_0 es el elemeneto mínimo de Y) Pero entonces, $m_0 - 1$ **cumple** $\mathcal{P}$. Y, ahora, utilizando (1.5), llegamos a que: m_0 cumple $\mathcal{P}$ (en contradicción con (1.6))

Por lo tanto, $Y = \emptyset$. O sea, para todo $n \geq n_0$ se cumple $\mathcal{P}$ ∎

En seguida, a partir del **P.B.O**, obtendremos el: **Segundo Principio de Inducción Completa:**

Supongamos que para cada número natural $n \geq n_0$, hay asociada una afirmación A_n

> **Si** A_{n_0} es verdadera, y podemos probar que la veracidad de A_k (para $n_0 \leq k < n$) implica la veracidad de A_n, (1.7)

entonces, A_n es verdadera, para cualquier $n \geq n_0$.

Demostración: Sea $S = \{n \in \mathbb{N}$: $n \geq n_0$ y A_n es falsa $\}$

Debemos demostrar que $S = \emptyset$.

Supongamos que $S \neq \emptyset$.

Entonces, de acuerdo al P.B.O, S tiene un elemento mínimo (designémoslo por m_0). Tenemos que:

$$m_0 \geq n_0 \quad \text{y} \quad A_{m_0} \quad \text{es falsa.} \tag{1.8}$$

Como A_{n_0} es verdadera, concluímos que $m_0 > n_0$. También, para todo k, con $n_0 < k < m_0$, es A_k verdadera (por la minimalidad de m_0).

Luego, según (1.7), A_{m_0} es verdadera, en contradición con (1.8). De modo que $S = \emptyset$, y A_n es verdadera, para todo $n \geq n_0$. ∎

A continuación probaremos que el segundo Principio de Inducción tiene como consecuencia el P.B.O.

Efectivamente, sea $A \subset \mathbb{N}$, **no vacío**. Demostraremos que A posee un elemento mínimo.

Si $0 \in A$, no necesitamos hacer más nada.

Supongamos entonces, que $0 \notin A$. Sea X, el conjunto de los números naturales n, tales que $\{0, 1, 2, \ldots, n\} \subseteq \mathbb{N} - A$. (Notemos que $0 \in X$).

Como $X \subseteq N - A$ y $A \neq \emptyset$, deducimos que $X \neq \mathbb{N}$.

Entonces, en virtud del Segundo Principio de Inducción Completa, debe existir un $m_0 \in \mathbb{N}$, tal que, X contiene todos los números naturales **menores** que m_0, pero $m_0 \notin X$ (luego, $m_0 > 0$).

Es decir, $m_0 \in A$ y $0, 1, 2, \ldots, m_0 - 1$ no están en A. Esto significa que m_0 es el elemento mínimo de A. ∎

En resumen, ha quedado probado que: el Primer Principio de Inducción Completa, el P.B.O, y el Segundo Principio de Inducción Completa son **equivalentes** entre sí. ∎

El próximo Principio es de enunciado muy sencillo, pero de gran importancia, conocido como el **Principio del nido de las palomas:**

Si $n+1$ **palomas** son colocadas en n **nidos**, entonces, por lo menos, un nido deberá tener 2 ó más palomas. En efecto, si el número **máximo** de palomas, en cada nido, fuese 1, estarían distribuídas, a lo sumo, n palomas (contradicción).

Este principio también es llamado: **Principio de las gavetas de Dirichlet**, por el hecho de ser usualmente, enunciado así: Si colocamos n objetos en un número r de gavetas (con $r < n$), entonces por lo menos, una gaveta deberá contener, al menos, dos objetos.

Una forma más general de enunciar el citado Principio es:

"Si **n** nidos son asignados a **n.k+1 palomas** entonces, por lo menos, un nido albergará, al menos, a **k+1** palomas"

Efectivamente, si cada nido abrigara, a lo máximo , a **k palomas**, se tendría, a lo sumo, un total de **n.k palomas**, lo cual es contradictorio.

Ejemplos:

1.1) Una gran ciudad tiene 5.000.011 habitantes. El número máximo de cabellos que puede crecer en una cabeza humana es de 500.000. Demostrar que hay, al menos, 11 habitantes, de la citada ciudad, con el mismo número de cabellos.

Solución: En este caso, $k+1 = 11 \therefore$ **k=10**; $n = 500 \cdot 001$ (un "nido"para las personas de **0** cabellos, un "nido"para las personas de **un** cabello, ..., un "nido"para las personas de **500.000** cabellos)

Luego, $n.k + 1 = 500011$.

De manera que, una aplicación directa de la última versión dada del Principio que nos ocupa, prueba lo afirmado.

1.2) Demostrar que si se marcan 5 puntos, **al azar**, en la superficie de un cuadrado, de lado 2cm, por lo menos, uno de los segmentos marcados, tiene longitud menor o igual a $\sqrt{2}$cm.

Solución: Dividamos el cuadrado dado, en cuatro cuadrados, de lado 1cm. (éstos serán los "nidos": n=4). Como hay 5 puntos (5 "palomas"), entonces, en **alguno de los 4 cuadrados** caerán, al menos, **dos** de dichos puntos. Cualquiera que sea la ubicación de dichos puntos en el cuadrado (de lado 1cm), la longitud del segmento formado será menor o igual que la longitud de la diagonal del cuadrado, la cual es $\sqrt{2}$cm.

1.3) Diremos que un punto (x, y), de $\mathbb{R}^2$, es "entero" si sus coordenadas son enteras. Por ejemplo, $(1, 7), (-2, 5), (0, 32)$, son todos "enteros". Mientras que, $(\frac{5}{3}, 7), (8, \frac{-2}{5})$, no lo son. Consideremos, **al azar,** 5 **puntos** "enteros", de $\mathbb{R}^2$. Demostrar que **el punto medio** de alguno de los segmentos que unen parejas de **esos puntos, es** "**entero**".

Solución: consideremos los **cuatro** "nidos"siguientes:

n_1= $\{(x, y) \in \mathbb{R}^2 : (x, y)$ es "entero", x **par**, y **par**$\}$

n_2= $\{(x, y) \in \mathbb{R}^2 : (x, y)$ es "entero", x **impar**, y **par**$\}$

n_3= $\{(x, y) \in \mathbb{R}^2 : (x, y)$ es "entero", x **par**, y **impar**$\}$

n_4= $\{(x, y) \in \mathbb{R}^2 : (x, y)$ es "entero" , x **impar**, y **impar**$\}$

Entonces, por el principio del nido de las palomas, al menos **dos** de los puntos "enteros" dados, caen en el mismo "nido", digamos, (x_1, y_1), (x_2, y_2).

Como par + par da par e impar + impar da par, resulta que:

$$\frac{x_1 + x_2}{2} \quad \text{e} \quad \frac{y_1 + y_2}{2}$$

son enteros; o sea , el punto medio del segmento determinado por (x_1, y_1), (x_2, y_2) es "entero".

Es inmediato ver que, con sólo 4 puntos no es cierta la conclusión; consideremos, por ejemplo, los puntos: $(2, 2), (1, 1), (2, 3)$ y $(1, 4)$ ∎

El concepto siguiente es uno de los más importantes en toda la Matemática. Se trata de **Los números primos**.

Ellos son los "ladrillos" de construcción, a partir de los cuales, los otros enteros son formados, multiplicativamente.

Recordemos que un **número natural**, mayor que 1, y que sólo es divisible por 1 y **por él mismo**, es llamado **número primo**.

Los números primos son: $2, 3, 5, 7, 11, 13, 17, \ldots$ Un número mayor que 1, y que no es primo, sera llamado compuesto.

Cada uno de estos números se puede descomponer, progresivamente, en factores hasta llegar finalmente a tener sólo factores primos. Por ejemplo, se puede descomponer 120 en $12 \cdot 10$; 12 como $2 \cdot 2 \cdot 3$, y 10 como $2 \cdot 5$, para finalmente obtener:

$120 = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 5 = \mathbf{2^3 \cdot 3 \cdot 5}$.

También pudimos haber procedido así:

$120 = 8 \cdot 15$; $\quad 8 = 2 \cdot 2 \cdot 2$; $\quad 15 = 3 \cdot 5$, de donde, $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = \mathbf{2^3 \cdot 3 \cdot 5}$. El obtener el mismo resultado en ambos casos , parece obvio porque estamos acostumbrados a ello.

Damos por sentado que, si descomponemos en factores un número entero, hasta donde sea posible, **obtendremos siempre los mismos factores; no importa cómo realicemos la descomposición.**

Consideremos ahora, un número mayor, por ejemplo, el 18.833. Después de mucho tabajo llegaríamos a que es igual a $37 \cdot 509$, y que estos factores son primos. Pero, ¿cómo saber si hay, o no, otra factorización del número 18.833, completamente distinta a la mostrada?

La respuesta a esta inquietud nos la dará el **Teorema Fundamental de la Aritmética**, que analizaremos un poco más adelante. Por los momentos para liberarnos de ideas preconcebidas, consideraremos un sistema numérico que no es el usual.

Nuestro "nuevo" sistema numérico, denotado por $\mathbb{Z}[\sqrt{-5}]$, va a estar constituído por los elementos de la forma $a + b\sqrt{-5}$, con $a, b \in \mathbb{Z}$. (Tenemos así, un subconjunto de números complejos, con las operaciones de suma y multiplicación, usuales, de $\mathbb{C}$).

Nos será muy útil la noción de **norma** de un elemento de dicho sistema: $N(a + b\sqrt{-5}) = a^2 + 5b^2$ (esta expresión se obtiene multiplicando $a + b\sqrt{-5}$

por su **conjugado**, $a - b\sqrt{-5}$). Sucede que en $\mathbb{Z}[\sqrt{-5}]$, se cumple:

$$21 = 3 \cdot 7$$

y también,

$$21 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}). \tag{1.9}$$

De manera que si logramos probar que, en $\mathbb{Z}[\sqrt{-5}]$, los elementos: $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$, son **irreducibles** (lo que sustituye la noción de primos, de nuestro sistema ordinario), **entonces** (1.9) nos indicaría que hay **dos** diferentes factorizaciones del número 21, en $\mathbb{Z}[\sqrt{-5}]$.

Supongamos que $3 = \alpha.\beta$

Ahora bien, una computación directa muestra que se cumple:

$$N(\alpha.\beta) = N(\alpha).N(\beta), \quad \text{cualesquiera sean} \quad \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$$

Así que,

$$N(3) = N(\alpha.\beta) = N(\alpha).N(\beta)$$

O sea,

$$9 = N(\alpha).N(\beta)$$

Por lo tanto,

$$N(\alpha) = 1, \quad 3 \quad \text{ó} \quad 9.$$

Supongamos que

$$\alpha = a + b\sqrt{-5}$$

Entonces, si $N(\alpha) = 1$, se tendría:

$$a^2 + 5b^2 = 1.$$

Luego, $b = 0 \quad$ y $a = \pm 1 \quad \therefore \quad \alpha = \pm 1$

Por otro lado, el caso $N(\alpha) = 3$ queda descartado, ya que no puede tenerse

$$a^2 + 5b^2 = 3, \quad \text{con} \quad a \quad \text{y} \quad b \quad \text{enteros.}$$

Si $N(\alpha) = 9$, entonces, es $N(\beta) = 1$, y resulta $\beta = \pm 1$.

En todo caso, no se obtiene una factorización (no trivial) de 3, en $\mathbb{Z}[\sqrt{-5}]$, así como en el sistema númerico ordinario no se considera $3 = 1 \cdot 3$, como una factorización del 3. En otras palabras, 3 es **irreducible**, en $\mathbb{Z}[\sqrt{-5}]$.

Un argumento similar prueba que 7 es irreducible, en $\mathbb{Z}[\sqrt{-5}]$

Supongamos ahora que:

$$1 + 2\sqrt{-5} = \gamma.\delta$$

Entonces

$$21 = N(1 + 2\sqrt{-5}) = N(\gamma.\delta) = N(\gamma).N(\delta)$$

Luego,

$$N(\gamma) = 1, \quad 3, \quad 7 \quad \text{ó} \quad 21.$$

Sea

$$\gamma = m + n\sqrt{-5}.$$

Entonces

$$N(\gamma) = 1 \quad \text{implica que} \quad m = \pm 1 \quad \text{y} \quad n = 0 \quad \therefore \quad \gamma = \pm 1$$

Si fuera $N(\gamma) = 3$ resultaría $m^2 + 5n^2 = 3$, lo cual no se cumple, para valores enteros de m y n.

Análogamente, si $N(\gamma) = 7$, llegamos a una contradicción.

Finalmente, para $N(\gamma) = 21$, se obtiene $N(\delta) = 1$, lo cual implica que $\delta = \pm 1$.

De modo que, $1 + 2\sqrt{-5}$ es **irreducible**, en $\mathbb{Z}[\sqrt{-5}]$

Similarmente, $1 - 2\sqrt{-5}$ es **irreducible**, en $\mathbb{Z}[\sqrt{-5}]$.

Conclusión: 21 es factorizable, **de dos maneras diferentes**, como producto de irreducibles, en $\mathbb{Z}[\sqrt{-5}]$.

Un hecho como ese no podrá ocurrir en el sistema númerico ordinario, pues una particularidad del mismo es que la descomposición en factores primos es **única**. Además, los números primos son suficientes para generar todos los números naturales. Este es el contenido del **Teorema Fundamental de la Aritmética:**

Todo número natural, mayor que 1, o es primo, o se escribe de modo **único** (salvo el orden de los factores) como un producto de factores primos.

Para demostrarlo, necesitaremos dos lemas.

Denotaremos por $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ al conjunto de los números primos.

Lema 1.1: Sean: $p \in \mathbb{P}$, y $m, n \in \mathbb{N} - \{0\}$

Si p divide a $m.n$, entonces, p divide a m ó p divide a n.

(Este lema lo encontraremos, ya, en Los Elementos de Euclides, proposición 30, libro VII).

