Actividades Matemáticas

para el desarrollo de procesos lógicos

Representar estructuras algebraicas finitas y enumerables

Carlos Julio Luque Arias
Haydee Jiménez Tafur
José Leonardo Ángel Bautista

UNIVERSIDAD PEDAGOGICA NACIONAL
Educadora de educadores

Actividades Matemáticas

para el desarrollo de procesos lógicos:

Representar estructuras algebraicas finitas y enumerables

Segunda edición

Carlos Julio Luque Arias
Haydee Jiménez Tafur
José Leonardo Ángel Bautista

UNIVERSIDAD PEDAGOGICA NACIONAL
Educadora de educadores

Luque Arias, Carlos Julio
Actividades matemáticas para el desarrollo de procesos lógicos: representar estructuras algebraicas finitas y enumerables. / Carlos Julio Luque Arias… [et. al.].-- 2ª. ed. -- Bogotá: Universidad Pedagógica Nacional, 2013

354 p.
Incluye bibliografía p. 343

ISBN : 978-958-8650-53-1

1. Isomorfismo (Matemáticas). 2. Axiomas. I. Jiménez Tafur, Haydee. II. Ángel Bautista, José Leonardo. III. Tít.

512 cd. 21 ed.

Juan Carlos Orozco Cruz
Rector

Edgar Alberto Mendoza Parada
Vicerrector Académico

Víctor Manuel Rodríguez Sarmiento
Vicerrector de Gestión Universitaria

Actividades Matemáticas
para el desarrollo de procesos lógicos
Representar estructuras algebraicas finitas y enumerables

© Universidad Pedagógica Nacional
ISBN: 978 - 958 - 8650 - 53 - 1
Primera edición, 2009
Segunda edición, 2013

Autores
© Carlos Julio Luque Arias
Haydee Jiménez Tafur
José Leonardo Ángel Bautista

Prohibida la reproducción total o parcial sin permiso escrito

Preparación editorial
Universidad pedagógica Nacional
Fondo Editorial

Víctor Eligio Espinosa Galán
Coordinador Fondo Editorial

Alba Lucía Bernal Cerquera
Editora

Haydee Jiménez Tafur
Diagramación en LaTeX

Mauricio Esteban Suárez Barrera
Diseño de carátula

Impresión Javegraf
Bogotá, Colombia, 2013

A la memoria de mi madre, Flor María Arias
Carlos Julio Luque Arias.

A mis padres, Marina Tafur y Santos Jiménez
Haydee Jiménez Tafur.

A mis padres, Virginia Bautista y José Ángel
José Leonardo Ángel Bautista.

Índice general

Prólogo

Prólogo a la segunda edición

Este libro es la segunda edición de un producto de la investigación: *Actividades matemáticas para el desarrollo de procesos lógicos: el proceso matemático de representar*, la cual fue desarrollada en la Universidad Pedagógica Nacional durante los años 2005 y 2006, con el propósito de determinar cuáles actividades matemáticas elementales favorecen la abstracción de estructuras algebraicas y el proceso matemático de representarlas, en los estudiantes para profesores de matemáticas, que han cursado los espacios académicos Aritmética y Sistemas Numéricos, del proyecto curricular de Licenciatura en Matemáticas de la Universidad Pedagógica Nacional y, con ellas, establecer lineamientos curriculares que sirvieran como base para el espacio académico Construcción de Estructuras Algebraicas, en la línea de Álgebra, del Proyecto Curricular de Licenciatura en Matemáticas que se está construyendo en el Departamento de Matemáticas de la Universidad Pedagógica Nacional.

Esta edición difiere de la primera no solo en su formato y presentación sino en que se han corregido varios errores y se han ampliado algunas actividades, producto del trabajo de cuatro años con los estudiantes del los cursos de Sistemas Numéricos y de Estructuras Algebraicas de la Universidad Pedagógica Nacional, bajo la guía de profesores pertenecientes al grupo de álgebra, con el mismo espíritu de investigación que generó la primera edición.

Tiene más referencias históricas en particular en el capítulo 7, varias secciones se aumentaron como en el capítulo 3 lo relacionado con las extensiones del campo de Klein; en el capítulo 4 se incluyeron nuevos teoremas en la axiomática de Peano y en el capítulo 6 lo referente a conjuntos equipotentes. La distribución y orden de los capítulos es la misma que en la primera edición.

Adicionalmente se modificó completamente el software *Propiedades de estructuras algebraicas finitas* 3.0. por presentar algunas incompatibilidades con los nuevos sistemas operativos, en particular Windows 7; lo reemplazamos por el programa *Álgebra finita* donde resolvimos los problemas presentados y ampliamos el número de propiedades que se estudian.

Extracto de la introducción de la primera edición

El libro tuvo su origen en la necesidad de superar las dificultades presentadas por los estudiantes de la Universidad, en el desarrollo de los procesos lógicos, y en particular las carencias que se revelan en el manejo de las nociones, propiedades y procedimientos referidos al concepto de estructura.

Hacemos énfasis en la actividad matemática relacionada con el proceso matemático de representar; este es un proceso compuesto, vinculado con procesos más simples como simbolizar, codificar, decodificar, visualizar, modelar, y no se presenta de manera aislada sino que habitualmente aparece junto con los procesos de abstraer, clasificar, sintetizar, conjeturar y generalizar.

En las estructuras finitas ejercitamos el paso de las representaciones a la estructura mediante la abstracción de axiomas que la caractericen, y el proceso inverso de construir representaciones a partir de axiomas.

En las estructuras infinitas no intentamos la abstracción de los axiomas, en su lugar estudiamos diferentes sistemas axiomáticos y los comparamos demostrando su equivalencia. A partir de ellos construimos representaciones.

Diseñamos un conjunto de siete actividades, unas con el propósito de mostrar ambientes académicos de trabajo matemático en los cuales el estudiante esté en condiciones de crear conocimiento matemático nuevo para él; como las descritas en los tres primeros capítulos y en el quinto; otras para estudiar y comparar propuestas matemáticas establecidas como las descritas en los capítulos restantes.

La actividad que se desarrolla en el aula de clase está fundamentada

en preguntas, respuestas, contrapreguntas y reformulación de respuestas en una construcción colectiva donde el profesor y los estudiantes cuestionan, argumentan, ejemplifican, proponen contraejemplos, establecen acuerdos, generalizan, abstraen y, en general, cada actividad simula un ambiente científico; sin embargo, *la presentación* que hacemos de cada actividad, en este libro, está organizada en una forma secuencial que no necesariamente es la misma seguida en clase aunque el espíritu y los resultados son productos de esta interacción.

En el primer capítulo de este libro pretendemos abstraer la estructura algebraica $(Z_2, +)$ comparando varias representaciones de la misma, hasta lograr una caracterización de ella con tablas de Cayley[1] y de ellas obtener otra caracterización en términos de propiedades, lo que nos permite conseguir otras representaciones e identificar el mecanismo de paso de una representación a otra, conocido como isomorfismo, para luego aplicar este proceso a otras operaciones con dos elementos y obtener nuevas representaciones de ellas. Usamos el software *Álgebra finita*[2] para estudiar dichas estructuras y notamos que las estructuras isomorfas tienen las mismas propiedades algebraicas.

Seguidamente estudiamos $(Z_2, \times)$ y, de manera similar a como se hizo para $(Z_2, +)$, partimos de algunas de sus representaciones para llegar a las propiedades que caracterizan esta estructura, establecemos relaciones entre las dos estructuras y buscamos otras estructuras con dos elementos, obteniendo las 16 operaciones posibles en un conjunto con dos elementos; luego establecemos relaciones entre unas operaciones y otras.

A partir de las operaciones conseguidas, buscamos propiedades necesarias y suficientes que nos permitan determinar la estructura, de una única manera, salvo isomorfismos; con ello, logramos formar conjuntos de operaciones y estableciendo axiomas demostramos algunos teoremas, haciendo así miniteorías al interior de este capítulo y nuevamente, buscamos relaciones entre las operaciones caracterizadas, formando así una estructura a partir de estructuras. Finalmente, presentamos una aplicación de Z_2 a la lógica.

En el capítulo dos estudiamos estructuras formadas en conjuntos con tres elementos, en particular el campo $(Z_3, +, \times)$, resolvemos ecuaciones en él, de manera análoga a la que usamos en la secundaria para resolver

[1] ILSE, Dieter; LEHMANN, Ingmar & SCHULZ, Wolfgang. Gruppoide und Funktionalgleichungen. Berlín: VEB Deutscher Verlag der Wissenschaften, 1984. p. 16.

[2] Elaborado por el grupo de Álgebra y programado por Leonardo Ángel, profesor de la Universidad Pedagógica Nacional.

ecuaciones entre números reales, con el propósito de establecer que estos procedimientos no dependen de la naturaleza de los objetos que operamos, sino de las propiedades de las operaciones que entre ellos definamos.

Luego establecemos el mecanismo de paso de una representación a otra, lo que permite abstraer el concepto de isomorfismo y con él, un procedimiento para copiar operaciones que preserva sus propiedades.

En seguida, construimos nuevas estructuras con tres elementos no isomorfas a las ya construidas, modificando la condición de isomorfismo o usando los axiomas del capítulo 1 que nos permitieron obtener estructuras con dos elementos.

Finalmente, construimos estructuras algebraicas a partir de relaciones de orden, los retículos, y presentamos algunas aplicaciones de estos en la construcción de lógicas trivalentes.

En el tercer capítulo mostramos algunas representaciones no triviales de estructuras con un elemento y con cuatro elementos, pero ante el enorme número de operaciones posibles nos restringimos a las dos estructuras de grupo que se pueden formar con cuatro elementos, presentamos algunas de sus representaciones, y con una de ellas, el grupo de Klein, formamos un campo donde estudiamos algunas identidades algebraicas y las ecuaciones de segundo grado, extendiendo tal campo cuando alguna ecuación no tiene solución.

Seguidamente presentamos algunos grupos finitos caracterizables con pocas condiciones como los grupos cíclicos, los grupos de permutaciones, los grupos diedros y el grupo de los cuaternios.

El capítulo 4 tiene un énfasis diferente, la actividad se centra, de una parte en comparar sistemas axiomáticos por lo hecho en la línea de álgebra en el libro del proceso de contar [3], donde a partir de representaciones de los números naturales (no posicionales, posicionales en distintas bases y configuraciones de puntos a la manera pitagórica, entre otras), llegamos a los axiomas de Peano. Y de otra, por la naturaleza de los objetos matemáticos que manejamos, pues al tratarse de conjuntos infinitos estamos ante la imposibilidad de construir tablas, por lo que debemos recurrir a caracterizaciones axiomáticas. En el caso de los números naturales existen varias de ellas epistemológicamente diferentes:

La de Peano que deriva toda la estructura de las nociones primitivas de un *primer elemento* y la noción de *sucesor*, construyendo con ellas las operaciones y el orden; de esta teoría hacemos un desarrollo detallado siguiendo

[3]LUQUE, MORA y PÁEZ, Op. cit., p. 216-227.

los lineamientos de Edmund Landau pero iniciando en 0 y luego mostramos una versión moderna para comparar algunas demostraciones con las versiones originales.

La de Peirce quien asume como términos indefinidos un conjunto N y *una relación de orden* en este conjunto y define las operaciones en forma recursiva; demostramos que esta versión es equivalente a la de Peano.

La de Warner que caracteriza a los números naturales utilizando una *estructura algebraica de semigrupo naturalmente ordenado*; demostramos que esta versión es equivalente a la de Peirce y por lo tanto a la de Peano.

La de Lawvere que es una propuesta radicalmente diferente que consiste en traducir los axiomas de Peano a un *lenguaje de objetos y morfismos* propio de la teoría de categorías, de donde obtenemos la noción de *objeto números naturales*; mostramos que esta versión también es equivalente a la de Peano.

Finalmente, incluimos la teoría de los números naturales en una teoría más general: la teoría de conjuntos a la manera de Zermelo-Fraenkel-Skolem, deducimos de ella los axiomas de Peano y construimos los números naturales como ciertos conjuntos bien ordenados.

En el capítulo cinco nos dedicamos a construir representaciones de los números naturales, primero la representación más conocida, que llamaremos *representación usual* y de ella, con pequeñas variaciones, construimos sucesiones infinitas de números naturales, partiendo de un primer número y adicionándole otro número fijo para conseguir progresiones aritméticas, luego a partir de un primer número multiplicamos por otro fijo y obtenemos progresiones geométricas, luego cambiamos el número fijo que se adiciona por una progresión aritmética obteniendo sucesiones cuadráticas, y repitiendo la secuencia adicionamos una sucesión cuadrática a un primer número para obtener sucesiones cúbicas y así sucesivamente.

Enseguida estudiamos algunas sucesiones definidas por recurrencia a partir de dos elementos y en un caso particular expresamos esto como una sucesión no recurrente. En el siguiente paso construimos sucesiones sumando los primeros términos de otra sucesión obteniendo las series aritméticas y geométricas. Si en lugar de sumar, restamos obtenemos las series telescópicas.

Nuestra siguiente actividad se dirige a copiar la estructura de los números naturales a conjuntos más grandes en el sentido de que los naturales sean un subconjunto propio de ellos y tomamos como ejemplo al conjunto subyacente a la estructura de los números enteros.

En el capítulo seis definimos equivalencia de conjuntos, suponemos la

existencia de los números naturales y los usamos para definir los conjuntos finitos y estudiar sus propiedades, luego los comparamos con otros conjuntos no finitos, y para ello definimos la enumerabilidad y mostramos que la unión finita o enumerable y el producto cartesiano de conjuntos enumerables es enumerable, resultados que usamos para demostrar que los números racionales y los algebraicos son conjuntos enumerables. Al final presentamos someramente a los números cardinales y ordinales transfinitos, definimos operaciones entre ellos y mostramos algunas de sus propiedades.

El capítulo siete lo dedicamos a estudiar otros conjuntos enumerables de números; presentamos una construcción de los números enteros debida a Russell y dos axiomatizaciones: una de Padoa basada en las ideas de sucesor y simétrico y otra de Le Veque basada en la estructura algebraica de dominio de integridad ordenado; demostramos que son equivalentes.

Seguidamente hacemos un breve repaso histórico de representaciones de los números racionales y dos caracterizaciones de ellos una de Weierstrass y otra de Dedekind. Con respecto a los números algebraicos, los autores no conocemos axiomatización alguna, y solo damos de ellos una somera descripción.

Esperamos que el lector disfrute la experiencia de hacer matemática proponiendo variantes a los temas estudiados y profundizando en los ejercicios propuestos.

CAPÍTULO 1

Estructuras algebraicas con dos elementos

> De esto nace la diferencia entre el método de enseñanza y el de invención: quien enseña, sabe adónde va, y conoce el camino que ha de seguir; porque ya le ha recorrido otras veces; mas el que descubre, tal vez no se propone nada determinado, sino examinar lo que hay en el objeto que le ocupa; quizás se prefija un blanco, pero ignorando si es posible alcanzarle, o dudando si existe, si es más que un capricho de su imaginación; y, en caso de estar seguro de su existencia, no conoce el sendero que a él le ha de conducir.
>
> *Jaime Balmes*

En los libros *Actividades matemáticas para el desarrollo de procesos lógicos: clasificar, medir e invertir*[1] y *Estructuras análogas a los números reales*[2], diseñados especialmente para profesores de matemáticas en formación y en particular, como documentos base para los cursos de Aritmética y Sistemas numéricos hemos estudiado estructuras algebraicas como el campo de los números reales, los anillos de los números duales, de los números de Minkowski y de los polinomios con coeficientes en un campo, los campos Z_p con p primo, sin especificar lo que entendemos por estructura algebraica.

En este primer capítulo pretendemos abstraer la estructura $(Z_2, +)$ comparando varias representaciones de la misma; iniciaremos con operaciones en conjuntos con dos elementos, los cuales hasta ahora no hemos considerado como números, por ejemplo la idea de paridad en los números naturales, transformaciones del plano como reflexiones, entre otras, hasta

[1] LUQUE, MORA y TORRES, Op. cit., 2005, p. 263-317.
[2] LUQUE, MORA y TORRES, Op. cit., 2006, p. 27-170.

lograr una caracterización de ella con tablas de Cayley y de ellas obtener otra caracterización en términos de propiedades, lo que nos permite conseguir otras representaciones e identificar el mecanismo de paso de una representación a otra, conocido como isomorfismo, para luego aplicar este proceso a otras operaciones con dos elementos y obtener nuevas representaciones de ellas.

Estudiamos las propiedades que tienen estas estructuras con la ayuda del software *Álgebra finita* y notamos que las estructuras isomorfas tienen las mismas propiedades algebraicas.

Seguidamente estudiamos $(Z_2, \times)$ y, de manera similar a como se hizo para $(Z_2, +)$, partimos de algunas de sus representaciones para llegar a las propiedades que caracterizan esta estructura, basados en las tablas construidas. Posteriormente, establecemos un par de relaciones entre ellas. Luego, buscamos otras estructuras con dos elementos utilizando mecanismos ya propuestos como *el cambio de nombre* de cada uno de los elementos de una tabla en particular y modificaciones de éste, con ello obtenemos las 16 operaciones posibles en un conjunto con dos elementos; con base en esto, buscamos relaciones entre unas operaciones y otras.

A partir de las operaciones establecidas, buscamos propiedades necesarias y suficientes que nos permitan determinar la estructura, de una única manera, salvo isomorfismo; con ello, logramos hacer conjuntos de operaciones y estableciendo axiomas, demostramos algunos teoremas, haciendo así miniteorías al interior de este capítulo y nuevamente, buscamos relaciones entre las operaciones caracterizadas, formando así una estructura a partir de estructuras. Finalmente, presentamos una aplicación de Z_2 a la lógica.

Con todo esto, dejamos el terreno abonado para estudiar, de manera análoga, otras estructuras finitas, tarea que nos asignamos para los dos capítulos siguientes.

1.1. Estructuras isomorfas a $(Z_2, +)$

1.1.1. De las representaciones de $(Z_2, +)$ a la estructura

Presentamos enseguida varias situaciones en las que hay un conjunto con dos elementos y una manera de operarlos, en cada caso el significado de la situación es diferente, los contextos son diversos pero hay algo en común, que es lo que esperamos abstraer.

1.1.1.1. Adición con la idea de paridad e imparidad

Si representamos con P a la propiedad de ser par en los números naturales y con I a la propiedad de ser impar, y sumamos números de la misma o distinta *paridad*, tenemos que al sumar un número par con otro par, obtenemos como resultado un número par, si sumamos par con impar o impar con par, obtenemos un impar y si sumamos impar con impar, obtenemos como resultado un par, estos resultados los podemos resumir en la siguiente tabla:

+	P	I
P	P	I
I	I	P

Tabla 1

1.1.1.2. La composición de reflexiones en el plano

Vayamos ahora a un ambiente geométrico[3]; supongamos, que sobre un plano a tenemos una recta m y un punto P que no pertenece a ella, podemos encontrar un punto P' sobre el mismo plano de tal manera que m sea el eje de reflexión. Y si reflejamos perpendicularmente a P', a través de m, obtendremos nuevamente P; gráficamente tenemos:

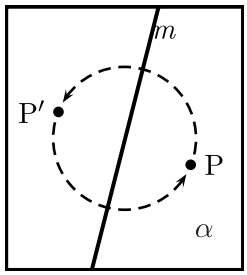


Figura 1

Algebraicamente, esta situación la podemos describir de la siguiente forma: para cada punto de un plano consideramos dos transformaciones, una que llamamos reflexión ortogonal con respecto a la recta dada y notamos con la letra R, y la otra, que a todo punto del plano lo deja en el mismo lugar, la notamos con I; es decir, si a un punto Q sobre el plano le aplicamos I, obtenemos Q.

[3]ALFONSO, Hernando. Geometría plana y del espacio desde un punto de vista euclidiano. Bogotá: Universidad Pedagógica Nacional, 1997. p. 338.

Si efectuamos una transformación y, a continuación, sobre el resultado de esta, aplicamos la otra, decimos que hemos hecho la *composición* de las dos transformaciones, la cual notamos con el símbolo ∘. Las posibles composiciones de reflexiones ortogonales con respecto a una recta sobre un punto cualquiera del plano, las resumimos en la siguiente tabla:

∘	I	R
I	I	R
R	R	I

Tabla 2

1.1.1.3. La composición de rotaciones de 180° en el plano

Supongamos ahora, que tenemos una figura plana cualquiera y un punto fijo M fuera de ella, si la rotamos 180° con respecto a M y notamos esta operación con R, la figura cambia, en relación con su posición inicial, como observamos en la figura 2:

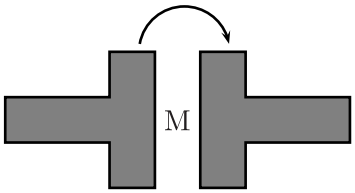


Figura 2

Si reiteramos la operación obtenemos la posición inicial; es decir, la figura queda invariante, notamos esta situación con T. Si aplicamos una transformación a continuación de la otra obtenemos la composición (∘) de ellas, que se resume en:

∘	T	R
T	T	R
R	R	T

Tabla 3

1.1.1.4. La multiplicación de 1 y -1

Supongamos que tenemos un conjunto cuyos elementos son los números enteros 1 y -1, si hallamos los productos entre estos dos números, obtenemos la siguiente tabla:

$\times$	1	-1
1	1	-1
-1	-1	1

Tabla 4

Este conjunto corresponde a las dos raíces cuadradas de 1 en los números enteros, o sea que el producto de dos raíces cuadradas de la unidad es también una de ellas.

1.1.1.5. El conjunto ordenado $\underline{2}$ y la disyunción exclusiva

En lógica clásica[4], utilizamos proposiciones que solo admiten dos valores de verdad, verdadero o falso, representados con los símbolos 1 y 0, respectivamente.

Además de las proposiciones simples, se estudian proposiciones compuestas que se forman a partir de proposiciones y conectivos[5]; los más usuales son la *conjunción* ($\wedge$), la *disyunción* ($\vee$), la *implicación* ($\Rightarrow$), la *doble implicación* ($\Leftrightarrow$) o *equivalencia lógica* y la *disyunción exclusiva* ($\underline{\vee}$).

Si notamos $\{0, 1\} = \underline{2}$, la tabla de verdad de la disyunción exclusiva se obtiene asignando valor de verdad 1 cuando las proposiciones tienen diferente valor de verdad y 0 si coinciden, es decir, cuando el valor de verdad de las dos proposiciones sea excluyente; por ejemplo, un animal está vivo o muerto, una cosa está aquí o allá, pero no en ambos sitios al mismo tiempo, etc. En suma:

$\underline{\vee}$	0	1
0	0	1
1	1	0

Tabla 5

[4]Leibniz formuló por primera vez la idea de un cálculo lógico, los trabajos de Woodhouse, Peacock y Gregory enfatizaron el carácter abstracto de las operaciones lógicas, y con ello se inicia una lógica de las operaciones simbólicas y de las relaciones.

[5]El nuevo impulso al desarrollo de la lógica matemática venía desde finales del siglo XIX con C. S. Peirce. A comienzos del siglo XX, Gottlob Frege de un lado, y Bertrand Russell y Alfred North Whitehead de otro, ampliaron el número de posibles argumentaciones e introdujeron símbolos para frases compuestas y para los conectivos que las unen, como "o", "y", "si... entonces...". Peano también introdujo símbolos y nociones para desarrollar un sistema de signos capaces de enunciar todas las proposiciones de lógica y de matemáticas sin recurrir al lenguaje ordinario.

1.1.1.6. La multiplicación de matrices de Pauli

La Física cuántica describe el comportamiento de las partículas que forman los átomos, como electrones, protones, etc., una de las características comunes a todas ellas es conocida como el *spin*[6], una propiedad que se comporta de manera similar al momento angular de una partícula cuando gira sobre sí misma; matemáticamente se describen usando unas matrices conocidas como matrices de Pauli[7], ellas son:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Estas matrices tienen la propiedad de que al multiplicarse por sí mismas, el producto es la matriz identidad. Resumiendo esto en tablas, obtenemos:

$\times$	1	σ_1
1	1	σ_1
σ_1	σ_1	1

Tabla 6

$\times$	1	σ_2
1	1	σ_2
σ_2	σ_2	1

Tabla 7

$\times$	1	σ_3
1	1	σ_3
σ_3	σ_3	1

Tabla 8

Notemos que estas tablas son, en esencia, la misma; es decir, si notamos cualquiera de las matrices en cuestión $\sigma_1, \sigma_2, \sigma_3$ con la letra M, tenemos:

$\times$	1	M
1	1	M
M	M	1

Tabla 9

1.1.1.7. La estructura $(Z_2, +)$

Observando todas las tablas obtenidas en cada una de las situaciones descritas notamos algo en común que podemos resumir poniendo nombres genéricos, así si el conjunto es $\{a, b\}$ y si notamos con el símbolo $+$ a la operación definida en él, representamos la estructura obtenida mediante la tabla:

[6] GRIFFITHS, David. Introduction to Quantum Mechanics. New Yersey: Prentice Hall, 1994. p. 154.

[7] Las matrices de Pauli junto con la matriz unidad forman una base para el espacio vectorial de las matrices 2×2; esto significa que cualquier matriz 2×2 puede representarse como una combinación lineal de ellas.

$+$	a	b
a	a	b
b	b	a

Tabla 10

Notaremos a esta estructura $(Z_2, +)$.

1.1.2. De la estructura $(Z_2, +)$ a las representaciones

Una pregunta válida en este momento es: ¿podemos describir la tabla 10 en términos de algunas propiedades de la operación? Una opción es: en un conjunto con dos elementos, uno de ellos tiene una conducta particular, es el elemento idéntico, para la tabla anterior, es a; y el otro, b, tiene la característica que al operarlo consigo mismo nos da el elemento idéntico; simbólicamente tenemos:

$$a + a = a$$

$$a + b = b = b + a$$

$$b + b = a$$

Ahora invirtamos el proceso y preguntémonos, ¿dadas las propiedades anteriores podemos recuperar la tabla? La respuesta es sí; pero encontramos dos posibilidades: una cuando el elemento idéntico es a, cuya tabla es la número 10.

Y la otra cuando el elemento idéntico es b:

$\blacklozenge$	a	b
a	b	a
b	a	b

Tabla 11

Pero si intercambiamos en esta última tabla los nombres de a y b, obtenemos:

	b	a
b	a	b
a	b	a

pero al reordenar la tabla conseguimos:

	a	b
a	a	b
b	b	a

Tabla 12

que es exactamente la tabla 10; lo que significa, que las dos tablas representan *la misma operación* con el nombre de los elementos intercambiado.

1.1.2.1. Propiedades de $(Z_2, +)$

Para establecer en cuáles aspectos las dos operaciones $+$ y $\blacklozenge$ *son la misma*, estudiemos las propiedades que ellas cumplen, e iniciemos con las propiedades usualmente estudiadas en los conjuntos numéricos, como la asociativa, conmutativa y existencia de elementos inversos.

Para probar que alguna de ellas, por ejemplo $+$, cumple la propiedad asociativa debemos verificar que para todos los casos posibles, siempre se tiene que

$$x + (y + z) = (x + y) + z$$

donde x, y, z son elementos del conjunto $\{a, b\}$. La tarea no es muy larga, pues solo son ocho casos, veámoslos:

$$a + (a + a) = a + a = (a + a) + a$$

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

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

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

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

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

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

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

Si observamos la tabla de la operación $+$, notamos que el elemento idéntico aparece una sola vez en cada fila y en cada columna, lo que significa que para cada uno de los elementos x del conjunto existe un elemento inverso, que lo notaremos como $-x$, así:

$$-a = a$$

$$-b = b$$

puesto que

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

$$b + (-b) = b + b = (-b) + b = a.$$

La propiedad conmutativa es evidente, se verifica por la simetría de la tabla con respecto a la diagonal ($x = y$). Con esto, concluimos que ($\{a, b\}$, $+$) tiene estructura de grupo abeliano, con elemento idéntico a.

Ejercicio

Verifique que el conjunto $\{a, b\}$ *con la operación* ♦ *cumple las mismas propiedades enunciadas para* $(\{a, b\}, +)$.

Con lo hecho, hemos obtenido dos tablas, *consiguiendo una de la otra con solo un cambio de nombre*, y comprobado que ambas operaciones cumplen las propiedades que caracterizan a un grupo abeliano.

1.1.2.2. Otras caracterizaciones de la misma estructura

Establezcamos ahora si las propiedades enunciadas son las únicas posibles, si son suficientes, y si son necesarias todas. De hecho, hay varias maneras de caracterizar la estructura (Z_2, $+$), por ejemplo:

1. Un conjunto con dos elementos y una operación, donde uno de los elementos es el *elemento idéntico y cada uno de ellos es su propio inverso.*

2. Un conjunto con dos elementos y una operación, que tiene estructura de *grupo abeliano.*

3. Un conjunto con dos elementos y una operación, que tiene estructura de *grupo.*

4. Un conjunto con dos elementos y una operación $*$, donde uno de los elementos es el *elemento idéntico* y cumple la *propiedad cancelativa*, es decir, que para todo x, y, z en el conjunto se tiene que $x * y = x * z$ implica que $y = z$.

Si intentamos recuperar la tabla por ejemplo a partir de la condición 4, la primera parte nos determina tres elementos de ella:

$*$	a	b
a		a
b	a	b

Tabla 13

donde hemos escogido a b como elemento idéntico. La segunda parte de la condición implica que no deben aparecer elementos repetidos en una fila o en una columna; luego el elemento faltante es b, lo que completa la tabla.

Ejercicio

Tome al elemento a como elemento idéntico y verifique que bajo la condición 4 se obtiene la misma tabla 13.

Lo que tienen en común todas las tablas mostradas es lo que llamamos *el grupo abeliano* $(Z_2, +)$ o *el grupo* $(Z_2, +)$ o *el monoide cancelativo* $(Z_2, +)$ y cada uno de los ejemplos es una *representación* de él. Y decimos *él*, porque solo hay uno, con diferentes caras pero uno solo, salvo el nombre; lo que cambia de una representación a otra son los *significados* de los elementos y de la operación.

En particular, si intercambiamos el nombre de los elementos en la tabla 5 de la disyunción exclusiva de la lógica bivalente, obtenemos la tabla correspondiente a la equivalencia lógica:

$\leftrightarrow$	0	1
0	1	0
1	0	1

Tabla 14

Por supuesto que estas dos operaciones son casos particulares de la estructura $(Z_2, +)$ y por lo tanto cumplen las mismas propiedades mencionadas; *la equivalencia lógica no tiene el mismo significado que la disyunción exclusiva*, podríamos decir que son opuestas, en el sentido de que cuando una es verdadera la otra es falsa, pero *sus propiedades algebraicas son las mismas, esto significa que desde el punto de vista algebraico son dos representaciones de una sola estructura. Ambas son representaciones del grupo abeliano* $(Z_2, +)$ *o del monoide cancelativo* $(Z_2, +)$.

1.1.2.3. Paso de una representación a otra

Describamos un poco más en detalle el proceso de construir una operación intercambiando el nombre de los elementos involucrados en otra operación dada: supongamos un conjunto con dos elementos, sea este $C = \{a, b\}$ y la operación $+$ definida como sigue:

$+$	a	b
a	a	b
b	b	a

Tabla 15

intercambiamos el nombre de sus elementos, lo que corresponde a definir la siguiente función:

$$\begin{aligned} \neg : \{a, b\} &\to \{a, b\} \\ a &\mapsto b \\ b &\mapsto a \end{aligned}$$

Ahora, en cada uno de los resultados de la tabla aplicamos la función$\neg$, con esto obtenemos una nueva tabla:

	$\neg a$	$\neg b$
$\neg a$	$\neg a$	$\neg b$
$\neg b$	$\neg b$	$\neg a$

Tabla 16

O sea,

	b	a
b	b	a
a	a	b

y reordenamos la tabla obteniendo la operación definida por:

$\blacklozenge$	a	b
a	b	a
b	a	b

Tabla 17

que tiene la misma estructura algebraica de $(C, +)$, donde cada uno de los elementos de las casillas se obtiene así:

$$x \blacklozenge y = \neg((\neg x) + (\neg y))$$

para elementos arbitrarios x, y en el conjunto C. O de forma equivalente

$$(\neg x) + (\neg y) = \neg(x \blacklozenge y).$$

Si comparamos todos los ejemplos expuestos concluimos que de alguna manera estamos ante la *misma* situación, la única diferencia entre ellas, desde el punto de vista de la operación, es el *nombre* de los entes que ellos representan, en álgebra se les conoce como *estructuras isomorfas*[8].

1.2. Estructuras isomorfas a $(Z_2, \times)$

1.2.1. De las representaciones de $(Z_2, \times)$ a la estructura

1.2.1.1. Multiplicación con la idea de paridad

Apliquemos ahora el mecanismo de copiar estructuras anteriormente expuesta a la idea de *multiplicar* números naturales de la misma o distinta paridad: si multiplicamos un número par con otro par, obtenemos como resultado un número par, si multiplicamos par con impar o impar con par, obtenemos un par y si multiplicamos impar con impar, obtenemos como resultado un impar, en resumen:

$\times$	P	I
P	P	P
I	P	I

Tabla 18

Si aplicamos la función de intercambiar nombre que seguiremos notando $\neg$ al conjunto {P, I} en cada uno de los resultados de la tabla 18 tenemos

	$\neg$ P	$\neg$ I
$\neg$ P	$\neg$ P	$\neg$ P
$\neg$ I	$\neg$ P	$\neg$ I

que es equivalente a

	I	P
I	I	I
P	I	P

[8]FRALEIGH, John. A first course in abstract Algebra. 6 ed. New York: Addison-Wesley, 1999. p. 44.

y la reordenamos obteniendo:

$\Diamond$	P	I
P	P	I
I	I	I

Tabla 19

Esta operación no es la suma, ni la multiplicación entre números naturales pares e impares, pero le podemos asignar un *significado*, si la interpretamos en términos de suma y multiplicación entre paridad e imparidad tenemos que:

$$a \Diamond b = a \times b + (a + b).$$

1.2.1.2. La conjunción y la disyunción lógica

Si aplicamos el procedimiento que hemos venido utilizando a la conjunción de la lógica bivalente que solo es verdadera cuando ambas proposiciones son verdaderas y cuya tabla de verdad es:

$\wedge$	0	1
0	0	0
1	0	1

Tabla 20

nos resulta una nueva operación[9] –la disyunción– haciendo

$$\neg((\neg p) \wedge (\neg q)) = p \vee q$$

cuya tabla es

$\vee$	0	1
0	0	1
1	1	1

Tabla 21

[9]Con "nueva operación" nos estamos refiriendo a otra representación de la misma estructura; es decir, tal como ya lo hemos mencionado, lo que estamos haciendo es obtener estructuras algebraicas isomorfas a otras dadas, solo que sus significados, sus nombres, son distintos, en este sentido son diferentes, la operación que resulta por el procedimiento aplicado es nueva; pero desde el punto de vista algebraico, son iguales, o mejor, isomorfas.

1.2.2. La estructura $(Z_2, \times)$

Nuevamente, la conjunción y la disyunción no tienen el mismo significado pero sí las mismas propiedades; tratemos de caracterizar su estructura[10] buscando algunas propiedades que determinen sus tablas, por ejemplo:

1. Un conjunto con dos elementos y una operación $*$, donde uno de los elementos es el elemento idéntico y cada uno de ellos es *idempotente*, es decir, $a * a = a$ para todo a en el conjunto.

2. Un conjunto con dos elementos y una operación, que tiene estructura de monoide conmutativo y cada uno de sus elementos es idempotente.

3. Un conjunto con dos elementos y una operación, que tiene estructura de monoide y cada uno de sus elementos es idempotente.

