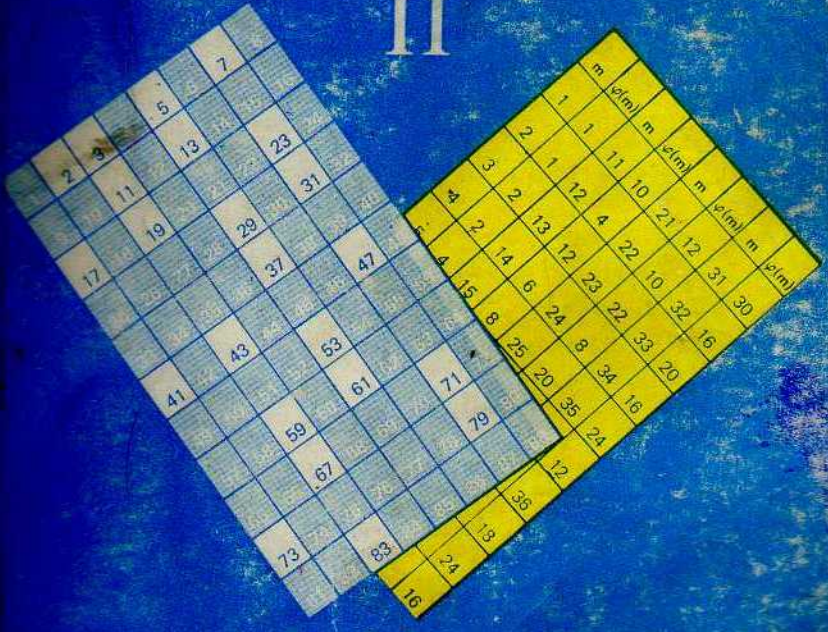
ALAMIRO ROBLEDO H.

LECCIONES DE ARITMETICA ELEMENTAL MODERNA

II



UNIVERSIDAD DE CONCEPCION
(CHILE)

LECCIONES DE ARITMETICA ELEMENTAL MODERNA

ALAMIRO ROBLEDO H.
Profesor Titular del Instituto de Matemática
Universidad de Concepción (Chile)

TOMO II

Santiago de Chile, 1977

EDITORIAL UNIVERSITARIA
San Francisco 454 - Casilla 10220
Santiago - Chile

INDICE GENERAL DEL TOMO II

Capítulo IX

El Número Entero

Capítulo X

El Número Racional

Capítulo XI

El Número Real

Capítulo XII

El Número Complejo

BIBLIOGRAFIA

1. *Topics in Number Theory* (Vol. II). William J. Le Veque.
2. *The Number - System*. H. A. Thurston.
3. *Lecciones de Algebra Elemental Moderna* (Vol. III). A. Robledo H.
4. *El Número Natural y sus Generalizaciones*. M. Balanzat.
5. *Lecciones de Algebra Moderna*. Alberto E. Sagastume B.
6. *Instroducción a la Teoría de los Números reales y naturales*. Héctor Merklen.
7. *Algebra Moderna*. Frank Ayres.
8. *The Theory of Algebraic Numbers*. Harry Pollard.
9. *Irrational Numbers*. Iván Niven.

PROLOGO

El propósito de haber escrito este segundo tomo de mi libro LECCIONES DE ARITMETICA ELEMENTAL MODERNA y que los alumnos del curso de Enseñanza Media en Matemática y Física de nuestra Universidad tienen que usar como Texto Guía en el cuarto semestre de sus estudios, ha sido principalmente el de proporcionarles un texto moderno de aquellos tópicos que son necesarios en Matemática para facilitar el paso al álgebra, la geometría, al cálculo, y, en general, para poner al estudiante en contacto con el modo de razonar y operar de la *Matemática Actual*, que posteriormente les permitirá adquirir nuevas nociones teóricas y nuevos métodos matemáticos, auxiliares indispensables en la creación científica.

Por esto, este segundo tomo del libro es de método netamente axiomático en su desarrollo, porque ya se cuenta con la suficiente madurez adquirida por el alumno al estudiar las lecciones contenidas en el primer tomo del libro.

Por consiguiente, el lenguaje de conjuntos, el concepto de relaciones, el concepto de operación binaria interna y el concepto de estructuras algebraicas, constituirán el lenguaje necesario mínimo para poder desarrollar cómodamente, por medio del método genético, la construcción de todos los sistemas numéricos usuales de que trata este segundo tomo.

Estos sistemas numéricos a que nos referimos son: los números naturales, los números enteros, los números racionales, los números reales y los números complejos, los cuales constituyen, como sabemos, el escenario en que se cultivan las matemáticas clásicas.

Bajo el concepto moderno de Matemática, esto es, como un sistema formal de tipo convencional, es decir hipotético-deductivo, este segundo tomo de la obra será de corte formalista, o lo que es lo mismo, logístico y axiomático, en su desarrollo.

Pues bien, partiendo de la axiomática de Peano que define al NUMERO NATURAL, se establecen los conceptos de igualdad y desigualdad con esta clase de números; se definen después todas las operaciones que con ellos pueden efectuarse, estableciendo y demostrando las leyes formales de cada operación inductivamente. Por tanto, el método demostrativo de la Inducción Matemática desempeña aquí, en esta teoría de Peano, un papel preponderante.

Ahora bien, si quisiéramos agregar a esto todo lo estudiado en el tomo primero, el alumno habría construido, partiendo de conceptos muy simples, lo que pudiéramos llamar *Aritmética del Número Natural*. Pero, en esta aritmética, debido al restringido concepto del número, se

hacen imposibles varias operaciones, cuando los datos no cumplen determinadas condiciones.

A fin de hacer posibles algunas de estas operaciones, se amplía, mediante el método genético, el concepto restringido del llamado número natural, ideando o inventando otros entes abstractos denominados números enteros y números fraccionarios o razones de enteros, y el conjunto de éstos y de los números del sistema primitivo del cual derivan, constituyen sucesivamente los sistemas de los NUMEROS ENTEROS y de los NUMEROS RACIONALES.

De esta manera se desarrolla la parte que pudiéramos llamar, *Aritmética del Número Entero* y *Aritmética del Número Racional.*

Dentro del campo de los números racionales quedan todavía operaciones y problemas que siguen imposibles, y para evitar estas imposibilidades, nuevamente por medio del método genético vuelve a ampliarse el concepto de número, ideando o inventando otros entes abstractos, denominados números irracionales, que en unión de los racionales constituyen el sistema de los NUMEROS REALES, y así sucesivamente se va ampliando, siempre por medio del método genético, el concepto de número, hasta llegar al sistema de los NUMEROS COMPLEJOS.

De esta manera se desarrolla la parte que pudiéramos llamar *Aritmética del Número Real* y *Aritmética del Número Complejo,* que utilizan las ciencias aplicadas basadas en la matemática pura.

Con respecto a estas adjunciones o creaciones, se enfatiza haciendo ver que los nuevos números que se introducen se constuyen libremente, o sea que se inventan, es decir, surgen como el resultado de un acto de creación matemática y que para ello sólo es necesario definir de manera no contradictoria la igualdad de dos de estos entes nuevos, como también las reglas operatorias que ellos verifican.

Desde el punto de vista aritmético, no es necesario una nueva ampliación del campo de los números, pues, en el sistema de los números complejos quedan resueltos todos los problemas aritméticos elementales, como son: adición, sustracción, multiplicación, división, potenciación, radicación, potencias de base e y logaritmos neperianos, y también sucesiones y series de términos complejos.

Pero, si se intentara una nueva ampliación del sistema de los números complejos, introduciendo los números hipercomplejos o complejos de orden superior, ya dejarían de cumplirse algunas de las propiedades formales de las operaciones, por ejemplo, ya no se cumpliría la propiedad conmutativa del producto. Por consiguiente, no existe ningún sistema de números complejos de más de dos unidades, la real 1 y la imaginaria i, que satisfaga a todas las leyes formales de la Aritmética y para el cual el producto de dos factores no nulos, no sea nulo. Por lo tanto, podemos decir que la ARITMETICA construida siguiendo el PRINCIPIO DE PERMANENCIA DE LAS LEYES FORMALES, termina con el estudio de los números complejos ordinarios o a dos unidades: la real (1, 0) y la imaginaria (0, 1).

Ya no es posible continuar la serie de ampliaciones:

$$\mathbb{N} \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{R} \rightarrow \mathbb{C}$$

del concepto de número, llegando a su término natural el desarrollo de la ARITMETICA.

En resumen, mediante la formulación de definiciones precisas y de simple pero de exacta presentación de las ideas fundamentales, ARITMETICA ELEMENTAL MODERNA expone, en ambos tomos de que se compone el libro, los conceptos difíciles de la aritmética moderna, haciéndolos accesibles a los futuros profesores de la asignatura y en ejercicio de su profesión.

Por tratarse de un texto destinado a la enseñanza, esto es, que no aspira a la novedad, la exposición de los diversos temas en él contenidos se desarrolla mediante explicaciones lentas y cuidadosas, como resultado de una elaboración condicionada por la experiencia pedagógica de varios lustros del autor. En realidad, en ambos tomos, nos hemos guiado por el sentimiento de que es mejor pecar por mucha explicación, que pecar por poca explicación.

El libro completo, tomos I y II, es el resultado de un esfuerzo para exponer la materia de tal forma que sea accesible a personas con menor preparación matemática que la que necesitaría para leer normalmente algún tratado sobre Teoría de los Números.

Por otra parte, al escribir estos libros, el autor tenía en mente sobre todo a aquellos temas que el Ministerio de Educación Nacional tiene planeado enseñar en las Escuelas Básicas y Medias.

Y esta es la razón del porqué nuestros alumnos necesitan una discusión completa del SISTEMA NUMERICO que, después de todo, forma las bases del Algebra, así como las manipulaciones de los mismos números.

La teoría de los números contiene multitud de hechos interesantes, que pueden usarse para dar más vida y esclarecer la enseñanza elemental de la Matemática en nuestros liceos y universidades.

El estudioso que sobresalga del nivel medio y tenga curiosidad por ahondar algunos puntos interesantes, encontrará en la bibliografía

indicada al final de cada uno de los tomos de que se compone la obra, los complementos apropiados para satisfacer tal curiosidad, ampliando los conceptos contenidos en este libro elemental.

Ciertos conceptos no se comprenden hasta después de varias lecturas y numerosas horas de reflexión. Este es un fenómeno natural que no debe provocar ningún desaliento. Este esfuerzo continuo en la práctica del ejercicio, en la reflexión teórica, conducirá lentamente, por adquisiciones sucesivas, a una visión sintética que es la finalidad de toda formación intelectual.

En resumen, y tal como lo hice al finalizar el prólogo de mi primer tomo, me dirijo nuevamente a los alumnos, diciéndoles ahora:

1° Que los estudiantes sepan que los grandes matemáticos han desempeñado un papel en la evolución del pensamiento científico y filosófico, comparable al de los filósofos y hombres de ciencia. Es por eso que en sus obras, todas avaladas por sólidos conocimientos, es difícil separar las fronteras de la investigación pura y de la imaginación exuberante;

2° Que los estudiantes sepan que no deberán creer que la única función de la Matemática —"la sirvienta de las ciencias"— es servir a la ciencia.

En efecto, la Matemática, que también ha sido denominada "la reina de las ciencias", y si alguna vez la reina ha parecido mendigar de las otras ciencias, ha mendigado en forma muy orgullosa, ni ha pedido ni ha aceptado favores de ninguna de sus ciencias hermanas más influyentes. Lo que ella adquiere, ella lo paga; y por último,

3° Que los estudiantes sepan que los matemáticos tienen una visión y una sabiduría particular, por encima de cualquier aplicación posible a la ciencia, y suficientemente premiada cuando cualquier ser humano inteligente llega a vislumbrar lo que la Matemática significa por sí misma.

No se trata de la vieja doctrina del arte por el bien del arte, sino del arte por el bien de la humanidad.

En realidad, el propósito de la ciencia no es la tecnología. La ciencia explora también profundidades de un Universo que ni siquiera con la imaginación será visitado por los seres humanos, ni afectará nuestra existencia material, y que los matemáticos han considerado dignas de una cordial comprensión por su belleza intrínseca.

Por último, nos resta ahora expresar nuestros más sinceros agradecimientos a todos los que cooperaron en una u otra forma en la publicación de este libro, y entre los cuales mencionamos al señor Director del Area de Ciencias Física, Química y Matemática de nuestra Universidad, profesor señor don Renato Becker; a la Honorable Comisión renovadora de los planes y programas de estudio del curso de profesores de Matemática y Física, presidida por el profesor señor Antonio Camurri; a la señorita Gricelda Gallegos, Jefe del Departamento de Matemática Pura de nuestro Instituto, y a la señorita Verónica Contreras que tuvo a su cargo la tarea de mecanografiar el manuscrito y también al personal de la empresa editora, por su vigilancia durante el proceso de la impresión del libro.

Finalmente, nuestros más cálidos agradecimientos a la Universidad de Concepción, por su respaldo, que ha hecho posible la publicación del presente libro.

Prof. ALAMIRO ROBLEDO HERRERA

CONCEPCION, Ciudad Universitaria, diciembre de 1976.

OTRAS GENERALIDADES SOBRE LOS CONJUNTOS

1. En esta introducción expondremos las nociones y las notaciones fundamentales que se emplearán a lo largo del presente libro.

Esperamos que el estudiante no tenga dificultad alguna en lo que concierne a los conceptos fundamentales y al sentido de ciertas palabras, como ser: aplicación, operación, equivalencia regular, isomorfismo, homomorfismo,... que constituyen el lenguaje necesario mínimo a esta altura de nuestros estudios de Aritmética Elemental Moderna.

2. Sea X un conjunto que llamaremos *conjunto de definición* y sea Y otro conjunto, que eventualmente podría coincidir con X, que llamaremos *conjunto de valores.*

Definición. Una correspondencia tal que todo elemento $x \in X$ asocia un elemento y uno sólo $y \in Y$, será llamado una FUNCION o APLICACION de X dentro de Y.

Se la representa por una letra f, y si $x \in X$ corresponde $y \in Y$, se escribe

$$y = f(x)$$

decimos que y es la imagen de x mediante f.

Es claro que en el caso en que X e Y denotan conjuntos de números reales, el segundo miembro de esta última igualdad describe la gráfica de la función en el sentido usual de la palabra.

No afirmamos en la definición que se acaba de dar que los valores de la función agoten totalmente el conjunto Y. Pero cuando esta condición se cumpla, diremos que la función f es una aplicación de X sobre Y.

En caso contrario, f será una aplicación de X en Y.

El concepto de función que acabamos de dar es un caso particular del concepto de relación en el sentido de la teoría de conjuntos.

Precisamente, función significa, en este sentido, un subconjunto f del producto cartesiano $X \times Y$ con la propiedad de que para cada $x \in X$ existe un elemento $y \in Y$, y sólo uno, tal que $(x,y) \in f$.

En resumen, llamaremos función o aplicación del conjunto X dentro del conjunto Y, a toda relación f de $X \times Y$ que cumple las dos condiciones siguientes:

a) *Existencia.* Para cada elemento $x \in X$, existe un elemento $y \in Y$ tal que $(x, y) \in f$.

b) *Unicidad.* $(x, y) \in f \wedge (x, z) \in f \Rightarrow y = z$.

El conjunto de partida X es el DOMINIO de la función f, y el conjunto de llegada Y es el CONTRADOMINIO de f.

El conjunto formado por los valores de f, es decir, el conjunto de los elementos f(x) para cada $x \in X$, será llamado el RECORRIDO de la función f, y se denotará por el símbolo f(X). Luego,

$$f(X) = \{y \in Y : x \in X \text{ tal que } f(x) = y\}$$

La función f misma suele representarse simbólicamente así:

$$f : X \longrightarrow Y$$

o también,

$$X \xrightarrow{f} Y$$

para poner en evidencia donde actúa f.

Definición. Dos funciones,

$$f : X \longrightarrow Y$$
$$g : X \longrightarrow Y$$

son iguales, y lo que se escribe

$$f = g$$

si, y sólo si $f(x) = g(x)$, $\forall x \in X$.

Definición. Una función,

$$f : X \longrightarrow Y$$

se dirá *inyectiva* si,

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

o equivalentemente,

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Definición. Una función,

$$f : X \Longrightarrow Y$$

se llamará *biyectiva* si se verifica:

i) $f(X) = Y$

ii) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

esto es, si f es sobreyectiva e inyectiva a la vez.

En este caso decimos que los conjuntos X e Y, dominio y recorrido de f, están en correspondencia biunívoca o que son coordinables.

En otras palabras, dos conjuntos X e Y son coordinables cuando entre sus elementos se puede establecer, mediante una ley adecuada, una correspondencia biunívoca; es decir, que la ley permita definir para cada elemento de X un elemento de Y y sólo uno y, recíprocamente, dado un elemento de Y, él proviene de un solo elemento de X.

Por consiguiente, cuando una función

$$f : X \longrightarrow Y$$

es biyectiva, entonces queda definida automáticamente una función

$$g : Y \text{ en } X$$

que se llama la inversa de f, y se denota por f^{-1}. Luego, si $f : X \longrightarrow Y$ es biyectiva, entonces existe la función $f^{-1} : Y \longrightarrow X$.

3. Sean las funciones siguientes:

$$f : X \longrightarrow Y$$
$$g : Y \longrightarrow Z$$

tales que $f(X) \subset Y$.

Entonces, se puede deducir una tercera función o aplicación

$$h : X \longrightarrow Z$$

haciendo $h(x) = g(f(x)), \forall x \in X$.

Es decir, la nueva función es el conjunto de los pares (x, z) que tienen la propiedad siguiente:

Para cada $x \in X$ existe al menos un $y \in Y$ tal que

$$(x, y) \in f, \quad (y, z) \in g$$

La aplicación así definida h se designa por la notación

$$h = g \circ f$$

y se llamará la aplicación compuesta o el producto de las aplicaciones f y g, en este orden. Luego,

$$h = g \circ f = \{(x,z) : \exists\ y \in Y \text{ tal que } y = f(x), z = g(y)\}$$
$$= \{(x,z) : \exists\ y \in Y \text{ tal que } z = g(f(x))\}$$

Entonces, por definición se tendrá:

$$h(x) = (g \circ f)(x) = g(f(x))$$

La aplicación compuesta g o f no está definida más que cuando el conjunto de llegada de f es idéntico al conjunto de partida de g.

En general, g o f es diferente de f o g, pudiendo no tener sentido este último símbolo.

Esto es, la operación "o" que, partiendo de las funciones f y g, permite definir la función compuesta g o f no es pues, en general, conmutativa; pero en cambio, es siempre asociativa.

Por último, la compuesta de funciones sobreyectivas, inyectivas y biyectivas, es también sobreyectiva, inyectiva y biyectiva, respectivamente.

4. Si E es un conjunto no vacío, entonces una aplicación de E x E dentro de E será llamada una OPERACION BINARIA INTERNA en el conjunto E. Luego,

Definición. Una operación binaria interna sobre un conjunto no vacío E, es una función de $E \times E$ dentro de E; es decir, es una aplicación que a cada par ordenado (a, b) de elementos de E le hace corresponder un elemento y uno solo $c \in E$.

Se acostumbra representar dicha función con el símbolo "o"; entonces, para indicar que c es el elemento que corresponde al par (a, b), se escribe,

$$a \circ b = c$$

y decimos que c es el resultado de *a* operado con *b*.

De la definición resulta que cualquier operación binaria interna definida sobre un conjunto E, verifica las dos propiedades siguientes:

a) Cualesquiera sean $a, b \in E$, entonces $a \circ b \in E$.

Para expresar esta propiedad, decimos que E es *cerrado* con respecto a esa operación, o bien que la operación "o" es *cerrada* en el conjunto E.

b) Si $a = a'$, $b = b'$, entonces $a \circ b = a' \circ b'$.

En efecto, si $a = a'$, $b = b'$, entonces los pares ordenados (a,b) y (a', b') son iguales, y como la operación binaria interna "o" es una función de $E \times E$ dentro de E, entonces las imagenes de (a, b) y (a', b') son iguales, es decir, $a \circ b = a' \circ b'$.

Para expresar esta propiedad, decimos que la operación es *uniforme*.

La propiedad a) es la condición de *existencia* y la b) es la condición de *unicidad* de la operación en cuestión.

Una operación se llama asociativa si cualesquiera que sean $a, b, c \in E$ se verifica la identidad

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Una operación se dirá conmutativa si cualesquiera que sean $a, b \in E$ se cumple la identidad

$$a \circ b = b \circ a$$

Si "o" y "$*$" son dos operaciones definidas sobre un mismo conjunto E, entonces diremos que, por ejemplo, la operación "o" es distributiva respecto a la operación "$*$", si se cumplen las identidades

$$a \circ (b * c) = (a \circ b) * (a \circ c)$$

$$(b * c) \circ a = (b \circ a) * (c \circ a)$$

cualesquiera que sean $a, b, c \in E$.

Un conjunto E, en el que están definidas una o más operaciones binarias internas, se dirá que es un conjunto algebrizado.

Elementos especiales. Un elemento particular $e \in E$ se llamará *neutro* o *unidad* para la composición "o", si se verifica

$$e \circ a = a \circ e = a$$

cualquiera que sea $a \in E$.

Este elemento puede existir o no, pero cuando existe es único.

En una operación con elemento unidad, un elemento $b \in E$ se llamará *inverso* o *simétrico* de un elemento $a \in E$, si se cumple,

$$b \circ a = a \circ b = e$$

El elemento neutro o unidad es siempre simétrico de sí mismo. Puede suceder que el único elemento que tenga simétrico sea el neutro; tal es el caso de la multiplicación de números naturales.

5. *Equivalencias Regulares y Ley Inducida.* Consideremos un conjunto E provisto simultáneamente de una relación de equivalencia y de una ley de composición interna.

Definición. Diremos que la equivalencia "$\sim$" es regular o compatible con la ley "o" si,

$$a \sim a' \ y \ b \sim b' \Rightarrow a \circ b \sim a' \circ b'$$

es decir, si el compuesto de dos elementos cualesquiera a y b se cambia en uno equivalente cuando se reemplazan a y b por elementos equivalentes a ellos.

Consideremos ahora el conjunto cociente $Q = E/\sim$ cuando "$\sim$" es una equivalencia regular. Podemos entonces definir una operación en Q, a partir de la operación definida en E, de la manera siguiente: sean

C_a y C_b dos clases de equivalencia cualesquiera de Q, y mostraremos que se les puede asociar una clase de equivalencia bien determina de Q. En efecto, como C_a y C_b son subconjuntos de E, tomemos $a \in C_a$ y $b \in C_b$, y consideremos el elemento $c = a \circ b$.

Entonces, definiremos el compuesto $C_a \bar{\circ} C_b$ como el elemento C_c de Q que contiene $c = a \circ b$, es decir,

$$C_a \bar{\circ} C_b = C_{a \circ b}$$

Ahora bien, para ver que esta operación está bien definida hay que ver que a cada par de clases le corresponde una y una sola como producto, y para ello bastará hacer ver que C_c es independiente de la elección de a en C_a y de b en C_b.

En efecto, tenemos otros dos elementos $a' \in C_a$ y $b' \in C_b$; entonces tendremos

$$a \sim a' \text{ y } b \sim b'$$

y como "$\sim$" es regular o compatible con "o", resulta

$$a \circ b \sim a' \circ b'$$

luego, $a' \circ b' \in C_c$.

Así hemos probado que se llega al mismo resultado cualesquiera que sean $a \in C_a$ y $b \in C_b$.

Por consiguiente, la clase producto $C_c = C_a \bar{\circ} C_b$ no depende más que de las clases factores C_a y C_b, y lo cual permite definir sobre el conjunto cociente $Q = E/\sim$ una ley bien definida de composición $\bar{\circ}$.

Llamaremos a esta ley $\bar{\circ}$ la LEY INDUCIDA por la ley "o" de E.

Las propiedades de la ley inducida están contenidas en el teorema que sigue:

Teorema. Sea E un conjunto sobre el cual se ha definido una relación de equivalencia "$\sim$" regular o compatible con respecto a una o más leyes de composición "o", "$*$", ... definidas sobre el mismo conjunto E.

Entonces:

1) una ley asociativa o conmutativa en E, induce una ley asociativa o conmutativa en el conjunto cociente $Q = E/\sim$.

2) dos leyes distributivas en E, inducen dos leyes distributivas en $Q = E/\sim$.

3) una ley con unidad en E, induce una ley con unidad en $Q = E/\sim$.

4) si un elemento $a \in E$ tiene inverso o simétrico $a^{-1} \in E$, entonces en la ley inducida sobre $Q = E/\sim$, la clase de equivalencia C_a de elemento a tiene como inverso la clase de equivalencia $C_{a^{-1}}$ del elemento a^{-1}.

Demostraciones.

1) Supongamos que "o" sea una operación asociativa sobre E. Entonces, se puede escribir:

$$\begin{aligned} C_a \bar{\circ} (C_b \bar{\circ} C_c) = C_a \bar{\circ} C_{b \circ c} &= C_{a \circ (b \circ c)} \\ &= C_{(a \circ b) \circ c} \\ &= C_{a \circ b} \bar{\circ} C_c \\ &= (C_a \bar{\circ} C_b) \bar{\circ} C_c \end{aligned}$$

lo que prueba que la ley inducida $\bar{\circ}$ sobre $Q = E/\sim$ es también asociativa.

Ahora, si la ley "o" es conmutativa en E, se tiene

$$C_a \bar{\circ} C_b = C_{a \circ b} = C_{b \circ a} = C_b \bar{\circ} C_a$$

lo que prueba que también es conmutativa la ley inducida $\bar{\circ}$ sobre $Q = E/\sim$.

2) Supongamos ahora que la ley "o" es distributiva con respecto a la ley "$*$" en E; entonces podemos escribir:

$$\begin{aligned} C_a \bar{\circ} (C_b \bar{*} C_c) = C_a \bar{\circ} C_{b * c} &= C_{a \circ (b * c)} \\ &= C_{(a \circ b) * (a \circ c)} \\ &= C_{a \circ b} \bar{*} C_{a \circ c} \\ &= (C_a \bar{\circ} C_b) \bar{*} (C_a \bar{\circ} C_c) \end{aligned}$$

lo que demuestra que la ley inducida $\bar{\circ}$ es distributiva a la izquierda con respecto a la ley inducida $\bar{*}$ en $Q = E/\sim$.

De la misma manera se demuestra la distributividad a la derecha.

3) Supongamos en seguida que la ley "o" en E tenga unidad e; entonces tendremos:

$$C_e \bar{\circ} C_a = C_{e \circ a} = C_a$$

$$C_a \bar{\circ} C_e = C_{a \circ e} = C_a$$

lo que prueba que la ley inducida $\bar{\circ}$ sobre $Q = E/\sim$ tiene la unidad C_e; es decir, la clase de equivalencia del elemento unidad e de E.

4) Por último, supongamos que el elemento $a \in E$ tiene respecto a la unidad e de E como inverso el elemento $a^{-1} \in E$; entonces se tendrá

$$C_{a^{-1}} \bar{\circ} C_a = C_{a^{-1} \circ a} = C_e$$

$$C_a \bar{\circ} C_{a^{-1}} = C_{a \circ a^{-1}} = C_e$$

lo que prueba que $C_{a^{-1}}$ es el inverso o simétrico de C_a en $Q = E/\sim$.

Todas estas conclusiones, prueban el teorema. Por consiguiente, toda relación de igualdad entre diversos elementos que se componen siguiendo las leyes de E se conservan cuando se pasa a las leyes inducidas sobre el conjunto cociente $Q = E / \sim$.

6. *Isomorfismo y Homomorfismo.* Consideremos dos conjuntos E y F, distintos o no, en los que se ha definido una o más operaciones que se corresponden dos a dos (homólogas).

Una aplicación

$$f : E \longrightarrow F$$

se dirá regular o compatible para las leyes homólogas de E y F, si la igualdad,

$$a \circ b = c$$

verificada sobre E implica para los elementos imágenes f(a), f(b) y f(c) la igualdad,

$$f(a) * f(b) = f(c) = f(a \circ b)$$

verificada sobre F, cualesquiera que sean a y b en E. Es decir, que el transformado del compuesto sobre E de dos elementos es el compuesto sobre F de los transformados de estos elementos.

Esta propiedad la expresamos diciendo que la aplicación f respeta o preserva las operaciones homólogas "o" y "*" definidas en E y en F; o que, f es un HOMOMORFISMO de E y F.

Si la aplicación f fuera biyectiva, entonces el homomorfismo f toma el nombre de ISOMORFISMO.

Los conceptos precedentes se extienden también a sistemas algebraicos sobre los que están definidas homólogamente más de una operación binaria interna. Dos conjuntos E y F, entre los que se puede definir un isomorfismo (respectivamente, un homomorfismo), con respecto a operaciones prefijadas, los llamaremos *isomorfos* (respectivamente, *homomorfos).*

El isomorfismo lo designaremos con la notación $\cong$ y el homomorfismo con $\simeq$. De modo que, si A es isomorfo con B, escribiremos

$$A \cong B$$

y si A es homomorfo con B, se escribirá

$$A \simeq B$$

Es fácil probar que la relación isomorfismo es de equivalencia; esto es:

1) $A \cong A$ (reflexiva)

2) $A \cong B \Rightarrow B \cong A$ (simétrica)

3) $A \cong B$ y $B \cong C \Rightarrow A \cong C$ (transitiva)

(Haga la demostración como ejercicio).

Por consiguiente, si H denota un conjunto cuyos elementos

$$H = \{A, B, C, D, \ldots\}$$

son conjuntos y en cada uno de los cuales se han definido una o más operaciones binarias internas, entonces si una aplicación f entre pares de estos conjuntos es un isomorfismo, ella agrupa los elementos de H en conjuntos isomorfos.

Cada clase de equivalencia define por abstracción un sistema algebraico único que conserva todas las propiedades. La invariancia de las propiedades algebraicas bajo isomorfismo quedan establecidos en el teorema que sigue.

Teorema. Sean (A; o, ...) y (B; *, ...) dos sistemas algebraicos isomorfos, esto es, que pertenecen a una misma clase de equivalencia. Entonces, si las operaciones en A tienen las propiedades asociativa, conmutativa o distributiva, las operaciones homólogas en B tienen también estas propiedades.

Además, si A tiene respecto a una operación elemento neutro, B también lo tiene; y si un elemento $a \in A$ tiene su inverso, entonces la imagen de a tiene como inverso en B la imagen del inverso de a.

Demostraciones:

1) Supongamos que "o" y "*" sean, en A y B, operaciones homólogas y que la ley "o" sea asociativa en A.

Probaremos que la ley "*" es también asociativa en B. En efecto, sean a', b', c' tres elementos arbitrarios en B, entonces existen tres elementos únicos a, b, $c \in A$, tales que:

$$a' = f(a),\ b' = f(b),\ c' = f(c)$$

por ser f una biyección de A sobre B.

Luego, se puede escribir

$$\begin{aligned} a' * (b' * c') &= f(a) * [f(b) * f(c)] \\ &= f(a) * f(b \circ c) \\ &= f[a \circ (b \circ c)] \end{aligned}$$

por ser f un isomorfismo.

Ahora bien, como "o" es asociativa en A, tendremos

$$a' * (b' * c') = f[a\ o(b\ o\ c)] = f[(a\ o\ b)\ o\ c]$$
$$= f(a\ o\ b) * f(c)$$
$$= [f(a) * f(b)] * f(b)] * f(c)$$
$$= (a' * b') * c'$$

lo que prueba la asociatividad de "$*$" en B.

Si la operación "o" hubiese sido conmutativa en A, tendríamos como antes:

$$a' * b' = f(a) * f(b) = f(a\ o\ b)) = f(b\ o\ a)$$
$$= f(b) * f(a)$$
$$= b' * a'$$

lo que prueba la conmutatividad de "$*$" en B.

De manera análoga probaremos la conservación de la propiedad distributiva.

En efecto, como antes, tendremos:

$$a' * (b'\ T\ c') = f(a) * [f(b)\ T\ f(c)] = f(a) * f(b \perp c)$$
$$= f[a\ o\ (b \perp c)]$$
$$= f[(a\ o\ b) \perp (a\ o\ c)]$$
$$= f(a\ o\ b) \top f(a\ o\ c)$$
$$= [f(a) * f(b)]\ T\ [f(a) * f(c)]$$
$$= (a' * b')\ T\ (a' * c')$$

lo que prueba la distributividad de "$*$" respecto a "T" en B, si "o" es distributiva con respecto "$\perp$" en A.

2) Sea ahora $e \in A$ el elemento unidad para "o", y sea $e' = f(e)$. Sea además $a' \in B$ arbitrario tal que $a' = f(a)$.

Tendremos:

$$e' * a' = f(e) * f(a) = f(e\ o\ a) = f(a) = a'$$
$$a' * e' = f(a) * f(e) = f(a\ o\ e) = f(a) = a'$$

lo que prueba que $e' = f(e)$ es el elemento unidad para "$*$" en B.

3) Sea $a \in A$ con su inverso $a^{-1} \in A$; y sean $a' = f(a)$ y $a'' = f(a^{-1})$; se tiene:

$$a' * a'' = f(a) * f(a^{-1}) = f(a\ o\ a^{-1}) = f(e) = e'$$
$$a'' * a' = f(a^{-1}) * f(a) = f(a^{-1}\ o\ a) = f(e) = e'$$

lo que prueba que a'' es el inverso de a' en B, respecto a la unidad e'; es decir:

$$a'' = f(a^{-1}) = [f(a)]^{-1}$$

este resultado y los anteriores, demuestran el teorema.

En consecuencia, dos conjuntos isomorfos son indistinguibles desde el punto de vista algebraico; esto es, toda propiedad de uno de ellos que se exprese únicamente con la intervención de los signos operatorios, implica para los elementos imágenes la misma propiedad, y recíprocamente.

En cambio, como la aplicación homomorfismo f no es biyectiva, entonces los papeles de A y B no pueden, en general, intercambiarse. Por lo tanto, el homomorfismo no es reflexivo ni simétrico como lo era el isomorfismo, pero en cambio tiene la propiedad transitiva.

En efecto, sean

$f : A \longrightarrow B$ un homomorfismo
$g : B \longrightarrow C$ un homomorfismo

Probaremos que la aplicación compuesta,

$$h = g\ o\ f : A \longrightarrow C$$

es un homomorfismo. Tenemos:

$$f(a\ o\ b) = f(a) * f(b), \forall\ a, b \in A$$
$$g(c * d) = g(c)\ T\ g(d), \forall c, d \in B$$

entonces,

$$h(a\ o\ b) = (g\ o\ f)\ (a\ o\ b) = g\ (f(a\ o\ b))$$
$$= g\ (f(a) * f(b))$$
$$= g\ (f(a))\ T\ g\ (f(b))$$
$$= (g\ o\ f)\ (a)\ T\ (g\ o\ f)\ (b)$$
$$= h\ (a)\ T\ h(b),\ \forall\ a, b \in A$$

resultado que prueba que $h = g\ o\ f$ es un homomorfismo de A en C.

El homomorfismo no tiene por qué conservar, como lo hacía el isomorfismo, todas las propiedades algebraicas. Pues, puede haber en B propiedades que no había en A y recíprocamente. Pero hay algunas propiedades en A que son siempre válidas en B, como lo afirma el teorema que sigue.

Teorema. Sea $f : A \longrightarrow B$ un homomorfismo sobreyectivo. Entonces:

1) si las operaciones en A tienen las propiedades asociativa, conmutativa o distributiva, las operaciones homólogas en B también tienen estas propiedades;

2) además, si A tiene elemento neutro, B también lo tiene;

3) si un elemento $a \in A$ tiene su inverso, la imagen de a tiene como inverso en B la imagen del inverso de a.

Demostración. Hacerla como ejercicio.

Ejemplo importantísimo. Sea E un conjunto provisto de una ley de composición "o" y de una relación "$\sim$" de equivalencia regular con respecto a esta operación de E.

Anteriormente vimos que esta operación "o" de E induce a una ley de composición "$\bar{o}$" en el conjunto cociente $Q = E / \sim$.

Probaremos que con respecto a esta operación "$\bar{o}$", Q es una imagen homomorfa de A, siendo la aplicación de homomorfismo

$$f : E \longrightarrow Q = E / \sim$$

definida por

$$f(a) = C_a$$

En efecto, por definición de composición de clases en Q se puede escribir:

$$C_{a\,o\,b} = C_a \,\bar{o}\, C_b$$

o sea,

$$f(a \,o\, b) = f(a) \,\bar{o}\, f(b), \forall\, a, b \in E$$

donde se ve que f es un homomorfismo.

Naturalmente este razonamiento se extiende al caso en que en E hay varias operaciones y siempre que la equivalencia sea regular con respecto a todas ellas.

Por consiguiente, para todo entero positivo n, el conjunto $\mathbb{Z}_n$ de las clases residuales módulo n (ver TOMO I, Capítulo V, sección 5.2.) es una imagen homomorfa de $\mathbb{Z}$:

$$\mathbb{Z}_n \simeq \mathbb{Z}, \text{ para } n = 2, 3, 4, 5, \ldots$$

puesto que la relación de congruencia módulo n es regular o compatible con las operaciones de adición y multiplicación de $\mathbb{Z}$; por tanto, ellas inducen una adición y una multiplicación en el conjunto cociente $\mathbb{Z}_n$, dadas por las reglas:

$$\begin{cases} \bar{a} + \bar{b} = \overline{a + b} \\ \bar{a} \cdot \bar{b} = \overline{a \cdot b} \end{cases}$$

Pero entre los dos sistemas algebraicos homomorfos $\mathbb{Z}$ y $\mathbb{Z}_n$ existen diferencias esenciales.

En efecto, si bien es cierto que las propiedades formales (asociatividad, conmutatividad y distributividad) de las operaciones de adición y multiplicación se conservan mediante la aplicación

$$a \longrightarrow f(a) = C_a$$

hay, un cambio, en uno u otro conjunto $\mathbb{Z}$ y $\mathbb{Z}_n$ propiedades que no se conservan bajo esta aplicación $f(a) = C_a$ de homomorfismo.

Así, por ejemplo, para el caso $n = 6$, existen en $\mathbb{Z}_6$ elementos tales como C_2, C_3 y C_4 que verifican las relaciones:

$$C_2 \cdot C_3 = C_6 = C_0$$
$$C_3 \cdot C_4 = C_{12} = C_0$$

es decir, existen en $\mathbb{Z}_6$ divisores de cero (Ver TOMO I, Capítulo V, sección 5.2.); cosa que no ocurre en el anillo $\mathbb{Z}$.

Por otra parte, para el caso $n = 5$, sucede que en $\mathbb{Z}_5$ cada elemento no nulo tiene un inverso para la multiplicación, puesto que:

$$C_1 \cdot C_1 = C_{1.1} = C_1$$
$$C_2 \cdot C_3 = C_6 = C_1$$
$$C_4 \cdot C_4 = C_{16} = C_1$$

y cosa que no sucede en $\mathbb{Z}$; porque $\mathbb{Z}_5$ es un cuerpo y $\mathbb{Z}$ no lo es.

Capítulo VI

EL SISTEMA DEDUCTIVO

6.0. Una de las características más sorprendentes de las matemáticas de nuestro tiempo es el enfoque abstracto y axiomático que las hace materia de estudio. Por este enfoque entenderemos el método por el cual usando un razonamiento deductivo se obtienen, de un pequeño número de supuestos básicos llamados axiomas, propiedades de los sistemas matemáticos; y en lo abstracto, bástanos con señalar sólo un ejemplo para mostrar su importancia: los sistemas de los números naturales y racionales, aunque diferentes entre sí, realmente tienen muchas propiedades en común. Así, por ejemplo, cuando dos números a y b han de ser sumados, el orden en que esto se realice no tiene importancia; esto es, el número $a + b$ es el mismo número que $b + a$, ya sea que a y b sean números naturales o racionales.

Por consiguiente, parece provechoso investigar sistemas matemáticos más generales que obedezcan a leyes parecidas a la recién mencionada, y de tal manera que los sistemas numéricos sean meramente casos especiales de estas estructuras más generales, y que ahora decimos abstractas si prescindimos de la naturaleza de los elementos con los cuales se opera. Si así se hace, entonces todo resultado que se obtenga para el caso general o abstracto, se traslada inmediatamente a los sistemas más especializados o concretos.

De esta manera, la técnica axiomática nos provee de un método que nos libera de la labor de profundizar y memorizar propiedades por separado en muchos sistemas parecidos. Lo que es más, como un efecto secundario, las matemáticas se amplían más en el sentido de que varios conceptos se hacen parte de una configuración más grande y general.

6.1. La axiomatización de una teoría consiste en establecer un grupo de conceptos llamado *conceptos primitivos* y un grupo de proposiciones y relaciones llamadas *proposiciones y relaciones primitivas* tales que:

a) los conceptos primitivos no se definen explícitamente, únicamente se enuncian sin tratar de especificar su sentido;

b) las proposiciones primitivas se aceptan sin tratar de demostrar su veracidad;

c) las proposiciones primitivas deben caracterizar en forma unívoca y completa a los conceptos primitivos y también a las relaciones primitivas, que unidas a la de la lógica constituirán los recursos operatorios con los cuales deberá edificarse deductivamente toda la disciplina;

d) una vez establecidos los conceptos, proposiciones y relaciones primitivas, al desarrollar una teoría matemática por el método axiomático, hay que seguir paso a paso las dos reglas siguientes:

1) Todo nuevo concepto o término que se introduzca debe siempre definirse mediante los conceptos primitivos y los que, a partir de éstos, ya hayan sido definidos.

2) Toda proposición nueva o teorema debe apoyarse únicamente en los axiomas o en los teoremas previamente demostrados.

El sistema de axiomas de una disciplina no es único; pueden darse diversos sistemas equivalentes e igualmente aceptables; una misma proposición puede ser axioma en un sistema y teorema en otro. Basta pensar, por ejemplo, que si una propiedad es condición necesaria y suficiente para otra, ambas son lógicamente equivalentes y puede, por tanto, reemplazarse una por otra sin ningún inconveniente.

Por consiguiente, para elaborar una teoría axiomática hay siempre bastante libertad para escoger los conceptos y las proposiciones primitivas, pero cuidando que los sistemas que puedan así formarse sean equivalentes.

Los conceptos no definidos y las proposiciones no probadas se eligen por convención.

Debemos insistir en que, desde el punto de vista de la matemática, los conceptos y proposiciones primitivas no son más que meras hipótesis o convenciones y lo que preocupa al matemático es deducir las consecuencias de estos conceptos y proposiciones primitivas, que serán indiscutiblemente verdaderas si lo son las proposiciones y conceptos primitivos.

En otras palabras, en un razonamiento deductivo, la verdad de la tesis se reduce a la verdad supuesta de la hipótesis; pero la validez de un razonamiento es algo distinto de la verdad de las proposiciones que en él intervienen. Dicho de otro modo: La verdad formal o corrección lógica es distinta de la verdad material o real, es decir, del contenido de las proposiciones.

Ahora bien, si los axiomas son meras convenciones, no es posible tampoco considerar cualquier conjunto de definiciones y axiomas como una teoría matemática, sino que ellos deben justificarse. Las condiciones para una tal justificación son, desde el punto de vista del "formalismo", cuyo representante principal fue el célebre matemático alemán David Hilbert (1862-1943), las siguientes: compatibilidad, saturación e independencia.

a) La primera condición, la de compatibilidad, o la de no contradicción, como también se la denomina, se la puede definir de la manera siguiente: cuando dadas las proposiciones contradictorias p y p', una de

ellas por lo menos no puede nunca ser probada en la teoría, es decir, cuando no se puede probar a la vez, partiendo del sistema de axiomas, una proposición y su negación.

El problema de la compatibilidad o de la no contradicción de un sistema de axiomas, es el problema lógico por excelencia, pues la existencia de una contradicción en una teoría la invalida completamente.

El problema de la compatibilidad ha sido atacado con pleno éxito en casi todas las teorías matemáticas; así, por ejemplo, Hilbert demuestra de una manera acabada, la no contradicción de la Geometría, aceptando la no contradicción de la teoría de los números reales. La aritmetización del análisis reduce también su no contradicción a la de los números reales; la no contradicción de éstos se reduce, a su vez, a la no contradicción de los números naturales.

Por otra parte, la compatibilidad de otras disciplinas matemáticas se reduce a la de la teoría elemental de conjuntos.

Por consiguiente, queda así, con este proceso de reducción, la compatibilidad de la Matemática dependiendo de la compatibilidad de la aritmética de los Números Naturales y de la Teoría de Conjuntos, disciplinas que desempeñan por esto el papel especial de cimientos de la Matemática.

b) La segunda condición, la de saturación o completicidad de un sistema de axiomas, exige que dada una proposición que sea expresable en los términos de una teoría, entonces o ella es demostrable, o es demostrable su negación.

En otras palabras, la completicidad o saturación del sistema de axiomas exige que a partir del sistema dado sea posible demostrar todas las demás proposiciones de la teoría.

c) La tercera condición, la de independencia de los axiomas, exige que ningún axioma del sistema, ni parte de uno, pueda deducirse de los demás.

Si uno de los axiomas de una teoría pudiera deducirse de los demás, conviene eliminarlo del sistema dado de axiomas, pues, por la condición de saturación entra en la teoría como teorema, y el sistema de axiomas se simplifica.

Es claro que esta condición no es indispesable desde el punto de vista lógico, sino solamente deseable; aún más, puede ser útil el dar sistemas de axiomas que no la cumplan, en el sentido de ser abundante, porque el inconveniente de la no independencia queda compensado por una sencillez mucho mayor que la que se podría obtener con un sistema independiente.

La historia de la Matemática nos da un notable ejemplo que prueba la importancia del concepto de independencia de los sistemas de axiomas:

durante más de veinte siglos los matemáticos se esforzaron infructuosamente en demostrar el axioma v de Euclides, o postulado de las paralelas, hasta que Gauss, Lobatschewsky, Bolyai y Riemann plantearon y resolvieron el problema de la independencia de este postulado o axioma, creando las geometrías no euclideanas, las cuales contienen los mismos axiomas que la geometría euclideana, excepto el v que se reemplaza por su negación.

Los problemas de compatibilidad o no contradicción y el de saturación o completicidad de un sistema de axiomas, cuando se trata de axiomatizar en forma absoluta las teorías matemáticas, presenta grandes dificultades que todavía no están completamente dilucidadas, pero investigaciones debidas al matemático austriaco Gödel, hacen prever que la solución total del problema sea imposible de alcanzar.

El método de edificación de una ciencia basado en los principios expuesto, se denomina METODO DEDUCTIVO y SISTEMAS DEDUCTIVOS los construidos de acuerdo con ellos.

Cada vez se extiende más la idea de que el método deductivo es el único rasgo esencial que distingue a las disciplinas o sistemas matemáticos de las restantes ciencias. Sin embargo, no solamente toda disciplina matemática es una ciencia deductiva, sino que recíprocamente toda ciencia deductiva es también una disciplina matemática. Según esto, la lógica deductiva debería considerarse como una disciplina matemática.

6.2. La estructura actual de la Matemática es formalista. Esto es, 1°) los axiomas son arbitrarios; sólo están sujetos a una condición esencial, que es la compatibilidad. Por lo tanto, pueden construirse tantas disciplinas matemáticas como sistemas compatibles de postulados o axiomas; 2°) los axiomas son relaciones entre no importa qué clase de entes que vienen caracterizados implícitamente por estas relaciones. Luego, un sistema de axiomas no individualiza necesariamente un sistema de entes, sino un sistema de relaciones, y la Matemática deducida de él puede aplicarse a todos los sistemas de entes que satisfagan esos axiomas y, 3°) el sistema de axiomas está destinado a fundamentar simultáneamente la lógica y la Matemática.

El formalismo se diferencia del logicismo en que juntamente con los axiomas lógicos acepta otros de índole exclusivamente matemático, no reductibles a los de la lógica. El tratamiento simultáneo de las dos disciplinas tiene por objeto satisfacer uno de los propósitos principales del formalismo: suprimir toda suposición que no esté contenida en los axiomas.

Consecuencia de todo lo anterior es que la axiomática desempeñe

un papel capital en su fundamentación. Esta es la razón del porqué las teorías matemáticas se presentan como sistemas hipotético-deductivos, es decir, sus conclusiones no tienen una validez independiente sino con respecto al sistema de axiomas de cada teoría.