Demostración: Asumimos que p divide a $m.n$, pero que **no** divide a m. (También se dice en este caso que p y m son primos entre sí. Ver [2], páginas 60-61). Entonces, existen $r, s \in N$, tales que:

$$rp - sm = 1$$

Por lo tanto

$$rpn - smn = n \tag{1.10}$$

Ahora, p divide al primer miembro de (1.10). Por lo tanto, p divide a n. ∎

Lema 1.2: Sean: $p, q_1, q_2, \ldots, q_n \in \mathbb{P}$.

Supongamos que p divide a $q_1.q_2 \ldots q_n$.

Entonces, $p = q_j$, para algún $j \in \{1, 2, \ldots, n\}$.

Demostración: Usaremos el **Primer Principio de Inducción Completa.**

Si **n=1**, lo afirmado es cierto, pues tenemos que **p** es un divisor de q_1, **diferente de 1**, es decir, $p = q_1$.

> Asumamos ahora, que el resultado es válido para cualquier producto con k factores (hipótesis inductiva) (1.11)

Escribamos:

$$q_1.q_2 \ldots q_{k+1} = (q_1.q_2 \ldots q_k).q_{k+1}$$

Como p divide a este producto tenemos, según el lema 1.1, que p divide a $q_1.q_2 \ldots q_k$ ó p divide a q_{k+1}. O sea, p divide a $q_1.q_2 \ldots q_k$ ó $p = q_{k+1}$.

De modo que si usamos, ahora, (1.11) podemos afirmar:

$$p = q_j, \quad \text{para algún} \quad j \in \{1, 2, \ldots, n\}$$

∎

Ya estamos en condiciones de demostrar el Teorema Fundamental de la Aritmética.

Recordemos lo que dice: Sea $n \in \mathbb{N}$, con $n > 1$. Entonces, existen números primos (únicos) $p_1 \leq p_2 \leq \ldots \leq p_j$, tales que: $n = p_1.p_2 \ldots p_j$.

Demostración:

a) Existencia de la descomposición de n.

Si n fuese primo, basta escoger $p_1 = n$.

Supongamos entonces que $n \notin \mathbb{P}$. Como n es un número **compuesto**, existe $d \in \mathbb{N}$, tal que: $1 < d < n$ y d divide a n, digamos, $n = d.n_1$.

Luego, también tenemos que : $1 < n_1 < n$. Ahora, vamos a utilizar el Segundo Principio de Inducción Completa, cuya hipótesis inductiva consiste en admitir que: **todo número menor que n** puede ser escrito como un producto de primos. Por lo tanto, existen:

$$r_1, r_2, \ldots, r_m, q_1, q_2, \ldots, q_s \in \mathbb{P}, \quad \text{tales que,}$$

$$d = r_1.r_2 \ldots r_m; \qquad n_1 = q_1.q_2 \ldots q_s$$

Así,

$$n = r_1.r_2 \ldots r_m.q_1.q_2 \ldots q_s$$

Es decir, n **también** puede ser escrito como un producto de primos.

b) Unicidad de la descomposición $n = p_1.p_2.\ldots.p_j$

Supongamos que n posee dos descomposiciones en factores primos, digamos, $n = p_1.p_2 \ldots .p_k = q_1.q_2.\ldots.q_l$.

Sin pérdida de generalidad, asumamos que $l \geq k$. Como p_1 divide a $q_1.q_2.\ldots.q_l$, aplicamos el lema 1.2, y concluímos que existe $j \in \{1, 2, \ldots, l\}$, tal que $p_1 = q_j$.

Reordenando los índices de los $q_{j's}$ (si es necesario) podemos suponer que $p_1 = q_1$, para obtener:

$$p_1.p_2 \ldots p_k = p_1.q_2 \ldots q_l,$$

luego,

$$p_2 \ldots p_k = q_2 \ldots q_l$$

Continuando con este razonamiento, llegamos a que, para todo $i \in \{1, 2, \ldots, k\}$ existe $j \in \{1, 2, \ldots, l\}$, tal que $p_i = q_j$.

Así, reordenando los índices de los $q_{j's}$ (si es necesario), podemos asumir que:

$$p_i = q_i, \quad \text{para todo} \quad i \in \{1, 2, \ldots, k\}$$

Si $l = k$, la demostración habrá terminado.

Sea, entonces $l > k$.

En este caso, llegaremos a que:

$$p_1.p_2 \dots p_k = p_1.p_2 \dots p_k.q_{k+1} \dots q_l$$

lo cual implica que,

$$1 = q_{k+1} \dots q_l, \quad \text{absurdo}$$

Por lo tanto, concluímos que $l = k$, y que $p_i = q_i$, para todo $i \in \{1, 2, \dots, k\}$, quedando establecida la unicidad de la descomposición. ∎

Observación: En la descomposición de un número natural n, en la forma indicada por el Teorema Fundamental de la Aritmética, es posible que tengamos repetición de algunos primos. Es común reagrupar estos factores primos y escribir:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_t^{\alpha_t}.$$

Donde los $p_{i's}$ son distintos, y α_i es un natural que cuenta el número de veces que el primo p_i aparece en la factorización de n.

A estas alturas, surge una cuestión natural: ¿ Cuántos elementos tiene $\mathbb{P}$? Euclides, en los Elementos, libro IX, nos dice:

"**El conjunto de los números primos es infinito**"

Demostración: Supongamos que $\mathbb{P}$ es finito, digamos,

$$\mathbb{P} = \{P_1, P_2, \dots, P_k\}.$$

Consideremos el número

$$u = P_1.P_2 \dots P_k + 1.$$

Este u no puede ser primo, pues $u > P_i$ para todo $i \in \{1, 2, \dots, k\}$.

Entonces, en virtud del Teorema Fundamental de la Aritmética, existe $P_j \in \mathbb{P}$, tal que P_j divide a u.

Luego, podemos escribir, para algún $m \in N$,

$$u = P_1.P_2 \dots P_k + 1 = m.P_j,$$

lo cual implica que:

$$1 = m.P_j - P_1.P_2 \dots P_k = P_j.(m - P_1.P_2 \dots P_{j-1}.P_{j+1} \dots P_k).$$

O sea, P_j divide a 1 (absurdo).

Conclusión: $\mathbb{P}$ es infinito. ∎

A continuación veremos dos proposiciones en las cuales se utiliza el Teorema Fundamental de la Aritmética, ambas tienen que ver con números irracionales: una, con el número $\sqrt{\mathbf{2}}$; otra, con el número **e**, base de los logaritmos neperianos.

He aquí, la clásica prueba de que $\sqrt{2}$ es irracional:

Supongamos lo contrario, es decir, que existen m y n, naturales, tales que $\frac{m}{n} = \sqrt{2}$, en donde, se utiliza la (única) expresión de m y n, respectivamente, como producto de números primos, y además, suponemos que hemos cancelado ya, aquellos factores comunes a ambos. O sea, m y n **son primos entre sí**. Como $(\frac{m}{n})^2 = 2$ obtenemos: $m^2 = 2n^2$, o sea, m^2 es par, lo cual implica que **m es par**.

Así podemos escribir: $m = 2k$, para algún natural k.

$$\therefore \quad m^2 = (2k)^2 = 2n^2 \quad \therefore \quad 4k^2 = 2n^2 \quad \therefore \quad n^2 = 2k^2.$$

Luego, también **n es par**.

Pero entonces hemos llegado a una contradicción: 2 es factor común de m y n, sabiendo, de antemano, que ellos eran primos entre sí.

Luego, no pueden existir tales m y n.

Conclusión: $\sqrt{2}$ es irracional. ∎

Ahora bien, $\sqrt{2}$ es solución de la ecuación

$$x^2 - 2 = 0$$

Lo cual se expresa diciendo que $\sqrt{2}$ es un **irracional algebraico**, para diferenciarlo de los **irracionales trascendentes** (como **e**, π), que no pueden ser soluciones (raíces) de ecuaciones polinómicas con coeficientes enteros. (Para analizar la irracionalidad de **e** y π, ver [3], volumen 2).

Charles Hermite (1822-1901), matemático francés, en 1873 demostró la trascendencia del número e. Sin embargo, no tuvo éxito en demostrar que π es trascendente, hecho logrado por el matemático alemán Ferdinand Lindemann (1852-1939), en 1882, con lo que quedó resuelto, definitivamente, el problema de la cuadratura del círculo, de un modo negativo, es decir, tal problema no se puede resolver con regla y compás.

Resumiendo entonces, ni e ni π pueden ser raices de una ecuación algebraica, con coeficientes enteros:

$$a_o + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0,$$

No importa lo grande que sean los enteros $a_0, a_1, a_2, \ldots, a_n$, y el grado n.

Lo esencial es que los coeficientes sean enteros. Aunque seria suficiente, sin embargo, decir **racionales**, puesto que siempre podemos convertirlos en enteros, multiplicando por el mínimo común múltiplo de los denominadores.

En el curso de la demostración de la trascendencia del número e, usaremos propiedades sencillas de los números enteros, como la divisibilidad, y el hecho de que existen infinitos números primos. El plan de la demostración es el siguiente:

Supondremos que:

$$a_0 + a_1 e + a_2 e^2 + \ldots + a_n e^n = 0, \tag{1.12}$$

donde, $a_0 \neq 0$, con $a_0, a_1, a_2, \ldots, a_n$ enteros.

Escribimos

$$e = \frac{M_1 + \epsilon_1}{M}, \quad e^2 = \frac{M_2 + \epsilon_2}{M}, \quad \ldots, \quad e^n = \frac{M_n + \epsilon_n}{M}, \tag{1.13}$$

donde, $M, M_1, M_2, ..., M_n$, son enteros, y $\frac{\epsilon_1}{M}$, $\frac{\epsilon_2}{M}, \ldots, \frac{\epsilon_n}{M}$ son fracciones positivas muy pequeñas. Entonces usando (1.13) y multiplicando por M, llegamos a que (1.12) toma la forma:

$$(a_0 M + a_1 M_1 + \ldots + a_n M_n) + (a_1 \epsilon_1 + a_2 \epsilon_2 + \ldots + a_n \epsilon_n) = 0 \tag{1.14}$$

El primer paréntesis, en (1.14), encierra un número entero (que veremos, es **diferente de cero**). En cuanto a la suma encerrada en el segundo paréntesis, probaremos que es una **fracción propia** (denominador mayor que el númerador) **positiva**. Tendremos así, una **contradicción:**

Un número entero, diferente de cero, $a_0 M + a_1 M_1 + \ldots + a_n M_n$, **aumentado** en una fracción propia, $a_1 \epsilon_1 + a_2 \epsilon_2 + \ldots + a_n \epsilon_n$, da como resultado el número cero. Así, la igualdad (1.12) no puede ser posible.

En el camino, usaremos el hecho siguiente: si un número **entero** k no es divisible por un **cierto número** (**distinto de cero**), entonces k no puede ser cero (puesto que cero es divisible por cualquier número, no nulo).

Probaremos que $M_1, M_2, \ldots, M_n,$ son divisibles por un determinado número p, pero que p **no** divide a a_0M. Entonces, p no divide al número $a_0M + a_1M_1 + a_2M_2 + \ldots + a_nM_n$. En consecuencia, **esta última suma** es diferente de cero.

Una gran ayuda, en la ruta hacia nuestra meta, la proporcionará una integral creada por Hermite:

$$M = \int_0^{+\infty} \frac{z^{p-1}\ [(z-1)(z-2)\ldots(z-n)]^p}{(p-1)!}\ e^{-z}dz, \tag{1.15}$$

donde, n es el que aparece en (1.12), y p es un número primo, suficientemente grande.

Usaremos la siguiente notación:

$$M_\lambda = e^\lambda \int_\lambda^{+\infty} \frac{z^{p-1}\ [(z-1)(z-2)\ldots(z-n)]^p}{(p-1)!}\ e^{-z}dz \tag{1.16}$$

$$\epsilon_\lambda = e^\lambda \int_0^{\lambda} \frac{z^{p-1}\ [(z-1)(z-2)\ldots(z-n)]^p}{(p-1)!}\ e^{-z}dz \tag{1.17}$$

Ahora, la demostración en detalles:

Empecemos con la **función gamma:**

$$\Gamma(\mu) = \int_0^{+\infty} z^{\mu-1}\ e^{-z}dz,$$

de la cual sabemos que si μ es natural, entonces:

$$\Gamma(\mu) = (\mu-1)! \tag{1.18}$$

Con (1.18) podemos evaluar fácilmente la integral de Hermite. Veamos:

$$[(z-1)(z-2)\ldots(z-n)]^p = [z^n + \ldots + (-1)^n n!]^p = z^{np} + \ldots + (-1)^n (n!)^p,$$

donde, sólo hemos escrito los términos de mayor y menor grado, respectivamente; el valor de la integral de Hermite será:

$$M = \frac{(-1)^n\ (n!)^p}{(p-1)!} \int_0^{\infty} z^{p-1}\ e^{-z}dz + \sum_{j=p+1}^{np+p} \frac{C_j}{(p-1)!} \int_0^{+\infty} z^{j-1}\ e^{-z}dz,$$

donde, las $C_{j's}$ son constantes enteras que se deducen del desarrollo del polinomio $[(z-1)(z-2)\ldots(z-n)]^p$. Aplicando ahora, a cada una de las integrales, la fórmula (1.18), obtenemos:

$$M = \frac{(-1)^n\ (n!)^p\ (p-1)!}{(p-1)!}\ +\ \sum_{j=p+1}^{np+p} \frac{C_j\ (j-1)!}{(p-1)!}.$$

Como, en la sumatoria, el índice j es, siempre, mayor que p, resulta que:

$$\frac{(j-1)!}{(p-1)!} \quad \textbf{es un entero múltiplo de} \quad p$$

Así, sacando p como factor común de toda la suma, llegamos a:

$$M = (-1)^n\ (n!)^p\ + p\ [C_{p+1} + C_{p+2}(p+1) + C_{p+3}(p+1)(p+2) + ...]$$

De modo que, si tomamos p, **primo, suficientemente grande**, obtendremos que p no divide a $(-1)^n(n!)^p$ y, en consecuencia, p **no divide a** M.