4. Un conjunto con dos elementos y una operación $*$, donde para todo x, y en el conjunto se tiene que $x * x = x$ y $x * y = y * x$.

Si ponemos nombres genéricos, esto es, consideramos el conjunto $\{a, b\}$ y la operación $\times$, la tabla dada por las propiedades anteriores es:

$\times$	a	b
a	a	a
b	a	b

Tabla 22

Donde se eligió a b como elementos idéntico. Notaremos a esta estructura $(Z_2, \times)$.

Si definimos el resultado de operar elementos arbitrarios x e y del conjunto como $\neg((\neg x) \times (\neg y))$, obtenemos una nueva operacion ♠, que tiene al elemento a como elemento idéntico, y por supuesto, es otra representación de $(Z_2, \times)$.

♠	a	b
a	a	b
b	b	b

Tabla 23

[10]Siempre que mencionemos el término estructura nos estamos refiriendo a estructura algebraica.

1.3. Relaciones entre las estructuras construidas

1.3.1. Propiedad distributiva

Las estructuras $(\{a,\, b\},\, \times)$ y $(\{a,\, b\},\, \spadesuit)$ tienen algo que no tienen las estructuras $(\{a,\, b\},\, +)$ y $(\{a,\, b\},\, \blacklozenge)$ construidas anteriormente: la operación $\times$ es distributiva con respecto a la operación $\spadesuit$, esto significa que para todo elemento x, y, z en el conjunto $\{a,\, b\}$ se cumple:

$$x \times (y \spadesuit z) = (x \times y) \spadesuit (x \times z).$$

Pero hay más, también la operación $\spadesuit$ es distributiva con respecto a la operación $\times$, o sea que

$$x \spadesuit (y \times z) = (x \spadesuit y) \times (x \spadesuit z).$$

¡Una operación que es distributiva con respecto a una copia de ella misma!

Y para completar sus acoples, la operación $\times$ también es distributiva con respecto a la operación $+$ y la operación $\spadesuit$ es distributiva con respecto a la operación $\blacklozenge$.

En particular tenemos que $(\{a,\, b\}, +, \times)$ tiene estructura de campo, al igual que $(\underline{2},\, \veebar,\, \wedge)$ y que $(\underline{2}, \leftrightarrow, \vee)$.

Para demostrar cada una de estas relaciones, debemos hacer las cuentas correspondientes (8 en cada caso), por ejemplo para probar que

$$x \times (y \spadesuit z) = (x \times y) \spadesuit (x \times z)$$

debemos verificar que se cumplen cada una de las igualdades;

$$a \times (a \spadesuit a) = (a \times a) \spadesuit (a \times a)$$

$$a \times (a \spadesuit b) = (a \times a) \spadesuit (a \times b)$$

$$a \times (b \spadesuit a) = (a \times b) \spadesuit (a \times a)$$

$$a \times (b \spadesuit b) = (a \times b) \spadesuit (a \times b)$$

y así para cada combinación posible de los elementos a y b.

Ejercicios

1. *Demuestre que* $(\{a,\, b\},\, \blacklozenge,\, \spadesuit)$ *tiene estructura de campo.*
2. *Demuestre que* $(\{a, b\}, +, \spadesuit)$ *no tiene estructura de campo.*

1.3.2. Propiedad absorbente

Otra relación entre las operaciones ♠ y $\times$ es que para todo x y y

$$x \times (x \spadesuit y) = x = x \spadesuit (x \times y)$$

conocida como ley de absorción[11]. Si suponemos que esta propiedad es válida, podemos deducir las leyes de idempotencia para $\times$ y ♠, para la primera basta reemplazar $y = x \times x$ en la primera igualdad y hacer $y = x$ en la segunda igualdad, obteniendo

$$x \times (x \spadesuit (x \times x)) = x \times x = x.$$

Ejercicio

Demuestre la propiedad de idempotencia para la estructura $(\{a, b\}, \spadesuit)$.

1.4. Otras estructuras con dos elementos

1.4.1. A partir de la conjunción

Hemos visto que

$$x \blacklozenge y = \neg((\neg x) + (\neg y))$$

nos permite construir una operación ♦ a partir de la operación $+$ y que a pesar de tener significados diferentes son algebraicamente iguales.

Modifiquemos este mecanismo para construir otras operaciones –que esperamos sean algebraicamente distintas–, usando otras igualdades, basadas en la anterior[12], por ejemplo, partiendo de la operación $\wedge$ en $\{0, 1\}$, iniciemos eliminando las negaciones en el interior de los paréntesis en el lado derecho de la igualdad, con esto obtenemos una nueva operación[13] que notamos con $|$:

[11] Esta propiedad se usa como uno de los axiomas para definir algebraicamente una estructura conocida como retículo. (BIRKHOFF, Garrett. Lattice Theory. Providence (Rhode Island): AMS, 1940. p. 8).

[12] Usamos el nombre de conjunción, disyunción, etc., para las operaciones en un conjunto con dos elementos que notamos 0 y 1, y negación para la función biyectiva que intercambia los nombres de 0 y 1, por analogía con los nombres correspondientes de la lógica.

[13] Esta operación conocida como *barra de Sheffer*, fue descubierta por Peirce en 1902 y redescubierta por Sheffer en 1913, con ella es posible construir todas las otras operaciones lógicas y por ello forma uno de los *conjuntos completos de conectivos* para el cálculo proposicional clásico, actualmente se usa en el diseño de circuitos lógicos con el nombre de compuerta NAND.

1. $x|y = \neg(x \wedge y)$ cuya tabla es

$\|$	0	1
0	1	1
1	1	0

Tabla 24

También podemos eliminar solo la negación en el primer elemento que se opera y obtener:

2. $x \rightarrow y = \neg(x \wedge (\neg y))$ cuya tabla es

$\rightarrow$	0	1
0	1	1
1	0	1

Tabla 25

que corresponde con la *implicación* habitual de la lógica clásica. O eliminar solo la negación en el segundo elemento que se opera y encontrar:

3. $x \leftarrow y = \neg((\neg x) \wedge y)$ cuya tabla es

$\leftarrow$	0	1
0	1	0
1	1	1

Tabla 26

que corresponde con la *implicación recíproca* de $x \rightarrow y$, o sea $y \rightarrow x$ y que la simbolizamos con $x \leftarrow y$. O eliminar la negación que afecta al primer paréntesis y conseguir la operación[14]:

[14]Conocida como *flecha, funtor* o *functor de Peirce*, fue descubierta por Peirce en 1880 y es otro de los conectivos completos para el cálculo proposicional clásico, actualmente se usa en el diseño de circuitos lógicos con el nombre de compuerta NOR.

4. $x \downarrow y = (\neg x) \wedge (\neg y)$ cuya tabla es

$\downarrow$	0	1
0	1	0
1	0	0

Tabla 27

o considerar las alternativas:

5. $x - \bullet y = x \wedge (\neg y)$
6. $x \bullet - y = (\neg x) \wedge y$

cuyas tablas son

$-\bullet$	0	1
0	0	0
1	1	0

Tabla 28

y

$\bullet-$	0	1
0	0	1
1	0	0

Tabla 29

respectivamente; a estas operaciones las llamaremos *diferencia* y *diferencia recíproca* en ese orden. O finalmente, quitar –lo que parece inútil– todas las negaciones y llegar a donde partimos:

$$x \wedge y = x \wedge y.$$

Podemos también intercambiar el lugar de x e y, pero debido a que la operación con que iniciamos el proceso es conmutativa[15], obtenemos las mismas operaciones. Sin embargo, podríamos esperar que cuando los mecanismos mencionados se apliquen a operaciones no conmutativas obtuviéramos otras operaciones diferentes a las ya obtenidas, pero curiosamente esto no es así, como se puede ver en la siguiente tabla:

[15]O si invertimos el razonamiento, el hecho de que las tablas obtenidas intercambiando x e y sean las mismas indican que la operación es conmutativa.

	$\wedge$	$\vee$	$\mid$	$\downarrow$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$
$x \textcircled{c} y$	$\wedge$	$\vee$	$\mid$	$\downarrow$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$
$\neg((\neg x)\textcircled{c}(\neg y))$	$\vee$	$\wedge$	$\downarrow$	$\mid$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$
$\neg(x\textcircled{c}y)$	$\mid$	$\downarrow$	$\wedge$	$\vee$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$
$\neg(x\textcircled{c}(\neg y))$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\wedge$	$\downarrow$	$\mid$	$\vee$
$\neg((\neg x)\textcircled{c}y)$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\downarrow$	$\wedge$	$\vee$	$\mid$
$(\neg x)\textcircled{c}(\neg y)$	$\downarrow$	$\mid$	$\vee$	$\wedge$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$
$x\textcircled{c}(\neg y)$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$\mid$	$\vee$	$\wedge$	$\downarrow$
$(\neg x)\textcircled{c}y$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\vee$	$\mid$	$\downarrow$	$\wedge$
$y\textcircled{c}x$	$\wedge$	$\vee$	$\mid$	$\downarrow$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$
$\neg((\neg y)\textcircled{c}(\neg x))$	$\vee$	$\wedge$	$\downarrow$	$\mid$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$
$\neg(y\textcircled{c}x)$	$\mid$	$\downarrow$	$\wedge$	$\vee$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$
$\neg(y\textcircled{c}(\neg x))$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\wedge$	$\downarrow$	$\mid$	$\vee$
$\neg((\neg y)\textcircled{c}x)$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\downarrow$	$\wedge$	$\vee$	$\mid$
$(\neg y)\textcircled{c}(\neg x)$	$\downarrow$	$\mid$	$\vee$	$\wedge$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$
$y\textcircled{c}(\neg x)$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\mid$	$\vee$	$\wedge$	$\downarrow$
$(\neg y)\textcircled{c}x$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$\vee$	$\mid$	$\downarrow$	$\wedge$

Tabla 30

1.4.2. A partir de la equivalencia

En busca de nuevas operaciones, apliquemos cada uno de los procedimientos efectuados con la conjunción, a una operación que no aparezca en la tabla 30, por ejemplo a la *equivalencia lógica*:

$\leftrightarrow$	0	1
0	1	0
1	0	1

Tabla 14

como ya sabemos, si aplicamos $\neg((\neg x) \leftrightarrow (\neg y))$ obtenemos la *disyunción exclusiva*

$$x \veebar y = \neg((\neg x) \leftrightarrow (\neg y))$$

cuya tabla es:

$\veebar$	0	1
0	0	1
1	1	0

Tabla 5

pero lamentablemente al aplicar cualquiera de los procedimientos anteriores a la disyunción exclusiva y a la equivalencia lógica, obtenemos de nuevo las mismas dos operaciones, como lo puede verificar un lector ligeramente acucioso.

1.4.3. A partir de la primera proyección

Como nuestro intento de conseguir nuevas operaciones con lo conocido no tuvo éxito, observemos que cada tabla de las que hemos obtenido es un arreglo de cuatro números que son unos o ceros y en total hay 16 posibilidades para hacer esta elección, que corresponden con los números con cuatro cifras entre 0000 y 1111 escritos en base 2.

Hemos estudiado las cuatro tablas que tienen 3 ceros y 1 uno, las cuatro tablas que tienen 3 unos y 1 cero y 2 tablas que tienen 2 unos en una diagonal y 2 ceros en la otra; nos faltan las que tienen 2 ceros (o 2 unos) en una misma columna o en una misma fila y para ello hay 4 posibilidades: π_1 que llamaremos *primera proyección*, $\otimes$ que corresponde a la *negación de la primera proyección; la segunda proyección* π_2 y su negación $*$:

π_1	0	1
0	0	0
1	1	1

Tabla 31

$*$	0	1
0	1	0
1	1	0

Tabla 32

$\otimes$	0	1
0	1	1
1	0	0

Tabla 33

π_2	0	1
0	0	1
1	0	1

Tabla 34

y todas ellas se obtienen unas de otras con alguno de los mecanismos mencionados. Por ejemplo

$$\begin{aligned} x \otimes y &= \neg(x\,\pi_1\,y) \\ x * y &= \neg(y\,\pi_1\,x) \\ x\,\pi_2\,y &= (y\,\pi_1\,x) \end{aligned}$$

Ejercicio

Demuestre que cualquiera de las operaciones π_1, π_2, $\otimes$ o $*$ sirve para expresar las demás en términos de ella.

1.4.4. A partir de la tautología

Solo quedan las tablas con 4 unos y con 4 ceros, que corresponden a:

$\top$	0	1
0	1	1
1	1	1

Tabla 35

$\bot$	0	1
0	0	0
1	0	0

Tabla 36

La primera operación la llamamos *tautología* y la segunda *contradicción*. Si aplicamos los mecanismos definidos para conseguir otras operaciones a estas tablas obtenemos las mismas dos operaciones. Resumamos lo observado en la siguiente tabla:

	$\wedge$	$\vee$	$\mid$	$\downarrow$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\veebar$	$\leftrightarrow$	$*$	$\otimes$	π_1	π_2	$\top$	$\bot$
$x \textcircled{c} y$	$\wedge$	$\vee$	$\mid$	$\downarrow$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\veebar$	$\leftrightarrow$	$*$	$\otimes$	π_1	π_2	$\top$	$\bot$
$\neg((\neg x) \textcircled{c} (\neg y))$	$\vee$	$\wedge$	$\downarrow$	$\mid$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$	$\leftrightarrow$	$\veebar$	$*$	$\otimes$	π_1	π_2	$\bot$	$\top$
$\neg(x \textcircled{c} y)$	$\mid$	$\downarrow$	$\wedge$	$\vee$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$	$\leftrightarrow$	$\veebar$	π_2	π_1	$\otimes$	$*$	$\bot$	$\top$
$\neg(x \textcircled{c} (\neg y))$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\wedge$	$\downarrow$	$\mid$	$\vee$	$\veebar$	$\leftrightarrow$	$*$	π_1	$\otimes$	π_2	$\bot$	$\top$
$\neg((\neg x) \textcircled{c} y)$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\downarrow$	$\wedge$	$\vee$	$\mid$	$\veebar$	$\leftrightarrow$	π_2	$\otimes$	π_1	$*$	$\bot$	$\top$
$(\neg x) \textcircled{c} (\neg y)$	$\downarrow$	$\mid$	$\vee$	$\wedge$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$	$\veebar$	$\leftrightarrow$	π_2	π_1	$\otimes$	$*$	$\top$	$\bot$
$x \textcircled{c} (\neg y)$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$\mid$	$\vee$	$\wedge$	$\downarrow$	$\leftrightarrow$	$\veebar$	π_2	$\otimes$	π_1	$*$	$\top$	$\bot$
$(\neg x) \textcircled{c} y$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\vee$	$\mid$	$\downarrow$	$\wedge$	$\leftrightarrow$	$\veebar$	$*$	π_1	$\otimes$	π_2	$\top$	$\bot$
$y \textcircled{c} x$	$\wedge$	$\vee$	$\mid$	$\downarrow$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$	$\veebar$	$\leftrightarrow$	$\otimes$	$*$	π_2	π_1	$\top$	$\bot$
$\neg((\neg y) \textcircled{c} (\neg x))$	$\vee$	$\wedge$	$\downarrow$	$\mid$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$	$\leftrightarrow$	$\veebar$	$\otimes$	$*$	π_2	π_1	$\bot$	$\top$
$\neg(y \textcircled{c} x)$	$\mid$	$\downarrow$	$\wedge$	$\vee$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$	$\leftrightarrow$	$\veebar$	π_1	π_2	$*$	$\otimes$	$\bot$	$\top$
$\neg(y \textcircled{c} (\neg x))$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\rightarrow$	$\wedge$	$\downarrow$	$\mid$	$\vee$	$\veebar$	$\leftrightarrow$	$\otimes$	π_2	$*$	π_1	$\bot$	$\top$
$\neg((\neg y) \textcircled{c} x)$	$\rightarrow$	$\bullet\!\!-$	$-\!\!\bullet$	$\leftarrow$	$\downarrow$	$\wedge$	$\vee$	$\mid$	$\veebar$	$\leftrightarrow$	π_1	$*$	π_2	$\otimes$	$\bot$	$\top$
$(\neg y) \textcircled{c} (\neg x)$	$\downarrow$	$\mid$	$\vee$	$\wedge$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\bullet\!\!-$	$\veebar$	$\leftrightarrow$	π_1	π_2	$*$	$\otimes$	$\top$	$\bot$
$y \textcircled{c} (\neg x)$	$\bullet\!\!-$	$\rightarrow$	$\leftarrow$	$-\!\!\bullet$	$\mid$	$\vee$	$\wedge$	$\downarrow$	$\leftrightarrow$	$\veebar$	π_1	$*$	π_2	$\otimes$	$\top$	$\bot$
$(\neg y) \textcircled{c} x$	$-\!\!\bullet$	$\leftarrow$	$\rightarrow$	$\bullet\!\!-$	$\vee$	$\mid$	$\downarrow$	$\wedge$	$\leftrightarrow$	$\veebar$	$\otimes$	π_2	$*$	π_1	$\top$	$\bot$

Tabla 37

1.4.5. Relaciones entre las estructuras obtenidas

De la tabla anterior es posible obtener igualdades que relacionan unas operaciones con otras, tales como:

$$(\neg y) \wedge x = x - \bullet y$$

o

$$y \wedge (\neg x) = x \bullet - y$$

o

$$\neg((\neg y) \downarrow x) = x \leftarrow y$$

$$y \downarrow (\neg x) = x - \bullet y$$

y si comparamos la primera igualdad con la última obtenemos que

$$(\neg y) \wedge x = y \downarrow (\neg x).$$

Leyendo la segunda fila de la tabla 37 en sus dos primeras columnas encontramos dos relaciones entre las operaciones conjunción y disyunción que en lógica son conocidas como las leyes de De Morgan[16]:

$$\neg((\neg x) \wedge (\neg y)) = x \vee y$$

$$\neg((\neg x) \vee (\neg y)) = x \wedge y$$

Y en las otras columnas relaciones análogas para cada par de conectivos, por ejemplo:

$$\neg((\neg x) \downarrow (\neg y)) = x|y$$

$$\neg((\neg x)|(\neg y)) = x \downarrow y$$

En la cuarta fila aparece

$$\neg(x \copyright (\neg y))$$

que relaciona en la primera columna a la conjunción con la implicación, es decir que

$$\neg(x \rightarrow (\neg y)) = x \wedge y$$

y por una de las leyes de De Morgan, deducimos que

$$\neg((\neg x) \vee (\neg y)) = \neg(x \rightarrow (\neg y)).$$

[16]En honor al matemático inglés, nacido en India, Augustus De Morgan (1806-1871).

También tenemos que

$$\neg(x \wedge (\neg y)) = x \to y$$

o sea que

$$x \to y = \neg x \vee y.$$

Ejercicio

Halle otras relaciones entre las operaciones mencionadas en la tabla 37.

1.5. Caracterización de las estructuras con dos elementos

Volvamos a las 16 operaciones (conectivos) posibles en un conjunto con dos elementos y tratemos de caracterizarlas con algunas *propiedades básicas* (axiomas), es decir, propiedades necesarias y suficientes para que la estructura quede determinada de manera única, salvo isomorfismos.

1.5.1. La conjunción y la disyunción

Las condiciones:

Para todo x, y en $\{0, 1\}$ se cumple que[17]

A1. $xx = x$ (Idempotencia)
A2. $xy = yx$, (Conmutativa)

determinan las operaciones conjunción $\wedge$, y disyunción $\vee$ de la lógica usual. La primera, A1, determina la diagonal principal:

$\wedge$	0	1
0	0	
1		1

$\vee$	0	1
0	0	
1		1

y la segunda dice que los elementos de la diagonal secundaria deben ser iguales y para ello hay dos posibilidades: o son 0 o son 1, la primera opción determina la conjunción y la segunda la disyunción.

[17]Omitiremos el símbolo de la operación, con el ánimo de simplificar la escritura, esto quiere decir que xy representa $x \copyright y$ y xx representa $x \copyright x$, la operación se hace explícita en el texto.

Estas dos operaciones también son asociativas y tienen elemento idéntico, y cumplen otras propiedades que no se mencionan[18] ni se estudian en los libros de texto de álgebra que habitualmente consultamos a nivel de la Licenciatura o de los programas de matemáticas, por ejemplo:

i. Identidad I de Stein[19]: $x(xy) = yx$

ii. Identidad II de Stein: $x(yx) = (yx)y$

iii. Identidad I de Schröder[20]: $x(xy) = (xy)y$

iv. Elasticidad: $x(yx) = (xy)x$

v. Asociativa cíclica I: $x(yz) = z(xy)$

vi. Asociativa cíclica II: $x(yz) = (zx)y$

vii. Identidad de Abel – Graßmann I: $x(yz) = z(yx)$

viii. Identidad de Abel – Graßmann II: $x(yz) = (yx)z$

ix. Permutabilidad a izquierda: $x(yz) = y(xz)$

x. Permutabilidad a derecha: $(xy)z = (xz)y$

xi. Propiedad del producto reducido o cruzado[21] : $(xy)z = x(zy)$

xii. Autodistributividad a izquierda: $x(yz) = (xy)(xz)$

xiii. Autodistributividad a derecha: $(xy)z = (xz)(yz)$

xiv. Autodistributividad a izquierda abeliana: $x(yz) = (xy)(zx)$

xv. Autodistributividad a derecha abeliana: $(xy)z = (zx)(yz)$

xvi. Bisimetría: $(xy)(uv) = (xu)(yv)$

[18]ILSE, LEHMANN & SCHULZ, Op. cit., p. 67-68.

[19]STEIN, Sherman. On the foundations of quasigroups, Trans. Amer. Math. Soc. 85, 1957. p. 228-256.

[20]SCHRÖDER, Ernst. Lehrbuch der arithmetik und algebra fuer lehrer und studierende, Band 1, Leipzig: Teubner, 1873. Schröder fue corresponsal de Peirce y uno de los principales responsables de que las ideas lógico-matemáticas de éste último ingresaran al corpus de la ciencia.

[21]El original en alemán es *Eingewandtes Produkt.*

Sin embargo, en este caso, *todas* estas propiedades pueden deducirse de los axiomas A1 y A2. Por ejemplo derivemos las propiedades de elasticidad, la identidad I de Stein y la I de Schröder.

T1. *Elasticidad*: para todo x, y en el conjunto $X = \{0, 1\}$, $x(yx) = (xy)x$.

$$\begin{aligned} x(yx) &= x(xy) \quad \text{por A2} \\ &= (xy)x \quad \text{por A2} \end{aligned}$$

Esto significa que cualquier estructura que sea conmutativa es elástica. Pero la recíproca no es cierta por ejemplo:

π_1	0	1
0	0	0
1	1	1

es elástica pero no conmutativa.

T2. *Identidad I de Stein:* para todo x, y en el conjunto $X = \{0, 1\}$, $x(xy) = yx$.

Como en X solo hay dos elementos dividimos la prueba en dos partes,
Si $xy = y$

$$\begin{aligned} x(xy) &= xy && \text{Por hipótesis} \\ &= yx && \text{Por A2} \end{aligned}$$

Si $xy = x$

$$\begin{aligned} x(xy) &= xx && \text{Por hipótesis} \\ &= x && \text{Por A1} \\ &= xy && \text{Por hipótesis} \\ &= yx && \text{Por A2} \end{aligned}$$

T3. *Identidad I de Schröder:* para todo x, y en el conjunto $X = \{0, 1\}$, $x(xy) = (xy)y$.

Dividimos de nuevo la prueba en dos partes,
Si $xy = y$

$$\begin{aligned} x(xy) &= xy && \text{Por hipótesis} \\ &= (xy)(xy) && \text{Por A1} \\ &= (xy)y && \text{Por hipótesis} \end{aligned}$$

Si $xy = x$

$x(xy) = xx$	Por hipótesis
$x(xy) = x$	Por A1
$x(xy) = xy$	Por hipótesis
$xx = xy$	Por hipótesis
$x = xy$	Por A1
$xy = (xy)y$	Operando con y a ambos lados de la igualdad
$(xy)(xy) = (xy)y$	Por A1
$x(xy) = (xy)y$	Por hipótesis

Ejercicio

Pruebe la identidad de Stein II.

Ahora usando los axiomas A1 y A2, probemos

T4. *Propiedad asociativa de la conjunción y la disyunción:* para todo x, y, z en el conjunto $X = \{0, 1\}$, se cumple que $x\,(yz) = (xy)\,z$.

Como en el conjunto solo hay dos elementos entonces, $z = x$ o $z = y$, dividimos de nuevo la prueba en dos partes,
Si $z = x$

$x(yx) = (xy)x$	Por hipótesis y la propiedad de elasticidad (T1)

Si $z = y$

$x(yy) = xy$	Por hipótesis y por A1
$= yx$	Por A2
$= x(xy)$	Por la identidad I de Stein (T2)
$= (xy)y$	Por la identidad I de Schröder (T3).

T5. *Existencia del elemento idéntico.*

Como en X solo hay dos elementos dividimos la prueba en dos partes,
Si $xy = y$ entonces x es el elemento idéntico puesto que $xx = x$.
Si $xy = x$ entonces y es el elemento idéntico puesto que $yy = y$.

En nuestro caso particular del conjunto $X = \{0, 1\}$ y de las operaciones de conjunción y disyunción, las propiedades enunciadas están relacionadas

unas con otras y podemos demostrar unas de ellas y usarlas como argumento para abreviar la demostración de las demás; por ejemplo, las propiedades asociativa cíclica I y II, las identidades de Abel–Graβmann I y II, la permutabilidad a izquierda y a derecha, la propiedad del producto reducido y la bisimetría son consecuencias inmediatas de la asociatividad y la conmutatividad, mientras que las propiedades de autodistributividad a izquierda y a derecha y las correspondientes abelianas requieren para su prueba, además la propiedad de idempotencia.

Sin embargo debemos limitar el alcance de nuestras afirmaciones, no hemos afirmado que la propiedad asociativa se deduzca de las propiedades de idempotencia y conmutativa; hemos afirmado que esto es válido en un conjunto con dos elementos, pero *en contextos más generales*, se pueden enunciar las mismas propiedades y que ellas sean independientes unas de otras, por ejemplo: la operación *construcción del punto medio*, definida para todo par de puntos P y Q de un plano α, mediante $P * Q = R$ donde R es el punto medio del $\overline{PQ}$ y $P * P = P$, es conmutativa y bisimétrica pero no asociativa. Tampoco la conmutatividad es consecuencia de la bisimetría, por ejemplo la sustracción entre números enteros es bisimétrica, pero no asociativa, ni conmutativa, pues para enteros cualesquiera x, y, u, v se tiene que

$$(x - y) - (u - v) = (x - u) - (y - v).$$

El juego de la axiomática consiste en elegir unas propiedades que nos sirvan como axiomas para definir una estructura y demostrar las demás en términos de ellas.

Las propiedades que se eligen como axiomas no son las únicas que definen la estructura, puede haber varios conjuntos de axiomas que definan la misma estructura, como lo vimos en la sección 1.2.2.

La caracterización habitual[22] de las operaciones conjunción y disyunción de la lógica bivalente, dentro de la teoría de retículos, es que son asociativas, conmutativas e idempotentes, pero como hemos visto, *en este caso* la propiedad asociativa se puede deducir de las otras dos.

También podríamos pensar en reemplazar la condición de idempotencia, como axioma, por la existencia de un elemento idéntico; no obstante, esto último no determina la estructura pues la equivalencia lógica y la disyunción exclusiva son otras operaciones, con dos elementos, que son monoides conmutativos y no son isomorfas con la conjunción o la disyunción.

[22]LENTIN, André y RIVAUD, Jacques. Álgebra Moderna. Madrid: Aguilar, 1971. p. 40.

La propiedad asociativa generalmente se asume como axioma[23] para la mayoría de las estructuras que se definen en el álgebra abstracta: semigrupos, monoides, grupos, anillos, campos, etc. Pero como vimos en esta sección, para el caso de la disyunción y la conjunción, esto no es necesario.

1.5.2. La flecha de Peirce y la barra de Sheffer

Las condiciones:

Para todo x, y en $\{0, 1\}$ se cumple que

A2. $xy = yx$, (Conmutativa)

A3. $xx = y$ con $x \neq y$.

determinan las operaciones barra de Sheffer $|$, u operador NAND, y funtor de Peirce[24] $\downarrow$, u operador NOR de la lógica bivalente. La condición A3 determina la diagonal principal:

$\mid$	0	1
0	1	
1		0

$\downarrow$	0	1
0	1	
1		0

y la condición A2 dice que los elementos de la diagonal secundaria deben ser iguales y para ello hay dos posibilidades: o son 1 o son 0, la primera opción determina la barra y la segunda el funtor.

Estas dos operaciones cumplen, de las propiedades enunciadas anteriormente, solo la propiedad elástica, que es deducible de la propiedad conmutativa como lo mostramos en el teorema T1.

A pesar de que la flecha o funtor de Peirce carece de casi todas las propiedades enunciadas para otras operaciones, esta operación permite expresar todas las demás operaciones lógicas solo en términos de ella, por ejemplo:

La negación:

$$\neg p = p \downarrow p.$$

[23] MOSTOW, George; SAMPSON, Joseph y MEYER, Jean-Pierre. Fundamental Structures of Algebra. New York: McGraw Hill, 1963. p. 8.

[24] El aporte de Peirce a la lógica también incluye el invento de la lógica de relaciones, la lógica de cuantificadores y la lógica trivalente; estudió la axiomatización del cálculo proposicional, el cálculo implicativo débil, la negación intuicionista, las tablas de verdad, los conectivos completos, las definiciones reticulares y la notación de los conectivos proposicionales.

La disyunción:

$$p \vee q = (p \downarrow q) \downarrow (p \downarrow q).$$

Y la conjunción:

$$p \wedge q = (p \downarrow p) \downarrow (q \downarrow q).$$

Ejercicios

1. *Verifique que se cumple*

   - $p \perp q = (p \downarrow q) \downarrow ((p \downarrow q) \downarrow (p \downarrow q))$
   - $p \top q = ((p \downarrow q) \downarrow ((p \downarrow q) \downarrow (p \downarrow q))) \downarrow ((p \downarrow q) \downarrow ((p \downarrow q) \downarrow (p \downarrow q)))$
   - $p \bullet -q = (p \downarrow q) \downarrow p$
   - $p \leftarrow q = ((p \downarrow q) \downarrow p) \downarrow ((p \downarrow q) \downarrow p)$
   - $p - \bullet q = (p \downarrow q) \downarrow q$
   - $p \rightarrow q = ((p \downarrow q) \downarrow q) \downarrow ((p \downarrow q) \downarrow q)$
   - $p \, \pi_1 \, q = (p \downarrow q) \downarrow (p \downarrow p)$
   - $p \otimes q = ((p \downarrow q) \downarrow (p \downarrow p)) \downarrow ((p \downarrow q) \downarrow (p \downarrow p))$
   - $p \, \pi_2 \, q = (p \downarrow q) \downarrow (q \downarrow q)$
   - $p * q = ((p \downarrow q) \downarrow (q \downarrow q)) \downarrow ((p \downarrow q) \downarrow (q \downarrow q))$
   - $p \leftrightarrow q = ((p \downarrow q) \downarrow p) \downarrow ((p \downarrow q) \downarrow q)$
   - $p \veebar q = (((p \downarrow q) \downarrow p) \downarrow ((p \downarrow q) \downarrow q)) \downarrow (((p \downarrow q) \downarrow p) \downarrow ((p \downarrow q) \downarrow q))$
   - $p|q = ((p \downarrow p) \downarrow (q \downarrow q)) \downarrow ((p \downarrow p) \downarrow (q \downarrow q))$.

2. *Se denomina conjunto completo de conectivos*[25] *a un conjunto de conectivos tal que toda función de verdad puede representarse por medio de una fórmula que contenga solamente conectivos del conjunto. Demuestre que el conjunto* $\{|\}$ *cuyo único elemento es la barra de Sheffer y el conjunto* $\{\vee, \neg\}$*, son conjuntos completos de conectivos. Naturalmente* $\{\downarrow, \neg\}$, $\{|, \neg\}$, $\{|, \downarrow\}$ *son conjuntos completos de conectivos.*

3. *¿Los conjuntos* $\{\rightarrow, \neg\}$ *y* $\{\leftrightarrow, \neg\}$ *son conjuntos completos de conectivos?*

[25] Encontrar conjuntos completos de conectivos es útil para analizar las compuertas lógicas en electrónica pues permiten diseñar cualquier circuito usando un conjunto muy reducido de dispositivos.

Al incluir varios conectivos en un conjunto completo de conectivos se simplifican las expresiones.

1.5.3. La implicación y la diferencia recíproca

Las condiciones:

Para todo x, y en $\{0, 1\}$ se cumple que

A4. $xx = yy$ (Unipotencia)

A5. $xy = y$ con $x \neq y$

determinan las operaciones *implicación* $\rightarrow$*, y diferencia recíproca* $\bullet-$, y las únicas propiedades de las enunciadas que cumplen son permutabilidad a izquierda y autodistributiva a izquierda, esto es: $x(yz) = y(xz)$ y $x(yz) = (xy)(xz)$ respectivamente.

1.5.4. La diferencia y la implicación recíproca

Las condiciones:

Para todo x, y en 0, 1 se cumple que

A4. $xx = yy$ (Unipotencia)

A6. $xy = x$ con $x \neq y$.

determinan la estructura de las operaciones *diferencia* $-\bullet$*, e implicación recíproca* $\leftarrow$, y las únicas propiedades de las enunciadas que cumplen son permutabilidad a derecha y autodistributiva a derecha, esto es: $(xy)z = (xz)y$ y $(xy)z = (xz)(yz)$ respectivamente.

1.5.5. La tautología y la contradicción

Las condiciones:

Para todo x, y en $\{0, 1\}$ se cumple que

A4. $xx = yy$ (Unipotencia)

A7. $xy = yx = xx$

Determinan las operaciones $\bot$, $\top$, que forman un semigrupo conmutativo.

1.5.6. La equivalencia y la disyunción exclusiva

Las condiciones:

Para todo x, y en $\{0, 1\}$ se cumple que

A4. $xx = yy$ (Unipotencia)

A8. $xy = yx \neq xx$

determinan los grupos abelianos $\leftrightarrow$, $\veebar$, que cumplen además la propiedad elástica, consecuencia de la conmutativa; las asociativas cíclicas I y II, las identidades de Abel–Graßmann I y II, la permutabilidad a izquierda y a derecha, la propiedad del producto reducido y la bisimetría, que son consecuencias inmediatas de la asociatividad y de la propiedad conmutativa.

Ejercicios

1. *Demuestre la propiedad asociativa de las operaciones* $\leftrightarrow$ *y* $\veebar$ *a partir de los axiomas* A4 *y* A8.

2. *Demuestre que estas dos operaciones también cumplen las siguientes propiedades:*

   xvii. Semisimétrica a izquierda: $x\,(yx) = y$

   xviii. Semisimétrica a derecha: $(xy)\,x = y$

   xix. Identidad de Schwitzer a izquierda: $(xy)\,(xz) = zy$

   xx. Identidad de Schwitzer a derecha: $(xy)\,(zy) = zx$

   xxi. Identidad de Tarski: $x(y\,(zx)) = zy$

   xxii. Transitividad a izquierda: $(xy)\,(xz) = yz$

   xxiii. Transitividad a derecha: $(xy)\,(zy) = xz$

   xxiv. Transitividad media: $(xy)\,(yz) = xz$

   xxv. Identidad de Neumann: $x\,((yz)\,(yx)) = z$

3. *Demuestre que la implicación y la diferencia recíproca son permutables a izquierda y auto distributivas a izquierda, con base en los axiomas* A4. *y* A5.