Para justificar la estructura formalista es necesario aceptar la legitimidad de las teorías matemáticas elementales: Aritmética Elemental y Teoría Elemental de Conjuntos como una verdad de hecho, justificada por el manifiesto contenido intuitivo de estas teorías, que permite que la mente humana las acepte sin resistencia.

David Hilbert intentó construir la Matemática como disciplina autónoma, en el sentido de considerarla independiente de la filosofía y de la experiencia. Para ello perfecciona el método axiomático, asignándole un papel excepcional en la estructura de la Matemática.

Hilbert y su escuela han dado al método axiomático el alto grado de perfección con que actualmente lo conocemos, habiendo llegado merced a esos trabajos a constituirse, conjuntamente con el método genético, en los métodos únicos con los cuales se fundamentan y desarrollan las diferentes ramas que constituyen la Matemática.

Dice Hilbert: "Quisiera resumir en cuatro palabras mi concepto general del método axiomático", y continúa: "Según mi opinión, todo lo que puede ser objeto de pensamiento científico, se adquiere por el método axiomático, y, por tanto, e indirectamente, por la Matemática, siempre que su forma esté en razón para una teoría. Mientras más penetremos en las capas cada vez más profundas, seremos más conscientes de la unidad de nuestros pensamientos. Por último, la Matemática parece llamada a desempeñar un papel director en el edificio de las ciencias constituidas por el método axiomático".

En efecto, según esta idea hilbertiana, se observa que en todas las ramas de la Física y de la Química, también en la Biología, y en general en casi todas las disciplinas científicas y aun en las llamadas humanistas, se trata de establecer una sistematización, consistente en un encadenamiento u ordenación lógica de los conceptos y proposiciones que las constituyen, de manera que una proposición o concepto posterior esté lógicamente fundamentado en los anteriores. En esta ordenación hay, pues, un grupo primario de proposiciones y conceptos. Por lo tanto, esto nos indica que estas disciplinas tratan de estructurarse conforme al método axiomático.

Este sistema ideado por Hilbert requiere la solución de un problema vital: la compatibilidad. Problema extremadamente difícil y hay casi unanimidad en afirmar, por investigaciones modernas, que la solución total del problema en referencia sea imposible de alcanzar.

Si Hilbert hubiera logrado su objetivo, tendríamos un sistema formal perfecto de tipo convencional, es decir, hipotético-deductivo, al que llamaríamos MATEMATICA, y sería, por tanto, una disciplina autónoma.

Mientras quede sin solución el problema de compatibilidad es necesario, para mantener la estructura formalista de la Matemática, postular esa compatibilidad, o bien aceptarla como verdad de hecho comprobada por la experiencia de la existencia de la matemática, o también aceptarla por el argumento de los intuicionistas que consideran justificada la compatibilidad por el contenido intuitivo de los axiomas.

El uso de los axiomas ha permitido a los matemáticos fundamentar su obra rigurosamente y, al mismo tiempo, introducir una simplicidad y claridad básica en su materia de estudio. Esto, a su vez, ha conducido a una comprensión más profunda de los sistemas matemáticos. Además, el método axiomático ha llevado a muchos descubrimientos matemáticos nuevos e importantes.

En conclusión, el trabajo de Hilbert, por el rigor de su lenguaje y de sus razonamientos y por su negativa a cualquier concesión, es el modelo del trabajo matemático moderno, y lo será sin duda durante muchos siglos y, al mismo tiempo, la admiración de las generaciones.

Capítulo VII

EL NUMERO NATURAL

7.0. El sistema de los números naturales constituye un buen ejemplo, como lo veremos a continuación, de un sistema deductivo o de una teoría axiomatizada.

El número natural puede introducirse, como se vio en el Capítulo I de la Primera Parte, como derivado de la teoría de conjuntos. En esta forma vimos que el número natural se define por abstracción partiendo del cálculo de clases, y las propiedades del número resultan teoremas deducidos de los de ese cálculo. Este camino, iniciado por Cantor y seguido por Frege, ha sido perfeccionado por Russell y Whitehead, los cuales lo exponen en forma completa en su obra "Principia Mathematica".

Ahora introduciremos el número natural como concepto primitivo, y en tal caso debe fundamentarse axiomáticamente, tal es el camino seguido por el célebre matemático italiano Giuseppe Peano (1858-1932), fundador de la escuela italiana de la Lógica Simbólica.

Peano fundamenta axiomáticamente la teoría de los números naturales en la forma siguiente:

I. Introduce tres conceptos primitivos, a saber:

1) NUMERO NATURAL

2) UNO

3) "SIGUIENTE DE...", o bien "SUCESOR DE...." el primero es un conjunto o una clase, el segundo un objeto matemático y el tercero es una relación.

Estos conceptos no se definen explícitamente, puesto que los consideramos primitivos, pero se caracterizan implícitamente por las siguientes proposiciones primitivas:

II. Axiomas del número natural, y que son:

Ax. 1): Los números naturales son entes de una clase $\mathbb{N}$. Es decir, se admite la existencia del conjunto $\mathbb{N}$ cuyos elementos se llaman números naturales.

Ax. 2): A cada elemento $a \in \mathbb{N}$ se le puede hacer corresponder unívocamente otro elemento $a' \in \mathbb{N}$, que se llama el siguiente de a.

Ax. 3): Existe un elemento particular de $\mathbb{N}$, que designaremos con la notación 1, que llamaremos UNO y que no es siguiente de ningún elemento de $\mathbb{N}$; esto es, $x' = 1$ para todo $x \in \mathbb{N}$.

Ax. 4): $a' = b' \Rightarrow a = b$; es decir, si los siguientes de dos elementos son iguales, los dos elementos son también iguales.

Ax. 5): Se admite el denominado Principio de Inducción, es decir, si A es un subconjunto de IN que contiene al 1, y si de la hipótesis de que contenga un $x \in IN$ se deduce que también contiene al siguiente x', entonces se puede afirmar que el conjunto A contiene a todos los elementos de IN; esto es, $A = IN$.

Este axioma, en símbolos, se escribe así: Sea $A \subseteq IN$ con las propiedades siguientes

1) $1 \in A$

2) $x \in A \Rightarrow x' \in A$

Luego, $A = IN$.

El axioma 5) es fundamental en la teoría del número natural; constituye el Principio de la Inducción Matemática, o Principio de Inducción Completa y puede expresarse también en la forma siguiente:

"Sea P una propiedad de los números naturales que tiene las siguientes condiciones:

a) La propiedad se cumple para el uno.

b) Si la propiedad se cumple para un número natural x, la propiedad se cumple también para el siguiente x', entonces la propiedad se cumple para todos los números naturales".

Para pasar de una forma a otra basta, si se da el conjunto A, considerar como propiedad P la de pertenecer a A, y si se da P, basta considerar como conjunto A el de los elementos que cumplen P.

Consecuencias inmediatas de los axiomas

1. El Ax. 2) nos garantiza que, dado *a* queda determinado unívocamente a'; y el A. 4) nos garantiza que, dado a' queda determinado unívocamente *a*.

Por consiguiente, la correspondencia entre cada número y su siguiente es biunívoca, de modo que se puede enunciar la proposición siguiente:

Teorema 1)

$$a' = b' \Longleftrightarrow a = b$$

o también:

$$a' \neq b' \Longleftrightarrow a \neq b$$

2. *Teorema 2)* Todo número es distinto de su siguiente; es decir,

$$a' \neq a$$

Demostración. Lo probaremos por inducción.

Sea A el conjunto de los números naturales que son distintos de su siguiente.

$$A = \{x \in IN : x' \neq x\}$$

Entonces, ya A cumple, por su definición, con la propiedad de que

$$A \subseteq IN$$

Por otra parte, por el Ax. 3) sabemos que

$$1 \neq x', \forall x \in IN$$

y en particular, $1 \neq 1'$

lo que expresa que $1 \in A$.

Por otro lado, sea ahora $x \in A$; entonces por la definición de A resulta ser $x \neq x'$. Pero, por el teorema 1) se tiene

$$x \neq x' \Rightarrow x' \neq (x')'$$

luego, $x' \in A$.

Por consiguiente, el subconjunto A de IN posee todas las propiedades del Ax. 5) y se tiene $A = IN$, y el teorema está demostrado.

3. *Teorema 3)* Todo número, salvo el 1, es el siguiente de un número; esto es,

Si $a \neq 1$, entonces existe $b \in IN$ tal que $a = b'$

Demostración. Llamemos A al conjunto de los números naturales compuesto con el 1 y los números que son siguientes de algún otro. Por lo tanto, un elemento de A, ó es 1, ó es de la forma b'.

Probaremos que este conjunto A satisface todas las propiedades del Ax. 5).

En efecto, por definición de A tenemos $1 \in A$; y si $x \in A$, entonces x', por ser siguiente de x, también pertenece a A. Luego, $A = IN$ y entonces, todo número a que no sea 1, es de la forma $a = b'$, y el teorema está demostrado.

4) Partiendo de los axiomas anteriores, en los que los conceptos: número, uno, siguiente de....., son de carácter primitivo y en particular del hecho ya probado en el Teorema 2) de que

$$a \neq a'$$

podemos definir conjuntos que verifiquen los axiomas de Peano.

Así, por ejemplo, si a partir del símbolo 1, definimos sucesivamente los símbolos:

$$2 = 1',\ 3 = 2',\ 4 = 3', \ldots\ldots,\ n + 1 = n', \ldots$$

el conjunto A = {1, 2, 3, ... , n, n + 1, ...} puede considerarse como el conjunto IN, pues en él se verifican los axiomas de 1) al 5).

Asimismo, si partimos de la palabra UNO y definimos sucesivamente las palabras:

DOS = UNO', TRES = DOS', ... DIEZ = NUEVE', ...

también el conjunto B = {UNO, DOS, TRES, ...} puede considerarse como el conjunto IN, pues en él se cumplen los axiomas de 1) al 5).

Naturalmente, este proceso puede repetirse en cualquier otro idioma, o en cualquier otro tipo de símbolos, y éstos y las reglas para formar el "siguiente de..." variarán, pero siempre tendremos IN que verifican los axiomas de Peano.

Entre dos cualesquiera de esos conjuntos podrá establecerse una correspondencia biunívoca que respeta o preserva la relación "siguiente de...".

En virtud de este isomorfismo entre los distintos conjuntos, toda la propiedad o teorema basado exclusivamente en la noción "siguiente de...." y en los axiomas, vale indistintamente para todos los conjuntos IN, y puede ella ser probada en abstracto, sin hacer referencia a ninguno de los conjuntos concretos que puedan considerarse. Así lo haremos en el desarrollo de esta teoría del número natural.

Por consiguiente, los axiomas de Peano no caracterizan en forma unívoca a los números naturales, sino a un sistema de relaciones aplicables a todas las sucesiones.

Diremos que un sistema de axiomas cumple la condición de CATEGORICIDAD (término debido a Veblen), cuando ellos caracterizan esencialmente un sistema de entes, es decir, si hay dos sistemas de entes E y F que los satisfacen, se puede establecer entre E y F un isomorfismo, o sea una correspondencia biunívoca que deje invariante las propiedades definidas por los axiomas.

Las sucesiones son los sistemas de entes isomorfos al de los números naturales; por lo tanto deben ellas satisfacer el sistema de axiomas que caracterizan a éstos.

Bertrand Russell presentó una objeción a la teoría de Peano achacándola que era susceptible de diversas interpretaciones, pero esta objeción no tenía en cuenta la propiedad esencial de los números naturales de definirse salvo un isomorfismo.

Por otra parte, cuando Russell presentó sus objeciones tampoco se había establecido claramente que la definición de las operaciones de adición y multiplicación, que pronto veremos, formaban parte de la definición de los números naturales.

En consecuencia, toda definición aritmética de los números naturales, tal como:

Definición. Llamaremos Números Naturales a los elementos de un conjunto IN, que denominaremos conjunto natural, no vacío, algebrizado mediante dos operaciones de adición y multiplicación dadas por las reglas:

$$\begin{cases} a + 1 = a' \\ a + b' = (a + b)' \end{cases} ; \quad \begin{cases} a \cdot 1 = a \\ a \cdot b' = ab + a \end{cases}$$

y que cumple los siguientes axiomas:

1) A cada número natural *a* le corresponde otro único a', que se llama el siguiente de a.

2) Existe un elemento de IN, que designamos con la notación 1 y que llamamos uno que no es siguiente de ningún otro elemento de IN.

3) $a' = b' \Rightarrow a = b$.

4) Sea $A \subseteq IN$ con las propiedades siguientes:

a) $1 \in A$.

b) $x \in A \Rightarrow x' \in A$; entonces $A = IN$

sólo puede hacerlo mediante un isomorfismo, y dos de estos conjuntos isomorfos son el mismo desde el punto de vista aritmético, aun cuando puedan tener propiedades diferentes desde otros puntos de vista, por ejemplo la diferencia de palabras para los números en los distintos idiomas, o el ejemplo más interesante de los distintos sistemas de numeración; las propiedades aritméticas son independientes del sistema adoptado.

La sucesión fundamental de la aritmética

Para determinar a los números naturales mediante los axiomas de Peano de manera que coincidan con la noción intuitiva de ellos, es necesario dar a las ideas primitivas 1 y "siguiente de..." la interpretación intuitiva que nos es familiar. De este modo resulta que:

1, 1', (1')', ((1')')', etc.

son números naturales, y los indicaremos respectivamente con los símbolos siguientes:

1, 2, 3, 4, etc.

Esta sucesión constituye la Sucesión Fundamental de la Aritmética o la Serie Natural de los Números y en ella están contenidos todos los números naturales, ordenados mediante la relación "siguiente de...".

7.1. *Operaciones sobre* IN

Se observará que en las definiciones de adición y multiplicación sobre IN que siguen en esta sección no se acude a nada que sobrepase los axiomas de Peano.

I) *Adición en* IN.

Teorema. Existe una y una sola operación binaria interna en IN, que designaremos por:

$$(x, y) \longrightarrow x + y$$

llamada ADICION que satisface las dos propiedades siguientes:

$$(*) \quad \begin{cases} a + 1 = a' \\ a + b' = (a + b)', \end{cases} \quad \begin{cases} \forall\, a \in \mathbb{N} \\ \forall\, a, b \in \mathbb{N} \end{cases}$$

Demostración. Para demostrar que así tenemos una operación binaria interna, tenemos que probar que la suma:

$$(a + b)$$

está definida unívocamente, esto es, que existe y es única para cada par de números naturales, a y b.

En efecto, sea A el conjunto de los $x \in \mathbb{N}$ tales que la suma $(a + x)$ está definida unívocamente, donde a es un número natural arbitrario fijado de antemano.

$$A = \{x \in \mathbb{N} : a + x \text{ está definida unívocamente}\}$$

De acuerdo con la definición (*) y el Ax. 2) se tiene que $1 \in A$.

Sea ahora $x \in A$; entonces por la definición de A, $a + x$ está definida unívocamente.

Probaremos que también la suma $a + x'$ está definida unívocamente.

En efecto, de acuerdo con la definición (*) y el Ax. 2),

$$a + x' = (a + x)'$$

está definida unívocamente. Luego, $x' \in A$.

Así hemos demostrado que el conjunto A posee todas las propiedades del Ax. 5) y por esto resulta ser

$$A = \mathbb{N}$$

Por consiguiente, si $b \in \mathbb{N}$ entonces $b \in A$, y por lo tanto la suma $a + b$ está definida unívocamente para cualquier par de números naturales, a y b; esto es, dados dos números naturales, existe un único número natural igual a la suma de los dos, y el teorema está demostrado.

A partir de este teorema y los axiomas de Peano, podremos ahora demostrar las propiedades de la adición en IN.

Teorema. En IN, la operación de adición está regida por las leyes siguientes:

1) $a + b \neq b$

2) $(a + b) + c = a + (b + c)$ (propiedad asociativa)

3) $a + b = b + a$ (propiedad conmutativa)

4) $a + c = b + c \Rightarrow a = b$ (propiedad de cancelación)

Demostraciones: El procedimiento de demostración es siempre el de inducción completa. Tendremos:

1) Cualquiera que sean $a, b \in \mathbb{N}$ se tiene

$$a + b \neq b$$

En efecto, sea a un número dado en IN, y sea A el conjunto de todos los $x \in \mathbb{N}$ tales que

$$a + x \neq x$$

Se tiene $1 \in A$, ya que por la definición (*) y el Ax. 3) tenemos,

$$a + 1 = a' \neq 1$$

Sea ahora $x \in A$, por la definición de A, o hipótesis de inducción, Teorema 1) y definición (*) se tiene

$$a + x \neq x \Rightarrow (a + x)' \neq x' \Rightarrow a + x' \neq x'$$

luego, $x' \in A$.

Por consiguiente, por el Ax. 5) resulta $A = \mathbb{N}$; por tanto, $b \in \mathbb{N}$ implica $b \in A$, y por esto es $a + b \neq b$, y la propiedad 1) está demostrada.

2) Cualesquiera sean $a, b, c \in \mathbb{N}$ se tiene

$$(a + b) + c = a + (b + c)$$

En efecto, sean a y b dados en IN y sea A el conjunto de los $x \in \mathbb{N}$ tales que,

$$(a + b) + x = a + (b + x)$$

Se tiene $1 \in A$, ya que por la definición (*) resulta

$$(a + b) + 1 = (a + b)' = a + b' = a + (b + 1)$$

Supongamos ahora $x \in A$; entonces por la definición (*) y por la hipótesis de inducción, o lo que es lo mismo por la definición del conjunto A, se tiene

$$(a+b)+x' = [(a+b)+x]' = [a+(b+x)]' = a+(b+x)'$$

$$= a+(b+x')$$

luego, $x' \in A$.

Por el Ax. 5) resulta ser $A = \mathbb{N}$, por tanto, $c \in \mathbb{N}$ implica $c \in A$, y por esto es

$$(a+b)+c = a+(b+c)$$

y la propiedad 2) está demostrada.

3) Cualesquiera sean $a, b \in \mathbb{N}$ se tiene

$$a+b = b+a$$

En efecto, en una primera inducción respecto de b para $a = 1$, se tiene:

Sea A el conjunto de los $x \in \mathbb{N}$ tales que,

$$1+x = x+1$$

Es inmediato que $1 \in A$, porque evidentemente

$$1+1 = 1+1$$

es verdad.

Supongamos ahora $x \in A$, esto es

$$1+x = x+1$$

y probaremos que también $x' \in A$.

En efecto, por la definición (*), la propiedad 2) recién probada, la hipótesis de inducción y nuevamente por la definición (*), se puede escribir

$$1+x' = 1+(x+1) = (1+x)+1 = (x+1)+1 = x'+1$$

luego, $x' \in A$ y con el razonamiento de siempre se demuestra que se verifica la propiedad

$$1+b = b+1, \quad \forall\, b \in \mathbb{N}$$

es decir, que 1 conmuta con cualquier elemento de $\mathbb{N}$ con respecto a la adición.

Habiendo probado esto, haremos una nueva inducción respecto de b para un a cualquiera fijado de antemano.

Designemos por B el conjunto de los $x \in \mathbb{N}$ tales que,

$$a+x = x+a$$

Entonces, por la inducción anterior es inmediato que $1 \in B$, puesto que se verifica la propiedad,

$$a+1 = 1+a$$

Sea ahora $x \in B$; es decir se cumple la propiedad.

$$a+x = x+a$$

Probaremos que también $x' \in B$.

En efecto, haciendo uso de la definición (*), de la hipótesis de inducción, de la propiedad 3) de asociatividad y del resultado obtenido en la primera inducción, resulta

$$a+x' = a+(x+1) = (a+x)+1 = (x+a)+1 = x+(a+1) =$$

$$= x+(1+a) = (x+1)+a = x'+a$$

luego, $x' \in B$.

Por consiguiente, por el Ax. 5) se tiene $B = \mathbb{N}$.

Ahora, si $b \in \mathbb{N}$ entonces $b \in B$ y por esto vale la propiedad,

$$a+b = b+a, \quad \forall\, a, b \in \mathbb{N}$$

así se ha demostrado la ley 3).

4) Por último demostraremos la ley 4), es decir la propiedad,

$$a+c = b+c \Rightarrow a = b$$

cualesquiera sean $a, b, c \in \mathbb{N}$.

En efecto, sea A el conjunto de los $x \in \mathbb{N}$ tales que

$$a+x = b+x \Rightarrow a = b$$

Es inmediato que $1 \in A$, puesto que

$$a+1 = b+1 \Rightarrow a' = b' \Rightarrow a = b$$

en virtud del Ax. 4).

Supongamos ahora que $x \in A$ y mostremos que también $x' \in A$.

En efecto, por hipótesis de inducción tenemos:

$$a+x = b+x \Rightarrow a = b$$

y suponiendo que se tuviese,

$$a+x' = b+x'$$

o sea, $(a + x)' = (b + x)' \Rightarrow a + x = b + x$

y por la hipótesis hecha, resulta $a = b$; por lo tanto, $x' \in A$.

Por el Ax. 5), se obtiene $A = \mathbb{N}$, y con el razonamiento de siempre se llega a la propiedad

$$a + c = b + c \Rightarrow a = b$$

cualesquiera sean a, b, $c \in \mathbb{N}$; es decir, todo número natural es cancelable respecto a la adición.

Este último resultado y los anteriores, demuestran el teorema.

Tabla de Adición. La formación de una tabla de sumar se deduce de las definiciones dadas por las fórmulas:

$$\begin{cases} a + 1 = a' \\ a + b' = (a + b)' \end{cases}$$

Se trata, como puede observarse, de una definición por inducción completa: la primera define la operación de sumar 1 a un número cualquiera, de modo que, "siguiente de..." significa sumar 1; la segunda de las fórmulas define la operación de sumar el siguiente de un número natural cuando ya se sabe sumar éste. Así, pues, sabiendo sumar 1, sabremos sumar 2; pudiendo sumar 2 podremos sumar 3, y así indefinidamente.

Veamos a título de ejemplo cómo se forma la tabla del 2. Tenemos en este caso $a = 2$, luego:

$$\begin{aligned} 2 + 1 &= 2' = 3 \\ 2 + 2 &= 2 + 1' = (2 + 1)' = 3' = 4 \\ 2 + 3 &= 2 + 2' = (2 + 2)' = 4' = 5 \\ 2 + 4 &= 2 + 3' = (2 + 3)' = 5' = 6 \end{aligned}$$

II) *Multiplicación en* $\mathbb{N}$.

Teorema. Existe una y una sola operación binaria interna en $\mathbb{N}$, que designaremos por:

$$(x, y) \longrightarrow x \cdot y$$

llamada MULTIPLICACION que satisface las dos propiedades siguientes:

$$(**) \begin{cases} a \cdot 1 = a & , \forall\, a \in \mathbb{N} \\ a \cdot b' = a \cdot b + a, & \forall\, a, b \in \mathbb{N} \end{cases}$$

Demostración. Como en el caso de la suma, para probar que así tenemos una operación binaria interna, tenemos que demostrar que el producto:

$$(a \cdot b)$$

está unívocamente definido, esto es, que existe y es único para cada par de números naturales, a y b.

En efecto, sea A el conjunto de los $x \in \mathbb{N}$ tales que el producto $a \cdot x$ está unívocamente definido, siendo el factor *a* un número natural arbitrario fijado de antemano.

Es claro que $1 \in A$, ya que por la definición (**) se tiene:

$$a \cdot 1 = a$$

Sea ahora $x \in A$; entonces por la definición de A, el producto $a \cdot x$ está definido unívocamente (hipótesis de inducción); luego, como también lo está la suma

$$a \cdot x + a = a \cdot x' \qquad (**)$$

resulta entonces que el producto $a \cdot x'$ está definido unívocamente; luego, $x' \in A$.

Por consiguiente, el conjunto A posee todas las propiedades del Ax. 5); esto es, $A = \mathbb{N}$.

Por lo tanto, $b \in \mathbb{N} \Rightarrow b \in A$ y por esto el producto $a \cdot b$ está definido unívocamente para cualquier par de números naturales, a y b; es decir, dados dos números naturales, existe un único número natural igual al producto de los dos números dados, y el teorema está demostrado.

A partir de este teorema y de los axiomas de Peano, demostraremos, como en el caso de la suma, las propiedades de la multiplicación en $\mathbb{N}$.

Teorema. En $\mathbb{N}$, la operación de multiplicación está regida por las leyes siguientes:

1) $a \cdot b = b \cdot a$ (propiedad conmutativa)

2) $a \cdot (b + c) = a \cdot b + a \cdot c$ (propiedad distributiva)

3) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (propiedad asociativa)

Demostraciones: Tal como en el caso de la adición, el procedimiento que emplearemos para demostrar estas propiedades de la multiplicación será también el de inducción completa. Tendremos:

1) Cualesquiera sean a, $b \in \mathbb{N}$ se tiene:

$$a \cdot b = b \cdot a$$

Probaremos esta propiedad en tres etapas, a saber:

i) $a \cdot 1 = 1 \cdot a$

ii) $b' \cdot a = b \cdot a + a$

iii) $a \cdot b = b \cdot a$

Para i) se tiene:

Sea A el conjunto de los $x \in \mathbb{N}$ tales que,

$$x \cdot 1 = 1 \cdot x$$

Es inmediato que $1 \in A$, porque evidentemente

$$1 \cdot 1 = 1 \cdot 1$$

es verdad.

Supongamos ahora $x \in A$, esto es

$$x \cdot 1 = 1 \cdot x \quad \text{(hipótesis de inducción)}$$

y probaremos que también $x' \in A$.

En efecto, teniendo en cuenta esta hipótesis y las definiciones (*) y (**) de adición y multiplicación, se tiene:

$$1 \cdot x' = 1 \cdot x + 1 = x \cdot 1 + 1 = x + 1 = x' = x' \cdot 1$$

luego, $x' \in A$.

En virtud del Ax. 5) resulta $A = \mathbb{N}$.

Por lo tanto, $a \in \mathbb{N}$ implica $a \in A$, y por esto se tiene

$$a \cdot 1 = 1 \cdot a, \quad \forall\, a \in \mathbb{N}$$

es decir, que 1 conmuta con cualquier elemento de $\mathbb{N}$ respecto a la multiplicación.

Para ii) se tiene:

Sea A el conjunto de los $x \in \mathbb{N}$ tales que,

$$b' \cdot x = b \cdot x + x$$

$1 \in A$, puesto que:

$$b' \cdot 1 = 1 \cdot b' = 1 \cdot b + 1 = b + 1 + 1$$
$$\text{i)} \qquad (**) \qquad \text{i)}$$

Sea ahora $x \in A$, es decir

$$b' \cdot x = b \cdot x + x \text{ (hipótesis de inducción)}$$

Utilizando esta hipótesis, las definiciones (*) y (**), la propiedad asociativa y conmutativa de la adición, se tiene:

$$b' \cdot x' = b'x + b' = (bx + x) + b' = bx + (x + b') =$$
$$(**) \qquad (**)$$

$$= bx + (x + b)' = bx + (b + x)' = bx + (b + x') =$$

$$= (bx + b) + x' = bx' + x'$$
$$(**)$$

luego, $x' \in A$.

En virtud del Ax. 5) resulta $A = \mathbb{N}$. Por lo tanto, $a \in \mathbb{N}$ implica $a \in A$ y por esto se verifica la propiedad:

$$b'a = b \cdot a + a$$

Para iii) se tiene:

Sea A el conjunto de los $x \in \mathbb{N}$ tales que,

$$a \cdot x = x \cdot a$$

Por i) resulta $1 \in A$.

Sea ahora $x \in A$, y teniendo en cuenta esta hipótesis, la definición (**) y la propiedad ii) recién probada, se puede escribir:

$$a \cdot x' = a \cdot x + a = x \cdot a + a = x' \cdot a$$
$$(**) \qquad \text{(ii)}$$

luego, $x' \in A$.

Por Ax. 5) resulta entonces que $A = \mathbb{N}$.

Por lo tanto, $b \in \mathbb{N}$ implica $b \in A$ y por esto resulta la propiedad conmutativa de la multiplicación.

$$ab = ba, \quad \forall\, a, b \in \mathbb{N}$$

2) Cualesquiera sean $a, b, c \in \mathbb{N}$ se verifica la propiedad:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

En efecto, sea A el conjunto de los $x \in \mathbb{N}$ tales que,

$$a(b + x) = a \cdot b + a \cdot x$$

siendo a, b números naturales arbitrarios fijados de antemano.

Tenemos $1 \in A$, puesto que:

$$a(b + 1) = a \cdot b' = a \cdot b + a = a \cdot b + a \cdot 1$$

Sea ahora $x \in A$, esto es:

$$a(b + x) = a \cdot b + a \cdot x \text{ (hipótesis de inducción)}$$

Utilizando esta hipótesis y las definiciones (*) y (**), se tiene:

$$a(b+x') = a\cdot(b+x)' = a(b+x) + a = ab + ax + a =$$
$$\text{(**)} \qquad \text{(**)}$$
$$= ab + ax'$$
$$\text{(**)}$$

luego, $x' \in A$.

Hemos probado así que A posee todas las propiedades del Ax. 5); luego, $A = \mathbb{N}$.

Si $c \in \mathbb{N}$, entonces $c \in A$ y por esto resulta:

$$a(b+c) = ab + ac, \quad \forall\, a, b, c \in \mathbb{N}$$

es decir, la multiplicación es distributiva respecto a la adición.

3) Cualesquiera sea $a, b, c \in \mathbb{N}$ se cumple la propiedad:

$$(a\cdot b)\cdot c = a\cdot(b\cdot c)$$

En efecto, sea A el conjunto de los $x \in \mathbb{N}$ tales que:

$$(a\cdot b)\cdot x = a\cdot(b\cdot x)$$

Es inmediato que $1 \in A$, ya que por (**) se tiene:

$$(a\cdot b)\cdot 1 = a\cdot(b\cdot 1)$$

o sea,

$$a\cdot b = a\cdot b$$

que es verdad.

Sea ahora $x \in A$; es decir, se cumple

$$(a\cdot b)\cdot x = a\cdot(b\cdot x) \text{ (hipótesis de inducción)}$$

Utilizando esta hipótesis, la definición (**) y la propiedad distributiva, se puede escribir:

$$(a\cdot b)\cdot x' = (a\cdot b)\cdot x + a\cdot b = a\cdot(b\cdot x) + a\cdot b =$$
$$\text{(**)}$$
$$= a(b\cdot x + b) = a\cdot(b\cdot x')$$
$$\text{(**)}$$

luego, $x' \in A$.

De las propiedades del Ax. 5) resulta entonces que $A = \mathbb{N}$. Por lo tanto, si $c \in \mathbb{N}$ entonces $c \in A$ y por esto resulta

$$(a\cdot b)\cdot c = a\cdot(b\cdot c), \ \forall\, a, b, c \in \mathbb{N}$$

que es la propiedad asociativa de la multiplicación en el conjunto $\mathbb{N}$ de los números naturales.

Este último resultado y los anteriores, demuestran el teorema.

Tabla de Multiplicación. La formación de una tabla de multiplicar se deduce de las definiciones dadas por las fórmulas:

$$\begin{cases} a\cdot 1 = a \\ a\cdot b' = a\cdot b + a \end{cases}$$

Se trata, como puede notarse, de una definición por inducción completa: la primera fórmula define la operación de multiplicar por 1 a un número cualquiera; la segunda, define la operación de multiplicar por el siguiente de un número natural cuando ya se sabe multiplicar por éste. Por lo tanto, sabiendo multiplicar por 1, sabremos multiplicar por 2; pudiendo multiplicar por 2 podremos multiplicar por 3, y así indefinidamente.

Veamos, por ejemplo, cómo se forma la tabla del 2. Tenemos en este caso $a = 2$, luego:

$$2\cdot 1 = 2$$
$$2\cdot 2 = 2\cdot 1' = 2\cdot 1 + 2 = 2 + 2 = 4$$
$$2\cdot 3 = 2\cdot 2' = 2\cdot 2 + 2 = 4 + 2 = 6$$
$$2\cdot 4 = 2\cdot 3' = 2\cdot 3 + 2 = 6 + 2 = 8$$

Observación importante. En la teoría de Peano que estamos desarrollando, vemos que el cero, indicado por el símbolo 0, no aparece como número natural. Sin embargo, ella puede desarrollarse en otra forma de modo que lo contenga. Para ello no hay que hacer ningún cambio en los axiomas, salvo el puramente formal de reemplazar el signo 1 por el signo 0 en los enunciados de los mismos; pero en cambio hay que modificar las definiciones de las operaciones en las que el papel del cero no es ahora siguiente de ningún otro, cambia radicalmente. Estas definiciones toman ahora la forma siguiente:

$$\begin{cases} a + 0 = a \\ a + b' = (a+b)' \end{cases} \quad ; \quad \begin{cases} a\cdot 0 = 0 \\ a\cdot b' = ab + a \end{cases}$$

Por otra parte, la teoría se sigue desarrollando como lo hemos hecho hasta ahora, jugando en toda ella, igualmente un papel importante en las propiedades de las operaciones, el principio de inducción completa.

En esta nueva forma de desarrollo se define el 1 como el siguiente del 0, y se tiene:

$$a + 1 = a + 0' = (a + 0)' = a'$$
$$a \cdot 1 = a \cdot 0' = a \cdot 0 + a = 0 + a = a$$

es decir, que se demuestran las reglas que en nuestra teoría y desarrollo anterior admitíamos por definición.

EJERCICIOS

1) Para todo $a, b \in \mathbb{N}$, probar que se verifican las igualdades siguientes:

a) $(a + b')' = a' + b'$

b) $a' + b' = (a + b)' + 1$

c) $(a \cdot b')' = a \cdot b + a'$

d) $(a' \cdot b')' = a' + a \cdot b + b'$

e) $a' \cdot b' = (a \cdot b)' + a + b$

2) Demostrar que la suma de dos números naturales es un número natural (Ley de clausura para la adición).
(Sugerencia: Fije uno de los sumandos y haga en seguida una inducción sobre el otro).

3) Demostrar que el producto de dos números naturales es un número natural (Ley de clausura para la multiplicación).
(Sugerencia: Fije uno de los factores y haga en seguida una inducción sobre el otro).

4) Conocida la ley conmutativa de la adición, probar la ley asociativa:

$$(a + b) + c = a + (b + c)$$

por medio de una inducción sobre b.

5) Probar la ley distributiva de la multiplicación respecto a la adición:

$$a(b + c) = a \cdot b + a \cdot c$$

mediante una inducción sobre a.

6) Demostrar, por inducción, la proposición siguiente:

$$a \neq b \Longrightarrow a + c \neq b + c, \quad \forall a, b, c \in \mathbb{N}$$

7) Demostrar por inducción que,

$$1 \cdot a = a, \quad \forall a \in \mathbb{N}$$

8) Demostrar que para todo a, b, c, $d \in \mathbb{N}$ se verifican las igualdades siguientes:

a) $a(b + c + d) = ab + ac + ad$

b) $(a + b) \cdot (c + d) = ac + bc + ad + bd$

En general, probar que se verifican:

c) $a(b_1 + b_2 + \ldots + b_m) = ab_1 + ab_2 + \ldots + ab_m$

d) $(a_1 + \ldots + a_n)(b_1 + \ldots + b_m) = a_1b_1 + a_1b_2 + \ldots + a_1b_m +$
$$= a_2b_1 + a_2b_2 + \ldots + a_26_m +$$
$$= a_nb_1 + a_nb_2 + \ldots + a_nb_m$$

7.2. *Ordenación de los números naturales*

Teorema. Dados dos números naturales cualesquiera, a y b siempre se presenta uno, y sólo uno, de los tres casos siguientes:

1) $a = b$

2) Existe $x \in \mathbb{N}$ tal que $a + x = b$

3) Existe $y \in \mathbb{N}$ tal que $a = b + y$

Demostración. 1) Mostraremos primeramente que no pueden presentarse simultáneamente dos de los casos 1), 2) y 3).

En efecto, por el método de reducción al absurdo, tendremos:

Supongamos que se verificaran al mismo tiempo 1) y 2), esto es:

$$\begin{cases} a = b \\ a + x = b \end{cases}$$

lo cual implica,

$$a + x = a$$

imposible por la propiedad bien conocida de la adición que es:

$$a + b \neq b$$

Análogamente, si se verificaran a la vez 1) y 3), se tendría:

$$\begin{cases} a = b \\ a = b + y \end{cases}$$

lo cual implica,

$$b = b + y$$

absurdo, en virtud de la misma propiedad: $a + b \neq b$.

Por último, supongamos ahora que se verificaran al mismo tiempo los casos 2) y 3), esto es

$$\begin{cases} a + x = b \\ a = b + y \end{cases}$$

lo cual implica,

$$a = a + (x + y)$$

también imposible por esa misma propiedad de la adición y que es: la suma es distinta de cada sumando.

Así hemos demostrado en primer lugar que los tres casos 1), 2) y 3) se excluyen mutuamente; es decir, si se verifica uno de ellos, los otros dos no tienen lugar.

II) En segundo lugar, mostraremos ahora que para cada par a y b en IN se presenta efectivamente uno de los casos 1), 2) y 3).

En efecto, sea $a \in \mathbb{N}$ dado, y sea A el conjunto de los $b \in \mathbb{N}$ para los que se presenta uno de los casos 1), 2) y 3).

Si fuese $a = 1$, basta tomar $b = 1$ para tener el caso 1), esto es $a = b$.

Pero, si fuese $a \neq 1$, entonces existe $b \in \mathbb{N}$ tal que

$$a = b' = b + 1$$

lo cual satisfará el caso 3).

Luego, en ambos casos, $a = 1$, ó $a \neq 1$, resulta $1 \in A$.

Supongamos ahora $b \in A$ y probaremos que también $b' \in A$.

En efecto, examinemos los tres casos posibles:

a) $a = b$

Entonces, $a' = b'$, o sea $a + 1 = b'$; es decir b' satisface el caso 2); por tanto $b' \in A$.

b) $b = a + x$

Entonces, $b' = (a + x)' = a + x'$; es decir, b' satisface el caso 2), y por tanto, $b' \in A$.

c) $b + y = a$

Entonces, $(b + y)' = a \Rightarrow b' + y = a + 1$

Hay dos casos que contemplar:

$b' + y = a + 1$ { Si $y = 1$, entonces $b' = a$; o sea, b' satisface 1)
Si $y \neq 1$, entonces existe $c \in \mathbb{N}$ tal que $y = c' = c + 1 \Rightarrow$ $b' + c = a$, o sea b' satisface el caso 3).

Luego, en todos los casos resulta $b' \in A$; luego, por Ax. 5), $A = \mathbb{N}$.

Así hemos probado que para cada par dado de números naturales

se presenta uno, y sólo uno, de los casos 1), 2) y 3); el teorema está demostrado.

Una de las consecuencias más importantes de este teorema que acabamos de demostrar, es la posibilidad de definir una relación de orden entre los números naturales

Definición. Para dos números naturales, a y b, definimos la relación siguiente:

$$a < b, \text{ equivalente a, } b > a$$

si, y sólo si existe $x \in \mathbb{N}$ tal que, $a + x = b$.

De modo que:

$$a < b \Longleftrightarrow \exists\ x \in \mathbb{N} \text{ tal que } a + x = b$$

La relación "$<$", que se lee: "menor que...", se llamará de ORDEN en IN.

Teorema. Nuestra relación de orden "$<$" tiene las propiedades siguientes:

1) $a < b$ y $b < c \Rightarrow a < c$ (transitiva)

2) Para cada par (a, b) de elementos de IN se presenta uno y sólo uno de los tres casos siguientes:

$$a = b, a < b, b < a \text{ (Ley de Tricotomía)}$$

Demostración: 1) Sea $a < b$ y $b < c$; entonces por la definición de la relación "$<$" existen x e y en IN tales que;

$$\begin{aligned} a + x &= b \\ b + y &= c \end{aligned}$$

lo que implica,

$$a + (x + y) = c$$

luego,

$$a < c$$

2) Es una traducción de la parte II del teorema anterior.

Definiciones: 1) El orden "$<$" se llamará el *Orden Natural de* IN; su opuesto "$>$", el *Orden Natural de* IN.

2) Una consecuencia de la definición del orden natural "$<$" de IN es que siempre se tiene:

$$a < a + b$$

y en particular, para b = 1 resulta:

$$a < a'$$

es decir, todo número natural es menor que su siguiente o sucesor.

3) La negación de $a > b$, es por la ley de tricotomía, la relación $a \leq b$, que significará por esto las dos alternativas siguientes:

$$\text{ó es } a < b, \quad \text{ó es } a = b$$

Luego,

$$\boxed{a \leq b \Longleftrightarrow a < b, \text{ ó } a = b}$$

4) Asimismo, la negación de $a < b$ es, por la ley de tricotomía, la relación $a \geq b$, que significará, por consiguiente, las dos alternativas:

$$\text{ó es } a > b, \quad \text{ó es } a = b$$

Por lo tanto,

$$\boxed{a \geq b \Longleftrightarrow a > b, \text{ ó } a = b}$$

Teorema. La relación "$\leq$" tiene las propiedades siguientes:

1) $a \leq a$ (reflexiva)

2) $a \leq b$ y $b \leq a \Rightarrow a = b$ (antisimétrica)

3) $a \leq b$ y $b \leq c \Rightarrow a \leq c$ (transitiva)

4) $\forall$ a, b se tiene siempre $a \leq b$ ó $b \leq a$ (lineal)

Es decir, la relación "$\leq$" es de orden total en IN.

Demostración. Tenemos:

1) $a \leq a$ significa como sabemos que:

$$\text{o bien es } a < a, \text{ o bien es } a = a$$

la primera alternativa es falsa y la segunda es verdadera; luego, la disjunción $a \leq a$ es verdadera para todo $a \in$ IN.

2) Si $a \leq b$ y $b \leq a$, entonces sólo caben las combinaciones siguientes:

$$\begin{cases} a < b \\ b < a \end{cases} ; \quad \begin{cases} a < b \\ b = a \end{cases} ; \quad \begin{cases} a = b \\ b < a \end{cases} ; \quad \begin{cases} a = b \\ b = a \end{cases}$$

sólo la última es verdadera y las otras tres son incompatibles; luego,

$$a \leq b \text{ y } b \leq a \Rightarrow a = b$$

3) Sean $a \leq b$ y $b \leq c$; entonces bastará que sólo probemos que $a < b$ y

$b < c \Rightarrow a < c$, y lo cual es cierto en virtud de la propiedad transitiva de la relación "$<$"; luego, $a \leq b$ y $b \leq c \Rightarrow a \leq c$.

Por consiguiente, la relación "$\leq$" en el conjunto IN de los números naturales, es una relación de orden total, o cadena.

Teorema. La relación "$<$" es transitiva, pero no reflexiva ni simétrica.

Demostración. Tenemos:

i) Sea $a < b$ y $b < c$; entonces, por la definición de la relación "$<$" en IN, existen $x, y \in$ IN tales que:

$$\begin{aligned} a + x &= b \\ b + y &= c \end{aligned}$$

lo que implica,

$$a + (x + y) = c$$

de donde,

$$a < c$$

Así pues, $a < b$ y $b < c \Rightarrow a < c$ (transitiva)

ii) Sea $a \in$ IN arbitrario.

Como $a < a$ es falso, porque si fuera verdadera existiría algún $x \in$ IN tal que,

$$a + x = a$$

en contradicción a la propiedad $a + b \neq b$ de la adición. Luego, la relación "$<$" no es reflexiva.

iii) Por último, sean $a, b \in$ IN y supongamos que se tuviese $a < b$ y $b < a$.

Ahora bien, como "$<$" es transitiva, resulta:

$$a < b \text{ y } b < a \Rightarrow a < a$$

en contradicción con lo probado en ii).

Luego, la relación "$<$" no es simétrica.

Teorema. En IN se verifica:

1) $x \geq 1, \forall x \in$ IN

O sea, 1 es el primer elemento de IN.

2) $x < y \Rightarrow x + 1 \leq y$

En particular, no hay números naturales entre los números $x, x + 1$.

Demostración:

a) Sea $x \in \mathbb{N}$, $x \neq 1$; luego, por Teorema 3), existe $y \in \mathbb{N}$ tal que: $x = y' = y + 1 \Rightarrow x > 1$.

Luego, 1 es el primer elemento de $\mathbb{N}$.

b) Sea ahora $x < y$; entonces existe $a \in \mathbb{N}$ tal que,

$$x + a = y$$

Si $a = 1$, entonces es $x + 1 = y$

Si $a \neq 1$, entonces existe $b \in \mathbb{N}$ tal que,

$$a = b' = b + 1$$

luego, $$x + a = x + b + 1 = y$$

o bien, $$(x + 1) + b = y$$

lo que implica, $$x + 1 < y$$

Por consiguiente, $x < y \Rightarrow x + 1 \leq y$

En particular, como es:

$$x < x'$$

o sea, $$x < x + 1$$

resulta entonces, por la propiedad que se acaba de demostrar, que la relación $x < x + 1$ sólo puede implicar la igualdad:

$$x + 1 = x + 1$$

es decir, no hay números naturales entre los naturales x, $x + 1$.

Diremos en este caso que los número x, $x + 1$ son consecutivos.

Luego, el concepto de "siguiente de..." en la teoría de Peano coincide con el concepto general de "Siguiente de" o "consecutivos" de la teoría de conjuntos ordenados. En consecuencia, en virtud de este hecho y del teorema recién probado, podemos enunciar la propiedad siguiente: "El conjunto ordenado de los números naturales, tiene a 1 como primer elemento, carece de último elemento (porque cada número tiene un siguiente), un número y su siguiente son elementos consecutivos y todo elemento distinto de 1 tiene un precedente (ya que si $a \neq 1$, existe $b \in \mathbb{N}$ tal que $a = b'$).

Teorema. Los números naturales poseen con respecto a su orden natural "$<$", la propiedad siguiente:

Si se tiene $a < b$, entonces existe un número natural n tal que,

$$a\,n > b \text{ (Teorema de Arquímedes)}$$

Demostración. Si fuese $a = 1$, basta tomar $n = b'$, ya que

$$a \cdot b' = 1 \cdot b' = b' > b$$

Ahora, si fuese $a \neq 1$, basta tomar $n = b$, ya que

$$a > 1 \Rightarrow a = 1 + x \Rightarrow ab = b + bx \Rightarrow ab > b$$

Llamaremos ARQUIMEDIANA a esta propiedad del conjunto ordenado de los números naturales. Más adelante se verá que de esta misma propiedad gozan también los demás sistemas de números: enteros, racionales y reales, que pronto estudiaremos.

EJERCICIOS

1) Demostrar que las relaciones $a < b$; $a = b$; $a > b$, implican respectivamente las relaciones:

$$a + c < b + c;\ a + c = b + c;\ a + c > b + c$$

Probar, además, que estas últimas implican respectivamente las primeras.

2) Demostrar que las relaciones $a < b$; $a = b$; $a > b$, implican respectivamente las relaciones:

$$ac < bc;\ ac = bc;\ ac > bc$$

Demostrar, además, que estas últimas implican respectivamente las primeras.

3) Demostrar las propiedades siguientes:

a) $a < b \text{ y } c < d \Rightarrow a + c < b + d$

b) $a < b \text{ y } c \leq d \Rightarrow a + c < b + d$

c) $a \leq b \text{ y } c < d \Rightarrow a + c < b + d$

d) $a \leq b \text{ y } c \leq d \Rightarrow a + c \leq b + d$

4) Probar las propiedades siguientes:

a) $a > b \text{ y } c > d \Rightarrow a + c > b + d$

b) $a > b \text{ y } c > d \Rightarrow a + c > b + d$

c) $a \leq b \text{ y } c > d \Rightarrow a + c > b + d$

d) $a \geq b \text{ y } c \geq d \Rightarrow a + c \geq b + d$

5) Demostrar las propiedades siguientes:

a) $a<b \text{ y } c<d \Rightarrow ac<bd$

b) $a<b \text{ y } c\leq d \Rightarrow ac<bd$

c) $a\leq b \text{ y } c<d \Rightarrow ac<bd$

d) $a\leq b \text{ y } c\leq d \Rightarrow ac\leq bd$

6) Probar las propiedades siguientes:

a) $a>b \text{ y } c>d \Rightarrow ac>bd$

b) $a>b \text{ y } c\geq d \Rightarrow ac>bd$

c) $a\geq b \text{ y } c>d \Rightarrow ac>bd$

d) $a\geq b \text{ y } c\geq d \Rightarrow ac\geq bd$

7) Demostrar que si en $\mathbb{N}$ se tiene $a\cdot b=1$, entonces es $a=1$ y $b=1$.

