

¿POR QUÉ NUESTRO SISTEMA NUMÉRICO ES ÚNICO?

FERNANDO HERNÁNDEZ-HERNÁNDEZ

1. INTRODUCCIÓN

Corría el año de 1989 y después de sentir una decepción en la Escuela de Ingeniería Química conocí el primer teorema que literalmente cambiaría mi vida entera. Como muchos jóvenes, yo elegí la carrera de mi profesor más admirado para seguir sus pasos y hacer cosas como las que ella hacía. Sí, mi profesora de matemáticas era ingeniera química y por eso entré a la escuela de ingeniería química en la BUAP, buscando no aprender ingeniería química sino matemáticas. Mientras yo estudiaba cosas rutinarias de matemáticas, mis compañeros que sí habían ingresado a estudiar computación en la escuela de ciencias demostraban teoremas interesantes y se quebraban la cabeza para *demostrar* que $2 > 0$ usando los axiomas de los reales. Finalmente decidí ingresar a la escuela de ciencias y en mi primer semestre conocí uno de los resultados más fantásticos que he encontrado. De ese teorema trata esta nota.

Teorema 1.1. \mathbb{R} es el único (salvo isomorfismo) campo ordenado completo.

Se tratará de explicar qué quiere decir este teorema y cómo usarlo para hacer que nuestros estudiantes tengan un mejor aprovechamiento. Todo lo que aquí relataré puede consultarse con mayor profundidad en el libro de M. Spivak [Spi80] y mi libro de Teoría de Conjuntos [HH98].

2. EL GRAN TEOREMA

Primeramente debemos explicar qué entendemos por nuestro sistema numérico y cómo se relaciona eso con el teorema anterior.

Una idea intuitiva de lo que es nuestro sistema numérico creo que sí es clara: nuestro sistema numérico es el sistema de números que a diario usamos. Sin embargo, al pensar con más cuidado las cosas veremos que hay muchas más cosas detrás de las que uno imagina. Es decir, para que los números cotidianos funcionen como estamos acostumbrados a que funcionen, se requiere de

propiedades alejadas de la cotidianidad que son fundamentales para la existencia de números que sí surgen de manera cotidiana. Sólo por mencionar alguno con un bagaje histórico muy conocido, el número irracional $\sqrt{2}$. Sí, en efecto, la existencia de raíces cuadradas, algo muy cotidiano, requiere de propiedades fundamentales del sistema numérico.

Sigo hablando del sistema numérico y de sus propiedades pero aún no digo nada de qué estoy entendiendo por eso. Como dije antes, el sistema numérico primeramente lo encontramos de manera intuitiva a través de los números naturales, \mathbb{N} ; o sea, los números para contar. Los números enteros, \mathbb{Z} ; es decir, los naturales positivos y negativos incluyendo ahora al número cero, también pueden ser alcanzados de una manera más o menos intuitiva como soluciones a ecuaciones del estilo $x + m = n$; donde m y n son números naturales o el cero. Escolarmente mucho más difíciles pero totalmente intuitivos y de propiedades muy cotidianas siguen los números racionales; es decir, los números fraccionarios:

$$\mathbb{Q} = \{ m/n : m \in \mathbb{Z} \ \& \ n \in \mathbb{N} \}.$$

La intuición nos puede llevar hasta aquí. Obviamente conozco maneras “geométricas” de construir $\sqrt{2}$; pero todas esas formas no son realmente honestas. Pasar a los números irracionales no es una tarea fácil que pueda hacerse con un “dibujito”. En mi libro de Teoría de Conjuntos se presenta una construcción completa de los números reales, \mathbb{R} , nuestro sistema numérico partiendo de los números naturales y estos definidos en base a los Axiomas de Zermelo-Fraenkel, que están prácticamente aceptados de manera universal como una base para todas las matemáticas. Pero esa no es la manera común de llegar a los números reales pues requiere de mayor madurez matemática. Para los cursos básicos de cálculo y álgebra basta con definir de manera axiomática a los números reales.

Aquí es donde entra en juego el Teorema 1.1 pues este dice que no importa la manera en que uno defina a los números reales, ya sea por alguna extraña construcción o por una definición axiomática, si el sistema resultante tiene las propiedades fundamentales de ser un campo algebraico; o sea, un sistema que permita hacer álgebra de la manera acostumbrada con sumas y productos, que tenga una relación de orden que además de ordenar totalmente al conjunto sea compatible con la suma y el producto y que sea completo en el sentido de que el orden “no deja hoyos”; entonces el sistema debe ser único.