4. *Demuestre que la diferencia y la implicación recíproca satisfacen la permutabilidad a derecha y la auto distributividad a derecha, utilizando solo los axiomas* A4. *y* A6. *Demuestre que la tautología y la contradicción forman un semigrupo conmutativo, basándose en* A4. *y* A7.

1.5.7. La primera proyección

La condición:

Para todo x, y en $\{0, 1\}$ se cumple que

A9. $xy = x$

determina la operación π_1 que forma con el conjunto un semigrupo, y además cumple las propiedades idempotente, elástica, I y II de Schröder[26], permutable a derecha, la del producto reducido, la transitiva a derecha y media, la autodistributiva izquierda, derecha, la izquierda abeliana y la bisimétrica.

1.5.8. La segunda proyección

La condición:

Para todo x, y en $\{0, 1\}$ se cumple que

A10. $xy = y$

determina la operación π_2 que forma con el conjunto un semigrupo, y además cumple las propiedades idempotente, elástica, de Abel Graßman II, permutable a izquierda, la del producto reducido, la transitiva a izquierda, la autodistributiva izquierda, derecha, la derecha abeliana y la bisimétrica. Además π_2 y π_1 distribuyen cada una con respecto a la otra.

1.5.9. La negación de la primera proyección

Las condiciones A3 y A10 determinan la operación $\otimes$ que es permutable a derecha, autodistributiva a derecha y bisimétrica y es distributiva a izquierda con respecto a $*$.

1.5.10. La negación de la segunda proyección

Las condiciones A3 y A9 determinan la operación $*$ que cumple la identidad II de Schröder, es permutable a izquierda, autodistributiva a izquierda y bisimétrica.

[26]La identidad de Schröder II es: $(xy)(yx) = x$.

1.6. Relaciones entre las operaciones: una estructura formada con estructuras

1.6.1. Las funciones R y T

Estudiemos ahora algunas relaciones entre las tablas obtenidas según el número de ceros y unos que hay en cada una[27]:

Nº de tablas	Nº de unos	Nº de ceros
1	4	0
1	0	4
4	1	3
4	3	1
6	2	2

Tabla 38

En las 4 tablas que tienen tres ceros y un uno:

$\wedge$	0	1
0	0	0
1	0	1

Tabla 20

$-\bullet$	0	1
0	0	0
1	1	0

Tabla 28

$\downarrow$	0	1
0	1	0
1	0	0

Tabla 27

$\bullet-$	0	1
0	0	1
1	0	0

Tabla 29

vemos que a partir de la conjunción y haciendo una semejanza con las rotaciones en el plano, la tabla del conectivo $(-\bullet)$ se obtiene *rotando* 90º grados alrededor de un punto en el centro de la tabla en el *sentido de las manecillas del reloj* las entradas de la tabla 20; la tabla de $\downarrow$ resulta de una *rotación* de 180º en el mismo sentido de las manecillas del reloj y la tabla del $(\bullet-)$ se consigue a partir de una rotación de 270º en el sentido de las manecillas del reloj; y si se realiza una rotación de 360º en el sentido de las manecillas del reloj, obtendremos la misma tabla de la conjunción; y si notamos con ⓒ a una de las cuatro operaciones consideradas, este paso de una tabla a la otra se consigue con el procedimiento

$$(\neg y)\,ⓒ\,x$$

que notaremos como $x\,(\mathrm{R}\,ⓒ\,)\,y$, es decir que para todo elemento x, y en $\{0, 1\}$,

$$x\,(\mathrm{R}\,ⓒ\,)\,y = (\neg y)\,ⓒ\,x.$$

[27]Si las filas de la tabla 38 se ordena así: 4-0, 3-1, 2-2, 1-3, 0-4 entonces en la primera columna aparecen los coeficientes binomiales 1-4-6-4-1.

De lo dicho, inferimos que si aplicamos cuatro veces R a la operación ⓒ, obtenemos de nuevo la operación ⓒ.

Si notamos I a la función que asigna a cada par de elementos x, y en $\{0,1\}$ de la tabla ⓒ el elemento $x\,ⓒ\,y$, tenemos que:

$$\mathrm{R}^4 = \mathrm{I}.$$

La función R también satisface la igualdad:

$$\mathrm{IR} = \mathrm{RI} = \mathrm{R}$$

lo que se interpreta como: aplicar a ⓒ, primero I y luego R o, primero R y luego I.

También podemos partir de la conjunción y obtener la tabla de la operación $(\bullet -)$ mediante una *rotación de 90º grados en sentido contrario de las manecillas del reloj*; la tabla del $\downarrow$ mediante una *rotación* de 180º en sentido contrario a las manecillas del reloj y la tabla del $(-\bullet)$, haciendo una rotación de 270º en sentido contrario a las manecillas del reloj y si nuevamente se realiza una rotación de 360º en sentido contrario de las manecillas del reloj, obtendremos la misma tabla de la conjunción; este mecanismo que notaremos $x\,(\mathrm{T}\,ⓒ\,)y$ es el mismo definido por

$$x\,(\mathrm{T}\,ⓒ\,)y = y\,ⓒ\,(\neg x)$$

y por supuesto que si aplicamos cuatro veces T a la operación ⓒ, obtenemos la operación ⓒ. Esto también lo podemos reescribir como:

$$\mathrm{T}^4 = \mathrm{I}.$$

La función T también satisface la igualdad:

$$\mathrm{IT} = \mathrm{TI} = \mathrm{T}.$$

Si consideramos las operaciones que tienen tres unos y un cero:

$\vee$	0	1
0	0	1
1	1	1

Tabla 21

$\leftarrow$	0	1
0	1	0
1	1	1

Tabla 26

$\mid$	0	1
0	1	1
1	1	0

Tabla 24

$\rightarrow$	0	1
0	1	1
1	0	1

Tabla 25

Notamos que estas se consiguen unas de otras usando el mismo procedimiento anterior.

Ahora estudiemos las tablas que tienen dos ceros y dos unos; si iniciamos con la disyunción exclusiva y le aplicamos la función R o la función T obtenemos la equivalencia y viceversa, si iniciamos con la equivalencia y le aplicamos la función R o la función T obtenemos disyunción exclusiva,

$\veebar$	0	1
0	0	1
1	1	0

$\leftrightarrow$	0	1
0	1	0
1	0	1

pero en este caso solo obtenemos dos operaciones, no cuatro como en el caso anterior.

Y si aplicamos el procedimiento a las 4 tablas en que los dos 1 están en una misma columna o en una misma fila:

π_1	0	1
0	0	0
1	1	1

Tabla 31

$*$	0	1
0	1	0
1	1	0

Tabla 32

$\otimes$	0	1
0	1	1
1	0	0

Tabla 33

π_2	0	1
0	0	1
1	0	1

Tabla 34

de nuevo se obtiene una de la anterior mediante la función R o la función T, dependiendo del sentido de los giros.

1.6.2. Las funciones N y H

Solo quedan por estudiar las tablas con cuatro unos y con cuatro ceros, que corresponden a:

$\top$	0	1
0	1	1
1	1	1

$\bot$	0	1
0	0	0
1	0	0

Estas tablas no las podemos obtener una de la otra por rotaciones, pero sí al cambiar los 1 por 0 y los 0 por 1, lo que corresponde al primer mecanismo que definimos para obtener nuevas operaciones, esto es $\neg((\neg x)\,©\,(\neg y))$, que aquí notaremos H©, es decir:

$$x(\mathrm{H}\,©\,)y = \neg((\neg x)\,©\,(\neg y));$$

sin embargo, para el caso de la tautología y de la contradicción, este procedimiento equivale a $\neg(x \copyright y)$, al que notaremos aquí con N; esto es $x\,(\mathrm{N}\copyright)y = \neg(x \copyright y)$; con ello vemos que

$$x\,(\mathrm{N}\top)y = \neg(x\top y) = x\bot y$$

y

$$x(\mathrm{N}\,\bot)y = \neg(x\bot y) = x\top y.$$

En otros términos,

$$\mathrm{N}\top = \bot$$

y si reiteramos N notamos que

$$\mathrm{N}(\mathrm{N}\top) = \top$$

$$\mathrm{N}(\mathrm{N}\bot) = \bot$$

y como en ambos casos por reiteración obtenemos el resultado inicial, tenemos que

$$\mathrm{N}^2 = \mathrm{NN} = \mathrm{I}.$$

Con las funciones R, N e I, hemos obtenido 16 operaciones (que son todas las posibles con dos elementos) a partir de la conjunción, la disyunción, la equivalencia y la tabla donde los cuatro valores son 1.

Y como la disyunción podemos obtenerla de la conjunción usando el procedimiento H©, concluimos que con las funciones R, H, N e I, podemos obtener todas las operaciones a partir de la conjunción, la equivalencia y la tautología.

Ahora, aplicando N a la conjunción obtenemos la barra de Sheffer y a esta, la conjunción, veamos algunos ejemplos[28]

$$\mathrm{N}\wedge = |$$
$$\mathrm{N}| = \wedge$$
$$\mathrm{N}\leftrightarrow = \veebar$$
$$\mathrm{N}\veebar = \leftrightarrow$$

[28] $\mathrm{N}\wedge = |$, indica que $x(\mathrm{N}\wedge)y = \neg(x \wedge y) = x|y$, de manera similar se deben entender $\mathrm{N}|$, $\mathrm{N}\leftrightarrow$ y $\mathrm{N}\veebar$; esto es fácilmente verificable observando la tercera fila de la tabla 37. Análogamente, en adelante, se debe entender para representaciones equivalentes usadas para otras funciones.

y aplicando nuevamente N:

$$\begin{aligned} \mathrm{N}(\mathrm{N}\wedge) &= \wedge \\ \mathrm{N}(\mathrm{N}|) &= | \\ \mathrm{N}(\mathrm{N}\leftrightarrow) &= \leftrightarrow \\ \mathrm{N}(\mathrm{N}\veebar) &= \veebar \end{aligned}$$

Como era de esperarse, de acuerdo a lo establecido antes.

1.6.3. Las funciones S y C

Surge ahora la inquietud sobre si estas son las únicas funciones y las únicas operaciones que permiten obtener a todas las demás, o podemos cambiar las funciones o reducir el número de operaciones de inicio.

Para resolver el primer punto, cambiemos el punto de vista y agrupemos las tablas comparando sus diagonales; por ejemplo si tienen el mismo elemento en una diagonal y en la otra diferente, como en:

$\wedge$	0	1
0	0	0
1	0	1

Tabla 20

$\downarrow$	0	1
0	1	0
1	0	0

Tabla 27

$\vee$	0	1
0	0	1
1	1	1

Tabla 21

$\|$	0	1
0	1	1
1	1	0

Tabla 24

Vemos que la tabla del $\wedge$ y de $\downarrow$ tienen la misma diagonal secundaria y tiene invertidos los valores de la diagonal principal. Estas dos tablas las podemos obtener una a partir de la otra aplicando el procedimiento $(\neg y)\,©\,(\neg x)$ que notaremos como $x\,(\mathrm{S}©\,)y$; así:

$$x\,(\mathrm{S}\wedge)y = x \downarrow y$$

$$x\,(\mathrm{S}\downarrow)y = x \wedge y$$

de nuevo obtenemos que

$$\mathrm{S}^2 = \mathrm{I} \qquad \text{y} \qquad \mathrm{IS} = \mathrm{SI} = \mathrm{S}.$$

Las tablas del $\vee$ y del $|$ también se obtienen una de la otra mediante la función S.

Y si comparamos las que tienen la misma diagonal principal y tiene invertidos los valores de la diagonal secundaria, como en:

$-\bullet$	0	1
0	0	0
1	1	0

Tabla 28

$\bullet-$	0	1
0	0	1
1	0	0

Tabla 29

$\leftarrow$	0	1
0	1	0
1	1	1

Tabla 26

$\rightarrow$	0	1
0	1	1
1	0	1

Tabla 25

podemos obtener una a partir de la otra en cada pareja horizontal, aplicándole el procedimiento[29] $y \copyright x$ que notaremos como $x\,(\mathrm{C}\copyright)y$, o sea:

$$x\,(\mathrm{C}-\bullet)y = x \bullet -y$$
$$x\,(\mathrm{C}\bullet -)y = x - \bullet y$$

y

$$x\,(\mathrm{C}\rightarrow)y = x \leftarrow y$$
$$x\,(\mathrm{C}\leftarrow)y = x \rightarrow y.$$

Este resultado nos indica que

$$\mathrm{C}^2 = \mathrm{I}$$

y que también

$$\mathrm{IC} = \mathrm{CI} = \mathrm{C}.$$

Hemos obtenido 7 funciones: I, R, T, N, H, S y C que transforman unas tablas en otras, por lo que nos preguntamos ¿es posible elegir algunas de esas funciones y por composición de ellas obtener todas las demás?

[29]Este procedimiento es usado por OOSTRA, Arnold. Huellas en los encuentros de Geometría y Aritmética. Bogotá: Universidad Pedagógica Nacional, 2005. p. 233-268.

Iniciemos haciendo la composición de R con R, que notaremos R^2; esto es:

$$x\,(\mathrm{R}^2 \copyright)y = x\,(\mathrm{R}(\mathrm{R} \copyright))y = (\neg y)(\mathrm{R} \copyright)x = (\neg x) \copyright (\neg y).$$

Con el ánimo de elegir a R como una posible función a partir de la cual podemos obtener las demás funciones, compongamos R con N; así:

$$x(\mathrm{R}(\mathrm{N} \copyright))y = (\neg y)(\mathrm{N} \copyright)x = \neg(\neg y \copyright x)$$

Notemos que cuando simbolizamos $x\,(\mathrm{R}(\mathrm{N} \copyright))\,y$, primero efectuamos R y luego N, a esto lo expresamos RN.

Es decir que partiendo de R y N, hemos obtenido dos funciones que antes no teníamos; un cuadro como el siguiente nos puede ayudar para determinar cuáles funciones podemos elegir para hallar las demás:

∘	I	R	T	N	H	S	C
I	I	R	T	N	H	S	C
R	R	$(\neg x) \copyright (\neg y)$	I	$\neg((\neg y) \copyright x)$	$\neg(y \copyright (\neg x))$	$\neg x \copyright y$	$x \copyright (\neg y)$
T	T	I	$(\neg x) \copyright (\neg y)$	$\neg(y \copyright (\neg x))$	$\neg((\neg y) \copyright x)$	$x \copyright (\neg y)$	$(\neg x) \copyright y$
N	N	$\neg((\neg y) \copyright x)$	$\neg((\neg y) \copyright x)$	I	$(\neg x) \copyright (\neg y)$	$\neg((\neg y) \copyright (\neg x))$	$\neg(y \copyright x)$
H	H	$\neg(y \copyright (\neg x))$	$\neg((\neg y) \copyright x)$	$(\neg x) \copyright (\neg y)$	I	$\neg(y \copyright x)$	$\neg((\neg y) \copyright (\neg x))$
S	S	$x \copyright (\neg y)$	$(\neg x) \copyright y$	$\neg((\neg y) \copyright (\neg x))$	$\neg(y \copyright x)$	I	$(\neg x) \copyright (\neg y)$
C	C	$\neg x \copyright y$	$x \copyright (\neg y)$	$\neg(y \copyright x)$	$\neg((\neg y) \copyright (\neg x))$	$(\neg x) \copyright (\neg y)$	I

Tabla 39

En estos resultados hemos encontrado algunas funciones, pero faltan otras, como $\neg(x \copyright (\neg y))$ o $\neg((\neg x) \copyright y)$, por lo que debemos intentar otras combinaciones; por ejemplo, si efectuamos:

$$x\,(\mathrm{N}(\mathrm{C}(\mathrm{R} \copyright)))y = \neg(x(\mathrm{C}(\mathrm{R} \copyright))y) = \neg(y(\mathrm{R} \copyright)x) = \neg((\neg x) \copyright y)$$

llegamos a una función que no aparece en el cuadro.

También podemos hacer composición entre funciones ya obtenidas:

$$x\,(\mathrm{S}(\mathrm{T}^2 \copyright))y = (\neg y)(\mathrm{T}^2 \copyright)(\neg x) = y \copyright x.$$

Esto quiere decir que tenemos múltiples posibilidades de combinación; haciendo algunos cálculos como los mencionados aquí, hallamos funciones que, haciendo composición entre ellas, nos permiten obtener las demás; algunos de los resultados encontrados los resumimos en el siguiente cuadro, en la primera columna listamos las 16 funciones posibles, en la parte superior de la tabla las funciones elegidas y al interior, la manera cómo se obtienen las funciones de la primera columna:

	N, R, C	H, S, T	H, N, R, S	H, R, C
$x \copyright y$	N^2	$H^2 = S^2$	$H^2 = S^2 = N^2$	$H^2 = C^2$
$\neg((\neg x) \copyright (\neg y))$	NR^2	H	H	H
$\neg(x \copyright y)$	N	HT^2	HR^2	HR^2
$\neg(x \copyright (\neg y))$	NCR^3	HST	SNR	HCR
$\neg((\neg x) \copyright y)$	NCR	HST^3	SNR^3	HRC
$(\neg x) \copyright (\neg y)$	R^2	T^2	R^2	R^2
$x \copyright (\neg y)$	RC	TS	SR	CR^3
$(\neg x) \copyright y$	CR	ST	RS	CR
$y \copyright x$	C	ST^2	SR^2	C
$\neg((\neg y) \copyright (\neg x))$	NCR^2	HST^2	SN	HC
$\neg(y \copyright x)$	NC	HS	SNR^2	HCR^2
$\neg(y \copyright (\neg x))$	NR^3	HT^3	HR	HR
$\neg((\neg y) \copyright x)$	NR	HT	HR^3	HR^3
$(\neg y) \copyright (\neg x)$	CR^2	S	S	CR^2
$y \copyright (\neg x)$	R^3	T	R^3	R^3
$(\neg y) \copyright x$	R	T^3	R	R

Tabla 40

Ejercicio

Encuentre otros conjuntos de funciones que generen las demás.

1.7. Una aplicación: Z_2 y la lógica

Hemos visto que dentro del estudio de las representaciones de $(Z_2, +, \times)$ como campo aparecen elementos que permiten construir otras operaciones y relaciones entre ellas, estas operaciones las podemos enmarcar dentro de la *lógica proposicional* que estudia las formas válidas del razonamiento matemático.

Si interpretamos el 1 como el valor de verdad *verdadero* de una proposición, el 0 como el valor de verdad falso y *la igualdad como equivalencia lógica*, de cada una de las igualdades anteriores obtenemos afirmaciones lógicas que son válidas sin importar el valor de verdad de las proposiciones componentes; estas afirmaciones se llaman *tautologías*. Veamos algunos ejemplos.

1.7.1. Las leyes de De Morgan

En la tabla 37 encontramos que

$$x \leftrightarrow y = \neg(\neg x \veebar \neg y)$$
$$x \vee y = \neg(\neg x \wedge \neg y)$$
$$\neg(\neg x \leftrightarrow \neg y) = x \veebar y$$
$$\neg(\neg x \vee \neg y) = x \wedge y$$

estas igualdades se convierten en las tautologías:

$$(p \leftrightarrow q) \leftrightarrow \neg((\neg p) \veebar (\neg q))$$
$$(p \vee q) \leftrightarrow \neg((\neg p) \wedge (\neg q))$$
$$\neg((\neg p) \leftrightarrow (\neg q)) \leftrightarrow (p \veebar q)$$
$$\neg((\neg p) \vee (\neg q)) \leftrightarrow (p \wedge q)$$

y teniendo en cuenta que

$$(\neg(\neg p)) \leftrightarrow p$$

estas cuatro igualdades las podemos escribir así:

$$((\neg p) \veebar (\neg q)) \leftrightarrow (\neg(p \leftrightarrow q)) \quad (1)$$
$$((\neg p) \wedge (\neg q)) \leftrightarrow (\neg(p \vee q)) \quad (2)$$
$$((\neg p) \leftrightarrow (\neg q)) \leftrightarrow (\neg(p \veebar q)) \quad (3)$$
$$((\neg p) \vee (\neg q)) \leftrightarrow (\neg(p \wedge q)) \quad (4)$$

Con el mismo argumento tenemos otras leyes análogas a las de De Morgan para cada una de las operaciones lógicas que son isomorfas, es decir las que están relacionadas mediante la función H:

$$x(\mathrm{H}\,©\,)y = \neg[(\neg x)\,©\,(\neg y)].$$

Por ejemplo,

$$x(\mathrm{H}\downarrow)y = \neg[(\neg x) \downarrow (\neg y)]$$

nos conduce a la equivalencia

$$(\neg(p|q)) \leftrightarrow ((\neg p) \downarrow (\neg q))$$

y análogamente,

$$(\neg(p \downarrow q)) \leftrightarrow ((\neg p)|(\neg q)).$$

Una de las maneras habituales de demostrar que estas equivalencias lógicas son válidas es usando una tabla de verdad[30], donde se ubican todas las posibles combinaciones de los valores de verdad de las proposiciones componentes y si el resultado total es verdadero en todos los casos para cualquier posible valor de p y q, la proposición compuesta es una tautología. Por ejemplo:

$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q.$$

Se demuestra con la tabla:

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\leftrightarrow$	$\neg p \vee \neg q$
1	1	1	0	1	0
1	0	0	1	1	1
0	1	0	1	1	1
0	0	0	1	1	1

Tabla 41

1.7.2. Las leyes algebraicas

1.7.2.1. Las propiedades de campo

Dado que $(\{\underline{2}\}, \veebar, \vee)$ es campo[31], tenemos que en 2, la disyunción exclusiva es asociativa, tiene elemento neutro 0, tiene elemento inverso para cada elemento y es conmutativa; y la conjunción, también es asociativa, conmutativa, tiene elemento neutro y distribuye respecto a la disyunción exclusiva. En símbolos, si p, q y r son elementos de $2 = \{0, 1\}$ se tiene que:

1. $p \veebar (q \veebar r) = (p \veebar q) \veebar r$
2. $p \veebar 0 = p$
3. $p \veebar (-p) = 0$
4. $p \veebar q = q \veebar p$

[30]La idea de este procedimiento aparece en Peirce en 1885 y luego fue perfeccionado por Post y Wittegstein en 1920. (ZALAMEA, Fernando. Una jabalina lanzada hacia el futuro: anticipos y aportes de C. S. Peirce a la lógica matemática del siglo XX. En : Mathesis 9. (1993). p. 391 - 404).

[31]En 1847 George Boole inicia el *álgebra de la lógica*, que se considera inicio de la lógica matemática, como disciplina independiente. Aplicó en la lógica, los métodos de la matemática, basado en el empleo de un lenguaje especial de símbolos y fórmulas.

5. $p \wedge (q \wedge r) = (p \wedge q) \wedge r$
6. $p \wedge q = q \wedge p$
7. $p \wedge 1 = p$
8. $p \wedge (q \veebar r) = (p \wedge q) \veebar (p \wedge r)$

donde el inverso aditivo[32] de p (notado como $-p$) es p, luego:

$$p \veebar p = 0.$$

Nuevamente, en la lógica proposicional, estas igualdades nos reportan tautologías, cambiando la igualdad por la equivalencia lógica:

$$(p \veebar (q \veebar r)) \leftrightarrow ((p \veebar q) \veebar r) \tag{5}$$
$$(p \veebar q) \leftrightarrow (q \veebar p) \tag{6}$$
$$(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r) \tag{7}$$
$$(p \wedge q) \leftrightarrow (q \wedge p) \tag{8}$$
$$(p \wedge (q \veebar r)) \leftrightarrow ((p \wedge q) \veebar (p \wedge r)). \tag{9}$$

La equivalencia

$$(p \veebar (-p)) \leftrightarrow 0$$

afirma que

$$p \veebar (-p)$$

es en todos los casos falso, y como $-p = p$, esto significa que

$$\neg(p \veebar p) \tag{10}$$

es una tautología.

Ejercicio

Proponga una interpretación para las equivalencias

$$(p \wedge 1) \leftrightarrow p \tag{11}$$
$$(p \veebar 0) \leftrightarrow p \tag{12}$$

[32]El inverso aditivo $-p$ de p no coincide con $\neg p$, la negación de p.

De manera análoga, como $(2, \leftrightarrow, \vee)$ es un campo, obtenemos que si p, q y r son elementos de $\underline{2} = \{0, 1\}$ entonces en la lógica proposicional, las siguientes expresiones son tautologías:

$$(p \leftrightarrow (q \leftrightarrow r)) \leftrightarrow ((p \leftrightarrow q) \leftrightarrow r) \tag{13}$$
$$(p \leftrightarrow 1) \leftrightarrow p \tag{14}$$
$$(p \leftrightarrow (-p)) \leftrightarrow 1 \tag{15}$$
$$(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p) \tag{16}$$
$$(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r) \tag{17}$$
$$(p \vee q) \leftrightarrow (q \vee p) \tag{18}$$
$$(p \vee 0) \leftrightarrow p \tag{19}$$
$$(p \vee (q \leftrightarrow r)) \leftrightarrow ((p \vee q) \leftrightarrow (p \vee r)) \tag{20}$$
$$(p \wedge (q \veebar r)) \leftrightarrow ((p \wedge q) \veebar (p \wedge r)) \tag{21}$$
$$(p \vee (q \leftrightarrow r)) \leftrightarrow ((p \vee q) \leftrightarrow (p \vee r)) \tag{22}$$

Además de que $(\underline{2}, \leftrightarrow, \vee)$ y $(\underline{2}, \veebar, \wedge)$ sean campos, también tienen otras propiedades que en general no se cumplen en otros campos, por ejemplo en los campos numéricos $(\mathrm{Q}, +, \times)$, $(\mathrm{R}, +, \times)$ y $(C, +, \times)$ un ejemplo de ello son las siguientes leyes.

1.7.2.2. Leyes de idempotencia

En la caracterización de las estructuras por sus propiedades encontramos que la conjunción, la disyunción y las dos proyecciones son las únicas operaciones con dos elementos que son idempotentes, es decir que para todo p en $\{0, 1\}$ obtenemos:

$$(p \wedge p) \leftrightarrow p \tag{23}$$
$$(p \vee p) \leftrightarrow p \tag{24}$$

Las propiedades que hemos presentado son derivadas de la estructura del campo de $\underline{2}$ con sus operaciones respectivas; pero además, entre la disyunción y la conjunción, aparecen otras relaciones, por ejemplo:

1.7.2.3. Leyes distributivas de $\wedge$ y $\vee$

Para todo p, q, r en $\{0, 1\}$

$$(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r)) \tag{25}$$
$$(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r)) \tag{26}$$

1.7.2.4. Leyes absorbentes de $\wedge$ y $\vee$

Para todo p, q, r en $\{0, 1\}$

$$(p \wedge (p \vee q)) \leftrightarrow p \tag{27}$$
$$(p \vee (p \wedge q)) \leftrightarrow p \tag{28}$$

1.7.2.5. Complementos: leyes de contradicción y tercero excluido

Si miramos la fila 7 de la tabla 37 en su columna 1 dice que $(x \wedge \neg y) = x - \bullet y$, de donde

$$(p \wedge \neg q) \leftrightarrow (p - \bullet q).$$

Si elegimos $p = q$ y observamos la tabla de $-\bullet$, tenemos que $(p - \bullet p) \leftrightarrow 0$ y por lo tanto $\neg(p - \bullet p) \leftrightarrow 1$, lo que significa que

$$\neg(p \wedge \neg p) \tag{29}$$

es una tautología, conocida como el *principio de contradicción*[33].

Si aplicamos una de las leyes de De Morgan a este resultado, obtenemos que *el principio del tercero excluido:*

$$p \vee \neg p \tag{30}$$

es también una tautología.

Además, cada elemento tiene un único *complemento*, en el sentido de que para cada p en $\underline{2}$:

$$p \vee \neg p = 1 \tag{31}$$
$$p \wedge \neg p = 0 \tag{32}$$

El conjunto $\{0, 1\}$ con las operaciones $\vee$, $\wedge$, tienen una estructura conocida como *álgebra de Boole*[34].

Ejercicio

La equivalencia y la disyunción exclusiva forman una pareja donde cada una es una copia de la otra. ¿Son distributivas una respecto de la otra? ¿Deberían serlo? Justifique.

[33]ZEHNA, Peter y JOHNSON, Robert. Elements of set theory. Boston: Allyn and Bacon, 1972. p.13.

[34]BRAUNSS, Günter & ZUBROD, Heinz. Einführung in die Booleschen Algebren. Frankfurt am Main: Akademische Verlagsgesellschaft, 1974. p.19.

1.7.3. Las leyes lógicas

En el álgebra de los conjuntos numéricos habituales la igualdad juega un papel preponderante, pues las ecuaciones forman parte importante de su trabajo, en lógica este papel lo asume la implicación, en ella se estudian las consecuencias lógicas de las afirmaciones hechas, y esto en general se expresa en términos de implicaciones, por ello estudiaremos inicialmente algunas relaciones de la implicación con otras operaciones lógicas.

1.7.3.1. La implicación

La operación $x \to y = \neg(x \wedge (\neg y))$ podemos escribirla como sigue, de acuerdo con la tabla 37:

$$\begin{aligned} x \to y &= \neg x \vee y \\ &= \neg(x - \bullet y) \\ &= \neg(y \bullet - x) \\ &= (\neg x) \leftarrow (\neg y)) \\ &= x|(\neg y) \\ &= y \leftarrow x \\ &= \neg(y \downarrow (\neg x)) \end{aligned}$$

o en términos de ella misma[35] como

$$x \to y = (\neg y) \to (\neg x)$$

corresponde en la lógica bivalente usual a la *implicación* y es la que utilizamos para efectuar razonamientos lógicos válidos; su tabla:

$\to$	0	1
0	1	1
1	0	1

Tabla 25

muestra que aunque no hay un elemento idéntico, sí hay un elemento, el 1, que actúa como un elemento idéntico a izquierda, es decir que

$$1 \to x = x.$$

[35]La tautología: $(p \to q) \leftrightarrow ((\neg q) \to (\neg p))$ es conocida como *ley de contrapositiva*. Y en la forma parcial $((\neg q) \to (\neg p)) \to (p \to q)$ es tomado por Russell como un axioma de la lógica proposicional.

Además no es conmutativa ni asociativa, pues:

$$(0 \to 1) \to 0 \neq 0 \to (1 \to 0).$$

Aunque pareciera que la implicación no cumple propiedad algebraica alguna, ya mencionamos que es unipotente, o sea que para todo x, y en $\{0, 1\}$ se cumple que

$$x \to x = y \to y$$

y también cumple que es permutable a izquierda:

$$x \to (y \to z) = y \to (x \to z)$$

y auto distributiva a izquierda[36], esto es

$$x \to (y \to z) = (x \to y) \to (x \to z).$$

Como en los casos anteriores, cada igualdad nos reporta una tautología sustituyendo la igualdad por la equivalencia lógica, por ejemplo:

$$(p \to q) \leftrightarrow ((\neg p) \vee q) \tag{33}$$
$$(p \to q) \leftrightarrow (\neg(p \wedge (\neg q))) \tag{34}$$
$$(p \vee q) \leftrightarrow (\neg p \to q) \tag{35}$$
$$(p \wedge q) \leftrightarrow (\neg(p \to (\neg q))) \tag{36}$$
$$(p \to q) \leftrightarrow ((\neg q) \to (\neg p)) \tag{37}$$
$$[p \to (q \to r)] \to [(p \to q) \to (p \to r)] \tag{38}$$

donde p y q representan los valores de verdad de dos proposiciones cualesquiera.

Además la implicación satisface la identidad $(xy)x = x$ que llamaremos *identidad de Peirce* y corresponde a la tautología $((p \to q) \to p) \to p$ conocida como *ley de Peirce*.

1.7.3.2. Negación de la implicación

La equivalencia (34) también puede escribirse como

$$\neg(p \to q) \leftrightarrow (p \wedge (\neg q)) \tag{39}$$

[36]La tautología correspondiente a esta propiedad cuando se considera una sola implicación $[p \to (q \to r)] \to [(p \to q) \to (p \to r)]$ es tomada como uno de los axiomas de la lógica proposicional. (CAICEDO, Xavier. Elementos de lógica y calculabilidad. Bogotá: Una Empresa Docente, Universidad de los Andes, 1990. p. 38).

1.7.3.3. Combinación de la implicación con otras

Para encontrar algunas relaciones entre la implicación y otras operaciones iniciemos con las propiedades ya anotadas:

$$(p \to 1) \leftrightarrow p$$

$$(p \to p) \leftrightarrow 1$$

y usemos la equivalencia (33) para calcular

$$\begin{aligned}(p \to 0) &\leftrightarrow (\neg p \vee 0)\\ &\leftrightarrow (\neg p)\end{aligned}$$

lo que significa que tenemos otra propiedad conocida:

1.7.3.3.1. Ley del absurdo

$$(p \to 0) \to \neg p \tag{40}$$

o sea que si una proposición p implica una proposición falsa, y el valor de la implicación es verdadero, entonces podemos concluir $\neg p$, este resultado es muy usado para hacer demostraciones de teoremas en matemáticas.

1.7.3.3.2. Con la conjunción

Ensayemos ahora varias formas de combinar la implicación con la conjunción, por ejemplo

$$(p \wedge (p \to q))$$

y usemos la equivalencia (33) para transformar la expresión,

$$\begin{aligned}(p \wedge (p \to q)) &\leftrightarrow (p \wedge (\neg p \vee q)) && \text{Por la equivalencia (33)}\\ &\leftrightarrow ((p \wedge (\neg p)) \vee (p \wedge q)) && \text{Por la equivalencia (25)}\\ &\leftrightarrow (0 \vee (p \wedge q)) && \text{Por la equivalencia (32)}\\ &\leftrightarrow (p \wedge q) && \text{Por la equivalencia (19)}\end{aligned}$$

es decir,

$$(p \wedge (p \to q)) \leftrightarrow (p \wedge q) \tag{41}$$

O podemos intercambiar la implicación y la conjunción en la fórmula anterior:

$$\begin{aligned}
(p \to (p \wedge q)) &\leftrightarrow (\neg p \vee (p \wedge q)) && \text{Por la equivalencia (33)}\\
&\leftrightarrow ((\neg p \vee p) \wedge (\neg p \vee q)) && \text{Por la equivalencia (26)}\\
&\leftrightarrow (1 \wedge (\neg p \vee q)) && \text{Por la equivalencia (31)}\\
&\leftrightarrow (\neg p \vee q) && \text{Por la equivalencia (11)}\\
&\leftrightarrow (p \to q) && \text{Por la equivalencia (33)}
\end{aligned}$$

Lo que significa que la siguiente fórmula es una tautología

$$(p \to (p \wedge q)) \leftrightarrow (p \to q) \tag{42}$$

Y si escribimos la pareja del paréntesis al comienzo

$$\begin{aligned}
((p \wedge q) \to p) &\leftrightarrow (\neg(p \wedge q) \vee p)\\
&\leftrightarrow ((\neg p \vee \neg q) \vee p)\\
&\leftrightarrow ((\neg p \vee p) \vee \neg q)\\
&\leftrightarrow (1 \vee \neg q)\\
&\leftrightarrow 1
\end{aligned}$$

lo que significa que

$$((p \wedge q) \to p) \tag{43}$$

es una tautología[37].