8) Sean $a, b\in \mathbb{N}$ tales que $a<b$. Probar que se verifica:

$$a^2 < a\cdot b < b^2$$

9) Sean $a, b\in \mathbb{N}$. Demostrar que se verifica:

a) Si $a=b$, entonces $c'\cdot a>b$, $\forall c\in \mathbb{N}$

b) Si $c'a=b$ para algún $c\in \mathbb{N}$, entonces es $a<b$.

7.3. *Principio del Mínimo Entero Positivo o de Buena Ordenación del conjunto ordenado* $\mathbb{N}$.

Consideremos los siguientes conjuntos de números naturales:

$A = \{5, 7, 9, 11, 13, 15, \ldots\}$
$B = \{8, 9, 10, 11, 12, 13, 14, 15\}$
$C = \{6, 8, 10, 12, 14, 16, \ldots\}$
$D = \{2, 3, 5, 7, 11, 13, 17, 19\}$

Estos ejemplos nos muestran que si bien los conjuntos no vacíos de números naturales, o de enteros positivos, pueden no tener un elemento mayor que todos los demás, como ocurre en A y C, en cambio, siempre tienen un elemento que es menor que todos los demás, sucede en A donde el mínimo es 5, 8 en B, 6 en C y 2 en D.

Intuitivamente parece evidente que cualquier conjunto no vacío S de números naturales o enteros positivos debe tener un elemento mínimo, es decir, menor que todos los demás.

Efectivamente, sea n un elemento de S.

Si $1\in S$, entonces evidentemente 1 es el mínimo elemento de S.

Si $1\notin S$ pero $2\in S$, entonces será 2 el mínimo elemento de S.

Si 1 y 2 no pertenecen a S y $3\in S$, entonces 3 será su mínimo elemento.

Reiterando este razonamiento, se llegará "al cabo de n pasos", esto es, después de n pasos alcanzaremos el elemento n que pertenece a S y este número será el mínimo elemento del conjunto S.

Sin embargo, este razonamiento no puede considerarse como una demostración matemática mientras no se dé rigurosamente el significado de la expresión "al cabo de n pasos". Esto nos obligará a aceptar explícitamente como axioma, la proposición siguiente:

Principio del Mínimo Entero Positivo: "Cada subconjunto no vacío S de $\mathbb{N}$ tiene un número mínimo; es decir, tiene un primer elemento menor o igual a todos los demás".

Este principio es un monopolio de los números naturales; es decir, no es compartido, en general, por otros sistemas de números y puede ser sorprendentemente útil para la demostración de Teoremas.

Para destacar la fuerza de este principio, demostraremos, a modo de aplicación, las proposiciones siguientes:

Proposición 1) Sea $\mathbb{N}_0=\{0, 1, 2, 3, \ldots\}$ el conjunto de los números naturales que incluye al cero como número natural. Entonces:

a) No existe ningún número natural comprendido entre 0 y 1.

b) No existe ningún número natural comprendido entre a, $a+1$, ni entre $a-1$, a, siendo a un número natural cualquiera distinto de 1.

Demostración. Todo esto se ve inmediatamente sin más que echar una ojeada al orden natural de $\mathbb{N}_0$:

$$0, 1, 2, 3, \ldots, a-1, a, a+1, \ldots$$

pero lo que pretendemos es probar la proposición utilizando el Principio de Mínimo, sin necesidad de acudir a la referida serie fundamental de los números naturales ordenados por la relación "siguiente de...".

Daremos una demostración indirecta de la proposición; es decir, una prueba por reducción al absurdo.

a) En efecto, supongamos que hay algún número natural b tal que:

$$0<b<1$$

entonces, el conjunto S de tales números naturales no es vacío. Luego, por el principio de mínimo, hay un número natural mínimo m en este conjunto y será:

$$0<m<1$$

Multiplicando esta doble desigualdad por m resultará:

$$0 < m^2 < m < 1$$

Entonces, m^2 es otro número del conjunto S y menor que el supuesto elemeno mínimo m de S.

Esta contradicción, demuestra la propiedad a).

b) Sea ahora $a \in \mathbb{N}$ cualquiera; $a \neq 1$.

Probaremos entonces que no hay ningún número natural c tal que:

$$\text{i)} \qquad a < c < a + 1$$

y ningún número natural d tal que:

$$\text{ii)} \qquad a - 1 < d < a$$

En efecto, en la hipótesis de que existiera, se tendría restando *a* a los tres miembros de i):

$$0 < c - a < 1$$

resultado contrario a la propiedad a) anteriormente demostrada.

Sumando 1 a los tres miembros de ii), se tiene:

$$a < c + 1 < a + 1$$

contra lo que se acaba de establecer.

Este resultado y el anterior demuestran la proposición.

Proposición 2). Un conjunto S de números naturales que contenga al 1 y que contenga al $n+1$ siempre que contenga al n, contiene a todos los números naturales.

Demostración. Nótese que esta proposición no es otra que el Ax. 5) de Peano y que ahora será probado como teorema, si aceptamos como axioma el Principio del Mínimo Entero Positivo.

En efecto, la proposición en cuestión quedará demostrada si logramos probar que el conjunto S' de todos los números naturales no contenidos en S es vacío.

$$S' = \mathbb{N} - S$$

Supongamos, por el contrario, que S' no es vacío; entonces contendrá un elemento mínimo m.

$$m \in S'$$

Por la hipótesis, resulta que $m \neq 1$, porque $1 \in S$. Por la proposición 1) será $m > 1$; luego, $m - 1 > 0$. Por otro lado, como es

$$m - 1 < m$$

resultará por la definición de m, que $m - 1 \in S$.

Entonces, se deduce de la hipótesis que,

$$(m - 1) + 1 = m$$

estará en S, lo que es falso.

Esta contradicción demuestra la proposición.

Observación. Esta proposición, o Ax. 5) de Peano, como se sabe, constituye el Principio de la Inducción Matemática, o el Principio de Inducción Completa, y que en otra forma de enunciado es:

"Asociemos a cada entero positivo n una propiedad P(n), la cual puede ser verdadera o falsa. Entonces:

Si, primero, P(1) es verdadera y, segundo, para cualquier entero positivo K la verdad de P(K) implica la verdad de P(K +1), entonces la propiedad P(n), será verdadera para todo entero positivo n".

Demostración. Sea S el conjunto de todos los números naturales para los cuales P(n) es verdadera. De acuerdo con las hipótesis hechas, el conjunto S verifica las dos condiciones siguientes:

1) $1 \in S$

2) si $K \in S$, entonces $K + 1 \in S$

Luego, por la Proposición 2), resulta $S = \mathbb{N}$, es decir, P(n) es verdadera para todos los números naturales.

Observación. La demostración del Principio de Inducción que se acaba de hacer, ha sido posible si aceptamos como axioma el Principio de Mínimo. Recíprocamente, es posible demostrar este último si aceptamos como axioma el Principio de Inducción.

Esto significa entonces que entre ambos axiomas existe una relación de dependencia, esto es, que si uno de los dos principios es cierto, necesariamente el otro también lo es. Así, pues:

Teorema. Si el Principio de Inducción Completa es cierto, también lo es del Mínimo Entero Positivo.

Demostración. Deberemos probar que en todo conjunto no vacío S de números naturales existe un elemento mínimo —evidentemente úni-

co— es decir, un elemento de S menor que todos los demás números de S, si existen.

En efecto, definamos para cada número natural K, el conjunto siguiente:

$$S(K) = \{1, 2, 3, \ldots, K\} \cap S$$

Es claro que si, por ejemplo, $K \in S$, entonces $S(K)$ no es vacío. Por lo tanto, hay al menos un $S(K)$ no vacío.

Ahora, si $S(1)$ no es vacío, entonces $1 \in S$ y 1 es evidentemente el mínimo elemento de S. Si $S(1) = \phi$ pero $S(2)$ no es vacío, entonces $2 \in S$ y 2 será el mínimo elemento de S. Si $S(1) = \phi$ y $S(2) = \phi$ y $S(3)$ no es vacío, entonces $3 \in S$ y 3 será el mínimo elemento, etc.

Sea, pues, $S(1) = \phi$. Si siendo $S(K) = \phi$, lo fuera también $S(K+1)$, para cualquier entero positivo K, entonces por el Principio de Inducción todos los $S(K)$ serían vacíos y lo cual es falso.

Esta contradicción prueba que existe un número natural K tal que $S(K)$ es vacío, pero $S(K+1)$ no lo es.

Es claro entonces que $m = k+1 \in S$ y $m \leq a$, $\forall a \in S$; es decir, m es el mínimo elemento de S, y el teorema está demostrado.

En consecuencia, ambos principios, el de mínimo y el de inducción, son equivalentes en el sentido que aceptando uno cualquiera de ellos como axioma, el otro puede demostrarse como teorema. Por lo tanto, son versiones diferentes del mismo principio y pueden usarse indistintamente. El Principio de Inducción Completa es una propiedad fundamental de los números naturales que proporciona un método de demostración llamado por INDUCCION FINITA O POR RECURRENCIA.

Así, para demostrar que todos los números naturales verifican una cierta propiedad, es suficiente:

1) demostrar que es verdadera para $n = 1$

2) suponiéndola verdadera para un entero positivo arbitrario K, intentaremos probarla para el siguiente $K + 1$.

Si esta última es verdadera, entonces la propiedad en cuestión será verdadera para todo entero positivo n.

Ejemplo 1) Demostrar por inducción la propiedad:

$$P(n) : 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

Demostración. Podemos comprobar fácilmente que el enunciado es verdadero para $n = 1$, puesto que:

$$1 = \frac{1 \cdot (1+1)}{2} = \frac{1 \cdot 2}{2} = \frac{2}{2} = 1 \text{ (verdadero)}$$

Asimismo se comprueba que también es verdadera para $n = 2, 3, 4, \ldots$ y de esto vamos a partir para llegar a la conclusión de que nuestra fórmula o propiedad P(n) es verdadera en todos los casos.

En efecto, para ello, supongamos que la fórmula es verdadera cuando tomamos k términos; es decir, supongamos que sea cierto que,

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2} \text{ (hipótesis de inducción)}$$

e intentaremos demostrarla para $k+1$ términos; es decir,

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2} \text{ (tesis de inducción)}$$

En efecto, por la propiedad asociativa de la adición, escribimos:

$$1 + 2 + 3 + \ldots + k + (k+1) = (1 + 2 + \ldots + k) + (k+1)$$

el primer sumando del segundo miembro, por la hipótesis de inducción hecha, se escribe en la forma $\frac{k(k+1)}{2}$; luego:

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= (k+1)\left(\frac{k}{2} + 1\right)$$

$$= \frac{(k+1)(k+2)}{2}$$

resultado que es de la misma forma del que asumimos como verdadera.

Ahora bien, como es verdadera para $n = 1$, resultará por la prueba que se acaba de hacer que también es verdadera para $n = 2$; si lo es para $n = 2$ lo será también para $n = 3$, y así sucesivamente para todo entero positivo n.

Luego, el resultado o fórmula es verdadera para cualquier número de términos.

Ejemplo 2) Demostrar que todo número natural es de la forma: $2p$, o $(2p-1)$, donde p es un número natural.

Demostración. Sea S el conjunto de todos los números naturales n tales que:

$$S = \{n \in \mathbb{N} : n = 2p, \text{ o } n = 2p - 1, \text{ donde } p \in \mathbb{N}\}$$

Tenemos:

a) $1 \in S$, ya que $1 = 2 \cdot 1 - 1$

b) Supongamos $k \in S$ y probemos que $(k+1) \in S$

En efecto, si $k \in S$ entonces $k = 2p$, o $k = 2p - 1$, $p \in \mathbb{N}$.

Si fuese $k = 2p$, entonces $k+1 = 2p+1 = 2(p+1) - 1$, $p+1 \in \mathbb{N}$. Si fuera $k = 2p - 1$ entonces $k+1 = 2p - 1 + 1 = 2p$, $p \in \mathbb{N}$. Luego, en cualquier caso resulta $k+1 \in S$; por tanto $S = \mathbb{N}$ y la proposición queda demostrada.

A los números naturales de la forma $2p$ con $p \in \mathbb{N}$ se los llama *Números pares* y a los números de la forma $2p-1$ con $p \in \mathbb{N}$, *números impares*.

De la proposición recién demostrada resulta que cualquier número natural es par o impar.

EJERCICIOS

1) Demostrar por inducción las fórmulas o propiedades siguientes:

a) $1 + 3 + 5 + \ldots + (2n-1) = n^2$

b) $2 + 4 + 6 + \ldots + 2n = n(n+1)$

c) $3 + 7 + 11 + \ldots + (4n-1) = n(2n+1)$

d) $3 + 8 + 13 + \ldots + (5n-2) = \dfrac{n(5n+1)}{2}$

e) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

f) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \dfrac{n^2(n+1)^2}{4}$

g) $2^1 + 2^2 + 2^3 + \ldots + 2^n = 2(2^n - 1)$

h) $4[1 + 5 + 5^2 + \ldots + 5^n] + 1 = 5^{n+1}$

i) $(a-1)[1 + a + a^2 + \ldots + a^n] + 1 = a^{n+1}$

2) Utilizando el principio de inducción, enunciado en la última forma vista, demostrar todas las propiedades vistas para las operaciones de adición y multiplicación (asociatividad, conmutatividad, etc.)

3) Demostrar que:

a) Si n no es múltiplo de 3, entonces la expresión:

$1 + 2^n + 2^{2n}$, es múltiplo de siete.

b) Si n no es múltiplo de 4, entonces la expresión:

$1 + 2^n + 3^n + 4^n$, es múltiplo de diez.

4) Para todo a, $n \in \mathbb{N}$ se definen las reglas siguientes:

$$\begin{cases} 1a = a \\ (n+1)a = na + a \end{cases} \quad ; \quad \begin{cases} a^1 = a \\ a^{n+1} = a^n \cdot a \end{cases}$$

siempre que $n \cdot a$ y a^n estén definidas.

Con la ayuda de estas reglas, demostrar las siguientes leyes de cálculo para múltiplos naturales y potencias de exponentes naturales:

$$\begin{cases} ma + na = (m+n)a \\ n(ma) = (nm)a \\ na + nb = n(a+b) \end{cases} \quad ; \quad \begin{cases} a^m \cdot a^n = a^{m+n} \\ (a^m)^n = a^{mn} \\ a^n \cdot b^n = (a \cdot b)^n \end{cases}$$

(Sugerencias: Fije m y haga en seguida una inducción sobre n).

5) Probar por inducción que todos los números naturales son mayores o iguales que 1; esto es,

$$1 \leq n, \quad \forall\, n \in \mathbb{N}$$

6) Por inducción, demostrar que cualquiera sea el número natural n, no existe ningún número natural entre n y $(n-1)$, ni tampoco entre n y $(n+1)$.

7) Demostrar por inducción que el conjunto $\mathbb{N}$ de los números naturales es cerrado con respecto a la adición y con respecto a la multiplicación.

8) Sea A un conjunto de números naturales que tiene las propiedades siguientes:

1) $a \in A$

2) $x \in A \Rightarrow x' \in A$

entonces, el conjunto A contiene todos los números naturales mayores o iguales a *a*.

Demostración. Si $a = 1$, entonces la proposición que acabamos de enunciar no es otra que el principio de inducción completa.

Sea ahora $a \neq 1$; entonces, por el teorema 3), es $a = c' = c + 1$.

Definamos en seguida el conjunto B de los números naturales x con la propiedad de que $c + x \in A$.

$$B = \{x \in \mathbb{N} : a \neq 1 \Rightarrow a = c' = c + 1, \text{ tal que } c + x \in A\}$$

Probaremos primeramente que $B = \mathbb{N}$.

En efecto, tenemos:

$1 \in B$, puesto que $c + 1 = c' = a \in A$, en virtud de la hipótesis 1).

Sea ahora $x \in B$; entonces $c + x \in A$, en virtud de la definición del conjunto B, y mostremos que también $x' \in B$.

En efecto, se tiene:

$$c + x' = (c + x)' \in A \text{ , en virtud de la hipótesis 2)}$$

y en virtud de la hipótesis de inducción de que $c + x \in A$; luego, $x' \in B$; por tanto, por Ax. 5) de Peano, resulta $B = \mathbb{N}$.

Probado lo anterior, sea ahora $b \geq a = c + 1 \Rightarrow b > c$; luego, $b = c + u$

Como es $B = \mathbb{N}$, resulta entonces $u \in B$ y, por lo tanto, $b = c + u \in A$.

Así hemos probado que el conjunto A contiene todos los números naturales $b \geq a$, y la proposición queda demostrada.

Como en el caso del principio de inducción completa, esta proposición puede ponerse en la forma siguiente:

"Si P es una propiedad de los números naturales que es cumplida por el número *a* y tal que, si se cumple para un número natural x se cumple también para el siguiente x', entonces la propiedad P se cumple para todos los números naturales mayores o iguales a *a*".

Demostración. Sea A el conjunto de todos los números naturales para los que la propiedad P se cumple.

De acuerdo con las hipótesis hechas, el conjunto A verifica las dos condiciones siguientes:

1) $a \in A$

2) $x \in A \Rightarrow x' \in A$

Luego, por la proposición recién probada, resulta que A contiene todos los números naturales mayores o iguales a *a;* es decir, la propiedad se cumple para todos los números naturales mayores o iguales a *a*.

Esta forma de la inducción es de uso frecuente en matemáticas. Veamos un ejemplo.

Ejemplo. Demostrar por inducción, que $n^3 > n^2 + 5n + 3$, a partir de un cierto valor de n en adelante.

Demostración. Para $n = 1, 2, 3$ la desigualdad no se verifica, pero si para $n = 4$, puesto que:

$$4^3 > 4^2 + 5 \cdot 4 + 3$$

o sea, $$64 > 16 + 20 + 3 = 39$$

Probaremos ahora que de verificarse para un valor $h \geq 4$, se verifica también para $h + 1$.

En efecto, para $n = h$ tenemos:

$$h^3 > h^2 + 5h + 3$$

y la desigualdad para $n = h + 1$ sería:

$$(h + 1)^3 > (h + 1)^2 + 5(h + 1) + 3$$

o sea, $$h^3 + (3h^2 + 3h + 1) > (h^2 + 5h + 3) + (2h + 6)$$

Por la suma de desigualdades del mismo sentido, para que sea cierto para $n = h + 1$, bastará, en virtud de la hipótesis de inducción $h^3 > h^2 + 5h + 3$, que sea

$$3h^2 + 3h + 1 > 2h + 6$$

que equivale a $$3h^2 + h > 5$$

que es evidentemente cierto para $n = h = 4, 5, 6, \ldots$

7.4. *Buena ordenación del conjunto* $\mathbb{N}$. Sabemos por definición que un conjunto E es *bien ordenado,* cuando siendo totalmente ordenado, cualquier subconjunto no vacío de E tiene primer elemento.

Ahora bien, según el principio del mínimo entero positivo, para todo par a, $b \in \mathbb{N}$ el conjunto $\{a, b\}$ tiene primer elemento; esto es, o es $a \leq b$, o es $b \leq a$.

Por consiguiente, cualquier par de elementos de $\mathbb{N}$ son comparables mediante el orden "$\leq$" que, como sabemos, es de orden total en este conjunto.

Por este motivo, concluimos que el Principio del Mínimo Entero Positivo, es de *Buena Ordenación en* $\mathbb{N}$.

7.5. *Sustracción en* $\mathbb{N}$

Teorema. Si a, b son números naturales y $a < b$, entonces la diferencia $b - a$ es un número natural.

Demostración. Lo demostraremos por inducción.

En efecto, consideremos el conjunto S de todos los números naturales a que tienen la propiedad de que para todo número natural $b > a$, la diferencia $b - a$ es un número natural.

$$S = \{a \in \mathbb{N} : \forall b \in \mathbb{N} \text{ tal que } a < b \Rightarrow b - a \in \mathbb{N}\}$$

Tenemos:

1) $1 \in S$, puesto que $1 < b$, $\forall b \in \mathbb{N}$ implica la diferencia $b - 1 \neq 0$, y por definición de IN resulta que:

$$b - 1 \in \mathbb{N}$$

2) Supongamos ahora $k \in S$; esto es, $k < b$ implica $b - k \in \mathbb{N}$.

Probaremos que también $k + 1 \in S$; es decir, tendremos que demostrar que si $b \in \mathbb{N}$ y es $k + 1 < b$, entonces $b - (k + 1) \in \mathbb{N}$.

En efecto, observando que $b - 1 \in \mathbb{N}$, puesto que $b - 1 \neq 0$ y que si $k - 1 < b$, entonces $k < b - 1$, y por esto resulta que $(b - 1) - k \in \mathbb{N}$.

Pero, $(b - 1) - k = b - (k + 1)$, o sea, $b - (k + 1) \in \mathbb{N}$.

Luego, $S = \mathbb{N}$.

Este teorema nos enseña que la condición de posibilidad de la operación sustracción en IN, es que el minuendo b sea mayor que el sustraendo a.

Cumplida esta condición, probaremos que la sustración es una operación bien definida en IN; esto es, que existe y es único.

La existencia queda probada por el teorema recién demostrado. Probaremos sólo la unicidad.

Sea $a < b$ y supongamos que se tuviese:

$$b - a = d_1 \text{ y } b - a = d_2$$

lo que implica, $$a + d_1 = a + d_2$$

o sea, $$d_1 = d_2$$

lo cual es falso en virtud de la hipótesis hecha.

Esta contradicción demuestra la unicidad de la operación sustracción.

Con los resultados ahora establecidos, hemos puesto las bases para el desarrollo de la teoría aritmética de los números naturales en forma clara y rigurosa.

Las propiedades de la teoría de la divisibilidad, máximo común divisor y mínimo común múltiplo, la teoría de los números primos y la de las congruencias numéricas —todas desarrolladas en el TOMO I de estos apuntes— se deducen claras y rigurosamente de las propiedades que hemos demostrado en el presente capítulo.

Tampoco presenta dificultades la teoría de la numeración en un sistema de base cualquiera.

Capítulo VIII

EL PROBLEMA DE AMPLIACION Y EL METODO GENETICO

8.0. Sabemos que la operación de sustracción no es cerrrada en $\mathbb{N}$; esto es, que la ecuación

$$a + x = b, \quad \text{con } a, b \in \mathbb{N}$$

no tiene siempre solución en $\mathbb{N}$.

Para que esta ecuación sea siempre soluble es preciso ampliar el conjunto $\mathbb{N}$, introduciendo o creando los números enteros $\mathbb{Z}$.

Algo análogo a lo que ocurre con la resta en el conjunto $\mathbb{N}$ sucede con la operación de división en el conjunto $\mathbb{Z}$ de los números enteros, pues la ecuación

$$b x = a, \text{ con } a, \ b \in \mathbb{Z}, b \neq 0$$

no tiene siempre solución en $\mathbb{Z}$.

Para que esta última ecuación sea siempre soluble es preciso ampliar el conjunto $\mathbb{Z}$, introduciendo o inventando los números racionales.

Sólo en el sistema de los números racionales $\mathbb{Q}$ es posible resolver siempre la ecuación,

$$b x + c = a$$

donde a, b, c son números enteros y $b \neq 0$.

En este campo de los números racionales es siempre posible la operación de potenciación con exponente entero, pero no siempre la radicación que es una de sus inversas. Este hecho condujo a la introducción o creación de los números irracionales $\mathbb{I}$. Estos nuevos números permiten resolver la ecuación

$$x^n = a$$

donde n es un entero y *a* un racional no negativo.

El sistema de los números racionales ampliado con el sistema de los números irracionales recibe el nombre de sistema de los números reales y que se lo denota por $\mathbb{R}$. Luego,

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} = \mathbb{Q} + \mathbb{I}$$

Por útimo, para hacer posible la resolución de la ecuación,

$$x^n = a$$

en el caso que a sea negativo, es preciso complicar el sistema de los nú-

meros reales introduciendo o creando los números imaginarios y complejos $\mathbb{C}$.

Así, pues, como lo acabamos de ver, las operaciones inversas nos han conducido, en este caso especial, por sucesivas adjunciones a ampliar el concepto de número natural hasta alcanzar el concepto de número real o aún el del número complejo.

Con respecto a estas adjunciones o creaciones conviene observar lo siguiente:

1) Los nuevos números que se introducen se construyen libremente, o sea, se inventan; es decir, surgen como el resultado de un acto de creación matemática. Para ello es necesario definir de manera no contradictoria la igualdad de dos de estos entes nuevos y también las reglas operatorias que ellos verifican.

2) Siendo la adjunción de los números enteros, racionales, reales y complejos un acto de libre creación, cabe preguntarse si no será posible inventar otros sistemas de entes, diferentes de los números reales o complejos, entre los que estén definidas operaciones y propiedades completamente arbitrarias, pero no contradictorias. La respuesta es afirmativa; por ejemplo, la construcción de los números hipercomplejos.

En general, cualquier sistema nuevo que se invente, por arbitrario que él sea, será una teoría matemática siempre que sea lógicamente correcto y sus creaciones resulten de una necesidad en el tratamiento de ciertos problemas o en la unificación de teorías ya existentes. Por ejemplo, los números reales fueron introducidos en Matemática para expresar mediante números las magnitudes que varían "continuamente", y que se presentan en problemas de geometría, de mecánica, etc.

A este respecto, Poincaré ha dicho: "Si bien hemos inventado "*el continuo*", éste nos fue impuesto por el mundo exterior".

Por otra parte, una de las razones por las que tiene gran interés la creación de nuevos sistemas, es que la introducción de nuevos elementos permite estudiar mejor los elementos ya conocidos o antiguos. En general, muchas veces se hace necesario pasar a un campo más amplio para estudiar ciertas propiedades del campo original. Los ejemplos son numerosos a este respecto. Por consiguiente, pasar a un campo más amplio permite colocarse en un punto de vista más general, que abre, por esto, nuevas posibilidades.

En resumen:

Llamaremos METODO GENETICO, al método empleado modernamente para el desarrollo y estudio metódico y ordenado de la Aritmética.

Partiendo de la teoría de conjuntos se define el llamado NUMERO NATURAL, o bien se introduce su existencia axiomáticamente, como lo hace Peano.

En seguida se establecen los conceptos de igualdad y desigualdad con esta clase de números; se definen después todas las operaciones que con ellos pueden efectuarse, estableciendo y demostrando las leyes formales de cada operación; y como consecuencia inmediata de estas definiciones y leyes, se deducen las reglas para operar, con independencia de la expresión simbólica que para cada número se adopte.

De este modo se desarrolla la parte que pudiéramos llamar, *Aritmética del Número Natural*, en la cual, y debido al restringido concepto del número, se hacen imposibles varias operaciones (sustracción, y división), cuando los datos no cumplen determinadas condiciones.

A fin de hacer posible algunas de estas operaciones, se amplía el concepto restringido del llamado número natural, ideando o inventando otros entes abstractos denominados *números negativos* y el conjunto de éstos y el de los números naturales del conjunto primitivo, constituye el llamado SISTEMA DE LOS NUMEROS ENTEROS que da lugar al estudio de la segunda parte de la aritmética y que pudiéramos llamar, *Aritmética del Número Entero*, en la cual, y debido al restringido concepto del número, se hace imposible la operación de división, cuando los datos no cumplen determinadas condiciones.

A fin de hacer posible esta operación, se amplía el concepto restringido del llamado número entero, ideando o creando otros entes abstractos denominados *números fraccionarios* y el conjunto de éstos y el de los números enteros del conjunto primitivo, constituye el llamado SISTEMA DE LOS NUMEROS RACIONALES que da lugar al estudio de la tercera parte de la Aritmética y que pudiéramos llamar *Aritmética del Número Racional.*

Dentro del campo del número racional, quedan todavía operaciones y problemas que siguen imposibles, y para evitar estas imposibilidades, vuelve a ampliarse el concepto del número, ideando otros entes abstractos, denominados *números irracionales*, que en unión con los racionales del campo anterior, constituyen el llamado SISTEMA DE LOS NUMEROS REALES que da lugar al estudio de la cuarta parte de la Aritmética y que pudiéramos llamar *Aritmética del Número Real.*

8.1. Asimismo, y así sucesivamente se va ampliando el concepto del número hasta llegar al SISTEMA DE LOS NUMEROS COMPLEJOS, que es el más amplio campo numérico, que utilizan las ciencias aplicadas basadas en la matemática pura.

Es interesante observar, que como en cada campo numérico están incluidos los números del campo anterior:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

todas las definiciones de las operaciones en el campo ampliado (aunque arbitrarias, ya que toda definición no es sino un convenio), han de ser tales, que al aplicarlas a los números del campo anterior, que forman parte del ampliado, den los mismos resultados que los que se obtenían en el campo inmediatamente anterior.

Además, como todas las reglas operativas en cada campo, son consecuencias inmediatas de las definiciones de las operaciones en él, y de las leyes fundamentales de estas operaciones, las referidas definiciones han de ser tales que, con arreglo a ellas, subsistan las leyes formales inherentes a las distintas operaciones; esto es, que se satisfaga el llamado *Principio de Permanencia de las Leyes Formales*, enunciado así por Hankel: "Al generalizar un concepto se debe tratar de conservar el mayor número de propiedades, y al nuevo concepto debe corresponder como caso particular el anterior".

En consecuencia, el proceso de ampliación podemos describirlo, en líneas generales, de la siguiente manera:

1° Se tiene un conjunto de entes, que denotaremos abstractamente por A.

En este conjunto se pueden efectuar ciertas operaciones que designaremos, por ejemplo, con los signos $+$, $\cdot$, etc.

2° En seguida se construye, es decir, se idea un nuevo conjunto que denotaremos por E, con operaciones $\oplus$, $\odot$, etc., de modo que se satisfagan las condiciones siguientes:

a) El conjunto A está sumergido por isomorfismo en el nuevo E; es decir, E contiene a los entes antiguos y a otros más (los que se crean o inventan).

b) Si x e y pertenecen al conjunto primitivo A, entonces

$$x \oplus y = x + y$$
$$x \odot y = x \cdot y$$

o sea, que las nuevas operaciones $\oplus$ y $\odot$ aplicadas a elementos del conjunto primitivo A dan los mismos resultados que las antiguas operaciones $+$ y $\cdot$; es decir, que no haya contradicción.

c) Las nuevas operaciones definidas en el nuevo conjunto han de satisfacer a las mismas leyes formales que regían dichas operaciones en el conjunto primitivo; es decir, que haya armonía.

Esta condición se conoce con el nombre de Principio de Permanencia de las Operaciones, o de las Leyes Formales del Cálculo Aritmético.

Gracias a este principio, dichas leyes formales enunciadas como proposiciones primeras o axiomas, son las que tomó David Hilbert para caracterizar de una vez por todas lo que debemos entender por la palabra NUMERO.

Observaciones importantes. 1) Por lo general, todo elemento nuevo de E se puede deducir de los elementos primitivos, es decir, de los A, aplicando a estos las nuevas operaciones.

Así, por ejemplo, los números enteros negativos se deducen de los naturales aplicando a éstos una operación, la sustracción, que puede considerarse como nueva, puesto que ella no era siempre posible en el conjunto primitivo $A = \mathbb{N}$.

Asimismo, los números fraccionarios (racionales) se deducen de los números enteros aplicando a éstos una operación, la división, que puede considerarse como nueva puesto que ella no era siempre posible en el conjunto primitivo u original $A = \mathbb{Z}$; y así en seguida, para nuevas ampliaciones.

2) La condición que acabamos de mencionar en el punto 1), tiene el sentido siguiente:

Una vez obtenido el propósito que motivó la ampliación del conjunto primitivo A para obtener el nuevo E, no es necesario introducir más entes nuevos.

Así, por ejemplo, si el objeto por el cual se han introducido los enteros negativos y el cero, es el de hacer posible la operación de sustracción entre los naturales, basta, por lo tanto, con los números naturales (ahora, enteros positivos) y estos nuevos que son los enteros negativos para poder realizar siempre la operación de sustracción en el conjunto ampliado. En otras palabras, todo ente nuevo es el resultado de operar con entes primitivos.

3) La operación nueva no sólo debe hacerse con los entes primitivos, sino también con los entes nuevos, es decir, en E. Por ejemplo, la introducción de los enteros negativos no sólo debe hacer posible la sustracción de enteros naturales, sino también la sustracción de enteros negativos.

4) Por último, es necesario advertir que, si este procedimiento de ampliación se aplica en la misma forma por segunda vez en el conjunto ampliado o nuevo E, ello no conducirá a entes esencialmente nuevos.

Así, por ejemplo, los pares ordenados de números enteros no dan origen a nuevos números no enteros; tampoco los pares ordenados de nú-

meros racionales conducen a números no racionales; los pares ordenados de números reales no dan origen a nuevos números no reales.

Este hecho, puesto en evidencia por Hilbert, se conoce con el nombre de *Principio de Completidad.*

Capítulo IX

EL NUMERO ENTERO

9.0. Vamos ahora a estudiar en forma más precisa las ideas anteriormente expuestas.

Pues bien, después de haber introducido en forma axiomática el concepto del número natural, nos corresponde ahora, utilizando el Problema de Ampliación que hemos estudiado en el Capítulo VIII, ver las sucesivas extensiones del concepto de números hasta alcanzar el del número real y del número complejo, este último, como la forma más general de un número.

Empezaremos con la construcción y estudio de los números enteros, para continuar con la construcción y estudio de los números racionales, reales y complejos.

9.1. *Construcción de los números enteros.* a) El conjunto de los números naturales es, con respecto a la adición, un semigrupo abeliano. En él, la operación de restar $a - b$ es sólo posible si $a > b$.

Como ya dijimos en el Capítulo VIII, cuando en un sistema resulta imposible realizar ciertas operaciones, se amplía el sistema numérico para que estas operaciones sean posibles, y dicha ampliación se hace de acuerdo con el concepto de ampliación que hemos detallado en el capítulo precedente.

El problema de ampliar el sistema de los números naturales para hacer posible la operación de sustracción en todos los casos, es un caso particular del problema general de dar un grupo abeliano ampliación de un semigrupo abeliano dado, y la resolución de tal problema no ofrece ninguna dificultad, ni en el caso general, ni en el caso particular.

En efecto, dando por sentado el conocimiento de las propiedades de los números naturales, indicaremos ahora cómo se construyen los números enteros.

Empecemos por tomar el conjunto $\mathbb{N} \times \mathbb{N}$, producto cartesiano de $\mathbb{N}$ por sí mismo, es decir, el conjunto de los pares ordenados (a, b) de elementos de $\mathbb{N}$.

$$N = \mathbb{N} \times \mathbb{N} = \{(a, b) : a, b \in \mathbb{N}\}$$

b) Dos de tales pares (a, b) y (c, d) se dirán "iguales", o mejor, equivalentes y se escribirá:

$$(*) \quad (a, b) \sim (c, d) \text{ si, y sólo si, } a + d = b + c$$

Ejemplos:

$(8, 3) \sim (9, 4)$, porque $8 + 4 = 3 + 9$

$(5, 11) \not\sim (3, 7)$, porque $5 + 12 \neq 11 + 3$

$(a, a) \sim (b, b)$, porque $a + b = a + b$

$(a', a) \sim (b', b)$, porque $a' + b = a + b'$

puesto que, $(a + b)' = (a + b)'$

$(a', b' \sim (a, b)$, porque $a' + b = b' + a$

ya que, $(a + b)' = (b + a)'$

en donde, a, b $\in$ IN, siendo además a' y b' los sucesores de a y b, respectivamente.

También es inmediato que se tienen:

$$(a, b) \sim (a + x, b + x), \forall\, a, b, x \in \mathbb{N}$$

y, $$(a, b) \sim (a - x, b - x)$$

siempre que las diferencias $a - x$, $b - x$ sean posibles. Por otro lado, es fácil probar que la relación (*) es de equivalencia; esto es, reflexiva, simétrica y transitiva.

En efecto, tenemos:

i) $(a, b) \sim (a, b)$ porque es cierto que $a + b = b + a$; luego, la relación "$\sim$" es reflexiva.

ii) Sea $(a, b) \sim (c, d)$, es decir se verifica:

$$a + d = b + c$$

o sea, $$b + c = a + d$$

o bien, $$c + b = d + a$$

lo que implica, por (*), que:

$$(c, d) \sim (a, b)$$

luego, la relación "$\sim$" es simétrica.

iii) Sean ahora, $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$; es decir, se verifican las siguientes igualdades entre números naturales:

$$a + d = b + c$$

$$c + f = d + e$$

Sumando miembro a miembro, se tiene:

$$a + d + c + f = b + c + d + e$$

y aplicando las propiedades asociativa, conmutativa y de cancelación en IN, se obtiene:

$$a + f = b + e$$

es decir, $$(a, b) \sim (e, f)$$

lo que prueba la propiedad transitiva de la relación "$\sim$" y, por lo tanto, esta relación es de equivalencia.

c) Vamos ahora a definir en IN $\times$ IN una "adición" y una "multiplicación" mediante las reglas siguientes:

$$1)\ (a, b) + (c, d) = (a + c, b + d)$$

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

Es claro que estas dos operaciones están bien definidas para cada par de elementos (a, b) y (c, d) pertenecientes a IN $\times$ IN, porque operaciones bien definidas a partir de operaciones bien definidas son ellas mismas bien definidas. Además son asociativas, conmutativas y la multiplicación distributiva respecto a la adición como consecuencia inmediata de la validez de dichas propiedades en IN.

d) Vamos en seguida a probar que la equivalencia "$\sim$" definida en (*) es regular o compatible con cada una de estas dos operaciones en IN $\times$ IN.

En efecto, tenemos:

1) *Para la adición.* Sean,

$$\begin{cases} (a, b) \sim (c, d) \\ (a', b') \sim (c', d') \end{cases}$$

es decir,

$$\begin{cases} a + d = b + c \\ a' + d' = b' + c' \end{cases}$$

lo que implica por adición,

$$a + d + a' + d' = b + c + b' + c'$$

o sea, $$(a + a') + (d + d') = (b + b') + (c + c')$$

de donde, $$(a + a', b + b') \sim (c + c', d + d')$$

o bien, $$(a, b) + (a', b') \quad (c, d) + (c', d')$$

luego, la equivalencia "$\sim$" es compatible con respecto a la adición.

2) *Para la multiplicación.* Sean,

$$\begin{cases} (a, b) \sim (c, d) \\ (a', b') \sim (c', d') \end{cases}$$

es decir,

$$\left\{\begin{array}{l} a + d = b + c \\ a' + d' = b' + c' \end{array}\right. \left|\begin{array}{l} \cdot a' \\ \cdot c \end{array}\right| \left|\begin{array}{l} \cdot b' \\ \cdot d \end{array}\right.$$

Multiplicando la primera igualdad por a' y por b':

$$a a' + d a' = b a' + c a'$$

$$b b' + c b' = a b' + d b'$$

y la segunda por c y por d:

$$a' c + d' c = b' c + c' c$$

$$b' d + c' d = a' d + d' d$$

y sumando miembro a miembro las cuatro últimas igualdades y cancelando los términos comunes a ambos miembros, se obtiene la igualdad siguiente:

$$a a' + b b' + d' c + c' d = b a' + a b' + c c' + d d'$$

de donde,

$$(a a' + b b', b a' + a b') \sim (c c' + d d', d' c + c' d)$$

o bien,

$$(a, b) \cdot (a', b') \quad (c, d) \cdot (c', d')$$

resultado que muestra que la equivalencia "$\sim$" es compatible con respecto a la multiplicación.

e) Sea ahora $\mathbb{Z}$ el conjunto cociente $\mathbb{N} \times \mathbb{N} / \sim$

Designaremos por la notación $\overline{(a, b)}$ las clases de equivalencia correspondiente a todos los pares ordenados que son equivalentes al par (a, b). Luego,

$\mathbb{Z}$ = Conjunto de todas las clases de equivalencia $\overline{(a, b)}$ para todo a, $b \in \mathbb{N}$.

Los elementos de $\mathbb{Z}$ se llamarán NUMEROS ENTEROS. Por lo tanto, en esta teoría definiremos el número entero en la forma siguiente:

Definición. Definimos el Número Entero por abstracción, como la clase de equivalencia de todos los pares equivalentes a un par dado de números naturales.

Veremos más adelante que podremos dar a la clase $\overline{(a, b)}$ la interpretación siguiente:

$$\overline{(a, b)} = a - b$$

que tendrá un significado ya conocido cuando sea $a > b$, e introducirá una generalización de la operación sustracción para el caso cuando sea $a \leq b$.

Luego, el número entero 4 es la clase cuyos elementos son los pares ordenados:

$$4 = \{(5, 1), (6, 2), (7, 3), \ldots, (34, 30), \ldots\}$$

y el número entero (-4) será la clase de equivalencia cuyos elementos son los pares:

$$-4 = \{(1, 5), (2, 6), (3, 7), \ldots, (30, 34), \ldots\}$$

y el entero cero será la clase cuyos elementos son los pares:

$$0 = \{(1, 1), (2, 2), (3, 3), \ldots, (30, 30), \ldots\}$$

Por otra parte, los números enteros, o enteros racionales como también los llamaremos, pueden ordenarse en una serie que crece, poniendo (como lo veremos más adelante);

$$\overline{(a, b)} < \overline{(c, d)} \text{ si, y sólo si } a + d < b + c$$

obteniéndose así la serie:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

que nos es tan familiar desde la enseñanza básica y media.

EJERCICIOS

1) Verifique que la operación de adición en $\mathbb{N} \times \mathbb{N}$ es asociativa y conmutativa.

2) Verifique que la operación de multiplicación en $\mathbb{N} \times \mathbb{N}$ es asociativa, conmutativa y distributiva con respecto a la adición.

3) Demuestre que el elemento $(x, x) \in \mathbb{N} \times \mathbb{N}$ es independiente de x, y es el neutro para la adición.

4) Muestre que el elemento (y, x) es el inverso aditivo del elemento (x, y) en el conjunto $\mathbb{N} \times \mathbb{N}$.

9.2. *El anillo $\mathbb{Z}$ de los números enteros.* Siendo la equivalencia "$\sim$" compatible o regular con las operaciones de adición y multiplicación que hemos definido en $\mathbb{N} \times \mathbb{N}$, resulta entonces que ellas inducen también una adición y una multiplicación en el conjunto cociente $\mathbb{Z}$, que indicaremos con los mismos signos operatorios que aquéllos, y que son:

$$1)\ \overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$$

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

y con estas operaciones, $\mathbb{Z}$ es homomorfo a $\mathbb{N} \times \mathbb{N}$, siendo la aplicación de homomorfismo:

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Z}$$

definida por,

$$f((a, b)) = \overline{(a, b)}$$

Luego, las dos operaciones que acabamos de definir en $\mathbb{Z}$ son asociativas, conmutativas y la multiplicación es distributiva respecto a la adición. Además, $\mathbb{Z}$ tiene elemento neutro para la adición y que es, el elemento $\overline{(x, x)}$ independiente de x, y cada elemento $\overline{(a, b)}$ de $\mathbb{Z}$ tiene el inverso aditivo $\overline{(b, a)}$ en $\mathbb{Z}$, ya que:

$$\overline{(a, b)} + \overline{(b, a)} = \overline{(a + b, a + b)} = \overline{(x, x)}$$

Luego, $-\overline{(a, b)} = \overline{(b, a)}$, por definición.

Por último, $\mathbb{Z}$ contiene el elemento $\overline{(x + 1, x)}$, independiente de x, y que es neutro para la multiplicación, puesto que se verifica la propiedad:

$$\overline{(a, b)} \cdot \overline{(x + 1, x)} = \overline{(ax + a + bx, ax + bx + b)}$$
$$= \overline{(a, b)}$$

En consecuencia:

1° $\mathbb{Z}$ es un grupo abeliano respecto a la adición; es decir, un grupo aditivo.

2° $\mathbb{Z}$ es un anillo abeliano respecto a la adición y multiplicación, y con elemento unidad.

3° Probaremos ahora que $\mathbb{Z}$ es también, además de anillo, un dominio de integridad.

En efecto, supongamos que se tuviese

$$\overline{(a, b)} \cdot \overline{(c, d)} = 0, \text{ con } \overline{(a, b)} \neq 0$$

o sea,

$$\overline{(ac + bd, bc + ad)} = 0$$

lo que exige que se cumpla la igualdad:

$$ac + bd = bc + ad \qquad (1)$$

Ahora bien, como es $\overline{(a, b)} \neq 0$, resulta entonces que $a \neq b$, y lo que implica por la ley de tricotomía en $\mathbb{N}$ las alternativas siguientes:

$$a < b, \text{ o bien } b < a$$

Si fuese $a < b$, entonces $x \in \mathbb{N}$ tal que $a + x = b$, y reemplazando en la igualdad (1) se tiene:

$$ac + (a + x)d = (a + x)c + ad$$

$$ac + ad + dx = ac + cx + ad$$

que por cancelación implica:

$$dx = cx$$

y nuevamente, por cancelación, resulta finalmente:

$$d = c$$

es decir, la clase $\overline{(c, d)}$ es la clase nula.

Para la segunda alternativa, $b < a$, se razona idénticamente y obteniéndose el mismo resultado.

Por consiguiente, si en $\mathbb{Z}$ un producto es cero, entonces al menos un factor es cero; esto es, $\mathbb{Z}$ es un dominio de integridad; que es lo que queríamos demostrar.

EJERCICIOS

1) Sin hacer referencia al homomorfismo de $\mathbb{N} \times \mathbb{N}$ a $\mathbb{Z}$, demostrar todas las propiedades formales: asociatividad, conmutatividad de las operaciones de adición y multiplicación, como también la propiedad distributiva de la multiplicación respecto a la adición.

2) Si $\alpha = \overline{(a, b)}$, $\beta = \overline{(c, d)}$, $\gamma = \overline{(e, f)}$ denotan los números enteros que se indican, demostrar que se verifica:

   a) $-0 = 0$, siendo $0 = \overline{(x, x)} \in \mathbb{Z}$

   b) $-(-\alpha) = \alpha$

   c) $\alpha \cdot 0 = 0 \cdot \alpha = 0, \cup\ \alpha \in \mathbb{Z}$

   d) $(-1) \cdot \alpha = -\alpha, 1 = \overline{(x + 1, x)}$

e) $\alpha(-\beta) = -\alpha\beta$

f) $(-\alpha)\cdot\beta = -\alpha\beta$

g) $(-\alpha)\cdot(-\beta) = \alpha\beta$

3) Probar las leyes de cancelación:

$$\alpha + \gamma = \beta + \gamma \Rightarrow \alpha = \beta$$

$$\alpha \cdot \gamma = \beta \cdot \gamma, \gamma \neq 0 \Rightarrow \alpha = \beta$$

9.3. *Sustracción en* $\mathbb{Z}$. *Definición.* La sustracción de dos enteros se define como:

$$\alpha - \beta = \alpha + (-\beta)$$

esto es, en términos de la operación directa que es la suma.

O sea, $\overline{(a, b)} - \overline{(c, d)} = \overline{(a, b)} + \overline{(d, c)} = \overline{(a+d, b+c)}$

Es claro que,

$$\gamma = \alpha - \beta \text{ si, y sólo si, } \beta + \gamma = \alpha$$

La operación sustracción es evidentemente una operación binaria interna sobre $\mathbb{Z}$. Sin embargo, no es asociativa, puesto que:

$$\alpha - (\beta - \gamma) \neq (\alpha - \beta) - \gamma, \text{ con } \alpha, \beta, \gamma \in \mathbb{Z} \text{ y } \gamma \neq 0$$

En efecto, sean $\alpha = \overline{(a, b)}, \beta = \overline{(c, d)}, \gamma = \overline{(e, f)}$. Entonces:

$$\beta - \gamma = \beta + (-\gamma) = \overline{(c, d)} + \overline{(f, e)} = \overline{(c+f, d+e)}$$

$$-(\beta - \gamma) = \overline{(d+e, c+f)}.$$

$$\alpha - (\beta - \gamma) = (a, b) + (d+e, c+f) = (a+d+e, b+c+f)$$

Por otra parte, se tiene

$$\alpha - \beta = \overline{(a, b)} + \overline{(d, c)} = \overline{(a+d, b+c)}$$

$$(\alpha - \beta) - \gamma = \overline{(a+d, b+c)} + \overline{(f, e)} = (a+d+f, b+c+e)$$

Así, pues, con $\gamma \neq 0$, resulta

$$\alpha - (\beta - \gamma) \neq (\alpha - \beta) - \gamma$$

es decir, la operación sustracción no es asociativa. Tampoco es conmutativa, como es fácil de ver, pero sí la multiplicación es distributiva respecto a la sustracción.