3. LOS AXIOMAS DE \mathbb{R}

La forma más económica de llegar al sistema de los números reales es por medio de axiomas. Los axiomas aseguran las mínimas propiedades fundamentales de los números reales y todas las otras propiedades pueden establecerse por deducción a partir de los axiomas. Primeramente tenemos a los Axiomas de Campo; estos axiomas dicen que hay un par de operaciones binarias definidas sobre el conjunto de los números reales \mathbb{R} .

Axioma 3.1. *Para cualesquiera números reales $a, b, c \in \mathbb{R}$ se tiene que $a + (b + c) = (a + b) + c$, es decir, que la suma es asociativa.*

Axioma 3.2. *Existe un número real que es neutro para la suma; o sea, existe $0 \in \mathbb{R}$ de modo que para cualquier $a \in \mathbb{R}$ se tiene que $a + 0 = a$.*

Axioma 3.3. *Cualquier número real $a \in \mathbb{R}$ tiene inverso aditivo $-a \in \mathbb{R}$; es decir, $a + (-a) = (-a) + a = 0$.*

Axioma 3.4. *La suma es conmutativa; o sea que $a + b = b + a$, para cualesquiera $a, b \in \mathbb{R}$.*

Axioma 3.5. *El producto es asociativo; o sea, para cualesquiera números reales, $a, b, c \in \mathbb{R}$ se tiene que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

Axioma 3.6. *También existe un número $1 \in \mathbb{R}$ que es diferente de 0 y que es identidad para el producto; o sea, $a \cdot 1 = 1 \cdot a = a$, para cualquier $a \in \mathbb{R}$.*

Axioma 3.7. *Existen inversos multiplicativos para todo $a \in \mathbb{R}$ con $a \neq 0$; es decir, existe $a^{-1} \in \mathbb{R}$ tal que $a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1$.*

Axioma 3.8. *El producto también es conmutativo; o sea, $a \cdot b = b \cdot a$, para cualesquiera $a, b \in \mathbb{R}$.*

Axioma 3.9. *El producto distribuye sobre la suma; es decir, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, para cualesquiera $a, b, c \in \mathbb{R}$.*

Por su parte, los axiomas de orden, tal como los axiomas de campo, parten de la existencia de un par de operaciones binarias. Los axiomas de orden suponen que existe un subconjunto distinguido de números reales que es nombrado el conjunto de los números positivos, $P \subseteq \mathbb{R}$. Las propiedades de este subconjunto son las siguientes:

Axioma 3.10. *Para cualquier número $a \in \mathbb{R}$ una y sólo una de las siguientes propiedades se cumple: $a \in P$, $-a \in P$ o $a = 0$.*

Axioma 3.11. *Si $a, b \in P$, entonces $a + b \in P$.*

Axioma 3.12. *Si $a, b \in P$, entonces $a \cdot b \in P$.*

Es sin duda una forma extraña de definir el orden sobre los números reales. Se define entonces para $a, b \in \mathbb{R}$ que $a < b$ si y sólo si $b + (-a) \in P$ y también el acostumbrado $a \leq b$ si y sólo si $a < b$ o $a = b$. Se invita al lector a reflexionar el por qué de esta manera de hacer las cosas.

Por último, el Axioma del Supremo es el que realmente hace que los reales sean únicos. Desafortunadamente este axioma no es tan natural como los otros. Para establecerlo, primero recuerde que un subconjunto A de \mathbb{R} se llama *acotado superiormente* si existe algún número real z de modo que $a \leq z$, para todo $a \in A$. A uno de tales números z se les llama *cota superior* de A . No hay que perder de vista que por extraño que parezca, el conjunto vacío, \emptyset , sí es un conjunto acotado. El *supremo* de un conjunto acotado superiormente $B \subseteq \mathbb{R}$ es la mínima de sus cotas superiores; es decir, x es el supremo de B si x es cota superior de B y ningún $y < x$ es una cota superior de B . Puede mostrarse sin dificultad que el supremo de un conjunto, de existir, es único; por ello, de existir, se denota $\sup B$ al supremo del conjunto B .

Axioma 3.13. *Todo subconjunto A de números reales que no sea vacío y que esté acotado superiormente tiene supremo.*

Este extraño axioma es el que hace que nuestro sistema numérico sea único. Es decir, si existen dos sistemas numéricos en los que se satisfacen cada uno de estos axiomas; entonces, salvo los nombres de los objetos ambos sistemas funcionan de manera idéntica; es decir, hay un mecanismo para pasar de un sistema en el otro sin perder información alguna. Esto es muy importante porque como ya hemos dicho antes, hay varias maneras de construir a los números reales; tales métodos de construcción no está entre los objetivos de esta nota pues se requiere de mucha más teoría para entender correctamente lo que se hace. El lector interesado en esa parte puede consultar mi libro de Teoría de Conjuntos [HH98] o el libro de Rudin [Rud53] o diversos otros que hacen construcciones del sistema de los números reales. Por el momento, para nosotros bastará con suponer que existe al menos un sistema numérico que satisface los axiomas que hemos dado antes y esbozaremos someramente por qué otro sistema con las mismas propiedades debe ser idéntico, salvo los nombres de los objetos. Esto también puede y debe ser formalizado.