Como además, $a_0 \neq 0$, vemos que si escogemos p mayor que $|a_0|$, entonces a_0 **no es divisible por** p**.**

En fin, el producto a_0M no será divisible por p, primo, suficientemente grande.

Estudiemos ahora, los números M_λ, con $\lambda \in \{1, 2, \ldots, n\}$. (No olvidemos que queremos ver lo que sucede con $a_0M + a_1M_1 + \ldots + a_nM_n$).

Nos remitimos a (1.16), e introducimos el factor e^λ, bajo el signo integral. Tomemos, a su vez, $\beta = z - \lambda$, como nueva variable de integración. Resulta:

$$M_\lambda = \int_0^{+\infty} \frac{(\beta+\lambda)^{p-1}\ [(\beta+\lambda-1)(\beta+\lambda-2)\ldots\beta\ldots(\beta+\lambda-n)]^p}{(p-1)!}\ e^{-\beta}d\beta$$

Esta expresión tiene una forma análoga a la (1.15).

Si multiplicamos los factores del integrando tendremos una suma de potencias, con coeficientes enteros, de los cuales, el de menor grado será β^p.

La integral del númerador será, por lo tanto, una combinación lineal de las integrales:

$$\int_0^{+\infty} \beta^p\ e^{-\beta}d\beta, \quad \int_0^{+\infty} \beta^{p+1}\ e^{-\beta}d\beta, \quad \ldots, \quad \int_0^{+\infty} \beta^{(n+1)p-1}\ e^{-\beta}d\beta,$$

Las cuales, según (1.18), son iguales, respectivamente, a :

$$p!,\ (p+1)!,\ (p+2)!,\ \ldots,\ [(n+1)p-1]!;$$

de manera que:

$$M_\lambda = \frac{p!\ A_\lambda}{(p-1)!} = p\ A_\lambda,$$

donde, A_λ es un entero, y $\lambda = 1, 2, \ldots, n$.

En otras palabras, cada M_λ es un entero, **múltiplo de** p**.**

De modo que, en $a_0M + a_1M_1 + \ldots + a_nM_n$, todos los sumandos, excepto a_0M, son divisibles por p ; luego, $a_0M + a_1M_1 + \ldots + a_nM_n$ no es divisible por p, y consecuentemente, es distinto de cero.

¿Y qué ocurre con $a_1\epsilon_1 + a_2\epsilon_2 + \ldots + a_n\epsilon_n$?

Según (1.17),

$$\epsilon_\lambda = \int_0^\lambda \frac{z^{p-1}\ [(z-1)(z-2)\ldots(z-n)]^p}{(p-1)!}\ e^{-z+\lambda}dz.$$

Probaremos que estos ϵ_{λ}'$_s$ pueden hacerse tan pequeños como se quiera, si elegimos a p adecuadamente. Hasta ahora, las condiciones exigidas a p son: que sea primo, mayor que n, mayor que $|a_0|$; requisitos que son llenados por infinidad de números primos, suficientemente grandes.

Sean: G y g_λ, los **máximos**, respectivos, de los valores absolutos de

$$z(z-1)(z-2)\ldots(z-n) \quad \text{y} \quad (z-1)(z-2)\ldots(z-n).e^{-z+\lambda}, \quad \text{en} \quad [0,n].$$

Luego,

$$|z(z-1)(z-2)\ldots(z-n)| \le G \quad \text{y} \quad |(z-1)(z-2)\ldots(z-n)\cdot e^{-z+\lambda}| \le g_\lambda,$$

para $0 \le z \le n$.

Entonces,

$$|\epsilon_\lambda| \le \int_0^\lambda \frac{G^{p-1}\ g_\lambda}{(p-1)!}dz \le \frac{G^{p-1}\ g_\lambda\ \lambda}{(p-1)!} \tag{1.19}$$

Ahora bien, como G, g_λ y λ no dependen de p, y, además, $(p-1)!$ crece mas rápidamente que G^{p-1} (piénsese en la convergencia de la serie $\sum_1^{+\infty} \frac{a^k}{k!}$), la fracción,

$$\frac{G^{p-1}}{(p-1)!},$$

llega a ser, para valores de p suficientemente grandes, más pequeña que cualquier $\epsilon > 0$ dado.

Así, tomando en cuenta (1.19), podemos lograr que cada uno de los ϵ_λ llegue a ser tan pequeño como deseemos, eligiendo p suficientemente grande.

Luego, podemos conseguir que $a_1\epsilon_1 + a_2\epsilon_2 + \ldots + a_n\epsilon_n$ sea arbitrariamente pequeña.

Efectivamente,

$$|a_1\epsilon_1 + a_2\epsilon_2 + \ldots + a_n\epsilon_n| \leq |a_1||\epsilon_1| + |a_2||\epsilon_2| + \ldots + |a_n||\epsilon_n| \leq$$

$$(|a_1| \cdot 1 \cdot |g_1| + |a_2| \cdot 2 \cdot |g_2| + \ldots + |a_n| \cdot n \cdot |g_n|)\frac{G^{p-1}}{(p-1)!}$$

Ya que la suma entre paréntesis no depende de p, resulta que,

$$a_1\epsilon_1 \ + \ a_2\epsilon_2 \ + \ \ldots a_n\epsilon_n,$$

puede ser tan pequeña como queramos y, en particular, en valor absoluto, **menor que 1**.

Así que, (1.14) nos proporciona una contradicción:

Un número **entero**, **distinto de cero**, incrementado en el valor de una **fracción propia**, da como resultado el número cero.

Conclusión: e **es trascendente**.

Capítulo 2

El Teorema Fundamental del Álgebra.

En su tesis de doctorado en la Universidad de Helmstädt, escrita a los 20 años de edad (en 1797), **Gauss** dió la primera demostración plenamente satisfactoria del Teorema Fundamental del Álgebra. Newton, Euler, D'Alembert y Lagrange habían hecho tentativas, frustradas, de probar ese teorema. Casi 20 años después, en 1816, Gauss publicó dos nuevas demostraciones, y más tarde, en 1850, una cuarta demostración.

Teorema Fundamental del Álgebra:

Todo polinomio

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

donde, cada a_i es un número complejo, $a_n \neq 0$ y $n \geq 1$, **tiene una raíz**, o sea, existe un número complejo z_0, tal que: $f(z_0) = 0$.

Demostración: Sin pérdida de generalidad, suponemos $n \geq 2$. Tenemos:

$$\begin{aligned}
|f(z)| &= |a_n\ z^n + a_{n-1}\ z^{n-1} + \ldots + a_1\ z + a_0| \\
&\geq |a_n\ z^n| - |a_{n-1}\ z^{n-1} + \ldots + a_1\ z + a_0| \\
&\geq |a_n|\ |z|^n - |z|^{n-1} \left[|a_{n-1}| + \frac{|a_{n-2}|}{|z|} + \ldots + \frac{|a_1|}{|z|^{n-2}} + \frac{|a_0|}{|z|^{n-1}} \right] \\
&\geq |a_n|\ |z|^n - |z|^{n-1} \left[|a_{n-1}| + |a_{n-2}| + \ldots + |a_1| + |a_0| \right], \\
&= |z|^{n-1} \big[||a_n|\ |z| - R \big], \quad \text{para} \quad |z| \geq 1,
\end{aligned}$$

donde, $|z| \geq 1$ y $R = |a_{n-1}| + |a_{n-2}| + \ldots + |a_1| + |a_0|$.

Así que,

$$|f(z)| \geq |z|^{n-1}, \quad \text{para} \quad |z| \geq \text{máx}\left\{1, \frac{R+1}{|a_n|}\right\}. \tag{2.1}$$

Sea $P_0 = |f(0)| = |a_0|$.

Entonces, de (2.1) se sigue que: existe $T > 0$, tal que,

$$|f(z)| > P_0, \quad \text{para} \quad |z| > T. \tag{2.2}$$

(Recordar que $n - 1 \geq 1$ y que $|z|^{n-1} \to +\infty$, si $|z| \to +\infty$).

Consideremos $D = \{z \in \mathbb{C} : |z| \leq T\}$.

Resulta que D es un subconjunto cerrado y acotado de $\mathbb{C} = \mathbb{R}^2$; luego, D es **compacto** (Teorema generalizado de Heine-Borel. Ver [4]).

Como la función $|f| : D \to \mathbb{R}$ es continua, entonces, $|f|$ alcanza un **valor mínimo**, en algún punto $z_0 \in D$.

De modo que,

$$|f(z_0)| \leq |f(z)|, \quad \text{para todo} \quad z \in D.$$

Pero, por (2.2), para todo $z \notin D$, se tiene:

$$|f(z)| > P_0 = |f(z_0).$$

En consecuencia,

$$|f(z_0| \leq |f(z)|, \quad \text{para todo} \quad z \in \mathbb{C}. \tag{2.3}$$

A todas estas el lector ya sospechará que el z_0 **es la raíz buscada**. Y es aquí, donde viene una jugada magistral:

Hacemos una traslación, al definir:

$$P(z) = f(z + z_0).$$

De manera que según (2.3), queda:

$$|P(0)| \leq |f(z)|, \quad \text{para todo} \quad z \in \mathbb{C}. \tag{2.4}$$

Y el problema de probar que $f(z_0) = 0$, se convierte en demostrar que, $P(0) = 0$.

Pero,

$$P(z) = b_n z^n + b_{n-1} z^{n-1} + \ldots + b_1 z + b_0, \quad \text{donde,} \quad b_i \in \mathbb{C}$$

Luego, $P(0) = b_0$.

Por lo tanto, nuestro objetivo es probar que $b_0 = 0$. Supongamos que $b_0 \neq 0$, entonces

$$P(z) = b_0 + b_k z^k + z^{k+1} Q(z), \tag{2.5}$$

donde, b_k es el más pequeño $b_i \neq 0, \quad i > 0$ y $Q(z)$ es un polinomio.

Por ejemplo, si

$$P(z) = 5z^9 + 7z^5 + 4z^4 - 11z^3 + 2,$$

tenemos que: $b_k = -11$ y $P(z) = 2 - 11z^3 + z^4(4 + 7z + 5z^5)$, de modo que, $Q(z) = 4 + 7z + 5z^5$.

Prosiguiendo con la demostración, aparece otra jugada maestra, al considerar $w \in \mathbb{C}$, una raíz k-ésima del número:

$$-\frac{b_0}{b_k}, \quad \text{o sea,} \quad w^k = -\frac{b_0}{b_k}.$$

Por otro lado, para t real,

$$t|w^{k+1} Q(tw)| \longrightarrow 0, \quad \text{cuando} \quad t \to 0$$

Así que, existe $t_0 \in (0, 1)$, tal que:

$$t_0 |w^{k+1} Q(t_0 w)| < |b_0| \tag{2.6}$$

Ahora bien, de (2.5), se obtiene:

$$\begin{aligned} P(t_0 w) &= b_0 + b_k (t_0 w)^k + (t_0 w)^{k+1} Q(t_0 w) \\ &= b_0 + b_k t_0^k (-\frac{b_0}{b_k}) + t_0^{k+1} w^{k+1} Q(t_0 w) \\ &= b_0 (1 - t_0^k) + t_0^{k+1} w^{k+1} Q(t_0 w). \end{aligned}$$

Por lo tanto,

$$\begin{aligned} |P(t_0w)| &\leq |b_0|(1-t_0^k) + t_0^{k+1}|w^{k+1}Q(t_0w)| \\ &< |b_0|(1-t_0^k) + t_0^k|b_0| \quad \text{(usando (2.6))} \\ &= |b_0| = |P(0)| \end{aligned}$$

$$\therefore \quad |f(t_0w + z_0) = |P(t_0w)| < |P(0)|. \tag{2.7}$$

Pero (2.7) está en contradicción con (2.4). En consecuencia, la suposición $b_0 \neq 0$ no puede ser verdadera, es decir,

$$f(z_0) = P(0) = b_0 = 0$$

■

Corolario 2.1: Un polinomio complejo (no constante) se factoriza completamente en factores lineales.

Demostración: Usaremos el Segundo Principio de Inducción Completa.

Sea $p(x) \in \mathbb{C}[x]$, con grado de $p(x)$, mayor o igual a 1.

El corolario es claramente cierto si el grado de $p(x)$ es 1, ya que entonces, $p(x)$ es de la forma:

$$p(x) = a_1x + a_0, \quad \text{con} \quad a_1 \neq 0.$$

Supongamos que el grado de $p(x)$ es n, y que el corolario es cierto para todos los polinomios de grado **mayor o igual a 1**, y **menor que** n. Según el Teorema Fundamental del Álgebra, existe $x_0 \in C$, tal que, $p(x_0) = 0$.

Entonces, $p(x) = (x - x_0).g(x)$, con $g(x)$, polinomio **de grado menor que** n. Por la hipótesis inductiva, $g(x)$ se factoriza en factores lineales, digamos,

$$g(x) = \alpha(x - x_1)(x - x_2)\dots(x - x_{n-1})$$

Luego,

$$p(x) = \alpha(x - x_0)(x - x_1)(x - x_2)\dots(x - x_{n-1})$$

■

Corolario 2.2: Sea $p(x) \in \mathbb{C}[x]$, con grado de $p(x)$ igual a n.

Si las raíces de $p(x)$ son $x_1, x_2, \dots, x_n$, (puede haber repeticiones), entonces,

$$p(x) = \alpha(x - x_1)(x - x_2)\dots(x - x_n), \quad \text{con} \quad \alpha \in \mathbb{C}$$

Corolario 2.3: Un polinomio **real** (no constante) se factoriza en polinomios de grado 1 y 2.