9.4. *Isomorfismo de* IN *sobre una parte de* $\mathbb{Z}$. Definamos ahora la siguiente aplicación de IN a $\mathbb{Z}$ así:

$$f(a) = \overline{(a + x, x)}, \forall a \in \mathbb{N}$$

en donde x es un elemento cualquiera de IN.

A cada $a \in$ IN le corresponde un elemento de $\mathbb{Z}$; para ver que sólo le corresponde uno hay que probar que f(a) es independiente del elemento x; ello es consecuencia inmediata de que:

$$(a + x, x) \sim (a + y, y) \Rightarrow a + x + y = a + x + y$$

cualesquiera que sean x e y.

Luego, f es función.

Afirmamos en seguida que f es un monomorfismo (isomorfismo) de IN sobre una parte de $\mathbb{Z}$; es decir, que f es inyectiva y preserva las sumas y productos.

En efecto, probemos primeramente que f es inyectiva. Sea,

$$f(a) = f(b)$$

o sea,

$$\overline{(a + x, x)} = \overline{(b + y, y)}$$

y como la igualdad de clases de equivalencia se traduce en la equivalencia de los elementos que definen esas clases, resulta:

$$(a + x, x) \sim (b + y, y)$$

o sea,

$$a + x + y = b + x + y \Rightarrow a = b$$

luego, f es inyectiva.

Vamos ahora a demostrar que esta aplicación biyectiva de IN sobre un subconjunto de $\mathbb{Z}$ es un isomorfismo (monomorfismo de IN en parte de $\mathbb{Z}$).

En efecto, se tiene:

$$f(a + b) = \overline{(a + b + x, x)}$$

$$f(a) + f(b) = \overline{(a+y, y)} + \overline{(b+z, z)} = \overline{(a+b+y+z, y+z)}$$

$$= \overline{(a+b+t, t)}$$

luego,

$$f(a + b) = f(a) + f(b), \forall a, b \in \mathbb{N}$$

lo que prueba que f es un isomorfismo con respecto a las sumas de IN y de $\mathbb{Z}$.

Demostraremos en seguida que este isomorfismo f con respecto a la adición es también un isomorfismo con respecto a la multiplicación. En efecto, se tiene:

$$\begin{aligned} f(a \cdot b) &= \overline{(a \cdot b + x, x)} \\ f(a) \cdot f(b) &= \overline{(a + y, y)} \cdot \overline{(b + z, z)} \\ &= \overline{(ab + az + by + 2yz, by + yz + az + yz)} \\ &= \overline{(ab + t, t)} \end{aligned}$$

luego,

$$f(a \cdot b) = f(a) \cdot f(b), \forall\, a, b \in \mathbb{N}$$

lo que muestra que f es un isomorfismo con respecto a las multiplicaciones de $\mathbb{N}$ y de $\mathbb{Z}$.

Por consiguiente, el conjunto $\mathbb{Z}$ de los números enteros contiene un subconjunto propio isomorfo al de los números naturales.

Se suele identificar $\mathbb{N}$ con su imagen por este isomorfismo.

Merced a esta convención tenemos:

$$1)\ \mathbb{N} \subset \mathbb{Z}$$

$$2)\ a = \overline{(a + x, x)}$$

es decir, $\mathbb{N}$ aparece como si fuese un subconjunto de $\mathbb{Z}$. Con otra terminología, decimos que $\mathbb{N}$ está sumergido en $\mathbb{Z}$ bajo isomorfismo.

Por otra parte, mediante la convención precedente, tenemos siempre:

$$\overline{(a, b)} = a - b$$

aunque no unívocamente determinados a y b.

En efecto,

$$\begin{aligned} a &= \overline{(a + x, x)} \\ b &= \overline{(b + y, y)} \\ -b &= \overline{(y, b + y)} \end{aligned}$$

luego,

$$\begin{aligned} a - b = a + (-b) &= \overline{(a + x, x)} + \overline{(y, b + y)} \\ &= \overline{(a + x + y, b + x + y)} \\ &= \overline{(a, b)} \end{aligned}$$

En base a las consideraciones precedentes tendremos:

$$\overline{(a, b)} \in \mathbb{N} \subset \mathbb{Z}$$

si, y sólo si, $a > b$.

En efecto, si $a \in \mathbb{N}$ y $a = \overline{(a + x, x)}$, entonces es

$$a + x > x$$

Recíprocamente, sea $a > b$, es decir existe $x \in \mathbb{N}$ tal que

$$a = b + x$$

y entonces, $\overline{(a, b)} = \overline{(b + x, b)} = x \in \mathbb{N}$

9.5. *Tipos de números enteros.* De lo que acabamos de decir resulta que hay tres tipos de números enteros $\overline{(a, b)}$:

1°. aquéllos en que $a > b$, que son los números naturales;
2°, aquéllos en que $a = b$, y
3°. aquéllos en que $a < b$.

Representando, respectivamente, estos tres tipos en la forma:

$$\overline{(a + x, x)}\ ,\ \overline{(x, x)}\quad \overline{(x, b + x)}$$

se prueba que ellos son independientes de x, y por tanto, lo podemos identificar con los símbolos:

$$a,\ 0,\ -b$$

El primero será llamado *entero positivo*, el segundo el *entero cero* y el tercero *entero negativo*. Luego,

$$\overline{(a + x, x)} = a$$

$$\overline{(x, x)} = 0$$

$$\overline{(x, b + x)} = -b$$

En resumen, pues: El conjunto $\mathbb{Z}$ de los números enteros se compone de los enteros positivos $\mathbb{Z}^+_0$ números naturales, de los enteros negativos $\mathbb{Z}^-$ y del entero cero; esto es,

$$\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^- \cup \{0\}$$

o también, $\mathbb{Z} = \mathbb{Z}^+ + \mathbb{Z}^- + \{0\}$

luego, $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

9.6. *Regla de los signos.* Sean los números enteros siguientes:

$$a = \overline{(a + x, x)},\ -a = \overline{(x, a + x)},\ b = \overline{(b + y, y)},\ -b = \overline{(y, b + y)}$$

y formemos los productos indicados:

$$1)\ a \cdot b = \overline{(a + x, x)}\,\overline{(b + y, y)} = \overline{(ab, + bx + ay + xy, bx + xy + ay + x}$$

$$= \overline{(ab + t, t)} > 0$$

$$2)\ (-a) \cdot b = \overline{(x, a + x)} \cdot \overline{(b + y, y)} =$$

$$= \overline{(bx + xy + ay + xy, ab + bx + ay + xy + xy)}$$

$$= \overline{(t, ab + t)} < 0$$

$$3)\ a \cdot (-b) = \overline{(a + x, x)}\,\overline{(y, b + y)} =$$

$$= \overline{(ay + xy + bx + xy, xy + ab + bx + ay + xy)}$$

$$= \overline{(t, ab + t)} < 0$$

$$4)\ (-a) \cdot (-b) = \overline{(x, a + x)}\,\overline{(y, b + y)} =$$

$$= \overline{(xy + ab + bx + ay + xy, ay + xy + bx + xy)}$$

$$= \overline{(ab + t, t)} > 0.$$

Luego, el producto de dos enteros del mismo signo es positivo y el producto de dos enteros de distintos signos es negativo. Así, por ejemplo:

$$(+3) \cdot (+4) = +12$$

$$(-3) \cdot (-4) = +12$$

$$(+3) \cdot (-4) = -12$$

$$(-3) \cdot (+4) = -12$$

9.7. *Generalización de la adición y multiplicación de* IN. Utilizando la nueva forma de los números naturales, esto es,

$$a = \overline{(a + x, x)}$$

probaremos que la adición y multiplicación de los números enteros generaliza la adición y multiplicación de los números naturales.

En efecto, se tienen:

$$\overline{(a + x, x)} + \overline{(b + y, y)} = \overline{(a + b + x + y, x + y)} = a + b$$

$$\overline{(a + x, x)} \cdot \overline{(b + y, y)} = \overline{(ab + ay + bx + xy + xy, bx + xy + ay + xy)}$$

$$= a \cdot b$$

En consecuencia, el conjunto $\mathbb{Z}$ de los números enteros que se ha construido extendiendo el conjunto IN de los números naturales de modo que en él se haga posible la operación inversa de la adición, que se llama sustracción, cumple este conjunto $\mathbb{Z}$ con todas las condiciones que indicamos en el capítulo VIII al estudiar, en líneas generales, el Problema de Ampliación. Luego, por el procedimiento de construcción que hemos venido haciendo, el conjunto construido $\mathbb{Z}$ es una ampliación del conjunto IN.

EJERCICIOS

En las fórmulas que siguen, las letras griegas designan números enteros y los cuales deben ser sustituidos por sus respectivas clases de equivalencias, en las demostraciones que se piden hacer.

1) Probar las igualdades siguientes:

a) $\alpha + (\beta - \gamma) = a + \beta - \gamma$

b) $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$

c) $\alpha - (\beta - \gamma) = \alpha - \beta + \gamma$

2) Demostrar las igualdades que se indican:

a) $\beta - \gamma = (\beta + \alpha) - (\gamma + \alpha)$

b) $\alpha - \beta = \gamma - \delta$ si, y sólo si, $\alpha + \delta = \beta + \gamma$

c) $(\alpha + \beta) \cdot (\gamma + \delta) = (\alpha\gamma + \beta\gamma) + (\alpha\delta + \beta\delta)$

d) $(\alpha + \beta) \cdot (\gamma - \delta) = (\alpha\gamma + \beta\gamma) - (\alpha\delta + \beta\delta)$

e) $(\alpha - \beta) \cdot (\gamma - \delta) = (\alpha\gamma + \beta\delta) - (\alpha\delta + \beta\gamma)$

9.8. *Representación simplificada y notación canónica de los enteros*

Desde que:

$$(a, b) \sim (a - 1, b - 1) \sim (a - 2, b - 2) \sim \ldots . (a - x, b - x)$$

bajo la sola condición de posibilidad de las diferencias consideradas, tres casos pueden presentarse:

1) Si $a > b$, se tiene $(a, b) \sim (a - b, 0)$

Ya sabemos que en tal caso se trata de un entero positivo, y se escribe en general:

$$\overline{(m, 0)}, \text{ con m entero natural}$$

2) Si $a = b$, se tiene $(a, b) \sim (0, 0)$

Como sabemos, este número es el entero cero.

3) Si $a < b$, se tiene $(a, b) \sim (0, b - a)$

y este número, como se sabe, es un entero negativo, y se escribe en general:

$$\overline{(0, m)}, \text{ con m entero natural}$$

En los casos 1) y 3), el número natural m se llamará el *Valor Absoluto*, del número entero respectivo. Luego, cualquier número entero es de una de las formas siguientes:

1) $\overline{(m, 0)}$, si es positivo

2) $\overline{(0, m)}$, si es negativo

3) $\overline{(0, 0)}$, si es cero

Estas nuevas formas de un número entero, las llamaremos su FORMA SIMPLIFICADA, y pueden ser utilizadas en las definiciones de las operaciones de adición y multiplicación, teniéndose:

$$\overline{(m, 0)} + \overline{(n, 0)} = \overline{(m + n, 0)}$$

$$\overline{(0, m)} + \overline{(0, n)} = \overline{(0, m + n)}$$

$$\overline{(m, 0)} + \overline{(0, n)} = \overline{(m, n)} = \begin{cases} \overline{(m - n, 0)}, & m > n \\ \overline{(0, n - m)}, & n > m \end{cases}$$

$$\overline{(m, 0)} \cdot \overline{(n, 0)} = \overline{(mm, 0)}$$

$$\overline{(0, m)}\ \overline{(0, n)} = \overline{(mn, 0)}$$

$$\overline{(m, 0)}\ \overline{(0, n)} = \overline{(0, mn)}$$

$$\overline{(0, m)}\ \overline{(n, 0)} = \overline{(0, mn)}$$

Por otra parte, como a todo número entero corresponde su simétrico u opuesto del mismo valor absoluto, se puede escribir:

$$\overline{(m, 0)} + \overline{(0, m)} = \overline{(m, m)} = \overline{(0, 0)}$$

de donde, $$\overline{(0, m)} = -\overline{(m, 0)}$$

Por consiguiente, los enteros positivos y negativos podrán escribirse, en general, en la forma siguiente:

$$\overline{(m, 0)},\ -\overline{(m, 0)}$$

y puesto que el cero ocupa siempre el mismo lugar en estas dos notaciones, podremos entonces suprimirlo y convenir en representar por $+ m$ un entero positivo y por $- m$ un entero negativo, en donde m representa, como de costumbre, un entero natural que llamamos el valor absoluto del entero racional. Tal representación será llamada *la notación canónica* de los números enteros.

Este convenio, nos permite ahora escribir la serie ordenada de los números enteros en la forma:

$$\ldots\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\ldots$$

Advertimos, por otra parte, que los signos $+$ y $-$ prefijados al entero natural m, no indica una adición ni una sustracción, sino que es un signo predicatorio que permite distinguir las dos clases de números en que se divide el conjunto $\mathbb{Z}$ de los enteros racionales: el subconjunto $\mathbb{Z}^+$ de los enteros positivos y el subconjunto $\mathbb{Z}^-$ de los enteros negativos. El entero cero, 0, carece de signo, por lo que se le puede atribuir indistintamente el signo $+$, o el signo $-$.

Con esta nueva forma reducida que hemos adoptado para representar a los números enteros, las operaciones de adición, sustracción y multiplicación del anillo $\mathbb{Z}$,se escriben ahora en la forma siguiente:

$$(+m) + (+n) = +(m + n)$$

$$(-m) + (-n) = -(m + n)$$

$$(+m) + (-n) = \begin{cases} +(m - n), & m > n \\ -(n - m), & m < n \end{cases}$$

para la adición.

Para la sustracción, resulta:

$$(+m) - (+n) = (+m) + (-n) = \begin{cases} +(m - n), & m > n \\ -(n - m), & m < n \end{cases}$$

$$(-m) - (-n) = (-m) + (+n) = \begin{cases} +(n - m), & n > m \\ -(m - n), & n < m \end{cases}$$

$$(+m) - (-n) = (+m) + (+n) = +(m+n)$$

$$(-m) - (+n) = (-m) + (-n) = -(m+n)$$

y para la multiplicación se tiene:

$$(+m)\cdot(+n) = +mn$$

$$(-m)\cdot(-n) = +mn$$

$$(+m)\cdot(-n) = -mn$$

$$(-m)\cdot(+n) = -mn$$

Finalizaremos la presente sección haciendo ver la similaridad que existe entre los enteros positivos $+m$, y los números naturales m.

Hay, como ya sabemos, una diferencia esencial entre un elemento del conjunto $\mathbb{Z}$ y un elemento del conjunto $\mathbb{N}$. Sin embargo, los enteros positivos forman un conjunto isomorfo al conjunto $\mathbb{N}$ de los números naturales, ya que hay una correspondencia biunívoca:

$$m \rightleftarrows +m$$

entre sus elementos y esta correspondencia preserva las dos leyes de composición: adición y multiplicación, puesto que se verifica:

$$m + n = (+m) + (+n) = +(m+n)$$

$$m \cdot n = (+m)\cdot(+n) = +(mn)$$

entre ambos conjuntos.

En razón de este isomorfismo es como habitualmente se confunden estos dos conjuntos y lo que lleva a suprimir el signo predicatorio $+$ que caracteriza a un entero positivo, o aun a considerar un entero sin signo, como positivo en los cálculos. En realidad no hay ningún inconveniente en virtud de tal isomorfismo.

Bajo estas ideas, podemos considerar al conjunto $\mathbb{N}$ de los enteros naturales como un subconjunto del conjunto $\mathbb{Z}$, de los enteros racionales; es decir.

$$\mathbb{N} \subset \mathbb{Z}$$

9.9. *Ordenación de los Números Enteros.*

Teorema. Para dos enteros α y β cualesquiera, siempre se presenta uno y uno sólo de los tres casos siguientes:

1) $\alpha = \beta$

2) Existe un entero positivo $(\overline{n+x, x})$ tal que

$$\alpha + (\overline{n+x, x}) = \beta$$

3) Existe un entero positivo $(\overline{m+y, y})$ tal que

$$\alpha = \beta + (\overline{m+y, y})$$

Demostración. I) Mostremos primeramente que no pueden presentarse a la vez dos de los casos 1), 2) y 3).

En efecto, supongamos por el contrario que se verificaran al mismo tiempo 1) y 2); esto es

$$\begin{cases} (\overline{a, b}) = (\overline{c, d}) \\ (\overline{a, b}) + (\overline{n+x, x}) = (\overline{c, d}) \end{cases}$$

lo cual implica,

$$(\overline{a+n+x, b+x}) = (\overline{a, b})$$

de donde, $(a+n+x, b+x) \sim (a, b)$

o sea, $a+n+x+b = b+a+x$

o bien, $(a+b)+n = (a+b)$

imposible, por la propiedad de que la suma de dos números naturales es distinta de sus sumandos.

Asimismo y por idéntico razonamiento se prueba que las relaciones 1) y 3) no pueden verificarse simultáneamente.

Probemos ahora que tampoco pueden ocurrir a la vez los casos 2) y 3), porque si así fuera, se tendría

$$(\overline{a, b}) + (\overline{n+x, x}) = (\overline{c, d})$$

$$(\overline{a, b}) = (\overline{c, d}) + (\overline{m+y, y})$$

lo que implica,

$$(\overline{a, b}) = (\overline{a, b}) + (\overline{n+x, x}) + (\overline{m+y, y})$$

o sea, $(\overline{a, b}) = (\overline{a+n+x+m+y, b+x+y})$

de donde, $(a, b) \sim (a+n+m+x+y, b+x+y)$

o sea, $a+b+x+y = a+b+n+m+x+y$

que por cancelación se convierte en:

$$(a + b) = (a + b) + (n + m)$$

imposible por la misma propiedad de la suma mencionada más arriba.

Así hemos probado que los casos 1), 2) y 3) se excluyen mutuamente.

II) Mostremos ahora que sólo uno puede verificarse. En efecto, se puede escribir

$$\beta = \alpha + (\beta - \alpha), \alpha = \beta + (\alpha - \beta)$$

y, si $\alpha \neq \beta$, entonces uno y uno sólo de los enteros $\beta - \alpha$, $\alpha - \beta$ es positivo, y el teorema está demostrado.

Una consecuencia importante de este teorema es la posibilidad de definir una relación de ordenación entre los números enteros.

Definición. Para dos números enteros $\overline{(a, b)}$ y $\overline{(c, d)}$ definimos la relación:

$$\overline{(a, b)} < \overline{(c, d)}, \text{ equivalente, } \overline{(c, d)} > \overline{(a, b)}$$

si, y sólo si, existe un entero positivo $(n + x, x)$ tal que

$$\overline{(a, b)} + \overline{(n + x, x)} = \overline{(c, d)}$$

o sea,
$$\overline{(a + n + x, b + x)} = \overline{(c, d)}$$

y de donde,
$$(a + d) + n = (b + c)$$

lo que implica,
$$a + d < b + c$$

Luego, por definición se tiene:

$$\overline{(a, b)} < \overline{(c, d)} \Longleftrightarrow a + d < b + c$$

De esta definición resulta que $\overline{(a, b)} > 0$ si, y sólo si, $(a, b) \in \mathbb{Z}^+$.

$\overline{(a, b)} < 0$ significa que $\overline{(a, b)} \in \mathbb{Z}^-$

La relación »<« se llama de orden en $\mathbb{Z}$, porque es verdadera la proposición que sigue:

Teorema. Nuestra relación de orden »<« tiene las propiedades siguientes:

1) $\alpha < \beta$ y $\beta < \gamma \Rightarrow \alpha < \gamma$ (transitiva)

2) Para $\alpha, \beta \in \mathbb{Z}$ arbitrarios se presenta siempre uno y uno sólo de los tres casos siguientes:

$$\alpha = \beta, \alpha < \beta, \beta < \alpha \text{ (Ley de Tricotomía)}$$

La relación "$>$" opuesta de "$<$", tiene las mismas propiedades.

Demostración.

1) Por definición se tiene:

$$\alpha < \beta \Longleftrightarrow a + d < b + c$$

$$\beta < \gamma \Longleftrightarrow c + f < d + e$$

Por adición y cancelación en IN se encuentra:

$$a + f < b + e$$

o sea,
$$\overline{(a, b)} < \overline{(e, f)}$$

Luego,
$$\alpha < \beta \text{ y } \beta < \gamma \Rightarrow \alpha < \gamma$$

2) Por otra parte, como en IN se verifica una y una sola de las relaciones:

$$a + d = b + c, \quad a + d < b + c, \quad b + c < a + d$$

resulta que también en $\mathbb{Z}$ se cumple una y una sola de las relaciones:

$$\alpha = \beta, \alpha < \beta, \beta < \alpha$$

y el teorema está demostrado.

Idéntica demostración para las propiedades de la relación "$>$".

Ahora es fácil hacer ver que el orden "$<$" definido sobre $\mathbb{Z}$ generaliza el orden "$<$" que anteriormente definimos sobre IN. En efecto, tenemos:

$$\overline{(a + x, x)} < \overline{(b + y, y)}$$

implica,
$$a + x + y < b + x + y$$

o sea,
$$a < b$$

Luego, la relación "$<$" coincide sobre IN con la anteriormente definida sobre $\mathbb{Z}$.

Por lo tanto, el orden "$<$" de $\mathbb{Z}$ que prolonga el orden natural de IN, lo llamaremos el *Orden Natural de* $\mathbb{Z}$; su opuesto "$>$", el *Orden Natural Inverso de* $\mathbb{Z}$.

Definiciones. También en $\mathbb{Z}$ adoptaremos las mismas definiciones para las relaciones "$\leq$" y "$\geq$" que dimos en IN; esto es:

1) $\alpha \leq \beta$ significa $\alpha < \beta$, ó $\alpha = \beta$

2) $\alpha \geq \beta$ significa $\alpha > \beta$, ó $\alpha = \beta$

y que son, respectivamente, las negaciones de las relaciones ">" y "<", y el significado dado se debe a la ley de tricotomía.

Proposición. En $\mathbb{Z}$ es:

$$\alpha < \beta \text{ si, y sólo si, } \alpha - \beta < 0$$

Demostración. Sean $\alpha = \overline{(a, b)}$ y $\beta = \overline{(c, d)}$; entonces:

$$1)\ \alpha - \beta = \overline{(a, b)} - \overline{(c, d)} = \overline{(a, b)} + \overline{(d, c)} = \overline{(a + d, b + c)}$$

Ahora, si es $\alpha < \beta$, entonces por definición de la relación "<" se tiene $a + d < b + c$; luego, el número entero $\alpha - \beta$ es negativo; o sea,

$$\alpha < \beta \Rightarrow \alpha - \beta < 0$$

2) Recíprocamente, si es ahora $\alpha - \beta = \overline{(a+d, b+c)} < 0$ entonces $a + d < b + c$; luego, es $\alpha < \beta$, o sea

$$\alpha - \beta < 0 \Rightarrow \alpha < \beta$$

Por consiguiente, la condición necesaria y suficiente para que el entero α sea menor que el entero β, es que su diferencia $\alpha - \beta$ sea negativa; es decir,

$$\alpha < \beta \Leftrightarrow \alpha - \beta < 0$$

Análogamente,

$$\alpha > \beta \Leftrightarrow \alpha - \beta > 0$$

Así, pues, esta proposición que se acaba de demostrar nos proporciona una nueva definición de las relaciones "<" y ">" en $\mathbb{Z}$.

Teorema. Los números enteros poseen con respecto a su orden natural "<" la propiedad siguiente:

Si se tiene para dos enteros positivos α y β la relación $\alpha < \beta$, entonces existe un número natural n tal que:

$$n\alpha > \beta \text{ (propiedad arquimediana)}$$

Demostración. Si α y β son dos enteros positivos, entonces α y β son números naturales, y el teorema expresa la propiedad arquimediana conocida para los números naturales.

Luego, el dominio ordenado $\mathbb{Z}$ de los números enteros es arquimediano.

Teorema. En el orden natural de los números enteros, no hay ningún entero comprendido entre cero y uno.

Demostración. Si hubiera un entero α tal que $0 < \alpha < 1$, sería positivo y menor que 1, lo que es imposible ya que $1 = \overline{(1 + x, x)}$, por ser el primer elemento de los naturales, lo es también de los positivos.

De acá se deduce que, si α es un entero cualquiera, no hay ningún entero γ tal que,

$$\alpha < \gamma < \alpha + 1$$

ni tampoco ningún otro δ tal que,

$$\alpha - 1 < \delta < \alpha$$

En efecto, en la hipótesis de que existieran, sumando $-\alpha$ a los tres miembros de la primera desigualdad tendríamos:

$$0 < \gamma - \alpha < 1$$

en contra del teorema recién demostrado, y sumando 1 a los tres miembros de la segunda desigualdad tendríamos:

$$\alpha < \delta + 1 < \alpha + 1$$

resultado en contra de lo que acabamos de establecer.

Por consiguiente, en virtud de este hecho, podemos enunciar la propiedad siguiente:

"En el conjunto ordenado de los números enteros, cada elemento α tiene un precedente $\alpha - 1$, y un siguiente $\alpha + 1$, y por tanto, el conjunto $\mathbb{Z}$ no tiene ni primero ni último elemento:

$$\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots$$

Es claro entonces que el conjunto $\mathbb{Z}$ de los enteros no es bien ordenado, pero en cambio sí lo es el de los positivos.

EJERCICIOS

1) Si $\alpha, \beta, \gamma \in Z$, entonces demostrar que:

a) $\alpha + \gamma < \beta + \gamma$ sí, y sólo si, $\alpha < \beta$

Demostración. Tomando $\alpha = \overline{(a, b)}$, $\beta = \overline{(c, d)}$, $\gamma = \overline{(e, f)}$, supongamos que se tuviese:

$$\alpha + \gamma < \beta + \gamma$$

o bien,

$$\overline{(a, b)} + \overline{(e, f)} < \overline{(c, d)} + \overline{(e, f)}$$

o sea, $\overline{(a + e, b + f)} < \overline{(c + e, d + f)}$

lo que, a su vez, implica

$$a + e + d + f < b + f + c + e$$

y que por cancelación en IN, resulta:

$$a + d < b + c$$

de donde, $(\overline{a, b}) < (\overline{c + d})$

es decir, $\alpha < \beta$

Recíprocamente, supongamos ahora que se tenga

$$\alpha < \beta$$

o sea, $(\overline{a, b}) < (\overline{c, d})$

de donde, $a + d < b + c$

Probaremos que se tiene:

$$\alpha + \gamma < \beta + \gamma$$

y para lo cual compararemos las dos expresiones siguientes:

$$\alpha + \gamma = (\overline{a, b}) + (\overline{e, f}) = \overline{(a + e, b + f)}$$

$$\beta + \gamma = (\overline{c, d}) + (\overline{e, f}) = \overline{(c + e, d + f)}$$

esto es, se comparan:

$$(a + e, b + f) \text{ y } (c + e, d + f)$$

o bien, $(a + e) + (d + f)$ y $(b + f) + (c + e)$

o bien, $(a + d) + (e + f)$ y $(b + c) + (e + f)$

Como por hipótesis $a + d < b + c$, se sigue entonces que es:

$$(a + d) + (e + f) < (b + c) + (e + f)$$

o bien, $(a + e) + (d + f) < (c + e) + (b + f)$

o bien, $\overline{(a + e, b + f)} < \overline{(c + e, d + f)}$

o sea, $(\overline{a, b}) + (\overline{e, f}) < (\overline{c, d}) + (\overline{e, f})$

es decir, $\alpha + \gamma < \beta + \gamma$

Luego, $\alpha + \gamma < \beta + \gamma \Longleftrightarrow \alpha < \beta$

b) Si $\gamma < 0$, entonces es $\alpha\,\gamma < \beta\,\gamma$ si, y sólo si, $\alpha > \beta$.

En efecto, supongamos primeramente que se tenga,

$$\alpha\,\gamma < \beta\,\gamma, \gamma < 0$$

y probaremos que resulta $\alpha > \beta$.

Tenemos:

$$(\overline{a, b}) \cdot (\overline{e, f}) < (\overline{c, d}) \cdot (\overline{e, f})$$

o sea, $\overline{(ae + bf, be + af)} < \overline{(ce + df, de + cf)}$

de donde, $ae + bf + de + cf < be + af + ce + df$

Como $\gamma = (\overline{e, f}) < o$, entonces, es $e < f$; luego existe $x \in$ IN tal que $e + x = f$. Reemplazando este valor de f en la desigualdad anterior, resulta

$$ae + b(e + x) + de + c(e + x) < be + a(e + x) + ce + d(e + x)$$

$$ae + be + bx + de + ce + cx < be + ae + ax + ce + de + dx$$

que por cancelación implica:

$$b\,x + c\,x < a\,x + d\,x$$

o sea, $(b + c)\,x < (a + d)\,x$

y por cancelación nuevamente, resulta

$$b + c < a + d,$$

o bien, $(\overline{a, b}) > (\overline{c, d})$

es decir, $\alpha > \beta$

Recíprocamente, supongamos que se tenga:

$$\alpha > \beta$$

o sea, $(\overline{a, b}) > (\overline{c, d})$

luego, $a + d > b + c$

y probaremos que resulta

$$\alpha\,\gamma < \beta\,\gamma, \text{ si } \gamma < 0$$

En efecto, compararemos las dos expresiones que siguen:

$$\alpha\gamma = \overline{(a, b)} \cdot \overline{(e, f)} = \overline{(ae + bf, be + af)}$$

$$\beta\gamma = \overline{(c, d)} \cdot \overline{(e, f)} = \overline{(ce + df, de + cf)}$$

esto es, se comparan

$$\overline{(ae + bf, be + af)} \text{ y } \overline{(ce + df, de + cf)}$$

o bien, $\quad ae + bf + de + cf$, y, $be + af + ce + df$

Como $\gamma = \overline{(e, f)} < 0$, entonces existe $x \in \mathbb{N}$ tal que $e + x = f$.

Reemplazando este valor de f en ambas expresiones que estamos comparando, resulta

$$ae + be + bx + de + ce + cx, \text{ y, } be + ae + ax + ce + de + dx$$

o bien,

$$ae + be + de + ce + (b + c)x, \text{ y, } ae + be + de + ce + (a + d)x$$

y como por hipótesis es $b + c < a + d$, resulta entonces que

$$ae + be + de + ce + (b + c)x < ae + be + de + ce + (a + d)x$$

o sea, $\quad \overline{(ae + bf, be + af)} < \overline{(ce + df, de + cf)}$

o bien, $\quad \alpha\gamma < \beta\gamma$

Luego,

$$\alpha\gamma < \beta\gamma, \text{ con } \gamma < 0 \Longleftrightarrow \alpha > \beta$$

2) Si $\alpha, \beta, \gamma \in \mathbb{Z}$, entonces demostrar que se verifica:

a) $\alpha + \gamma > \beta + \gamma$ si, y sólo si, $\alpha > \beta$

b) Si $\gamma > 0$, es $\alpha\gamma < \beta\gamma$ si, y sólo si, $\alpha < \beta$

c) Si $\gamma > 0$, es $\alpha\gamma > \beta\gamma$ si, y sólo si, $\alpha > \beta$

d) Si $\gamma < 0$, es $\alpha\gamma > \beta\gamma$ si, y sólo si, $\alpha < \beta$

e) Es $\alpha < \beta$, si, y sólo si, $-\alpha > -\beta$

f) Es $\alpha > \beta$ si, y sólo si, $-\alpha < -\beta$

3) Demostrar que se verifican las relaciones:

a) $\alpha < \beta$ y $\gamma < \delta \Longrightarrow \alpha + \gamma < \beta + \delta$

b) $\alpha < \beta$ y $\gamma \leq \delta \Longrightarrow \alpha + \gamma < \beta + \delta$

c) $\alpha \leq \beta$ y $\gamma < \delta \Longrightarrow \alpha + \gamma < \beta + \delta$

d) $\alpha \leq \beta$ y $\gamma \leq \delta \Longrightarrow \alpha + \gamma \leq \beta + \delta$

e) $\alpha < \beta$ y $\gamma > \delta \Longrightarrow \alpha - \gamma < \beta - \delta$

4) Probar que se cumplen las propiedades siguientes:

a) $\alpha > \beta$ y $\gamma > \delta \Longrightarrow \alpha + \gamma > \beta + \delta$

b) $\alpha > \beta$ y $\gamma \geq \delta \Longrightarrow \alpha + \gamma > \beta + \delta$

c) $\alpha \geq \beta$ y $\gamma > \delta \Longrightarrow \alpha + \gamma > \beta + \delta$

d) $\alpha \geq \beta$ y $\gamma \geq \delta \Longrightarrow \alpha + \gamma \geq \beta + \delta$

e) $\alpha > \beta$ y $\gamma < \delta \Longrightarrow \alpha - \gamma > \beta - \delta$

9.10. *Valor absoluto de un número entero. Definición.* En el dominio ordenado $\mathbb{Z}$ de los números enteros, el VALOR ABSOLUTO, de un elemento cualquiera α no nulo, denotado por $|\alpha|$, es por definición el elemento positivo del par $\alpha, -\alpha$. El es cero para $\alpha = 0$. Por lo tanto, se tiene:

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

Por ejemplo: $|5| = 5; |0| = 0; |-5| = 5$

Las principales propiedades del valor absoluto que nos interesan, están dadas en los teoremas que siguen:

Teorema. Para todo número entero α se tiene:

1) $|\alpha| \geq 0$; es decir, el valor absoluto de α nunca es negativo.

2) $|\alpha|^2 = \alpha^2$

3) $\sqrt{\alpha^2} = |\alpha|$

4) $-|\alpha| \leq \alpha \leq |\alpha|$

Demostración. 1) Notando que $\alpha < 0$, $\alpha = 0$, $\alpha > 0$, entonces consecuentemente se tiene:

Si $\alpha < 0$, entonces $|\alpha| = -\alpha > 0$

Si $\alpha = 0$, entonces $|\alpha| = \alpha = 0$

Si $\alpha > 0$, entonces $|\alpha| = \alpha > 0$

Por consiguiente, $|\alpha| \geq 0$ para todo $\alpha \in \mathbb{Z}$

2) Nótese que $|\alpha|^2 = |\alpha| \cdot |\alpha|$

De donde, si $\alpha \geq 0$ entonces $|\alpha|^2 = \alpha \cdot \alpha = \alpha^2$; pero, si $\alpha < 0$, entonces $|\alpha|^2 = (-\alpha) \cdot (-\alpha) = \alpha^2$

Por consiguiente, en todos los casos resulta que,

$$|\alpha|^2 = \alpha^2$$

3) Recordando que en Algebra, a la raíz cuadrada positiva de un número n, se le llama raíz cuadrada principal de n y se la representa por $+\sqrt{n}$, entonces

$$+\sqrt{\alpha^2} = \begin{cases} \alpha, \text{ si } \alpha > 0 \\ 0, \text{ si } \alpha = 0 \\ -\alpha, \text{ si } \alpha < 0 \end{cases}$$

se observa precisamente que estas propiedades son las mismas de $|\alpha|$; por tanto, $+\sqrt{\alpha^2} = |\alpha|$

4) Según la definición de $|\alpha|$ tenemos:

Si $\alpha \geq 0$, entonces $\alpha = |\alpha|$; por otra parte, $\alpha < 0$ implica $\alpha = -\alpha > 0$, de donde $\alpha < 0 < |a|$

Por lo tanto, para todo $\alpha \in \mathbb{Z}$ se tiene $\alpha \geq |\alpha|$

Por otro lado, si $\alpha \geq 0$ entonces $-|\alpha| \leq 0 \leq \alpha$; de igual modo, si $\alpha < 0$ entonces $|\alpha| = -\alpha$ y $-|\alpha| \leq \alpha$.

Por lo tanto, para todo $\alpha \in \mathbb{Z}$ se tiene $-|\alpha| \leq \alpha$.

Ambos resultados se pueden combinar, quedando:

$$-|\alpha| \leq \alpha \leq |\alpha|, \quad \forall \alpha \in \mathbb{Z}$$

y el teorema está demostrado.

Teorema. Si $\alpha \geq 0$, entonces tenemos:

1) $|x| \leq \alpha$ si, y sólo si, $-\alpha \leq x \leq \alpha$

2) $|x| \geq \alpha$ si, y sólo si, es $x \geq \alpha$, o es $x \leq -\alpha$

Demostración. 1) Primeramente demostraremos que si $\alpha \geq 0$ y $|x| \leq \alpha$, entonces se verifica:

$$-\alpha \leq x \leq \alpha$$

En efecto, por el punto 4) del teorema anterior, tenemos la desigualdad:

$$-|x| \leq x \leq |x|$$

Ahora bien, puesto que $x \leq |x|$ y $|x| \leq \alpha$, entonces por transitividad de la relación "$\leq$" resulta:

$$x \leq \alpha \qquad (1)$$

Por otro lado, puesto que $|x| \leq \alpha \Rightarrow -|x| \geq -\alpha$, y, $-|x| \leq x$, o bien $-\alpha \leq -|x|$, y, $-|x| \leq x$, resulta por transitividad de "$\leq$", la desigualdad:

$$-\alpha \leq x \qquad (2)$$

Por tanto, de (1) y (2) se concluye que:

$$-\alpha \leq x \leq \alpha$$

Así hemos demostrado que:

$$|x| \leq \alpha \Rightarrow -\alpha \leq x \leq \alpha$$

En segundo lugar demostraremos que si $\alpha \geq 0$ y $-\alpha \leq x \leq \alpha$, entonces se verifica:

$$|x| \leq \alpha$$

En efecto, si $x \geq 0$, entonces $|x| = x$; esto junto con la hipótesis de que $x \leq \alpha$, demuestra que $|x| \leq \alpha$.

Si $x < 0$, entonces $|x| = -x$, y puesto que $-\alpha \leq x \Rightarrow \alpha \geq -x$, resulta que $|x| \leq \alpha$; luego, en ambos casos se obtiene la implificación:

$$-\alpha \leq x \leq \alpha \Rightarrow |x| \leq \alpha$$

Este resultado y el anterior prueban la equivalencia:

$$|x| \leq \alpha \Leftrightarrow -\alpha \leq x \leq \alpha$$

2) Análogamente, recordando que $|x| = x$, o bien $|x| = x$, resulta que:

$$|x| \geq \alpha \Leftrightarrow -x \geq \alpha, \text{ o } x \geq \alpha$$

o bien,

$$|x| \geq \alpha \Leftrightarrow x \leq -\alpha, \text{ o } x \geq \alpha$$

y el teorema está demostrado.

Teorema. Para dos elementos cualquiera α y β de $\mathbb{Z}$, se tiene siempre:

1) $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$

2) $|\alpha + \beta| \leq |\alpha| + |\beta|$ (Desigualdad triangular)

3) $|\alpha - \beta| \leq |\alpha| + |\beta|$

4) $|\alpha - \beta| \geq |\alpha| - |\beta|$

5) $|\alpha - \beta| \geq ||\alpha| - |\beta||$

Demostración.

1) En uno de los teoremas anteriores demostramos que $+\sqrt{\alpha^2} = |\alpha|$ por lo tanto:

$$|\alpha \cdot \beta| = +\sqrt{(\alpha \cdot \beta)^2} = +\sqrt{\alpha^2 \cdot \beta^2} = +\sqrt{\alpha^2} \cdot \sqrt{\beta^2} = |\alpha| \cdot |\beta|$$

En general, por inducción se prueba que:

$$|\alpha_1 \cdot \alpha_2 \ldots\ldots \alpha_n| = |\alpha_1| \cdot |\alpha_2| \ldots\ldots |\alpha_n|$$

2) Como se tiene:

$$-|\alpha| \leq \alpha \leq |\alpha|$$

$$-|\beta| \leq \beta \leq |\beta|$$

De estas desigualdades se sigue que,

$$-(|\alpha| + |\beta|) \leq \alpha + \beta \leq (|\alpha| + |\beta|)$$

y por el teorema anterior, esta desigualdad es equivalente a:

$$|\alpha + \beta| \leq |\alpha| + |\beta|$$

La igualdad tiene lugar solamente cuando los sumandos α y β son del mismo signo; esto es

$$|\alpha + \beta| = |\alpha| + |\beta|$$

Por ejemplo:

$$|3 + 5| = 8 = |3| + |5|; |(-3)\ (-5)| = 8 |-3| + |-5|.$$

Si los sumandos α y β son de signos contrarios, entonces se tiene:

$$|\alpha + \beta| < |\alpha| + |\beta|$$

Por ejemplo:

$$|3 + (-5)| = 2 < |3| + |-5|$$

es decir,

$$2 < 3 + 5$$

En general, por inducción se demuestra que:

$$|\alpha_1 + \alpha_2 + \ldots\ldots + \alpha_n| \leq |\alpha_1| + |\alpha_2| + \ldots\ldots + |\alpha_n|$$

3) Puesto que $|-\beta| = |\beta|$; entonces si en la relación

$$|\alpha + \beta| \leq |\alpha| + |\beta|$$

reemplazamos β por $-\beta$, se obtiene:

$$|\alpha - \beta| \leq |\alpha| + |\beta|$$

4) Si en la relación:

$$|\alpha - \beta| \leq |\alpha| + |\beta|$$

sustituimos α por $\beta - \alpha$, ésta puede escribirse en la forma:

$$|-\alpha| \leq |\beta - \alpha| + |\beta|$$

o bien,

$$|\alpha| \leq |\alpha - \beta| + |\beta|$$

luego,

$$|\alpha - \beta| \geq |\alpha| - |\beta|$$

5) Pongamos $\alpha - \beta = \gamma \Rightarrow \alpha = \beta + \gamma$

y por la desigualdad triangular:

$$|\alpha| \leq |\beta| + |\gamma|$$

o sea,

$$|\alpha| \leq |\beta| + |\alpha - \beta|$$

o bien,

$$|\alpha - \beta| \geq |\alpha| - |\beta|$$

(que es otra manera de demostrar la relación 4).

Intercambiando los papeles de α y β se tiene asimismo:

$$|\alpha - \beta| = |\beta - \alpha| \geq |\beta| - |\alpha|$$

o bien,

$$-|\alpha - \beta| \leq |\alpha| - |\beta|$$

y como,

$$|\alpha - \beta| \geq |\alpha| - |\beta|$$

obtenemos por el conjunto de ambas, la relación:

$$|\alpha - \beta| \geq ||\alpha| - |\beta||$$

y el teorema está demostrado.

EJERCICIOS

1) Sin utilizar clases de equivalencia, demostrar que la suma de dos elementos negativos de $\mathbb{Z}$ es un elemento negativo.

Demostración. Sean $\alpha < 0$ y $\beta < 0$; entonces

$$\begin{array}{r} -\alpha = |\alpha| \\ -\beta = |\beta| \\ \hline -\alpha - \beta = |\alpha| + |\beta| \end{array}$$

o sea, $$-(\alpha + \beta) = |\alpha + \beta|$$

luego, $$\alpha + \beta = -|\alpha + \beta| < 0$$

2) Demostrar que si α y β son enteros tales que:

$$\alpha \cdot \beta = 1$$

entonces α y β son ambos iguales a 1, o ambos iguales a -1; esto es:

$$\alpha \cdot \beta = 1 \Rightarrow \begin{cases} \alpha = 1, & \beta = 1 \\ \alpha = -1, \beta = -1 \end{cases}$$

(Sugerencia: utilizar la propiedad del valor absoluto del producto y la propiedad $a \cdot b = 1$ en $\mathbb{N}$).

3) En $\mathbb{Z}$, resolver la ecuación $|x - 4| = 3$

Solución.

$$|x - 4| = 3$$

implica $$x - 4 = \pm 3$$

luego, $$x - 4 = 3, \text{ o bien } x - 4 = -3$$

o sea, $$x = 7, \text{ o bien } x = 1$$

4) En $\mathbb{Z}$ resolver las ecuaciones siguientes:

a) $|3x + 2| = 6 - x$

b) $|3 - x| = |1 + x|$

c) $|x + 4| = |x + 2|$

d) $|x - 4| = |x - 2|$

5) En $\mathbb{Z}$ resolver la inecuación

$$|x - 5| \leq 3$$

Solución. Se tiene:

$$-3 \leq x - 5 \leq 3$$

o sea, $$2 \leq x \leq 8$$

Luego, las soluciones son: 2, 3, 4, 5, 6, 7, 8.

6) En $\mathbb{Z}$, resolver la inecuación

$$|x - 3| > 6$$

Solución. Se tiene:

$$x - 3 < -6, \text{ ó } x - 3 > 6$$

o sea, $$x < -3, \text{ ó } x > 9$$

Luego, la primera da por soluciones los infinitos valores enteros que son menores que -3, y la segunda los infinitos valores enteros que son mayores que 9.

7) En $\mathbb{Z}$, resolver las inecuaciones siguientes:

a) $|x - 2| < 3$

b) $|x - 4| \geq 7$

c) $|2x - 1| \leq 5$

8) Demostrar por inducción sobre n las propiedades siguientes:

a) $|\alpha_1 \cdot \alpha_2 \cdot \alpha_3 \ldots \alpha_n| = |\alpha_1| \cdot |\alpha_2| \cdot |\alpha_3| \ldots |\alpha_n|$

b) $|\alpha_1 + \alpha_2 + \alpha_3 \ldots + \alpha_n| \leq |\alpha_1| + |\alpha_2| + |\alpha_3| + \ldots + |\alpha_n|$

En este último caso, diga, además, en qué caso vale la igualdad y en qué otro la desigualdad.

Capítulo X

EL NUMERO RACIONAL

10.0. Nuestro próximo paso va a ser ahora la creación de los números racionales, es decir, las fracciones, después de los números naturales y enteros.

Así como los números enteros surgieron de la necesidad de resolver, sin excepción, ecuaciones del tipo:

$$b + x = a \Rightarrow x = a - b$$

es decir, de la necesidad de definir la operación inversa de la adición; los números racionales surgen, a su vez, de la necesidad de resolver, sin excepción, ecuaciones del tipo:

$$b\,x = a, \text{con } b \neq 0 \Rightarrow x = \frac{a}{b}$$

es decir, de la necesidad de definir la operación inversa de la multiplicación.

El sistema de los números enteros tiene un defecto manifiesto en que, dados dos enteros a y $b \neq 0$, la ecuación

$$b\,x = a$$

puede o no tener solución.

Por ejemplo, la ecuación

$$5x = 35$$

tiene la solución

$$x = 7$$

pero la ecuación

$$5x = 34$$

no tiene solución en $\mathbb{Z}$.

Este defecto lo remediaremos añadiendo a los números enteros otros números, llamados fracciones, para formar el sistema $\mathbb{Q}$ de los números racionales.

Ahora bien, con respecto a la adición, sabemos que no hay ningún número excepcional; todos tienen análogas propiedades. En. cambio, el cero ocupa un lugar excepcional respecto a la multiplicación; puesto que:

$$a \cdot 0 = 0, \forall\, a \in \mathbb{Z}$$

mientras que si $a \neq 0$, hay correspondencia biunívoca:

$$a\,b \longleftrightarrow \dot{b}$$

entre los productos ab y los multiplicadores b, ya que

$$ab_1 = ab_2 \Rightarrow b_1 = b_2$$

Por ello es conveniente, en una primera etapa, excluir el cero de nuestras consideraciones. Pongamos, pues:

$$Z = \mathbb{Z} - \{0\}$$

es decir, el conjunto de los enteros diferentes de cero; o sea, los enteros positivos y negativos

$$Z = \mathbb{Z}^+ \cup \mathbb{Z}^- = \mathbb{Z}^+ + \mathbb{Z}^-$$

10.1. *Construcción de los números racionales.*

a) En esta teoría vamos a definir también el número racional por abstracción, como par ordenado de números enteros en que el segundo componente del par es diferente de cero.

En efecto, dando por sentado el conocimiento de las propiedades de los números enteros, indicaremos en seguida cómo se construyen, en esta teoría, los números racionales.