O con combinaciones más sofisticadas podemos obtener

1.7.3.3.3. La ley del modus ponendo ponens

Esta ley es fundamental en todos los razonamientos científicos, afirma que si suponemos verdadera una proposición p y $p \to q$ es verdadera, entonces q debe ser verdadera, de manera que la siguiente expresión es una tautología

$$[p \wedge (p \to q)] \to q \tag{44}$$

[37]Esta tautología junto con $((p \wedge q) \to q))$ son conocidas como *leyes de eliminación* y forman parte de los axiomas en algunas teorías de la lógica proposicional.

que podemos calcular partiendo de

$$\begin{aligned}([p \wedge (p \to q)] \to q) &\leftrightarrow (\neg[p \wedge (p \to q)] \vee q)\\ &\leftrightarrow ([\neg p \vee \neg(p \to q)] \vee q)\\ &\leftrightarrow ([\neg p \vee (p \wedge \neg q)] \vee q)\\ &\leftrightarrow ([(\neg p \vee p) \wedge (\neg p \vee \neg q)] \vee q)\\ &\leftrightarrow ([1 \wedge (\neg p \vee \neg q)] \vee q)\\ &\leftrightarrow ([(\neg p \vee \neg q)] \vee q)\\ &\leftrightarrow \neg p \vee [(\neg q) \vee q)]\\ &\leftrightarrow \neg p \vee 1\\ &\leftrightarrow 1\end{aligned}$$

O una variación de ella como

1.7.3.3.4. La ley del modus tollendo tollens

$$[(p \to q) \wedge \neg q] \to \neg p \tag{45}$$

Ejercicios

1. *Encuentre una expresión equivalente a* $(p \wedge (p \leftrightarrow q))$ *en términos de la conjunción y la negación.*

2. *Encuentre una expresión equivalente a* $(p \leftrightarrow (p \wedge q))$ *en términos de la disyunción y la negación.*

3. *Demuestre que* $([(p \to q) \wedge \neg q] \to \neg p) \leftrightarrow 1$.

1.7.3.3.5. Con la disyunción

Combinando la implicación con la disyunción obtenemos

$$\begin{aligned}(p \to (p \vee q)) &\leftrightarrow (\neg p \vee (p \vee q))\\ &\leftrightarrow ((\neg p \vee p) \vee q)\\ &\leftrightarrow (1 \vee q)\\ &\leftrightarrow 1\end{aligned}$$

lo que significa que

$$(p \to (p \vee q)) \tag{46}$$

es una tautología[38].

1.7.3.3.6. Con la flecha de Peirce

$$\begin{aligned}(p \to (p \downarrow q)) &\leftrightarrow (\neg p \vee (p \downarrow q)) \\ &\leftrightarrow (\neg p \vee \neg(p \vee q)) \\ &\leftrightarrow \neg((p \wedge (p \vee q)) \\ &\leftrightarrow \neg((p \wedge p) \vee (p \wedge q)) \\ &\leftrightarrow \neg((p \vee (p \wedge q)) \\ &\leftrightarrow (\neg p \wedge (p|q)).\end{aligned}$$

O sea que la siguiente fórmula es una tautología

$$(p \to (p \downarrow q)) \leftrightarrow (\neg p \wedge (p|q)) \tag{47}$$

Si en el tercer renglón aplicamos la propiedad absorbente obtenemos la siguiente tautología

$$(p \to (p \downarrow q)) \leftrightarrow (\neg p). \tag{48}$$

1.7.3.3.7. Con la implicación

Combinando la implicación con ella misma obtenemos

$$(p \to (p \to q)) \leftrightarrow (p \to q) \tag{49}$$

o en la forma

$$\begin{aligned}(p \to (q \to p)) &\leftrightarrow (\neg p \vee (q \to p)) \\ &\leftrightarrow ((\neg p) \vee (\neg q \vee p)) \\ &\leftrightarrow ((\neg p \vee p) \vee \neg q) \\ &\leftrightarrow (1 \vee \neg q) \\ &\leftrightarrow 1\end{aligned}$$

[38]Esta tautología junto con $(q \to (p \vee q)$ son conocidas como *leyes de agregación* y forman parte de los axiomas en algunas teorías de la lógica proposicional. Esta regla se puede derivar de la tabla de verdad de la disyunción, pues si tenemos una proposición p cierta, entonces la proposición resultante de adicionarle otra proposición q a p con la disyunción también es verdadera, y si p es falsa, la implicación es verdadera; es decir que $p \to (p \vee q)$ es verdadera, independiente del valor de verdad de p y de q.

lo que significa que

$$(p \to (q \to p)) \tag{50}$$

es una tautología[39].

1.7.3.3.8. Con otras operaciones

Aunque es menos frecuente, también podemos combinar la implicación con otras operaciones lógicas como

$$(p \to (p|q)) \leftrightarrow (p|q) \tag{51}$$
$$(p \to (q \leftrightarrow p)) \leftrightarrow (p \to q) \tag{52}$$
$$(p \to (q \veebar p)) \leftrightarrow (p|q) \tag{53}$$
$$(p \to (p \bullet -q)) \leftrightarrow (\neg p \wedge (p \to q)) \tag{54}$$
$$(p \to (p\, \pi_1\, q)) \leftrightarrow 1 \tag{55}$$
$$(p \to (p\, \pi\, _2 q)) \leftrightarrow (p \to q) \tag{56}$$

O poniendo las parejas entre paréntesis al comienzo,

$$((p|q) \to p) \leftrightarrow p \tag{57}$$
$$((p \vee q) \to p) \leftrightarrow (q \to p) \tag{58}$$
$$((p \downarrow q) \to p) \leftrightarrow (p \vee q) \tag{59}$$
$$(p \leftrightarrow q) \to p) \leftrightarrow (p \wedge q) \tag{60}$$
$$((p \to q) \to p) \leftrightarrow (p \wedge (q \to p)) \tag{61}$$
$$((q \to p) \to p) \leftrightarrow (q \vee p) \leftrightarrow ((p \to q) \to q) \tag{62}$$

Como vemos han aparecido relaciones que antes no habíamos establecido; en la tabla 37 las operaciones aparecen por grupos de cuatro o de dos, pero no se mezclaban por ejemplo la implicación con las proyecciones.

Una relación muy importante es la que vincula la implicación con la igualdad lógica (equivalencia) la obtenemos de combinar la conjunción con la implicación en la forma

$$((p \to q) \wedge (q \to p)) \leftrightarrow (p \leftrightarrow q) \tag{63}$$

y de la disyunción con la implicación obtenemos $((p \to q) \vee (q \to p)) \leftrightarrow (p \top q)$, lo que significa que

[39] Esta tautología también forma parte de los axiomas en algunas teorías de la lógica proposicional.

$$(p \to q) \vee (q \to p) \tag{64}$$

es una tautología.

La relación entre la equivalencia y la implicación sugiere considerar expresiones como

$$\begin{aligned}((p \wedge q) \to (q \wedge p)) &\leftrightarrow ((p \wedge q) \to (p \wedge q)) \\ &\leftrightarrow 1\end{aligned}$$

e intercambiando p y q, conseguimos la propiedad conmutativa de la conjunción.

De manera similar la propiedad conmutativa de la flecha

$$\begin{aligned}((p \downarrow q) \to (q \downarrow p)) &\leftrightarrow ((p \downarrow q) \to (p \downarrow q)) \\ &\leftrightarrow (\neg(p \downarrow q) \vee (p \downarrow q)) \\ &\leftrightarrow 1\end{aligned}$$

Esto significa que la siguiente fórmula es una tautología

$$((p \downarrow q) \to (q \downarrow p)). \tag{65}$$

Y también para la barra

$$\begin{aligned}((p|q) \to (q|p)) &\leftrightarrow ((p|q) \to (p|q)) \\ &\leftrightarrow (\neg(p|q) \vee (p|q)) \\ &\leftrightarrow 1\end{aligned}$$

En cada caso hemos reducido una equivalencia a una implicación, expresando propiedades como la conmutativa en términos de implicaciones.

Si ensayamos con operaciones no conmutativas, con la misma implicación obtenemos

$$\begin{aligned}((p \to q) \to (q \to p)) &\leftrightarrow (\neg(p \to q) \vee (q \to p)) \\ &\leftrightarrow (p \wedge \neg q) \vee (\neg q \vee p)) \\ &\leftrightarrow [(p \wedge \neg q) \vee (\neg q)] \vee p) \\ &\leftrightarrow [(p \vee \neg q) \wedge (\neg q \vee \neg q)] \vee p \\ &\leftrightarrow [(p \vee \neg q) \wedge (\neg q)] \vee p) \\ &\leftrightarrow (\neg q) \vee p \\ &\leftrightarrow (q \to p)\end{aligned}$$

O incluyendo una tercera variable

$$[(p \to q) \wedge (p \to r)] \leftrightarrow [p \to (q \wedge r)] \tag{66}$$

y de manera similar otras leyes lógicas como las leyes de transitividad, en particular,

1.7.3.3.9. Transitividad de la equivalencia lógica

$$[(p \leftrightarrow q) \wedge (q \leftrightarrow r)] \to (p \leftrightarrow r) \tag{67}$$

1.7.3.3.10. Transitividad de la implicación

$$[(p \to q) \wedge (q \to r)] \to (p \to r) \tag{68}$$

1.7.3.3.11. Otras reglas

En una implicación podemos operar en ambos lados con la conjunción o con la disyunción y obtenemos una implicación en el mismo sentido, esto es:

$$(p \to q) \to [(p \vee r) \to (q \vee r)] \tag{69}$$
$$(p \to q) \to [(p \wedge r) \to (q \wedge r)] \tag{70}$$

1.7.3.3.12. Dilemas constructivos

También podemos partir de dos implicaciones y obtener una nueva implicación con la disyunción (o la conjunción) de los antecedentes como antecedente y la disyunción (o la conjunción) de los consecuentes como consecuente,

$$[(p \to q) \wedge (r \to s)] \to [(p \vee r) \to (q \vee s)] \tag{71}$$
$$[(p \to q) \wedge (r \to s)] \to [(p \wedge r) \to (q \wedge s)] \tag{72}$$

Ejercicio

Demuestre las tautologías (66) a (72).

1.7.3.4. Otras combinaciones lógicas

Hasta aquí hemos encontrado relaciones entre la implicación y otras operaciones lógicas, estudiemos ahora relaciones entre las demás; para simplificar de nuevo hagamos combinaciones de la conjunción con las otras tales como

$$(p \wedge (q \copyright p))$$

donde © representa alguna de las 16 operaciones con dos elementos. Por ejemplo,

$$\begin{aligned} 1.(p \wedge (q \wedge p)) &\leftrightarrow (p \wedge (p \wedge q)) \\ &\leftrightarrow ((p \wedge p) \wedge q) \\ &\leftrightarrow (p \wedge q) \end{aligned}$$

$$\begin{aligned} 2.(p \wedge (q \vee p)) &\leftrightarrow (p \wedge (p \vee q) \\ &\leftrightarrow ((p \wedge p) \vee (p \wedge q)) \\ &\leftrightarrow (p \vee (p \wedge q)) \\ &\leftrightarrow p \\ &\leftrightarrow (p \, \pi_1 \, q). \end{aligned}$$

Esta es una de las leyes de absorción que mencionamos antes y una relación entre la conjunción, la disyunción y una proyección.

$$\begin{aligned} 3.(p \wedge (p \downarrow q)) &\leftrightarrow (p \wedge \neg(p \vee q)) \\ &\leftrightarrow (p \wedge (\neg p \wedge \neg q)) \\ &\leftrightarrow ((p \wedge (\neg p)) \wedge \neg q) \\ &\leftrightarrow (0 \wedge \neg q) \\ &\leftrightarrow 0 \\ &\leftrightarrow (p \bot q) \end{aligned}$$

Esto significa que $(p \wedge (p \downarrow q))$ es falso para todos los valores de p y de q y por lo tanto

$$\neg(p \wedge (p \downarrow q)) \tag{73}$$

es una tautología.

$$\begin{aligned}4.(p \wedge (p|q)) &\leftrightarrow (p \wedge \neg(p \wedge q)) \\ &\leftrightarrow (p \wedge (\neg p \vee \neg q)) \\ &\leftrightarrow ((p \wedge (\neg p)) \vee (p \wedge \neg q) \\ &\leftrightarrow (0 \vee (p \wedge \neg q)) \\ &\leftrightarrow (p \wedge \neg q) \\ &\leftrightarrow \neg(p \rightarrow q)\end{aligned}$$

Otra forma simple de combinar incluyendo solo dos elementos es considerar las dos alternativas en el orden de los elementos que se toman para operar; si iniciamos combinando la conjunción con las operaciones conmutativas, $\wedge$, $\vee$, $\downarrow$, $|$, $\leftrightarrow$, $\veebar$, obtendremos las mismas operaciones pues

$$((p \copyright q) \wedge (q \copyright p)) \leftrightarrow ((p \copyright q) \wedge (p \copyright q))$$

y como la conjunción es idempotente

$$((p \copyright q) \wedge (p \copyright q)) \leftrightarrow (p \copyright q).$$

Si combinamos la conjunción con las operaciones conmutativas tendremos los mismos resultados. Ensayemos entonces a combinar una operación conmutativa pero no idempotente como el funtor de Peirce o la barra de Sheffer con las otras operaciones conmutativas:

$$((p \copyright q) \downarrow (q \copyright p)) \leftrightarrow ((p \copyright q) \downarrow (p \copyright q)) \leftrightarrow \neg(p \copyright q).$$

En el caso particular de la conjunción obtenemos la barra

$$\begin{aligned}5.((p \wedge q) \downarrow (q \wedge p)) &\leftrightarrow ((p \wedge q) \downarrow (p \wedge q)) \\ &\leftrightarrow \neg(p \wedge q) \\ &\leftrightarrow p|q\end{aligned}$$

con la barra obtenemos la conjunción

$$\begin{aligned}6.((p|q) \downarrow (q|p)) &\leftrightarrow ((p|q) \downarrow (p|q)) \\ &\leftrightarrow \neg(p|q) \\ &\leftrightarrow p \wedge q\end{aligned}$$

Con la disyunción obtenemos el funtor

$$\begin{aligned}7.((p \vee q) \downarrow (q \vee p)) &\leftrightarrow ((p \vee q) \downarrow (p \vee q)) \\ &\leftrightarrow \neg(p \vee q) \\ &\leftrightarrow p \downarrow q\end{aligned}$$

y con el funtor obtenemos la disyunción

$$\begin{aligned} 8.((p \downarrow q) \downarrow (q \downarrow p)) &\leftrightarrow (p \downarrow q) \downarrow \\ &\leftrightarrow \neg(p \downarrow q) \\ &\leftrightarrow p \vee q \end{aligned}$$

Con la equivalencia conseguimos la disyunción exclusiva y viceversa, obteniendo en todos los casos relaciones entre operaciones que ya estaban expuestas en la tabla 37.

Si combinamos la conjunción con la operación $\bullet-$ obtenemos la operación $\perp$:

$$\begin{aligned} 9.((p \bullet -q) \wedge (q \bullet -p)) &\leftrightarrow (\neg(p \leftarrow q) \wedge \neg(q \leftarrow p)) \\ &\leftrightarrow (\neg(q \rightarrow p) \wedge \neg(p \rightarrow q)) \\ &\leftrightarrow \neg((q \rightarrow p) \vee (p \rightarrow q)) \\ &\leftrightarrow \neg(p \top q) \\ &\leftrightarrow (p \perp q) \end{aligned}$$

El mismo resultado lo conseguimos con la operación $-\bullet$, es decir:

$$\begin{aligned} 10.((p - \bullet q) \wedge (q - \bullet p)) &\leftrightarrow (\neg(p \rightarrow q) \wedge \neg(q \rightarrow p)) \\ &\leftrightarrow \neg((p \rightarrow q) \vee (q \rightarrow p)) \\ &\leftrightarrow \neg(p \top q) \\ &\leftrightarrow (p \perp q) \end{aligned}$$

análogamente,

$$\begin{aligned} &11.((p \,\pi_1\, q) \wedge (q \,\pi_1\, p)) \leftrightarrow (p \wedge q) \\ &12.((p \,\pi_2\, q) \wedge (q \,\pi_2\, p)) \leftrightarrow (q \wedge p) \\ &13.((p * q) \wedge (q * p)) \leftrightarrow (p \downarrow q) \\ &14.((p \otimes q) \wedge (q \otimes p)) \leftrightarrow (q \downarrow p) \end{aligned}$$

Con la disyunción

$$\begin{aligned} 15.((p \bullet -q) \vee (q \bullet -p)) &\leftrightarrow (\neg(p \leftarrow q) \vee \neg(q \leftarrow p)) \\ &\leftrightarrow (\neg(q \rightarrow p) \vee \neg(p \rightarrow q)) \\ &\leftrightarrow \neg((q \rightarrow p) \wedge (p \rightarrow q)) \\ &\leftrightarrow \neg(p \leftrightarrow q) \\ &\leftrightarrow (p \veebar q) \end{aligned}$$

y

$$\begin{aligned} 16.((p - \bullet q) \vee (q - \bullet p)) &\leftrightarrow (\neg(p \to q) \vee \neg(q \to p)) \\ &\leftrightarrow \neg((p \to q) \wedge (q \to p)) \\ &\leftrightarrow \neg(p \leftrightarrow q) \\ &\leftrightarrow (p \veebar q) \end{aligned}$$

De forma similar

$$\begin{aligned} &17.(p\,\pi_1\,q) \vee (q\,\pi_1\,p)) \leftrightarrow (p \vee q) \\ &18.((p\,\pi_2\,q) \vee (q\,\pi_2\,p)) \leftrightarrow (q \vee p) \\ &19.((p * q) \vee (q * p)) \leftrightarrow (p|q) \\ &20.((p \otimes q) \vee (q \otimes p)) \leftrightarrow (q|p) \end{aligned}$$

1.7.4. Contralógica

Como hemos visto a lo largo de lo que hemos hecho, nada hemos ganado, desde el punto de vista algebraico, cambiando en la estructura de $(Z_2, +)$ o en la estructura $(Z_2, \times)$ el nombre 1 por a, o por -1, o por una matriz, o por cualquier otro nombre; tampoco intercambiando el nombre de los elementos 0 y 1, pero aquí surgen preguntas de tipo filosófico, en relación con las caras de $(Z_2, +, \times)$ y la lógica clásica, si el 1 representa *lo verdadero* y el 0 *lo falso*, ¿es posible construir una lógica alternativa donde lo verdadero lo cambiemos por lo falso y lo falso por lo verdadero? ¿Son la verdad y la falsedad relativas? ¿Tiene sentido la verdad en matemáticas? ¿Existe una única verdad? ¿Una proposición es verdadera? ¿Qué sucedería, si repentinamente cambiáramos los valores de verdad de todas las proposiciones y lo que es verdadero lo volviéramos falso y a todo lo falso lo hiciéramos verdadero? ¿Cambiaría la lógica? ¿Sería posible seguir razonando como lo hacemos? ¿Cuales serían las leyes de la nueva lógica? ¡Intentémoslo! ¡Construyamos una contralógica!

1.7.4.1. La negación de la equivalencia y la disyunción

Para construir la lógica de lo contrario podemos aplicar la función H

$$x(\mathrm{H}©)y = \neg((\neg x)\,©\,(\neg y))$$

o la función N

$$x(\mathrm{N}©)y = \neg(x\,©\,y).$$

Usaremos la primera opción y dejamos la otra como ejercicio.

Debemos construir una negación (vía la función H) para cada una de las operaciones de la lógica usual, como ya sabemos

$$\begin{aligned} \mathrm{H}(\veebar) &= \leftrightarrow \\ \mathrm{H}(\leftrightarrow) &= \veebar \\ \mathrm{H}(\vee) &= \wedge \\ \mathrm{H}(\wedge) &= \vee \end{aligned}$$

Si seguimos así, podríamos inferir que las operaciones de la contralógica son las mismas de la lógica usual, pero con otro nombre. *¡Y tendríamos una explicación, de por qué el mundo está así!*

1.7.4.2. La negación de la implicación: la contraimplicación

La contraimplicación es la imagen por H de la implicación que en nuestra notación es la operación

$\bullet-$	0	1
0	0	1
1	0	0

Tabla 29

Aunque esta operación no es muy popular en la lógica clásica, ya sabemos que cumple las mismas propiedades algebraicas que la implicación, en particular es permutable a izquierda y auto distributiva a izquierda, esto es:

$$p \bullet -(q \bullet -r) = q \bullet -(p \bullet -r)$$

y

$$p \bullet -(q \bullet -r) = (p \bullet -q) \bullet -(p \bullet -r)$$

donde p, q y r son los valores de verdad de proposiciones cualesquiera.

Además, por la definición de H está relacionada con la implicación de la forma

$$(\neg p) \bullet -(\neg q) = \neg(p \to q)$$

o sea que

$$p \bullet -q = (\neg p) \wedge q.$$

Transformemos ahora cada tautología de la lógica usual, cambiando en ella cada proposición y cada operación por su negación; obviamente si todo

funciona como hasta ahora no obtendremos nada nuevo, solo hallaremos, en lugar de una tautología, una contradicción, veamos un ejemplo:

En el caso del modus ponens clásico

$$(p \wedge (p \to q)) \to q$$

si escribimos $\neg p$ en lugar de p, $\bullet-$ en lugar de $\to$, $\wedge$ en lugar de $\vee$, obtenemos

$$(\neg p \vee (\neg p \bullet -\neg q)) \bullet -(\neg q)$$

que debe ser válida para todo p, en particular para $\neg p$ y $\neg q$, es decir

$$(\neg\neg p \vee (\neg\neg p \bullet -\neg\neg q)) \bullet -(\neg\neg q)$$

o sea

$$(p \vee (p \bullet -q)) \bullet -q$$

que es la contradicción buscada.

De manera similar, obtenemos igualdades como:

$$p \vee q = (p \bullet -q) \vee (q \bullet -p)$$

copia de

$$p \leftrightarrow q = (p \to q) \wedge (q \to p).$$

Con base en lo que hemos hecho, podemos construir teorías de conjuntos; y muchas otras teorías, cambiando el modelo de razonamiento y prueba; sin embargo, dejaremos este tema para abordarlo en otra ocasión. Por el momento, trataremos Z_3 para obtener otro ejemplo análogo al de Z_2 y estudiar, de manera más detallada, el concepto de isomorfismo, esto es lo que haremos en el siguiente capítulo.

CAPÍTULO 2

Estructuras algebraicas con tres elementos

El arte de proponer cuestiones es más importante que el de resolverlas.
Cantor

En el capítulo anterior estudiamos diferentes caras de estructuras definidas en conjuntos con dos elementos, y resaltamos el papel que tienen algunas de las propiedades de las operaciones, para establecer cuáles son las acciones permitidas en tal estructura.

En este capítulo estudiaremos estructuras formadas en conjuntos con tres elementos, pero esta vez aplicaremos las propiedades de las operaciones para resolver ecuaciones, de manera análoga a la forma en que las usamos en la secundaria para resolver ecuaciones entre números reales, con el propósito de establecer, que estos procedimientos no dependen de la naturaleza de los objetos que operamos, sino de las propiedades de las operaciones que entre ellos definamos.

Iniciamos con un conjunto con tres elementos cuyos elementos son conjuntos infinitos de números y entre ellos definimos una operación; luego presentamos una situación geométrica, en donde el conjunto está formado por tres funciones y la operación entre ellas es la composición usual; seguidamente abordamos un caso algebraico partiendo de las tres raíces cúbicas de la unidad y la operación es la multiplicación usual en los números complejos; y por último, estudiamos un conjunto cuyos elementos son tres matrices con su multiplicación habitual como operación.

De lo anterior, observamos que todos los ejemplos mencionados son representaciones de una estructura conocida como el grupo $(Z_3, +)$.

Seguidamente estudiamos cómo las propiedades de grupo de $(Z_3, +)$ no determinan una sola representación sino tres, que igual se pueden caracterizar, con otras propiedades básicas.

Luego establecemos el mecanismo de paso de una representación a otra, lo que permite abstraer el concepto de isomorfismo y con él, un procedimiento para copiar operaciones que preserva sus propiedades. De nuevo recurrimos al software *Álgebra finita* para verificar que las estructuras isomorfas tienen las mismas propiedades algebraicas.

Después aplicamos lo aprendido con $(Z_3, +)$ a la estructura $(Z_3, \times)$; ensamblando estas dos estructuras, obtenemos el campo $(Z_3, +, \times)$ y resolvemos ecuaciones en él.

Posteriormente, para conseguir nuevas estructuras con tres elementos no isomorfas a las ya construidas, modificamos la condición de isomorfismo o usamos los axiomas del capítulo 1, que nos permitieron obtener estructuras con dos elementos.

Finalmente, construimos estructuras algebraicas a partir de relaciones de orden, los retículos, y presentamos algunas aplicaciones de estos en la construcción de lógicas trivalentes.

2.1. De las representaciones de $(Z_3, +)$ a la estructura

Los siguientes ejemplos son representaciones de una sola estructura que notaremos $(Z_3, +)$.

2.1.1. Las familias [0], [1] y [2]

Consideremos el conjunto de los números enteros Z, inicialmente representados en una recta de la manera habitual; en el punto correspondiente al número 0, colocamos una circunferencia tangente a la recta, y la dividimos en 3 partes iguales; en cada una de ellas marcamos un punto que notamos con los números 0, 1 y 2, haciendo coincidir el 0 de la recta con el de la circunferencia, como si fuera un reloj de tres horas como lo ilustra la figura 1. Enrollamos la recta sobre la circunferencia, en el sentido de las manecillas del reloj la semirrecta de la derecha y en sentido contrario la semirrecta de la izquierda:

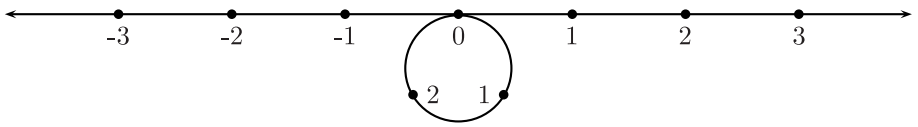


Figura 1

Sobre cada uno de los números de la circunferencia, quedarán ubicados infinitos números enteros, agrupados en familias; por ejemplo, la familia del cero es:

$$[0] = \{0, \pm 3, \pm 6, \pm 9, \ldots, \pm 3k \ldots\}, \text{ con } k = 0, 1, 2, 3, \ldots$$

Las demás familias son:

$$[1] = \{1, 4, 7, 10, \ldots, \pm 3k + 1, \ldots\}, \text{ con } k = 0, 1, 2, 3, \ldots$$
$$[2] = \{2, 5, 8, 11, \ldots, \pm 3k + 2, \ldots\}, \text{ con } k = 0, 1, 2, 3, \ldots$$

y no hay más; porque la familia del 3 es la misma que la del 0, la del 4 es la del 1 y así sucesivamente.

De esta forma hemos construido 3 familias, que van a formar nuestro universo de discurso y que notaremos

$$\mathrm{T} = \{[0], [1], [2]\}$$

Para simplificar, omitiremos los paréntesis y entenderemos, por ejemplo, que el símbolo 1 representa a la familia [1]. *Enfaticemos en que el significado del símbolo 1 en este contexto no es el mismo que tiene en los números naturales.*

Una manera directa de encontrar la familia en T a la que pertenece un número entero cualquiera, consiste en tomar el residuo que queda de dividirlo entre tres.

Una curiosidad de este sistema es que el número que sigue al 2 es el 0, en la recta era el 3, decimos entonces que el 3 es equivalente al 0, ($3 \approx 0$); por supuesto, los dos pertenecen a la misma familia; también 4 es equivalente a 1, etc.

Cuando sumamos 2+2 en los enteros, obtenemos 4 como resultado, pero en la circunferencia, la familia del 4 es la misma que la del 1; por lo tanto, asignaremos como resultado de la suma el 1 (notemos que el procedimiento no depende de los elementos que elijamos en cada familia); si lo miramos desde otro punto de vista, es como sumar en base 3 pero sin llevar:

$$2 + 2 = 11$$

en base 3; en T, tomamos el 1 de las unidades, y nos olvidamos del otro 1. Esto lo escribimos:

$$2 \oplus 2 = 1$$

El cambio en el símbolo de la suma se debe a que esta es una operación diferente a la suma de números enteros, aunque un poco más adelante, cuando no haya lugar a confusión, usaremos el mismo símbolo para las dos sumas.

La tabla de la suma queda:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabla 1

2.1.2. La composición de rotaciones de 120° en el plano

Supongamos que tenemos una figura plana cualquiera y un punto fijo M fuera de ella, si la rotamos 120° con respecto a M y notamos esta operación con R, la figura cambia, en relación con su posición inicial, como observamos:

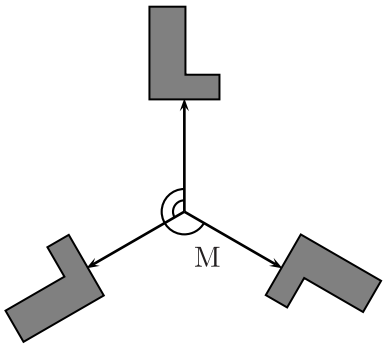


Figura 2

Si reiteramos la operación obtenemos un giro de 240° que notaremos como R^2, que es equivalente a realizar un giro de $-120°$. Y si nuevamente repetimos la operación, conseguimos la posición inicial, es decir, la figura queda invariante; a esta situación la notamos con I.

Si aplicamos una transformación a continuación de la otra obtenemos la composición ($\circ$) de ellas, que se resume en:

$(\circ)$	I	R	R^2
I	I	R	R^2
R	R	R^2	I
R^2	R^2	I	R

Tabla 2

2.1.3. Las raíces cúbicas de la unidad

Si consideremos la siguiente ecuación en los números complejos:

$$x^3 - 1 = 0$$

que es equivalente a $x^3 = 1$, obtenemos como primera solución $x = 1$ y al observar que:

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = 0$$

conseguimos las tres raíces: 1, α_1 y α_2 donde

$$\alpha_1 = \frac{-1 + \sqrt{3}i}{2} \qquad \text{y} \qquad \alpha_2 = \frac{-1 - \sqrt{3}i}{2}.$$

son las soluciones de la ecuación cuadrática; y si buscamos relaciones entre las raíces, podemos obtener una a partir de las otras, en la siguiente forma:

$$(\alpha_1)^2 = \alpha_2 \qquad \text{y} \qquad (\alpha_2)^2 = \alpha_1,$$

$$(\alpha_1)^3 = \alpha_1\alpha_2 \qquad \text{y} \qquad (\alpha_2)^3 = \alpha_1\alpha_2,$$

de modo que $(\alpha_1)^3 = (\alpha_1)^2\alpha_1 = \alpha_2\alpha_1 = 1$, igualmente, $(\alpha_2)^3 = 1$, así que a partir de α_1 se obtiene α_2 y 1, por tanto si $\alpha_1 = \alpha$, entonces $\alpha^2 = \alpha_2$ y $\alpha^3 = 1$, luego:

$\times$	1	α	α^2
1	1	α	α^2
α	α	α^2	1
α^2	α^2	1	α

Tabla 3

2.1.4. Una representación matricial de $(Z_3, +)$

La matriz

$$\mathrm{A} = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$$

tiene la propiedad de que al multiplicarse por sí misma, el producto es la matriz transpuesta

$$\mathrm{A}^t = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}$$

y que el producto de A con A^t es la matriz identidad. Lo anterior lo podemos resumir en la siguiente tabla:

$\times$	I	A	A^t
I	I	A	A^t
A	A	A^t	I
A^t	A^t	I	A

Tabla 4

2.1.5. La estructura $(Z_3, +)$

Observando todas las tablas obtenidas en cada una de las situaciones descritas notamos algo en común; poniendo un nombre genérico + a las operaciones que se muestran y llamando a, b y c a los elementos de los conjuntos, tenemos una sola información:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Tabla 5

A esta estructura la notaremos $(Z_3, +)$.

2.1.6. Propiedades de $(Z_3, +)$

Veamos cuáles propiedades de las enunciadas para los conjuntos numéricos usuales cumple la estructura $(Z_3, +)$.

Por ejemplo, para verificar si se cumple la propiedad asociativa, hay dos caminos: el primero es, como lo hicimos antes, realizar todas las cuentas de la forma

$$(a+b)+c \qquad \text{y} \qquad a+(b+c)$$

con todos los valores posibles para a, b, y c en $(Z_3, +)$, y comparar los resultados; si en todos los casos obtenemos una igualdad, la operación es asociativa.

El segundo camino es dejarle el trabajo a una máquina; con el programa *Álgebra finita*, una computadora verifica si una operación definida en un conjunto finito es asociativa, conmutativa, tiene elemento idéntico, elementos inversos, o si es distributiva con respecto a otra, entre otras cosas.

Usando el programa[1], comprobamos que la suma en $(Z_3, +)$ es asociativa, conmutativa, tiene como elemento idéntico a, y el inverso de a es a, de b es c y de c es b, es decir que:

$$-a = a$$
$$-b = c$$
$$-c = b$$

En resumen, $(Z_3, +)$ es un grupo abeliano. Sin embargo, $(Z_3, +)$ no solo cumple las propiedades anteriormente mencionadas, por ejemplo, también cumple las propiedades:

i. Elasticidad: $x + (y + x) = (x + y) + x$

ii. Asociativa cíclica I: $x + (y + z) = z + (x + y)$

iii. Asociativa cíclica II: $x + (y + z) = (z + x) + y$

iv. Identidad de Abel – Graβmann I: $x + (y + z) = z + (y + x)$

v. Identidad de Abel – Graβmann II: $x + (y + z) = (y + x) + z$

vi. Permutabilidad a izquierda: $x + (y + z) = y + (x + z)$

vii. Permutabilidad a derecha: $(x + y) + z = (x + z) + y$

viii. Propiedad del producto reducido: $(x + y) + z = x + (z + y)$

ix. Bisimetría: $(x + y) + (u + v) = (x + u) + (y + v)$

[1]Este mecanismo de validación de una afirmación es poco ortodoxo en matemáticas y no es universalmente aceptado.

2.2. De la estructura $(Z_3, +)$ a las representaciones

Nuevamente tratemos de caracterizar la estructura en términos de propiedades y una opción inicial es caracterizarlo como grupo abeliano, iniciemos determinando el elemento idéntico, por ejemplo, al elemento a; con esta condición tenemos que:

$+$	a	b	c
a	a	b	c
b	b		
c	c		

como b y c deben tener inversos aditivos, el elemento a debe estar en la fila y en la columna de b y c respectivamente, para ello hay dos posibilidades,

$+$	a	b	c
a	a	b	c
b	b	a	
c	c		a

o

$+$	a	b	c
a	a	b	c
b	b		a
c	c	a	

pero como existen inversos aditivos la operación debe ser cancelativa y esto implica que cada elemento aparezca una sola vez en cada fila y columna, luego esta condición obliga a que la tabla de la operación + sea:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Tabla 5

Si ahora suponemos que el elemento idéntico es b, la tabla resultante es:

$\Diamond$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Tabla 6

y si escogemos como elemento idéntico al elemento c, la tabla que obtenemos es:

∇	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

Tabla 7

Pareciera que con las condiciones dadas obtenemos tres operaciones distintas, pero al igual que en el caso de $(Z_2, +)$, lo que tenemos es un cambio de nombre, si en la tabla 6 cambiamos a por b y b por a, resulta:

	b	a	c
b	c	b	a
a	b	a	c
c	a	c	b

y al reordenarla, obtenemos:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

que es la misma tabla 5.

De manera similar, si en la tabla 7 cambiamos a por c, c por a y reordenamos, vamos a obtener la tabla 5. Lo anterior significa, que las tres tablas representan *la misma operación* con el nombre de los elementos intercambiado.

Por tanto las propiedades que determinan un grupo abeliano, *en el caso de un conjunto con tres elementos*[2], determinan una estructura, salvo isomorfismos, debido a que de las $3^9 = 19\,683$ operaciones posibles en un conjunto con tres elementos, solo una de ellas, con tres caras, tiene estructura de grupo abeliano.