Equivalentemente, los únicos polinomios reales, irreducibles, son los polinomios lineales, y los polinomios cuadráticos sin raíces reales.

Demostración: Sea $p(x) \in \mathbb{R}[x]$. Entonces, también se tiene: $p(x) \in \mathbb{C}[x]$.

Sean: $z_1, z_2, \ldots, z_n$, las únicas raíces complejas de $p(x)$.

Así, $p(x) = \alpha(x - z_1)(x - z_2)\ldots(x - z_n)$, donde, $\alpha \in \mathbb{R}$, ya que es el coeficiente de x^n.

Si z_i es real, entonces, $x - z_i$ es un factor lineal (real) en la factorización de $p(x)$.

Si $z_k \notin \mathbb{R}$, entonces, $z_k = a_k + ib_k$, con $a_k, b_k \in \mathbb{R}$ y $b_k \neq 0$. Ahora, sucede que $\overline{z_k} = a_k - ib_k$ (el conjugado de z_k), también es raíz de $p(x)$, (para que se cumpla este hecho es importante que todos los coeficientes de $p(x)$ sean reales).

De modo que, el producto $(x - z_k)(x - \overline{z}_k)$ aparece en la factorización de $p(x)$.

Pero,

$$(x - z_k)(x - \overline{z}_k) = x^2 - 2a_k x + a_k^2 + b_k^2,$$

polinomio real, irreducible, de grado 2.

Corolario 2.4: Un polinomio real (no constante), irreducible, debe ser de grado 1 ó 2. ∎

Finalmente, veamos una aplicación del Teorema Fundamental del Álgebra, en los predios del Álgebra Lineal.

Probaremos que, dada una transformación lineal $A : E \to E$, donde, E es un espacio vectorial (real) de dimensión finita, o bien existe un vector (no nulo) $w \in E$, tal que,

$$Aw = \lambda w,$$

o entonces, existen $u, v \in E$, linealmentes independientes, tales que, Au y Av son ambos, combinaciones lineales de u y v, o sea,

$$Au = \alpha u + \beta v$$
$$Av = \gamma u + \delta v$$

En otras palabras, existe, en E, un subespacio vectorial, de dimensión 1 ó 2, invariante por A, de acuerdo con la siguiente definición:

Definición: se dice que un subespacio vectorial $F \subset E$ es invariante por el operador lineal $A : E \to E$, cuando $A(F) \subseteq F$ es decir, cuando la imágen Av, de cualquier vector $v \in F$, pertenece a F.

Si F es un subespacio invariante por el operador $A : E \to E$, la restricción de A a los vectores de F, define un operador (que indicaremos con la misma notación, $A : F \to F$). Entonces, si $F \subsetneq E$, obtenemos un operador más simple, por estar definido en un dominio menor.

Ejemplos:

a) Los subespacios $\{\mathbf{0}\}$ y E son invariantes por cualquier operador lineal $A : E \to E$
Nota: $\mathbf{0}$ simboliza al vector nulo de E.

b) El núcleo $N(A) = \{v \in E : Av = \mathbf{0}\}$, y la imágen $Im(A) = \{Av : v \in E\}$, son también subespacios invariantes por el operador $A : E \to E$. ∎

Un **subespacio** $F \subset E$, espacio vectorial real, **de dimensión 1** (recta que pasa por el origen) es invariante por $A : E \to E$, si, y sólo si, existe un número real λ_0, tal que, $Av = \lambda_0 v$, para todo $v \in F$.

En efecto, tomando $u \neq \mathbf{0}$ en F, resulta que $\{u\}$ es una **base** de F.

Como $Au \in F$, se tiene: $Au = \lambda_0 u$, para algún $\lambda_0 \in \mathbb{R}$.

Sea $v \in F$; entonces, $v = \alpha u$, para algún $\alpha \in \mathbb{R}$.

Luego,

$$A(v) = A(\alpha u) = \alpha Au = \alpha\lambda_0 u = \lambda_0(\alpha u) = \lambda_0 v$$

∎

Si $u, v \in E$ son **linealmente independientes**, el subespacio F, generado por u y v (plano que pasa por el origen) es invariante por A si, y sólo si, $Au \in F$ y $Av \in F$,es decir, si:

$$\begin{aligned} Au &= \alpha u + \beta v \qquad \text{y} \\ Av &= \gamma u + \delta v \end{aligned}$$

∎

Un vector (no nulo) $v \in E$, se llama **auto-vector** (o vector propio) del operador lineal $A : E \to E$, cuando existe $\lambda \in \mathbb{R}$ tal que

$$Av = \lambda v.$$

El número $\lambda \in \mathbb{R}$, a su vez, se llama un **auto-valor** (o valor propio) del operador lineal $A : E \to E$, cuando existe un vector (no nulo) $v \in E$, tal que,

$$Av = \lambda v.$$

Se dice, entonces, que el auto-valor λ corresponde al auto-vector v y, viceversa, que el auto-vector v también corresponde al auto-valor λ. En tal caso se cumple, para todo $w = \alpha v$, que:

$$Aw = \alpha w.$$

De manera que, hallar un auto-vector (o, lo que es equivalente, un auto-valor) del operador lineal $A : E \to E$, es lo mismo que encontrar un subespacio de dimensión 1, invariante por A.

Ejemplos:

a) Una rotación $\theta : \mathbb{R}^2 \to \mathbb{R}^2$, entorno del origen, de ángulo diferente de 0^o y 180^o, sólo admite como subespacios invariantes: $\{\mathbf{0}\}$ y $\mathbb{R}^2$.

b) Para todo $\alpha \in \mathbb{R}$, la rotación $A : \mathbb{R}^3 \to \mathbb{R}^3$, de ángulo α, en torno del eje z,

$$A(x, y, z) = (x\cos\alpha - y\sin\alpha \ , \ x\sin\alpha + y\cos\alpha \ , \ z),$$

tiene al eje z y el plano $z = 0$, como subespacios invariantes.

c) Si un operador lineal $A : E \to E$ tiene **núcleo** no trivial, entonces, todo vector, no-nulo, $v \in N(A)$, (núcleo de A), es un autovector de A, pues:

$$Av = 0v$$

■

Dados: el polinomio $p(x) = a_0 + a_1x + ... + a_nx^n$ y el operador lineal $A : E \to E$, la notación $p(A)$ indica el operador lineal:

$$p(A) = a_0I + a_1A + a_2A^2 + ... + a_nA^n.$$

Lema 2.1: Para toda transformación lineal $A : E \to E$, donde, E es de dimensión finita, existen: Un polinomio **mónico** (o sea, el coeficiente de la

mayor potencia de x es el 1) **irreducible** $p(x)$ de grado 1 ó 2, y un vector, no-nulo, $v \in E$, tales que,

$$p(A)v = \mathbf{0}.$$

Demostración: Sea $n = dimE$.

Denotaremos con $\mathcal{L}(E, E)$, el espacio vectorial de todas las transformaciones lineales de E en E. Como la dimensión de $\mathcal{L}(E, E)$ es n^2, los $n^2 + 1$ operadores: $I, A, A^2, ..., A^{n^2}$, son **linealmente dependientes.**

Luego, existen números reales $\alpha_0, \alpha_1, ..., \alpha_n$,**no todos nulos**, tales que:

$$\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + ... + \alpha_n A^n = \mathbf{0} \tag{2.8}$$

Sea α_m, el coeficiente, **no nulo**, de mayor índice en (2.8).

Dividiendo, ambos miembros de (2.8), por α_m, resulta:

$$\beta_0 I + \beta_1 A + ... + \beta_{m-1} A^{m-1} + A^m = \mathbf{0} \tag{2.9}$$

Entonces, según (2.9), se cumple:

$$q(A) = \mathbf{0}, \tag{2.10}$$

para, $q(x) = \beta_0 + \beta_1 x + \ldots + \beta_{m-1} x^{m-1} + x^m$.

Sabemos, por una consecuencia del Teorema Fundamental del Álgebra (corolario 2.3) que:

$$q(x) = p_1(x).p_2(x).....p_k(x),$$

donde cada $p_i(x)$ es un polinomio mónico, irreducible, de grado 1 ó 2.

Así que: $p_1(A).p_2(A).....p_k(A) = \mathbf{0}$, según (2.10). Entonces, por lo menos, uno de los operadores $p_i(A)$ **no** es invertible, es decir, existe un vector, **no-nulo**, $v \in E$, tal que,

$$p_i(A)v = \mathbf{0}.$$

■

Ahora sí estamos en condiciones de presentar la aplicación anunciada inmediatamente después del corolario 2.4.

Teorema 2.1: Toda transformación, lineal en un espacio vectorial real de dimensión finita, posee un subespacio invariante de dimensión 1 ó 2.

Demostración: Dada $A : E \to E$, lineal, sean: p, el polinomio y $v \in E$, el vector no-nulo, dados por el lema 2.1, con $p(A)v = 0$.

Si $p(x) = x - \lambda$, entonces,

$$\mathbf{0} = p(A)v = (A - \lambda I)v = Av - \lambda v$$

Luego, $Av = \lambda v$.

Así, la recta que pasa por el origen, y contiene a v, es un subespacio (de dimensión 1) invariante por A.

Si $p(x) = x^2 + ax + b$, (polinomio mónico irreducible), entonces:

$$\mathbf{0} = p(A)v = (A^2 + aA + bI)v = A^2v + aAv + bv \tag{2.11}$$

Luego, $A(Av) = -aAv - bv$.

Es decir, el subepacio generado por v y Av es invariante por A.

Además, v y Av son **linealmente independientes**, pues en caso contrario, tendríamos:

$$Av = \lambda v,$$

y de (2.11) se seguiría:

$$\mathbf{0} = A^2v + aAv + bv = \lambda^2 v + a\lambda v + bv = (\lambda^2 + a\lambda + b)v.$$

Lo cual implica que:

$$\lambda^2 + a\lambda + b = 0,$$

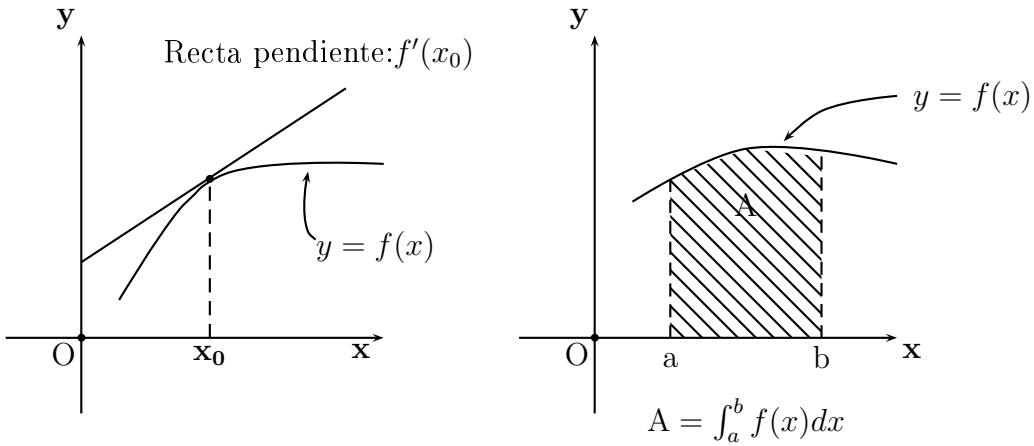
en contradicción con el hecho de que $p(x) = x^2 + ax + b$ no tiene raíz real.

De manera que, el subespacio invariante, generado por v y Av, tiene dimensión 2. ∎

Capítulo 3

El Teorema Fundamental del Cálculo

Recordemos que la noción de derivada nos resuelve el problema de hallar **la recta tangente** a una curva dada, **en uno de sus puntos**. Así mismo, la integración nos permite encontrar el área bajo una curva.



Lo notable y sorprendente, es que estos dos conceptos, aparentemente sin conexión alguna, están íntimamente relacionados: son inversos el uno del otro. Este es, en esencia, el contenido del Teorema Fundamental del Cálculo.

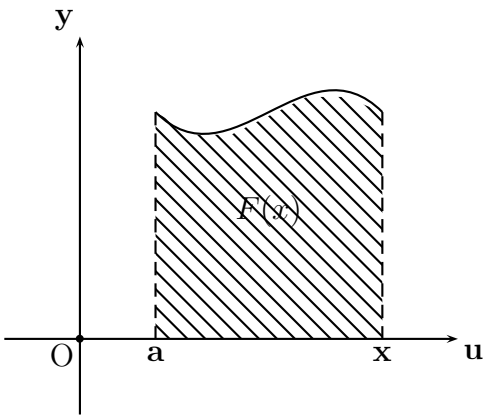
Se considera, en general, que Isaac Barrow (1630-1677), profesor de Isaac Newton, fue el primero en percibir plenamente, que la diferenciación y la integración son operaciones inversas entre sí. Pero los que reconocieron con claridad y explotaron por primera vez este Teorema Fundamental del Cálculo fueron Leibniz (1646-1716) y Newton (1642-1727).

Para formular el Teorema en cuestión, consideramos la integral de una función $y = f(x)$, desde un límite inferior fijo a, hasta el límite superior variable, x.