Definición 3.14. Un campo ordenado será un conjunto K con dos operaciones binarias definidas sobre sus elementos y que satisface cada uno de los axiomas antes enunciados para el caso específico de \mathbb{R} , excepto posiblemente el Axioma del Supremo. Si K también satisface el Axioma del Supremo, entonces se le llama campo ordenado completo.

Por ejemplo, los números racionales \mathbb{Q} y el conjunto $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ con las operaciones que heredan de los números reales son campos ordenados que no son isomorfos. Se reta al lector a establecer la veracidad de esta afirmación.

Definición 3.15. Dos campos ordenados K_0 y K_1 son isomorfos si existe una función $f : K_0 \rightarrow K_1$ tal que:

- (1) Si $x, y \in K_0$ y $x \neq y$, entonces $f(x) \neq f(y)$,
- (2) Si $z \in K_1$, entonces hay un $x \in K_0$ de modo que $f(x) = z$,
- (3) Para cualesquiera $x, y \in K_0$ se tiene que $f(x + y) = f(x) + f(y)$,
- (4) Para cualesquiera $x, y \in K_0$ se tiene que $f(x \cdot y) = f(x) \cdot f(y)$,
- (5) Para cualesquiera $x, y \in K_0$ se tiene que

$$x < y \Rightarrow f(x) < f(y).$$

Obviamente en esta definición se están usando los mismos símbolos para la suma, el producto y el orden en cada campo; pero debe quedar claro que formalmente son operaciones diferentes en cada campo y, por ejemplo, el tercer elemento de la definición dice que la función f respeta la suma; o sea, que el valor que corresponde a la suma de dos elementos del campo K_0 es enviado bajo f a la suma en el campo K_1 e los respectivos valores. Recuerde también que las partes (1) y (2) de esta definición dice que la función es biyectiva; es decir, inyectiva que es lo que dice (1) y sobreyectiva que es lo que dice (2).

4. EL TEOREMA, UN ESBOZO DE LA DEMOSTRACIÓN

Con la terminología que ya hemos introducido, el teorema principal puede ahora replantearse como sigue.

Teorema 4.1. Si F es un campo ordenado completo, entonces \mathbb{R} y F son isomorfos.

Veamos las ideas centrales de la construcción del isomorfismo. Denotaremos por $\mathbf{0}$, $\mathbf{1}$, etc. a importantes elementos del campo F . La construcción de un isomorfismo $f : \mathbb{R} \rightarrow F$ se hace por pasos definiendo f primero sobre \mathbb{Z} , \mathbb{Q} y finalmente sobre todo \mathbb{R} .

Evidentemente, todo isomorfismo f deberá satisfacer:

$$f(0) = \mathbf{0} \quad \text{y} \quad f(1) = \mathbf{1}.$$

Luego es fácil hacer:

$$f(n) = \underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n \text{ veces}}$$

para $n \in \mathbb{Z}$ y $n > 0$ y

$$f(n) = -\underbrace{(\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1})}_{|n| \text{ veces}}$$

para $n \in \mathbb{Z}$ y $n < 0$. Entonces se verifica con facilidad que

$$f(m+n) = f(m) + f(n), \quad f(m \cdot n) = f(m) \cdot f(n)$$

para todo $m, n \in \mathbb{Z}$.

Denotemos, convenientemente ahora $\mathbf{n} = f(n)$, para cada $n \in \mathbb{Z}$. Para los racionales extendamos la definición de f haciendo

$$f(m/n) = \mathbf{m}/\mathbf{n}.$$

Otra vez es fácil de verificar que

$$f(r_1 + r_2) = f(r_1) + f(r_2), \quad f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2).$$

Además, para números racionales r_1 y r_2 ,

$$r_1 < r_2 \quad \Rightarrow \quad f(r_1) < f(r_2).$$

Antes de pasar a la definición completa de f hagamos dos observaciones cruciales.