2.2.1. Otras caracterizaciones de la misma estructura

De las propiedades enunciadas anteriormente para caracterizar $(Z_3, +)$ tenemos que solo con algunas podemos seguir determinando la estructura, salvo isomorfismos, por ejemplo:

1. Un conjunto con tres elementos y una operación, que tiene estructura de *grupo*.

2. Un conjunto con tres elementos y una operación, que tiene estructura de monoide cancelativo.

3. Un conjunto con tres elementos y una operación, que tiene elemento idéntico y es cancelativa.

4. Un conjunto con tres elementos y una operación, que tiene estructura de *bucle*[3].

Otra manera de caracterizar $(Z_3, +)$ es recurriendo a propiedades no usuales, como:

5. Un conjunto con tres elementos y una operación, con elemento idéntico a y para los otros dos elementos b y c distintos de a, se cumple que $b^2 = c$, $c^2 = b$ y $cb = bc = a$.

[2]En el caso de cuatro elementos no es cierta esta afirmación, por ejemplo podemos encontrar dos estructuras que son grupos, el V de Klein y Z_4, y sin embargo estos no son isomorfos.

[3]Un *bucle* o *loop* es un conjunto H con una operación $+$, tal que: tiene un elemento idéntico y es un *cuasigrupo*, esto es, que para todo a y b en H, las ecuaciones $a + x = b$ y $y + a = b$ tienen soluciones únicas. El concepto de *loop* aparece en (ALBERT, Adrian. Quasigroups I. Trans. Amer. Math. Soc, 1943. v. 54. p. 507-519.). Algunos (BOL, Gerrit. Gewebe und Gruppen, Math. Ann. 1937. v. 114. p. 414-431.) lo llaman *Dominio normado* (Normbereich).

2.3. Paso de una representación a otra

Anteriormente se mencionó que las tablas 6 y 7 son la misma tabla 5 salvo por un cambio de nombre, es decir, que podemos definir una función biyectiva de Z_3 en Z_3, en el caso de la tabla 7:

$$\begin{aligned} h : Z_3 &\to Z_3 \\ a &\mapsto c \\ b &\mapsto b \\ c &\mapsto a \end{aligned}$$

y en el caso de la tabla 6:

$$\begin{aligned} g : Z_3 &\to Z_3 \\ a &\mapsto b \\ b &\mapsto a \\ c &\mapsto c \end{aligned}$$

donde el cambio de cada elemento y de cada uno de los resultados al operarlos mediante $+$, se puede interpretar como:

$$x \nabla y = h(h(x) + h(y))$$

y

$$x \diamondsuit y = g(g(x) + g(y))$$

construyendo así una operación con la ayuda de otra; sin embargo estamos, de nuevo, ante la *misma* situación desde el punto de vista algebraico, salvo el *nombre* de los entes que ellos representan, es decir, estamos ante *estructuras isomorfas*.

Como en el capítulo anterior, podemos cambiar los nombres a los elementos de un conjunto con tres elementos $\mathrm{T} = \{0, 1, 2\}$ donde se ha definido una operación $+$, y estudiar el efecto que ello tiene sobre esta; y como hay seis maneras de *cambiarle el nombre* a los elementos de T, en el sentido de *asignar un único nombre a cada uno de los elementos y que cada nombre corresponda a un solo elemento del conjunto*; es decir, hay seis funciones biyectivas de T en T, podemos esperar que hayan seis formas de presentar a T, una por cada una de las funciones biyectivas:

f_0	f_1	f_2	f_3	f_4	f_5
$0 \mapsto 0$	$0 \mapsto 0$	$0 \mapsto 2$	$0 \mapsto 1$	$0 \mapsto 2$	$0 \mapsto 1$
$1 \mapsto 1$	$1 \mapsto 2$	$1 \mapsto 1$	$1 \mapsto 0$	$1 \mapsto 0$	$1 \mapsto 2$
$2 \mapsto 2$	$2 \mapsto 1$	$2 \mapsto 0$	$2 \mapsto 2$	$2 \mapsto 1$	$2 \mapsto 0$

Cambiemos el nombre de los elementos de $(Z_3, +)$ con las funciones f_1 y f_4, ya que anteriormente ensayamos con $f_2 = h$ y $f_3 = g$, utilizando los dos mecanismos encontrados:

1. Cambiando los nombres en toda la tabla, según la función f_1 en la tabla 5 interpretando $a = 0$, $b = 1$ y $c = 2$, solo debemos cambiar el 1 por el 2 y el 2 por el 1; por tanto obtenemos:

	0	2	1
0	0	2	1
2	2	1	0
1	1	0	2

y si la reordenamos resulta:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabla 8

que corresponde a la misma tabla 5.

2. Reemplazando x e y por los elementos del conjunto en la expresión:

$$f_1(f_1(x) + f_1(y))$$

vemos que el resultado es el mismo, puesto que:

$$f_1(f_1(0) + f_1(0)) = 0$$
$$f_1(f_1(0) + f_1(1)) = 1$$
$$f_1(f_1(0) + f_1(2)) = 2$$
$$f_1(f_1(1) + f_1(0)) = 1$$

$$f_1(f_1(1)+f_1(1))=2$$
$$f_1(f_1(1)+f_1(2))=0$$
$$f_1(f_1(2)+f_1(0))=2$$
$$f_1(f_1(2)+f_1(1))=0$$
$$f_1(f_1(2)+f_1(2))=1$$

luego $x+y=f_1(f_1(x)+f_1(y))$.

Ahora, si aplicamos la función f_4, en la tabla 8 debemos cambiar el 0 por el 2, el 1 por el 0 y el 2 por el 1, con el primer mecanismo obtenemos:

	2	0	1
2	2	0	1
0	0	1	2
1	1	2	0

y reordenando:

∇	0	1	2
0	1	2	0
1	2	0	1
2	0	1	2

Tabla 9

que corresponde a la tabla 7, si interpretamos $a=0$, $b=1$ y $c=2$.

Con el segundo mecanismo,

$$f_4(f_4(0)+f_4(0))=0$$
$$f_4(f_4(0)+f_4(1))=1$$
$$f_4(f_4(0)+f_4(2))=2$$
$$f_4(f_4(1)+f_4(0))=1$$
$$f_4(f_4(1)+f_4(1))=2$$
$$f_4(f_4(1)+f_4(2))=0$$
$$f_4(f_4(2)+f_4(0))=2$$
$$f_4(f_4(2)+f_4(1))=0$$
$$f_4(f_4(2)+f_4(2))=1$$

obtenemos otro resultado, la tabla 8:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabla 8

Como los resultados no son los mismos, miremos en detalle qué es lo que sucede, describiendo el proceso que hicimos con la tabla 8 para conseguir la tabla 9: inicialmente le cambiamos el nombre en los encabezados a cada elemento, o sea escribimos

$$f_4(0) = 2 \quad f_4(1) = 0 \quad f_4(2) = 1$$

∇	$f_4(0)$	$f_4(1)$	$f_4(2)$
$f_4(0)$			
$f_4(1)$			
$f_4(2)$			

y en cada casilla escribimos el resultado de aplicar f_4 al elemento resultante de la operación $+$ que presenta la tabla 8,

∇	$f_4(0)$	$f_4(1)$	$f_4(2)$
$f_4(0)$	$f_4(0+0)$	$f_4(0+1)$	$f_4(0+2)$
$f_4(1)$			
$f_4(2)$		$f_4(2+1)$	

En resumen para cada par de elementos z, w de $(Z_3, +)$,

$$f_4(z) \nabla f_4(w) = f_4(z + w)$$

pero, ¿cómo convertimos esta expresión en la que teníamos anteriormente?, pues queremos que dada la operación $+$ podamos construir la operación ∇. Para ello podemos realizar un cambio de nombre:

$$x = f_4(z) \qquad \text{y} \qquad y = f_4(w)$$

donde

$$f_4^{-1}(x) = z \qquad \text{y} \qquad f_4^{-1}(y) = w$$

puesto que f_4 es una función biyectiva. Luego podemos escribir:

$$x \nabla y = f_4(f_4^{-1}(x) + f_4^{-1}(y)).$$

Notemos que f_4^{-1} es la función f_5.

Entonces, ¿por qué en el caso de las funciones f_1, f_2 y f_3 los dos mecanismos coincidieron? Resulta que[4]:

$$f_1 f_1 = f_0 \qquad f_2 f_2 = f_0 \qquad f_3 f_3 = f_0$$

es decir, que cada función es su propia inversa, por tanto la expresión que describe el mecanismo de copia de una estructura, se puede expresar como:

$$f_1(f_1(x) + f_1(y))$$

que fue lo que obtuvimos en el caso de la función f_1.

Otra manera de escribir el mecanismo de copia de una estructura es utilizando también el hecho de que la función f_4 es biyectiva, aplicando f_4^{-1} a la expresión

$$f_4(z) \nabla f_4(w) = f_4(z + w)$$

conseguimos

$$f_4^{-1}(f_4(z) \nabla f_4(w)) = f_4^{-1}(f_4(z + w))$$

que es equivalente a

$$f_4^{-1}(f_4(z) \nabla f_4(w)) = z + w.$$

A pesar de que contamos con seis funciones biyectivas, estas solo nos proporcionaron tres caras de $(Z_3, +)$, resultado que habíamos obtenido cuando caracterizamos la estructura por sus propiedades.

2.4. Construcción de estructuras isomorfas

El procedimiento que hemos desarrollado para conseguir copias de estructuras dadas, podemos extenderlo para *copiar una estructura algebraica* a un *conjunto sin estructura* usando funciones biyectivas, y con esto conseguir una nueva estructura, *isomorfa a la anterior*; sin importar si la estructura inicial está en el dominio o en el codominio de la función, *la nueva estructura tendrá las mismas propiedades que la original*, es decir que desde el punto de vista algebraico no serán distinguibles.

[4]Se omite el símbolo $\circ$ que indica la operación composición de funciones.

Precisando, si (A, +) es una estructura, B un conjunto y f una función biyectiva de A en B, definimos la operación $\oplus$ en B de la siguiente manera:

$$a \oplus b = f(f^{-1}(a) + f^{-1}(b))$$

para todo par de elementos a, b de B. La estructura (B, $\oplus$) es una copia de la estructura (A, +), en el sentido de que es la misma operación entre elementos que tienen diferente nombre, es decir, las dos estructuras son *isomorfas*.

Pero si (B, +) es una estructura, A un conjunto y f una función biyectiva de A en B, definimos la operación $\oplus$ en A de la siguiente manera:

$$a \oplus b = f^{-1}(f(a) + f(b))$$

para todo par de elementos a, b de A.

Y si ambos conjuntos tienen estructura (A, +) y (B, $\oplus$) ellas son isomorfas si existe una función biyectiva f entre ellas, que llamaremos un *isomorfismo* entre (A, +) y (B, $\oplus$) de manera que:

$$f(x) + f(y) = f(x \oplus y)$$

para todo x, y de A, o lo que es lo mismo:

$$f^{-1}(a + b) = f^{-1}(a) \oplus f^{-1}(b)$$

para todo a, b de B.

2.4.1. Propiedades

Como hemos mencionado que al aplicar el mecanismo de copia a una estructura, la nueva estructura tendrá las mismas propiedades que la original, demostremos algunos casos particulares como las propiedades usuales en los conjuntos numéricos y otras mencionadas en el capítulo anterior:

2.4.1.1. Propiedad asociativa

Supongamos que (A, $+$) cumple la propiedad asociativa, entonces (B, $\oplus$) también cumple la propiedad asociativa.

Prueba: para todo elemento a, b, $c \in$ B tenemos que:

$$\begin{aligned}
a \oplus (b \oplus c) &= a \oplus f(f^{-1}(b) + f^{-1}(c)) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(c)))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(b) + f^{-1}(c))) && \text{Biyectividad de } f \\
&= f((f^{-1}(a) + f^{-1}(b)) + f^{-1}(c)) && \text{Asociatividad de } + \\
&= f(f^{-1}(f(f^{-1}(a) + f^{-1}(b))) + f^{-1}(c)) && \text{Biyectividad de } f \\
&= f(f^{-1}(a \oplus b) + f^{-1}(c)) && \text{Definición de } \oplus \\
&= (a \oplus b) \oplus c && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.2. Existencia de elemento idéntico

Supongamos que e es el elemento idéntico de (A, $+$), entonces $f(e)$ es el elemento idéntico de (B, $\oplus$).

Prueba: para todo elemento $a \in$ B tenemos que:

$$\begin{aligned}
a \oplus f(e) &= f(f^{-1}(a) + f^{-1}(f(e))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + e) && \text{Biyectividad de } f \\
&= f(f^{-1}(a)) && \text{Elemento idéntico para } + \\
&= a && \text{Biyectividad de } f.
\end{aligned}$$

De la misma manera se prueba que $f(e) \oplus a = a$.

2.4.1.3. Existencia de elementos inversos

Sea $a \in$ B, como f es biyectiva existe $x \in$ A tal que $f(x) = a$ y si $-x$ es el elemento inverso de x de A, entonces $f(-x) = -f(x)$ es el elemento inverso de a en B.

Prueba: sea $a \in$ B, como f es biyectiva, existe $x \in$ A tal que $f(x) = a$, entonces:

$$\begin{aligned} a \oplus f(-x) &= f(f^{-1}(a) + f^{-1}(f(-x))) && \text{Definición de } \oplus \\ &= f(x + (-x)) && \text{Biyectividad de } f \\ &= f(e) && \text{Elemento inverso} \\ & && \text{para } + \end{aligned}$$

De la misma manera se prueba que $f(-x) \oplus a = f(e)$. Esto significa que $f(-x) = -a$ luego tenemos que:

$$f(-x) = -f(x).$$

2.4.1.4. Propiedad conmutativa

Supongamos que (A, +) cumple la propiedad conmutativa, entonces (B, $\oplus$) también cumple la propiedad conmutativa.

Prueba: para todo elemento a, $b \in$ B tenemos que

$$\begin{aligned} a \oplus b &= f(f^{-1}(a) + f^{-1}(b)) && \text{Definición de } \oplus \\ &= f(f^{-1}(b) + f^{-1}(a)) && \text{Conmutatividad de } + \\ &= b \oplus a && \text{Definición de } \oplus. \end{aligned}$$

2.4.1.5. Propiedad elástica

Supongamos que (A, +) cumple la propiedad elástica, entonces (B, $\oplus$) también cumple la propiedad elástica.

Prueba: para todo elemento a, $b \in$ B tenemos que

$$\begin{aligned} a \oplus (b \oplus a) &= a \oplus f(f^{-1}(b) + f^{-1}(a)) && \text{Definición de } \oplus \\ &= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(a)))) && \text{Definición de } \oplus \\ &= f(f^{-1}(a) + (f^{-1}(b) + f^{-1}(a))) && \text{Biyectividad de } f \\ &= f((f^{-1}(a) + f^{-1}(b)) + f^{-1}(a)) && \text{Propiedad elástica de } + \\ &= f(f^{-1}(f(f^{-1}(a) + f^{-1}(b))) + f^{-1}(a)) && \text{Biyectividad de } f \\ &= f(f^{-1}(a \oplus b) + f^{-1}(a)) && \text{Definición de } \oplus \\ &= (a \oplus b) \oplus a && \text{Definición de } \oplus. \end{aligned}$$

2.4.1.6. Propiedad de permutabilidad a izquierda

Supongamos que (A, +) cumple la propiedad de permutabilidad a izquierda, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, b,$c \in$ B tenemos que

$$\begin{aligned}
a \oplus (b \oplus c) &= a \oplus f(f^{-1}(b) + f^{-1}(c)) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(c)))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(b) + f^{-1}(c))) && \text{Biyectividad de } f \\
&= f(f^{-1}(b) + (f^{-1}(a) + f^{-1}(c))) && \text{Permutabilidad a} \\
& && \text{izquierda de } + \\
&= f(f^{-1}(b) + f^{-1}(f(f^{-1}(a) + f^{-1}(c)))) && \text{Biyectividad de } f \\
&= f(f^{-1}(b) + f^{-1}(a \oplus c) && \text{Definición de } \oplus \\
&= b \oplus (a \oplus c) && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.7. Identidad I de Stein

Supongamos que (A, +) cumple la identidad I de Stein, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, $b \in$ B tenemos que

$$\begin{aligned}
a \oplus (a \oplus b) &= a \oplus f(f^{-1}(a) + f^{-1}(b)) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(a) + f^{-1}(b)))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(a) + f^{-1}(b))) && \text{Biyectividad de } f \\
&= f(f^{-1}(b) + f^{-1}(a)) && \text{Identidad I de Stein} \\
& && \text{de } + \\
&= b \oplus a && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.8. Identidad II de Stein

Supongamos que (A, +) cumple la identidad II de Stein, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, $b \in$ B tenemos que

$$\begin{aligned}
a \oplus (b \oplus a) &= a \oplus f(f^{-1}(b) + f^{-1}(a)) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(a)))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(b) + f^{-1}(a))) && \text{Biyectividad de } f \\
&= f((f^{-1}(b) + f^{-1}(a)) + f^{-1}(b)) && \text{Identidad II de} \\
& && \text{Stein de } + \\
&= f(f^{-1}(f(f^{-1}(b) + f^{-1}(a))) + f^{-1}(b)) && \text{Biyectividad de } f \\
&= f(f^{-1}(b \oplus a) + f^{-1}(b)) && \text{Definición de } \oplus \\
&= (b \oplus a) \oplus b && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.9. Identidad I de Schröder

Supongamos que (A, +) cumple la identidad I de Schröder, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, $b \in$ B tenemos que

$$\begin{aligned}
a \oplus (a \oplus b) &= a \oplus f(f^{-1}(a) + f^{-1}(b)) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(a) + f^{-1}(b)))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(a) + f^{-1}(b))) && \text{Biyectividad de } f \\
&= f((f^{-1}(a) + f^{-1}(b)) + f^{-1}(b)) && \text{Identidad I de} \\
& && \text{Schröder de } + \\
&= f(f^{-1}(f(f^{-1}(a) + f^{-1}(b))) + f^{-1}(b)) && \text{Biyectividad de } f \\
&= f(f^{-1}(a \oplus b) + f^{-1}(b)) && \text{Definición de } \oplus \\
&= (a \oplus b) \oplus b && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.10. Identidad de Tarski

Supongamos que (A, +) cumple la identidad de Tarski, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, $b \in$ B tenemos que

$$\begin{aligned}
a \oplus (b \oplus (c \oplus a)) &= a \oplus (b \oplus (f(f^{-1}(c) + f^{-1}(a)))) && \text{Definición de } \oplus \\
&= a \oplus (f(f^{-1}(b) + f^{-1}(f(f^{-1}(c) + f^{-1}(a))))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(f(f^{-1}(c) \\
&\qquad + f^{-1}(a)))))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(b) + (f^{-1}(c) + f^{-1}(a)))) && \text{Biyectividad de } f \\
&= f(f^{-1}(c) + f^{-1}(b)) && \text{Identidad de} \\
& && \text{Tarski de } + \\
&= c \oplus b && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.11. Identidad de Abel – Graßmann I

Supongamos que (A, +) cumple la identidad de Abel – Graßmann I, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, b, $c \in$ B tenemos que

$$\begin{aligned}
a \oplus (b \oplus c) &= a \oplus f(f^{-1}(b) + f^{-1}(c)) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(c)))) && \text{Definición de } \oplus \\
&= f(f^{-1}(a) + (f^{-1}(b) + f^{-1}(c))) && \text{Biyectividad de } f \\
&= f(f^{-1}(c) + (f^{-1}(b) + f^{-1}(a))) && \text{Identidad de} \\
& && \text{Abel - Graßmann I de } + \\
&= f(f^{-1}(c) + f^{-1}(f(f^{-1}(b) + f^{-1}(a)))) && \text{Biyectividad de } f \\
&= f(f^{-1}(c) + f^{-1}(b \oplus a) && \text{Definición de } \oplus \\
&= c \oplus (b \oplus a) && \text{Definición de } \oplus.
\end{aligned}$$

2.4.1.12. Propiedad bisimétrica

Supongamos que (A, +) cumple la propiedad bisimétrica, entonces (B, $\oplus$) también cumple esta propiedad.

Prueba: para todo elemento a, b, $c \in$ B tenemos que

$$\begin{aligned}
(a \oplus b) \oplus (c \oplus d) &= (a \oplus b) \oplus (f(f^{-1}(c) + f^{-1}(d))) && \text{Definición de } \oplus \\
&= (f(f^{-1}(a) + f^{-1}(b))) \oplus (f(f^{-1}(c) + f^{-1}(d))) && \text{Definición de } \oplus \\
&= f(f^{-1}(f(f^{-1}(a) + f^{-1}(b))) + f^{-1}(f(f^{-1}(c) \\
&\qquad + f^{-1}(d)))) && \text{Definición de } \oplus \\
&= f((f^{-1}(a) + f^{-1}(b)) + (f^{-1}(c) + f^{-1}(d))) && \text{Biyectividad de } f \\
&= f((f^{-1}(a) + f^{-1}(c)) + (f^{-1}(b) + f^{-1}(d))) && \text{Propiedad bisimétrica} \\
&&& \text{de } + \\
&= f(f^{-1}(f(f^{-1}(a) + f^{-1}(c))) + f^{-1}(f(f^{-1}(b) \\
&\qquad + f^{-1}(d)))) && \text{Biyectividad de } f \\
&= (f(f^{-1}(a) + f^{-1}(c))) \oplus (f(f^{-1}(b) + f^{-1}(d))) && \text{Definición de } \oplus \\
&= (a \oplus c) \oplus (f(f^{-1}(b) + f^{-1}(d))) && \text{Definición de } \oplus \\
&= (a \oplus c) \oplus (b \oplus d) && \text{Definición de } \oplus.
\end{aligned}$$

Aunque decimos que la nueva estructura tiene las mismas propiedades que la original, con las herramientas desarrolladas hasta ahora, solo podemos demostrar algunas de ellas[5], puesto que no podemos enunciar *todas* las propiedades[6] de una estructura determinada.

2.5. De las representaciones de $(Z_3, \times)$ a la estructura

2.5.1. Multiplicación en las familias [0], [1] y [2]

Para multiplicar dos familias en T $= \{[0], [1], [2]\}$ efectuamos un procedimiento similar al empleado en la suma: multiplicamos un elemento cualquiera de una familia por uno cualquiera de la otra, encontramos la familia a la que pertenece el resultado y esta la asignamos como resultado de multiplicar las dos familias (este procedimiento no depende de los elementos

[5]Con el álgebra universal si es posible demostrar la validez en B de todas las identidades que valen en A.

[6]Nos referimos a propiedades algebraicas de operaciones f y g, en las que intervienen n y m elementos respectivamente, definidas sobre el mismo conjunto M, expresables como una igualdad de la forma $f(x_1, x_2, \ldots, x_n) = g(y_1, y_2, \ldots, y_m)$ para x_i , y_i elementos arbitrarios de M. En el caso de las propiedades asociativa y distributiva, $m = n = 3$ y para la propiedad conmutativa $m = n = 2$.

elegidos en las familias). Por ejemplo 2×2 es 4 y la familia a la que pertenece el número 4 es la del 1; por tanto:

$$2 \otimes 2 = 1$$

Así, la tabla de la multiplicación queda como sigue:

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabla 10

La multiplicación, y en general cualquier operación, la podemos copiar de la misma forma que hicimos con (T, $\oplus$), con funciones biyectivas; por ejemplo si usamos f_1 para copiar la multiplicación de T,

	$f_1(0)$	$f_1(1)$	$f_1(2)$
$f_1(0)$	$f_1(0)$	$f_1(0)$	$f_1(0)$
$f_1(1)$	$f_1(0)$	$f_1(1)$	$f_1(2)$
$f_1(2)$	$f_1(0)$	$f_1(2)$	$f_1(1)$

resulta la tabla

$\otimes'$	0	2	1
0	0	0	0
2	0	2	1
1	0	1	2

al reorganizarla resulta:

$\otimes'$	0	1	2
0	0	0	0
1	0	2	1
2	0	1	2

Tabla 11

Si usamos la función f_2 para copiar (T, $\otimes$) obtenemos la tabla:

$\otimes''$	0	1	2
0	1	0	2
1	0	1	2
2	2	2	2

Tabla 12

Si utilizamos la función f_3 obtenemos la tabla:

$\otimes'''$	0	1	2
0	0	1	2
1	1	1	1
2	2	1	0

Tabla 13

Si copiamos (T, $\otimes$) con la función f_4 conseguimos la tabla:

$\otimes'^{v}$	0	1	2
0	0	1	2
1	1	0	2
2	2	2	2

Tabla 14

y con la función f_5 la tabla que obtenemos es:

$\otimes^{v}$	0	1	2
0	2	1	0
1	1	1	1
2	0	1	2

Tabla 15

A diferencia de (T, $\oplus$), hemos conseguido seis representaciones diferentes de la estructura (T, $\otimes$), una por cada función biyectiva empleada.

Cada una de las tablas obtenidas anteriormente es una representación de una estructura que notaremos (Z_3, $\times$).

2.5.2. Propiedades de $(Z_3, \times)$

Usando el programa *Álgebra finita*, comprobamos que la operación $\times$ en Z_3 es asociativa, conmutativa, tiene como elemento idéntico a 1, el inverso multiplicativo de 1 es 1, de 2 es 2 y 0 no tiene inverso; es decir que:

$$0^{-1} = \frac{1}{0} \qquad \text{No existe}$$

$$1^{-1} = \frac{1}{1} = 1 \qquad \text{y} \qquad 2^{-1} = \frac{1}{2} = 2$$

En resumen, $(Z_3, \times)$ es un monoide conmutativo, pero también cumple las propiedades: elasticidad, asociativa cíclica I, asociativa cíclica II, identidad de Abel – Graβmann I, identidad de Abel – Graβmann II, permutabilidad a izquierda, permutabilidad a derecha, propiedad del producto reducido y bisimetría.

2.6. De la estructura $(Z_3, \times)$ a las representaciones

Tratemos de caracterizar la estructura $(Z_3, \times)$ buscando algunas propiedades que determinen sus tablas, una posibilidad es:

1. Existe un elemento x en M $= \{0, 1, 2\}$, tal que para todo y, z en M, con $x \neq y$, $y \neq z$ y $x \neq z$:

i. $xy = xz = xx = zx = yx = x$

ii. $yy = zz \neq x$

iii. $yz = zy \neq x$

iv. $yz \neq yy$

Tenemos tres opciones para escoger el elemento x y cumplir con la condición *i.*,

$\times$	0	1	2
0	0	0	0
1	0		
2	0		

$\times$	0	1	2
0		1	
1	1	1	1
2		1	

$\times$	0	1	2
0			2
1			2
2	2	2	2

para la condición *ii*. tenemos dos opciones por cada una de las tablas anteriores, teniendo en cuenta que $x \neq y$, $y \neq z$ y $x \neq z$, así:

$\times$	0	1	2
0	0	0	0
1	0	1	
2	0		1

$\times$	0	1	2
0	0	0	0
1	0	2	
2	0		2

$\times$	0	1	2
0	0	1	
1	1	1	1
2		1	0

$\times$	0	1	2
0	2	1	
1	1	1	1
2		1	2

$\times$	0	1	2
0	0		2
1		0	2
2	2	2	2

$\times$	0	1	2
0	1		2
1		1	2
2	2	2	2

y con las dos últimas condiciones podemos completar las casillas que faltan en cada tabla, con lo que obtenemos las tablas 4, 5, 6, 7, 8, 9 que son las seis representaciones de la estructura $(Z_3, \times)$.

Una segunda opción es:

2. Existen dos elementos diferentes x y z en M $= \{0, 1, 2\}$, tales que para todo y en M:

i. $xy = yx = y$

ii. $yz = zy = z$

iii. $yy = x$ con $y \neq z$

Ejercicios

1. *Verifique que la opción 2 caracteriza* $(Z_3, \times)$ *salvo isomorfismos.*

2. *Encuentre otras caracterizaciones de la estructura* $(Z_3, \times)$.

2.7. El campo $(Z_3, +, \times)$

Una relación entre las estructuras $(\{0,1,2\},+)$ y $(\{0,1,2\},\otimes)$ es que la operación $\otimes$ es distributiva con respecto a la operación $+$, al igual que la operación $\otimes'$ es distributiva respecto a la operación $+$, $\otimes'''$ distribuye respecto a $\diamondsuit$, $\otimes^v$ distribuye respecto a $\diamondsuit$, $\otimes''$ distribuye respecto a ∇ y $\otimes'^v$ distribuye respecto a ∇.

Las relaciones entre las diferentes estructuras nos permiten concluir que

$$(\{0,1,2\},+,\otimes)$$
$$(\{0,1,2\},+,\otimes')$$
$$(\{0,1,2\},\diamondsuit,\otimes''')$$
$$(\{0,1,2\},\diamondsuit,\otimes^v)$$
$$(\{0,1,2\},\nabla,\otimes'')$$
$$(\{0,1,2\},\nabla,\otimes'^v)$$

tienen estructura de campo.

Finalmente, llamaremos *el campo* $(Z_3, +, \times)$, a la estructura formada por un conjunto que aquí notaremos Z_3, cuyos elementos nombramos 0, 1, 2, pero que puede ser cualquier conjunto con tres elementos, junto con dos operaciones que aquí notamos $+$ y $\times$ (que igual pueden nombrarse de otra manera), de manera que $(Z_3, +)$ sea un grupo abeliano; la operación $\times$ sea asociativa, tenga un elemento idéntico, todo elemento diferente del elemento idéntico de la operación $+$ tenga un inverso multiplicativo y que sea distributiva con respecto a $+$. Cada uno de los ejemplos de la estructura que mencionamos anteriormente es *una representación* de ella.

2.7.1. Ecuaciones en $(Z_3, +, \times)$

$(Z_3, +, \times)$ es un campo, al igual que los números reales, y por lo tanto *los procedimientos algebraicos que efectuamos para resolver ecuaciones de primer grado con una o varias incógnitas son los mismos.*

2.7.1.1. Ecuaciones de primer grado

En $(Z_3, +, \times)$ podemos realizar todas las sumas, las restas, las multiplicaciones y todas las divisiones posibles, excepto dividir por 0, como en los números reales; pues con la existencia de un inverso para cada elemento respecto a la operación $+$, podemos definir la *sustracción* como:

$$a - b = a + (-b)$$

para todo a, b en Z_3.

Con la ayuda de la existencia de un inverso respecto a la operación $\times$, para cada elemento distinto del elemento idéntico de $+$, definimos la *división* como:

$$\frac{a}{b} = a \times \left(\frac{1}{b}\right) = a \times b^{-1}$$

para todo a, b en Z_3 con $b \neq 0$.

Para resolver cualquier ecuación de primer grado con una incógnita, como por ejemplo:

$$(2 \times x) + 1 = 2$$

sumamos a ambos lados de la igualdad el inverso de 1 respecto a la operación $+$, o sea -1 que en nuestro caso es 2:

$$(2 \times x) + (1 + 2) = 2 + 2$$

asociamos y realizamos las operaciones, con lo que resulta:

$$(2 \times x) + 0 = 1$$

o sea

$$2 \times x = 1$$

Dividimos a ambos lados entre 2 y tenemos que

$$x = \frac{1}{2} = 2$$

Para verificar que la solución es correcta, reemplazamos $x = 2$ en

$$(2 \times x) + 1 = 2$$

y obtenemos

$$(2 \times 2) + 1 = 1 + 1 = 2$$

¡como debe ser!

2.7.1.2. Ecuaciones simultáneas con dos incógnitas

De manera similar, los métodos desarrollados en R para resolver ecuaciones simultáneas con dos o más incógnitas, funcionan en $(Z_3, +, \times)$, por ejemplo, para resolver el sistema de dos ecuaciones con dos incógnitas:

$$(2 \times x) + y = 2$$

$$-x + (2 \times y) = -2$$

reemplazamos $-2 = 1$ y aplicamos el método de reducción; multiplicamos la segunda ecuación por 2

$$(2 \times x) + y = 2$$

$$(-2 \times x) + y = 2$$

sumamos las dos ecuaciones y conseguimos:

$$2 \times y = 1$$

o sea

$$y = \frac{1}{2} = 2$$

Para encontrar el valor de x, reemplazamos y en la ecuación:

$$(2 \times x) + y = 2$$

y obtenemos

$$(2 \times x) + 2 = 2$$

sumamos el inverso de 2 respecto a la operación $+$, es decir, 1 en ambos lados,

$$2 \times x = 0$$

y entonces

$$x = 0.$$

Para verificar el resultado reemplazamos los valores obtenidos en las ecuaciones originales:

$$(2 \times 0) + 2 = 2$$

$$-0 + (2 \times 2) = 1 = -2.$$

2.7.1.3. Ecuaciones de segundo grado

La ecuación cuadrática:

$$ax^2 + bx + c = 0$$

en el conjunto de los números reales, la podemos resolver utilizando la fórmula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

sin embargo, si intentamos aplicarla aquí, aparecen varios problemas; por ejemplo, ¿qué significa el exponente 2 del elemento b?, ¿es diferente del 2 en el denominador del lado derecho de la igualdad?, también tenemos que en Z_3 no existe 4, entonces ¿debemos interpretarlo como 2×2?

Supongamos que x^2 significa $x \times x$ y procuremos resolver la ecuación

$$x^2 + (2 \times x) + 2 = 0$$

Podemos escribir esta expresión como:

$$(x^2 + (2 \times x) + 1) + 1 = 0$$

y como es válida la propiedad distributiva de $\times$ con respecto a $+$, tenemos que,

$$(x+1)^2 = (x+1) \times (x+1) = x^2 + x + x + 1 = x^2 + (2 \times x) + 1$$

luego, podemos factorizar[7] $(x^2 + (2 \times x) + 1) + 1 = 0$, como:

$$(x+1)^2 + 1 = 0$$

de donde

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

pero ¡hasta aquí llegamos! Porque en $(Z_3, +, \times)$ no existe un número x cuyo cuadrado, $x \times x = x^2$ sea 2, es decir no existe $\sqrt{2}$.

Ejercicio

El método para resolver ecuaciones de segundo grado se deja usar en otros ejemplos cuyas soluciones sí existen, explore algunos casos.

[7]Debemos tener cuidado con hacer afirmaciones en conjuntos de números diferentes a los números reales, pues aunque los símbolos sean los mismos, los significados pueden variar, por ejemplo, en el conjunto Z_2, del capítulo anterior, $(x+1)^2 = (x+1) \times (x+1) = (x^2 + x + x + 1) = (x^2 + 1)$!

2.8. Otras estructuras con tres elementos

2.8.1. A partir de modificaciones de la condición de isomorfismo

Modifiquemos la condición de isomorfismo entre dos estructuras, como lo hicimos en el capítulo anterior, pero ahora usando combinaciones de una de las seis funciones biyectivas mencionadas anteriormente y la operación +, para construir otras operaciones en un conjunto sin estructura, por ejemplo, si (A, +) es una estructura, B un conjunto y f una función biyectiva de A en B, definimos la operación $\oplus$ en B eliminando solo la función inversa de f en el primer elemento que se opera, con lo que obtenemos que:

$$a \oplus b = f(a + f^{-1}(b))$$

para todo par de elementos a, b de B.