Escribimos:

$$F(x) = \int_a^x f(u)du$$

Esta función $F(x)$ es el área bajo la curva $y = f(u)$ desde $u = a$ hasta $u = x$



El Teorema Fundamental del Cálculo establece que:

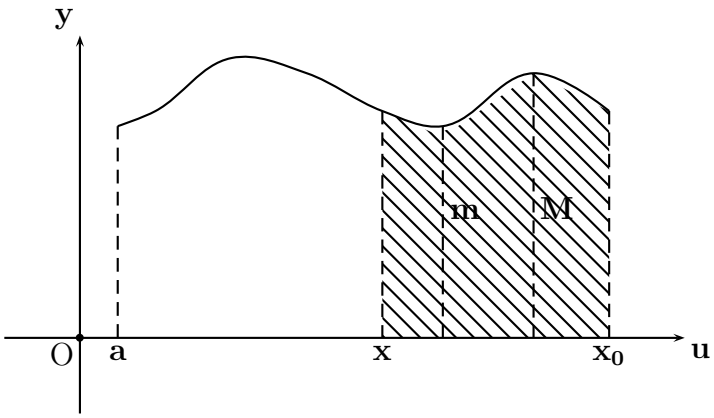
$$\text{Si} \quad F : [a, b] \to \mathbb{R}, \qquad \text{es integrable, y}$$

$$F : [a, b] \to \mathbb{R} \quad \text{es definida por:} \quad F(x) = \int_a^x f(u)du,$$

entonces, **en cada x** $\in (a, b)$ **donde f es continua**, existe la derivada $F'(x)$ y además, en cada uno de esos puntos x, es:

$$F'(x) = f(x).$$

Desde un punto de vista intuitivo la demostración es muy simple:



La diferencia $F(x) - F(x_0)$ indica el área desde x hasta x_0. Notemos que esta área está comprendida entre $(x_0 - x) \cdot m$ y $(x_0 - x) \cdot M$, siendo M y m, **respectivamente,** los valores **mayor** y **menor** de $f(u)$ en $[x, x_0]$.

O sea,

$$(x_0 - x)m \leq F(x_0) - F(x) \leq (x_0 - x)M.$$

Luego,

$$m \leq \frac{F(x_0) - F(x)}{x_0 - x} \leq M.$$

Como F es continua en x se tiene que cuando $x_0 \to x^+$, entonces, tanto m como M se aproximan a $f(x)$.

Así que:

$$F'(x) = \lim_{x_o \to x^+} \frac{F(x) - F(x_0)}{x_0 - x} = f(x)$$

■

Cuando $F'(x) = f(x)$, para todo $x \in [a, b]$, se dice que F es **una primitiva** de f (claro que en a y b se consideran derivadas laterales)

Decimos **una** función primitiva, y no **la** función primitiva, pues si, también $G'(x) = f(x)$, para todo $x \in [a, b]$ entonces, $H(x) = G(x) + c$, donde, c es cualquier constante, es una primitiva de f ya que:

$$H'(x) = G'(x) = f(x).$$

Recíprocamente, si G y H son dos primitivas de f, en [a,b] consideremos:

$$U = G - H, \qquad \text{definida en} \qquad [a, b].$$

Entonces,

$$U'(x) = G'(x) - H'(x) = f(x) - f(x) = 0.$$

Luego, como el dominio de U es un intervalo, debe ser U igual a una constante (digamos, c).

$$\therefore \qquad U(x) = G(x) - H(x) = c.$$

Esto nos proporciona una importante y útil regla para encontrar $\int_a^b f(x)dx$, para f continua en $[a, b]$, si conocemos una primitiva **G** de f

En efecto, como $F(x) = \int_a^x f(u)du$ es también una primitiva de f, por lo anterior resulta:

$$F(x) = G(x) + c, \quad \text{siendo} \quad c \quad \text{una constante.}$$

Pero, $F(a) = G(a) + c$

$$\therefore \quad 0 = G(a) + c \qquad \therefore \quad c = -G(a).$$

Así queda:

$$F(x) = G(x) - G(a),$$

y para $x = b$, obtenemos:

$$\int_a^b f(u)du = G(b) - G(a).$$

Ejemplos:

a) Como $(\ln x)' = \frac{1}{x}$, entonces

$$\int_1^2 \frac{1}{x}dx = \ln 2 - \ln 1 = \ln 2.$$

b) Como $(\operatorname{sen} x)' = \cos x$, entonces

$$\int_0^{\frac{\pi}{2}} \cos x dx = \operatorname{sen} \frac{\pi}{2} - \operatorname{sen} 0 = 1.$$

c) Como $(e^{x^2})' = e^{x^2} \cdot 2x$, entonces

$$\int_0^1 2xe^{x^2}dx = e^1 - e^0 = e - 1.$$

■

Ahora, veamos una propiedad que nos será muy útil en seguida:

Sea f continua en $[a,b]$ y $F(x)=\int_a^x f(u)du$, para $x\in[a,b]$, entonces, existe $\mathbf{c}\in(a,b)$ tal que:

$$\int_a^b f(u)du = f(\mathbf{c})\cdot(b-a). \tag{3.1}$$

Demostración: F es continua en $[a,b]$ y derivable en (a,b), con $F'(x)=f(x)$, para todo $x\in(a,b)$.

Luego, aplicando el **Teorema del valor intermedio de Lagrange**, a la función F, tenemos: existe $c\in(a,b)$, tal que;

$$F(b)-F(a)=F'(c)(b-a),$$

es decir,

$$\int_a^b f(u)du = f(c)(b-a).$$

■

¿Y cómo será la derivada de

$$F(x)=\int_a^{\alpha(x)} f(u)du,$$

donde, f es continua, y α es derivable?

Usando (3.1), podemos escribir:

$$\frac{F(x_0)-F(x)}{x_0-x}=\frac{\int_{\alpha(x)}^{\alpha(x_0)} f(u)du}{x_0-x}=\frac{f(c)[\alpha(\mathbf{x_0})-\alpha(\mathbf{x})]}{\mathbf{x_0}-\mathbf{x}},$$

donde, c está entre $\alpha(x)$ y $\alpha(x_0)$.

$$\therefore \quad \lim_{x_0\to x}\frac{F(x_0)-F(x)}{x_0-x}=f(\alpha(x))\cdot\alpha'(x),$$

o sea,

$$F'(x)=f(\alpha(x))\cdot\alpha'(x). \tag{3.2}$$

■

Un resultado más general es el siguiente:

Sea $\mathcal{R}=\{(x,y): a\le x\le b, \quad c\le y\le d\}$.

Supongamos que f y $\frac{\mathfrak{d}f}{\mathfrak{d}y}$ sean continuas en $\mathcal{R}$.

Consideremos, también, p y q , funciones derivables, en $[c,d]$, con $a \leq p(y) \leq b, \quad a \leq q(y) \leq b, \quad$ para cada $y \in [c,d]$.

Definimos $F : [c,d] \to \mathbb{R}$ por

$$F(y) = \int_{p(y)}^{q(y)} f(x,y)dx.$$

Entonces, existe $F'(y)$, para $y \in (c,d)$, dada por:

$$F'(y) = \int_{p(y)}^{q(y)} \frac{\mathfrak{d}}{\mathfrak{d}y} f(x,y)dx + f(q(y),y) \cdot q'(y) - f(p(y),y) \cdot p'(y).$$

Demostración: Consideremos,

$$G(x_1,x_2,x_3) = \int_{x_1}^{x_2} f(t,x_3)dt,$$

con $x_1, x_2 \in [a,b], \quad x_3 \in [c,d]$.

Así,

$$F(y) = G\ (p(y),q(y),y).$$

Usando la **regla de derivación en cadena**, (ver [5]), obtenemos:

$$\begin{aligned} F'(y) =& \frac{\mathfrak{d}G}{\mathfrak{d}x_1}\ (p(y),q(y),y) \cdot p'(y) + \frac{\mathfrak{d}G}{\mathfrak{d}x_2}\ (p(y),q(y),y) \cdot q'(y) \\ &+ \frac{\mathfrak{d}G}{\mathfrak{d}x_3}\ (p(y),q(y),y) \cdot 1 \end{aligned} \tag{3.3}$$

Por otro lado, utilizando (3.2), se sigue:

$$\frac{\mathfrak{d}G}{\mathfrak{d}x_1} = \frac{\mathfrak{d}}{\mathfrak{d}x_1}\left(- \int_{x_2}^{x_1} f(t,x_3)dt \right) = -f(x_1,x_3).$$

Luego,

$$\frac{\mathfrak{d}G}{\mathfrak{d}x_1}(p(y),q(y),y) = -f(p(y),y)$$

Análogamente,

$$\frac{\mathfrak{d}G}{\mathfrak{d}x_2} = f(x_2,x_3).$$

Por lo tanto:

$$\frac{\mathfrak{d}G}{\mathfrak{d}x_2}(p(y),q(y),y) = f(q(y),y)$$

Finalmente,

$$\frac{\mathfrak{d}G}{\mathfrak{d}x_3} = \int_{x_1}^{x_2} \frac{\mathfrak{d}}{\mathfrak{d}x_3} f(t,x_3)dt.$$

(Ver [6], página 336).

Así que,

$$\frac{\mathfrak{d}G}{\mathfrak{d}x_3}(p(y),q(y),y) = \int_{p(y)}^{q(y)} \frac{\mathfrak{d}}{\mathfrak{d}y} f(t,y)dt.$$

Sustituyendo los resultados parciales, en (3.3), se obtiene lo afirmado. ∎

Ejemplos:

1) Sea $g(t) = \int_1^{t^2} sen(x^2)dx$. Hallar $g'(\sqrt[4]{\frac{\pi}{2}})$

Solución:

$$g'(t) = sen(t^4)\cdot 2t. \qquad \therefore \quad g'\left(\sqrt[4]{\frac{\pi}{2}}\right) = 2\cdot\left(\sqrt[4]{\frac{\pi}{2}}\right)$$

2) Si $g(x) = \int_x^{tgx} e^{-t^2}dt$. Hallar $g'(0)$

Solución:

$$g'(x) = e^{-(tgx)^2}\cdot sec^2x - e^{-x^2}\cdot 1 \qquad \therefore \quad g'(0) = 1-1 = 0$$

3) Sea $f:[0,1]\to\mathbb{R}$, continua, tal que: $f(x) = \int_0^x f(t)dt$. Probar que:

$$f(x) = 0, \quad \text{para todo} \quad x\in[0,1].$$

Solución: $f'(x) = f(x)$. Luego,

$$f(x) = ce^x, \quad \text{para cierta constante} \quad c.$$

Pero,

$$f(0) = \int_0^0 f(t)dt = 0.$$

Así,

$$c = 0. \quad \therefore \quad f(x) = 0, \quad \text{para todo} \quad x\in[0,1].$$

4) Calcular el

$$\lim_{x\to 0^+} \frac{\int_0^x sent^2 dt}{x^3}.$$

Solución: Como el límite es de la forma indeterminada $\frac{0}{0}$, y se reunen las condiciones para aplicar la Regla de L'Hopital, tenemos:

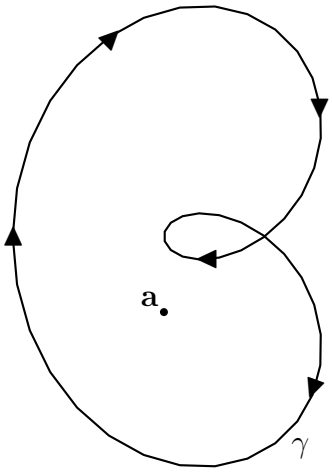
$$\lim_{x\to 0} \frac{\int_0^x sent^2 dt}{x^3} = \lim_{x\to 0} \frac{senx^2}{3x^2} = \frac{1}{3}.$$

5) Una de las maravillas sorprendentes que nos presenta la integración a lo largo de una curva plana es la siguiente:

Si γ es una curva continuamente diferenciable, a trozos, **cerrada**, y que no pasa por el punto a, entonces,

$$\frac{1}{2\pi i}\int_\gamma \frac{dz}{z-a}$$

es un **número entero** (llamado el número de giros de γ, alrededor de a)



Demostración: Si la ecuación de γ es:

$$z = z(t), \quad \alpha \le t \le \beta, \quad \text{con} \quad z(\alpha) = z(\beta),$$

Consideremos $h : [\alpha, \beta] \to \mathbb{C}$, dada por:

$$h(t) = \int_\alpha^t \frac{z'(u)}{z(u)-a} du. \tag{3.4}$$

Entonces,

$$\begin{aligned}[e^{-h(t)}(z(t)-a)]' &= e^{-h(t)}(-h'(t))(z(t)-a) + e^{-h(t)}\cdot z'(t)\\ &= e^{-h(t)}[-z'(t)+z'(t)]\\ &= 0,\end{aligned}$$

donde, hemos utilizado (3.4).

De modo que, $[e^{-h(t)}(z(t)-a)]'$ se **anula en** $[\alpha,\beta]$, con excepción, tal vez, de un número finito de valores de t; de ello, y la continuidad de $e^{-h(t)}(z(t)-a)$, resulta que, existe una **constante** k, tal que,

$$e^{-h(t)}(z(t)-a) = k.$$

O, lo que es lo mismo,

$$e^{h(t)} = \frac{z(t)-a}{k}.$$

Como $h(\alpha)=0$, se sigue que $k = z(\alpha)-a$.

Luego,

$$e^{h(t)} = \frac{z(t)-a}{z(\alpha)-a}.$$

$$\therefore \quad e^{h(\beta)} = \frac{z(\beta)-a}{z(\alpha)-a} = 1, \quad \text{pues} \quad z(\beta)=z(\alpha).$$

Por lo tanto,

$$h(\beta) = 2n\pi i, \quad \text{para algún} \quad n\in\mathbb{Z},$$

(recordar que $e^{i\theta} = \cos\theta + i\cos\theta$)

De manera que:

$$\int_\alpha^\beta \frac{z'(t)}{z(t)-a}dt = 2n\pi i,$$

O sea,

$$\frac{1}{2\pi i}\int_\gamma \frac{dz}{z-a} = n\in\mathbb{Z}.$$

■

6) Sean:

$$f(x) = \left(\int_0^x e^{-t^2}dt\right)^2, \qquad g(x) = \int_0^1 \frac{e^{-x^2(t^2+1)}}{t^2+1}dt.$$

i) Demostrar que $g'(x) + f'(x) = 0$, para todo x.

ii) Utilizar i) para probar que

$$\lim_{x\to+\infty} \int_0^x e^{-t^2} dt = \frac{\sqrt{\pi}}{2}.$$

Solución:

i) Consideremos $f, g : (a, b) \to \mathbb{R}$, donde, $a, b \in \mathbb{R}$, cualesquiera, con $a < b$ y $0 \notin (a, b)$. Tenemos:

$$\begin{aligned} f'(x) &= 2\left(\int_0^x e^{-t^2} dt \right) \cdot e^{-x^2} \\ &\text{y} \\ g'(x) &= \int_0^1 \frac{(t^2+1)e^{-x^2(t^2+1)}}{t^2+1} dt = -2xe^{-x^2} \int_0^1 e^{-x^2t^2} dt \end{aligned} \tag{3.5}$$

Ahora bien, en la última integral, hagamos el cambio de variable: $w = tx$; por lo tanto, $dw = xdt$, y resulta,

$$g'(x) = -2xe^{-x^2} \int_0^x \frac{e^{-w^2}}{x} dw = -2e^{-x^2} \int_0^x e^{-w^2} dw \tag{3.6}$$

Así, de (3.5) y (3.6) se sigue:

$$f'(x) + g'(x) = 0, \quad \text{para todo} \quad x \in (a, b),$$

donde, $a, b \in \mathbb{R}$, son cualesquiera, con $0 \notin (a, b)$.