Empecemos por tomar el conjunto $\mathbb{Z} \times Z = \mathbb{Z} \times (\mathbb{Z} - \{0\})$.

$$\mathbb{Z} \times Z = \{(a, b): a, \in \mathbb{Z} \text{ y } b \in Z\}$$

b) Dos de estos pares (a, b) y (c, d) se dirán "iguales" o equivalentes y se escribirán:

$$(**) \quad \underline{(a, b) \sim (c, d) \text{ si, y sólo si, } ad = bc}$$

Ejemplos:

$(8, 6) \sim (4, 3)$, porque $8 \cdot 3 = 6 \cdot 4$

$(3, 5) \sim (9, 15)$, porque $3 \cdot 15 = 5 \cdot 9$

$(6, -2) \not\sim (12, 4)$, porque $6\,4 \neq (-2) \cdot 12$

También es inmediato que se tienen:

$$(a, b) \sim (a\,x, b\,x), \forall\, a, b, x \in \mathbb{Z}$$

y

$$(a, b) \sim (a{:}x, b{:}\,x)$$

siempre que los cocientes a:x, b:x sea posibles.

Por otra parte, es fácil demostrar que nuestra relación (**) es de equivalencia.

En efecto, tenemos:

i) $(a, b) \sim (a, b)$, porque es verdad que $a \cdot b = b \cdot a$ para todo par $(a,b) \in \mathbb{Z} \times Z$; luego, la relación es reflexiva.

ii) Sea $(a, b) \sim (c, d)$; esto es, se verifica

$$a \cdot d = b \cdot c$$

o sea,

$$b \cdot c = a \cdot d$$

o bien,

$$c \cdot b = d \cdot a$$

lo que implica,

$$(c, d) \sim (a, b)$$

luego, la relación es simétrica.

iii) Sean ahora,

$$(a, b) \sim (c, d) \text{ y } (c, d) \sim (e, f)$$

es decir, se verifican las igualdades siguientes:

$$a \cdot d = b \cdot c$$

$$c \cdot f = d \cdot e$$

Multiplicándolas miembro a miembro, resulta:

$$a\,d\,c\,f = b\,c\,d\,e$$

que por cancelación se obtiene

$$af = b\,e$$

o sea,

$$(a, b) \sim (e, f)$$

luego, la relación es transitiva.

Este resultado y los dos anteriores, prueban que la relación "$\sim$" definida en (**) es de equivalencia.

c) Definiremos en seguida en $\mathbb{Z} \times Z$ una "adición" y una "multiplicación" por medio de las reglas siguientes:

$$1)\ (a, b) + (c, d) = (ad + bc, bd)$$

2) $(a, b) \cdot (c, d) = (ac, bd)$

Como $\mathbb{Z}$ es un dominio de integridad y siendo $b \neq 0$ y $d \neq 0$, se tiene $bd \neq 0$, y como, por otra parte, operaciones definidas a partir de operaciones bien definidas son ellas mismas bien definidas, resulta que las operaciones 1) y 2) están bien definidas para todo par de elementos de conjunto $\mathbb{Z} \times Z$.

Son consecuencias inmediatas, del hecho de que $\mathbb{Z}$ es un dominio de integridad, la conmutatividad de la adición y la asociatividad y conmutatividad de la multiplicación.

Veremos en seguida que la adición es también asociativa. En efecto, tendremos:

$$\begin{aligned}[(a, b) + (c, d)] + (e, f) &= (ad + bc, bd) + (e, f) \\ &= (adf + bcf + bde, bdf)\end{aligned}$$

y por otro lado,

$$\begin{aligned}(a, b) + [(c, d) + (e, f)] &= (a, b) + (cf + de, df) \\ &= (adf + bcf + bde, bdf)\end{aligned}$$

resultados que muestran que se cumple la igualdad:

$$[(a, b) + (c, d)] + (e, f) = (a, b) + [(c, d) + (e, f)]$$

es decir, la adición es asociativa.

d) Mostraremos ahora que la equivalencia "$\sim$" definida en (**) es compatible o regular con cada una de estas dos operaciones que se acaban de definir en el conjunto $\mathbb{Z} \times Z$.

En efecto, se tiene:

1) *Para la adición.* Sean,

$$\begin{cases} (a, b) \sim (c, d) \\ (a', b') \sim (c', d') \end{cases}$$

es decir,

$$\begin{cases} ad = bc \\ a'd' = b'c' \end{cases} \quad \begin{matrix} \cdot b'd' \\ \cdot bd \end{matrix}$$

y sumando miembro a miembro, se obtiene

$$adb'd' + a'd'bd = bcb'd' + b'c'bd$$

$$(ab' + a'b)dd' = (c'd + cd')bb'$$

de donde, $(ab' + a'b, bb') \sim (cd' + c'd, dd')$

y lo que implica, por la definición de suma de pares:

$$(a, b) + (a', b') \sim (c, d) + (c', d')$$

luego, la equivalencia "$\sim$" es compatible respecto a la adición.

2) *Para la multiplicación.* Sean,

$$\begin{cases} (a, b) \sim (c, d) \\ (a', b') \sim (c', d') \end{cases}$$

o sea,

$$\begin{cases} ad = bc \\ a'd' = b'c' \end{cases}$$

Multiplicando miembro a miembro, se obtiene:

$$adad' = bcb'c'$$

o bien, $(aa') \cdot (dd') = (cc') \cdot (bb')$

y de donde, $(aa', bb') \sim (cc', dd')$

y lo que implica, por la definición de producto de pares:

$$(a, b) \cdot (a', b') \sim (c, d) \cdot (c', d')$$

luego, la equivalencia "$\sim$" es también compatible respecto al producto de pares.

e) Sea ahora $\mathbb{Q}$ el conjunto cociente $\mathbb{Z} \times Z/\sim$.

Como de costumbre, denotamos por $\overline{(a, b)}$ las clases de equivalencia correspondientes a todos los pares ordenados que son equivalentes al par (a, b) de números enteros.

$\mathbb{Q}$ = conjunto de todas las clases de equivalencia $\overline{(a, b)}$, para todo a, b $\in \mathbb{Z}$ siendo $b \neq 0$.

Los elementos de $\mathbb{Q}$ se llamarán NUMEROS RACIONALES.

Por consiguiente, en esta teoría, se define el número racional, por abstracción, de la manera siguiente:

Definición. Un número racional es la clase de los pares equivalentes a un par dado (a, b) de dos números enteros y cuyo segundo componente b es distinto de cero.

Más adelante, se verá que podremos dar a la clase $\overline{(a, b)}$ la interpretación siguiente:

$$\overline{(a, b)} = \frac{a}{b}$$

que tendrá un significado ya conocido cuando sea a = b, e introducirá una generalización de la operación división para el caso cuando no sea a = b.

Luego, el número racional 3 es la clase cuyos elementos son los pares ordenados:

$$3 = \{(3, 1), (6, 2), (9, 3), \ldots, (60, 20), \ldots\}$$

El número racional $\frac{2}{3}$ será la clase de equivalencia cuyos elementos son los pares:

$$\frac{2}{3} = \{(2, 3), (4, 6), (6, 9), \ldots, (20, 30), \ldots\}$$

y el número racional $-\frac{2}{3}$ es la clase cuyos elementos son los pares:

$$-\frac{2}{3} = \{(-2, 3), (-4, 6), (-6, 9), \ldots, (-20, 30), \ldots\}$$

y el racional cero será la clase cuyos elementos son los pares:

$$0 = \{(0, x) : x \in \mathbb{Z} - \{0\}\}$$

EJERCICIOS

1) Verificar que la operación de adición en $\mathbb{Z} \times Z$ es asociativa y conmutativa.
2) Verificar que la operación de multiplicación en $\mathbb{Z} \times Z$ es asociativa y conmutativa.
3) Demostrar que el elemento $(0, x) \in \mathbb{Z} \times Z$ es independiente de x, y es el neutro o unidad para la adición.
4) Demostrar que el elemento (x, x) $\mathbb{Z} \times Z$ es independiente de x, y es el neutro o la unidad para la multiplicación.
5) Muestre que el elemento $(-a, b)$ es el inverso aditivo del elemento (a, b) en el conjunto $\mathbb{Z} \times Z$.
6) Muestre que el elemento (b, a) es el inverso multiplicativo del elemento (a, b) en el conjunto $\mathbb{Z} \times Z$.

10.2. *El cuerpo* $\mathbb{Q}$ *de los núeros racionales.* Como la equivalencia "$\sim$" es compatible con las operaciones de adición y multiplicación de $\mathbb{Z} \times Z$, resulta entonces que ellas inducen en el conjunto cociente $\mathbb{Q} = \mathbb{Z} \times Z/\sim$ una adición y una multiplicación definidas por las reglas siguientes:

$$1)\ \overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$$
$$2)\ \overline{(a, b)} \cdot \overline{(c, d)} = \overline{(a c, b d)}$$

Estas operaciones así definidas en términos de operaciones bien definidas entre números enteros, son bien definidas ellas mismas.

Con estas operaciones, $\mathbb{Q}$ es homomorfo a $\mathbb{Z} \times \mathbb{Z}$, siendo la aplicación de homomorfismo.

$$f : \mathbb{Z} \times Z \to \mathbb{Q}$$

definida por $f((a, b)) = \overline{(a, b)}$

Por consiguiente, las dos operaciones definidas en $\mathbb{Q}$ son asociativas y conmutativas.

Probaremos ahora que en $\mathbb{Q}$ la multiplicación es distributiva con respecto a la adición; en efecto:

$$\overline{(a, b)} \cdot [\overline{(c, d)} + \overline{(e, f)}] = \overline{(a, b)} \cdot \overline{(c f + d e, d f)}$$
$$= \overline{(a c f + a d e, b d f)} \qquad (1)$$

$$\overline{(a, b)} \cdot \overline{(c, d)} + \overline{(a, b)} \cdot \overline{(e, f)} = \overline{(ac, bd)} + \overline{(ac, bf)}$$
$$= \overline{(a b c f + a b d e, b^2 d f)}$$
$$= \overline{((a c f + a d e) b, b d f \cdot b)} \qquad (2)$$

Ahora bien, como $(a, b) \sim (a x, b x)$, entonces

$$\overline{(a, b)} = \overline{(a x, b x)}$$

Por lo tanto, las clases (1) y (2) encontradas anteriormente como resultados de ciertas operaciones, son iguales. Luego, en $\mathbb{Q}$ se verifica la propiedad:

$$\overline{(a, b)} \cdot [\overline{(c, d)} + \overline{(e, f)}] = \overline{(a, b)}\,\overline{(c, d)} + \overline{(a, b)} \cdot \overline{(e, f)}$$

que muestra la distributividad de la multiplicación respecto a la adición.

Vamos a ver en seguida que existe un elemento neutro para la adición y es, el elemento $\overline{(0, x)}$ independiente de x.

En efecto, siempre se tiene $(0, x) \sim (0, y)$, y por otra parte si se tiene

$$(0, x) \sim (a, b)$$

se tendrá $$0 \cdot b = a \cdot x$$

O sea, $$a \cdot x = 0$$

y como $x \neq 0$ y $\mathbb{Z}$ es un dominio de integridad, resulta

$$a = 0$$

Por otra parte, se tiene:

$$\overline{(a, b)} + \overline{(0, x)} = \overline{(a x, b x)} = \overline{(a, b)}$$

luego, $(0, x)$ es el elemento neutro o unidad para la adición.

Tomemos ahora un elemento $\overline{(a, b)}$ cualquiera de $\mathbb{Q}$; vamos a mostrar que tiene siempre un inverso con respecto a la adición y al elemento neutro $\overline{(0, x)}$.

En efecto, se tiene:

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(ab - ab, b^2)} = \overline{(0, b^2)} = \overline{(0, x)}$$

Estudiemos ahora las propiedades de $\mathbb{Q}$ respecto a la multiplicación.

En primer lugar, existe un elemento neutro para la multiplicación y es, el elemento $\overline{(x, x)}$ independiente de x.

En efecto, siempre se tiene $\overline{(x, x)} \sim (y, y)$, y por otra parte si se tiene

$$\overline{(x, x)} \sim \overline{(a, b)}$$

se tendrá $$b x = a x$$

o sea, $$b = a$$

Sea ahora $\overline{(a, b)}$ cualquier elemento de $\mathbb{Q}$ se tiene:

$$\overline{(a, b)} \cdot \overline{(x, x)} = \overline{(a x, b x)} = \overline{(a, b)}$$

luego, $\overline{(x, x)}$ es el elemento neutro con respecto a la multiplicación.

En fin, sea ahora un elemento cualquiera $\overline{(a, b)}$ que no sea el elemento neutro respecto a la adición, es decir tal que $a \neq 0$. Probaremos que este elemento tiene siempre un inverso respecto a la multiplicación y que es $\overline{(b, a)}$.

En efecto, se tiene:

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ab)} = \overline{(x, x)}$$

Luego, $\overline{(a, b)}^{-1} = \overline{(b, a)}$.

En consecuencia:

1°. $\mathbb{Q}$ es un grupo abeliano respecto a la adición.

2°. $\mathbb{Q}$ es un anillo abeliano respecto a la adición y multiplicación; este anillo tiene, además, elemento unidad.

3°. $\mathbb{Q}$ es un cuerpo conmutativo (abeliano).

EJERCICIOS

1) Sin hacer referencia al homomorfismo de $\mathbb{Z} \times \mathbb{Z}$ a $\mathbb{Q}$, probar todas las propiedades: asociatividad y conmutatividad de las operaciones de adición y multiplicación definidas en $\mathbb{Q}$.

2) Si se pone $r = \overline{(a, b)}$, $s = \overline{(c, d)}$, $t = \overline{(e, f)}$, probar que se verifican las propiedades siguientes:

a) $-0 = 0$

b) $-(-r) = r$

c) $r \cdot 0 = 0 \cdot r = 0, \forall\, r \in \mathbb{Q}$

d) $(-1) \cdot r = -r$, siendo $-1 = \overline{(-x, x)}$

e) $r(-s) = -rs\,;\ (-r) \cdot s = -rs$

f) $(-r) \cdot (-s) = r s$

g) $(r \cdot s)^{-1} = s^{-1} \cdot r^{-1}$

3) Demostrar las leyes de cancelación para la adición y la multiplicación en $\mathbb{Q}$ esto es:

$$r + t = s + t \Rightarrow r = s$$

$$r \cdot t = s \cdot t \Rightarrow r = s$$

10.3. *Sustracción y División en* $\mathbb{Q}$. La sustracción y la división sobre $\mathbb{Q}$ se definen por las reglas siguientes:

i) $r - s = r + (-s) = \overline{(a, b)} - \overline{(c, d)} = \overline{(a, b)} + \overline{(-c, d)}$

$$= \overline{(a d - b c, b d)}$$

ii) $r : s = r \cdot s^{-1} = \overline{(a, b)} : \overline{(c, d)} = \overline{(a, b)} \cdot \overline{(d, c)}$

$$= \overline{(a d, b c)}$$

Estas operaciones no son ni asociativas ni conmutativas. Pero, lo mismo que ocurre en $\mathbb{Z}$, en $\mathbb{Q}$ la multiplicación es distributiva respecto a la sustracción.

10.4. *Isomorfismo de $\mathbb{Z}$ sobre una parte de $\mathbb{Q}$.* Definamos la siguiente aplicación de $\mathbb{Z}$ a $\mathbb{Q}$ así:

$$f(a) = \overline{(a, 1)}, \quad \forall\, a \in \mathbb{Z}$$

Probemos primeramente que esta aplicación es inyectiva.

En efecto, se tiene:

$$f(a) = f(b)$$

o sea, $\overline{(a, 1)} = \overline{(b, 1)}$

de donde, $(a, 1) \sim (b, 1)$

luego, $a \cdot 1 = 1 \cdot b$

o sea, $a = b$

Afirmamos en seguida que f es un monomorfismo (isomorfismo) de $\mathbb{Z}$ sobre una parte de $\mathbb{Q}$.

En efecto, ya vimos que es inyectiva; sólo falta mostrar que ella preserva las sumas y los productos. Tenemos:

$$f(a + b) = \overline{(a + b, 1)}$$

$$f(a) + f(b) = \overline{(a, 1)} + \overline{(b, 1)} = \overline{(a \cdot 1 + b \cdot 1, 1 \cdot 1)}$$

$$= \overline{(a + b, 1)}$$

luego,

$$f(a + b) = f(a) + f(b), \forall\, a, b \in \mathbb{Z}$$

lo que prueba que f es un isomorfismo con respecto a las sumas de $\mathbb{Z}$ y de $\mathbb{Q}$.

Veamos que también f es un isomorfismo con respecto a la multiplicación. Pues bien:

$$f(a \cdot b) = \overline{(a \cdot b, 1)}$$

$$f(a) \cdot f(b) = \overline{(a, 1)} \cdot \overline{(b, 1)} = \overline{(a \cdot b, 1 \cdot 1)} = \overline{(a \cdot b, 1)}$$

luego,

$$f(a \cdot b) = f(a) \cdot f(b), \quad \forall\, a, b \in \mathbb{Z}$$

resultado que muestra que f es un isomorfismo con respecto a los productos de $\mathbb{Z}$ y de $\mathbb{Q}$.

Por consiguiente, vemos que el cuerpo $\mathbb{Q}$ de los números racionales contiene un subconjunto propio isomorfo al de los números enteros.

Se suele identificar $\mathbb{Z}$ con su imagen por este isomorfismo.

En virtud de esta convención, se tiene:

1) $\mathbb{Z} \subset \mathbb{Q}$

2) $a = \overline{(a, 1)}$

es decir, $\mathbb{Z}$ aparece como si fuese un subconjunto propio de $\mathbb{Q}$.

Con esta terminología, diremos que $\mathbb{Z}$ está sumergido por isomorfismo en $\mathbb{Q}$.

Ahora bien, como $\mathbb{N} \subset \mathbb{Z}$, resulta entonces la cadena de inclusiones:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$

Por otra parte, mediante la convención que acabamos de hacer, tenemos siempre:

$$\overline{(a, b)} = \frac{a}{b}$$

aunque no unívocamente determinados a y b.

En efecto, la notación $\frac{a}{b}$ que se acaba de indicar se justifica, porque siempre se tiene:

$$\overline{(a, b)} = \frac{\overline{(a, 1)}}{\overline{(b, 1)}}$$

puesto que $\overline{(a, b)} \cdot \overline{(b, 1)} = \overline{(a \cdot b, b \cdot 1)} = \overline{(ab, b)} = \overline{(a, 1)}$

es decir, que cada elemento del cuerpo $\mathbb{Q}$ es el cociente de dos elementos del subconjunto isomorfo al dominio de integridad $\mathbb{Z}$.

Por este motivo, el cuerpo $\mathbb{Q}$ de los números racionales se denominará EL CUERPO DE LOS COCIENTES DEL DOMINIO DE INTEGRIDAD $\mathbb{Z}$ DE LOS NUMEROS ENTEROS. Esto nos mueve a dar una nueva definición de número racional y que es:

Definición. Llamaremos Número Racional al cociente entre dos números enteros, con divisor distinto de cero.

Luego,

$$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ con } b \neq 0\}$$

Con esta nueva terminología para los números racionales, las operaciones racionales de adición, sustracción, multiplicación y división, se definen ahora de la manera siguiente:

$$1)\ \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$2)\ \frac{a}{b} - \frac{c}{d} = \frac{ad - +bc}{bd}$$

$$3)\ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

$$4)\ \frac{a}{b} : \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}$$

Ahora, para ver que estas definiciones son legítimas, es necesario demostrar que los cocientes indicados en los segundos miembros de 1), 2), 3) y 4), sólo dependen de los indicados en los primeros miembros, pero no individualmente de los enteros a, b, c, d.

Así, por ejemplo, para probar la legitimidad de 1), procedemos de la siguiente manera:

Sean,

$$\frac{x}{y} = \frac{a}{b}, \ \frac{z}{t} = \frac{c}{d}$$

o sea,

$$b\,x = a\,y, z\,d = c\,t$$

Multiplicando respectivamente por $t\,d$ e $y\,b$, y sumando miembro a miembro, se obtiene:

$$b\,x\,t\,d + z\,d\,y\,b = a\,y\,t\,d + c\,t\,y\,b$$

o bien,

$$(x\,t + z\,y)\,b\,d = (a\,d + b\,c)\,y\,t$$

lo que implica,

$$\frac{xt + zy}{yt} = \frac{ad + bc}{bd}$$

Asimismo se prueban las reglas 2), 3) y 4).

10.5. *Generalización de la adición y multiplicación de* $\mathbb{Z}$. Utilizando la nueva notación de los números racionales, es decir, la forma:

$$a = \overline{(a\,x, x)} = \overline{(a, 1)}$$

puede fácilmente mostrarse que la adición, sustracción y multiplicación de los números racionales generaliza las operaciones de adición, sustracción y multiplicación de los números enteros.

En efecto, se tiene:

$$\overline{(a, 1)} + \overline{(b, 1)} = \overline{(a + b, 1)} = a + b$$

$$\overline{(a, 1)} - \overline{(b, 1)} = \overline{(a, 1)} + \overline{(-b, 1)} = \overline{(a - b, 1)} = a - b$$

$$\overline{(a, 1)} \cdot \overline{(b, 1)} = \overline{(a\,b, 1)} = a\,b$$

Por consiguiente, el conjunto $\mathbb{Q}$ de los números racionales que se ha construido extendiendo el conjunto $\mathbb{Z}$ de los números enteros de manera que en él se haga posible la operación inversa de la multiplicación, que se llama división, cumple con todas las condiciones señaladas en el Capítulo VIII, en lo referente al problema de ampliación.

Por lo tanto, en virtud del procedimiento de construcción que hemos venido practicando, resulta que el cuerpo $\mathbb{Q}$ de los números racionales es una ampliación del anillo $\mathbb{Z}$ de los números enteros, y este anillo $\mathbb{Z}$ puede ser sumergido, bajo isomorfismo, en el cuerpo $\mathbb{Q}$ de manera que todo elemento del cuerpo sea el cociente de dos enteros.

Merced a este hecho, la resolución de la ecuación

$$b\,x = a, \quad b \neq 0$$

cuando en $\mathbb{Z}$ el coeficiente b no divide a a, se la traslada sobre el subconjunto de $\mathbb{Q}$ isomorfo a $\mathbb{Z}$, y la que deviene ahora en la forma:

$$\overline{(b, 1)}\,x = \overline{(a, 1)}$$

y cuya solución es

$$x = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = \overline{(a, 1)} \cdot \overline{(1, b)}$$

$$x = \overline{(a, b)} = \frac{a}{b}$$

EJERCICIOS

En las fórmulas siguientes, las letras que se indican representan números racionales, y las cuales deben ser reemplazadas por sus respectivas clases de equivalencia, tal como $r = \overline{(a, b)}$, en las demostraciones que se piden hacer:

1) Demostrar las igualdades siguientes:

a) $r + (s - t) = r + s - t$
b) $r - (s + t) = r - s - t$
c) $r - (s - t) = r - s + t$

2) Probar que se verifican las igualdades siguientes:

a) $s - t = (s + r) - (t + r)$
b) $r - s = t - u$ si, y sólo si, $r + u = s + t$
c) $(r + s)(t + u) = (r\,t + s\,t) + (r\,u + s\,u)$
d) $(r - s)(t - u) = (r\,t + s\,u) - (r\,u + s\,t)$

10.6. *Representación simplificada de los números racionales.* Desde que se verifica:

$$(a, b) \sim (a\,x, b\,x) \sim (a : x, b : x)$$

bajo la sola condición de posibilidad de los cocientes en $\mathbb{Z}$, resulta entonces que si d es el máximo común divisor positivo de a y b, se podrá escribir:

$$(a, b) \sim (a'\,d, b'\,d) \sim (a', b')$$

Luego, cualquier número racional no nulo se puede escribir de manera única en la forma:

$$\overline{(a, b)} = \overline{(a', b')} = \frac{a'}{b'}$$

donde a' y b' son dos enteros primos entre sí.

Cuando $\overline{(a, b)}$ se reemplaza por $\frac{a'}{b'}$ decimos que el número racional o fraccionario $\overline{(a, b)}$, o $\frac{a}{b}$ ha sido simplificado o reducido a sus términos mínimos, con lo que ahora es irreducible.

En lo sucesivo, todo número racional escrito en la forma de fracción que intervenga en cualquier discusión se considerará como irreducible.

10.7. *Clasificación de los números racionales.* Vamos a clasificar los números racionales en dos clases, POSITIVOS y NEGATIVOS, de la manera siguiente:

Comencemos por observar que en todo número racional $\overline{(a, b)} = \frac{a}{b}$ puede, si se desea suponerse siempre el segundo componente o el denominador b positivo, pues si no lo fuese bastaría tomar

$$\overline{(a, b)} = \frac{a}{b} = \frac{-a}{-b}$$

y entonces uno de los números del par b, $-b$ es positivo. Luego, pudiendo reemplazar siempre la fracción $\frac{a}{b}$ por otra fracción igual y de denominador positivo, podremos entonces llamar *Positivo* a todo número racional cuyo numerador es positivo, y *Negativo* a todo número racional cuyo numerador es negativo.

En resumen, supuestos los denominadores positivos, el signo del numerador, o bien el signo del primer componente del par ordenado, decide el signo del número racional.

Con esto es evidente que un número racional es siempre, o positivo, o cero, o negativo, y los tres casos se excluyen mutuamente.

10.8. *Ordenación de los números racionales*

Definición. Para dos números racionales $\overline{(a, b)}$ y $\overline{(c, d)}$, con segundos componentes b y d positivos, definimos la relación:

$$\overline{(a, b)} < \overline{(c, d)}, \text{ equivalente a } \overline{(c, d)} > \overline{(a, b)}$$

si, y sólo si, $\overline{(a, b)} - \overline{(c, d)} < 0$

O sea, $\overline{(a, b)} - \overline{(c, d)} = \overline{(ad - bc, bd)} < 0$.

lo que implica $a\,d - b\,c < 0$

es decir, cuando sea $a\,d < b\,c$ en la ordenación de los números enteros.

Luego,

$$\boxed{\overline{(a, b)} < \overline{(c, d)} \Longleftrightarrow a\,d < b\,c}$$

La relación "$<$" se llama de orden $\mathbb{Q}$, porque es cierto el teorema que sigue:

Teorema. La relación "$<$" tiene en $\mathbb{Q}$ las dos propiedades siguientes:

1) $r < s \quad y \quad s < t \Rightarrow r < t$ (transitiva)

2) Para $r, s \in \mathbb{Q}$ arbitrarios se presenta siempre uno y uno sólo de los tres casos siguientes:

$r = s, r < s, \quad s < r$ (Ley de Tricotomía)

La relación opuesta "$>$" tiene las mismas propiedades.

Demostración. 1) Por definición, y recordando que los segundos componentes de cada par ordenado son positivos, se tiene:

$$r < s, \text{ o sea, } \overline{(a, b)} < \overline{(c, d)} \Rightarrow c\,d < b\,c$$

$$s < t, \text{ o sea, } \overline{(c, d)} < \overline{(e, f)} \Rightarrow c\,f < d\,e$$

lo que implica, $\begin{cases} a\,d\,f < b\,c\,f \\ b\,c\,f < b\,d\,e \end{cases}$

y lo que implica a su vez, por transitividad, que:

$$a\,d\,f < b\,d\,e$$

de donde, $a\,f < b\,e$

esto es, $\overline{(a, b)} < \overline{(e, f)}$

o bien, $r < t$

2) Por otra parte, como en $\mathbb{Z}$ se verifica por tricotomía, una y una sola de las relaciones:

$$a\,d = b\,c, \quad a\,d < b\,c, \quad b\,c < a\,d$$

y las cuales se excluyen mutuamente, resulta que también en $\mathbb{Q}$ se cumple una y una sola de las relaciones:

$$\overline{(a, b)} = \overline{(c, d)}, \overline{(a, b)} < \overline{(c, d)}, \overline{(c, d)} < \overline{(a, b)}$$

o sea,

$$r = s, \quad r < s, \quad s < r$$

y las cuales se excluyen también mutuamente, y el teorema está demostrado.

Idéntica demostración para las propiedades de la relación opuesta "$>$".

Es fácil probar que el orden "$<$" definido sobre $\mathbb{Q}$ generaliza o prolonga el orden "$<$" que anteriormente definimos sobre $\mathbb{Z}$. En efecto, tenemos:

$$\overline{(a, 1)} < \overline{(b, 1)}$$

implica

$$a \cdot 1 < b \cdot 1$$

o sea,

$$a < b$$

Luego, la relación "$<$" coincide sobre $\mathbb{Z}$ con la que anteriormente definimos sobre $\mathbb{Q}$. Por este motivo, el criterio "$<$" para los números racionales puede continuar llamándose el *Orden Natural de* $\mathbb{Q}$ y su opuesto "$>$", el *Orden Natural Inverso de* $\mathbb{Q}$.

Definiciones: También en $\mathbb{Q}$ adoptaremos las mismas definiciones para las relaciones "$\leq$" y "$\geq$" que se dieron en $\mathbb{Z}$ y en $\mathbb{N}$; es decir;

1) $r \leq s$ significa $r < s$, ó $r = s$

2) $r \geq s$ significa $r > s$, ó $r = s$

Teorema. Los números racionales poseen, con respecto a su orden natural, las dos propiedades siguientes:

1) El cuerpo ordenado $\mathbb{Q}$ es "denso"; es decir, entre dos números racionales existe siempre otro racional, y, en consecuencia, infinitos.

2) El cuerpo ordenado $\mathbb{Q}$ es arquimediano; esto es, si se tiene para dos números racionales positivos r y s la relación $r<s$, entonces existe un número natural n tal que:

$$nr > s$$

Demostración. 1) Sea $r<s$; entonces se puede escribir:

$$\overline{(a, b)} < \overline{(c, d)}, \text{ o bien } \frac{a}{b} < \frac{c}{d}$$

luego,

$$a\,d < b\,c$$

Sumando a ambos miembros, primero ab, y en seguida cd, se obtiene:

$$\begin{cases} a\,d + ab < b\,c + ab \\ a\,d + cd < b\,c + cd \end{cases}$$

o bien,

$$\begin{cases} a(b + d) < b(a + c) \\ (a + c)d < (b + d) \cdot c \end{cases}$$

lo cual implica,

$$\begin{cases} \dfrac{a}{b} < \dfrac{a + c}{b + d} \\ \dfrac{a + c}{b + d} < \dfrac{c}{d} \end{cases}$$

y de donde resulta por la transitividad de la relación "$<$":

$$\frac{a}{b} < \frac{a + c}{b + d} < \frac{c}{d}$$

o sea,

$$r < t < s$$

donde, $t = \dfrac{a + c}{b + d}$ es un número racional.

Como a su vez se puede encontrar un elemento $x \in \mathbb{Q}$ tal que $r<x<t$, otro $y \in \mathbb{Q}$ tal que $r<y<x$, se deduce que entre r y s hay una infinidad de elementos del cuerpo ordenado $\mathbb{Q}$.

2) Sean $r = \overline{(a, b)} = \dfrac{a}{b}$ y $s = \overline{(c, d)} = \dfrac{c}{d}$ dos elementos positivos de $\mathbb{Q}$ tales que $r<s$, o sea

$$a\,d < b\,c$$

siendo, en este caso, positivos los cuatro números enteros a, b, c, d.

Vemos primeramente que:

$$2r = r + r = \frac{a}{b} + \frac{a}{b} = \frac{ab + ab}{b^2} = \frac{a + a}{b} = \frac{2a}{b}$$

$$3r = 2r + r = \frac{2a}{b} + \frac{a}{b} = \frac{2ab + ab}{b^2} = \frac{2a + a}{b} = \frac{3a}{b}$$

y así sucesivamente; de modo que,

$$nr = (n - 1)r + r = \frac{(n - 1)a}{b} + \frac{a}{b} = \frac{na}{b}$$

En segundo lugar, observando que el dominio $\mathbb{Z}$ es arquimediano, la relación

$$a\,d < b\,c, \text{ con } a\,d, b\,c \in \mathbb{Z}^-$$

implica que existe un número natural n tal que,

$$n\,(a\,d) > b\,c$$

o lo que es lo mismo,

$$(n\,a)\,d > b\,c$$

o bien,

$$\frac{n\,a}{b} > \frac{c}{d}$$

es decir,

$$n\,r > s$$

y el teorema está demostrado.

EJERCICIOS

1) Utilizando clases de equivalencia, se pide demostrar:

a) $r > 0 \Rightarrow r^{-1} > 0;\ r < 0 \Rightarrow r^{-1} < 0$

b) $0 < r < s \Rightarrow 0 < s^{-1} < r^{-1}$

c) $r < s < 0 \Rightarrow 0 > r^{-1} > s^{-1}$

d) Es $r + t < s + t$ si, y sólo si, $r < s$

e) Es $r + t > s + t$ si, y sólo si, $r > s$

f) Si $t > 0$, entonces es $r\,t < s\,t$ si, y sólo si, $r < s$

g) Si $t < 0$, entonces es $r\,t < s\,t$ si, y sólo si, $r > s$

h) Es $r < s$ si, y sólo si, $-r > -s$

i) Es $r > s$ si, y sólo si, $-r < -s$

2) Demostrar que:

a) $\mathbb{Q}^+$ es cerrado con respecto a la adición y multiplicación. Probar, además, que si $r \in \mathbb{Q}^+$ también $r^{-1} \in \mathbb{Q}^+$

b) $\mathbb{Q}^-$ es cerrado con respecto a la adición, pero no con respecto a la multiplicación.
Probar, además, que si $r \in \mathbb{Q}^-$ también $r^{-1} \in \mathbb{Q}^-$.

3) Demostrar que si $r, s \in \mathbb{Q}^+$ y es $r < s$, entonces se verifica que,

$$r^2 < r\,s < s^2$$

¿Cuál es la desigualdad correspondiente si $r, s \in \mathbb{Q}^-$?

4) Demostrar que si $r, s \in \mathbb{Q}$ entonces:

$$r \cdot s = 0 \Rightarrow r = 0, \quad \text{ó} \quad s = 0$$

5) Demostrar que se verifican las propiedades siguientes:

a) $r < s \wedge x < y \Rightarrow r + x < s + y$

b) $r > s \wedge x > y \Rightarrow r + x > s + y$

6) Dados los números racionales $\frac{a}{b}$ y $\frac{c}{d}$ tales que,

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

probar que el número racional $\frac{na + mc}{nb + md}$, siendo m y n números naturales, está comprendido entre los dos primeros.

10.9. *Valor absoluto de un número racional*

Teorema. El valor absoluto en $\mathbb{Q}$ está definido por:

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|},\ a, b \in \mathbb{Z},\ b \neq 0$$

Demostración. Observando que, siendo

$$\frac{a}{b} = \frac{-a}{-b}$$

sin restricción pueden suponerse positivos los denominadores b, con lo cual $b = |b|$, y además el criterio de racionales positivos y negativos dados en la sección 10.7 nos permite escribir:

$$\frac{a}{b} \in \mathbb{Q}^+ \quad \text{si, y sólo si,} \quad a \in \mathbb{Z}^+, \text{ o } \quad a = |a|$$

Por consiguiente, para un elemento cualquiera $\frac{a}{b} \in \mathbb{Q}$ sólo puede ocurrir uno de los tres casos siguientes:

1) $\frac{a}{b} \in \mathbb{Q}^+$ entonces $\left|\frac{a}{b}\right| = \frac{a}{b} = \frac{|a|}{|b|}$

2) $\frac{a}{b} = 0$, entonces $a = 0, \left|\frac{a}{b}\right| = 0 = \frac{|a|}{|b|}$

3) $-\frac{a}{b} = \frac{-a}{b} \in \mathbb{Q}^+$, entonces $-a = |a|, \left|\frac{a}{b}\right| = -\frac{a}{b} = \frac{-a}{b} = \frac{a}{b}$

y el teorema está demostrado.

Este valor absoluto de un número racional tiene las mismas propiedades que las que se vieron para el valor absoluto de un número entero y las cuales se demuestran textualmente como aquéllas.

EJERCICIOS

1) Resolver las ecuaciones siguientes:

a) $|3x + 2| = 5 - x$

b) $|7 - 3x| = |2x + 1|$

2) Resolver las inecuaciones siguientes:

a) $|5x| \geq 3 \; ; |7x| > 4$

b) $|2x - 3| \leq 4 \; ; |5x + 2| < 3$

c) $|x - \frac{1}{2}| > \frac{3}{2}$

10.10. *Representación decimal de los números racionales.* Consideremos el número racional positivo $s = \frac{a}{b}$ con $b > 1$.

Por el algoritmo de división se puede escribir:

$$a = b\,q_1 + r_1 \,, 0 \leq r_1 < b$$

y

$$10r_1 = b\,q_2 + r_2 \,, 0 \leq r_2 < b$$

Ahora bien, como $r_1 < b$, entonces

$$b\,q_2 + r_2 = 10r_1 < 10b$$

y lo que implica $q_2 < 10$.

Si $r_2 = 0$, entonces es:

$$r_1 = \frac{b\,q_2}{10}$$

luego,

$$a = b\,q_1 + r_1 = b\,q_1 + \frac{b\,q_2}{10}$$

y de donde resulta que:

$$s = \frac{a}{b} = q_1 + \frac{q_2}{10} = q_1 \,, q_2$$

y decimos que q_1, q_2 es la *expresión decimal que termina* del número racional $s = \frac{a}{b}$.

Pero, si $r_2 \neq 0$, se tiene:

$$10r_2 = b\,q_3 + r_3 \,, 0 \leq r_3 < b$$

y como $r_2 < b$, entonces

$$b\,q_3 + r_3 = 10r_2 < 10b$$

y lo que implica $q_3 < 10$.

Si $r_3 = 0$, entonces es:

$$r_2 = \frac{b\,q_3}{10}$$

luego,

$$a = b\,q_1 + \frac{b\,q_2}{10} + \frac{r_2}{10^2} = b\,q_1 + \frac{b\,q_2}{10} + \frac{b\,q_3}{10^2}$$

y de donde,

$$s = \frac{a}{b} = q_1 + \frac{q_2}{10} + \frac{q_3}{10^2}$$

y la representación decimal que termina de $s = \frac{a}{b}$ es $q_1, q_2\, q_3$.

Si $r_3 \neq 0$, el proceso se repite, encontrándose para el racional $s = \frac{a}{b}$ la representación decimal general:

$$s = \frac{a}{b} = q_1, q_2\, q_3\, q_4 \ldots$$

Pero los distintos restos r_1, r_2, r_3, ... son elementos del conjunto $\{0, 1, 2, 3, \ldots, b-1\}$ de los restos módulo b; por tanto, uno de estos restos debe repetirse, y la representación decimal del número $s = \frac{a}{b}$ es decimal periódica:

$$s = x, y\,z\,c\,d\,e\,c\,d\,e\,c\,d\,e \ldots = x, y\,z\,\overbrace{c\,d\,e}$$

En consecuencia, todo número racional puede ser expresado como un número decimal que termina o que es periódico.

Ejemplos: 1) Hallar la representación decimal de los números racionales siguientes:

1) $s = \frac{13}{8}$. Se tiene:

$$\begin{aligned} 13 &= 8 \cdot 1 + 5 \;;\; q_1 = 1 \;,\; r_1 = 5 \\ 10 \cdot 5 &= 8 \cdot 6 + 2 \;;\; q_2 = 6 \;,\; r_2 = 2 \\ 10 \cdot 2 &= 8 \cdot 2 + 4 \;;\; q_3 = 2 \;,\; r_3 = 4 \\ 10 \cdot 4 &= 8 \cdot 5 \;;\; q_4 = 5 \;,\; r_4 = 0 \end{aligned}$$

luego, se obtiene para $s = \frac{13}{8}$ el decimal que termina:

$$s = \frac{13}{8} = q_1, q_2\, q_3\, q_4 = 1,625$$

2) $s = \frac{29}{7}$. Tenemos:

$$\begin{aligned} 29 &= 7 \cdot 4 + 1 \;;\; q_1 = 4 \;,\; r_1 = 1 \\ 10 \cdot 1 &= 7 \cdot 1 + 3 \;;\; q_2 = 1 \;,\; r_2 = 3 \\ 10 \cdot 3 &= 7 \cdot 4 + 2 \;;\; q_3 = 4 \;,\; r_3 = 2 \\ 10 \cdot 2 &= 7 \cdot 2 + 6 \;;\; q_4 = 2 \;,\; r_4 = 6 \\ 10 \cdot 6 &= 7 \cdot 8 + 4 \;;\; q_5 = 8 \;,\; r_5 = 4 \\ 10 \cdot 4 &= 7 \cdot 5 + 5 \;;\; q_6 = 5 \;,\; r_6 = 5 \\ 10 \cdot 5 &= 7 \cdot 7 + 1 \;;\; q_7 = 7 \;,\; r_7 = 1 = r_1 \end{aligned}$$

luego, se obtiene para $s = \frac{29}{7}$ el decimal periódico:

$$s = \frac{29}{7} = 4,\overbrace{142857}$$

3) $s = \frac{25}{7}$. Tenemos:

$$\begin{aligned} 25 &= 7 \cdot 3 + 4 \;;\; q_1 = 3 \;,\; r_1 = 4 \\ 10 \cdot 4 &= 7 \cdot 5 + 5 \;;\; q_2 = 5 \;,\; r_2 = 5 \\ 10 \cdot 5 &= 7 \cdot 7 + 1 \;;\; q_3 = 7 \;,\; r_3 = 1 \\ 10 \cdot 1 &= 7 \cdot 1 + 3 \;;\; q_4 = 1 \;,\; r_4 = 3 \\ 10 \cdot 3 &= 7 \cdot 4 + 2 \;;\; q_5 = 4 \;,\; r_5 = 2 \\ 10 \cdot 2 &= 7 \cdot 2 + 6 \;;\; q_6 = 2 \;,\; r_6 = 6 \\ 10 \cdot 6 &= 7 \cdot 8 + 1 \;;\; q_7 = 8 \;,\; r_7 = 4 = r_1 \end{aligned}$$

luego, se obtiene para el racional $s = \frac{25}{7}$ el decimal periódico:

$$s = \frac{25}{7} = 3,\overbrace{571428}$$

Hemos demostrado que todo número racional puede representarse, o por un decimal que termina, o por un decimal que es periódico.

Pero, por otra parte, todo decimal que termina es también periódico. En efecto, sea el decimal que termina:

$$s = a, b\,3$$

donde a y b son cifras cualesquiera.

Consideremos ahora el número: a, b 2999 . . .; o sea, el número:

$$s' = a + \frac{b}{10} + \frac{2}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \frac{9}{10^5} + \ldots$$

y como a partir del cuarto sumando se tiene una serie geométrica, se podrá escribir:

$$\begin{aligned} s' &= a + \frac{b}{10} + \frac{2}{10^2} + \frac{\frac{9}{10^3}}{1 - \frac{1}{10}} \\ &= a + \frac{b}{10} + \frac{2}{10^2} + \frac{9}{10^3 - 10^2} \\ &= a + \frac{b}{10} + \frac{2}{10^2} + \frac{9}{10^2\,(10 - 1)} \\ &= a + \frac{b}{10} + \frac{2}{10^2} + \frac{1}{10^2} \\ &= a + \frac{b}{10} + \frac{3}{10^2} \\ &= a, b\,3 = s \end{aligned}$$

Por lo tanto, el número dado s = a, b3, que es un decimal que termina, puede ser también representado por el número s = a, b $2\overline{9}$, es decir, por un decimal periódico (semiperiódico).

Por consiguiente, nuestra conclusión final es que todo número racional puede ser representado por un decimal periódico.

Recíprocamente, probaremos que todo decimal periódico es un número racional.

En efecto, sea el decimal periódico

$$s = a, b\,c\,\overbrace{x\,y\,z}$$

o sea, $$s = a, b\,c + \frac{x\,y\,z}{100 \cdot 1000} + \frac{xyz}{100 \cdot 1000^2} + \ldots$$

luego $s = a, b, c + \dfrac{\frac{z\,y\,z}{100 \cdot 1000}}{1 - \frac{1}{1000}}$

$$s = a.\,b\,c + \frac{xyz}{100 \cdot 1000 - 100}$$

$$s = a, b\,c + \frac{xyz}{100\,(1000 - 1)}$$

$$s = a, b\,c + \frac{x\,y\,z}{99900}$$

resultado que es un número racional.

EJERCICIOS

1) Hallar la representación decimal de los números racionales siguientes:

$$\frac{3}{8}\,;\,\frac{5}{7}\,;\,\frac{11}{4}\,;\,\frac{2}{3}\,;\,\frac{14}{9}\,;\,\frac{13}{6}$$

2) Hallar los números racionales representados por los decimales periódicos siguientes:

$$1,\widehat{23}\,;\,3{,}5\widehat{13}\,;\,0{,}04\widehat{9}\,;\,7{,}26\widehat{135}\,;\,0{,}475\widehat{235}$$

3) ¿Qué números racionales definen las series geométricas siguientes?:

a) $5 + \frac{5}{3} + \frac{5}{3^2} + \frac{5}{3^3} + \ldots$

b) $\frac{1}{8} + \frac{4}{8^2} + \frac{6}{8^3} + \frac{3}{8^4} + \frac{1}{8^5} + \frac{4}{8^6} + \frac{6}{8^7} + \frac{3}{8^8} + \ldots$

c) $\frac{1}{11} + \frac{3}{11^2} + \frac{5}{11^3} + \quad + \frac{9}{11^5} + \frac{1}{11^6} + \frac{3}{11^7} + \frac{5}{11^8} + \frac{7}{11^9} + \frac{9}{11^{10}}$

Capítulo XI

EL NUMERO REAL

11.0. Los Capítulos IX y X comenzaban con la observación de que el sistema A de números estudiados hasta entonces tenía un defecto manifiesto, defecto que se remediaba ampliando el sistema A. Para lo cual se definía en el conjunto de pares ordenados $A \times A$ una relación de equivalencia que resultaba compatible con un par de operaciones binarias internas definidas también en este conjunto $A \times A$.

De este modo se formaron a partir de $\mathbb{N}$ sistemas $\mathbb{Z}$ y $\mathbb{Q}$ que cumplen la cadena de inclusiones:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$

y tales que cada uno de estos nuevos sistemas $\mathbb{Z}$ y $\mathbb{Q}$ posee la característica siguiente:

1) $\mathbb{Z}$ es el menor conjunto en el cual, para elementos arbitrarios $a, b \in \mathbb{N}$; la ecuación,

$$b + x = a$$

tiene siempre solución.

2) $\mathbb{Q}$ es el menor conjunto en el cual, para elementos cualesquiera $a, b \neq 0 \in \mathbb{Z}$, la ecuación,

$$b\,x = a$$

tiene siempre solución.

La situación que se presenta ahora no es que $\mathbb{Q}$ tenga un defecto solo; más bien, tiene muchos y tan diversos que el procedimiento de ampliación que hemos venido estudiando en los dos capítulos anteriores no los remedia todos. Mencionemos, por ejemplo, la ecuación:

$$x^2 = 2$$

no tiene solución en $\mathbb{Q}$, porque si la tuviese, el racional $\frac{a}{b}$, ya reducido, sería tal que:

$$\left(\frac{a}{b}\right)^2 = 2$$

o bien,

$$a^2 = 2\,b^2$$

lo que implica $2 \mid a^2$, lo que implica a su vez $2 \mid a$, porque todo número primo que divide a una potencia, divide también a su base. Luego, se tendrá

$$a = 2\,a'$$

y entonces, por sustitución, se encuentra:

$$(2a')^2 = 2b^2$$

$$4a'^2 = 2b^2$$

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

lo que implica ahora $2 \mid b^2$, o sea $2 \mid b$; es decir,

$$b = 2b'$$

Pero esto contradice a la hipótesis de que la fracción racional $\frac{a}{b}$ era irreducible.

El método que vamos a emplear en la sección siguiente para ampliar el sistema $\mathbb{Q}$ será, pues, diferente al que hemos venido utilizando en las ampliaciones anteriores.

11.1. *El Número Irracional.* En el Capítulo IX, sección 9.7 vimos que dados los enteros n, n +1, no existe ningún entero x comprendido entre ellos; es decir, tal que:

$$n < x < n + 1$$

Por ello diremos que los números enteros presentan saltos, o bien, que forman un *conjunto discreto.* Lo mismo ocurre con los números naturales.