De acuerdo con lo anterior, si utilizamos la función f_1 y la operación + obtenemos las siguientes operaciones con sus respectivas tablas:

1. $x * y = f_1(x + y)$

$*$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Tabla 16

2. $x *' y = f_1(x + f_1(y))$

$*'$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Tabla 17

3. $x *'' y = f_1(f_1(x) + y)$

$*''$	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

Tabla 18

En los casos siguientes las nuevas operaciones coinciden con las ya obtenidas:

4. $x * y = f_1(x) + f_1(y)$
5. $x *'' y = x + f_1(y)$
6. $x *' y = f_1(x) + y$

Empleando la función f_1 y la operación $\diamondsuit$ obtenemos las siguientes operaciones y sus respectivas tablas:

1. $x \blacktriangle y = f_1(x \diamondsuit y)$

$\blacktriangle$	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

Tabla 19

2. $x \blacktriangle' y = f_1(x \diamondsuit f_1(y))$

$\blacktriangle'$	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

Tabla 20

3. $x \blacktriangle'' y = f_1(f_1(x) \diamondsuit y)$

$\blacktriangle''$	0	1	2
0	1	0	2
1	2	1	0
2	0	2	1

Tabla 21

4. $x\blacktriangle'''y = f_1(x)\diamondsuit f_1(y)$

$\blacktriangle'''$	0	1	2
0	2	1	0
1	1	0	2
2	0	2	1

Tabla 22

5. $x\blacktriangle'^{v}y = x\diamondsuit f_1(y)$

$\blacktriangle'^{v}$	0	1	2
0	2	1	0
1	0	2	1
2	1	0	2

Tabla 23

6. $x\blacktriangle^{v}y = f_1(x)\diamondsuit y$

$\blacktriangle^{v}$	0	1	2
0	2	0	1
1	1	2	0
2	0	1	2

Tabla 24

Y si utilizamos la función f_1 y la operación ∇ conseguimos las mismas operaciones que resultaron al aplicar la función f_1 y la operación $\diamondsuit$:

1. $x\blacktriangle'''y = f_1(x\nabla y)$

2. $x\blacktriangle^v y = f_1(x\nabla f_1(y))$
3. $x\blacktriangle'^v y = f_1(f_1(x)\nabla y)$
4. $x\blacktriangle y = f_1(x)\nabla f_1(y)$
5. $x\blacktriangle'' y = x\nabla f_1(y)$
6. $x\blacktriangle' y = f_1(x)\nabla y$

Podemos también intercambiar el lugar de x e y, pero debido a que las operaciones $+$, $\diamondsuit$, y ∇ que empleamos en el proceso, son conmutativas, obtenemos las mismas operaciones anteriores.

Con los procedimientos realizados hemos obtenido 9 estructuras, pero ¿algebraicamente todas son distintas entre sí? Para ello tomamos dos estructuras y miramos si podemos definir entre ellas una función biyectiva f, que cumpla la condición mencionada en la sección 2.4.

Para ejemplificar, podemos elegir una de las estructuras, por ejemplo $(\{0,1,2\}, *')$ y en la tabla aplicamos una de las seis funciones biyectivas a cada elemento de los encabezados y en cada casilla al elemento resultante de la operación $*'$, por ejemplo, si utilizamos la función f_2, cambiamos los nombres y reorganizamos, obtenemos la operación $\blacktriangle^v$:

	2	1	0
2	2	1	0
1	0	2	1
0	1	0	2

$\blacktriangle^v$	0	1	2
0	2	0	1
1	1	2	0
2	0	1	2

Tabla 24

Con la función f_1 obtenemos la misma operación $*'$, con la función f_3 obtenemos la operación $\blacktriangle'$, con f_4 obtenemos $\blacktriangle^v$ y f_5 conseguimos $\blacktriangle'$. Es decir tenemos que

$$(\{0,1,2\}, *')$$
$$(\{0,1,2\}, \blacktriangle')$$
$$(\{0,1,2\}, \blacktriangle^v)$$

son representaciones de la misma estructura.

Algunas propiedades que cumple esta estructura son la unipotencia, sistema de reglas a derecha, identidad II de Schweitzer, permutable a izquierda, transitiva izquierda y bisimétrica.

Al aplicar este procedimiento a:

$$(\{0,1,2\},*'') \quad (\{0,1,2\},\blacktriangle'') \quad \text{y} \quad (\{0,1,2\},\blacktriangle'^{v})$$

obtenemos una misma estructura no isomorfa a la anterior.

Algunas propiedades que cumple esta estructura son la unipotencia, sistema de reglas a izquierda, identidad I de Schweitzer, identidad de Tarski, identidad I de Abel–Graβmann, permutable a derecha, transitiva a derecha y bisimétrica.

También tenemos que $(\{0,1,2\},\blacktriangle)$ y $(\{0,1,2\},\blacktriangle''')$ son isomorfas y algunas propiedades que cumplen son la conmutativa, sistema de reglas a izquierda, sistema de reglas a derecha, semisimétrica a izquierda, semisimétrica a derecha, elástica y bisimétrica.

Mientras que $(\{0,1,2\},*)$ define una estructura, que no es isomorfa con alguna de las 3 estructuras obtenidas. Ella cumple las propiedades conmutativa, idempotente, sistema de reglas a izquierda, sistema de reglas a derecha, semisimétrica a izquierda, semisimétrica a derecha, elástica, autodistributiva a izquierda, autodistributiva a derecha, autodistributiva a izquierda abeliana, autodistributiva a derecha abeliana y bisimétrica.

En resumen, modificando la condición de isomorfismo utilizando la función f_1 y la operación $+$, hemos obtenido 4 estructuras algebraicamente diferentes.

Caractericemos ahora cada estructura buscando algunas propiedades que determinen sus tablas, por ejemplo, las condiciones:

1. $(\forall x,y,z)((x\neq y\wedge x\neq z\wedge y\neq z)\wedge(xx=x)\wedge(xy=yx=z))$

determinan la estructura de $(\{0,1,2\},*)$.

2. $(\exists x)(\forall y,z)((x\neq y\wedge x\neq z\wedge y\neq z)\wedge(xx=x=yy)\wedge(xy=y\wedge yx=z\wedge yz=y))$

determinan la estructura de $(\{0,1,2\},*')$ y sus otras representaciones.

3. $(\exists x)(\forall y,z)((x\neq y\wedge x\neq z\wedge y\neq z)\wedge(xx=x=yy)\wedge(xy=z\wedge yx=y\wedge yz=z))$

determinan la estructura de $(\{0,1,2\},*'')$ y sus otras representaciones.

4. $(\forall x,y)((x\neq y)\wedge(xx=y)\wedge(xy=yx\wedge xy\neq xx\wedge xy\neq yy))$

determinan la estructura de $(\{0,1,2\},\blacktriangle)$ y sus otras representaciones.

Ejercicios

1. *Con cada una de las 9 operaciones obtenidas modifique la condición de isomorfismo y establezca cuántas estructuras se definen.*

2. *Utilice la función f_5 y otra representación de $(Z_3, +)$ para modificar la condición de isomorfismo y obtener otras operaciones con tres elementos.*

3. *Utilice las funciones f_4, f_2 y una representación de $(Z_3, \times)$ y modifique la condición de isomorfismo para obtener nuevas operaciones con tres elementos.*

2.8.2. A partir de los axiomas que definen estructuras con dos elementos

Cuando estudiamos las estructuras definidas sobre un conjunto con dos elementos, nos resultaron diez estructuras salvo isomorfismos, que caracterizamos con diez conjuntos de axiomas; usémoslos para construir estructuras con tres elementos.

Por ejemplo, el axioma A9. $xy = x$, que define la primera proyección, π_1, en un conjunto con dos elementos, también define la estructura:

π_1	0	1	2
0	0	0	0
1	1	1	1
2	2	2	2

Tabla 25

que llamaremos primera proyección y la notamos de la misma forma.

Análogamente el axioma A10. $xy = y$ define la segunda proyección π_2:

π_2	0	1	2
0	0	1	2
1	0	1	2
2	0	1	2

Tabla 26

Si escogemos como axiomas:

A1. $xx = x$ (Idempotencia)

A2. $xy = yx$ (Conmutativa)

que determinan las operaciones conjunción $\wedge$, y disyunción $\vee$ de la lógica usual, aplicadas a un conjunto con tres elementos determinan 27 operaciones, puesto que A1 fija la diagonal principal y A2 deja tres casillas libres y en cada una de ellas tenemos 3 opciones para completar:

	0	1	2
0	0	a	b
1	a	1	c
2	b	c	2

Por tanto determinemos cuáles estructuras resultan salvo isomorfismos; para ello asignémosle un valor para a, b, c y apliquemos las funciones biyectivas f_1, f_2, f_3, f_4 y f_5 para copiar la operación.

Opción I: si escogemos $a = 0 = b$ y $c = 1$, tenemos:

$\spadesuit$	0	1	2
0	0	0	0
1	0	1	1
2	0	1	2

Tabla 27

y utilizando las funciones biyectivas para copiar la operación, obtenemos las siguientes estructuras isomorfas con $(\{0, 1, 2\}, \spadesuit)$:

1. $x \spadesuit' y = f_1(f_1(x) \spadesuit f_1(y))$

$\spadesuit'$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	2

Tabla 28

2. $x \spadesuit'' y = f_2(f_2(x) \spadesuit f_2(y))$

$\spadesuit''$	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

Tabla 29

3. $x\spadesuit'''y = f_3(f_3(x)\spadesuit f_3(y))$

$\spadesuit'''$	0	1	2
0	0	1	0
1	1	1	1
2	0	1	2

Tabla 30

4. $x\spadesuit'^{v}y = f_4(f_5(x)\spadesuit f_5(y))$

$\spadesuit'^{v}$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Tabla 31

5. $x\spadesuit^{v}y = f_5(f_4(x)\spadesuit f_4(y))$

$\spadesuit^{v}$	0	1	2
0	0	1	2
1	1	1	1
2	2	1	2

Tabla 32

La estructura de $(\{0,1,2\},\spadesuit)$ y por supuesto todas sus representaciones, cumplen otras propiedades como la asociativa, elemento neutro, identidad I y II de Stein, identidad I de Schröder, elástica, asociativa cíclica I y II,

identidad I y II de Abel – Graβmann, permutable a izquierda y a derecha, producto reducido, autodistributiva a izquierda y a derecha, autodistributiva a izquierda abeliana y a derecha abeliana y bisimétrica[8].

Opción II: si escogemos $a = 2$ y $b = 1 = c$, tenemos:

♥	0	1	2
0	0	2	1
1	2	1	1
2	1	1	2

Tabla 33

Utilizando las funciones biyectivas para copiar la operación, obtenemos las siguientes estructuras isomorfas con $(\{0, 1, 2\}, \heartsuit)$:

1. $x\heartsuit' y = f_1(f_1(x)\heartsuit f_1(y))$

♥′	0	1	2
0	0	2	1
1	2	1	2
2	1	2	2

Tabla 34

2. $x\heartsuit'' y = f_2(f_2(x)\heartsuit f_2(y))$

♥″	0	1	2
0	0	1	1
1	1	1	0
2	1	0	2

Tabla 35

3. $x\heartsuit''' y = f_3(f_3(x)\heartsuit f_3(y))$

[8]Estas propiedades pueden verificarse con el programa *Álgebra finita.*

$\heartsuit'''$	0	1	2
0	0	2	0
1	2	1	0
2	0	0	2

Tabla 36

4. $x\heartsuit'^{v}y = f_4(f_5(x)\heartsuit f_5(y))$

$\heartsuit'^{v}$	0	1	2
0	0	0	1
1	0	1	0
2	1	0	2

Tabla 37

5. $x\heartsuit^{v}y = f_5(f_4(x)\heartsuit f_4(y))$

$\heartsuit^{v}$	0	1	2
0	0	2	2
1	2	1	0
2	2	0	2

Tabla 38

La estructura de $(\{0,1,2\},\heartsuit)$ y, por supuesto, sus representaciones cumplen además de las propiedades idempotencia y conmutativa, la propiedad elástica.

Opción III: si escogemos $a = b = c = 1$, tenemos:

$\triangle$	0	1	2
0	0	1	1
1	1	1	1
2	1	1	2

Tabla 39

Recurriendo a las funciones biyectivas para copiar la operación, obtenemos que las siguientes estructuras son isomorfas con $(\{0,1,2\},\triangle)$:

1. $x\triangle' y = f_1(f_1(x)\triangle f_1(y)) = f_5(f_4(x)\triangle f_4(y))$

$\triangle'$	0	1	2
0	0	2	2
1	2	1	2
2	2	2	2

Tabla 40

2. $x\triangle y = f_2(f_2(x)\triangle f_2(y))$
3. $x\triangle'' y = f_3(f_3(x)\triangle f_3(y)) = f_4(f_5(x)\triangle f_5(y))$

$\triangle''$	0	1	2
0	0	0	0
1	0	1	0
2	0	0	2

Tabla 41

La estructura de $(\{0,1,2\},\triangle)$ y sus otras representaciones, cumplen otras propiedades como la asociativa, elástica, identidades I y II de Stein, identidad I de Schröder, asociativa cíclica I y II, identidades I y II de Abel – Graßmann, permutable a izquierda y a derecha, producto reducido, autodistributiva a izquierda y a derecha, autodistributiva a izquierda abeliana y a derecha abeliana y la bisimétrica.

Opción IV: si escogemos $a = 0$, $b = 1$ y $c = 2$, tenemos:

$\ominus$	0	1	2
0	0	0	1
1	0	1	2
2	1	2	2

Tabla 42

Si empleamos las funciones biyectivas para copiar la operación, obtenemos las siguientes estructuras isomorfas con $(\{0,1,2\},\ominus)$:

1. $x \ominus' y = f_1(f_1(x) \ominus f_1(y)) = f_5(f_4(x) \ominus f_4(y))$

$\ominus'$	0	1	2
0	0	2	0
1	2	1	1
2	0	1	2

Tabla 43

2. $x \ominus y = f_2(f_2(x) \ominus f_2(y))$

3. $x \ominus'' y = f_3(f_3(x) \ominus f_3(y)) = f_4(f_5(x) \ominus f_5(y))$

$\ominus''$	0	1	2
0	0	1	2
1	1	1	0
2	2	0	2

Tabla 44

La estructura de $(\{0,1,2\}, \ominus)$ y sus representaciones, cumplen otras propiedades como la existencia de elemento idéntico, existencia de elementos inversos y la elástica, pero no es asociativa; lo que demuestra que la propiedad asociativa es independiente de las otras que definen la estructura de grupo.

Opción V: si escogemos $a = 2$, $b = 1$ y $c = 0$, tenemos:

$\square$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Tabla 45

y si utilizamos la funciones para encontrar otras representaciones de la estructura de $(\{0,1,2\}, \square)$ obtenemos que es la única en el conjunto $\{0,1,2\}$ y que cumple otras propiedades como el sistema de reglas a izquierda y a derecha, semisimétrica a izquierda y a derecha, elástica, autodistributiva a izquierda y a derecha, autodistributiva a izquierda abeliana y a derecha abeliana y la bisimétrica.

Opción VI: si escogemos $a = 1$, $b = 0$ y $c = 2$, tenemos:

$\bigstar$	0	1	2
0	0	1	0
1	1	1	2
2	0	2	2

Tabla 46

Usando las funciones para encontrar estructuras isomorfas con $(\{0, 1, 2\}, \bigstar)$ obtenemos las siguientes:

1. $x \bigstar' y = f_1(f_1(x) \bigstar f_1(y)) = f_2(f_2(x) \bigstar f_2(y)) = f_3(f_3(x) \bigstar f_3(y))$

$\bigstar'$	0	1	2
0	0	0	2
1	0	1	1
2	2	1	2

Tabla 47

2. $x \bigstar y = f_4(f_5(x) \bigstar f_5(y)) = f_5(f_4(x) \bigstar f_4(y))$

La estructura de $(\{0, 1, 2\}, \bigstar)$ y sus representaciones, cumplen también la identidad I y II de Stein, identidad I de Schröder y la propiedad elástica.

Opción VII: si escogemos $a = 0$, $b = 1 = c$, tenemos:

$\maltese$	0	1	2
0	0	0	1
1	0	1	1
2	1	1	2

Tabla 48

cuyas copias son:

1. $x \maltese' y = f_1(f_1(x) \maltese f_1(y))$

$✠'$	0	1	2
0	0	2	0
1	2	1	2
2	0	2	2

Tabla 49

2. $x✠''y = f_2(f_2(x)✠f_2(y))$

$✠''$	0	1	2
0	0	1	1
1	1	1	2
2	1	2	2

Tabla 50

3. $x✠'''y = f_3(f_3(x)✠f_3(y))$

$✠'''$	0	1	2
0	0	1	0
1	1	1	0
2	0	0	2

Tabla 51

4. $x✠'^{v}y = f_4(f_5(x)✠f_5(y))$

$✠'^{v}$	0	1	2
0	0	0	2
1	0	1	0
2	2	0	2

Tabla 52

5. $x✠^{v}y = f_5(f_4(x)✠f_4(y))$

✠^{v}	0	1	2
0	0	2	2
1	2	1	1
2	2	1	2

Tabla 53

La estructura de $(\{0,1,2\}, ✠)$ y sus representaciones, cumplen la propiedad elástica.

Partiendo de los axiomas A1 y A2 hemos obtenido 6 estructuras algebraicamente diferentes, pero para caracterizarlas de manera única, salvo isomorfismos, es necesario agregar otros axiomas, por ejemplo, las condiciones:

Existe x, para todo y, z en $\{0,1,2\}$ de manera que se cumple:

A3′. $xy = xz \neq x$, $yz = x$, $x \neq y$, $x \neq z$, $y \neq z$

junto con A1 y A2, determinan las operaciones que resultaron en la opción II.

Las condiciones

Existe z, para todo x, y en $\{0,1,2\}$ de manera que se cumple:

A3″. $xy = z$, $x \neq y$

junto con A1 y A2, determinan las operaciones que resultaron en la opción III.

Y las condiciones

Para todo x, y, z en $\{0,1,2\}$ se cumple que:

A3‴. $xy = z$, $x \neq y$, $x \neq z$, $y \neq z$

junto con A1 y A2, determinan la operación que resultó en la opción V.

La estructura de la opción III que determinan los axiomas A1, A2 y A3″, cumple algunas propiedades mencionadas anteriormente, que pueden deducirse de estos. Por ejemplo, derivemos las propiedades identidad de Stein I, II y la asociativa cíclica I:

T1. *Identidad I de Stein*: para todo x, y en el conjunto X $= \{0,1,2\}$, $x(xy) = yx$.

Si $x \neq y$, el axioma A3″ garantiza que el resultado de operar cualquier par de elementos distintos es el mismo, por tanto tenemos que existe z en X tal que:

$$x(xy) = xz$$

si $x \neq z$ por A3″

$$x(xy) = xz = z = yx,$$

y si $x = z$ por A1 y A3$''$

$$x(xy) = xz = xx = x = yx.$$

Si $x = y$, por el axioma A1 tenemos que

$$x(xx) = xx = x = xx.$$

T2. *Identidad II de Stein*: para todo x, y en el conjunto X $= \{0, 1, 2\}$, $x(yx) = (yx)y$.

$$\begin{aligned} x(yx) &= x(xy) && \text{Por A2} \\ &= yx && \text{Identidad I de Stein} \\ &= xy && \text{Por A2} \\ &= y(yx) && \text{Identidad I de Stein} \\ &= (yx)y && \text{Por A2} \end{aligned}$$

T3. *Asociativa cíclica I*: para todo x, y, z en el conjunto X $= \{0, 1, 2\}$, $x(yz) = z(xy)$.

Si $y = z$ tenemos que

$$\begin{aligned} x(yz) &= x(yy) \\ &= xy && \text{Por A1} \\ &= y(yx) && \text{Identidad I de Stein} \\ &= y(xy) && \text{Por A2} \end{aligned}$$

Si $x = y$

$$\begin{aligned} x(yz) &= x(xz) \\ &= zx && \text{Identidad I de Stein} \\ &= z(xx) && \text{Por A1} \\ &= z(xy) \end{aligned}$$

Si $x = z$

$$\begin{aligned} x(yz) &= x(yx) \\ &= x(xy) && \text{Por A2} \\ &= z(xy) \end{aligned}$$

si $y \neq z$, el axioma A3$''$ garantiza que existe u en X tal que:

$$x(yz) = xu$$

Si $x = u$

$$\begin{aligned} x(yz) = xu &= xx \\ &= yz && \text{Por A1 y A3}'' \\ &= z(zy) && \text{Identidad I de Stein} \\ &= zx && \text{Por A3}''. \end{aligned}$$

y si $x \neq y$

$$\begin{aligned} x(yz) &= zx \\ &= z(xy) && \text{Por A3}'' \end{aligned}$$

Si $x = y$

$$\begin{aligned} x(yz) &= zx \\ &= z(xx) && \text{Por A1} \\ &= z(xy) \end{aligned}$$

Si $x \neq u$

$$\begin{aligned} x(yz) = xu &= u && \text{Por A3}'' \\ &= yz && \text{Por A3}'' \\ &= z(zy) && \text{Identidad I de Stein} \\ &= zu \end{aligned}$$

y si $x \neq y$

$$\begin{aligned} x(yz) &= zu \\ &= z(xy) && \text{Por A3}'' \end{aligned}$$

Si $x = y$ entonces $y \neq u$ pues $x \neq u$, y como X tiene tres elementos $z = u$, por tanto

$$\begin{aligned} x(yz) &= zu \\ &= z && \text{Por A1} \\ &= zx && \text{Por A3}'' \\ &= z(xx) && \text{Por A1} \\ &= z(xy) \end{aligned}$$

La propiedad elástica se deduce del axioma A2 al igual que sucedió en la actividad anterior con las estructuras conmutativas con dos elementos, pues su demostración es independiente del número de elementos del conjunto.

La propiedad asociativa, identidad de Abel – Graßmann I y asociativa cíclica II se deducen de la asociativa cíclica I y del axioma A2; la identidad I de Schröder se deduce de la identidad I de Stein y de A2; la identidad de Abel – Graßmann II se deduce de Identidad de Abel – Graßmann I y de A2; la propiedad permutable a izquierda se deduce de la asociativa cíclica II y del axioma A2; la propiedad permutable a derecha se deduce de la propiedad permutable a izquierda y del axioma A2, y el producto reducido se deduce de la propiedad permutable a izquierda y de A2.

Ejercicios

1. *Termine las demostraciones de las propiedades que cumplen las estructuras de la opción III.*

2. *Para las estructuras de las opciones I, IV, VI, VII, agregue condiciones para caracterizarlas de manera única, salvo isomorfismos.*

3. *Escoja otras propiedades básicas que definen una estructura con dos elementos, aplíquelas en un conjunto con tres elementos, determine cuántas estructuras resultan y clasifíquelas salvo isomorfismos.*

2.8.3. A partir de relaciones de orden

En el estudio de las estructuras finitas hecho hasta ahora no hemos mencionado a las relaciones de orden, tan importantes en los conjuntos numéricos como los números naturales, enteros, racionales o reales.

Estudiaremos aquí las relaciones de orden desde otro punto de vista, no para ordenar un conjunto donde están definidas unas operaciones y ver si son compatibles o no, sino para generar operaciones a partir de relaciones de orden. Precisaremos inicialmente algunos términos y luego construiremos las operaciones.

2.8.3.1. Relaciones de Orden

Una *relación de orden*[9] en un conjunto X, que notamos $\leq$, es una relación en X que cumple las siguientes condiciones:

[9]Este tema sigue los lineamientos propuestos en LUQUE, Carlos; DONADO, Alberto y PAÉZ, Jorge. H-conjuntos (una generalización de la noción de conjunto). XIV Coloquio

1. Reflexiva: $a \leq a$ para todo $a \in \mathrm{X}$

2. Antisimétrica: Si $a \leq b$ y $b \leq a$ entonces $a = b$

3. Transitiva: Si $a \leq b$ y $b \leq c$ entonces $a \leq c$

Para cada relación de orden existe una representación gráfica conocida como el *diagrama de Hasse* de la relación y que consiste en dibujar un punto por cada elemento del conjunto y un segmento de línea recta ascendente entre los puntos que estén relacionados de modo que el punto para a quede encima del punto para b si $a < b$; es decir, que trazamos un segmento entre a y b si $a < b$ y no existe otro elemento x en A tal que $a < x < b$.

Ejemplos

1. El conjunto $\wp(\mathrm{X})$ de subconjuntos de un conjunto dado X, está ordenado por la relación de inclusión, $\mathrm{A} \subseteq \mathrm{B}$, si todo elemento de A es un elemento de B. Si $\mathrm{X} = \{a, b\}$ entonces $\wp(\mathrm{X}) = \{\varnothing, \{a\}, \{b\}, \mathrm{X}\}$ y el diagrama de Hasse correspondiente es:

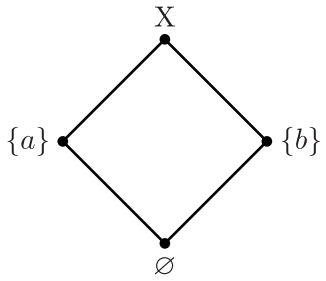


Figura 3

2. En el conjunto N de los números naturales definimos el orden $a \leq b$ si y solo si existe un natural c tal que $a + c = b$. El diagrama correspondiente es una cadena ascendente infinita de puntos enlazados por segmentos.

3. Si tenemos una relación de orden definida en un conjunto X, podemos definir una relación de orden en cualquiera de sus subconjuntos, usando el orden que tenían los elementos en el conjunto original. Por ejemplo el conjunto $\underline{n} = \{0, 1, 2, \ldots, n-1\}$ es un conjunto ordenado.

Distrital de Matemáticas y Estadística. Bogotá: Universidad Pedagógica Nacional, 1997. p. 1-49.

Naturalemente en un conjunto cualquiera podemos definir varios órdenes. Por ejemplo en un conjunto con cuatro elementos, $\underline{4} = \{0, 1, 2, 3\}$ podemos definir el orden del ejemplo 1. Reservaremos la notación $\underline{n}$ para el conjunto ordenado con n elementos y el orden aditivo usual de N.

2.8.3.2. Morfismos de conjuntos ordenados

Una función $f : (\mathrm{A}, \leq) \to (\mathrm{B}, \subseteq)$ entre dos conjuntos ordenados es un *morfismo de conjuntos ordenados* si para todo a y b en A tales que $a \leq b$ se tiene que $f(a) \subseteq f(b)$ en B. En el caso en que $a \leq b$ si y sólo si $f(a) \subseteq f(b)$ y f es sobre (se llama un *isomorfismo entre conjuntos ordenados*. En este caso las dos relaciones de orden son esencialmente la misma.

2.8.3.3. Retículos

Sea A un subconjunto no vacío de un conjunto ordenado X, si en X existen elementos z que sean mayores o iguales que todos los elementos de A les llamamos *cotas superiores* de A y si existe una *mínima cota superior* a ésta le llamamos el *supremo* de A, abreviado *sup*A y lo notamos $\vee$A. Si $\mathrm{A} = \{x, y\}$ escribimos $\vee\mathrm{A} = x \vee y$.

Más precisamente, $x = sup\mathrm{A}$ significa que $y \leq x$ para todo $y \in$ A y si $y \leq z$ para todo y en A, entonces $x \leq z$. De manera análoga, un elemento que sea el mayor de las cotas inferiores lo llamaremos el inf A. Lo notamos $\wedge$A, y si A es un conjunto con dos elementos x e y, escribimos $\wedge\mathrm{A} = x \wedge y$.

Un conjunto ordenado X donde exista *sup*A e infA para cualquier subconjunto A con dos elementos se llama un *retículo.*

Ejemplos

1. En el conjunto $\underline{2} = \{0, 1\}$ las tablas para $\wedge$ y $\vee$ son respectivamente:

$\wedge$	0	1
0	0	0
1	0	1

Tabla 54

$\vee$	0	1
0	0	1
1	1	1

Tabla 55

Estas son las conocidas conjunción y disyunción de la lógica de dos valores.

2. En $\underline{3} = \{0, 1, 2\}$ tenemos:

$\wedge$	0	1	2
0	0	0	0
1	0	1	1
2	0	1	2

Tabla 56

$\vee$	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

Tabla 57

3. El conjunto $\wp(X)$ ordenado por la relación de contenencia es un retículo donde el $sup\{A, B\}$ es la unión de A con B y el $inf\{A, B\}$ es la intersección de A con B.

2.8.3.3.1. Propiedades de los retículos

En un retículo la operación $\vee$ es asociativa puesto que si existe $sup(\mathrm{A} \cup \{y\})$ entonces también existe $sup(sup\mathrm{A}, y)$ para todo y en X y además son iguales; dicho de otra forma tenemos que para todo x, y, z, en un retículo cualquiera X se cumple:

$$(x \vee y) \vee z = x \vee (y \vee z).$$

Además que la existencia de supA para cualquier subconjunto finito A de X implica la existencia de $x \vee y$ para cualquier par x, y de sus elementos.

Razonando por analogía obtenemos que en cualquier retículo X, la operación $\wedge$ también es *asociativa*; además estas dos operaciones son *conmutativas, idempotentes* y *absorbentes* una respecto a la otra, esta última lo que significa es:

$$a \vee (b \wedge a) = a \qquad \text{y} \qquad a \wedge (b \vee a) = a$$

para todo a, b en el retículo. Todas estas afirmaciones se siguen de las definiciones.

2.8.3.3.2. Retículos distributivos

En un retículo cualquiera se cumplen las siguientes propiedades:

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

y

$$x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$$

como vemos, estas propiedades son parecidas en forma a las propiedades distributivas que se cumplen en las estructuras de campo, dominio de integridad y anillo, donde una operación distribuye con respecto a la otra; en este caso aparece como diferencia que el papel de las igualdades lo desempeñan las desigualdades. Demostremos la primera desigualdad:

Si en ambos lados de las desigualdades

$$y \wedge z \leq y$$

$$y \wedge z \leq z$$

operamos con x utilizando el operador $\vee$ obtenemos:

$$x \vee (y \wedge z) \leq x \vee y$$

$$x \vee (y \wedge z) \leq x \vee z$$

y como $(x \vee y) \wedge (x \vee z)$ es la máxima de las cotas inferiores, obtenemos que:

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

La segunda desigualdad tiene una demostración análoga. Un retículo en el que se tenga la igualdad en cada una de las propiedades anteriores, se llama un *retículo distributivo.*

Una característica de los retículos distributivos es la doble distributividad, lo que significa que si una operación es distributiva con respecto a la otra, entonces esta distribuye respecto a la primera; es decir, en un retículo distributivo cada una de las propiedades distributivas implica la otra, veamos:

Supongamos que:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

si aplicamos esta igualdad dos veces, a la expresión $(x \vee y) \wedge (x \vee z)$ obtenemos:

$$\begin{aligned}
(x \vee y) \wedge (x \vee z) &= [(x \vee y) \wedge x] \\
&\quad \vee [(x \vee y) \wedge z] && \text{Por hipótesis} \\
&= x \vee [(x \vee y) \wedge z] && \text{Por la propiedad absorbente} \\
&= x \vee [(x \wedge z) \vee (y \wedge z)] && \text{Por hipótesis} \\
&= [x \vee (x \wedge z)] \vee (y \wedge z) && \text{Por la propiedad asociativa de } \vee \\
&= x \vee (y \wedge z) && \text{Por la propiedad absorbente}
\end{aligned}$$

que es lo que deseábamos demostrar.

Otra forma de caracterizar la distributividad en un retículo la obtenemos de la propiedad cancelativa de las operaciones $\wedge$ y $\vee$; un *un retículo* X *es distributivo si y solo si las operaciones* $\wedge$ *y* $\vee$ *son cancelativas.*

Probemos que si un retículo X es distributivo y se cumplen:

$$x \vee z = y \vee z, x \wedge z = y \wedge z$$

entonces $x = y$.

$x = x \wedge (x \vee z)$	Por la propiedad absorbente
$= x \wedge (y \vee z)$	Por hipótesis
$= (x \wedge y) \vee (x \wedge z)$	Por la propiedad distributiva
$= (x \wedge y) \vee (y \wedge z)$	Por hipótesis
$= y \wedge (x \vee z)$	Por la propiedad distributiva
$= y \wedge (y \vee z)$	Por hipótesis
$= y$	Por la propiedad absorbente.

Ejercicio

Pruebe la afirmación recíproca.

2.8.3.3.3. Retículos Complementados

En el retículo $\underline{2}$ cuyas operaciones son la conjunción y la disyunción también está definida la negación para cada elemento x notada $\neg x$ y que tiene una relación con las operaciones mediante $x \vee \neg x = 1$ y $x \wedge \neg x = 0$.

Esta característica se copia al retículo $\wp$(X) con la noción de *complemento*, diciendo que un elemento x de X pertenece al complemento de un conjunto A que se nota A$'$ si no pertenece a A. También se cumple que:

$$A \cap A' = \varnothing \qquad \text{y} \qquad A \cup A' = \text{X}$$

La noción de complemento la podemos extender a otros retículos que tengan elemento mínimo 0 y elemento máximo 1.

Un elemento y de un retículo X es *un complemento* para el elemento x de X si cumple que

$$x \wedge y = 0 \qquad \text{y} \qquad x \vee y = 1$$

Un retículo donde todo elemento x tenga por lo menos un complemento lo llamamos *retículo complementado.*

Ejemplos

1. El retículo $\underline{2}$ es distributivo y complementado.

2. El retículo $\underline{3}$ es distributivo pero no complementado pues 1 no tiene complemento ya que si existiera debería tenerse que para algún z de $\underline{3}$:

$$z \wedge 1 = 0 \qquad \text{y} \qquad z \vee 1 = 2$$

pues el elemento máximo en $\underline{3}$ es 2, y el mínimo es 0, pero el único z que cumple la primera condición es el 0, y la otra el 2.

3. No siempre los complementos son únicos, en el retículo M_3

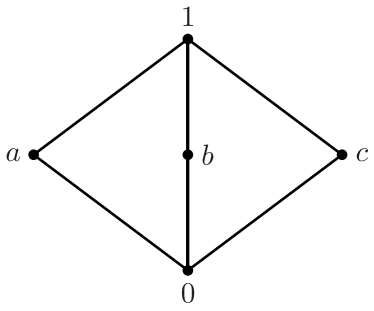


Figura 4

cada uno de los elementos a, b y c es complemento de los otros dos, en particular b y c son complementos de a.

Un retículo donde cada elemento tenga un único complemento se llama *únicamente complementado*. Para que un retículo complementado sea únicamente complementado es condición suficiente que las operaciones $\wedge$ y $\vee$ sean cancelativas.

Para probarlo, supongamos que en el retículo distributivo X, x' y x'' son dos complementos de x, por tanto las igualdades:

$$x' \vee x = x'' \vee x \qquad \text{y} \qquad x' \wedge x = x'' \vee x$$

implican la igualdad de los complementos.

Otra forma de ver esta unicidad es la siguiente:

$$x'' = x'' \wedge 1 = x'' \wedge (x' \vee x) = (x'' \wedge x') \vee (x'' \wedge x) = (x'' \wedge x') \vee 0 = x'' \wedge x'$$

y de la misma manera $x' = x' \wedge x''$. Luego $x'' = x'$.

En un retículo únicamente complementado el complemento de x se nota x'; en ellos se cumple:

1. $(x \wedge y)' = x' \vee y'$
2. $(x \vee y)' = x' \wedge y'$
3. $(x')' = x$

Un retículo distributivo y complementado se llama *álgebra de Boole*[10].

2.8.3.4. Funciones adjuntas

Sean X y Y retículos con 0 y 1, $f : \mathrm{X} \to \mathrm{Y}$ y $g : \mathrm{Y} \to \mathrm{X}$ funciones tales que para todo x en X y y en Y se tiene que:

$$f(x) \leq y \text{ si y solo si } x \leq g(y)$$

La función g se llama *adjunta a derecha* de f. También f es llamada la *adjunta a izquierda* de g[11].

Otra caracterización equivalente a la definición de que f es adjunta a derecha de g es:
a. Para todo x en X,

$$x \leq g(f(x))$$

b. Para todo y en Y

$$f(g(y)) \leq y.$$

c. f y g son morfismos de conjuntos ordenados.