- El conjunto $\{\mathbf{n} \in F : n \in \mathbb{N}\}$ debe ser no acotado en F ,
- Dados $a, b \in F$ con $a < b$, debe haber un número racional $r \in \mathbb{Q}$ tal que

$$a < f(r) < b.$$

Las demostraciones de estos dos hechos son idénticas a las similares para los números reales y pienso que es un buen ejercicio para el lector realizarlas por cuenta propia. El primer hecho realmente dice que los “naturales” del campo F son como los naturales reales, no acotados. Por otro lado, el segundo hecho dice que los “rationales” de F también son densos. Recuerde que la densidad de \mathbb{Q} ; o sea, que entre dos reales cualesquiera siempre hay racionales, se basa en que los números naturales no son acotados superiormente y de ahí se obtiene la famosa Propiedad Arquimediana; con ella establecer la densidad de \mathbb{Q} ya es una tarea no tan difícil.

Ahora, para un $x \in \mathbb{R}$ arbitrario considere el conjunto

$$A_x = \{ f(r) : r \in \mathbb{Q} \ \& \ r < x \}.$$

Este conjunto no debe ser vacío y debe estar acotado superiormente en F . Entonces definimos

$$f(x) = \sup A_x.$$

Claro que esto es posible porque estamos suponiendo que F es un campo ordenado completo; o sea, que conjuntos no vacíos y acotados superiormente tienen supremo.

¿Será cierto que

$$f(m/n) = m/n = \sup A_r = f(r)$$

si $r = m/n$? Si $s \in \mathbb{Q}$ es tal que $s < r$, entonces $f(s) \in A_r$ y así $\sup A_r \leq m/n$. Si ocurriera que $\sup A_r < f(r)$, podemos hallar $t \in \mathbb{Q}$ tal que

$$\sup A_r < f(t) < m/n;$$

pero entonces $f(t) \in A_r$ que es una contradicción. Por lo tanto, $\sup A_r = m/n$. Una consecuencia de esto es que $f : \mathbb{R} \rightarrow F$ está bien definida.

Ahora debemos verificar que f satisface todas las propiedades para ser el isomorfismo buscado. Primeramente si $x, y \in \mathbb{R}$ y $x < y$ se tiene que $A_x \subseteq A_y$ y consecuentemente $f(x) \leq f(y)$. Pero no pueden ser iguales, porque existen racionales r y s que satisfacen

$$x < r < s < y$$

y entonces

$$f(x) \leq f(r) < f(s) \leq f(y).$$

De lo anterior se sigue que f es inyectiva. Veamos que es también sobreyectiva. Fijemos $a \in F$. Sea

$$B = \{ r \in \mathbb{Q} : f(r) < a \}.$$

Entonces $B \neq \emptyset$ y B está acotado superiormente en \mathbb{R} . Sea $x = \sup B$. Es posible verificar que $f(x) < a$ y que $f(x) > a$ son ambas imposibles. Consecuentemente $f(x) = a$.

Para verificar que f preserve la suma, sean $x, y \in \mathbb{R}$. Supóngase por un momento que $f(x+y) < f(x) + f(y)$. Es posible hallar un $r \in \mathbb{Q}$ tal que $f(x+y) < f(r) < f(x) + f(y)$. Ahora también se pueden hallar $r_1, r_2 \in \mathbb{Q}$ tales que

$$r = r_1 + r_2 \quad x < r_1 \quad \text{y} \quad y < r_2.$$

Entonces

$$f(r) = f(r_1 + r_2) = f(r_1) + f(r_2) > f(x) + f(y),$$

una contradicción ya que f sí respeta las sumas de racionales. Por eso la desigualdad $f(x+y) < f(x)+f(y)$ es imposible. Del mismo modo lo es la desigualdad $f(x+y) > f(x)+f(y)$. Por lo tanto, la única posibilidad es $f(x+y) = f(x)+f(y)$. Análogamente se demuestra que $f(x \cdot y) = f(x) \cdot f(y)$.

Ahora la pregunta es: ¿Por qué tuvimos éxito? En otras palabras: ¿Qué es lo que hace que la demostración funcione?

5. ¿QUÉ HACE A \mathbb{R} ÚNICO?

¿Será acaso el álgebra lo que hace a \mathbb{R} único? ¿Qué quiere decir esto? ¿Serán los axiomas de orden para \mathbb{R} ? No, las dos piezas fundamentales de la demostración sí tienen que ver con el orden pero no son sólo los axiomas de orden.

- La completez de \mathbb{R} fue fundamental,
- La densidad de \mathbb{Q} en \mathbb{R} es incluso más importante.