En cambio, los números racionales, como se vio, poseen la propiedad de que: Dados dos números racionales cualesquiera r y s, $r<s$, existe otro número racional x que verifica la relación:

$$r < x < s$$

En efecto, basta elegir $x = \frac{r+s}{2}$ para tener:

$$\frac{r+s}{2} < \frac{s+s}{2} = s$$

y,

$$\frac{r+s}{2} > \frac{r+r}{2} = r$$

por tanto,

$$r < \frac{r+s}{2} < s$$

Análogamente se puede encontrar otro número racional t, tal que:

$$r < t < x, \quad \text{o bien,} \quad x < t < s$$

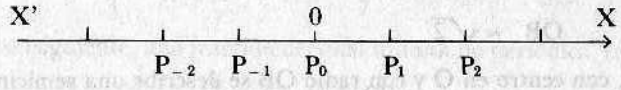
y así un número infinito de tales números.

Esta propiedad se expresa, brevemente, diciendo que los números racionales forman un *conjunto denso* respecto de la relación "$<$".

El término denso que hemos empleado para calificar esta propiedad de los números racionales, proviene de la siguiente representación geométrica:

Fijemos sobre una recta orientada X'X un punto O, que llamaremos *origen* y que llevemos infinitas veces un segmento unitario hacia la izquierda y hacia la derecha de ese punto. Obtendremos así los puntos

$$\ldots, P_{-2}, P_{-1}, P_0, P_1, P_2, \ldots$$



La recta orientada X'X, que recibe ahora el nombre de EJE NUMERICO, el origen 0 representa al cero, P_1 al 1, P_2 al 2,..., P_{-1} al -1, P_{-2} al -2,...

Por lo tanto, los puntos..., P_{-2}, P_{-1}, P_0, P_1, P_2,... dan la representación geométrica de los números enteros $\mathbb{Z}$. Estos puntos están separados entre sí, porque el conjunto formado por ellos es discreto.

Ahora, si dividimos cada uno de los segmentos... P_{-2} P_{-1}, P_{-1} P_0, P_0 P_1, P_1 P_2,... en n partes iguales, obtendremos la representación geométrica de todas las fracciones de denominador n.

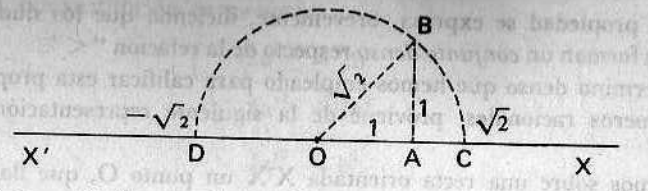
Haciendo esta construcción para cada entero natural n, obtendremos infinitos puntos de la recta numérica, que representan números racionales. Llamaremos *Puntos Racionales* a tales puntos imágenes de números racionales. Estos puntos están distribuidos ya no en forma discreta, sino en forma densa en la recta, esto último, en el sentido que entre cada dos de estos puntos racionales hay una infinidad de otros puntos de este tipo.

Sin embargo, veremos a continuación que los puntos racionales no *llenan* completamente la recta numérica X'X.

La comprobación de este hecho fue uno de los más sorprendentes descubrimientos de los antiguos matemáticos griegos, que data de unos veinticinco siglos y se debió a la escuela pitagórica.

En primer lugar, no existe ningún número racional cuyo cuadrado sea igual a dos, como lo vimos en la sección 11.0 de este capítulo.

Es fácil entonces, mediante una construcción geométrica simple, determinar un punto en la recta numérica que no es racional.



En efecto, en la figura adjunta, supongamos que el segmento OA se elige como unidad de longitud y que OA = AB = 1.

Entonces, por el teorema de Pitágoras resulta que:

$$\overline{OB}^2 = \overline{OA}^2 + \overline{AB}^2 = 1^2 + 1^2 = 1 + 1 = 2$$

y $$OB = \sqrt{2}$$

Ahora, con centro en O y con radio OB se describe una semicircunferencia, se obtienen sobre la recta numérica los puntos C y D, que por lo demostrado anteriormente no pueden ser racionales.

Los griegos, que crearon los números racionales para poder medir las longitudes con números, descubrieron así que existían segmentos, tales como $OC = \sqrt{2}$, no susceptibles de ser medidos, es decir, inconmensurables.

Este descubrimiento es un acontecimiento científico de gran trascendencia, que dejó profunda huella en la matemática y la filosofía desde entonces hasta hoy. La teoría de los inconmensurables de Eudoxo (siglo IV a. de J.C.), expuesto en forma geométrica en los Elementos de Euclides, es una obra maestra de la matemática griega, no debidamente apreciada hasta la segunda mitad del siglo XIX, después que Dedekind, Frege, Cantor y Weierstrass construyeron una teoría rigurosa del número real.

Si se desea establecer una correspondencia biunívoca entre los números y todos los puntos de la recta numérica X'X, es necesario ampliar el sistema de los números racionales $\mathbb{Q}$, introduciendo los números, tales como $\sqrt{2}, \sqrt{3}, \pi, \ldots$

A estos números los llamaremos NUMEROS IRRACIONALES $\mathbb{I}$. La denominación "irracional", viene de los griegos, proviene de la imposibilidad de representar el número como razón de dos enteros.

11.2. *El Número Real.* La reunión de estos dos sistemas de números constituye el sistema de los NUMEROS REALES $\mathbb{R}$.

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} = \mathbb{Q} + \mathbb{I}$$

Ahora sí que podemos decir que estos números llenan o cubren toda la recta numérica X'X, que pasa por esto, a tomar el nombre de la RECTA REAL.

Además, es evidente que los números reales poseen la propiedad de densidad respecto a la relación "<".

Por otra parte, sabemos que todo número racional $\frac{a}{b}$, al efectuar la división de a por b, en el sistema decimal se expresa:

1) o bien, como una fracción decimal finita o que termina, si se llega a un resto cero, como por ejemplo:

$$\frac{1}{2} = 0{,}5\ ;\quad \frac{1}{5} = 0{,}2\ ;\quad \frac{3}{8} = 0{,}375;\ \text{etc.}$$

2) o bien, como una fracción decimal periódica, como por ejemplo:

$$\frac{4}{3} = 1{,}33\ldots = 1{,}\widehat{3}\ ;\quad \frac{1}{7} = 0{,}\widehat{142857}\ ;\ \text{etc.}$$

Por consiguiente, una fracción decimal infinita no periódica, tal como

$$\sqrt{2} = 1{,}41421\ldots$$

no puede representar un número racional, sino a un número irracional.

Gracias a la densidad del conjunto $\mathbb{Q}$ de los números racionales, todo número irracional se puede expresar por números racionales con tanta aproximación como se quiera. Por ejemplo, el número irracional $\sqrt{2} = 1{,}41421\ldots$ se aproxima indefinidamente por los números racionales expresados por decimales finitos, siguientes:

$$1\ ;\ 1{,}4\ ;\ 1{,}41\ ;\ 1{,}414\ ;\ 1{,}4142\ ;\ \ldots$$

Esta es una sucesión de números racionales cuyos cuadrados se aproximan a 2 por su izquierda. Por ejemplo, 1,414 está incluido en esta sucesión porque:

$$1{,}414^2 = 1{,}999396 < 2$$

en cambio se excluye de esa sucesión el número racional 1,415 porque:

$$1{,}415^2 = 2{,}002225 > 2$$

Para el siguiente término podemos calcular $1{,}4141^2$; $1{,}4142^2$; $1{,}4143^2$ y encontramos que 2 está entre el segundo y el tercero; es decir

$$1{,}4142^2 < 2 < 1{,}4143^2$$

en consecuencia incluimos en la sucesión el segundo, es decir, el número 1,4142.

Procediendo así, se amplía la sucesión:

(1) $$1\ ;\ 1{,}4\ ;\ 1{,}41\ ;\ 1{,}414\ ;\ 1{,}4142\ ;\ 1{,}41421\ ;\ \ldots$$

hasta encontrar un número cuyo cuadrado se aproxime a 2 tanto como deseemos.

Esto puede demostrarse formalmente como sigue:

Mediante nuestro proceso indicado más arriba, para cualquier entero positivo n, encontramos un número racional x_n de la sucesión en cuestión que tiene la propiedad de que,

$$x_n^2 < 2 < \left(x_n + \frac{1}{10^n}\right)^2$$

Ahora bien, ya que todos los números involucrados son racionales, podemos emplear sus propiedades para ver que,

$$0 < 2 - x_n^2 < \left(x_n + \frac{1}{10^n}\right)^2 - x_n^2 = \frac{2x_n}{10^n} + \frac{1}{10^{2n}}$$

y como es, $$x_n < 2, \quad \frac{1}{10^{2n}} < \frac{1}{10^n}$$

entonces, $$\frac{2x_n}{10^n} < \frac{4}{10^n}$$

por tanto, $$\frac{2x_n}{10^n} + \frac{1}{10^{2n}} < \frac{4}{10^n} < \frac{1}{10^n} = \frac{5}{10^n}$$

luego, resulta que:

$$0 < 2 - x_n < \frac{5}{10^n}$$

Esto demuestra que escogiendo n lo suficientemente grande podemos aproximar x_n^2 a 2 tanto como deseemos.

Esta sucesión no define un número racional, ya que, como ahora demostramos, no existe un número racional más pequeño que sea mayor que todos los decimales de la sucesión (1).

Para demostrar esto, supongamos que existiera y designémoslo por r. Entonces, primero r^2 no puede ser menor que 2 porque un término de la sucesión (1) de números racionales tendría un cuadrado más próximo a 2 que r^2 y, en consecuencia, sería mayor que r.

Segundo, r^2 no puede ser mayor que 2, porque entonces uno de los decimales

$$2\ ;\ 1{,}5\ ;\ 1{,}42\ ;\ 1{,}415\ ;\ 1{,}4143\ ;\ 1{,}41422\ ;\ \ldots$$

sería menor que r y aun mayor que todos los decimales de la sucesión (1); cada uno de los decimales del conjunto anterior es racional. Esto contradice nuestra hipótesis de que r es el más pequeño.

Así, hemos probado que $r^2 = 2$ es imposible si r es racional.

Por lo tanto, existen expresiones decimales de la forma:

$$e, a_1\ a_2\ a_3\ \ldots$$

donde e es un número entero o cero y para cada índice de i, a_i es un número entero no negativo menor que 10. Entonces, definimos un nuevo tipo de número, llamado *número real,* como sigue:

Definición provisoria. Llamaremos NUMERO REAL a todo decimal finito o infinito, positivo, nulo o negativo.

En esta definición, el término "número real" incluye a todos los racionales, ya que el desarrollo decimal de un número racional define en esta forma al número racional; incluye a los números enteros, ya que por ejemplo, 8 puede escribirse como:

$$8 = 8{,}000\ldots$$

y a $\frac{3}{4}$ puede escribirse como:

$$\frac{3}{4} = 0{,}75000\ldots$$

Sin embargo, como hemos visto anteriormente, también incluye los números que no son racionales y los que llamaremos números irracionales.

Los números reales negativos pueden definirse como hemos definido anteriormente los enteros y racionales negativos. Es posible demostrar que obedecen todas las leyes de los números racionales, cosa que omitimos por su dificultad.

Esta era la definición que hasta mediados del siglo XIX se daba por los números reales.

Sin embargo, esta definición no es enteramente satisfactoria y es más conveniente dar una definición de los números reales independiente del modo de representarlos, sin hacer referencia al sistema de numeración decimal.

Recién, a fines del siglo pasado, en el período de revisión de los fundamentos y principios de la Matemática, Dedekind, Cantor y Weierstrass, elaboraron teorías rigurosas para definir los números reales a partir de los números racionales.

También los números reales pueden introducirse axiomáticamente, como lo ha hecho Hilbert.

11.3. *Axiomas de Hilbert para el número real.* Nos encontramos ahora en situación de presentar un conjunto de axiomas que en ningún caso son únicos, pero que definen o caracterizan el conjunto de los números reales.

El método que vamos a exponer es el más utilizado modernamente por su mayor agilidad y se debe al eminente matemático alemán David Hilbert (1862-1943), quien expuso su fundamento en un célebre artículo, publicado en 1900, "Sobre el concepto de Número".

En este método se definen los conjuntos $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ como subconjuntos especiales de $\mathbb{R}$.

Hilbert admite la existencia de un conjunto $\mathbb{R}$ cuyos elementos se llaman NUMEROS REALES y que está caracterizado por tres listas de axiomas: axiomas de cuerpo conmutativo, axiomas de orden y axioma de plenitud.

I. *Axiomas de Cuerpo conmutativo*

En el conjunto $\mathbb{R}$ de los números reales hay una operación " $+$" llamada *adición*, que verifica:

1) $\forall\, a, b \in \mathbb{R} \Rightarrow a + b \in \mathbb{R}$

2) $\forall\, a, b, c, \in \mathbb{R}$ se tiene: $(a + b) + c = a + (b + c)$

3) $\forall\, a, b \in \mathbb{R}$ se tiene: $a + b = b + a$

4) Existe un elemento particular, denotado por 0, que se llama el *número real cero*, que es neutro para la adición, es decir,

$$0 + a = a + 0 = a, \quad \forall\, a \in \mathbb{R}$$

5) A cada número real a corresponde un único número real $(-a)$, llamado el *opuesto* de a, tal que:

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

En el conjunto $\mathbb{R}$ de los números reales hay una segunda operación "$\cdot$", llamada *multiplicación*, que verifica:

6) $\forall\, a, b \in \mathbb{R} \Rightarrow a \cdot b \in \mathbb{R}$

7) $\forall\, a, b, c \in \mathbb{R}$ se tiene: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

8) $\forall\, a, b \in \mathbb{R}$ se tiene: $a \cdot b = b \cdot a$

9) Existe un elemento particular, denotado por 1, que se llama el *número real uno*, que es neutro para la multiplicación, es decir,

$$1 \cdot a = a \cdot 1 = a\,, \ \forall\, a, \in \mathbb{R}$$

10) A cada número real no nulo a corresponde un único número real $a^{-1} = \frac{1}{a}$, llamado el *inverso* de a, tal que:

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

11) Las operaciones de adición y de multiplicación en $\mathbb{R}$ están vinculadas por la propiedad distributiva:

$$a \cdot (b + c) = a \cdot b + a \cdot c\,, \ \forall\, a, b, c \in \mathbb{R}$$

II. *Axiomas de Orden*

Entre los números reales se puede establecer una relación "$<$" (menor que), con estas propiedades:

Definición I. 01) Si $a, b \in \mathbb{R}$, entonces una, y sólo una, de las proposiciones siguientes es verdadera:

$$a = b\,,\ a < b\,,\ b < a \text{ (Ley de Tricotomía)}$$

02) Si $a, b, c \in \mathbb{R}$ y son tales que $a < b$ y $b < c$, entonces es $a < c$ (transitividad).

03) Si $a, b, c \in \mathbb{R}$ y son tales que $a < b$, entonces es

$a + c < b + c$ (monotonía de la adición)

$a \cdot c < b \cdot c$, si $c > 0$ (monotonía de la multiplicación)

04) Dados dos números reales cualesquiera a y b tales que $a > 0$ y $b > 0$, sumando a a, ella misma repetidas veces, es posible obtener una suma que tenga la propiedad:

$$a + a + \ldots + a > b$$

esto es, existe un número natural n tal que $n\,a > b$ (Ax. de Arquímedes).

La propiedad de tricotomía establece que $\mathbb{R}$, como conjunto, es un conjunto totalmente ordenado, y las propiedades de monotonía vinculan la relación de orden con las operaciones de adición y multiplicación definidas en $\mathbb{R}$.

Luego, cuando un cuerpo como $\mathbb{R}$ cumple el sistema constituido por las propiedades 01), 02) y 03), se dirá que el par $(\mathbb{R}\,;\,\leq)$ es un *Cuerpo Ordenado*. No confundir esto cuando en $\mathbb{R}$, como conjunto, esté definida una relación de orden. Lo esencial en un cuerpo ordenado es la vinculación entre el orden "$<$" y las operaciones "$+$" y "$\cdot$" definidas en el cuerpo $\mathbb{R}$ dadas por 03).

Otro modo de definir el orden en el cuerpo $\mathbb{R}$ es el siguiente:

Definición II. Diremos que $\mathbb{R}$ es un cuerpo ordenado si hemos distinguido, es decir, si admitimos la existencia de un subconjunto $\mathbb{R}^+ \subset \mathbb{R}$ cuyos

elementos se llaman NUMEROS POSITIVOS, caracterizándonos $\mathbb{R}^+$ por los tres axiomas siguientes:

$\mathbb{R}$ 01) $\mathbb{R}^+$ es cerrado para la adición, vale decir:

$$a, b \in \mathbb{R}^+ \Rightarrow a + b \in \mathbb{R}^+ \text{ (Ley de adición)}$$

$\mathbb{R}$ 02) $\mathbb{R}^+$ es cerrado con respecto a la multiplicación; vale decir:

$$a, b \in \mathbb{R}^+ \Rightarrow a \cdot b \in \mathbb{R}^+ \text{ (Ley de multiplicación)}$$

$\mathbb{R}$ 03) Para cada $a \in \mathbb{R}$ se verifica siempre una y una sola de las tres posibilidades siguientes:

$$a \in \mathbb{R}^+, \ -a \in \mathbb{R}^+, \ a = 0 \text{ (Ley de Tricotomía)}$$

Los elementos a tales que $(-a) \in \mathbb{R}^+$, se llaman NUMEROS NEGATIVOS y constituyen el subconjunto $\mathbb{R}^- \subset \mathbb{R}$.

Probaremos ahora que los dos sistemas de axiomas de ordenación dados en las definiciones I) y II) son equivalentes. Por tanto, escoger uno u otro es sólo una cuestión de convenio.

En efecto, primeramente demostraremos que:

$$\text{Definición I)} \Longrightarrow \text{Definición II)}$$

En efecto, admitamos que se cumplan los axiomas 01), 02) y 03) de la Definición I), y definamos $\mathbb{R}^+$ como el conjunto de aquellos elementos de $\mathbb{R}$ tales que $0 < a$. Luego:

$$(*) \qquad \underline{0 < a \text{ significa } a \in \mathbb{R}^+}$$

Luego, existen un subconjunto de $\mathbb{R}$ con la propiedad de que:

$$\mathbb{R}^+ \subset \mathbb{R}$$

y probaremos que se cumplen los axiomas de la Definición II).

En efecto, por 01), para cada $a \in \mathbb{R}$ se verifica:

$$a = 0, \quad 0 < a, \quad a < 0$$

pero, por 03) se tiene:

$$a < 0 \Rightarrow a + (-a) < 0 + (-a) \Rightarrow 0 < -a$$

Así, pues, se cumple $\mathbb{R}$ 03).

Por último, sean $a, b \in \mathbb{R}^+$, esto es:

$$0 < a, 0 < b$$

Por 03) se tiene:

$$0 < a \Rightarrow 0 + b < a + b \Rightarrow b < a + b$$

y como $0 < b$, entonces por 02) resulta

$$0 < a + b \Rightarrow a + b \in \mathbb{R}^+$$

Así, pues, se cumple $\mathbb{R}$ 01).

De $0 < a$, $0 < b$ resulta por 03) que:

$$0 \cdot b < a\,b \Rightarrow 0 < ab \Rightarrow a\,b \in \mathbb{R}^+$$

Así, pues, se cumple $\mathbb{R}$ 02).

Así hemos probado que Definición I) $\Rightarrow$ Definición II).

Recíprocamente, probaremos que:

$$\text{Definición II)} \Longrightarrow \text{Definición I)}$$

En efecto, admitamos ahora que se cumplen los axiomas $\mathbb{R}$ 01), $\mathbb{R}$ 02) y $\mathbb{R}$ 03) de la Definición II), y definamos $a < b$ como equivalente de $b - a \in \mathbb{R}^+$. Luego:

$$(**) \qquad \underline{a < b \text{ significa } b - a \in \mathbb{R}^+}$$

y probaremos que se cumplen los axiomas de la Definición I).

En efecto, dados $a, b \in \mathbb{R}$, entonces por $\mathbb{R}$ 03) se verifica uno y uno sólo de los casos:

$$a - b = 0, \quad a - b \in \mathbb{R}^+, \quad -(a - b) = b - a \in \mathbb{R}^+$$

o sea,

$$a = b, \quad b < a, \quad a < b$$

Así, pues, se cumple 01).

Si $a < b$ y $b < c$, entonces por la definición $(**)$ resulta que:

$$b - a \in \mathbb{R}^+, \quad c - b \in \mathbb{R}^+$$

y por $\mathbb{R}$ 01) se obtiene:

$$(b - a) + (c - b) = c - a \in \mathbb{R}^+ \Rightarrow a < c$$

Así, pues, se cumple 02).

De $a < b$, por definición $(**)$, se tiene:

$$b - a = (b + c) - (a + c) \in \mathbb{R}^+ \Rightarrow a + c < b + c$$

y se cumple así 03).

De $a < b \Longleftrightarrow b - a \in \mathbb{R}^+$ y $c \in \mathbb{R}^+$, por $\mathbb{R}$ 02) resulta:

$$(b - a)\, c \in \mathbb{R}^+ \Rightarrow bc - ac \in \mathbb{R}^+ \Rightarrow ac < bc$$

y se cumple así la segunda parte de 03).

Así hemos probado que Definición II) $\Rightarrow$ Definición I).

Este resultado y el anterior, demuestran la equivalencia de las dos definiciones I) y II).

En lo sucesivo emplearemos de preferencia el sistema dado por la Definición I), por estar más habituado al uso "$\leq$" de su notación de orden.

III. *Axioma de Plenitud o de Completidad*

Sea S un subconjunto no vacío de $\mathbb{R}$; entonces:

1) Si S tiene una cota superior, entonces existe la menor cota superior de S en $\mathbb{R}$ (axioma del supremo).

2) Si S tiene una cota inferior, entonces existe la mayor cota inferior de S en $\mathbb{R}$ (axioma del ínfimo).

Un cuerpo que satisface los axiomas de ordenamiento indicados en la lista II, el axioma del supremo indicado en III, se llamará un *Cuerpo Ordenado Completo*. Puede demostrarse, usando métodos más avanzados, que el sistema de los números reales $\mathbb{R}$ es el único, salvo isomorfismos, un cuerpo ordenado completo.

Por otra parte, el axioma de Arquímedes (indicado en el punto 04) de la lista II, conjuntamente con el axioma de plenitud, sirven para fundamentar la continuidad del conjunto $\mathbb{R}$ de los números reales. Es decir, postulamos diciendo: "El conjunto de los números reales es continuo"; esto es, no es posible agregar al sistema $\mathbb{R}$ nuevos entes numéricos de manera que el sistema que así resulta satisfaga a todos los axiomas de las listas I, II y III, ya que resultaría nuevamente un número real.

Con este hecho se puede ahora postular que dado un eje de abscisas (recta numérica), a cada punto del eje corresponde un número real (su abscisa) y, recíprocamente a cada número real le podemos hacer corresponder un punto sobre el eje (su imagen).

El admitir que a cada punto de la recta numérica X'X pueda hacerse corresponder biunívocamente un número real (su abscisa, respecto a un origen y un segmento unidad prefijados) equivale a admitir como una verdad de hecho la continuidad de la recta; es decir, postulamos que la recta, como sistema de puntos, es un sistema continuo.

En resumen, hemos dado las tres listas de axiomas propuestas por Hilbert para fundamentar, por la vía axiomática, directamente la teoría del número real, sin partir del número natural y recorrer el camino;

$$\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R}$$

Este método directo consiste, pues, en introducir el sistema o estructura $(\mathbb{R}: +, \cdot,)$ en el cual el conjunto subyacente $\mathbb{R}$ es un conjunto abstracto cuyos elementos se llaman números reales satisfaciendo ciertas propiedades que las podemos resumir en el siguiente axioma general:

Axioma de los números reales. "El sistema de los números reales es un cuerpo ordenado completo".

Es decir, postulamos que el sistema de los números reales es un conjunto abstracto, cuyos elementos se llaman números reales, en el cual están definidas unívocamente dos operaciones binarias internas llamadas "adición" y "multiplicación" y una relación de orden en forma tal que se verifican los axiomas de cuerpo ordenado completo.

Todas las propiedades de los números reales se pueden deducir de este postulado o axioma general.

Por consiguiente, vemos que en $\mathbb{R}$ subsisten todas las propiedades algebraicas señaladas para los números enteros y para los números racionales que estudiamos en los capítulos anteriores. Entonces, subsisten en $\mathbb{R}$ y con las mismas demostraciones todos los teoremas demostrados para $\mathbb{Z}$ y para $\mathbb{Q}$, como ser, por ejemplo, propiedades cancelativas de la adición y multiplicación, involutiva $-(-x) = x$, $(x^{-1})^{-1} = x$, regla de los signos, valor absoluto y sus propiedades, etc.

Asimismo, subsiste en $\mathbb{R}$ con igual demostración la propiedad demostrada en $\mathbb{Q}$ de la existencia de solución única de la ecuación:

$$b \cdot x = a, \quad b \neq 0$$

y que es

$$x = a \cdot b^{-1} = \frac{a}{b}$$

Otras ecuaciones algebraicas no solubles en $\mathbb{Q}$, pero sí en $\mathbb{R}$, como por ejemplo, la ecuación:

$$x^2 - 2 = 0$$

que en $\mathbb{R}$ tiene como soluciones $x = \sqrt{2}$ y $x = -\sqrt{2}$, ya que:

$$(\pm\sqrt{2})^2 - 2 = 2 - 2 = 0$$

En general, subsisten en $\mathbb{R}$ todas las propiedades y todos los teoremas demostrados y con igual demostración que se dan sobre dominio de integridad y cuerpos conmutativos y las propiedades de orden sobre estas dos estructuras algebraicas, con todas sus consecuencias.

Más adelante veremos también la enorme importancia que tiene el axioma de plenitud en el estudio de los números reales.

Finalmente, una vez establecida por completo la teoría del número real, es posible establecer la teoría de las *magnitudes abstractas continuas*.

Definimos como magnitudes abstractas continuas a aquellos conjuntos de objetos abstractos (de los cuales pueden existir una imagen o representación concreta), que pueden ponerse en correspondencia isomórfica con los números reales. Como ejemplo tenemos las longitudes, áreas, volúmenes, peso, tiempo, etc.

Las llamamos absolutas continuas para distinguirlas de otras magnitudes, llamadas *discretas*, que no forman conjuntos isomorfos con los números reales, sino con números naturales.

El problema de demostrar que una clase de objetos constituye una magnitud absoluta continua se reduce, pues, a probar el isomorfismo entre el conjunto de objetos de que se trata y los números reales; o en otras palabras, probar que a cada objeto del conjunto, llamado *cantidad* se le puede hacer corresponder unívocamente un número real llamado *medida* de la cantidad. Esto se consigue una vez que se ha definido entre los objetos del conjunto, la operación suma y las relaciones de igualdad, desigualdad y la propiedad de continuidad, y se ha probado que aquella operación, esa relación y esta propiedad tienen las mismas propiedades formales que las análogas operaciones y relaciones entre números reales. Una vez probado esto, se fija luego una cantidad como unidad, y de la comparación por cociente de cada cantidad con la unidad resulta un número real o medida de la cantidad; allí se obtiene el isomorfismo buscado.

11.4. *Subsistemas de los números reales.* En el conjunto $\mathbb{R}$ de los números reales se distinguen tres subconjuntos especiales: el subconjunto $\mathbb{N}$ de los números naturales, el subconjunto $\mathbb{Z}$ de los números enteros y el subconjunto $\mathbb{Q}$ de los números racionales, subconjuntos que pasamos a definirlos.

I. *Números naturales*

Definición. Un subconjunto S de $\mathbb{R}$ se llamará ARITMETICO o INDUCTIVO si:

1) $1 \in S$

2) $x \in S \Rightarrow x + 1 \in S$

Esta definición implica que un conjunto aritmético o inductivo no es vacío. Además, se ve inmediatamente que la intersección de una colección arbitraria, finita o no, de subconjuntos inductivos de $\mathbb{R}$ es un subconjunto inductivo.

Definición. Llamaremos $\mathbb{N}$ a la intersección de todos los subconjuntos aritméticos o inductivos de $\mathbb{R}$.

Los elementos de $\mathbb{N}$ los llamaremos NUMEROS NATURALES.

De la definición resulta que $\mathbb{N}$ es un conjunto aritmético o inductivo, y es el menor de todos los subconjuntos aritméticos o inductivos de $\mathbb{R}$, ya que:

$$\mathbb{N} = \bigcap_{i \in I} S_i \subset S_i, \text{ para todo } i \in I$$

Vamos ahora a estudiar algunas propiedades esenciales de los números naturales.

Teorema. (Principio de Inducción Matemática).

Sea $S \subseteq \mathbb{N}$ con las propiedades siguientes:

1) $1 \in S$

2) $n \in S \Rightarrow n + 1 \in S$

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

Demostración. La hipótesis significa que S es un subconjunto aritmético o inductivo de $\mathbb{R}$.

Por otra parte, siendo $\mathbb{N}$ por definición la intersección de todos los subconjuntos aritméticos de $\mathbb{R}$, resulta entonces por la definición de intersección que:

(1) $$\mathbb{N} \subseteq S$$

Por otro lado, por hipótesis también sabemos que S es un subconjunto de $\mathbb{N}$; luego:

(2) $$S \subseteq \mathbb{N}$$

De (1) y (2) se concluye que $S = \mathbb{N}$, y el teorema está demostrado.

Este mismo teorema que hace legítimo el empleo de la "inducción matemática", suele enunciarse también en la forma siguiente:

Teorema. Si a cada número natural n se le asocia una proposición bien determinada P(n), que puede ser verdadera o falsa, y si verifica que:

1) P(1) es verdadera:

2) Para cualquier $k \in \mathbb{N}$, si de la hipótesis de que P(k) es verdadera se sigue que P(k +1) es también verdadera, entonces la proposición P(n) es verdadera para todo número natural n.

Demostración. Sea S el conjunto de todos los números naturales para los que P(n) es verdadera.

De acuerdo con las hipótesis hechas, S verifica las dos condiciones siguientes:

1) $1 \in S$

2) si $k \in S$, entonces $k + 1 \in S$

Luego, por el teorema anterior es $S = \mathbb{N}$, es decir P(n) es verdadera para todos los números naturales.

El Principio de Inducción Completa es una propiedad fundamental de los números naturales que proporciona un método de demostración llamado por *Inducción Finita o por Recurrencia.*

Para demostrar que todos los números naturales verifican una cierta propiedad, es suficiente:

1) demostrar que es verdadera para $n = 1$;

2) suponiéndola verdadera para $n = k$, se intenta probarla que es verdadera para $n = k + 1$.

Como aplicación del método de inducción, pasaremos a demostrar algunas propiedades de los números naturales.

Proposición 1). Se tiene $\mathbb{N} \subset \mathbb{R}^+$.

O sea, todos los enteros naturales son números reales positivos.

Demostración. En primer lugar, siendo $\mathbb{R}$ un cuerpo ordenado, sabemos que el cuadrado de todo elemento no nulo es positivo; esto es, para todo $a \in \mathbb{R}$, $a \neq 0$, entonces $a^2 \in \mathbb{R}^+$. En particular, como $1 \neq 0$, entonces $1^2 = 1 \in \mathbb{R}^+$.

Sea ahora $n \in \mathbb{N}$ y supongamos que $n \in \mathbb{R}^+$. Entonces, como $\mathbb{R}^+$ es cerrado para la adición, resulta $n + 1 \in \mathbb{R}^+$. Así, pues, procediendo por inducción, concluimos que la prueba por inducción es completa.

Proposición 2). El conjunto $\mathbb{N}$ de los números naturales es cerrado con respecto a la adición y multiplicación.

Es decir, $\forall\, a, b \in \mathbb{N} \Rightarrow a + b \in \mathbb{N}$ y $a \cdot b \in \mathbb{N}$.

Demostración. Fijando de antemano $a \in \mathbb{N}$, razonamos por inducción sobre b. Tendremos:

1) Si $b = 1$, entonces $a + b = a + 1 \in \mathbb{N}$, ya que $\mathbb{N}$ es un conjunto aritmético.

Supongamos ahora $b \in \mathbb{N}$, entonces $a + b \in \mathbb{N}$ por hipótesis de inducción. Probaremos que también $a + (b + 1) \in \mathbb{N}$.

En efecto, $a + (b + 1) = (a + b) + 1 \in \mathbb{N}$, por la hipótesis de inducción y la aritmeticidad de $\mathbb{N}$.

Luego, la prueba por inducción para la clausura de $\mathbb{N}$ respecto a la adición, es completa.

2) Si $b = 1$, entonces $a \cdot b = a \cdot 1 = 1 = a \in \mathbb{N}$.

Supongamos ahora $b \in \mathbb{N}$, entonces por hipótesis de inducción se tiene $a \cdot b \in \mathbb{N}$. Mostraremos que también $a \cdot (b + 1) \in \mathbb{N}$.

En efecto, $a \cdot (b + 1) = a \cdot b + a \in \mathbb{N}$, por la hipótesis de inducción y de que $\mathbb{N}$ es cerrado con respecto a la adición.

Luego, la prueba por inducción para la cerradura de $\mathbb{N}$ con respecto a la multiplicación, es completa.

Otras propiedades de los números naturales, aunque ya conocidas en el Capítulo VII, pero que ahora pueden probarse por inducción, son las siguientes, y cuya demostración se pide al lector:

Proposición 3). $n \in \mathbb{N}$, $n \neq 1$, implica $n > 1$.

Es decir, 1 es el menor entero natural.

Proposición 4). Cualquiera sea el número natural n, no existe ningún número natural entre n y $n - 1$, y por consiguiente no existe ningún número natural comprendido entre n y $n + 1$.

Proposición 5). Si a y b son números naturales tales que $a > b$, entonces la diferencia $a - b$ es un número natural.

Teorema. (Principio de Buena Ordenación). Cada subconjunto no vacío de $\mathbb{N}$ tiene un elemento mínimo (es decir, primer elemento).

Demostración. En el Capítulo VII, sobre el número natural, dimos la demostración de este importante teorema. Daremos ahora otra demostración del mismo, utilizando el Axioma de Plenitud y en la parte que se refiere al ínfimo.

Sea $S \subset \mathbb{N}$, $S \neq \emptyset$; S es en particular un subconjunto de $\mathbb{R}$.

Por la Proposición 1) sabemos que $\mathbb{N} \subset \mathbb{R}^+$; por lo tanto, se tiene:

$$0 < x\,, \forall\, x \in \mathbb{N}$$

y como $S \subset \mathbb{N}$, entonces S está acotado inferiormente; por el axioma del ínfimo resulta que S tiene una cota inferior máxima l en $\mathbb{R}$.

Ahora bien, por ser $l < l + 1$, resulta entonces por la definición de ínfimo que existe por lo menos un $m \in S$ tal que:

$$l \leq m < l + 1$$

Probaremos que $m \leq x$ para todo $x \in S$; esto es, que m es el elemento mínimo de S.

En efecto, supongamos por el contrario que exista un $x \in S$ tal que $x \leq m$

Por ser l el ínfimo de S, será

$$l \leq x < m < l + 1$$

De $l \leq x$ resulta, $l + 1 \leq x + 1$; luego

$$l \leq x < m < l + 1 \leq x + 1$$

de donde, $$x < m < x + 1$$

lo que es falso, en virtud de la Proposición 4).

Esta contradicción prueba que no existe ningún $x \in S$ tal que $x < m$; es decir,

$$m \leq x, \forall x \in S$$

Luego, m es el mínimo elemento S; esto es, el elemento que es menor o igual a todos los demás.

Esta importante propiedad que acabamos de demostrar no la verifica ningún otro sistema numérico y la expresamos diciendo que el conjunto $\mathbb{N}$ de los números naturales está bien ordenado.

II. *Números enteros*

Definición. En el cuerpo $\mathbb{R}$ de los números reales, designamos por $\mathbb{N}^-$ al conjunto de los opuestos de los enteros naturales. Siendo $\mathbb{N} \subset \mathbb{R}^+$, resulta entonces que $\mathbb{N}^- \subset \mathbb{R}^-$.

Los elementos de $\mathbb{N}^-$ los llamaremos ENTEROS NEGATIVOS y los de $\mathbb{N}$, los ENTEROS POSITIVOS.

Podemos:

$$\mathbb{Z} = \mathbb{N} \cup \mathbb{N}^- \cup \{0\}$$

y siendo los conjuntos $\mathbb{N}$, $\mathbb{N}^-$, $\{0\}$ disjuntos a pares, entonces cada elemento de $a \in \mathbb{Z}$ cumple una y sólo una de las tres condiciones siguientes:

1) a es un entero natural o positivo

2) a es un entero negativo

3) $a = 0$.

Los elementos de $\mathbb{Z}$ los llamaremos ENTEROS RACIONALES, o, simplemente, NUMEROS ENTEROS.

Teorema. El conjunto $\mathbb{Z}$ de los números enteros es un dominio de integridad.

Demostración. Para ello debemos probar, en primer lugar, que la adición y la multiplicación de $\mathbb{R}$ restringidas a $\mathbb{Z}$ son operaciones en $\mathbb{Z}$; es decir, que $\mathbb{Z}$ es cerrado con respecto a esas operaciones.

1) *Para la adición se tiene:* Probaremos que

$$\forall a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$$

En efecto, descartando el caso trivial de que uno de los sumando sea cero, hay tres casos que contemplar:

$$s = a + b, \quad a = a - b, \quad s = -a - b, \quad \text{con } a, b \in \mathbb{N}$$

Ahora bien, como $a + b \in \mathbb{N}$, y, $-a - b = -(a + b) \in \mathbb{N}^-$, resulta que la suma s en los casos primero y tercero pertenece a $\mathbb{Z}$.

Veamos ahora el segundo de estos casos, es decir, cuando $s = a - b$. Dos posibilidades habrá que contemplar y que son:

$$a < b \quad \text{y} \quad a > b$$

Si $a < b$, entonces por la Proposición 5), $b - a \in \mathbb{N}$; luego,

$$s = a - b = -(b - a) \in \mathbb{N}^-$$

Si $a > b$, entonces por la misma proposición, $s = a - b \in \mathbb{N}$.

Luego, en este segundo caso resulta que también la suma s pertenece a $\mathbb{Z}$.

Finalmente, no excluyendo el caso $a = b$, se tiene $a - b = 0 \in \mathbb{Z}$. En consecuencia, en todos los casos $s \in \mathbb{Z}$; esto es, $\mathbb{Z}$ es cerrado con respecto a la adición.

Como consecuencia de esto, es fácil ver que también el conjunto $\mathbb{Z}$ es cerrado con respecto a la sustracción.

En efecto, sea $a, b \in \mathbb{Z}$; entonces es inmediato que:

$$-b \in \mathbb{Z}$$

luego, $a - b = a + (-b) \in \mathbb{Z}$.

2) *Para la multiplicación se tiene:* Probaremos que $\forall a, b \in \mathbb{Z}$ $a \cdot b \in \mathbb{Z}$.

En efecto, sean $a, b \in \mathbb{Z}$. Si $a \cdot b \neq 0$, tenemos, como el caso de la adición, tres posibilidades:

$$p = a \cdot b, \quad p = a \cdot (-b), \quad p = (-a) \cdot (-b), \text{ con } a, b \in \mathbb{N}$$

Ahora bien, como $a \cdot b \in \mathbb{N}$, $(-a) \cdot (-b) = ab \in \mathbb{N}$ y $a(-b) = -ab \in \mathbb{N}^-$, resulta que el producto en las tres posibilidades pertenece a $\mathbb{Z}$.

Finalmente, no excluyendo el caso de que uno de los factores es cero, digamos $b = 0$, entonces $a \cdot b = a \cdot 0 = 0 \in \mathbb{Z}$.

Por consiguiente, en todos los casos $p \in \mathbb{Z}$; esto es, $\mathbb{Z}$ es cerrado con respecto a la multiplicación.

Este resultado y los anteriores nos muestran que el conjunto $\mathbb{Z}$ de los números enteros es cerrado con respecto a las tres operaciones racionales de adición, sustracción y multiplicación.

3) Por último, para probar que $\mathbb{Z}$ es un dominio de integridad, hay que demostrar que se verifican los axiomas correspondientes.

Pero, observando que aquellos axiomas que establecen identidades, como ser: las propiedades asociativas, conmutativas de la adición y multiplicación y la distributiva de la multiplicación respecto a la adición, como se verifican para todos los elementos de $\mathbb{R}$, se verificarán también para los elementos de cualquier subconjunto de $\mathbb{R}$. Luego, en particular, se verifican para $\mathbb{Z}$.

Resta probar entonces aquellos axiomas que se refieren a la existencia de elementos neutros para la adición y la multiplicación y de simétricos.

En efecto, existe en $\mathbb{Z}$ un elemento que es neutro para la adición, ya que por definición $0 \in \mathbb{Z}$, teniéndose:

$$0 + a = a + 0 = a, \forall\, a \in \mathbb{Z}$$

Por otra parte, cada elemento de $\mathbb{Z}$ tiene opuesto en $\mathbb{Z}$; luego, para cualquier $a \in \mathbb{Z}$ se tiene $-a \in \mathbb{Z}$, ya que: $a \in \mathbb{N}$ implica $(-a) \in \mathbb{N}^-$ y $(-a) \in \mathbb{N}$ implica $a \in \mathbb{N}^-$. También existe en $\mathbb{Z}$ un elemento que es neutro para la multiplicación, ya que por definición $1 \in \mathbb{Z}$, teniéndose para cada $a \in \mathbb{Z}$ la relación $a \cdot 1 = 1 \cdot a = a$.

De todo lo anterior resulta entonces que $\mathbb{Z}$ es un anillo conmutativo y con unidad. Además, como en $\mathbb{R}$ no existen divisores de cero, tampoco los habrá en $\mathbb{Z}$.

Queda probado así que $\mathbb{Z}$ es un dominio de integridad, y el teorema está demostrado.

Teorema. $\mathbb{Z}$ no es un cuerpo.

Demostración. Bastará demostrar que cualquiera que sea el número entero a, si $a \neq 0$, $a \neq 1$, $a \neq -1$, el inverso de a no es un número entero; esto es, que $a^{-1} \notin \mathbb{N}^+$ ni $a^{-1} \notin \mathbb{N}^-$, según que a sea positivo o negativo.

En efecto, sea $a \in \mathbb{Z}$, $a \neq 0$, $a \neq 1$, $a \neq -1$; luego $a \in \mathbb{N}$ o $(-a) \in \mathbb{N}$.

Si $a \in \mathbb{N}$, entonces $a > 0$ y, por tanto, su inverso en $\mathbb{R}$ es $a^{-1} > 0$. Como $a \neq 1$, entonces debe ser $a > 1$.

Multiplicando esta última desigualdad por a^{-1}, resulta:

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

o sea,

$$1 > a^{-1}$$

luego, $a^{-1} \notin \mathbb{N}$ y, por tanto, $a^{-1} \notin \mathbb{Z}$.

Así hemos probado que el inverso de todo entero positivo y distinto de 1, no es un número entero.

Supongamos ahora que $(-a) \in \mathbb{N}$, o sea, que $a < 0$ y, por tanto, su inverso en $\mathbb{R}$ es $a^{-1} < 0$.

Entonces, para que $a^{-1} \in \mathbb{Z}$ es necesario que $(-a^{-1}) \in \mathbb{N}$. Como $(-a) \in \mathbb{N}$ y $(-a) \neq 1$, entonces por lo anteriormente demostrado para el caso $a > 0$, resulta que $(-a^{-1}) \notin \mathbb{N}$.

Pero, por otra parte, se tiene:

$$-a^{-1} = -(a^{-1})$$

porque,

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

Por lo tanto, si $(-a^{-1}) \notin \mathbb{N}$, entonces también $a^{-1} \in \mathbb{N}$, y lo que implica $a^{-1} \notin \mathbb{Z}$.

Así hemos probado también que el inverso de todo entero negativo y distinto de (-1), no es un número entero. Este resultado y el anterior demuestran que el conjunto $\mathbb{Z}$ de los números enteros no es un cuerpo, y el teorema está demostrado.

Como una aplicación inmediata de los enteros racionales consideremos el problema de la potenciación de números reales de exponente entero.

Definición. Cualquiera que sea el número real a, damos en primer lugar la siguiente definición por recurrencia:

$$\begin{cases} a^1 = a \\ a^{n+1} = a^n \cdot a, \quad n \in \mathbb{N} \end{cases}$$

que nos define la operación de potenciación para todo exponente natural n.

Teorema. Las potencias de exponente natural de números reales, verifican las propiedades siguientes:

1) $a^m \cdot a^n = a^{m+n}, \forall\, a \in \mathbb{R}$ y $\forall\, m, n \in \mathbb{N}$

2) $(a^m)^n = a^{mn}, \forall\, a \in \mathbb{R}$ y $\forall\, m, n \in \mathbb{N}$

3) $(a \cdot b)^n = a^n \cdot b^n, \forall\, a, b \in \mathbb{R}$ y $\forall\, n \in \mathbb{N}$

4) $1^n = 1, \forall\, n \in \mathbb{N}$

Demostración. Todas estas reglas de cálculo se demuestran por inducción. Sólo demostraremos algunas, quedando las demás con ejercicios.

1) Fijando de antemano m, haremos una inducción sobre n; tendremos:
Para n = 1, se tiene

$$a^m \cdot a^1 = a^m \cdot a = a^{m+1}$$

lo cual es evidente según la definición anterior; luego, la relación 1) se verifica para n = 1.

Supongamos ahora la propiedad cierta para un n cualquiera:

$$a^m \cdot a^n = a^{m+n}$$

y probémosla para n +1; entonces, por la hipótesis hecha y por las definiciones, se tiene:

$$a^m \cdot a^{n+1} = a^m \cdot (a^n \cdot a) = (a^m \cdot a^n) \cdot a = a^{m+n} \cdot a = a^{m+n+1}$$

resultado que es de la misma forma que el de la hipótesis hecha. Luego, la inducción es completa.

Como consecuencia resulta:

$$a^m \cdot a^n = a^n \cdot a^m$$

2) Demostrarla como ejercicio.

3) En primer lugar demostraremos que:

$$a \cdot b^m = b^m \cdot a$$

En efecto, si m = 1, se verifica:

$$a \cdot b^1 = b^1 \cdot a$$

o sea,

$$a \cdot b = b \cdot a$$

lo cual es evidente en virtud de la conmutatividad del cuerpo $\mathbb{R}$.

Supongamos ahora la propiedad cierta para m, es decir,

$$a \cdot b^m = b^m \cdot a$$

e intentemos probarla para n +1; entonces, por la hipótesis hecha y por la definición, se tiene:

$$a \cdot b^{m+1} = a \cdot (b^m \cdot b) = (a \cdot b^m) \cdot b = (b^m \cdot a)\, b = b^m \cdot (ab) =$$

$$= b^m \cdot (b \cdot a) = (b^m \cdot b) \cdot a = b^{m+1} \cdot a$$

resultado conforme a la hipótesis que acabamos de hacer.

Con este antecedente, probemos ahora la fórmula:

$$a^m \cdot b^m = (a \cdot b)^m$$

Haremos una inducción sobre m; tenemos:
Si m = 1, resulta:

$$a^1 \cdot b^1 = (a \cdot b)^1$$

o sea,

$$a \cdot b = a \cdot b$$

lo cual es verdad.

Supuesto que se verifica:

$$a^m \cdot b^m = (a \cdot b)^m$$

entonces se tendrá:

$$a^{m+1} \cdot b^{m+1} = (a^m \cdot a) \cdot (b^m \cdot b) = (a^m \cdot a \cdot b^m) \cdot b =$$

$$= (a^m \cdot (a \cdot b^m)) \cdot b = (a^m \cdot (b^m \cdot a)) \cdot b =$$

$$= ((a^m \cdot b^m) \cdot a) \cdot b = (a^m \cdot b^m) \cdot (a \cdot b)$$

$$= (a \cdot b)^m (a \cdot b) = (a \cdot b)^{m+1}$$

luego, la inducción es completa.

4) Probarla como ejercicio.