Para probar la equivalencia, demostremos que la definición implica las tres condiciones:
a. Reemplazando en la definición $y = f(x)$ tenemos que

$$f(x) \leq f(x) \text{ si y solo si } x \leq g(f(x)).$$

b. Reemplazando en la definición $x = g(y)$ tenemos que

$$f(g(y)) \leq y \text{ si y solo si } g(y) \leq g(y).$$

c. Si x_1, x_2 son elementos de X y suponemos que $x_1 \leq x_2$ entonces por *a*.

$$x_1 \leq x_2 \leq g(f(x_2))$$

[10]En el caso particular de $\underline{2}$ el complemento de p corresponde a $\neg p$.
[11]RUIZ, Carlos. Teoría de la adjunción. Trabajo de año sabático. Bogotá: Universidad Nacional, 1989. p. 1-3.

o sea

$$x_1 \leq g(f(x_2))$$

y por la definición

$$f(x_1) \leq f(x_2).$$

Por lo tanto f es un morfismo de conjuntos ordenados.

Para ver que g también lo es, supongamos que y_1, y_2 son elementos de Y y que $y_1 \leq y_2$ entonces por b,

$$f(g(y_1)) \leq y_1 \leq y_2$$

es decir

$$f(g(y_1)) \leq y_2$$

y por la definición

$$g(y_1) \leq g(y_2).$$

Ahora probemos que las tres condiciones implican la definición:

Suponemos que para todo x en X y y en Y se tiene que:

$$f(x) \leq y$$

y como g es morfismo de conjuntos ordenados

$$g(f(x)) \leq g(y)$$

y por $a.$ tenemos que

$$x \leq g(f(x))$$

por tanto

$$x \leq g(y).$$

Recíprocamente, suponemos que para todo x en X y y en Y se tiene que:

$$x \leq g(y)$$

y como f es morfismo de conjuntos ordenados

$$f(x) \leq f(g(y))$$

y por $b.$ tenemos que

$$f(x) \leq y.$$

Una forma práctica para construir la función adjunta a derecha g de una función dada $f : X \to Y$, en el caso en que exista, es

$$g(y) = sup\{x \in \mathrm{X} : f(x) \leq y\}.$$

Sea $y \in \mathrm{Y}$, si $x \in \mathrm{X}$ es tal que $f(x) \leq y$ entonces, por la definición de función adjunta

$$x \leq g(y)$$

por lo tanto $g(y)$ es una cota superior de $\{x \in X : f(x) \leq y\}$. Ahora supongamos que para todos los $x \in \mathrm{X}$, tales que $f(x) \leq y$, se cumple que $x \leq t$. Como por $b.$ se tiene que

$$f(g(y)) \leq y$$

entonces $g(y)$ cumple las condiciones para pertenecer al conjunto $\{x \in X : f(x) \leq y\}$ y por lo tanto

$$g(y) \leq t$$

con lo que concluimos la prueba.

Esta caracterización permite asegurar que la función adjunta para una función dada f es *única*, pues el supremo de un conjunto cuando existe es único.

2.8.3.4.1. Otras propiedades de las funciones adjuntas

Si una función $f : X \to Y$ entre dos conjuntos ordenados tiene adjunta a derecha g, entonces

1. $f(0) = 0$.

Prueba: como en X el elemento 0 es el mínimo, entonces $0 \leq g(0)$ y por la definición de adjunta tenemos que $f(0) \leq 0$, pero como 0 es elemento mínimo en Y se cumple que $0 \leq f(0)$, de donde concluimos que $f(0) = 0$.

2. $g(1) = 1$.

Prueba: como en Y el elemento 1 es el máximo, entonces $f(1) \leq 1$, y por la definición de adjunta tenemos que $1 \leq g(1)$, pero como 1 es elemento máximo en X se cumple que $g(1) \leq 1$, de donde concluimos que $g(1) = 1$.

3. *f conmuta con extremos superiores*, esto significa que para todo x, y en X

$$f(x \vee y) = f(x) \vee f(y).$$

Prueba: como $x \leq x \vee y$ y $y \leq x \vee y$, entonces por ser f un morfismo de conjuntos ordenados

$$f(x) \leq f(x \vee y)$$

y

$$f(y) \leq f(x \vee y)$$

entonces por la definición de supremo

$$f(x) \vee f(y) \leq f(x \vee y).$$

También tenemos la desigualdad en sentido contrario

$$f(x \vee y) \leq f(x) \vee f(y),$$

pues por la definición de supremo

$$f(x) \leq f(x) \vee f(y) \text{ y } f(y) \leq f(x) \vee f(y)$$

y por la definición de función adjunta

$$x \leq g(f(x) \vee f(y)) \text{ y } y \leq g(f(x) \vee f(y))$$

de nuevo, por la definición de supremo

$$x \vee y \leq g(f(x) \vee f(y))$$

y por la definición de función adjunta

$$f(x \vee y) \leq f(x) \vee f(y).$$

Ejercicio

Demuestre que g conmuta con extremos inferiores, esto significa que para todo x, y en Y

$$g(x \wedge y) = g(x) \wedge g(y).$$

Un *álgebra de Heyting* es un retículo H con 0 y 1 donde para cada y en H, las funciones

$$\begin{aligned} f_y : \mathrm{H} &\to \mathrm{H} \\ x &\mapsto f_y(x) = y \wedge x \end{aligned}$$

tienen adjunta a derecha. Notaremos

$$g_y(x) = y \to x$$

a la adjunta de f_y evaluada en x.

Para cada y en H definimos el *seudocomplemento* de y como

$$y^c = y \to 0.$$

En un álgebra de Heyting H se tienen las siguientes propiedades:

1. $x \wedge (x \to y) \leq y$.

   Sustituyendo $z = (x \to y)$ en la definición.

2. $z \leq (x \to (x \wedge z))$

   Sustituyendo $y = x \wedge z$ en la definición.

3. $x \wedge x^c = 0$

   Sustituyendo $y = 0$ en la propiedad 1.

4. $x \leq (x^c)^c$

5. $x \leq y$ implica que $y^c \leq x^c$.

6. $((x^c)^c)^c \leq x$.

Ejercicio

Demuestre las propiedades 4, 5 *y* 6.

Una de las igualdades que caracteriza el complemento en las álgebras de Boole, $x \vee x^c = 1$,no se verifica en álgebras de Heyting; por ejemplo, en el retículo $\underline{3}$, el valor $x = \frac{1}{2}$ no satisface la igualdad.

La propiedad distributiva si se cumple en toda álgebra de Heyting, puesto que $(x \to \_\_)$ es adjunto a derecha de $(x \wedge \_\_)$ y en consecuencia debe conmutar con extremos superiores, es decir :

$$(x \vee y) \wedge z = (x \vee z) \wedge (y \vee z).$$

2.8.3.5. Una lógica con tres elementos

De manera similar a como definimos estructuras algebraicas con dos elementos que representaban los valores de verdad Falso y Verdadero es posible definir estructuras algebraicas con otros conjuntos de más de dos elementos, por ejemplo, podemos modificar los símbolos del ejemplo 2 de la sección 2.8.3.3, con el propósito de que el valor de verdad 1 corresponda a Verdadero, el 0 a Falso y el tercer valor sea intermedio entre ellos, digamos $\frac{1}{2}$, o sea, lo que equivale a definir la función

$$\begin{aligned} \mathrm{H} : \{0,1,2\} &\to \{0,\tfrac{1}{2},1\} \\ 0 &\to 0 \\ 1 &\to \tfrac{1}{2} \\ 2 &\to 1 \end{aligned}$$

Pondremos el mismo nombre al conjunto $\underline{3} = \{0, \frac{1}{2}, 1\}$, en el que las operaciones conjunción y disyunción son:

$\wedge$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 58

$\vee$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

Tabla 59

Para construir la implicación tenemos varias opciones: podemos definir la implicación con algún criterio y con ella definir la negación en la forma

$$\neg p = p \to 0.$$

o definir, por ejemplo, primero una negación y con ella usar alguna de las equivalencias de la implicación en la lógica usual como

$$(p \to q) = \neg p \vee q.$$

Elijamos el primer procedimiento y definamos una implicación por *adjunción a derecha de la conjunción*; para ello, calculamos la adjunta a derecha para cada una de las funciones

$$\begin{aligned} f_0 : \underline{3} &\to \underline{3} \\ x &\mapsto f_0(x) = 0 \wedge x \end{aligned}$$

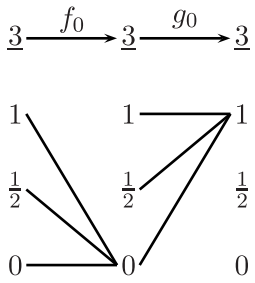
$$f_{1/2} : \underline{3} \to \underline{3}$$
$$x \mapsto f_{1/2}(x) = \tfrac{1}{2} \wedge x$$

$$f_1 : \underline{3} \to \underline{3}$$
$$x \mapsto f_1(x) = 1 \wedge x$$

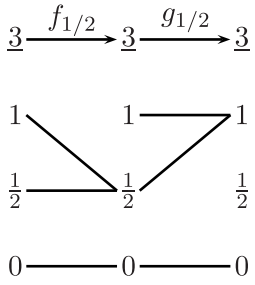
y usando la caracterización

$$g_0(x) = Sup\,\{y \in \underline{3} : f_0(y) \leq x\},$$

en el caso de f_0 obtenemos

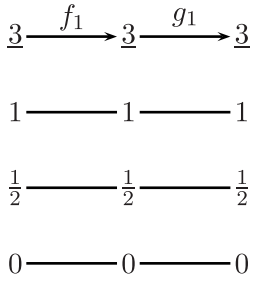


Lo que significa que $g_0(0) = 1$, $g_0(\frac{1}{2}) = 1$ y $g_0(1) = 1$. En el caso de $f_{1/2}$ obtenemos



lo que significa que $g_{1/2}(0) = 0$, $g_{1/2}(\frac{1}{2}) = 1$ y $g_{1/2}(1) = 1$.

Y en el caso de f_1 obtenemos



lo que significa que $g_1(0) = 0$, $g_1(\frac{1}{2}) = \frac{1}{2}$ y $g_1(1) = 1$, reuniendo todas las informaciones en una sola tabla y notando

$$g_y(x) = y \to x$$

conseguimos

$\to$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	1	1
1	0	$\frac{1}{2}$	1

Tabla 60

Por lo tanto $(\underline{3}, \wedge, \to, 0, 1)$ es un álgebra de Heyting.

Con la implicación definimos la negación en la forma:

$$\neg p = p \to 0$$

que en nuestro caso es

p	0	$\frac{1}{2}$	1
$\neg p$	1	0	0

Tabla 61

y la equivalencia (o doble implicación) la obtenemos con la definición

$$p \leftrightarrow q = (p \to q) \wedge (q \to p)$$

y la tabla que resulta es

$\leftrightarrow$	0	$\frac{1}{2}$	1
0	1	0	0
$\frac{1}{2}$	0	1	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 62

Con estas definiciones, podemos construir tablas de verdad para verificar que, independientemente del valor de p, q y r en $\underline{3}$, el valor de las siguientes proposiciones es 1, por lo que las llamaremos tautologías.

1. *Leyes de adición:* $p \to (p \vee q)$
$q \to (p \vee q)$.

2. *Leyes de eliminación*: $(p \wedge q) \to p$
$(p \wedge q) \to q$.

3. *Leyes de De Morgan*: $\neg(p \wedge q) \leftrightarrow (\neg p) \vee (\neg q)$
$\neg(p \vee q) \leftrightarrow (\neg p) \wedge (\neg q)$.

4. *Ley de contradicción*: $\neg(p \wedge \neg p)$.

5. $(p \to (q \to p))$.

6. *Ley de los casos*: $((p \to q) \wedge (r \to q)) \to ((p \vee r \to q))$, además se cumple la equivalencia.

7. $((p \to q) \wedge (p \to r)) \leftrightarrow (p \to (q \vee r))$.

8. *Ley de importación*: $(p \to (q \to r)) \to ((p \wedge q) \to r))$.

9. *Ley de exportación*: $((p \wedge q) \to r) \to (p \to (q \to r))$.

10. *Modus tollendo ponens*: $((p \vee q) \wedge \neg p) \to q$.

11. *Ley del absurdo*: $((p \to q) \wedge (p \to \neg q)) \to \neg p$.

12. *Ley de la doble negación*: $p \to \neg(\neg p)$.

Veamos la tabla de verdad para el caso de la ley del absurdo:

p	q	$\neg p$	$\neg q$	$p \to q$	$p \to \neg q$	$(p \to q) \wedge (p \to \neg q)$	$((p \to q) \wedge (p \to \neg q)) \to \neg p$
0	0	1	1	1	1	1	1
0	$\frac{1}{2}$	1	0	1	1	1	1
0	1	1	0	1	1	1	1
$\frac{1}{2}$	0	0	1	0	1	0	1
$\frac{1}{2}$	$\frac{1}{2}$	0	0	1	0	0	1
$\frac{1}{2}$	1	0	0	1	0	0	1
1	0	0	1	0	1	0	1
1	$\frac{1}{2}$	0	0	$\frac{1}{2}$	0	0	1
1	1	0	0	1	0	0	1

Tabla 63

Algunas tautologías que son válidas en la lógica bivalente pero no lo son en la lógica trivalente son:

1. *Recíproca de la doble negación*: $\neg(\neg p) \rightarrow p$ falla en el caso de $p = \frac{1}{2}$.
2. *Ley de la contrapositiva*: $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ falla en el caso $p = 1$ y $q = \frac{1}{2}$.

   Esta propiedad es una tautología en una sola dirección

   $$(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$$

   pero la recíproca

   $$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q) \text{ falla en el caso } p = 1 \text{ y } q = \tfrac{1}{2}.$$

3. *Tercero excluido*: $p \vee \neg p$ falla en el caso $p = \frac{1}{2}$.
4. *Reducción al absurdo*:

   $$((p \wedge \neg q) \rightarrow (r \wedge \neg r)) \leftrightarrow (p \rightarrow q) \text{ falla en el caso } p = 1 \text{ y } q = \tfrac{1}{2}.$$

   Esta propiedad es una tautología en una sola dirección

   $$(p \rightarrow q) \rightarrow ((p \wedge \neg q) \rightarrow (r \wedge \neg r))$$

   pero la recíproca

   $$((p \wedge \neg q) \rightarrow (r \wedge \neg r)) \rightarrow (p \rightarrow q)$$

   falla en el caso $p = 1$ y $q = \frac{1}{2}$.

2.8.3.6. Otra lógica con tres elementos: Lukasiewicz

Construiremos ahora otra estructura algebraica para los valores de verdad de una lógica trivalente propuesta por Jan Lukasiewicz[12] en 1920; iniciamos definiendo la negación, con la fórmula

$$\neg p = 1 - p$$

donde la sustracción se efectúa como en los números racionales, y obtenemos,

[12]LUKASIEWICZ, Jan. Selected Works. Amsterdam: North Holland Publishing, 1970. p. 87-88.

p	0	$\frac{1}{2}$	1
$\neg p$	1	$\frac{1}{2}$	0

Tabla 64

Luego definimos la implicación con la tabla

$\rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	0	$\frac{1}{2}$	1

Tabla 65

la disyunción mediante la fórmula

$$p \vee q = (p \rightarrow q) \rightarrow q$$

con el resultado

$\vee$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

Tabla 62

y la conjunción con

$$p \wedge q = \neg(\neg p \vee \neg q)$$

cuya tabla es

$\wedge$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 58

Como notamos, corresponden al sup e inf en el reticulo $\underline{3}$, y por lo tanto distribuyen una con respecto a la otra, pero en este caso la implicación no es adjunta a derecha de la conjunción.

En esta lógica no se cumple el principio del tercero excluido, pues en el caso de $p = \frac{1}{2}$, $p \vee \neg p = \frac{1}{2}$.

Ejercicio

Verifique cuáles tautologías de la lógica usual se cumplen en la lógica de Lukasiewicz.

Una alternativa[13] para presentar esta lógica es iniciar con la misma negación

$$\neg p = 1 - p$$

y definir la operación

$$p \oplus q = min\{1, p + q\}$$

donde el orden es el usual, $0 \leq \frac{1}{2} \leq 1$, y la suma se efectúa como en los números racionales, con esto obtenemos la tabla[14]

$\oplus$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	1	1	1

Tabla 66

Hacemos una copia de la operación $\oplus$ con la función biyectiva $\neg$ y obtenemos

$$(p \otimes q) = \neg((\neg p) \oplus (\neg q))$$

cuya tabla correspondiente es

$\otimes$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 67

[13]Esta presentación es la de: OOSTRA, Arnold. Lógicas de Lukasiewicz y sus álgebras. En : _____. Huellas en los encuentros de Geometría y Aritmética. Bogotá: Universidad Pedagógica Nacional, 2005. p. 317-350.

[14]Notemos que estas operaciones no corresponden con el infA ni con el supA para algún conjunto A de dos elementos, por lo tanto no estamos considerando el conjunto $\{0, \frac{1}{2}, 1\}$ como retículo.

Las operaciones $\oplus$ y $\otimes$ son asociativas, conmutativas, tienen elemento idéntico, 1 para $\otimes$ y 0 para $\oplus$, además cumplen las propiedades elástica, asociativa cíclica I y II, identidades de Abel Grassmann I y II, son permutables a izquierda y a derecha, bisimétricas y del producto reducido.

En este caso, ni la operación $\otimes$ distribuye con respecto a $\oplus$, pues

$$\tfrac{1}{2} \otimes (\tfrac{1}{2} \oplus \tfrac{1}{2}) = \tfrac{1}{2} \otimes 1 = \tfrac{1}{2} \text{ pero } (\tfrac{1}{2} \otimes \tfrac{1}{2}) \oplus (\tfrac{1}{2} \otimes \tfrac{1}{2}) = 0 \oplus 0 = 0,$$

ni $\oplus$ distribuye con respecto a $\otimes$, pues

$$\tfrac{1}{2} \oplus (\tfrac{1}{2} \otimes \tfrac{1}{2}) = \tfrac{1}{2} \oplus 0 = \tfrac{1}{2} \text{ pero } (\tfrac{1}{2} \oplus \tfrac{1}{2}) \otimes (\tfrac{1}{2} \oplus \tfrac{1}{2}) = 1 \otimes 1 = 1.$$

Enseguida definimos la implicación usando

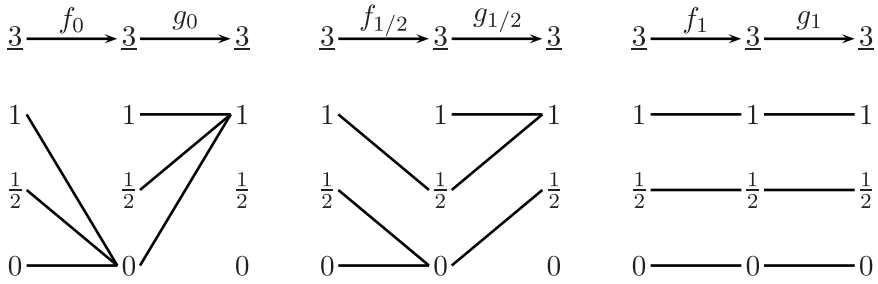
$$\begin{aligned} p \to q &= \neg p \oplus q \\ &= min\{1, (1-p)+q\} \end{aligned}$$

cuya tabla es:

$\to$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	0	$\frac{1}{2}$	1

Tabla 65

Otra forma de construir esta implicación es por adjunción a partir de la operación $\otimes$, en la forma:



Aunque esto no significa que la estructura algebraica subyacente en la lógica de Lukasiewicz sea un álgebra de Heyting pues la operación $\otimes$ no corresponde con el inf en el retículo $\underline{3}$.

La disyunción la definimos en términos de la operación $\oplus$, como:

$$p \vee q = \neg((\neg p) \oplus q) \oplus q$$

o lo que es equivalente

$$p \vee q = (p \to q) \to q,$$

la conjunción con

$$p \wedge q = \neg((\neg p) \otimes q) \otimes q$$

y la doble implicación como

$$p \leftrightarrow q = (p \to q) \wedge (q \to p)$$

cuya tabla es

$\leftrightarrow$	0	$\frac{1}{2}$	1
0	1	$\frac{1}{2}$	0
$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 68

Notemos que las definiciones dadas tienen sentido en cualquier subconjunto del intervalo real $[0, 1]$, lo que nos permite construir lógicas como esta con infinitos valores.

Ejercicio

Construya las tablas para una lógica de cuatro valores utilizando el esquema de Lukasiewicz.

Un conjunto de axiomas, escritos solamente en términos de la implicación y la negación, para la *lógica* de *Lukasiewicz* con tres valores es:

1. $p \to (q \to p)$
2. $(p \to q) \to ((q \to r) \to (p \to r))$
3. $((p \to q) \to q) \to ((q \to p) \to p)$
4. $(\neg q \to \neg p) \to (p \to q)$
5. $(\neg p \to (\neg p \to p)) \to (\neg p \to p)$

Estos axiomas son teoremas del cálculo proposicional clásico, y por lo tanto la lógica de Lukasiewicz con dos valores es una sublógica de la clásica.

Algunas tautologías de este sistema deductivo[15] son:

T1. $p \to ((p \to q) \to q)$

T2. $(p \to (q \to r)) \to (q \to (p \to r))$

T3. $p \to p$

T4. $((p \to p) \to p) \to p$

T5. $(q \to r) \to ((p \to q) \to (p \to r))$

T6. $\neg\neg p \to (q \to p)$

T7. $\neg\neg p \to p$

T8. $(p \to \neg q) \to (q \to \neg p)$

T9. $p \to \neg\neg p$

T10. $(p \to q) \to (\neg q \to \neg p)$

T11. $(\neg p \to q) \to (\neg q \to p)$

T12. $\neg(p \to q) \to p$

T13. $\neg(p \to q) \to \neg q$.

La afirmación T1 corresponde con la ley de adición $p \to p \vee q$ y T4 corresponde con $(p \vee p) \to p$.

Ejercicios

1. *Con la operación*

$\to$	0	$\frac{1}{2}$	1
0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{2}$	0	$\frac{1}{2}$	1
1	1	$\frac{1}{2}$	$\frac{1}{2}$

Tabla 69

[15]OOSTRA, Op. cit., p. 334-335.

defina una negación y operaciones correspondientes a la disyunción, la conjunción y la doble implicación. Estudie cuáles tautologías son válidas en este ejemplo.

2. *Con la operación*

$\wedge$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 67

y la negación

p	0	$\frac{1}{2}$	1
$\neg p$	1	0	0

Tabla 61

construya operaciones correspondientes a la disyunción, la implicación y la doble implicación. Estudie cuáles tautologías son válidas en este ejemplo.

3. *Otra posibilidad para una lógica de tres valores sugerida por Reichenbach*[16] *utiliza los siguientes conectivos:*

$\vee$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

Tabla 59

$\wedge$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 58

$\rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	1	1	1
1	0	0	1

Tabla 70

$\leftrightarrow$	0	$\frac{1}{2}$	1
0	1	$\frac{1}{2}$	0
$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

Tabla 68

[16]JAMMER, Max. Conceptual development of quantum mechanics. New York: John Willey & Sons, 1974. p. 366-367.

que se combinan con tres posibles negaciones:

Cíclica

p	0	$\frac{1}{2}$	1
$\sim p$	1	0	$\frac{1}{2}$

Tabla 71

Diametral

p	0	$\frac{1}{2}$	1
$\neg p$	1	$\frac{1}{2}$	0

Tabla 64

Completa

p	0	$\frac{1}{2}$	1
$-p$	1	1	$\frac{1}{2}$

Tabla 72

Estudie cuáles tautologías son válidas en este ejemplo.

CAPÍTULO 3

Otras estructuras algebraicas finitas

La esencia de la matemática es su libertad.
Cantor

En los dos capítulos anteriores estudiamos estructuras finitas con dos y tres elementos, pero no mencionamos estructuras con un elemento, pues no parece natural operar con un solo elemento y si lo hacemos, pareciera que no podamos sacar alguna conclusión interesante.

En este capítulo estudiamos la única estructura posible con un elemento y mostraremos algunas representaciones no triviales de ella; enseguida dirigimos nuestra atención a estructuras con cuatro elementos, pero ante el enorme número de operaciones posibles nos restringimos a las dos estructuras de grupo; presentamos algunas de sus representaciones, y con una de ellas, el grupo de Klein, formamos un campo donde estudiamos algunas identidades algebraicas y las ecuaciones de segundo grado, extendiendo el campo cuando alguna ecuación no tiene solución.

Seguidamente presentamos algunos grupos finitos caracterizables con pocas condiciones como los grupos cíclicos, los grupos de permutaciones, los grupos diedros y el grupo de los cuaternios.

3.1. Estructuras con un elemento

En un conjunto A cuyo único elemento es a, la única operación posible es

$$\begin{aligned} * : A \times A &\to A \\ (a, a) &\mapsto a \end{aligned}$$

Es decir, podemos caracterizar la estructura (A, $*$) de manera única, salvo isomorfismos, por la propiedad de idempotencia, $a*a = a$, la cual tuvo mucha importancia en el capítulo 1 para axiomatizar las operaciones conjunción $\wedge$, y disyunción $\vee$; y que aunque no es habitual en la caracterización de estructuras como las de grupo, anillo o campo, si tiene importancia en las estructuras de álgebra de Boole, álgebra de Heyting y en general en la teoría de retículos. Además esta única propiedad permite demostrar en el caso de un conjunto con un elemento (A, $*$) las propiedades que definen una estructura de grupo abeliano.

A pesar de lo aparentemente elemental de esta estructura, existen representaciones de ella que no son triviales; por ejemplo, si consideramos las tablas de las operaciones lógicas con dos elementos como matrices 2×2 con entradas en los números naturales y para no recargar la notación las representamos con los mismos símbolos, de la siguiente forma

$$\bot = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \downarrow = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \otimes = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad * = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\wedge = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad \leftrightarrow = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \pi_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

obtenemos que las duplas (M, $\cdot$) con M un conjunto unitario cuyo elemento es una de las matrices mencionadas y la operación $\cdot$ es la multiplicación usual de matrices, son representaciones de (A, $*$), pues en todos los casos las potencias n-ésimas de ellas son ellas mismas, en particular

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}^n = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

3.2. Estructuras con cuatro elementos

Si deseamos considerar estructuras algebraicas sobre un conjunto con más de tres elementos, tenemos un gran problema pues con solo cuatro

elementos existen $4^{16} = 4\ 294\ 967\ 296$ operaciones posibles, por lo que intentar siquiera una clasificación como lo hicimos con dos y tres elementos resulta una tarea monumental. Veamos entonces estructuras con cuatro elementos pero que tengan cualidades particulares, por ejemplo ¿cuántas operaciones con cuatro elementos tienen elemento idéntico?

Sea $\mathrm{H} = \{0, 1, 2, 3\}$, si escogemos a 0 como elemento idéntico, la fila y columna donde se ubica quedará llena, luego la tabla sería:

	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

quedando nueve casillas que se pueden llenar de cuatro formas distintas, es decir, resultarían $4^9 = 262\ 144$ operaciones con elemento idéntico.

Pero como hay 4 opciones para escoger el elemento idéntico, debemos multiplicar esta cantidad por cuatro, o sea hay en total 1 048 576 operaciones con elemento idéntico en un conjunto con cuatro elementos. Aún son demasiadas operaciones para intentar una clasificación.

Haciendo una cuenta similar, concluimos que para un conjunto con k elementos hay $k(k^{(k-1)^2})$ operaciones con elemento idéntico.

Ejercicio

Demuestre por inducción sobre k la anterior afirmación.

Veamos ahora cuántas operaciones con 4 elementos son conmutativas, en este caso la tabla solo debe llenarse en el triángulo superior (o inferior):

	0	1	2	3
0	?	?	?	?
1		?	?	?
2			?	?
3				?

o sea tenemos que llenar $4 + 3 + 2 + 1 = 10$ casillas y cada una de ellas tiene cuatro elementos opcionales, en total $4^{10} = 1\ 048\ 576$ operaciones conmutativas.

En general, en un conjunto con k elementos podemos definir k^{T_k} operaciones binarias conmutativas donde T_k es el k-ésimo número triangular.

Ejercicio

Demuestre por inducción sobre k la anterior afirmación.

Como el número no disminuye, impongamos condiciones más fuertes, digamos que el conjunto con la operación forme estructura de grupo, y ahora el número cae drásticamente ¡solo hay dos grupos no isomorfos con cuatro elementos! y cada uno de los ellos tiene a lo más, 24 caras cada uno.

Dado el conjunto $\mathrm{N} = \{a, b, c, d\}$ si queremos definir sobre N una operación $+$ que determine sobre N una estructura de grupo, iniciemos eligiendo un elemento idéntico, por ejemplo a, con esto obtenemos:

$+$	a	b	c	d
a	a	b	c	d
b	b			
c	c			
d	d			

Ahora ubiquemos los elementos inversos, pero antes recordemos que como la tabla debe corresponder a la operación de un grupo y en un grupo se cumple la propiedad cancelativa, de esta concluimos que si $y \neq z$ debemos tener que $x + y \neq x + z$ al igual que $y + x \neq z + x$, lo que significa que en dos casillas de una misma fila o una misma columna de la tabla no se pueden encontrar dos elementos iguales.

Teniendo en cuenta lo anterior, si por ejemplo, $b + b = a$ entonces en la siguiente fila $c+c = a$ o $c+d = a = d+c$ pues la operación es conmutativa, lo que nos determina dos tablas:

$+$	a	b	c	d
a	a	b	c	d
b	b	a		
c	c		a	
d	d			

Tabla 1

$+$	a	b	c	d
a	a	b	c	d
b	b	a		
c	c			a
d	d		a	

Tabla 2

Y en la tabla 1 por la propiedad cancelativa $d + d = a$. Con la elección del elemento idéntico y de los elementos inversos, las casillas vacías en cada tabla pueden llenarse de una sola manera teniendo en cuenta la propiedad cancelativa, esto es:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Tabla 3

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Tabla 4

Este proceso lo podemos reiterar escogiendo otro inverso para b o eligiendo como elemento idéntico a cada uno de los elementos diferentes de a, y repitiendo el procedimiento descrito anteriormente, pero lo que conseguiríamos serían diferentes representaciones de las estructuras de la tablas 3 y 4. En resumen tenemos dos estructuras:

3.2.1. El grupo $(Z_4, +)$

El grupo $(Z_4, +)$ está determinado salvo isomorfismos por las condiciones:

1. Un grupo con cuatro elementos donde, de los tres diferentes al elemento neutro, hay uno que es inverso de si mismo y los otros dos son inversos entre si.

2. Un grupo con cuatro elementos donde existe un elemento idéntico e y un elemento $a \neq e$, tal que para todo x en Z_4, $x = a^k = a\,a\,a\,a\,a\,a\ldots a$ donde a aparece k veces[1], para algún $k = 1, 2, 3, 4$ y $a^4 = e$.

   O en forma de tabla:

$+$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

Tabla 5

[1]Hemos omitido el símbolo de la operación cuando escribimos $a^k = a\,a\,a\,a\,a\ldots a$.

3.2.2. El grupo cuarto de Klein $(V, \oplus)$

El grupo (V, $\oplus$)[2] está determinado salvo isomorfismos por las condiciones:

1. Un grupo con cuatro elementos donde cada uno de ellos es su propio inverso.
2. Un grupo con cuatro elementos, donde existen dos elementos a y r diferentes de e y diferentes entre sí tales que:
   1. $r^2 = a^2 = e$
   2. $ra = ar \neq r$ y $ar \neq a$

   donde e es el elemento idéntico. O en forma de tabla:

$\oplus$	e	a	r	ar
e	e	a	r	ar
a	a	e	ar	r
r	r	ar	e	a
ar	ar	r	a	e

Tabla 6

3.2.3. Representaciones de $(Z_4, +)$

Estas estructuras se presentan en diferentes contextos como por ejemplo:

3.2.3.1. Las raíces cuartas de la unidad

El subconjunto de los números complejos C = $\{1, i, -1, -i\}$ con la multiplicación usual entre ellos tiene como tabla:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
-1	-1	$-i$	1	i
i	i	-1	$-i$	1
$-i$	$-i$	1	i	-1

Tabla 7

[2]El nombre V del grupo es la primera letra de la palabra alemana *Vier* que significa cuatro.

que es una representación de Z_4, correspondiente a las raíces cuartas de la unidad, o sea a las soluciones de la ecuación

$$x^4 - 1 = 0$$

factorizada en la forma

$$(x^2 - 1)(x^2 + 1) = 0.$$

3.2.3.2. Las rotaciones de 90 grados en el plano

Una representación geométrica de Z_4 la obtenemos en el conjunto de las rotaciones de 90 grados en sentido antihorario en el plano con la operación composición, cuya tabla es

$\circ$	1	R	R^2	R^3
1	1	R	R^2	R^3
R	R	R^2	R^3	1
R^2	R^2	R^3	1	R
R^3	R^3	1	R	R^2

Tabla 8

donde el exponente indica el número de veces que se compone R consigo misma y 1 representa a la función idéntica.

3.2.3.3. Una representación matricial para Z_4

El conjunto de matrices:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \; -i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

con la multiplicación usual de matrices forma un grupo isomorfo a Z_4.

3.2.4. Representaciones del grupo de Klein

Una manera de obtener una representación para el grupo de Klein es mediante el producto directo del grupo $(Z_2, +)$ consigo mismo, veamos como se construye.

3.2.4.1. El producto directo $Z_2 \times Z_2$

Definimos el *producto directo* de dos grupos (G, #) y (H, $*$) operando componente a componente, en la forma

$$\begin{aligned} \& : (\mathrm{G} \times \mathrm{H}) \times (\mathrm{G} \times \mathrm{H}) &\to (\mathrm{G} \times \mathrm{H}) \\ ((a,b),(c,d)) &\mapsto ((a\#c, b*d)) \end{aligned}$$

En particular, si efectuamos el producto directo del grupo $(Z_2, +)$ consigo mismo, obtenemos una estructura sobre el conjunto

$$Z_2 \times Z_2 = \{(x,y) : x \in Z_2 \wedge y \in Z_2\} = \{(0,0),(0,1),(1,0),(1,1)\}$$

operando,

$$(a,b) \oplus (c,d) = (a+c, b+d)$$

para cada (a,b), $(c,d) \in Z_2 \times Z_2$, donde el símbolo $+$ indica la adición definida en Z_2, resulta la tabla:

$\oplus$	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 0)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

Tabla 9

Si cambiamos el nombre a los elementos de manera que

$$\begin{aligned} (0,0) &= x \\ (0,1) &= y \\ (1,0) &= z \\ (1,1) &= w \end{aligned}$$

la estructura corresponde a la del grupo de Klein. Con esto hemos demostrado que *el grupo* $(Z_2, +) \times (Z_2, +)$ *es isomorfo al grupo cuarto de Klein*, es usual escribir este resultado así:

$$Z_2 \times Z_2 \sim \mathrm{V}.$$

3.2.4.2. El conjunto $Z_2^{Z_2}$ de las funciones de Z_2 en Z_2 con la operación suma de funciones

Otra representación de (V, $\oplus$) se logra estudiando el conjunto de las funciones de Z_2 en Z_2:

$$\mathrm{F} = \{f_0, f_1, f_2, f_3\}$$

donde

$$\begin{aligned} f_0 : Z_2 &\to Z_2 \\ 0 &\mapsto 0 \\ 1 &\mapsto 1 \end{aligned}$$

$$\begin{aligned} f_1 : Z_2 &\to Z_2 \\ 0 &\mapsto 0 \\ 1 &\mapsto 0 \end{aligned}$$

$$\begin{aligned} f_2 : Z_2 &\to Z_2 \\ 0 &\mapsto 1 \\ 1 &\mapsto 1 \end{aligned}$$

$$\begin{aligned} f_3 : Z_2 &\to Z_2 \\ 0 &\mapsto 1 \\ 1 &\mapsto 0 \end{aligned}$$

y la operación entre funciones está definida de la manera usual para cada x de $(Z_2, +)$ por la fórmula:

$$(f_i \oplus f_j)(x) = f_i(x) \oplus f_j(x)$$

para $i, j = 0, 1, 2, 3$.