Alrededor de 1920, Mikhail Yakovlevich Souslin se preguntó si era posible debilitar la densidad de \mathbb{Q} y seguir teniendo la unicidad de \mathbb{R} . La idea de Souslin fue como sigue:

Cada vez que damos una colección infinita de intervalos abiertos en los reales, es fácil observar que no hay más intervalos que números racionales. ¿Por qué?

A los conjuntos que tienen la misma cantidad de elementos que \mathbb{Q} se les llama *numerables*. Entonces el cuestionamiento de Souslin, que después se conoció como *el problema de Souslin*, dice:

Problema 5.1 (Souslin). *Supóngase que (X, \leq) es un conjunto totalmente ordenado y completo en el que toda colección de intervalos abiertos y ajenos por pares es a lo más numerable. ¿Es X isomorfo (como orden) a \mathbb{R} ?*

Para el tiempo en que el joven Souslin planteaba su problema ya era conocido un resultado fundamental del G. Cantor que estableció unos 15 años antes.

Teorema 5.2. *Cualesquiera dos órdenes totales y numerables, sin puntos finales y densos en sí mismos son isomorfos.*

Un orden total (X, \leq) es *denso en sí mismo* si para cualesquiera $x, y \in X$ existe $z \in X$ tal que $x < z < y$. Obsérvese que así son los racionales.

Es posible establecer que \mathbb{Q} es único como conjunto ordenado con las propiedades que ya le conocemos a \mathbb{Q} . La idea es más fácil dibujarla que escribirla; espero que en la charla esta parte quede clara, aquí no voy a abordarla por el momento, simplemente asumiremos el siguiente resultado.

Teorema 5.3. *Salvo isomorfismo, \mathbb{Q} es el único orden numerable, sin puntos finales y denso en sí mismo.*

Otro resultado que por el espacio aquí y las dificultades técnicas ya no me es posible abordar con calma es el siguiente.

Teorema 5.4. *\mathbb{R} puede verse como la completación (en términos de orden) de \mathbb{Q} ; por eso es único.*

La conjunción de los dos resultados anteriores puede escribirse de la siguiente manera.

Teorema 5.5. *\mathbb{R} es el único conjunto ordenado que tiene un conjunto numerable que es denso en \mathbb{R} , que no tiene puntos finales y que es completo.*

Ya a la luz de estos resultados podemos hacer una precisión en el problema de Souslin.

Problema 5.6 (Souslin). *Supóngase que (X, \leq) es un conjunto totalmente ordenado y completo en el que toda colección de intervalos abiertos y ajenos por pares es a lo más numerable. ¿Es X isomorfo (como orden) a \mathbb{R} ?*

Dado que el problema no fue resuelto por los matemáticos de la época, poco a poco fue cobrando importancia y de hecho se llegó a formular el concepto de línea de Souslin.

Definición 5.7. *Una línea de Souslin es un conjunto totalmente ordenado, completo, sin puntos finales, en el que toda familia de intervalos abiertos y ajenos por pares es a lo más numerable pero que no es isomorfo a \mathbb{R} .*

Así, una forma más concreta del mismo problema de Souslin es:

Problema 5.8 (Souslin). *¿Existen las líneas de Souslin?*

Ya se mencionó anteriormente, que es un problema que apareció en los años 20's del siglo pasado. En Jech en 1967 y Tennenbaum en 1968 publicaron artículos donde se establecía que las líneas de Souslin existen en ciertos modelos de la teoría de conjuntos. En 1971, Solovay y

Tennenbaum mostraron que no es posible establecer con la axiomática usual la existencia de líneas de Souslin. En 1972, Jensen demuestra que las líneas de Souslin existen en el modelo de los conjuntos construibles de Gödel.

En resumen, los reales \mathbb{R} están hechos a la perfección pues rebajar un poquito una de sus propiedades conduce a la insertidumbre de las líneas de Souslin cuya existencia no es posible demostrar pero tampoco es posible demostrar su inexistencia, en base a la axiomática usual de las matemáticas contemporáneas.

REFERENCES

- [HH98] Fernando Hernández Hernández. *Teoría de conjuntos*, volume 13 of *Aportaciones Matemáticas: Textos [Mathematical Contributions: Texts]*. Sociedad Matemática Mexicana, México, 1998.
- [Rud53] Walter Rudin. *Principles of mathematical analysis*. McGraw-Hill Book Company, Inc., New York-Toronto-London, 1953.
- [Spi80] Michael Spivak. *Calculus. 2nd ed.* Berkeley, California: Publish Perish, Inc. XIII, 647 p. , 1980.

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS, UNIV. MICHOACANA DE SAN NICOLÁS DE HIDALGO, MORELIA MICHOACÁN, MÉXICO, 58060.

E-mail address: `fhernandez@fismat.umich.mx`