Definición. $a^0 = 1, \forall\, a \in \mathbb{R}$

En virtud de esta definición, las leyes anteriores valen también, ya que se tienen:

1') $a^m \cdot a^0 = a^{m+0}$

$a^m \cdot 1 = a^m$

$a^m = a^m$

2') $(a^m)^0 = a^{m\,0}$

$1 = a^0$

$1 = 1$

3') $a^0 \cdot b^0 = (a \cdot b)^0$

$1 \cdot 1 = 1$

$1 = 1$

4') $1^0 = 1$, por definición.

Por consiguiente, las fórmulas del teorema anterior valen para todos los enteros no negativos. Probaremos que ellas valen también para todos los enteros negativos. Para esto, es necesario demostrar, primeramente, el teorema siguiente:

Teorema. Se tiene:

$$(a^n)^{-1} = (a^{-1})^n, \forall a \in \mathbb{R}, \forall n \in \mathbb{N}$$

Demostración. Procediendo por inducción sobre n, tendremos:
Si n = 1, se verifica:

$$(a^1)^{-1} = (a^{-1})^1$$

o sea,

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

lo cual es verdad, según la penúltima definición. Ahora, supongamos que se tenga:

$$(a^n)^{-1} = (a^{-1})^n$$

entonces, por definición y por la fórmula $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$, resulta:

$$(a^{n+1})^{-1} = (a^n \cdot a)^{-1} = (a^n)^{-1} \cdot a^{-1}$$

y por la hipótesis de inducción, se escribe:

$$(a^{n+1})^{-1} = (a^{-1})^n \cdot (a^{-1}) = (a^{-1})^{n+1}$$

luego, la inducción es completa, y el teorema está demostrado.

Este teorema nos permitirá definir las potencias de exponente entero negativo.

Definición. $a^{-n} = (a^n)^{-1} = (a^{-1})^n = \frac{1}{a^n}$ para todo $a \in \mathbb{R}$ y $\forall n \in \mathbb{N}$.

Teorema. $\forall a, b \in \mathbb{R}$ y $\forall m, n \in \mathbb{N}$ se verifican:

1) $a^{-m} \cdot a^{-n} = a^{-m-n}$
2) $(a^m)^{-m} = a^{-mn}; (a^{-m})^n = a^{-mn}; (a^{-m})^{-n} = a^{mn}$
3) $a^{-n} \cdot b^{-n} = (a \cdot b)^{-n}$
4) $1^{-n} = 1$

Demostración. Demostraremos sólo algunas y las demás quedan como ejercicios.

1) Hacerla como ejercicio

2) $(a^m)^{-n} = ((a^m)^n)^{-1} = (a^{mn})^{-1} = a^{-mn}$;

$(a^{-m})^n = ((a^m)^{-1})^n = ((a^{-1})^m)^n = a^{-mn}$

$(a^{-m})^{-n} = ((a^m)^{-1})^{-n} = ((a^{-1})^m)^{-n} = (a^{-1})^{-mn} = a^{(-)(-mn)} = a^{mn}$

3) Probarla como ejercicio.

4) $1^{-n} = (1^n)^{-1} = (^{-1})^n = 1^n = 1$

En conclusión, las fórmulas valen todas para exponentes enteros cualesquiera.

EJERCICIOS

1) Demostrar por inducción las proposiciones 3), 4) y 5) de la sección 11.4, relativas a los números naturales.
2) Completar las demostraciones de los teoremas relativos a las leyes de cálculo de potencias con exponentes enteros.
3) Se definen las reglas siguientes:

$$\begin{cases} 0 \cdot a = 0, \forall a \in \mathbb{R} \\ 1 \cdot a = a, \forall a \in \mathbb{R} \\ (n+1)a = na + a, \forall a \in \mathbb{R} \quad y \quad \forall n \in \mathbb{N} \end{cases}$$

Demostrar, entonces, las leyes siguientes:

a) $ma + na = (m + n)a$
b) $n(ma) = (nm)a$
c) $na + nb = n(a + b)$

4) Demostrar que,

$$-(na) = n(-a), \forall n \in \mathbb{N}$$

5) Se define la regla siguiente:

$$(-n)a = -(na) = n(-a), \forall a \in \mathbb{R} \quad y \quad \forall n \in \mathbb{N}$$

Demostrar, entonces, las leyes siguientes:

a) $(-m)a + (-n)a = -(m + n)a$
b) $(-n) \cdot (ma) = (-nm)a$; $n(-m)a = (-nm)a$;
$(-n) \cdot (-m)a = (nm)a$

c) $(-m)a + (-m)b = (-m)(a + b)$

6) Demostrar las fórmulas siguientes:

a) $(m\,a)\cdot b = a\,(m\,b) = m\,(ab)$

b) $(m\,a)\cdot(n\,b) = (m\,n)\,(ab)$

cualesquiera sean $a, b \in \mathbb{R}$ y $m, n \in \mathbb{Z}$.

III. *Números Racionales*

Definición. Los números reales de la forma $a\cdot b^{-1}$, donde a y b son números enteros y $b \neq 0$, se llamarán NUMEROS RACIONALES, y el conjunto de todos ellos será denotado por $\mathbb{Q}$.

Luego:

$$\mathbb{Q} = \{x \in \mathbb{R} : x = a\cdot b^{-1} = \frac{a}{b},\ a, b \in \mathbb{Z} \text{ y } b \neq 0\}$$

Un número racional es entonces un cociente de enteros, y si:

$$\frac{a}{b} = \frac{c}{d}, \text{ con } a, b, c, d \in \mathbb{Z} \quad \text{y} \quad b \neq 0, d \neq 0$$

estos dos cocientes definen el mismo número racional. Luego, un mismo número racional puede representarse por diferentes cocientes de enteros, todos iguales entre sí.

Teorema. El conjunto $\mathbb{Z}$ de los números enteros es un subconjunto propio del conjunto $\mathbb{Q}$ de los números racionales.

Demostración. Cualquiera que sea $a \in \mathbb{Z}$ podemos escribir:

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

luego, $a \in \mathbb{Q}$, es decir, que $\mathbb{Z} \subset \mathbb{Q}$.

Por otra parte, existen números racionales que no son enteros, pues cualquiera que sea el número a, $a \neq 0$, se tiene:

$$a^{-1} = 1\cdot a^{-1} = \frac{1}{a} \in \mathbb{Q}$$

En consecuencia, habiendo visto que $\mathbb{Z} \subset \mathbb{Q}$ y que existen algunos elementos de $\mathbb{Q}$ que no pertenecen a $\mathbb{Z}$ concluimos entonces que $\mathbb{Z}$ es un subconjunto propio de $\mathbb{Q}$, es decir, $\mathbb{Z} \subset \mathbb{Q}$, y el teorema está demostrado.

Observación. Recuérdese que de la definición de $\mathbb{Z}$, se tiene que $\mathbb{N}$ es un subconjunto propio de $\mathbb{Z}$, y ahora, por el teorema que se acaba de demostrar, es $\mathbb{Z}$ un subconjunto propio de $\mathbb{Q}$, por tanto, se tiene la cadena de inclusiones:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Teorema. $\mathbb{Q}$ es un cuerpo conmutativo.

Demostración. Para ello deberemos probar, en primer lugar, que la adición y la multiplicación de $\mathbb{R}$ restringidas a $\mathbb{Q}$ son operaciones en $\mathbb{Q}$; esto es, que $\mathbb{Q}$ es cerrado con respecto a esas operaciones.

En efecto, sean $x, y \in \mathbb{Q}$, $x = \frac{a}{b}$, $y = \frac{c}{d}$, con $a, b, c, d, \in \mathbb{Z}$ y $b \neq 0$, $d \neq 0$. Tendremos:

$$x + y = \frac{a}{b} + \frac{c}{d} = a\cdot b^{-1} + c\cdot d^{-1} = a\cdot b^{-1}\cdot 1 + c\,d^{-1}\cdot 1$$

$$x + y = a\cdot b^{-1}\,d^{-1}\,d + c\,d^{-1}\cdot b^{-1}\,b$$

$$x + y = (a\,d + b\,c)\,b^{-1}\,d^{-1} = (a\,d + b\,c)\cdot(b\,d)^{-1}$$

$$x + y = \frac{a\,d + b\,c}{b\,d} \in \mathbb{Q}$$

$$x \cdot y = \frac{a}{b}\cdot\frac{c}{d} = a\cdot b^{-1}\cdot c\cdot d^{-1} = (a\cdot c)\cdot(b\,d)^{-1}$$

$$x \cdot y = \frac{a\cdot c}{b\cdot d} \in \mathbb{Q}$$

ya que, $a\,d + b\,c \in \mathbb{Z}$, $a\,c, b\,d \in \mathbb{Z}$ y $b\,d \neq 0$.

Luego, $\mathbb{Q}$ es cerrado con respecto a la adición y multiplicación.

Por último, en segundo lugar, para probar que $\mathbb{Q}$ es un cuerpo conmutativo, hay que mostrar que se verifican los axiomas correspondientes a la estructura de cuerpo conmutativo. Aquéllos que establecen identidades, como son: las propiedades asociativas y conmutativas de la adición y multiplicación y la distributiva de la multiplicación respecto a la adición, como se verifican para los elementos de $\mathbb{R}$, se verifican también en cualquier subconjunto de $\mathbb{R}$, en particular en $\mathbb{Q}$.

Resta solamente mostrar entonces los axiomas que se refieren a la existencia de elementos neutros para la adición y multiplicación y, además, los de opuestos e inversos. En efecto, se tiene que:

1) Existe en $\mathbb{Q}$ un elemento neutro para la adición, desde que:

$$0 = \frac{0}{1} \in \mathbb{Q}$$

2) Existe en Q un elemento neutro para la multiplicación, desde que:

$$1 = \frac{1}{1} \in \mathbb{Q}$$

3) Cada elemento de $\mathbb{Q}$ tiene un opuesto, desde que:

$$x = \frac{a}{b} \in \mathbb{Q} \text{ implica } -x = -\frac{a}{b} = \frac{-a}{b} \in \mathbb{Q}$$

4) Cada elemento no nulo de Q tiene un inverso, desde que:

$$x = \frac{a}{b} \in \mathbb{Q}, a \neq 0, b \neq 0, \text{ implica } x^{-1} = \left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \in \mathbb{Q}$$

En consecuencia, queda demostrado así que $\mathbb{Q}$ es un cuerpo conmutativo. Más precisamente, $\mathbb{Q}$ es un subcuerpo de $\mathbb{R}$. Por consiguiente, $\mathbb{Q}$ es cerrado con respecto a las cuatro operaciones racionales: adición, sustracción, multiplicación y división. El teorema está demostrado.

Teorema. Cada subcuerpo de $\mathbb{R}$ contiene a $\mathbb{Q}$. En otras palabras, $\mathbb{Q}$ es la intersección de todos los subcuerpos de $\mathbb{R}$ (por lo tanto, el más pequeño subcuerpo de $\mathbb{R}$).

Demostración. Sea S un subcuerpo de $\mathbb{R}$; es decir, S cerrado con respecto a las cuatro operaciones racionales.

Ahora bien, siendo S, en particular, cerrado con respecto a la adición y sustracción, resulta que $\mathbb{Z} \subset S$.

Sea ahora $a, b \in \mathbb{Z}, b \neq 0$, entonces $\frac{a}{b} \in S$, ya que S es cerrado con respecto a la división. Luego, se tiene:

$$\mathbb{Q} \subset S$$

y el teorema está demostrado.

Observación. Considerando la relación de orden definida entre los números reales $\mathbb{R}$ restringida al subconjunto $\mathbb{Q}$ de los números racionales, es claro que $\mathbb{Q}$ resulta ser un cuerpo ordenado. Más adelante probaremos que no es completo.

11.5. A. Las consecuencias inmediatas de los axiomas de Hilbert, vienen dadas en los ejemplos y ejercicios que siguen:

EJEMPLOS Y EJERCICIOS

1) Demostrar que para todo $a, b, c \in \mathbb{R}$, se verifica:

$$a \cdot (b - c) = a \cdot b - a \cdot c$$

$$(b - c) \cdot a = b \cdot a - c \cdot a$$

2) En $\mathbb{R}$ se verifican las propiedades siguientes:

a) $a \cdot 0 = 0 \cdot a = 0, \forall a \in \mathbb{R}$

b) $(-a) \cdot b = -ab; \quad a \cdot (-b) = -ab$

c) $(-a) \cdot (-b) = ab$

(Sugerencia: utilizar el ejercicio 1)).

3) Si $a \cdot b = 0$, entonces es $a = 0$, o es $b = 0$

4) Es $\frac{a}{b} = \frac{c}{d}$ sí, y sólo si $a\,d = b\,c$ $(b \neq 0, d \neq 0)$

5) Demostrar que en $\mathbb{R}$ se verifican las propiedades siguientes:

a) $\frac{a}{b} \pm \frac{c}{d} = \frac{a\,d \pm b\,c}{b\,d}$ $(b \neq 0, d \neq 0)$

b) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ $(b \neq 0, d \neq 0)$

c) $\frac{a}{b} = \frac{a\,c}{b\,c}$ $(b \neq 0, c \neq 0)$

d) $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ $(b \neq 0, a \neq 0)$

e) $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a\,d}{b\,c}$ $(b \neq 0, d \neq 0, c \neq 0)$

f) $\frac{\frac{a}{b}}{c} = \frac{a}{bc}$ $(b \neq 0, c \neq 0)$

g) $\frac{c}{\frac{a}{b}} = \frac{bc}{a}$ $(b \neq 0, a \neq 0)$

6) En $\mathbb{R}$ se verifican las propiedades siguientes:

a) $\frac{-a}{b} = -\frac{a}{b}$ $(b \neq 0)$

b) $\frac{a}{-b} = -\frac{a}{b} \quad (b \neq 0)$

c) $\frac{-a}{-b} = \frac{a}{b} \quad (b \neq 0)$

7) Demostrar que:

a) Si $a = b, a \neq 0, b \neq 0$, entonces $\frac{1}{a} = \frac{1}{b}$

b) Si $a = -b$, entonces $b = -a$

c) Si $a = \frac{1}{b}, a \neq 0, b \neq 0$, entonces $b = \frac{1}{a}$

8) Demostrar que en $\mathbb{R}$ se verifica:

a) $1 \neq 0$

b) El cero no tiene inverso.

B) *Números reales positivos y negativos*

Definición. Un número real r es *positivo* si $r > 0$, y *negativo* si $r < 0$.

Luego, dado un elemento cualquiera $a \in \mathbb{R}$, resulta por la ley de tricotomía aplicada al par $(a, 0)$, se verifica siempre una y una sola de las siguientes relaciones:

$$a < 0, \qquad a = 0, \qquad 0 < a$$

es decir, el elemento a es necesariamente negativo, nulo o positivo.

Por consiguiente, $\mathbb{R}$ está dividido en tres subconjuntos disjuntos dos a dos, a saber: el de los elementos negativos $\mathbb{R}^-$, el de los elementos positivos $\mathbb{R}^+$ y el que tiene por único elemento a 0.

Luego:

$$\mathbb{R} = \mathbb{R}^{-1} \cup \{0\} \cup \mathbb{R}^+ = \mathbb{R}^- + \{0\} + \mathbb{R}^+$$

El subconjunto $\mathbb{R}^+$ de los positivos es cerrado para la suma y el producto.

En efecto, sean $a, b \in \mathbb{R}$ dos elementos cualesquiera; entonces, por la ley de monotonía de la adición, se escribe:

$$0 < a \Rightarrow 0 + b < a + b, \text{ o sea } b < a + b$$

y de las raciones:

$$0 < b \quad y \quad b < a + b$$

por transitividad de la relación »<«, resulta:

$$0 < a + b$$

es decir, la suma de positivos es positiva.

Análogamente, aplicando la ley de monotonía de la multiplicación, se obtiene:

$$0 < a \text{ y } 0 < b \Rightarrow 0 \cdot b < a \cdot b, \text{ o sea, } 0 < a \cdot b$$

es decir, el producto de positivos es positivo.

En consecuencia:

$$\forall a, b \in \mathbb{R}^+ \Rightarrow a + b \in \mathbb{R}^+ \text{ y } a \cdot b \in \mathbb{R}^+$$

es decir, $\mathbb{R}^+$ es un conjunto *estable* para la adición y la multiplicación de $\mathbb{R}$.

EJERCICIOS

1) Sean $a, b \in \mathbb{R}$; entonces se verifica:

a) Es $a < b$ si, y sólo si, $a - b < 0$

b) Es $a > b$ si, y sólo si, $a - b > 0$

c) Es $a < b$ si, y sólo si, $-a > -b$

d) Es $a > b$ si, y sólo si, $-a < -b$

e) Es $a > 0$ si, y sólo si, $-a < 0$

f) Es $a < 0$ si, y sólo si, $-a > 0$

g) Es $a > 0$, si, y sólo si, $a^{-1} = \frac{1}{a} > 0$

h) Es $a < 0$ si, y sólo si, $a^{-1} = \frac{1}{a} < 0$

i) $a \neq 0 \Rightarrow a^2 > 0$; en particular, $1 > 0$

2) Sea $a \in \mathbb{R}$ arbitrario; entonces se verifica:

a) $a < a + 1$

b) $a - 1 < a$

3) En $\mathbb{R}$ se verifican las relaciones siguientes:

a) $a < b \wedge c < d \Rightarrow a + c < b + d$

b) $a < b \wedge c < d \Rightarrow a \cdot c < b \cdot d, (a > 0, b > 0, c > 0, d > 0)$

c) $a < b \wedge c > d \Rightarrow a - c < b - d$

d) $a > b \wedge c < d \Rightarrow a - c > b - d$

e) $a < b \wedge c < 0 \Leftrightarrow ac > bc$

f) $a > b \wedge c < d \Leftrightarrow a \cdot c < b \cdot c$

4) Demostrar que en $\mathbb{R}^+$ se verifican las propiedades siguientes:

a) Si $a < b$, entonces $a^{-1} > b^{-1}$

b) Si $a > b$, entonces $a^{-1} < b^{-1}$

c) $a < b \wedge c > d \Rightarrow \frac{a}{c} < \frac{b}{d}$

d) $a > b \wedge c < d \Rightarrow \frac{a}{c} > \frac{b}{d}$

e) Si $a > 1$, entonces $a^2 > a$

f) Si $a < 1$, entonces $a^2 < a$

g) Si $a < b$, entonces $a^2 < b^2$

h) Si $a > b$, entonces $a^2 > b^2$

i) Si $a < b$, entonces $a^n < b^n$, $n \in \mathbb{N}$

j) Si $a > b$, entonces $a^n > b^n$, $n \in \mathbb{N}$

k) Si $a^n < b^n$, $n \in \mathbb{N}$, entonces es $a < b$

l) Si $a^n > b^n$, $n \in \mathbb{N}$, entonces es $a > b$

(Sugerencia: los ejercicios i, j, k, l, se prueban fácilmente utilizando el método de reducción al absurdo y aplicando la ley de tricotomía.

C. *Intervalos de números reales*

Definiciones. Sean dados dos números reales a y b tales que $a < b$. Entonces, definimos los conceptos siguientes:

a) Llamaremos *intervalo abierto*, $]a, b[$, el conjunto de todos los números reales x tales que $a < x < b$.

$$]a, b[= \{x \in \mathbb{R} : a < x < b\}$$

b) Llamaremos *intervalo cerrado*, $[a, b]$, el conjunto de todos los números reales x tales que $a \leq x \leq b$.

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

c) Llamaremos *intervalo semiabierto* o *semicerrado*, $[a, b[$ o $]a, b]$, el conjunto de todos los números reales x tales que $a < x \leq b$, o $a \leq x < b$.

$$]a, b] = \{x \in \mathbb{R} : a < x \leq b\}$$

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\}.$$

En estos cuatro casos, los números a y b se llaman *extremos del intervalo* y la diferencia $d = b - a$, es la *amplitud del intervalo.*

d) También llamaremos intervalos a los conjuntos siguientes:

$$]a, +\infty[= \{x \in \mathbb{R} : x > a\}$$

$$[x, +\infty[= \{x \in \mathbb{R} : x \geq a\}$$

$$]-\infty, a[= \{x \in \mathbb{R} : x < a\}$$

$$]-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$$

$$]-\infty, +\infty[= \{x \in \mathbb{R} : x \in \mathbb{R}\} = \mathbb{R}$$

Los símbolos $(+\infty)$ y $(-\infty)$ no deben considerarse como números, sino simplemente como signos útiles para abreviar y uniformar las notaciones.

EJEMPLOS

1) Sea S el subconjunto de $\mathbb{R}$ definido por:

$$S = \{x \in \mathbb{R} : 3 < x < 5\}$$

Este conjunto está acotado a ambos lados, inferiormente por 3 y superiormente por 5. Luego, por el axioma de plenitud tiene ínfimo y supremo en $\mathbb{R}$ y que son:

$$\text{Inf}(S) = 3, \quad \text{Sup}(S) = 5$$

ambos no pertenecen a S.
Pero, si se define $S = \{x \in \mathbb{R} : 3 \leq x \leq 5\}$, entonces sí que ambos, ínfimos y supremos, pertenecen a S.

2) Sea ahora, $S = \{x \in \mathbb{R} : x < 3\}$; entonces, el conjunto está solamente acotado superiormente, y por eso sólo tiene supremo en $\mathbb{R}$ y que es 3, que no pertenece a S. El ínfimo no existe.

3) Sea el conjunto

$$S = \{x \in \mathbb{R} : x^2 < 2\} = \{x \in \mathbb{R} : -\sqrt{2} < x < \sqrt{2}\}$$

Este conjunto está acotado inferiormente y superiormente; luego, por el axioma de plenitud tiene ínfimo y supremo en $\mathbb{R}$ y que son:

$$\text{Inf}(S) = -\sqrt{2}, \text{Sup}(S) = \sqrt{2}$$

Pero, si hubiera sido $S = \{x \in \mathbb{R} : x > 0, x^2 < 2\}$, entonces S está acotado inferiormente por 0 y superiormente por $\sqrt{2}$; luego, $\text{Inf}(S) = 0, \text{Sup}(S) = \sqrt{2}$

4) Sea el conjunto

$$S = \{x \in \mathbb{R}\ x^2 > 0\} = \{x \in \mathbb{R} : x > \sqrt{2}, \text{ó } x < -\sqrt{2}\}$$

Este conjunto no está acotado ni inferiormente ni superiormente. Por lo tanto, no existe ni ínfimo ni supremo.

5) Demostrar que el conjunto $\mathbb{Z}^+$ de los enteros positivos no está acotado superiormente.

Demostración. Haremos una prueba indirecta; esto es, supondremos, por el contrargio, que $\mathbb{Z}^+$ tiene una cota superior. Entonces, por ser $\mathbb{Z}^+ \subset \mathbb{R}$ y acotado superiormente, $\mathbb{Z}^+$ tiene, por el axioma de plenitud, supremo en $\mathbb{R}$.
Sea s este supremo o mínimo cota superior.
Luego, se tendrá:

$$x \leq s, \quad \forall x \in \mathbb{Z}^+$$

Ahora bien, si $x \in \mathbb{Z}^+$, también $x + 1 \in \mathbb{Z}^+$, luego:

$$x + 1 \leq s, \quad \forall x \in \mathbb{Z}^+$$

o sea,

$$x \leq s - 1, \quad \forall x \in \mathbb{Z}^+$$

resultado que contradice el hecho de que s es la mínima cota superior de $\mathbb{Z}^+$.
Esta contradicción, demuestra la proposición.

6) Probar que el conjunto $S = \{-2, 0, 1, 3\}$ contiene a su ínfimo y supremo. ¿Cuáles son ellos?

Demostración. Se tiene:

$$-2 \leq x, \quad \forall x \in S$$

$$x \leq 3, \quad \forall x \in S$$

luego, -2 es una cota inferior y la máxima cota inferior de S, y 3 es una cota superior y la mínima cota superior de S. Luego,

$$\text{Inf}(S) = -2 \in S \text{ y } \text{Sup}(S) = 3 \in S.$$

En general, todo conjunto finito $S = \{a_1, a_2, a_3, \ldots, a_n\}$, por el axioma de tricotomía puede ordenarse y su mínimo elemento es el ínfimo del conjunto y su máximo elemento es el supremo.
Luego, todo conjunto finito es acotado y contiene a su ínfimo y supremo.

7) Demostrar que el cuerpo ordenado $\mathbb{Q}$ de los números racionales no es completo.

Demostración. Sólo nos basta dar un ejemplo (contra-ejemplo) de subconjuntos no vacíos de números racionales y acotados superiormente (o inferiormente) que no tienen supremo (o ínfimo) en $\mathbb{Q}$.

En efecto, consideremos, por ejemplo, el conjunto siguiente:

$$S = \{x \in \mathbb{Q} : x > 0, x^2 < 3\}$$

Este conjunto no es vacío, pues $1 \in \mathbb{Q}$ y está acotado superiormente, ya que por ejemplo 3 es una cota superior. Entonces, S como subconjunto de $\mathbb{R}$ tiene supremo en $\mathbb{R}$ y que es $\sqrt{3}$.

Pero, como $\sqrt{3}, \notin \mathbb{Q}$, resulta entonces que S como subconjunto de $\mathbb{Q}$ no tiene supremo en $\mathbb{Q}$.

Por consiguiente, $\mathbb{Q}$ no es cuerpo ordenado completo.

11.6. *Otras propiedades sobre los números reales.* Demostraremos ahora algunas propiedades fundamentales, y por esto muy útiles, de los números reales, utilizando la existencia de cotas superiores mínimas en $\mathbb{R}$, o la existencia de cotas inferiores máximas en $\mathbb{R}$, todas las cuales están garantizadas por el axioma de plenitud.

Anteriormente dijimos que el axioma de plenitud conjuntamente con el axioma de Arquimedes constituyen el axioma de continuidad de los números reales. En efecto, el de Arquimedes asegura la existencia de una cota superior y el de plenitud la existencia de una cota superior mínima.

Sin embargo, debemos advertir que estos dos axiomas no son independientes, ya que el de Arquimedes puede demostrarse como teorema utilizando la primera parte del axioma de plenitud y que se refiere a la cota superior mínima.

En efecto, tenemos el teorema siguiente:

Teorema de Arquimedes. Para todo a, b $\in \mathbb{R}^+$, existe un número natural n tal que:

$$n\,a > b$$

Demostración. Como la propiedad es trivial para $a \geq b$, suponemos entonces que sea $a < b$.

Haremos una prueba indirecta; esto es, supongamos que se tenga por el contrario:

$$b \geq na; \quad \forall n \in \mathbb{N}$$

Consideremos el conjunto S formado por todos los múltiplos naturales de a; es decir,

$$S = \{n\,a : a \in \mathbb{R}^+, \quad n \in \mathbb{N}\}$$

Entonces, se tiene:

1) $S \neq 0$, lo cual es evidente por la definición de S.

2) S está acotado superiormente por b, puesto que:

$$n\,a \leq b, \qquad \forall n \in \mathbb{N}$$

luego, S tiene supremo en IR. Sea c este supremo; es decir:

$$n\,a \leq c, \qquad \forall n \in \mathbb{N}$$

luego también, $(n+1)\,a \leq c, \qquad \forall n \in \mathbb{N}$

o bien, $$n\,a \leq c - a, \qquad \forall n \in \mathbb{N}$$

Ahora bien, como $a > 0$, entonces $c - a < c$; luego $c - a$ es una cota superior de S y menor que su mínima cota superior c, lo que contradice a la hipótesis de que c era el supremo de S en IN.

Esta contradicción demuestra el teorema.

Por consiguiente, si a y b son dos números reales positivos cualesquiera, entonces existe un número natural n tal que:

$$n\,a > b$$

Otras propiedades sobre los números reales son las que pasaremos a estudiar a continuación.

Teorema de Eudoxo. Dado un número real cualquiera r, existe un número natural n mayor que r.

Demostración. Sea $r \in \mathbb{R}$ arbitrario. Entonces tendremos:

1) Si $r \leq 0$, y como $0 < 1$, resulta entonces por transitividad que $r < 1$.

Luego, el teorema está demostrado para el caso de cualquier número real negativo o nulo, puesto que el natural $n = 1$ se verifica la propiedad $n > r$.

2) Es obvio que también vale para el caso $0 < r < 1$, pues $n = 1$ verifica la propiedad $n > r$.

3) Sólo resta considerar el caso $r > 1$.

Por el teorema de Arquimedes se encuentra:

$$r < 1 \cdot n = n \cdot$$

y la propiedad también se verifica en este tercer caso, y el teorema está demostrado en general.

Una consecuencia importante de este teorema es que ningún $r \in \mathbb{R}$ es una cota superior de IN.

En otros términos, IN no está acotado superiormente.

Otra consecuencia derivada de este mismo teorema es la siguiente:

Corolario. Para todo $a > 0$ en IR, existe $n \in \mathbb{N}$, tal que $\frac{1}{n} < a$.

En efecto, por el teorema de Eudoxo, existe $n \in \mathbb{N}$, tal que:

$$n > \frac{1}{a}$$

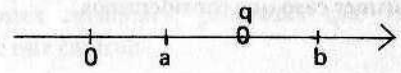
luego, $$\frac{1}{n} < a$$

Teorema. Dados dos números reales cualesquiera a y b tales que $a < b$, existe siempre un número racional q, tal que:

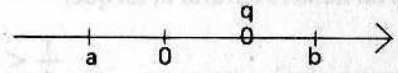
$$a < q < b$$

Demostración. Cabe contemplar los casos siguientes:

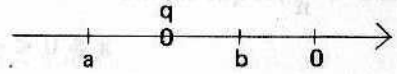
1) $a > 0$ y $b > 0$



2) $a \leq 0$ y $b > 0$



3) $a < 0$ y $b < 0$



Primer caso. Si $a < b$, entonces $b - a > 0$, y por el corolario del teorema anterior, existe un número natural tal que:

$$\frac{1}{n} < b - a \qquad (1)$$

Por otro lado, por el teorema de Eudoxo, sea m el menor número natural tal que:

$$n\,a < m \qquad (2)$$

Entonces, será:

$$m - 1 \leq n\,a$$

o bien,

$$\frac{m-1}{n} \leq a \qquad (3)$$

Pero,

$$\frac{m}{n} = \frac{m-1}{n} + \frac{1}{n}$$

luego, de (1) y (3) resulta:

$$\frac{m}{n} < a + (b - a) = b \qquad (4)$$

y de (2) se deduce que,

$$\frac{m}{n} > a \qquad (5)$$

Por lo tanto, de (4) y (5) se concluye que:

$$a < \frac{m}{n} < b$$

y el número racional $q = \frac{m}{n}$ cumple las condiciones del teorema para este primer caso que consideramos.

Segundo caso. Si $b > 0$, entonces por el corolario del teorema anterior, existe un número natural n, tal que:

$$\frac{1}{n} < b$$

y como $0 < \frac{1}{n}$, lo que implica

$$a \leq 0 < \frac{1}{n}$$

entonces, el número racional $q = \frac{1}{n}$ cumple con las condiciones del teorema:

$$a \leq \frac{1}{n} < b$$

para este segundo caso que consideramos:

Tercer caso. Si $a < b \leq 0$, entonces será $0 \leq -b < -a$.

Luego, estaremos en el primer caso si:

$$0 < -b < -a$$

y en el segundo caso si

$$0 \leq -b, \quad -a > 0$$

Por lo tanto, según ya lo visto para los dos primeros casos, existe un número racional q tal que:

$$-b < q < -a$$

o bien,

$$a < -q < b$$

y como $-q$ es también un número racional, el teorema se verifica también en este tercer caso que consideramos, y queda así completamente demostrado.

Es claro que, decir que entre dos números reales diferentes existe siempre un número racional, equivale a decir que existen infinitos números racionales.

Esta propiedad de que entre dos números reales distintos existe siempre un número racional, y por consiguiente infinitos números racionales, se expresa diciendo que *el conjunto* $\mathbb{Q}$ *de los números racionales es denso en el conjunto* $\mathbb{R}$ *de los números reales.*

Por consiguiente, en un intervalo cualquiera (finito o infinito; abierto, cerrado o semiabierto) de la recta numérica, existen siempre puntos racionales, infinitos puntos racionales, propiedad que ya habíamos señalado en el comienzo de este capítulo.

Teorema. Todo número real es supremo de un conjunto de números racionales.

Demostración. Sea r un número real cualquiera. Consideremos el conjunto S de todos los números racionales menores o iguales que r. Este conjunto no es vacío, pues

$$r - 1 < r$$

y por el teorema anterior existe un número racional q tal que:

$$r - 1 < q < r$$

luego, $q \in S$, y por esto resulta $S \neq \phi$, como afirmábamos. Por otra parte, como S está acotado superiormente por r, entonces tiene supremo en $\mathbb{R}$.

Probaremos que el número real considerado r, es el supremo de S.

En efecto, por el teorema anterior, ningún número real $s < r$ puede ser una cota superior de S, ya que de serlo, habría en S números racionales mayores que s, y por tanto, s no sería cota superior.

Por consiguiente, r es la menor de las cotas superiores de S, es decir, el supremo de S, y el teorema está demostrado.

Teorema. Todo número real es ínfimo de un conjunto de números racionales.

Demostración. Sea r un número real arbitrario. Consideremos el conjunto S de todos los números racionales mayores o iguales que r. Este conjunto no es vacío, puesto que siendo:

$$r < r + 1$$

y por la propiedad de densidad de $\mathbb{Q}$ en $\mathbb{R}$ existe un número racional q tal que:

$$r < q < r + 1$$

lo que implica $q \in S$, y por esto $S \neq \phi$.

Por otro lado, como S está acotado inferiormente por r, entonces tiene ínfimo en $\mathbb{R}$.

Demostraremos que el número real r considerado, es el ínfimo de S.

En efecto, en virtud de la propiedad de densidad de $\mathbb{Q}$ en $\mathbb{R}$, ningún número real s, tal que $r > s$, puede ser cota inferior de S, ya que de serlo habría en S números racionales menores que s, y por tanto, s no sería cota inferior.

Por consiguiente, r es la mayor de las cotas inferiores de S, es decir, el ínfimo de S, y el teorema está demostrado.

Observación. Las propiedades indicadas en los dos últimos teoremas dan una justificación de la idea intuitiva que se aplica en el cálculo de la solución de la ecuación,

$$x^2 = a$$

en donde a es un número positivo y no cuadrado perfecto.

Así, por ejemplo, en la ecuación:

$$x^2 = 2$$

la solución $x = \sqrt{2}$ se la indica por medio de aproximaciones decimales tales como:

$$1^2 < 2 < 2^2$$

$$(1,4)^2 < 2 < (1,5)^2$$

$$(1,41)^2 < 2 < (1,42)^2$$

$$(1,414)^2 < 2 < (1,415)^2$$

$$(1,4142)^2 < 2 < (1,4143)^2$$

. . . . . .

. . . . . .

Luego, podemos dar 1,4142 como un valor racional aproximado por defecto de $\sqrt{2}$, o bien 1,4143 como un valor racional aproximado por exceso de $\sqrt{2}$.

11.7. *Existencia de Números Irracionales en* $\mathbb{R}$. El complemento de $\mathbb{Q}$ en $\mathbb{R}$, es decir, $\mathbb{R} - \mathbb{Q}$, no es vacío; puesto que, por ejemplo,

$$\sqrt{2} \in \mathbb{R} \text{ y } \sqrt{2} \notin \mathbb{Q}.$$

Los elementos de $\mathbb{R} - \mathbb{Q}$ los llamaremos NUMEROS IRRACIONALES.

Es decir, los números reales que no son racionales se llaman números irracionales.

Teorema. Dados dos números reales a y b tales que $a < b$, existe un número irracional x tal que:

$$a < x < b$$

Demostración. 1) Supongamos que sea $0 < a < b$; vamos a mostrar que entre a y b existe un número irracional x de la forma,

$$x = \frac{r}{s}\sqrt{2}, \quad (r, s \in \mathbb{N})$$

En efecto, por el teorema de Eudoxo, existe $s \in \mathbb{N}$ tal que,

$$s > \frac{\sqrt{2}}{b - a}$$

lo que equivale a,

$$s\,a + \sqrt{2} < s\,b \qquad (1)$$

Por otra parte, por el teorema de Eudoxo, sea r el mínimo entero natural mayor que $\frac{s\,a}{\sqrt{2}}$.

$$\frac{s\,a}{\sqrt{2}} < r$$

lo que implica entonces que,

$$r - 1 \leq \frac{sa}{\sqrt{2}} < r$$

y lo que implica,

$$\frac{s\,a}{\sqrt{2}} < r \leq \frac{s\,a + \sqrt{2}}{\sqrt{2}}$$

lo que en virtud de (1), implica a su vez:

$$\frac{s\,a}{\sqrt{2}} < r < \frac{s\,b}{\sqrt{2}}$$

o sea,

$$a < \frac{r}{s}\sqrt{2} < b$$

y el teorema estaría demostrado, para este caso de a y b positivos y tales que $a < b$.

2) Finalmente, supongamos ahora que los números reales a y b sean enteramente arbitrarios, pero tales que $a < b$.

Por el teorema de Eudoxo, existe $n \in \mathbb{N}$ tal que $n > |a|$. Entonces, será $n + a > 0$, y como es $a < b$, tendremos:

$$0 < n + a < n + b$$

Luego, por lo visto en la parte 1), hay un número irracional $\frac{r}{s}\sqrt{2}$ entre $n + a$, $n + b$; es decir

$$n + a < \frac{r}{s}\sqrt{2} < n + b$$

o sea,

$$a < \frac{r}{s}\sqrt{2} - n < b$$

y el teorema se verifica también en este caso general, quedando así completamente demostrado.

Es claro que, decir que entre dos números reales distintos existe siempre un número irracional, equivale a decir que existen infinitos números irracionales.

Este teorema conjuntamente con el teorema análogo que muestra la existencia de números racionales entre dos números reales diferentes, los podemos refundir en uno solo, de la manera siguiente:

Teorema. Cada intervalo abierto de $\mathbb{R}$, $]a, b[$, contiene por lo menos un número racional y, por lo menos, un número irracional.

De esto se sigue que, en realidad, cada intervalo abierto de $\mathbb{R}$ contiene una infinidad de números racionales y una infinidad de números irracionales.

Esta propiedad de que entre dos números reales diferentes existe siempre un número real (infinitos números reales) se expresa diciendo que el conjunto $\mathbb{R}$ de los números reales es denso en sí mismo.

EJERCICIOS

1) Probar por reducción al absurdo que los números $\sqrt{3}$, $\sqrt{5}$, en general, $\sqrt{p}$ siendo p primo, son números irracionales.

2) Probar que si n es un número entero positivo que no es un cuadrado perfecto, entonces $\sqrt{n}$ es irracional.
(Sugerencia: suponer que n no contiene ningún factor cuadrado perfecto mayor que uno).

3) Demostrar que un cuerpo ordenado completo C, todo subconjunto no vacío S de C y acotado inferiormente tiene ínfimo en C.
(Sugerencia: utilizar el axioma del supremo).

4) Demostrar que un cuerpo ordenado completo C, todo subconjunto no vacío S de C y acotado superiormente tiene supremo en C.
(Sugerencia: utilizar el axioma del ínfimo).

11.8. *Existencia de Raíces en* $\mathbb{R}$. Por los teoremas que hemos venido estudiando, hemos visto que la propiedad de plenitud o completidad juega un papel muy importante en el estudio de los números reales.

Ahora veremos también que esta propiedad puede usarse para demostrar que para cada número real positivo a y para cada número natural n, existe un único número real y positivo b tal que:

$$b^n = a$$

Este número b lo designaremos por la notación:

$$b = \sqrt[n]{a}, \text{ o bien } b = a^{\frac{1}{n}}$$

y lo llamaremos la RAIZ ENESIMA (o *de orden* n) ARITMETICA DE a.

Si b es una raíz de orden 2 de a, decimos que b es una *raíz cuadrada* de a.

Si b es una raíz de orden 3 de a, diremos que b es una *raíz cúbica* de a; etc.

Para demostrar la existencia y unicidad de esta raíz aritmética, necesitamos conocer previamente algunas propiedades que utilizaremos en su demostración. Estas propiedades son:

Proposición 1). Si a y b son números reales positivos tales que $a<b$; entonces $0 < a^n < b^n$, $\forall n \in \mathbb{N}$.

Demostración. Probaremos la propiedad por inducción sobre n. Si $n = 1$, la proposición se verifica trivialmente.

Supongamos ahora que la propiedad se verifica para n, es decir:

$$0 < a^n < b^n \qquad \text{(hipótesis de inducción)}$$

y probemos que se cumple para $n + 1$.

En efecto, sean a y b dos números reales positivos cualesquiera y tales que $a < b$.

Por la hipótesis de inducción se tiene:

$$0 < a^n < b^n$$

y como es $0 < a$, por multiplicación resulta:

$$0 < a^{n+1} < a \cdot b^n$$

Asimismo, de $a < b$, $0 < b^n$, por multiplicación resulta:

$$a \cdot b^n < b^{n+1}$$

Luego, por transitividad obtendremos:

$$0 < a^{n+1} < b^{n+1}$$

lo que demuestra la proposición.

Proposición 2). Si x, y, a, son números reales positivos tales que $x \cdot y < a$, entonces existen números reales positivos x', y' tales que:

$$x < x',\ y < y',\ x' \cdot y' < a$$

Demostración. Si por hipótesis es $x\,y < a$, entonces $a - x\,y > 0$. Por otro lado, de la hipótesis de que $x > 0$, $y > 0$, resulta entonces que $x + y + 1 > 0$.

Luego, siendo $a - xy > 0$, $x + y + 1 > 0$, entonces por la propiedad arquimediana, existe un número natural n tal que:

$$x + y + 1 < n\,(a - x\,y)$$

o bien,

$$\frac{1}{n}(x + y + 1) < a - x\,y$$

Pero, $\frac{1}{n}(x + y + 1) = \frac{1}{n}(x + y) + \frac{1}{n} > \frac{1}{n}(x + y) + \frac{1}{n^2}$

Por lo tanto, podremos escribir:

$$\frac{1}{n}(x + y) + \frac{1}{n^2} < \frac{1}{n}(x + y + 1) < a - x\,y \qquad (1)$$

Veremos en seguida que los números:

$$x' = x + \frac{1}{n}, \quad y' = y + \frac{1}{n}$$

satisfacen las condiciones de la proposición que estudiamos.

En efecto, ambos x', y' son positivos y mayores que x e y respectivamente. Además, por (1) resulta:

$$x' \cdot y' = (x + \frac{1}{n}) \cdot (y + \frac{1}{n}) = x\,y + \frac{1}{n}(x + y) + \frac{1}{n^2} < a$$

y la proposición está demostrada.

Proposición 3). Si x, y, a, son números reales positivos tales que $a < x \cdot y$, entonces existen números reales positivos x', y' tales que

$$x' < x,\ y' < y,\ a < x'\,y'$$

Demostración. Si por hipótesis es $a < x\,y$, entonces $x\,y - a > 0$. Asimismo, de la hipótesis de que $x > 0$, $y > 0$, resulta $x + y > 0$.

Luego, por la propiedad arquimediana, existe un número natural n tal que:

$$\cdot x + y < n\,(x\,y - a)$$

o bien,

$$\frac{1}{n}(x + y) < x\,y - a$$

Pero,

$$\frac{1}{n}(x + y) - \frac{1}{n^2} < \frac{1}{n}(x + y) < x\,y - a$$

Por lo tanto, podemos escribir:

$$x\,y - \frac{1}{n}(x + y) + \frac{1}{n^2} > a \qquad (1)$$

Por otra parte, tenemos en virtud de (1) que:

$$(x - \frac{1}{n})(y - \frac{1}{n}) = x\,y - \frac{1}{n}(x + y) + \frac{1}{n^2} > a$$

Por consiguiente, los números

$$x' = x - \frac{1}{n}, y' = y - \frac{1}{n}$$

satisfacen las condiciones de la producción, quedando por esto demostrada.

Proposición 4). Si x, a, son números reales positivos y n un número natural tales que $x^n < a$, entonces existe un número real positivo x' tal que:

$$x < x', \quad x'^n < a$$

Demostración. La demostraremos por inducción sobre n.

Para n = 1, la proposición se verifica trivialmente.

Supongámosla ahora verdadera para n; es decir:

$x, a \in \mathbb{R}^+$ tales que $x^n < a$, $n \in \mathbb{N} \Longrightarrow \exists\, x' \in \mathbb{R}^+$ tal que $x < x', x'^n < a$

y probésmosla para n + 1.

En efecto, sean x, a, dos números reales positivos tales que:

$$x^{n+1} < a$$

o sea, $$x^n \cdot x < a$$

Entonces, por la proposición 2), existen dos números reales positivos x_1, x_2 tales que:

$$x^n < x_1, \; x < x_2, \; x_1 x_2 < a$$

Si $x^n < x_1$, entonces por la hipótesis de inducción existe un número real positivo x_3 tal que:

$$x < x_3, \quad x_3^n < x_1$$

Sea x' = Min (x_2, x_3); entonces $x < x_2$ y $x < x_3 \Longrightarrow x < x'$, y además resulta que se verifica:

$$x'^{n+1} = x'^n \cdot x' \leq x_3^n \cdot x_2 < x_1 x_2 < a$$

y la proposición está demostrada.

Proposición 5). Si x, a, son números reales positivos y n un número natural tales que $a < x^n$, entonces existe un número real positivo x' tal que:

$$x' < x, \; a < x'^n$$

Demostración. De la misma manera que la proposición anterior, demostraremos ésta también por inducción sobre n.

Para n = 1, la proposición se verifica trivialmente. Supongámosla ahora verdadera para n; esto es:

$x, a \in \mathbb{R}^+$ tales que $a < x^n$, $n \in \mathbb{N} \Longrightarrow \exists\, x' \in \mathbb{R}^+$ tal que $x' < x, a < x'^n$

y probémosla que también n se verifica para n + 1.

En efecto, sean x, a, dos números reales positivos tales que,

$$a < x^{n+1}$$

o sea, $$a < x^n \cdot x$$

Entonces, por la Proposición 3), existen dos números reales positivos x_1, x_2 tales que:

$$x_1 < x^n, x_2 < x, a < x_1 x_2$$

Ahora bien, si $x_1 < x^n$ entonces por la hipótesis de inducción existe un número real positivo x_3 tal que:

$$x_3 < x, x_1 < x_3^n$$

Sea x' = Max (x_2, x_3); entonces $x_3 < x$ y $x_2 < x \Longrightarrow x' < x$ y además resulta que se verifica:

$$x'^{n+1} = x'^n \cdot x' \geq x_3^n \cdot x_2 > x_1 \cdot x_2 > a$$

y la proposición está demostrada.

Ahora, en posesión de estas cinco proposiciones básicas, estamos en condiciones de demostrar la afirmación hecha al comienzo de esta sección; esto es, el teorema fundamental siguiente:

Teorema: Dado un número real positivo a y un número natural n existe un único número real positivo x tal que:

$$x^n = a$$

Demostración. Probaremos primero la existencia de tal número real positivo x, y luego su unicidad.

a) *Existencia.* Sea a un número real positivo y n un número natural. Si n = 1, entonces el número x = a verifica las condiciones del teorema.

Si a = 1, entonces el número x = 1 verifica las condiciones del teorema.

Exceptuando estos dos casos triviales, supondremos entonces $a \neq 1$ y $n \neq 1$.

Denotemos por S el conjunto de todos los números reales positivos tales que $z^n < a$.

$$S = \{z \in \mathbb{R}^+ : z^n < a\}$$

S es un conjunto no vacío y está acotado superiormente. En efecto, si $a < 1$, entonces

$$a^{n-1} < 1$$

luego,

$$a^n < a$$

por lo tanto, $a \in S$ y 1 es una cota superior de S. Si $a > 1$, entonces

$$a > 1^n = 1$$

luego, $1 \in S$ y a es una cota superior de S. En consecuencia, si un número positivo no pertenece a S, es una cota superior de S, o si se prefiere, si un número positivo no es cota superior S, pertenece a S.

Por lo anterior vemos que S tiene supremo en $\mathbb{R}$. Sea $c = \text{Sup}(S)$. Es claro que $c > 0$, y probaremos que:

$$c^n = a$$

es decir, c es el número real positivo buscado. En efecto, por el contrario, supongamos que fuese

$$c^n \neq a$$

entonces, por la ley de tricotomía debe ser:

$$c^n < a, \text{ ó } a < c^n$$

Si fuera $c^n < a$, entonces, por la Proposición 4), existiría un número real positivo c' tal que:

$$c < c', \quad c'^n < a$$

es decir, $c' \in S$, lo que contradice la hipótesis de que c es el supremo de S, esto es, la cota superior mínima.