Por otro lado,

$$f'(0) = \lim_{x\to 0} \frac{f(x) - f(0)}{x - 0} = \lim_{x\to 0} \frac{\left(\int_0^x e^{-t^2} dt \right)^2}{x}.$$

Usando la regla de L'Hôpital, tenemos:

$$f'(0) = \lim_{x\to 0} \frac{2\left(\int_0^x e^{-t^2} dt \right) e^{-x^2}}{1} = 0.$$

Análogamente,

$$g'(0) = \lim_{x\to 0} \frac{g(x) - g(0)}{x - 0} = \lim_{x\to 0} \frac{\int_0^1 \frac{e^{-x^2(t^2+1)}dt}{t^2+1} - \frac{\pi}{4}}{x}$$

$$= \lim_{x\to 0} \frac{-2e^{-x^2}\int_0^x e^{-w^2}dw}{1} = 0,$$

donde, hemos usado, nuevamente la Regla de L'Hôpital, (3.6), y que, se puede introducir el límite, bajo el signo integral, es decir,

$$\lim_{x\to 0}\int_0^1 \frac{e^{-x^2(t^2+1)}}{t^2+1}dt = \int_0^1 \lim_{x\to 0}\frac{e^{-x^2(t^2+1)}}{t^2+1}dt = \int_0^1 \frac{1}{t^2+1}dt = arctgt\Big|_0^1 = \frac{\pi}{4},$$

pues $\dfrac{e^{-x^2(t^2+1)}}{t^2+1} \to \dfrac{1}{t^2+1}$, uniformemente en $t \in [0,1]$, si $x \to 0$.

De manera, que ahora, podemos afirmar que $g'(x) + f'(x)$ es igual a 0, para todo $x \in \mathbb{R}$.

Luego, $g(x) + f(x)$ es constante.

Pero,

$$f(0) = 0 \quad \text{y} \quad g(0) = \frac{\pi}{4}.$$

Conclusión:

$$g(x) + f(x) = \frac{\pi}{4}.$$

ii) Por lo probado en i) tenemos que:

$$\Big(\int_0^x e^{-t^2}dt\Big)^2 + \int_0^1 \frac{e^{-x^2(t^2+1)}}{t^2+1}dt = \frac{\pi}{4}, \quad \text{para todo} \quad x \in \mathbb{R} \qquad (3.7)$$

Como $\dfrac{e^{-x^2(t^2+1)}}{t^2+1} \to 0$, uniformemente en $t \in [0,1]$, si $x \to +\infty$.

Entonces,

$$\lim_{x\to+\infty}\int_0^1 \frac{e^{-x^2(t^2+1)}}{t^2+1}dt = \int_0^1 \lim_{x\to+\infty}\frac{e^{-x^2(t^2+1)}}{t^2+1}dt = \int_0^1 0dt = 0.$$

(Ver [3], página 615).

Luego, de (3.7) se sigue que, existe el

$$\lim_{x\to+\infty}\Big(\int_0^x e^{-t^2}dt\Big)^2, \quad \text{y vale} \quad \frac{\pi}{4}$$

Ahora, sólo nos falta probar que existe el

$$\lim_{x\to+\infty}\int_0^x e^{-t^2}dt$$

Llamemos $a_n = \int_0^n e^{-t^2}dt$.

Tenemos que: (a_n) es una sucesión **creciente**, tal que (a_n^2) converge (su límite es $\frac{\pi}{4}$).

Luego (a_n^2) es acotada, y, en consecuencia, (a_n) también es **acotada**.

De modo que (a_n) converge, lo cual equivale a que:

$$\int_0^{+\infty} e^{-t^2}dt \qquad \text{existe.}$$

Podemos escribir, entonces:

$$\frac{\pi}{4} = \lim_{x\to+\infty}\Big(\int_0^x e^{-t^2}dt\Big)^2 = \Big(\lim_{x\to+\infty}\int_0^x e^{-t^2}dt\Big)\cdot\Big(\lim_{x\to+\infty}\int_0^x e^{-t^2}dt\Big).$$

Conclusión:

$$\lim_{x\to+\infty}\int_0^x e^{-t^2}dt = \frac{\sqrt{\pi}}{2}$$

■

Capítulo 4

El Teorema de Baire.

Este teorema tiene, entre otras cosas, la importancia de ser **la fuente** de notables resultados del Análisis Funcional.

Preparativos:

Un Subconjunto S, de un **espacio métrico** M, es llamado:

a) Raro en M (o denso en ninguna parte) si $\overline{S}$ no tiene puntos interiores

Ejemplo: Si $M = \mathbb{R}$, **con la métrica usual**, y $S = \{x_1, x_2, \ldots, x_k\}$, donde, $x_i \in \mathbb{R}, i = 1, 2, \ldots, k$, entonces, S es **raro en** $\mathbb{R}$

También, $\mathbb{N}$, $\mathbb{Q}$, y cualquier subconjunto de $\mathbb{R}$, **numerable**, es raro en $\mathbb{R}$ (con la métrica usual)

b) Magro en M (o de primera categoría), si es la unión numerable de conjuntos, cada uno de los cuales es raro en M.

Por ejemplo, si $M = \mathbb{R}$, con la métrica usual, y $S = \mathbb{Z}$, conjunto de los números enteros, entonces S es magro en M.

Ási mismo, $\mathbb{N}$ y $\mathbb{Q}$ son magros en $\mathbb{R}$ (con la métrica usual).

Otro ejemplo, menos trivial, lo podemos conseguir, en el espacio M, de las funciones continuas, $f : [0, 1] \to \mathbb{R}$.

La distancia entre dos elementos f, $g \in M$ se define como

$$d(f, g) = \max_{0 \leq x \leq 1} |f(x) - g(x)|.$$

Como S, tomamos el subconjunto de M, formado por todas aquellas funciones continuas con derivada en algún punto de $[0,1]$.

Resulta (ver [4], página 195) que S es magro en M. Por cierto, fue en 1872 cuando Karl Weierstrass asombró al mundo matemático presentando un ejemplo de función continua en todos sus puntos, tal que el conjunto de los puntos donde ella es derivable es vacío. Lo sorprendente es que la "mayoria"(en cierto sentido) de las funciones continuas son así.

c) De segunda categoría en M (o no-magro):

Si S no es magro en M

Ejemplo: sea $M = \mathbb{R}$ (con la métrica usual), y $S = \mathbb{R}$. Entonces, S es de segunda categoría en $\mathbb{R}$.

La justificación de ese hecho la conseguimos a través del

Teorema de Baire:

Si un espacio métrico M, no vacío, es **completo**, entonces, él **es de segunda categoría en él mismo**. En consecuencia, si $M \neq \emptyset$ es un espacio métrico completo y

$$M = \bigcup_{k=1}^{+\infty} A_k$$

(con cada A_k cerrado en M) entonces, el **interior** de, por lo menos, algún A_k, es **no vacío**.

Demostración:

Supongamos que el espacio métrico $M \neq \emptyset$ es completo y magro en sí mismo. Entonces,

$$M = \bigcup_{k=1}^{+\infty} A_k,$$

donde, cada A_k es **raro en M**. Construiremos una sucesión de Cauchy, (x_n), con $x_n \in M$, para todo n, la cual nos conducirá a una contradicción.

Veamos:

A_1 es raro en M, de modo que $\overline{A_1}$ no contiene un subconjunto abierto, no vacío. Pero M sí contiene a un abierto, no vacio (por ejemplo, M mismo). Luego, $\overline{A_1} \neq M$.

Entonces, $\bar{A_1}^c$ es **no vacío y abierto.**

Elijamos un punto x_1 en A_1, y una bola abierta, digamos,
$B_1 = B(x_1; r_1) \subset A_1$, con $r_1 < \frac{1}{2}$.

Como $\mathbf{A_2}$ es raro en M, tenemos que $\bar{A}_2$ no contiene un conjunto abierto, no vacío. Por ejemplo, no contiene la bola abierta $B(x_1; \frac{r_1}{2})$.

Así, $\bar{A_2}^c \bigcap B(x_1; \frac{r_1}{2})$ es un abierto, no vacío.

Sea

$$\mathbf{B_2} = B(x_2; r_2) \subset \bar{A_2}^c \bigcap B\big(x_1; \frac{r_1}{2}\big) \qquad \text{con} \qquad r_2 < \frac{r_1}{2}.$$

Por inducción, obtenemos una sucesión de bolas abiertas:

$$B_k = B(x_k; r_k), \quad \text{con} \quad r_k < \frac{1}{2^k},$$

$$\text{tales que,} \quad B_k \bigcap A_k = \emptyset \quad y \quad B_{k+1} \subset B\big(x_k; \frac{r_k}{2}\big) \subset B_k, \quad k = 1, 2, ...$$

Como $r_k < \frac{1}{2^k}$, la sucesión (x_k), de los centros, es de Cauchy.

Por la completitud de M, dicha sucesión converge, digamos, $x_k \to x \in M$

También, para m,n, con $n > m$, se tiene: $B_n \subset B(x_m; \frac{r_m}{2})$, de manera que:

$$d(x_m, x) \leq d(x_m, x_n) + d(x_n, x) < \frac{r_m}{2} + d(x_n, x). \tag{4.1}$$

Como $\frac{r_m}{2} + d(x_n, x) \to \frac{r_m}{2}$, cuando $n \to +\infty$, se sigue de (4.1), que:

$$d(x_m, x) \leq \frac{r_m}{2} < r_m, \quad \text{es decir,} \quad x \in B_m, \quad \textbf{para todo} \quad m.$$

Además, ya que $B_m \subset \overline{A_m}^{\,c}$, resulta que $x \notin A_m$, para todo m. Luego

$$x \notin \bigcup_{k=1}^{+\infty} A_m = M$$

(contradicción). Así, el Teorema de Baire está probado ∎

Teorema de la Acotación Uniforme (o de Banach-Steinhaus)

Sean: B, espacio de Banach; N, espacio vectorial normado; $\{T_i\}$, conjunto, no vacío, de transformaciones lineales continuas de B en N, con la propiedad de que $\{T_i(x)\}$ es un subconjunto acotado, de N, para cada $x \in B$, digamos,

$$||T_i(x)|| \leq c_x, \quad i = 1, 2, \ldots \tag{4.2}$$

Entonces, $\{||T_i||\}$ es un subconjunto, **acotado**, de $\mathbb{R}$; o sea, existe $c \in \mathbb{R}$, tal que

$$||T_i|| \leq c, \qquad i = 1, 2, \ldots \tag{4.3}$$

Demostración:

Para cada k, número natural, sea

$$A_{\mathbf{k}} = \{x \in B : ||T_n(x)|| \leq \mathbf{k} \quad \text{para} \quad n = 1, 2, ...\}.$$

Tenemos que: A_k es cerrado.

En efecto, sea $x \in \bar{A}_k$.

Entonces, existe (x_j), sucesión en A_k, tal que,

$$x_j \to x. \tag{4.4}$$

Pero, **para cada** n, fijo, se tiene:

$$||T_n(x_j)|| \leq k,$$

de lo cual se sigue que:

$$||T_n(x)|| \leq k,$$

al usar (4.4), la continuidad de T_n y la continuidad de la norma $||\cdot||$; de modo que, $x \in A_k$, y así, A_k es cerrado.

Por otro lado, **dado** $x \in B$, se tiene que, según (4.2), existe c_x, tal que $||T_n(x)|| \leq c_x$, para $n = 1, 2, 3, ...$

Entonces, x pertenece a algún A_k (basta tomar $k \geq c_x$). De modo que,

$$B = \bigcup_{k=1}^{+\infty} A_k$$

En este momento, aparece el toque mágico dado por el Teorema de Baire: Como B es completo, resulta que, algún A_k contiene una bola abierta, digamos:

$$B_0 = B(x_0; r) \subset A_{k_0}$$

Ahora viene, un lance magistral:

Dado cualquier $x \in B$**, no nulo**, lo multiplicamos por un escalar apropiado, luego trasladamos el vector resultante, y conseguimos que el nuevo

vector esté en B_0. Lo demás, corre por cuenta de la linealidad de T_n, para cada n; veámoslo:

Sea

$$z = \frac{r}{2||x||}\, x + x_0$$

$$\therefore \quad ||z - x_0|| = \frac{r}{2} < r$$

$$\therefore \quad z \in B_0$$

$$\therefore \quad ||T_n(z)|| \leq k_0, \quad n = 1, 2, 3, \ldots$$

$$\therefore \quad ||T_n\big(\frac{r}{2||x||}x + x_0\big)|| \leq k_0,$$

o sea,

$$||\frac{r}{2||x||}\, T_n(x) + T_n(x_0)|| \leq k_0$$

$$\therefore \quad \frac{r}{2||x||}\, ||T_n(x)|| \leq k_0 + ||T_n(x_0)|| \leq 2k_0$$

$$\therefore \quad ||T_n(x)|| \leq \frac{4k_0}{r}\, ||x||, \quad n = 1, 2, 3, \ldots$$

$$\therefore \quad ||T_n||\, \frac{4k_0}{r}, \quad n = 1, 2, 3, \ldots$$

Así, para obtener (4.3) basta tomar

$$c = \frac{4k_0}{r}$$

■

Corolario 4.1: El espacio vectorial normado X, de todos los polinomios; con la norma definida por:

$$||p|| = \max_i |\alpha_i|, \ \textbf{donde,} \quad \alpha_0,\ \alpha_1, \ldots \quad \textbf{son los coeficientes de} \quad p;$$

no es completo.