Esta contradicción muestra entonces que no puede ser $c^n < a$.

Veamos ahora el caso de que fuese $a < c^n$, entonces, por la Proposición 5), existiría un número real positivo c' tal que:

$$c' < c, \; a < c'^n$$

Esto implica que $z < c'$ para todo $z \in S$.

En efecto, si para algún $z \in S$ fuera:

$$z \geq c'$$

entonces, por Proposición 1), sería:

$$z^n \geq c'^n < a$$

lo que es imposible por la definición del conjunto S. Ahora bien, del hecho que $z < c'$ para todo $z \in S$, resulta entonces que c' es una cota superior de S y menor que su mínima cota superior c, esto contradice el hecho de que c es el supremo de S.

Esta contradicción muestra que tampoco puede ser $a < c^n$. Por lo tanto, debe necesariamente ser:

$$c^n = a$$

b) *Unicidad.* Probaremos ahora que la ecuación $x^n = a$ tiene una única solución real positiva.

Por el contrario, supongamos que x_1, x_2 son dos números reales positivos tales que:

$$x_1^n = a, \; x_2^n = a$$

luego,

$$x_1^n = x_2^n$$

Si fuera $x_1 < x_2$, por Proposición 1) sería $x_1^n < x_2^n$, lo que es imposible.

Si fuera $x_2 < x_1$, por la misma proposición sería $x_2^n < x_1^n$, lo que también es imposible.

Por lo tanto, como $x_1 < x_2$ y $x_2 < x_1$ conducen a una contradicción, debe necesariamente ser $x_1 = x_2$. Con este resultado b) y el anterior a) queda demostrado completamente el teorema.

Observaciones. 1) La propiedad que acabamos de probar, que se verifica siempre en $\mathbb{R}$ cualquiera que sea el número positivo a y cualquiera que sea $n \in \mathbb{N}$, no se verifica en el cuerpo $\mathbb{Q}$ de los números racionales, puesto que, como lo hemos demostrado anteriormente, la ecuación $x^2 = 2$ no tiene solución racional, ya que $\sqrt{2} \notin \mathbb{Q}$.

2) Ahora, ya que hemos mostrado la existencia de raíces en $\mathbb{R}$, en particular la existencia de raíces cuadradas, quedan completamente justificadas las demostraciones de los teoremas ya probados: "El conjunto $\mathbb{Q}$ de los números racionales forman un cuerpo ordenado que no es completo", y el de que en, "Cada intervalo abierto de $\mathbb{R}$ contiene por lo menos un número irracional".

11.9 *Radicación de números reales*

Definición. Dados un número real cualquiera a y un número na-

tural n, llamaremos RAIZ ENESIMA DE a, a toda solución de la ecuación $x^n = a$.

En virtud de esta definición y del teorema recién probado, sabemos que si $a > 0$ existe siempre una y una sola raíz enésima real positiva de a.

Sea b esta raíz; luego, ella verifica la relación:

$$b^n = a$$

Observemos que si el exponente n es par, entonces $(-b)$ también enésima de a, puesto que:

$$(-b)^n = (-b)^{2n} = [(-b)^2]^m = b^{2m} = b^n = a$$

En cambio, si n es impar la única raíz enésima de a es b, puesto que:

$$(-b)^n = (-b)^{2m+1} = (-b)^{2m} \cdot (-b) = b^{2m} \cdot (-b) = -b^{n+1} = -b^n \Longrightarrow b^n = -a$$

Por otro lado, si $a < 0$ y n es par, entonces no existe ningún número real que sea raíz enésima de a.

En efecto, supongamos que en la ecuación:

$$x^n = a$$

sea $a < 0$ y $n = 2m$.

Luego:

$$x^n = x^{2n} = a < 0$$

es decir,

$$(x^m)^2 = < 0$$

Como en un cuerpo ordenado cualquiera, en particular en $\mathbb{R}$, el cuadrado de cualquier elemento es positivo o nulo, resulta entonces que la relación:

$$(x^m)^2 = a < 0$$

no podrá ser verificada por ningún número real. En cambio, si $a < 0$ y n es impar, entonces a tiene una raíz enésima real que es negativa.

En efecto, observemos que si n es impar, se tiene:

$$(-x)^n = -x^n$$

porque, $(-x)^n = (-x)^{2m+1} = (-x)^{2m} \cdot (-x) = x^{2m} \cdot (-x) =$

$$= -(x^{2m} \cdot x) = -x^{2m+1} = -x^n$$

Luego,

$$x^n = -a \iff (-x)^n = a$$

si $a < 0$, $-a > 0$.

La primera de estas dos ecuaciones tiene una única solución real b, donde $b > 0$, por tanto, la segunda ecuación tiene una única solución real que es $(-b)$, es decir, *a* tiene una única raíz enésima real y esta es negativa.

De las consideraciones precedentes concluimos que el problema de la radicación de números reales que son soluciones de la ecuación:

$$x^n = a$$

presenta soluciones dispares según que a sea positivo o negativo y el exponente n sea par o impar.

Para evitar excepciones y ambigüedades adoptaremos la siguiente definición.

Definición. Dado un número real positivo a y un número natural n, el único número real positivo b tal que $b^n = a$, lo llamaremos la raíz enésima positiva de a, o la raíz aritmética de a de índice n, y la representaremos por el símbolo $\sqrt[n]{a}$.

Luego, por definición se tiene:

$$(\sqrt[n]{a})^n = a$$

Por lo tanto, la raíz aritmética está definida únicamente para los números reales positivos, y en tal caso es una operación en $\mathbb{R}$.

Teorema. La raíz aritmética tiene las propiedades siguientes:

a) $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$

b) $\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$

c) $\sqrt[m]{\sqrt[n]{a}} = \sqrt[mn]{a}$

d) $\sqrt[n]{a^m} = (\sqrt[n]{a})^m$

e) $\sqrt[mn]{a^{mp}} = \sqrt[n]{a^p}$

Demostración.

a) Para probar que:

$$\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$$

hay que, por la definición de raíz aritmética, demostrar que

$$(\sqrt[n]{a} \cdot \sqrt[n]{b})^n = a \cdot b$$

En efecto, por las reglas de las potencias naturales de números reales vistas en la sección 11.4. se tiene:

$$(\sqrt[n]{a}\cdot\sqrt[n]{b})^n = (\sqrt[n]{a})^n\cdot(\sqrt[n]{b})^n = a\cdot b$$

b) Podemos escribir:

$$a = \frac{a}{b}\cdot b$$

luego,

$$\sqrt[n]{a} = \sqrt[n]{\frac{a}{b}\cdot b} = \sqrt[n]{\frac{a}{b}}\cdot\sqrt[n]{b}$$

de donde,

$$\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$$

c) Para demostrar que:

$$\sqrt[m]{\sqrt[n]{a}} = \sqrt[mn]{a}$$

hay que probar que:

$$(\sqrt[m]{\sqrt[n]{a}})^{mn} = a$$

En efecto, se tiene:

$$(\sqrt[m]{\sqrt[n]{a}})^{mn} = [(\sqrt[m]{\sqrt[n]{a}})^m]^n = (\sqrt[n]{a})^n = a$$

d) Para demostrar que:

$$\sqrt[n]{a^m} = (\sqrt[n]{a})^m$$

hay que probar que:

$$[(\sqrt[n]{a})^m]^n = a^m$$

En efecto se tiene

$$[(\sqrt[n]{a})^m]^n = (\sqrt[n]{a})^{mn} = [(\sqrt[n]{a})^n]^m = a^m$$

e) Para demostrar que:

$$\sqrt[mn]{a^{mp}} = \sqrt[n]{a^p}$$

bastará demostrar que,

$$(\sqrt[n]{a^p})^{mn} = a^{mp}$$

En efecto, tendremos:

$$(\sqrt[n]{a^p})^{mn} = [(\sqrt[n]{a^p})^n]^m = (a^p)^m = a^{mp}$$

y el teorema está demostrado.

11.10. *Potencias de exponente racional.* En la sección 11.4. se definió las potencias de exponente entero y de base real. Ahora definiremos la operación de potenciación de base real positiva y de exponente racional cualquiera.

Definición. Dados un número real positivo a y dos números enteros p y q, $q > 0$, definimos la potencia $\frac{p}{a^q}$ como el número $\sqrt[q]{a^p}$.

Luego, por definición:

$$\underline{\frac{p}{a^q} = \sqrt[q]{a^p}}$$

Observemos que si $\frac{p}{q} = \frac{r}{s}$, $s > 0$, entonces $a^{\frac{p}{q}} = a^{\frac{r}{s}}$.

En efecto, aplicando la propiedad e) de la raíz aritmética, resulta:

$$a^{\frac{p}{q}} = \sqrt[q]{a^p} = \sqrt[qs]{a^{ps}} = \sqrt[qs]{a^{qr}} = \sqrt[s]{a^r} = a^{\frac{r}{s}}$$

En particular, se tiene:

$$\sqrt[n]{a} = a^{\frac{1}{n}}$$

La potenciación de exponente racional verifica las mismas propiedades que vimos para exponente entero.

En efecto, tenemos:

Teorema. Sean a y b números reales positivos y α, β números racionales cualesquiera. Entonces, se tiene:

a) $a^\alpha \cdot a^\beta = a^{\alpha+\beta}$

b) $(a^\alpha)^\beta = a^{\alpha\beta}$

c) $(a\cdot b)^\alpha = a^\alpha\cdot b^\alpha$

Demostración. Utilizando las propiedades de la raíz aritmética y la definición de potencia de exponente racional, podremos escribir

a) $a^{\alpha} \cdot a^{\beta} = a^{\frac{p}{q}} \cdot a^{\frac{r}{s}} = \sqrt[q]{a^p} \cdot \sqrt[s]{a^r} = \sqrt[qs]{a^{ps}} \cdot \sqrt[qs]{a^{qr}}$

$= \sqrt[qs]{a^{ps} \cdot a^{qr}} = \sqrt[qs]{a^{ps+qr}} = a^{\frac{ps+qr}{qs}}$

$= a^{\frac{p}{q} + \frac{r}{s}} = a^{\alpha + \beta}$

b) $(a^{\alpha})^{\beta} = (a^{\frac{p}{q}})^{\frac{r}{s}} = (\sqrt[q]{a^p})^r = (\sqrt[s]{\sqrt[q]{a^p}})^r$

$= \left(\sqrt[sq]{a^p}\right)^r = \sqrt[sq]{a^{pr}} = a^{\frac{pr}{sq}}$

$= a^{\frac{p}{q} \cdot \frac{r}{s}} = a^{\alpha\beta}$

c) $(a \cdot b)^{\alpha} = (a \cdot b)^{\frac{p}{q}} = \sqrt[q]{(a \cdot b)^p} = \sqrt[q]{a^p \cdot b^p}$

$= a^p \cdot \sqrt[q]{b^p} = a^{\frac{p}{q}} \cdot b^{\frac{p}{q}} = a^{\alpha} \cdot b^{\alpha}$

y el teorema está demostrado.

EJERCICIOS

1) Calcular:

a) $(11\frac{1}{5})^5 : (1\frac{3}{5})^5$

b) Si $38^7 = 114415582592$, ¿cuánto vale 19^7?

c) ¿Cuánto vale 5^{12}, si $5^6 = 15625$?

d) $1 : 0{,}2^{-6}$

e) $(-5)^2 + (-7)^5 - (-2)^7 + (-1)^{-1} + (-2)^{-2} - (0{,}3)^{-3} + (-4)^0$

f) $2\sqrt{0{,}5\sqrt{0{,}5\sqrt{0{,}5\sqrt{0{,}5}}}}$

2) $\sqrt[3]{\frac{27}{64}} + \sqrt[3]{\frac{64}{125}} - 4\sqrt[3]{3\frac{3}{8}} - 2\sqrt[3]{2\frac{10}{27}} + 3\sqrt[3]{1\frac{61}{64}}$

3) $16^{\frac{1}{2}} + 8^{\frac{2}{3}} + 16^{\frac{3}{4}} + 125^{\frac{1}{3}} - -512^{\frac{2}{3}} + 100^{0{,}5} + 81^{0{,}75}$

4) $\sqrt[\frac{1}{2}]{7} - \sqrt[\frac{2}{3}]{6\frac{1}{4}} + \sqrt[0{,}3]{8} - \sqrt[0{,}75]{27} + \sqrt[\frac{3}{4}]{64}$

5) Se sabe que $9^{-\frac{7}{6}} = 0{,}0770401$, ¿cuánto vale $9^{-\frac{2}{3}}$?

6) ¿Cuánto vale $10^{0{,}90309}$, si $10^{0{,}30103} = 2$?

7) Efectuar las operaciones siguientes:

a) $\sqrt[3]{8^5} \cdot \sqrt[5]{8^7}$

b) $\sqrt[4]{11^7} \cdot \sqrt[9]{11^4}$

c) $\sqrt[8]{5^7} : \sqrt[6]{5^5}$

Capítulo XII

EL NUMERO COMPLEJO

12.0. La introducción de los números reales nos permitió dar sentido a la operación $\sqrt[n]{a}$ para $a>0$, pero no a la operación $\sqrt[2n]{a}$ cuando $a<0$; es decir, no es posible resolver en el campo de los números reales el problema de la extracción de raíces de índice par de los números reales negativos.

Así, pues, no hay número real positivo o negativo que pueda ser considerado como igual a $\sqrt{-9}$.

Esto indica la necesidad de ampliar aún más el concepto de número, introduciendo entes que den sentido a esta operación; estos nuevos entes que se crean los llamaremos NUMEROS IMAGINARIOS.

Para esto introduciremos un nuevo símbolo numérico, que indicaremos por i, definido por la condición:

$$i^2 = -1$$

El símbolo i será llamado *unidad imaginaria*, en contraposición al símbolo 1 que es la *unidad real*.

El número imaginario $\sqrt{-9}$ puede descomponerse en la forma siguiente:

$$\sqrt{-9} = \sqrt{9\cdot(-1)} = \sqrt{9}\cdot\sqrt{-1} = 3\sqrt{-1}$$

En general, todo número imaginario puede descomponerse en un producto de un número real por la raíz cuadrada de menos uno.

En efecto, se puede escribir:

$$\sqrt{-a} = \sqrt{a(-1)} = \sqrt{a}\cdot\sqrt{-1}$$

Como por definición se tiene:

$$i^2 = -1$$

resulta $$i = \sqrt{-1}$$

entonces, $$\sqrt{-a} = i\sqrt{a}$$

Luego, todo número imaginario es de la forma:

$$\boxed{bi}$$

en donde b representa un número real.

En consecuencia, podremos escribir:

$$\sqrt{-9} = 3i$$

$$\sqrt{-2} = i\sqrt{2}$$

$$-\sqrt{-2} = -i\sqrt{2}, \text{ etc.}$$

Las potencias de la unidad imaginaria son iguales a la unidad real si son pares, o iguales a la unidad imaginaria si son impares.

$$i^{4k+1} = (i^4)^k \cdot i = i$$

$$i^{4k+2} = (i^4)^k i^2 = -1$$

$$i^{4k+3} = (i^4)^k i^3 = -i$$

$$i^{4k+4} = (i^4)^k i^4 = 1$$

Las cuatro primeras potencias de i son:

$$\boxed{\begin{array}{l} i^1 = i \\ i^2 = -1 \\ i^3 = -i \\ i^4 = +1 \end{array}}$$

y a partir de la quinta potencia estos valores se repiten en el mismo orden. Luego, en general:

$$i^n = i^{4k+x} = i^x, \; x < 4$$

Las potencias de un número imaginario son reales o imaginarias, según que el exponente sea par o impar.

$$(bi)^{2n} = b^{2n} \cdot i^{2n} = b^{2n} \cdot (\pm 1) = \pm b^{2n}$$

$$(bi)^{2n+1} = b^{2n+1} \cdot i^{2n+1} = b^{2n+1} i^{2n} \cdot i$$

$$= \pm b^{2n+1} \cdot i$$

La raíz de un entero imaginario es siempre imaginaria.

En efecto:

$$\sqrt[n]{bi} = \sqrt[n]{b} \cdot \sqrt[n]{i} = \sqrt[n]{b} \cdot \sqrt[n]{-1} = \sqrt[n]{b}\,\sqrt[2n]{-1}$$

12.1 *El número complejo.* Puede observarse que no es nada fácil imaginar ¿qué es i?, desde el punto de vista intuitivo. Pero desde mediados del siglo XIX, los matemáticos tomaron plena conciencia de que la base esencial del concepto de número esté en las operaciones y sus propiedades, y de que toda ampliación del campo numérico se obtiene *definiendo* nuevos números. Toda definición es *libre*, pero resulta de poco valor si no se la *elige* de manera adecuada.

En todas las sucesivas ampliaciones del campo numérico que hemos venido haciendo, hemos ido agregando, paso a paso, un eslabón hasta obtener la cadena de inclusiones siguiente:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Pero en todas estas generalizaciones hemos tenido en cuenta el llamado "Principio de la permanencia de las leyes formales de las operaciones", y el cual se resume en las dos condiciones siguientes:

a) Han de satisfacer los nuevos números a las leyes formales fundamentales de las operaciones, a saber: propiedad uniforme, conmutativa, asociativa y distributiva.

b) Que las nuevas definiciones que se den de las operaciones han de comprender a las antiguas como casos particulares.
En nuestro caso presente, deberemos definir los números complejos y las operaciones con ellos de modo que subsistan las propiedades algebraicas del sistema de los números reales $\mathbb{R}$.
Según esto, para construir el conjunto $\mathbb{C}$ de los números complejos, comenzaremos con el conjunto producto $\mathbb{R} \times \mathbb{R}$ y la relación de equivalencia sobre este conjunto se define así:

$$\boxed{(a, b) = (c, d) \text{ si, y sólo si, } a = c \text{ y } b = d}$$

Que esta relación es de equivalencia, es inmediato.

Como ahora cada una de las clases de equivalencia resultantes no contiene más que un solo elemento, denotaremos esta clase por (a, b) en vez de $\overline{(a, b)}$ y denotaremos en lo sucesivo $\mathbb{R} \times \mathbb{R}$ por $\mathbb{C}$.

Definición. Llamaremos NUMERO COMPLEJO a todo par ordenado de números reales y que satisfacen a ciertas condiciones. Así:

$$z = (a, b)$$

podría representar un número complejo.

El número a se denominará la *parte real* y el número b la *parte imaginaria.*

Para comprender, en esta definición, a los números reales e imaginarios, convendremos en que el número real a se escriba en la forma:

$$a = (a, 0)$$

y el número imaginario bi se escriba en la forma:

$$bi = (0, b)$$

Según estas convenciones, el cero se escribirá:

$$0 = (0,0)$$

la unidad real 1 se escribirá:

$$1 = (1, 0)$$

y la unidad imaginaria i se escribirá:

$$i = (0, 1)$$

Las condiciones de que se habla en la definición anterior son las siguientes:

a) *Condición de igualdad.* Dos números complejos son iguales si, y sólo si, son iguales sus partes reales e imaginarias separadamente; esto es:

$$(a, b) = (c, d) \text{ si, y sólo si, } a = c \text{ y } b = d$$

Como consecuencia de esto tenemos que un número complejo será nulo si es nula su parte real y nula también su parte imaginaria.

b) *Definición de adición.* La suma de dos números complejos se define mediante la expresión siguiente:

$$(a, b) + (c, d) = (a + c, b + d)$$

c) *Definición de multiplicación.* El producto de dos números complejos se define mediante la expresión siguiente:

$$(a, b) \cdot (c, d) = (a\,c - b\,d, a\,d + b\,c)$$

Como consecuencia de esto tenemos que el producto de un número complejo por un número real se define por la regla siguiente:

$$(a, b) \cdot m = (a, b) \cdot (m, 0) = (a\,m, b\,m)$$

También tenemos que:

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$$

lo que nos dice que el cuadrado de la unidad imaginaria es igual a menos uno. De donde resulta que se considere:

$$i = \sqrt{-1}$$

De las consideraciones anteriores, resulta que el número complejo (a, b) también suele representarse por la notación siguiente:

$(a, b) = (a, 0) + (0, b)$, por la definición de adición

$(a, b) = (a, 0) + (0, 1) \cdot b$, por la definición de producto de un factor

$(a, b) = a + bi$, por ser $(0, 1) = i$

que es la *forma aritmética* del número complejo.

Escribiendo las definiciones de suma y producto en esta nueva forma tendremos:

$$(a + bi) + (c + di) = (a + c) + (b + d)\,i$$

$$(a + bi) \cdot (c + di) = (a\,c - b\,d) + (a\,d + b\,c)\,i$$

12.2 *Propiedades de las operaciones de adición y de multiplicación*

a) *Adición:* $(a, b) + (c, d) = (a + c, b + d)$

Definida así la adición, vamos a ver que ella cumple con el principio de permanencia de las leyes formales: es decir, tiene las propiedades uniformes, conmutativa y asociativa.

La propiedad uniforme es inmediata a causa de la validez de una misma propiedad en $\mathbb{R}$.

Es conmutativa, es decir:

$$(a, b) + (c, d) = (c, d) + (a, b)$$

En efecto:

$$(a, b) + (c, d) = (a + c, b + d)$$

y

$$(c, d) + (a, b) = (c + a, d + b)$$

pero entre números reales se verifica:

$$a + c = c + a$$

$$b + d = d + b$$

luego,

$$(a + c, b + d) = (c + a, d + b)$$

o sea,

$$(a, b) + (c, d) = (c, d) + (a, b)$$

Es asociativa, es decir:

$$[(a, b) + (c, d)] + (e, f) = (a, b) + [(c, d) + (e, f)]$$

En efecto, se tiene:

$$[(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f)$$

$$= [(a + c) + e, (b + d) + f$$

$$y\ (a, b) + [(c, d) + (e, f)] = (a, b) + (c + e, d + f)$$

$$= [a + (c + e), b + (d + f)]$$

pero entre números reales se verifica:

$$(a + c) + e = a + (c + e)$$

$$(b + d) + f = b + (d + f)$$

luego, concluimos que:

$$[(a, b) + (c, d)] + (e, f) = (a, b) + [(c, d) + (e, f)]$$

En particular, el par (0,0) desempeña el papel del cero, y diremos por esto que es el elemento neutro para la adición en el conjunto $\mathbb{C}$ de los números complejos.

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$$

En particular, el elemento $(-a, -b)$ es el opuesto o el aditivo inverso del elemento (a, b), puesto que:

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

Este resultado conjuntamente con los anteriores muestran que la adición definida en $\mathbb{C}$ hace de $\mathbb{C}$ un grupo aditivo.

b) *Multiplicación.* $(a, b) \cdot (c, d) = (a\,c - b\,d, b\,c + a\,d)$

Definida así la multiplicación, probaremos que ella cumple con el principio de permanencia de las leyes formales de las operaciones; es decir, tiene las propiedades uniforme, conmutativa, asociativa y distributiva respecto a la adición.

La propiedad uniforme es inmediata a causa de la validez en $\mathbb{R}$ de las propiedades uniforme de la multiplicación, adición y sustracción.

Es conmutativa, es decir:

$$(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$$

En efecto, se tiene:

$$(a, b) \cdot (c, d) = (a\,c - b\,d, b\,c + a\,d)$$

$$(c, d) \cdot (a, b) = (c\,a - d\,b, d\,a + c\,b)$$

pero entre números reales se verifica:

$$a\,c - b\,d = c\,a - d\,b$$

$$b\,c + a\,d = d\,a + c\,b$$

luego,

$$(a\,c - bd, bc + a\,d) = (c\,a - db, da + c\,b)$$

o sea,

$$(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$$

Es asociativa, es decir:

$$[(a, b) \cdot (c, d)] \cdot (e, f) = (a, b) \cdot [(c, d) \cdot (e, f)]$$

y cuya demostración es sencilla.

Es distributiva, es decir:

$$[(a, b) + (c, d)] \cdot (e, f) = (a, b) \cdot (e, f) + (c, d) \cdot (e, f)$$

también es de fácil demostración.

En resumen, de todo lo anterior resulta que el conjunto $\mathbb{C}$ de los números complejos, algebrizado con las operaciones de adición y multiplicación, anteriormente definidas, es un anillo conmutativo. Además, este anillo es con unidad y que es el par (1, 0) que cumple la propiedad siguiente:

$$(a, b) \cdot (1, 0) = (a - 0, b + 0) = (a, b)$$

Veremos a continuación que este anillo conmutativo con unidad es también un dominio de integridad.

En efecto, bastará probar que si se tiene:

$$(a, b) \cdot (c, d) = (0, 0)$$

entonces al menos uno de los factores (a, b) ó (c, d) es cero. Tenemos:

$$(a, b) \cdot (c, d) = (0, 0)$$

o bien,

$$(a\,c - b\,d, b\,e + a\,d) = (0, 0)$$

y de donde resulta que:

$$\begin{cases} a\,c - b\,d = 0 \\ b\,c + a\,d = 0 \end{cases}$$

Elevando al cuadrado y sumando en seguida miembro a miembro estas igualdades, se obtiene:

$$a^2c^2 + b^2d^2 - abcd + b^2c^2 + a^2d^2 + abcd = 0$$

$$a^2(c^2 + d^2) + b^2(c^2 + d^2) = 0$$

$$(a^2 + b^2) \cdot (c^2 + d^2) = 0$$

Pero como $\mathbb{R}$ es un dominio de integridad, la última igualdad implica:

$$a^2 + b^2 = 0, \text{ó}, c^2 + d^2 = 0$$

o sea,

$$a = b = 0, \text{ó}, c = d = 0$$

y de donde resulta que:

$$(a, b) = 0, \text{ ó, } (c, d) = 0$$

y lo que prueba que $\mathbb{C}$ es un dominio de integridad. Por último, probaremos que todo elemento distinto de cero admite un inverso para la ley multiplicativa.

En efecto, sea (a, b) un elemento no nulo de $\mathbb{C}$, y busquemos un elemento (x, y) tal que:

$$(a, b) \cdot (x, y) = (1, 0)$$

o sea,

$$(ax - by, bx + ay) = (1, 0)$$

Luego, resulta que:

$$\boxed{\begin{aligned} ax - by &= 1 \\ bx + ay &= 0 \end{aligned}}$$

Este sistema de ecuaciones en x e y admite una solución única y que es:

$$x = \frac{a}{a^2 + b^2}$$

$$y = \frac{-b}{a^2 + b^2}$$

salvo que $a^2 + b^2 = 0$, es decir $a = b = 0$ en $\mathbb{R}$.

Luego, el inverso multiplicativo del elemento (a, b) es el elemento:

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b_2}\right)$$

En conclusión, el conjunto $\mathbb{C}$ de los números complejos es un cuerpo conmutativo. Por lo tanto, pueden realizarse en él, sin excepción, las cuatro operaciones racionales: adición, sustracción, multiplicación y división.

12.3. *Isomorfismo de* $\mathbb{R}$ *sobre una parte de* $\mathbb{C}$. Consideremos la aplicación.

$$f : \mathbb{R} \longrightarrow \mathbb{C}$$

definida por,

$$f(a) = (a, 0)$$

y que es inyectiva, puesto que:

$$f(a) = f(b)$$

o sea,

$$(a, 0) = (b, 0) \Longrightarrow a = b$$

Probemos que esta aplicación preserva las operaciones de adición y multiplicación de ambos conjuntos $\mathbb{R}$ y $\mathbb{C}$. En efecto, se tiene:

$$f(a + b) = (a + b, 0) = (a, 0) + (b, 0) = f(a) + f(b)$$

$$f(a \cdot b) = (a \cdot b, 0) = (a, 0) \cdot (b, 0) = f(a) \cdot f(b)$$

luego, f es un monomorfismo de $\mathbb{R}$ dentro de $\mathbb{C}$; es decir, $\mathbb{R}$ es isomorfo al subconjunto propio de $\mathbb{C}$ cuyos elementos son de la forma (a, 0).

En base a este isomorfismo, convendremos en identificar cada elemento $a \in \mathbb{R}$ con su imagen $(a, 0) \in \mathbb{C}$, pudiendo escribir:

$$a = (a, 0)$$

$$\mathbb{R} \subset \mathbb{C}$$

es decir, $\mathbb{R}$ aparece como si fuese un subconjunto propio de $\mathbb{C}$. Por lo tanto, nuestra serie de ampliaciones del campo numérico permite agregar otro eslabón a la cadena de inclusiones:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

12.4. *Complejos Conjugados.* Consideremos la aplicación de $\mathbb{C}$ en sí mismo tal que al número $z = a + bi$ hace corresponder el número $\bar{z} = a - bi$. El número $\bar{z}$ lo llamaremos el *complejo conjugado* de z.

La aplicacion $f : \mathbb{C} \longrightarrow \mathbb{C}$

tal que, $z \longrightarrow \bar{z}$

es evidentemente biyectiva.

Los números reales son los únicos elementos invariantes en esta aplicación.

Es fácil verificar que la suma y el producto de dos números complejos conjugados son reales.

$$z + \bar{z} = 2a; \qquad z \cdot \bar{z} = a^2 + b^2$$

Teorema La aplicacion $z \longrightarrow \bar{z}$ es un automorfismo de $\mathbb{C}$.

Demostracion. Siendo la aplicación $z \longrightarrow \bar{z}$ una biyección de $\mathbb{C}$ sobre $\mathbb{C}$, bastará mostrar que ella preserva la suma y el producto. En efecto, tenemos:

$$z = a + bi, \qquad z' = a' + b'i$$

$$z + z' = (a + a') + (b + b')i$$

$$z \cdot z' = (a\,a' - b\,b') + (a\,b' + a'b)\,i$$

entonces resulta:

$$\overline{z + z'} = (a + a') - (b + b')i = (a - bi) + (a' - b'i) = \bar{z} + \bar{z}'$$

$$\overline{z \cdot z'} = (a\,a' - b\,b') - (a\,b' + a'b)\,i$$

$$= a\,a' + b\,b'i^2 - a\,b'i - a'bi$$

$$= a\,(a' - b'i) - bi\,(a' - b'i)$$

$$= (a - bi)\,(a' - b'i)$$

$$= \bar{z} \cdot \bar{z}'$$

lo que prueba el automorfismo.

Nota. Veremos un poco más adelante que el concepto de complejo conjugado puede utilizarse en la operación de dividir dos números complejos.

En primer lugar, dividir el complejo $a + bi$ por el complejo $c + di$ equivale a encontrar el complejo $x + yi$, donde x e y son cantidades por determinar, tal que:

$$a + bi = (c + di)\,(x + yi)$$

o sea, $$a + bi = (c\,x - d\,y) + (d\,x + c\,y)\,i$$

Igualando las partes reales y las partes imaginarias, tendremos:

$$\begin{aligned} c\,x - d\,y &= a \\ d\,x + c\,y &= b \end{aligned}$$

las cuales nos dan al resolverlas:

$$x = \frac{a\,c + b\,d}{c^2 + d^2}, \quad y = \frac{b\,c - a\,d}{c^2 + d^2}$$

como la solución única y determinada para el cociente; esto es

$$\frac{a + bi}{c + di} = \frac{a + bi}{c + di} + \frac{a\,c + b\,d}{c^2 + d^2}\,i$$

En segundo lugar, a este mismo resultado se hubiese llegado si multiplicamos numerador y denominador por el conjugado del denominador, prácticamente esto es lo que se hace. En efecto:

$$\frac{a + bi}{c + di} = \frac{(a + bi)\,(c - di)}{(c + di)\,(c - di)} = \frac{(ac + bd) + (bc - ad)\,i}{c^2 + d^2}$$

$$= \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\,i$$

que es lo mismo de antes.

En particular, se encuentra el inverso:

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)\,(a - bi)} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\,i$$

12.5. *¿Orden en* $\mathbb{C}$*?* Hemos visto que el sistema de los números reales $\mathbb{R}$ y el sistema de los números complejos $\mathbb{C}$ son cuerpos conmutativos. El sistema $\mathbb{R}$ es un cuerpo ordenado; esto nos lleva a pensar: ¿Es ordenable el cuerpo de los números complejos? Esto es equivalente a preguntar si es posible definir una relación de orden "$<$" en $\mathbb{C}$, en forma tal que el conjunto $P = \{z \in \mathbb{C} : 0 < z\}$ satisfaga los axiomas siguientes:

Axioma 1) $(0, 0) \notin P$

Axioma 2) Si $z \in P$, entonces una y una sola de las proposiciones siguientes:

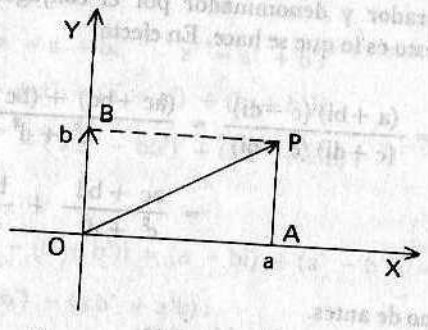
$$z \in P; \quad -z \in P, z = (0, 0)$$

es verdadera.

12.6. *Representación geométrica de los números complejos.* Aunque toda la teoría de los números complejos puede ser desarrollada aritméticamente sin utilizar representación geométrica ninguna, es, sin embargo, útil mostrar que la creación de estos nuevos números ha sido en parte motivada por la necesidad de poder representar numéricamente los puntos de un plano, de igual modo que los números reales surgieron en la mente de los matemáticos para poder representar todos los puntos de una recta.

En efecto, hemos dicho que a cada par ordenado de números reales corresponde un solo número complejo y, recíprocamente, a cada número complejo se puede hacer corresponder un determinado par ordenado de números reales.

Esta correspondencia biunívoca y la notación misma (a, b) de los números complejos, sugiere la posibilidad de representarlos por puntos de un plano.



Así, el complejo (a, b) puede representarse en el plano de los ejes ortogonales XY, por el punto P (a, b), o más precisamente por el vector OP cuyos componentes OA y OB tienen como medidas los dos números a y b.

Deducimos entonces que los puntos representativos de los complejos de la forma (a, O) que hemos llamado reales, se encuentran todos sobre el eje de las abscisas, llamado por esto *eje real.* Así también los imaginarios puros (0, b) se representan todos por puntos sobre el eje de las ordenadas, que ahora pasa a tomar el nombre de *eje imaginario.* El plano (XY) recibe ahora el nombre de *plano complejo,* o *plano de Argand-Gauss.*

En consecuencia, queda así determinado numéricamente cada punto P del plano por el número complejo (a, b) que componen sus dos coordenadas. Recíprocamente, todo número complejo (a, b) determina un punto P del plano, que llamaremos *afijo* del número complejo. Si el segundo componente b es nulo, es decir, si el número (a, 0) es real, obtenemos un punto sobre el eje de las x, y si el primer componente a es nulo,

Ax. 3) Si $z, z' \in P$, entonces $z + z' \in P$ y $z \cdot z \in P$.

La respuesta a esta interrogante está dada en el siguiente:

Teorema. El sistema de los números complejos $\mathbb{C}$ no es un cuerpo ordenado.

Demostración. Haremos una prueba indirecta; esto es, suponemos por el contrario que $\mathbb{C}$ es un cuerpo ordenado; por tanto, existe un subconjunto propio P de $\mathbb{C}$ con las propiedades dadas por los axiomas 1), 2) y 3) descritos anteriormente.

Vamos a demostrar que bajo esta suposición se tiene:

$$z \in \mathbb{C} \text{ y } z \neq (0,0) \Longrightarrow z \cdot z \in P$$

En efecto, vamos a considerar dos casos: $z \in P$ y $z \notin P$. Si $z \in P$, entonces por Ax. 3) resulta $z \cdot z \in P$.

Si $z \notin P$ y $z \neq (0, 0)$, entonces por el axioma 2) resulta $-z \in P$; luego, por Ax. 3) y por la propiedad de cuerpo que:

$$(-z)(-z) = z \cdot z \in P$$

Por consiguiente, en todos los casos resulta que:

$$z \in \mathbb{C} \text{ y } z \neq (0,0) \Longrightarrow z \cdot z \in P$$

Ahora bien, como $(1, 0) \in \mathbb{C}$ y $(0, 1) \in \mathbb{C}$, además $(1, 0) \neq (0, 0)$ y $(0, 1) \neq (0, 0)$, entonces por lo recién probado tenemos:

$$(1,0) \cdot (1,0) = (1,0) \in P$$

$$(0,1) \cdot (0,1) = (-1,0) = -(1,0) \in P$$

Todo esto es posible, pero por el Ax. 2), los números $(1, 0)$, $-(1, 0)$ no pueden ser ambos elementos de P.

Por consiguiente, la suposición de que $\mathbb{C}$ es un cuerpo ordenado, conduce a una contradicción y esta contradicción prueba el teorema.

Así, pues, como el cuerpo de los números complejos no es un cuerpo ordenado, entonces no podremos hablar de que un número complejo sea menor o mayor que otro número complejo, y ni que uno de ellos es positivo o negativo. Por lo tanto, los números complejos no pueden ser usados en desigualdades.

Sin embargo, bajo ciertas condiciones arbitrarias puede darse sobre $\mathbb{C}$ el siguiente criterio de orden:

$$(a, b) \leq (c, d) \text{ si es } a < c, \text{ y si al ser } a = c \text{ es } b \leq d$$

Puede demostrarse que esta relación es de orden total, pero no verifica el axioma de Arquimedes.

es decir, si el número (0, b) es imaginario, obtendremos entonces como representante un punto sobre el eje de las y.

Esta representación geométrica fue adoptada por Gauss (1777-1855) y también por Argand (1768-1822) a comienzos del siglo XIX. Es, desde luego, innecesaria para desarrollar aritméticamente la teoría del número complejo y de las operaciones en C; pero ejerció influencia positiva en tiempos en que los números complejos se consideraban como números ficticios o irreales (de allí el nombre de "imaginarios").

La geometría de la antigua Grecia es, sin duda alguna, una de las más valiosas joyas del pensamiento humano de todos los tiempos. Esta, llamada también geometría euclideana, en honor de quien tan maravillosamente organizó sus postulados, y deducciones lógicas, alcanzó a constituir una estructura tan perfecta que fue necesario el transcurso de muchos siglos para que una nueva idea lograra abrirle nuevos horizontes. Esta idea fue de René Descartes en el siglo XVII, quien, al unir la geometría con el álgebra mediante los ahora llamados sistemas cartesianos de coordenadas, dio el paso inicial de un asombroso resurgimiento de las matemáticas.

Precisamente, con el objeto de despojar a los números complejos del aspecto "irreal" o "misterioso", Gauss adoptó la idea de la representación geométrica cartesiana de los números complejos, representación que permite efectuar las operaciones fundamentales mediante sencillas construcciones geométricas, que lentamente se fueron abriendo paso en las matemáticas a través de la historia y contribuyendo a disipar la desconfianza y clarificar las ideas, preludiando el advenimiento de una teoría científica rigurosa.

12.7. *Números complejos de varias unidades y Teorema final de la Aritmética.* Desde el punto de vista aritmético, no es necesario una nueva aplicación del campo de los números, pues, en el sistema de los números complejos quedan resueltos todos los problemas aritméticos elementales, como son: adición, sustracción, multiplicación, división, potenciación, radicación, potencias de base e y logaritmos neperianos, y también sucesiones y series de términos complejos.

En cambio, no sucede lo mismo desde el punto de vista geométrico. Pues, aunque hemos logrado representar aritméticamente los puntos del plano e introducir un cálculo geométrico satisfactorio en la Geometría Plana, no sucede lo mismo en la Geometría del Espacio Ordinario ni mucho menos en la Geometría del Espacio de n dimensiones.

Por este motivo, parece natural intentar una nueva ampliación del sistema de los números complejos, introduciendo los HIPERCOMPLEJOS

O COMPLEJOS DE ORDEN SUPERIOR, definimos como conjuntos de n números reales dados en un cierto orden:

$$\alpha = (a_1, a_2, a_3, \ldots, a_n) = a_1 i_1 + a_2 i_2 + a_3 i_3 + \ldots + a_n i_n$$

donde los a_j son números reales y los i_j son unidades sobre las cuales se pueden hacer diversos convenios respecto a la multiplicación.

En particular, son interesantes por sus múltiples aplicaciones los vectores bidimensionales y tridimensionales, como también los *cuaterniones* de Hamilton, definidos de la manera siguiente:

$$\alpha = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3$$

donde a_0, a_1, a_2, a_3, son números reales, e i_1, i_2, i_3 son unidades imaginarias sujetas a las siguientes convenciones:

$$i_1^2 = i_2^2 = i_3^2 = -1$$

$$i_1 i_2 = -i_2 i_1 = i_3$$

$$i_2 i_3 = -i_3 i_2 = i_1$$

$$i_3 i_1 = -i_1 i_3 = i_2$$

Con estas convenciones se puede definir las operaciones. Cuando el cuaternión se reduce a su parte real, es decir, cuando sus componentes son $(a_0, 0, 0, 0)$ se llama *escalar*. En cambio, si los componentes son $(0, a_1, a_2, a_3)$, el cuaternión se llama simplemente *vector*.

Un cuaternión es, por tanto, la suma de un número real (su parte escalar) y un vector (su parte imaginaria).

Cabe inmediatamente la pregunta de si los vectores, cuaterniones u otros hipercomplejos (distintos de los complejos ordinarios) satisfarán a todas las leyes formales del cálculo aritmético; uniforme, asociativa, conmutativa, distributiva y el producto de factores no nulos es distinto de cero.

La contestación es negativa. La respuesta a esta pregunta constituye el llamado teorema final de la aritmética y suele enunciarse de la manera siguiente:

Teorema Final de la Aritmética.

No existe ningún sistema de números complejos de más de dos unidades (la real 1 y la imaginaria i) que satisfaga a todas las leyes formales de la Aritmética, y para el cual el producto de dos factores no nulos, no sea nulo.

Así, los cuaterniones no satisfacen la propiedad conmutativa de la multiplicación.

Por consiguiente, podemos, pues, decir que la ARITMETICA construida siguiendo el "Principio de Permanencia de las leyes Formales", termina con el estudio de los números complejos ordinarios o a dos unidades: la real (1, 0) y la imaginaria (0, 1).

Ya no es posible continuar la serie de ampliaciones $\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R} \longrightarrow \mathbb{C}$ del concepto de número. Con el teorema anterior llega a su término natural el desarrollo de la ARITMETICA.

EJEMPLOS Y EJERCICIOS

1) Dar forma compleja a las expresiones siguientes:

a) $\dfrac{1}{5 - i\sqrt{3}}$

Solución.

$$\frac{1}{5 - i\sqrt{3}} = \frac{5 + i\sqrt{3}}{(5 - i\sqrt{3})(5 + i\sqrt{3})} = \frac{5 + i\sqrt{3}}{25 + 3} = \frac{5}{28} + \frac{\sqrt{3}}{28}\,i$$

b) $\dfrac{\sqrt{3} - i\sqrt{5}}{2\sqrt{3} - i\sqrt{5}}$

c) $\dfrac{(1 + i)^3}{(1 - i)^2}$

d) $\dfrac{(3 + i)^2 - (3 - i)^2}{(3 + i)^2 + (3 - i)^2}$

2) *Definición.* Llamaremos Módulo o Valor Absoluto del número complejo $z = a + bi$, a la raíz cuadrada aritmética del número real y positivo $a^2 + b^2$.

Denotando el módulo de z por $|z|$, se tiene entonces por definición:

$$|z| = |a + bi| = +\sqrt{a^2 + b^2}$$

El módulo es cero si, y sólo si, $a = 0$ y $b = 0$; es decir:

$$|a + bi| = 0 \Longleftrightarrow (a = 0 \text{ y } b = 0)$$

Para un número real (a, 0) el módulo coincide con el valor absoluto; es decir:

$$|(a, 0)| = \sqrt{a^2 + 0^2} = \sqrt{a^2} = |a|$$

Con esta definición de módulo, dar forma compleja a las expresiones siguientes:

a) $\sqrt{6 + i\sqrt{13}}$

Solución: Pongamos:

$$\sqrt{6 + i\sqrt{13}} = x + yi$$

donde x e y son dos números reales por determinar. Elevando al cuadrado esta igualdad, se tiene:

$$6 + i\sqrt{13} = (x^2 - y^2) + 2xyi$$

de donde resulta

$$\begin{array}{|ll} x^2 - y^2 & = 6 \\ 2xy & = \sqrt{13} \end{array}$$

Elevando estas dos ecuaciones al cuadrado y sumándolas en seguida miembro a miembro, se obtiene:

o sea, $$(x^2 + y^2)^2 = 49$$

luego, $$x^2 + y^2 = 7$$

Por lo tanto, podemos escribir el sistema:

$$\begin{array}{|ll} x^2 + y^2 & = 7 \\ x^2 - y^2 & = 6 \end{array}$$

que resolviéndolo nos da las soluciones:

$$2x^2 = 13 \quad , \quad 2y^2 = 1$$

$$x = \pm\sqrt{\frac{13}{2}} \qquad y = \pm\sqrt{\frac{1}{2}}$$

Como es $2xy = \sqrt{13}$, entonces ambos x e y son del mismo signo. Por consiguiente, las soluciones del problema propuesto son los valores:

$$\sqrt{6 + i\sqrt{13}} = x + yi = \sqrt{\frac{13}{2}} + i\sqrt{\frac{1}{2}}$$

$$\sqrt{6 + i\sqrt{13}} = x + yi = -\left(\sqrt{\frac{13}{2}} + i\sqrt{\frac{1}{2}}\right)$$

b) $\sqrt{-11 - 60i}$

c) $\sqrt{7 - i\sqrt{13}}$

3) ¿Qué valores han de tener x e y para satisfacer la ecuación:

$$(2 - 5i)x + (1 + 3i)y - 8 + 9i = 0?$$

4) Poner en forma compleja las expresiones siguientes:

a) $\sqrt{i}$

b) $\frac{1}{\sqrt{i}}$

c) $\sqrt[3]{i}$

5) Averiguar si existe algún número complejo cuyo cuadrado o cubo sea igual a su conjugado; esto es:

a) $(a + bi)^2 = a - bi$

b) $(a + bi)^3 = a - bi$

6) La suma de dos números complejos es $4 + 2i$, siendo la parte real de uno de ellos 3, y el cociente de ellos es un número imaginario puro. Determinar estos números.

7) Reducir a su forma más sencilla las expresiones siguientes:

a) $\sqrt{-49} + \sqrt{-64} - \sqrt{-100} + 3\sqrt{-25} -$

$$-\sqrt{-2\frac{1}{4}} - 3\sqrt{-1\frac{7}{9}} - 5\sqrt{-1\frac{9}{16}}$$

b) $4\sqrt{-2}\cdot\sqrt{-3} - 3\sqrt{-5}\cdot\sqrt{-1\frac{1}{5}} + \sqrt{-2}(\sqrt{-2} + \sqrt{3}) -$

$$-\sqrt{-6}\left(\sqrt{-24} + \sqrt{6} - \sqrt{-\frac{1}{6}}\right)$$

c) $(1 - 2\sqrt{-3})(4 - 5\sqrt{-6}) - (7 - 8\sqrt{-9})(10 + 11\sqrt{-12})$

d) $\dfrac{2\sqrt{8} - \sqrt{-10}}{-\sqrt{-2}}$

e) $\dfrac{3\sqrt{-4} - 2\sqrt{-12} + \sqrt{6} - 9}{-3\sqrt{-2}}$

f) $\dfrac{69 + \sqrt{-3} - 6\sqrt{-5} - 7\sqrt{15}}{3 - \sqrt{-3} + 3\sqrt{-5}}$

8) Siendo $j_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{3}$, $j_2 = i - \frac{1}{2} - \frac{1}{2}\sqrt{-3}$, probar que:

a) $j_1^3 = 1$

b) $j_2^3 = 1$

c) $j_1^2 = j_2$

d) $j_2^2 = j_1$

9) ¿Qué valor tiene $x^2 - 2x + 2$, si $x = 1 \pm i$?

10) ¿Qué valor tiene $x^3 - 5x^2 + 12x - 7$, si $x = 2 \pm \sqrt{-3}$?

11) En el conjunto $\mathbb{C}$ de los números complejos se define la siguiente relación:

$(a, b) \leq (c, d)$ si es $a < c$, y si al ser $a = c$ es $b \leq d$

Probar que bajo estas condiciones arbitrarias, esta relación es de orden total.