Demostración:

Construiremos una **sucesión** (T_n) de transformaciones lineales de X en $\mathbb{R}$, la cual satisface (4.2), pero no cumple (4.3). Así, X no puede ser completo.

Escribamos un polinomio p, distinto del polinomio nulo, de grado N_p, en la forma:

$$p(t) = \sum_{j=0}^{+\infty} \alpha_j t^j, \quad \text{donde} \quad \alpha_j = 0, \quad \text{para} \quad j > N_p,$$

Para cada número natural n, definimos $T_{\mathbf{n}} : X \to \mathbb{R}$, por:

$$T_n(\mathbf{0}) = 0,$$

$$T_n(p) = \alpha_0 + \alpha_1 + ... + \alpha_{n-1}$$

La linealidad de T_n es inmediata; el que T_n es acotado (continuo) se obtiene así:

$$|\alpha_j| \leq ||p|| \quad \therefore \quad |T_n(p)| \leq n||p||.$$

Además, para cada $p \in X$, la sucesión $(|T_n(p)|)$ satisface (4.2), porque un polinomio p, de grado N_p, tiene $N_p + 1$ coeficientes, y así,

$$|T_n(p)| \leq (N_p + 1) \max_j |\alpha_j| = c_p,$$

lo cual es de la forma (4.2).

Ahora, veremos que (T_n) no satisface (4.3), o sea, no existe c, tal que $||T_n|| \leq c$, para $n = 1, 2, 3, ...$

Sea p_n definido por:

$$p_n(t) = 1 + t + t^2 + \ldots + t^n.$$

Entonces,

$$||p_n|| = 1, \quad \text{y} \quad T_n(p_n) = 1 + 1 + \ldots + 1 = n = n||p_n||$$

$$\therefore ||T_n|| \geq \frac{|T_n(p_n)|}{||p_n||} = n$$

Luego, $(||T_n||)$ no es acotada. ∎

Nota 4.1: Si consideramos

$$p_n = 1 + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots + \frac{t^n}{n!},$$

puede probarse que (p_n) es una sucesión de Cauchy, pero (p_n) no converge en X.

El tercer "gran" teorema, que presentaremos a continuación, es el **Teorema de la Aplicación Abierta**.

El está relacionado con la aplicaciones abiertas; éstas son funciones que envían conjuntos abiertos en conjuntos abiertos. Más específicamente, el Teorema

de la Aplicación Abierta establece condiciones bajo las cuales una transformación lineal acotada (o lo que es lo mismo, continua) es una aplicación abierta.

Como en el Teorema de la Aplicación Uniforme, la propiedad de **Completitud** es importante.

El Teorema también da condiciones para garantizar la continuidad de la inversa de una transformación lineal acotada.

Lema 4.1: Si B y B' son **espacios de Banach** y, si T es una transformación lineal continua de B **sobre** B', entonces, la imagen de cada bola abierta, centrada en el origen, en B, contiene una esfera abierta, centrada en el origen, en B'.

Demostración: Denotamos por S_r yS'_r, las bolas abiertas, con radio r, centradas en el origen, en B y B', respectivamente. Es simple probar que

$$T(S_r) = T(rS_1) = rT(S_1),$$

así que, es suficiente probar que $T(S_1)$ contiene alguna S'_r.

Comenzaremos mostrando que $\overline{T(S_r)}$ contiene alguna S'_r.

Ya que T es sobreyectiva, resulta que

$$B' = \bigcup_{n=1}^{+\infty} T(S_n).$$

Como B' es **completo**, se sigue del Teorema de Baire que algún $\overline{T(S_{n_0})}$ tiene un punto interior, y_0, el cual podemos asumir que está en $T(S_{n_0})$.

La aplicación $y \mapsto y - y_0$, es un **homeomorfismo** de B' sobre sí mismo, de manera que

$$\overline{T(S_{n_0})} - y_0 \quad \text{tiene el origen como punto interior} \tag{4.5}$$

Además, ya que $y_0 \in T(S_{n_0})$, se sigue que

$$T(S_{n_0}) - y_0 \subseteq T(S_{2n_0}), \tag{4.6}$$

de modo que:

$$\overline{T(S_{n_0})} - y_0 = \overline{T(S_{n_0}) - y_0} \subseteq \overline{T(S_{2n_0})},$$

lo cual, según (4.5), prueba que el origen es un punto interior de $\overline{T(S_{2n_0})}$.

Por otro lado, la multiplicación por un escalar, no nulo, es un homeomorfismo de B' sobre sí mismo, así,

$$\overline{T(S_{2n_0})} = \overline{2n_0 T(S_1)} = 2n_0 \overline{T(S_1)}.$$

Luego, el origen es, también, un punto interior de $\overline{T(S_1)}$, o sea,

$$S'_\epsilon \subseteq \overline{T(S_1)}, \quad \text{para algún} \quad \epsilon > 0 \tag{4.7}$$

Ahora probaremos que $S'_\epsilon \subseteq T(S_3)$, es decir, $S'_{\frac{\epsilon}{3}} \subseteq T(S_1)$.

Ya hemos utilizado la completitud de B'; es el momento de que aparezca la completitud de B.

Sea $y_0 \in B'$, tal que $||y_0|| < \epsilon$.

De (4.7) se sigue:

$$y_0 \in S'_\epsilon \subseteq \overline{T(S_1)}.$$

Luego, existe $\quad x_1 \in B, \quad$ con $\quad ||x_1|| < 1, \quad$ y $\quad ||y_0 - y_1|| < \frac{\epsilon}{2},$

donde,

$$y_1 = T(x_1). \tag{4.8}$$

También, de (4.7) se obtiene:

$$S'_{\frac{\epsilon}{2}} \subseteq \overline{T(S_{\frac{1}{2}})},$$

que, junto con (4.8), permite escribir:

$$y_0 - y_1 \in \overline{T(S_{\frac{1}{2}})}.$$

De modo que, existe $x_2 \in B$, tal que:

$$||x_2|| < \frac{1}{2}, \quad \text{y} \quad ||y_0 - (y_1 + y_2)|| < \frac{\epsilon}{4},$$

donde, $y_2 = T(x_2)$. Prosiguiendo de esta manera, conseguimos una sucesión (x_n), en B, tal que:

$$||x_n|| < \frac{1}{2^{n-1}} \tag{4.9}$$

y

$$||y_0 - (y_1 + y_2 + ...y_n)|| < \frac{\epsilon}{2^n}, \quad \text{donde}, \quad y_n = T(x_n), \quad n = 1, 2, \ldots \tag{4.10}$$

Llamemos $S_n = x_1 + x_2 + ... + x_n$;

De (4.9) se deduce que (S_n) es una sucesión de Cauchy, en B.

Como B **es completo**, existe $x \in B$, tal que $S_n \to x$.

Además,

$$||S_n|| \leq ||x_1|| + ||x_2|| + ... + ||x_n|| < 1 + \frac{1}{2} + \frac{1}{4} + ... + \frac{1}{2^{n-1}} < 2.$$

Por otro lado,

$$||x|| \leq ||\lim S_n|| = \lim ||S_n|| \leq 2 < 3, \quad \text{es decir,} \quad x \in S_3.$$

Ahora bien, usando la continuidad de T, se tiene:

$$T(x) = T(\lim S_n) = \lim T(S_n) = \lim(y_1 + y_2 + ... + y_n) = y_0,$$

(usando (4.10)).

Es decir,

$$y_0 \in T(S_3)$$

Conclusión: $S'_\epsilon \subseteq T(S_3)$. ∎

Teorema de la Aplicación Abierta.

Sean: B, B', espacios de Banach; $T : B \to B'$, transformación lineal, continua, **sobreyectiva.**

Entonces, T es una aplicación abierta.

Por lo tanto, si T es biyectiva, entonces T^{-1} es continua.

Demostración:

Sea $G \subseteq B$, abierto. Probemos que $T(G) \subseteq B'$, también es abierto.

Tomemos $y \in T(G)$.

Sea $x \in G$, tal que $y = T(x)$.

Como G es abierto, existe una **bola** abierta, con centro en x, **contenida en** G.

Dicha bola la podemos expresar como:

$$x + S_r, \tag{4.11}$$

donde, S_r es una bola abierta, de radio r, centrada en el origen de B.

Ahora bien, el lema 4.1 nos indica que $T(S_r)$ contiene alguna S'_{r_0}

Entonces, $y + S'_{r_0}$ es una bola abierta, centrada en y, contenida en $T(G)$, pues:

$$y + S'_{r_0} \subseteq y + T(S_r) = T(x) + T(S_r) = T(x + S_r) \subseteq T(G), \quad \text{usando (4,11)}$$

Finalmente, si $T^{-1} : B' \to B$, existe, resulta que, como T es abierta, T^{-1} es continua (vale decir, acotada. Ver [7], página 238) ∎

Ejercicios:

1) Una proyección P sobre un espacio de Banach B, es una proyección sobre B, en el sentido algebraico (es decir $P^2 = P$), que, además, es continua. Sea B un espacio de Banach, y sean M y N, subespacios vectoriales, **cerrados**, de B, tales que $B = M \bigoplus N$ (suma directa).

Si $z = x + y$ es la **única** representación de un vector $z \in B$, como una suma de vectores en M y N, entonces, $P : B \to B$, definida por $P(z) = x$ es una proyección sobre B, cuyo rango y núcleo son M y N, respectivamente.

Demostración:

Lo que no es tan trivial es la prueba de la continuidad de P.

Sea B', el espacio vectorial B, equipado con la norma definida por:

$$||z||' = ||x|| + ||y||.$$

Resulta que B' es un espacio de Banach (ejercicio para el lector: ahí se usa que M y N son cerrados en B).

Ahora bien, como:

$$||P(z)|| = ||x|| \leq ||x|| + ||y|| = ||z||',$$

se sigue que P es continua, como una aplicación de B' en B.

Basta entonces, para lograr nuestro propósito, probar que B' y B tienen **la misma topología.**

Sea $T : B' \to B$, definida por: $T(w) = w$.

Tenemos:

$$||T(z)|| = ||z|| = ||x + y|| \leq ||x|| + ||y|| = ||z||'.$$

Luego, T es continua, y, además, biyectiva.

Así, en virtud del Teorema de la Aplicación Abierta, T es un **homeomorfismo**, lo cual implica que B' y B tienen la misma topología. ∎

2) Demostrar que $T : \mathbb{R}^2 \to \mathbb{R}$, dada por: $T(\epsilon_1, \epsilon_2) = \epsilon_1$, es abierta.

¿Es $W : \mathbb{R}^2 \to \mathbb{R}^2$, definida por: $W(\epsilon_1, \epsilon_2) = (\epsilon_1, 0)$ una aplicación abierta?

Solución:

T es lineal, continua, sobreyectiva; $\mathbb{R}^2$ y $\mathbb{R}$ son espacios de Banach. Luego, por el Teorema de la Aplicación Abierta, T es abierta.

En cambio, W no lo es.

Basta considerar $A = B((0,0);1)$, y notar que $W(A) = (-1,1)$, el cual no es abierto en $\mathbb{R}^2$.

3) Sea X, el espacio vectorial normado cuyos puntos son las sucesiones de números complejos $x = (\epsilon_i)$, con sólo un número finito de términos diferentes de cero, y la norma dada por:

$$||x|| = \sup_i |\epsilon_i|$$

Sea $T : X \to X$, definida así:

$$y = Tx = \left(\epsilon_1, \frac{1}{2}\,\epsilon_2, \frac{1}{3}\,\epsilon_3, \ldots\right)$$

Demostrar que T es lineal y acotada, pero T^{-1} no es continua.

Solución:

Sea $\lambda \in \mathbb{C}$, entonces:

$$T(\lambda x) = T(\lambda\epsilon_1, \lambda\epsilon_2, \ldots) = (\lambda\epsilon_1, \frac{\lambda\epsilon_2}{2}, \frac{\lambda\epsilon_3}{3}, \ldots) = \lambda(\epsilon_1, \frac{\lambda\epsilon_2}{2}, \frac{\lambda\epsilon_3}{3}, \ldots) = \lambda Tx$$

Análogamente, si

$$x = (\epsilon_1, \epsilon_2, \epsilon_3, \ldots)$$
$$y = (\theta_1, \theta_2, \theta_3, \ldots),$$

entonces,

$$x + y = (\epsilon_1 + \theta_1, \epsilon_2 + \theta_2, \ldots)$$

$$\therefore T(x+y) = (\epsilon_1 + \theta_1, \frac{\epsilon_2 + \theta_2}{2}, \ldots)$$

$$(\epsilon_1, \frac{\epsilon_2}{2}, \frac{\epsilon_3}{3}, \ldots) + (\theta_1, \frac{\theta_2}{2}, \frac{\theta_3}{3}, \ldots) = Tx + Ty$$

$$\therefore \quad T \quad \text{es lineal.}$$

Ahora,

$$||Tx|| = ||(\epsilon_1, \frac{\epsilon_2}{2}, \frac{\epsilon_3}{3}, \ldots)|| = \sup_n \left|\frac{\epsilon_n}{n}\right| \leq \sup_n |\epsilon_n| = ||x||.$$

$$\therefore \quad T\text{es acotado, con} \quad ||T|| \leq 1.$$

Por otro lado,

$$T^{-1}(x) = (\epsilon_1, 2\ \epsilon_2, 3\ \epsilon_3, \ldots)$$

Si tomamos $x_0 = (0, 0, ..., 0, 1, 0, ...)$, donde el 1 está en la k-ésima casilla, tenemos:

$$||x_0|| = 1, \quad \text{pero} \quad ||T^{-1}x_0|| = k = k||x_0||$$

Como k puede ser tan grande como se quiera, no existe c, tal que:

$$||T^{-1}x|| \leq c||x||, \quad \textbf{para todo} \quad x \in X$$

Luego, T^{-1} no es **acotado** (vale decir, **continuo**).

4) Sean: X e Y, espacios de Banach; $T : X \to Y$, lineal, acotado, **inyectivo.**

Demostrar que:

$$T^{-1} : \mathfrak{R}(T) \to X, \quad (\text{donde}, \quad \mathfrak{R}(T) \quad \text{es el rango de} \quad T),$$

es acotado si, y sólo si, $\mathfrak{R}(T)$ es cerrado en Y.

Demostración:

Si $\mathfrak{R}(T)$ es cerrado en Y, entonces $\mathfrak{R}(T)$ es de Banach. Entonces, como $T : X \to \mathfrak{R}(T)$ es sobreyectiva, una utilización directa del Teorema de la Aplicación Abierta nos permite concluir que T^{-1} es continuo (o sea, acotado).

Supongamos, ahora, que: $T^{-1} : \mathfrak{R}(T) \to X$ es acotado.

Sea $y \in \overline{\mathfrak{R}(T)}$.

Luego, existe (y_n), sucesión en $\mathfrak{R}(T)$, tal que:

$$y_n \to y \in Y \tag{4.12}$$

Tenemos: $y_n = T(x_n), \quad x_n \in X$

Así que,

$$||x_n - x_m|| = ||T^{-1}(y_n) - T^{-1}(y_m)|| = ||T^{-1}(y_n - y_m)|| \leq ||T^{-1}|| \cdot ||y_n - y_m||$$

Como (y_n) converge, entonces, (y_n) es de Cauchy, y, usando la anterior desigualdad, concluímos que (x_n) también es de Cauchy.

De modo que, existe $x \in X$, tal que $x_n \to x$ (ya que X es completo)

Usando, ahora, la continuidad de T, tenemos:

$$y_n = T(x_n) \to Tx. \tag{4.13}$$

Así, de (4.12) y (4.13), se sigue: $y = Tx$, o sea, $y \in \mathfrak{R}(T)$

En otras palabras, $\mathfrak{R}(T)$ es cerrado en Y.

5) Recordemos que el conjunto $\mathcal{T}$, de **todos los subconjuntos abiertos** de un espacio métrico X, es llamado una **topología** para X. En consecuencia, cada norma sobre un espacio vectorial X define una topología para X. Si tenemos dos normas en X, tales que $X_1 = (X, ||\cdot||_1)$ y $X_2 = (X, ||\cdot||_2)$ son **espacios de Banach** y las topologías $\mathcal{T}_1$ y $\mathcal{T}_2$ definidas por $||\cdot||_1$ y $||\cdot||_2$, respectivamente, satisfacen $\mathcal{T}_2 \subset \mathcal{T}_1$ (se dice que $\mathcal{T}_1$ es más fina que $\mathcal{T}_2$),

Probar que $\mathcal{T}_1 = \mathcal{T}_2$.

Demostración: Consideremos la aplicación identidad I,

$$I : X_1 \to X_2$$

$$I(x) = x.$$

Tenemos que I es lineal; **continua,** pues todo abierto en X_2 es abierto en X_1

Como I es sobreyectiva, y además, X_1 y X_2 son espacios de Banach, resulta, en virtud del Teorema de la Aplicación Abierta, que I es una aplicación abierta, y, en consecuencia, $I^{-1} : X_2 \to X_1$ es continua.

Conclusión: $\mathcal{T}_1 = \mathcal{T}_2$. ∎

En muchas aplicaciones del Análisis, surgen transformaciones lineales que no son continuas, pero que , en compensación, tienen una propiedad importante, que es descrita en términos del concepto de gráfico de una función.

Sean B y B', espacios de Banach. Definimos una métrica sobre el producto $B \times B'$ por:

$$d((x_1, y_1), (x_2, y_2) = \text{máx} = \{||x_1 - x_2||, ||y_1 - y_2||\}.$$

La topología resultante es llamada **topología producto**, y la convergencia respecto a esta métrica es equivalente a la convergencia coordenada a coordenada.

Sea T una transformación lineal de B en B'

El gráfico de T es el subconjunto de $B \times B'$ que consiste de todos los pares ordenados de la forma (x, Tx).

Fácilmente, vemos que si T es continuo, entonces su gráfico, $\mathbf{Gr(T)}$, es cerrado, como subconjunto de $B \times B'$.

Por su parte, **El Teorema del Gráfico Cerrado establece que:** si B y B' son espacios de Banach, y si T es una transformación lineal de B en B', con $Gr(T)$ **cerrado**, entonces, **T es continua.**

Demostración: Denotemos por B_1, al espacio B, con la norma:

$$||x||_1 = ||x|| + ||Tx||.$$

Como

$$||Tx|| \leq ||x|| + ||Tx|| = ||x||_1,$$

resulta que T es continua como aplicación de B_1 en B'.

Resta probar que B y B_1 tienen la misma topología.

La aplicación identidad de B_1 **sobre** B es continua, pues:

$$||x|| \leq ||x|| + ||Tx|| = ||x||_1.$$

Si pudiéramos probar que B_1 es **completo**, entonces, el Teorema de la Aplicación Abierta, garantizaría que $I : B_1 \to B$ es un **homeomorfismo** y esto terminaría la prueba.

Sea (x_n), una sucesión de Cauchy, en B_1. Esto implica que (x_n) y (Tx_n) son sucesiones de Cauchy en B y en B', respectivamente.

Ya que ambos son espacios **completos**, existen: $x \in B, \quad y \in B'$, tales que:

$$||x_n - x|| \to 0 \quad \text{y} \quad ||Tx_n - y|| \to 0 \tag{4.14}$$

(o sea, $(x_n, Tx_n) \to (x, y)$).

Nuestra suposición de que $Gr(T)$ es cerrado en $B \times B'$, implica que:

$$(x, y) \in Gr(T).$$

Así, $y = Tx$.

De ello se obtiene que B_1 es completo, pues:

$$\begin{aligned} ||x_n - x||_1 &= ||x_n - x|| + ||T(x_n - x)|| \\ &= ||x_n - x|| + ||Tx_n - Tx|| \\ &= ||x_n - x|| + ||Tx_n - y|| \longrightarrow 0, \qquad \text{según (4.14)} \end{aligned}$$

■

Veamos, a manera de ilustración, un ejemplo de una transformación lineal, cuyo gráfico es cerrado, pero que no es continua.

Sea $T : X \longrightarrow Y$, dada por $Tx = x'$, donde, $Y = \mathcal{C}[0, 1]$, espacio de las funciones continuas de $[0, 1]$ en $\mathbb{R}$, con la norma de la convergencia uniforme:

$$||w|| = \max_{0 \le t \le 1} |w(t)|,$$

mientras que

$$X = \{x \in Y : x' \in Y\}.$$

Sea $(z, y) \in \overline{Gr(T)}$, entonces existe (z_n), sucesión en X, tal que:

$$z_n \longrightarrow z, \quad (\text{convergencia en} \quad X)$$

$$T(z_n) = z_n' \longrightarrow y \quad (\text{convergencia en} \quad Y)$$

Ya que la convergencia en Y es la **convergencia uniforme**, tenemos: Para $t \in [0, 1]$,

$$\begin{aligned} \int_0^t y(u)du &= \int_0^t \lim_{n \to +\infty} z_n'(u)du = \lim_{n \to +\infty} \int_0^t z_n'(u)du \\ &= \lim_{n \to +\infty} (z_n(t) - z_n(0)) = z(t) - z(0) \end{aligned}$$

O sea,

$$z(t) = z(0) + \int_0^t y(u)du.$$

De modo que, $z \in X$ y $Tz = z' = y$ (de acuerdo al Teorema Fundamental del Cálculo).

En otras palabras, $(z, y) \in Gr(T)$, y así, $Gr(T)$ es cerrado en $X \times Y$.

Para ver que T no es continua, basta considerar la sucesión (x_n), donde,

$$x_n : [0,1] \longrightarrow \mathbb{R} \quad \text{es dada por:} \quad x_n(t) = t^n.$$

Tenemos:

$$||x_n|| = \max_{0 \leq t \leq 1} |x_n(t)| = 1;$$

Mientras que,

$$||T(x_n|| = ||x_n'|| = \max_{0 \leq t \leq 1} |nt^{n-1}| = n$$

Así,

$$\frac{x_n}{n} \longrightarrow \mathbf{0}, \quad \text{cuando} \quad n \longrightarrow +\infty,$$

pero,

$$T\left(\frac{x_n}{n}\right) = \frac{x_n'}{n} \nrightarrow \mathbf{0} = T(\mathbf{0})$$

■

Ejercicio:

Sean, X e Y, espacios vectoriales normados; $T : X \longrightarrow Y$, lineal, **cuyo gráfico es cerrado.** Probar que:

a) Si $K \subset X$ es compacto, entonces $T(K)$ es cerrado en Y.

b) Si $K \subset Y$ es compacto, entonces $T^{-1}(K)$ es cerrado en X.

c) Si Y es compacto, entonces, T es acotado.

d) Si X es compacto, y T es biyectiva, Entonces T^{-1} es acotado.

Solución:

a) Sea $y \in \overline{T(K)}$, entonces existe (x_n), sucesion en K, tal que :

$$T(x_n) \longrightarrow y.$$

De la compacidad de K, se deduce que existe (x_{n_j}), subsucesión de (x_n), tal que:

$$x_{n_j} \longrightarrow x \in K.$$

Así,

$$(x_{n_j}, T(x_{n_j})) \longrightarrow (x, y).$$

Luego,

$$(x, y) \in \overline{Gr(T)} = Gr(T)$$

En consecuencia,

$$y = Tx, \quad \text{con} \quad x \in K$$

O sea,

$$y \in T(K).$$

Conclusión: $T(K)$ es cerrado en Y.

b) Tomemos $x \in \overline{T^{-1}(K)}$. Luego, existe (y_n), sucesión en K, tal que:

$$T^{-1}(y_n) \longrightarrow x.$$

Como K es compacto, existe (y_{n_j}), subsucesión de (y_n), tal que,

$$y_{n_j} \longrightarrow y \in K.$$

Sea $x_n = T^{-1}(y_n)$, es decir, $y_n = Tx_n$. Tenemos que:

$$(x_{n_j}, T(x_{n_j})) = (T^{-1}(y_{n_j}), y_{n_j}) \longrightarrow (x, y)$$

Así que,

$$(x, y) \in \overline{Gr(T)} = Gr(T)$$

Luego,

$$y = Tx,$$

O lo que es lo mismo,

$$x = T^{-1}(y).$$

De modo que,

$$x \in T^{-1}(K)$$

En resumen,

$$T^{-1}(K) \quad \text{es cerrado es} \quad X.$$

c) Sea $F \subset Y$, **cerrado**. Como Y es compacto, entonces F también es compacto.

Así que, por la parte b), $T^{-1}(F)$ es cerrado en X.

Queda, entonces, probado, que la imagen inversa de cada cerrado en Y, es un cerrado en X.

Es decir, T es continuo (léase, acotado).

d) Tenemos: $T^{-1} : Y \longrightarrow X$. Sea $F \subset X$, **cerrado**.

La compacidad de X implica que F también es compacto.

Para nuestro propósito, basta probar que

$$(T^{-1})^{-1}(F) \quad \text{es cerrado en} \quad Y;$$

O sea, que $T(F)$ es cerrado en Y; pero esto es, precisamente, lo que afirma la parte a). ∎

Bibliografía

[1] Trejo César A., El concepto de número, monografía nº 7, serie de matemática, Secretaría General de la O.E.A., 1973.

[2] A. Hefez, Elementos de Aritmética, Sociedad Brasileira de Matemática, Rio de Janeiro, 2005.

[3] Spivak Michael, Calculus, Volúmenes 1 y 2, Editorial Reverté, S.A., 1970.

[4] Lima, Elon Lages, Espacos Métricos, Projeto Euclides, Rio de Janeiro, 1977.

[5] Serge Lang, Cálculo, Volumen 2, Ao livro técnico S.A. Rio de Janeiro, 1974.

[6] Serge Lang, Analysis I, Addison-Wesley, Publishing Company, 1968.

[7] Bachman George-Narici Lawrence, Functional Analysis, Academic Press, 1966.

[8] F. Simmons George, Introduction to Topology and Modern Analysis, Mc Graw-Hill Book Company, INC., 1963

[9] Kreyszig, Erwin, Introductory Functional Analysis with Applications, John Wiley & sons,INC., 1978.

[10] T. M. Apostol, Análisis Matemático, Editorial Reverté, S.A.,1960.

[11] Kaplan Wilfred, Advanced Calculus, Addison-Wesley Publishing Company, 1969.

[12] Seymour Lipschutz, General Topology, Schaum Publishing Co., 1965.

[13] Hans Rademacher y Otto Toeplitz, Números y figuras, Ediciones Castilla, S.A., 1970

[14] John B. Fraleigh, A first course in abstract algebra, Addison-Wesley Publishing Company, 1976.

[15] Salahoddin Shokranian, Marcus Soares, Hermar Godinho, Teoría dos números, Editora Universidade de Brasilia, 1994.

[16] Howard Eves, Introducào à Historia da Matemática, Editora Universidade Estadual de Campinas, Brasil, 1995.