Por ejemplo

$$(f_1 \oplus f_3)(0) = f_1(0) \oplus f_3(0) = 0 + 1 = 1$$

$$(f_1 \oplus f_3)(1) = f_1(1) \oplus f_3(1) = 0 + 0 = 0$$

o

$$(f_1 \oplus f_3)(0) = 1$$

$$(f_1 \oplus f_3)(1) = 0$$

es decir que:

$$f_1 \oplus f_3 = f_3.$$

Efectuando las demás cuentas, obtenemos la tabla:

$\oplus''$	f_0	f_1	f_2	f_3
f_0	f_1	f_0	f_3	f_2
f_1	f_0	f_1	f_2	f_3
f_2	f_3	f_2	f_1	f_0
f_3	f_2	f_3	f_0	f_1

Tabla 10

Y, si cambiamos el nombre a cada elemento según:

$$f_0 \to y$$
$$f_1 \to x$$
$$f_2 \to z$$
$$f_3 \to w$$

mostramos que esta es otra representación del grupo de Klein.

3.2.4.3. Las reflexiones de un rectángulo

Una manera de obtener una representación geométrica para el grupo de Klein es considerando un rectángulo R en el plano con vértices numerados en la forma:

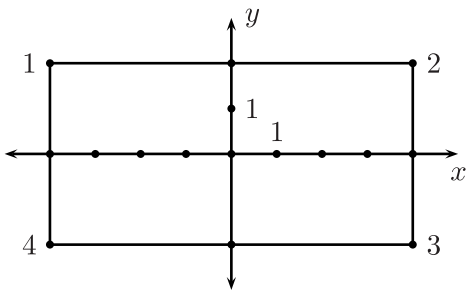


Figura 1

y las siguientes transformaciones de R (también llamadas isometrías):

- r : rotación de 180^0 alrededor del centro.
- h : reflexión sobre el eje horizontal.
- v : reflexión sobre el eje vertical.
- e : movimiento idéntico: cada punto lo deja donde está.

El conjunto $\mathrm{K} = \{e, r, h, v\}$ con la operación composición $\circ$ tiene como tabla:

$\circ$	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

Tabla 11

y su estructura es isomorfa a la del grupo de Klein.

3.2.4.4. Las inversas aditivas y multiplicativas de una función real

Consideremos las funciones

$$i(x) = x, \quad f(x) = -x, \quad g(x) = \frac{1}{x}, \quad h(x) = -\frac{1}{x},$$

con dominio y codominio en todos los números reales diferentes de 0. El conjunto

$$\mathrm{P} = \{i, f, g, h\}$$

con la operación composición de funciones forma una representación del grupo de Klein cuya tabla es:

$\circ$	i	f	g	h
i	i	f	g	h
f	f	i	h	g
g	g	h	i	f
h	h	g	f	i

Tabla 12

3.2.5. Los grupos (V, $\oplus$) y $(Z_4, +)$ no son isomorfos

Los dos grupos con cuatro elementos mencionados *no son isomorfos*, pues si lo fueran existiría una función biyectiva

$$f : (\mathrm{V}, \oplus) \to (Z_4, +)$$

tal que:

$$f(x) = a$$

siendo a el elemento idéntico en Z_4 y x el elemento idéntico en V, luego para cada y en V

$$f(x) = f(y \oplus y) = f(y) + f(y) = a$$

lo que significa que

$$f(-y) = -f(y)$$

y como f es biyectiva, cada elemento de Z_4 debe ser imagen de un único elemento de V, o sea que en Z_4 todos los elementos deben ser inversos de sí mismos y esto no sucede, por lo tanto los dos grupos no son isomorfos.

3.2.6. Un campo con cuatro elementos

Siguiendo nuestra línea de pensamiento de los capítulos anteriores, si queremos construir un campo debemos conseguir una operación $\otimes$ que sea distributiva respecto a alguno de los dos grupos abelianos con cuatro elementos, iniciemos tomando como suma a la definida en Z_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla 13

Una operación distributiva con respecto a ella es[3]

[3]Esta es la multiplicación correspondiente a Z_4, usando la definición: $a \times b = res\left(\frac{a \times b}{4}\right)$ donde $res\left(\frac{a \times b}{4}\right)$ significa tomar el residuo de la división entre 4 de la multiplicación usual como enteros de a y b.

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla 14

pero como $2 \times 0 = 2 \times 2 = 0$ pero $2 \neq 0$, la operación no es cancelativa, o dicho de otra forma 2 no tiene inverso multiplicativo y por lo tanto $(Z_4, +, \times)$ no es un campo, pero si tiene estructura de anillo[4].

Empecemos de nuevo, ahora notando que como la distributividad se debe cumplir para cualquier elemento, en particular para el elemento idéntico, 0, de la operación $+$, se debe tener que para todo a en Z_4:

$$a \times 0 = 0 = 0 \times a$$

porque $a \times 0 = a(0 + 0) = (a \times 0) + (a \times 0)$, con esto tenemos

$\times$	0	1	2	3
0	0	0	0	0
1	0			
2	0			
3	0			

y queda una tabla de 3×3 para llenar con la condición de que esta tabla forme un grupo; como ya habíamos encontrado que solo hay un grupo de tres elementos, usémoslo para llenar lo que falta, escogiendo un elemento como idéntico, que bien pude ser el 1, con lo que llegamos a

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Tabla 15

[4]LUQUE, MORA y TORRES, Op. cit., 2006, p. 56-63.

Pero la operación $\times$ no es distributiva con respecto a $+$, puesto que

$$2 \times (1 + 1) \neq (2 \times 1) + (2 \times 1).$$

Si escogemos como elemento idéntico al 2 o al 3, las tablas que resultan para la operación $\times$ tampoco son distributivas con respecto a $+$, pues ambas fallan en el caso

$$1 \times (1 + 1) \neq (1 \times 1) + (1 \times 1).$$

Pero como en el caso de dos elementos, podríamos pensar que aunque la operación $\times$ no es distributiva con respecto a esta representación de Z_4, si lo es respecto a otra representación, pero también fracasamos, pues ninguna de las representaciones de $(\{0, 1, 2, 3\}, \times)$ es distributiva con respecto a alguna representación de $(Z_4, +)$ lo que podemos verificar usando el programa *Propiedades algebraicas de estructuras finitas.*

Ensayemos entonces con el grupo de Klein

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Tabla 16

y tratemos de construir una multiplicación $\otimes$ que sea distributiva con respecto a la operación $\oplus$.

Para comenzar usemos el hecho de que el grupo V es un producto del grupo abeliano Z_2 consigo mismo y que Z_2 también tiene una multiplicación definida que le da estructura de campo, lo que nos ofrece una analogía con el campo de los números complejos que se pueden representar como un producto del campo de los números reales consigo mismo, con la suma definida componente a componente y la multiplicación de dos parejas (a, b) y (c, d) dada por

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Esto nos sugiere definir la operación multiplicación $\otimes$ en V como:

$$(a, b) \otimes (c, d) = (ac - bd, ad + bc)$$

donde a, b, c y $d \in Z_2$, las operaciones dentro del paréntesis se realizan en Z_2. De esta forma obtenemos la tabla:

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	2	1	3
2	0	1	2	3
3	0	3	3	0

Tabla 17

donde hemos cambiados los nombres de los elementos de $Z_2 \times Z_2$ de la siguiente manera:

$$(0,0) = 0$$
$$(0,1) = 1$$
$$(1,0) = 2$$
$$(1,1) = 3$$

y de nuevo fracasamos porque la multiplicación así definida tampoco es cancelativa.

Ejercicio

Ensaye a construir otra multiplicación distributiva con respecto al grupo de Klein, con las formas de multiplicar parejas en los números duales o los dobles.

Usemos entonces la tabla 15 como multiplicación para formar con el grupo V un campo. Esta operación es asociativa, conmutativa, con elemento idéntico 1 y milagrosamente resulta distributiva con respecto al grupo de Klein, lo que podemos verificar usando el programa *Álgebra finita*.

Los inversos multiplicativos para cada elemento diferente de 0 son:

$$1^{-1} = 1 \qquad 2^{-1} = \frac{1}{2} = 3 \qquad 3^{-1} = \frac{1}{3} = 2$$

con lo que obtenemos un campo (V, $\oplus$, $\times$) que llamaremos el *campo de Klein* y es el único campo con cuatro elementos salvo isomorfismos, pues cualquier par de campos finitos que tienen el mismo número de elementos son isomorfos[5].

[5]Una demostración de esta afirmación se encuentra en: HERSTEIN, Israel. Álgebra moderna. México: F. Trillas, 1970. p. 362.

3.2.6.1. Identidades Algebraicas

Si definimos a^n donde a es un elemento en (V, $\oplus$, $\times$) y n es un número natural distinto de 0, como

$$a^n = a \times a \times \ldots \times a \times a$$

donde a aparece n veces, se cumple que para todo a, b en (V, $\oplus$, $\times$)[6]:

1. $a^2 a = 1$
2. $\dfrac{1}{a} = a^2$ con $a \neq 0$.
3. $(a \oplus b)^2 = (a \oplus b)(a \oplus b) = a^2 \oplus ab \oplus ab \oplus b^2$,

   pero como
   $$ab \oplus ab = 0$$
   entonces
   $$(a \oplus b)^2 = a^2 \oplus b^2$$
4. Como sumar y restar es lo mismo, por ser cada elemento el inverso aditivo de sí mismo,
   $$(a - b)^2 = a^2 - b^2$$
5. Para todo a en (V, $\oplus$, $\times$) distinto de 0 y para todo número natural p distinto de 0,
   $$a^{3p} = a^3 = 1$$
   $$a^{3p-1} = a^2$$
   $$a^{3p+1} = a.$$

   En particular
   $$1^2 = 1 \qquad 2^2 = 3 \qquad 3^2 = 2$$
   que también podemos escribir como
   $$\sqrt{1} = 1 \qquad \sqrt{2} = 3 \qquad \sqrt{3} = 2$$
   respectivamente.

[6]En lo que sigue para simplificar la notación omitiremos el símbolo para la operación $\times$, notando $a \times b$ como ab.

6. Si $a \neq 0$, $b \neq 0$ y $a \oplus b \neq 0$ entonces,

$$\begin{aligned}(a \oplus b)^3 &= (a \oplus b)^2(a \oplus b) \\ &= a^3 \oplus a^2b \oplus ab^2 \oplus b^3 \\ &= 1 \oplus a^2b \oplus ab^2 \oplus 1 \\ &= a^2b \oplus ab^2\end{aligned}$$

o sea que

$$(a \oplus b)^3 = a^2b \oplus ab^2 = 1$$

7. También encontramos que si $a \neq 0$, $b \neq 0$ y $a \oplus b \neq 0$

$$\begin{gathered}(a \oplus b)^4 = a \oplus b \\ (a \oplus b)^5 = (a \oplus b)^2 = a^2 \oplus b^2 \\ (a \oplus b)^6 = (a \oplus b)^3\end{gathered}$$

y en general, para todo número natural p distinto de 0,

$$\begin{gathered}(a \oplus b)^{3p} = (a \oplus b)^3 = 1 \\ (a \oplus b)^{3p-1} = (a \oplus b)^2 = a^2 \oplus b^2 \\ (a \oplus b)^{3p+1} = a \oplus b.\end{gathered}$$

3.2.6.2. Una representación del campo de Klein

El conjunto de matrices

$$\mathrm{F} = \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} : a, b \in Z_2 \right\}$$

con la adición y multiplicación usual es una representación del campo de Klein.

Si reemplazamos a y b por sus posibles valores obtenemos:

$$\perp = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \leftrightarrow = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \vee = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad | = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Los nombres que les hemos puesto, son los de las tablas de las operaciones lógicas, correspondientes a los elementos de cada matriz. Explícitamente las tablas de las operaciones del campo son:

$+$	$\perp$	$\leftrightarrow$	$\vee$	$\mid$
$\perp$	$\perp$	$\leftrightarrow$	$\vee$	$\mid$
$\leftrightarrow$	$\leftrightarrow$	$\perp$	$\mid$	$\vee$
$\vee$	$\vee$	$\mid$	$\perp$	$\leftrightarrow$
$\mid$	$\mid$	$\vee$	$\leftrightarrow$	$\perp$

Tabla 18

$\cdot$	$\perp$	$\leftrightarrow$	$\vee$	$\mid$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
$\leftrightarrow$	$\perp$	$\leftrightarrow$	$\vee$	$\mid$
$\vee$	$\perp$	$\vee$	$\mid$	$\leftrightarrow$
$\mid$	$\perp$	$\mid$	$\leftrightarrow$	$\vee$

Tabla 19

La correspondencia

$$\begin{aligned} \perp &\mapsto 0 \\ \leftrightarrow &\mapsto 1 \\ \vee &\mapsto 2 \\ \mid &\mapsto 3 \end{aligned}$$

nos da el isomorfismo entre (F, $+$, $\cdot$) y el campo de Klein.

3.2.6.3. Ecuaciones en el campo de Klein

Enseguida resolveremos ecuaciones entre elementos del campo $(V, \oplus, \otimes)$ con las operaciones:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Tabla 16

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Tabla 15

La igualdad, entre elementos del conjunto V, *es compatible o estable*[7] con las operaciones $\oplus$ y $\otimes$ definidas en V, y por lo tanto: para todo $a, b, c, d \in V$, si

$$a = b \text{ y } c = d \text{ entonces } a \oplus c = b \oplus d$$

en particular

$$a \oplus c = b \oplus c$$

y también

$$a \otimes c = b \otimes d$$

y como caso particular

$$a \otimes c = b \otimes c.$$

3.2.6.3.1. Ecuaciones de primer grado con una incógnita

Toda ecuación de primer grado[8] en V con una incógnita se puede llevar a la forma

$$ax + b = 0$$

donde a, b y c son constantes, $a \neq 0$ y x es la incógnita, y se resuelven de la misma forma que en los números reales, pues como ya dijimos ambos conjuntos tienen la misma estructura algebraica de campo. Si partimos de

$$ax + b = 0$$

y sumamos el inverso aditivo de b, $(-b)$, a ambos lados de la igualdad, obtenemos:

$$(ax + b) + (-b) = 0 + (-b)$$

donde

$$ax = -b$$

y como en este caso $(-b) = b$

$$ax = b.$$

[7] WARNER, Seth. Modern Algebra. New York: Dover, 1990. p.70.

[8] Como en otras ocasiones omitiremos los símbolos $\oplus$ y $\otimes$ y usaremos $+$ para la suma y ningún símbolo para la multiplicación.

Ahora, multiplicamos a ambos lados de la igualdad por $\frac{1}{a}$ y conseguimos,

$$\begin{aligned}\frac{1}{a}(ax) &= \frac{1}{a}(b)\\ 1x &= \frac{b}{a}\\ x &= \frac{b}{a}\\ x &= ba^2.\end{aligned}$$

Por la manera en que fue obtenida, esta es la *única* solución para la ecuación planteada, y podemos afirmar que: *las ecuaciones de primer grado en el campo de Klein tienen a lo más una solución.*

Ejemplo

La ecuación

$$3x + 2 = 0$$

la resolvemos sumando el inverso aditivo de 2 en ambos lados

$$3x + 2 + 2 = 2$$

consiguiendo

$$3x = 2,$$

ahora multiplicamos a ambos lados de la igualdad por el inverso multiplicativo de 3,

$$\frac{1}{3}3x = \frac{1}{3} \times 2$$

y como $2 = \frac{1}{3}$, entonces

$$1x = 2 \times 2$$

$$x = 3.$$

Ejercicio

En el campo V resuelva las siguientes ecuaciones y justifique cada paso que realiza:

1. $2x - 3 = 1$

2. $3x + 1 = 0$

Las ecuaciones de primer grado con dos incógnitas y las ecuaciones simultáneas también tienen los mismos procedimientos de solución que en el caso de los números reales y por esto no haremos énfasis en ello.

Ejercicio

Resuelva en el campo V los sistemas de ecuaciones simultáneas:

$$3y + 2x = 0$$
$$-2x - y = 3$$

y

$$3x - y = -2$$
$$x - 3y = 1.$$

3.2.6.3.2. Ecuaciones cuadráticas

Las ecuaciones de segundo grado más simples son de la forma[9]

$$x^2 = c$$

y en todo caso tienen solución:

$$\sqrt{3} = 2$$
$$\sqrt{2} = 3$$
$$\sqrt{1} = 1$$
$$\sqrt{0} = 0.$$

Si alguno de los coeficientes es cero, una ecuación de la forma

$$ax^2 + bx + c = 0$$

se reduce a una de primer grado:

1. Si $a = 0$, la ecuación es $bx + c = 0$.

[9]Parte de este tema fue estudiado por los niños Yerko Contreras y Cristian Barrios estudiantes del programa de talentos de la Universidad Sergio Arboleda, durante el segundo semestre de 2004.

2. Si $b = 0$ y $x = 0$ no es una solución, la ecuación queda

$$ax^2 + c = 0$$

multiplicando por x y teniendo en cuenta que para todo x en V, $x^3 = 1$

$$a + cx = 0.$$

3. Si $c = 0$, la ecuación queda

$$ax^2 + bx = 0$$

factorizando x

$$x(ax + b) = 0$$

cuyas soluciones son $x = 0$ o $x = ba^2$.

4. Veamos ahora ecuaciones de la forma

$$ax^2 + bx + c = 0$$

donde a, b y c son diferentes de 0.

Supongamos que la ecuación *tiene solución*, entonces si sumamos c en ambos lados de la ecuación

$$c = ax^2 + bx$$

elevando al cubo

$$c^3 = (ax^2 + bx)^3$$

desarrollando el cubo (y aplicando de nuevo que para todo c en V se cumple que $c^3 = 1$),

$$1 = (ax^2)^2(bx) + (ax^2)(bx)^2$$

o sea

$$1 = a^2x^2b + axb^2$$

factorizando

$$1 = ab(ax^2 + xb)$$

reemplazando en el interior del paréntesis, $ax^2 + xb = c$, obtenemos finalmente que:

$$1 = abc.$$

Esto significa que la ecuación tiene solución si el producto de todos sus coeficientes es 1, lo que implica que *todos los coeficientes son iguales* o *todos son diferentes* entre sí; y diferentes de 0 y por lo tanto, si solo dos de los coeficientes son iguales, la ecuación no tiene solución.

Supongamos ahora que $a = b = c$, pero $a \neq 0$, entonces la ecuación es

$$ax^2 + ax + a = 0.$$

O lo que es igual

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

y cancelando a, queda

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

cuyas soluciones son $x = 2$ y $x = 3$.

La ecuación

$$ax^2 + ax + a = 0.$$

también admite la factorización[10]:

$$(ax + 2a)(x + 3) = 0$$

es decir que

$$a(x + 2) = 0 \quad \vee \quad x + 3 = 0$$

cuyas soluciones son $x = 2$ y $x = 3$.

En el campo de Klein se tiene que, si a, b y c son diferentes entre sí y todos diferentes de 0, entonces

$$a + c = b.$$

Reemplazamos en la ecuación y obtenemos

$$ax^2 + bx + c = ax^2 + (a + c)x + c = 0$$

multiplicamos por a

$$(ax)^2 + (a + c)ax + ca = 0$$

y factorizamos

$$(ax + a)(ax + c) = 0$$

[10]Debemos tener cuidado con la interpretación de $2a$ que significa 2 multiplicado por a y no $a + a$.

luego

$$ax + a = 0 \qquad \vee \qquad ax + c = 0$$

o lo que es igual

$$a(x + 1) = 0 \qquad \vee \qquad ax = c$$

lo que significa que

$$x = 1 \qquad \vee \qquad x = \frac{c}{a}$$

Ejemplo

Para resolver

$$3x^2 + 2x + 1 = 0$$

la factorizamos como

$$(3x + 1)(x + 1) = 0$$

y por lo tanto

$$3x + 1 = 0 \qquad \vee \qquad x + 1 = 0$$

o sea que

$$x = \frac{1}{3} = 2 \qquad \vee \qquad x = 1.$$

Las 18 ecuaciones que tienen como coeficientes a:

a	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	3	3
b	1	1	2	3	2	3	1	1	2	2	3	3	1	1	2	2	3	3
c	2	3	1	1	2	3	1	2	1	3	2	3	1	3	3	2	1	2

Tabla 20

y las tres ecuaciones de la forma $0x^2 + 0x + c = 0$, con $c \neq 0$, no tienen solución.

3.3. Extensiones del campo de Klein

Cuando estudiamos los números reales, también encontramos ecuaciones que no tenían solución y el problema lo arreglamos incluyendo un nuevo símbolo i, con la condición de que $i^2 = -1$, lo que dio como resultado el campo de los números complejos donde toda ecuación polinómica, no solo de segundo grado, sino de grado n tiene solución[11].

[11]Un campo donde toda ecuación polinómica tenga solución se llama *algebraicamente cerrado*. Para ver que los complejos lo son sugerimos ver (LENTIN, Op. cit., p. 259-261).

Aquí, esta solución no es útil, pues todo número en el campo de Klein tiene raíz cuadrada; pero podemos estudiar las condiciones para ampliar nuestro campo de números e incluir un nuevo símbolo, de manera que una ecuación particular, como por ejemplo

$$x^2 + x + 2 = 0$$

tenga solución dentro del nuevo campo, para ello incluyamos un símbolo δ que satisfaga la ecuación

$$\delta^2 + \delta + 2 = 0$$

y consideremos números de la forma

$$z = a + b\delta$$

los sumamos componente a componente y los multiplicamos de acuerdo a

$$(a + b\delta)(c + d\delta) = (ac) + (ad + bc)\delta + bd\delta^2$$

donde debemos reemplazar, cada vez que aparezca

$$\delta^2 = \delta + 2$$

entonces

$$(a + b\delta)(c + d\delta) = (ac + 2bd) + (ad + bc + bd)\delta$$

Con esto obtenemos un nuevo campo. El elemento idéntico para la multiplicación es $1 = 1 + 0\delta$, el inverso multiplicativo del número (a, b) es

$$(a, b)^{-1} = \left(\frac{a + b}{a^2 + ab + 2b^2}, \frac{b}{a^2 + ab + 2b^2} \right)$$

y la expresión $a^2 + ab + b^2$ solo es 0 cuando $a = b = 0$.

Ejercicios

En la extensión definida para el campo de Klein

1. *Verifique que la multiplicación es asociativa y distributiva con respecto a la suma.*

2. *Verifique que $a^2 + ab + b^2$ solo es 0 cuando $a = b = 0$.*

Si queremos construir un campo donde toda ecuación cuadrática con coeficientes en el campo de Klein tenga solución, parecería que deberíamos hacer 18 extensiones como la anterior. Por fortuna esto no es así; si multiplicamos la ecuación

$$\delta^2 + \delta = 2$$

por 2, obtenemos

$$2\delta^2 + 2\delta = 3$$

que es otra de las ecuaciones que no tiene solución y también si multiplicamos por 3

$$3\delta^2 + 3\delta = 1.$$

Esto quiere decir que tres ecuaciones tienen la misma solución δ. Así mismo con las otras ecuaciones lo que divide nuestro problema entre tres, es decir, nos quedan seis soluciones extrañas, las correspondientes a las ecuaciones:

1. $x^2 + x + 2 = 0$
2. $x^2 + x + 3 = 0$
3. $x^2 + 2x + 1 = 0$
4. $x^2 + 3x + 1 = 0$
5. $x^2 + 2x + 2 = 0$
6. $x^2 + 3x + 3 = 0.$

Podemos eliminar incluso tres de las soluciones; por ejemplo si asumimos como soluciones δ y β para las dos primeras ecuaciones y sumamos, tenemos que

$$\delta^2 + \delta + 2 = 0$$

$$\beta^2 + \beta + 3 = 0$$

$$\delta^2 + \beta^2 + \delta + \beta + 2 + 3 = 0$$

que es equivalente a

$$(\delta + \beta)^2 + (\delta + \beta) + 1 = 0$$

lo que significa que $\delta + \beta$ satisface la ecuación

$$x^2 + x + 1 = 0$$

cuyas soluciones son

$$x = 2 \text{ y } x = 3$$

esto es

$$\delta + \beta = 2 \text{ o } \delta + \beta = 3$$

y a su vez

$$\beta = \delta + 2 \text{ o } \beta = \delta + 3.$$

lo que significa que podemos eliminar β. Similarmente eliminamos otras dos soluciones y finalmente quedan tres soluciones extrañas que podemos llamar δ para la ecuación 1 ($\delta+2$, $\delta+3$ para 2), α para la ecuación 3 ($\alpha+1$, $\alpha+3$ para 5), y ϕ para la ecuación 6 ($\phi+1$, $\phi+2$ para 4).

Aún más, estas tres soluciones las podemos reducir a una: recordemos que cuando multiplicamos la ecuación

$$\delta^2 + \delta + 2 = 0$$

por 2, obtuvimos

$$2\delta^2 + 2\delta + 3 = 0$$

pero esta ecuación la podemos interpretar como

$$3^2\delta^2 + 3(3\delta) + 3 = 0$$

es decir,

$$(3\delta)^2 + 3(3\delta) + 3 = 0$$

lo que nos indica que 3δ es solución de la ecuación 6, luego $\phi = 3\delta$.

De manera similar si reinterpretamos

$$3\delta^2 + 3\delta + 1 = 0$$

como

$$2^2\delta^2 + 2(2\delta) + 1 = 0$$

es decir,

$$(2\delta)^2 + 2(2\delta) + 1 = 0$$

tenemos que 2δ es solución de la ecuación 3, por tanto, $\alpha = 2\delta$.

Todo lo anterior nos indica que las 18 ecuaciones que no tiene solución en V, sí tienen solución dentro del campo que construimos anteriormente, a partir de la inclusión del símbolo δ que satisface la ecuación $\delta^2 + \delta + 2 = 0$.

Formalmente, este campo es la extensión de V por δ, que llamamos

$$V(\delta) = \{a + b\delta : a, b \in V \wedge \delta^2 + \delta + 2 = 0\}.$$

Veamos entonces que en $V(\delta)$ toda ecuación de la forma

$$x^2 + cx + d = 0 \qquad (1)$$

con $c, d \in V$, tiene solución, es decir existe $a + b\delta \in V(\delta)$ tal que

$$(a + b\delta)^2 + c(a + b\delta) + d = 0.$$

Prueba: si partimos de la ecuación anterior obtenemos

$$(a^2 + 2b^2 + ca + d) + (b^2 + cb)\delta = 0$$

que tiene solución si y solo si

$$a^2 + 2b^2 + ca + d = 0 \qquad (2)$$

y

$$b^2 + cb = 0 \qquad (3)$$

Esta última ecuación implica que $b = 0$ o $b = c$.

Si la ecuación (1) tiene como solución a en V, entonces podemos tomar $b = 0$ y $a + 0\delta$ en $V(\delta)$ será solución de la ecuación (1).

Por otro lado, si la ecuación (1) no tiene solución en V, entonces haciendo $b = c$ y reemplazando en (2) obtenemos

$$a^2 + 2c^2 + ca + d = 0$$

que es equivalente a

$$a^2 + ca + (2c^2 + d) = 0,$$

una ecuación en V que tiene solución en V, ya que si la ecuación (1) no tiene solución en V entonces debe darse alguno de los siguientes seis casos

	c	d
1.	1	2
2.	1	3
3.	2	1
4.	2	2
5.	3	1
6.	3	3

En los casos 1, 3 y 6 tenemos que $2c^2 + d = 0$ por tanto

$$a^2 + ca + (2c^2 + d) = a^2 + ca = a(a + c) = 0$$

en consecuencia $a = 0$ o $a = c$, lo que nos permite concluir que $0 + c\delta$ y $c + c\delta$ son soluciones de (1) en $V(\delta)$.

Por otro lado, en los casos 2, 4 y 5 obtenemos que 1, c y $2c^2 + d$ son todos iguales o todos diferentes entre sí, lo que hace que la ecuación $a^2 + ca + (2c^2 + d) = 0$ tenga solución en V. Luego si e y f son las soluciones en V de tal ecuación, entonces verificamos fácilmente que $e + c\delta$ y $f + c\delta$ son soluciones de (1) en $V(\delta)$.

3.4. Estructuras en el conjunto de las ecuaciones con coeficientes en el campo de Klein

Las 43 ecuaciones que sí tienen solución en el campo de Klein, con sus soluciones respectivas son:

Ecuación	Soluciones
$0x^2 + 0x + 0 = 0$	0, 1, 2, 3
$0x^2 + x + 0 = 0$	0
$0x^2 + x + 1 = 0$	1
$0x^2 + x + 2 = 0$	2
$0x^2 + x + 3 = 0$	3
$0x^2 + 2x + 0 = 0$	0
$0x^2 + 2x + 1 = 0$	3
$0x^2 + 2x + 2 = 0$	1
$0x^2 + 2x + 3 = 0$	2
$0x^2 + 3x + 0 = 0$	0
$0x^2 + 3x + 1 = 0$	2
$0x^2 + 3x + 2 = 0$	3
$0x^2 + 3x + 3 = 0$	1
$x^2 + 0x + 0 = 0$	0
$x^2 + 0x + 1 = 0$	1
$x^2 + 0x + 2 = 0$	3
$x^2 + 0x + 3 = 0$	2

$x^2 + x + 0 = 0$	0, 1
$x^2 + x + 1 = 0$	2, 3
$x^2 + 2x + 0 = 0$	0, 2
$x^2 + 2x + 3 = 0$	1, 3
$x^2 + 3x + 0 = 0$	0, 3
$x^2 + 3x + 2 = 0$	1, 2
$2x^2 + 0x + 0 = 0$	0
$2x^2 + 0x + 1 = 0$	2
$2x^2 + 0x + 2 = 0$	1
$2x^2 + 0x + 3 = 0$	3
$2x^2 + x + 0 = 0$	0, 3
$2x^2 + x + 3 = 0$	1, 2
$2x^2 + 2x + 0 = 0$	0, 1
$2x^2 + 2x + 2 = 0$	2, 3
$2x^2 + 3x + 0 = 0$	0, 2
$2x^2 + 3x + 1 = 0$	1, 3
$3x^2 + 0x + 0 = 0$	0
$3x^2 + 0x + 1 = 0$	3
$3x^2 + 0x + 2 = 0$	2
$3x^2 + 0x + 3 = 0$	1
$3x^2 + x + 0 = 0$	0, 2
$3x^2 + x + 2 = 0$	1, 3
$3x^2 + 2x + 0 = 0$	0, 3
$3x^2 + 2x + 1 = 0$	1, 2
$3x^2 + 3x + 0 = 0$	0, 1
$3x^2 + 3x + 3 = 0$	2, 3

Tabla 21

En la tabla vemos que hay ecuaciones que tienen el mismo conjunto de soluciones, por ejemplo,

$$x^2 + 3x + 2 = 0$$

$$2x^2 + x + 3 = 0$$

$$3x^2 + 2x + 1 = 0$$

tienen como soluciones, $x = 1$ y $x = 2$.

Lo mismo sucede con los conjuntos de ecuaciones

$$x^2 + x + 0 = 0$$

$$2x^2 + 2x + 0 = 0$$

$$3x^2 + 3x + 0 = 0$$

que tienen como soluciones, $x = 0$ y $x = 1$.

En el conjunto de todas las ecuaciones cuadráticas solubles en el campo de Klein podemos definir una clasificación con el criterio de que tengan las mismas soluciones, y para simplificar la notación, escribiremos (a, b, c) para representar la ecuación

$$ax^2 + bx + c = 0.$$

Con esto obtenemos, en el caso de dos soluciones diferentes, las clases:

A $= \{(1, 1, 0), (2, 2, 0), (3, 3, 0)\}$ cuyas soluciones son $x = 0$ y $x = 1$.
B $= \{(1, 2, 0), (2, 3, 0), (3, 1, 0)\}$ cuyas soluciones son $x = 0$ y $x = 2$.
C $= \{(1, 3, 0), (2, 1, 0), (3, 2, 0)\}$ cuyas soluciones son $x = 0$ y $x = 3$.
D $= \{(1, 3, 2), (2, 3, 1), (3, 2, 1)\}$ cuyas soluciones son $x = 1$ y $x = 2$.
E $= \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\}$ cuyas soluciones son $x = 1$ y $x = 3$.
F $= \{(1, 1, 1), (2, 2, 2), (3, 3, 3)\}$ cuyas soluciones son $x = 2$ y $x = 3$.

En esta clasificación, las ecuaciones que tienen las mismas soluciones son esencialmente la misma, en el sentido habitual del algebra, pues podemos convertir una de ellas en otra, multiplicando por un mismo número en ambos lados de la ecuación, por ejemplo, si en la clase D multiplicamos la ecuación

$$x^2 + 3x + 2 = 0$$

por 3, obtenemos

$$3x^2 + 2x + 1 = 0.$$

Y si la multiplicamos por 2, nos da

$$2x^2 + x + 3 = 0.$$

En resumen, las tres ecuaciones son *equivalentes.*

En cada conjunto de ecuaciones equivalentes podemos definir una suma

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f)$$

y si agregamos en cada conjunto la ecuación

$$0x^2 + 0x + 0 = 0$$

que aunque no es equivalente a las demás, sí comparte con ellas las soluciones, obtenemos, en cada caso, una representación del grupo de Klein.

Ejercicios

1. *Encuentre la función que define el isomorfismo entre las clases A, B, etc., y el grupo de Klein.*
2. *Estudie estructuras para el conjunto de ecuaciones equivalentes con una sola solución.*
3. *Estudie estructuras en el conjunto de ecuaciones que comparten al menos una solución.*

3.5. Otras estructuras finitas

Cuando el número de elementos de un conjunto aumenta, el número de operaciones posibles se incrementa enormemente, pues en un conjunto con k elementos son posibles k^{k^2} operaciones; por esta razón miraremos solamente algunas estructuras de grupo.

Al referirnos a la operación de un grupo G, algunas veces utilizaremos la notación multiplicativa (sin símbolo para la operación), que nos permite definir para cualquier a en G,

$$a^0 = e, \qquad a^1 = a, \qquad a^2 = a \cdot a, \qquad a^3 = a \cdot a \cdot a$$

y de manera general,

$$a^k = a \cdot a^{k-1} \qquad \text{y} \qquad a^{-k} = (a^{-1})^k$$

donde e es el elemento idéntico, k es un número entero cualquiera, y además se cumple que $a^m \cdot a^n = a^{m+n}$ y $(a^m)^n = a^{mn}$ con n, m números enteros cualesquiera.

En un grupo G, para cada elemento a de G podemos formar el conjunto $\{a^i : i \in Z\}$. Este conjunto con la operación definida en G forma un grupo, que llamaremos el subgrupo generado por $\{a\}$ y lo notamos $\langle a \rangle$.

3.5.1. Grupos cíclicos

Un grupo G es *cíclico* si es generado por uno de sus elementos.

Ejemplo

Los grupos $(Z_n, +)$: si $\langle a \rangle$ es un grupo cíclico finito con n elementos, entonces

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Por la definición, los elementos del grupo cíclico $\langle a \rangle$ se pueden representar por la sucesión infinita de símbolos $\ldots, a^{-2}, a^{-1}, a, a^2, \ldots$ y como $\langle a \rangle$ es finito, en la sucesión anterior deben existir i, j tales que $a^i = a^j$. Si $i < j$ entonces multiplicamos en ambos lados de la igualdad por a^{-i} y obtenemos $a^{j-i} = e$, donde $j - i > 0$. Si m es el menor entero positivo tal que $a^m = e$ entonces los elementos $e, a, a^2, \ldots, a^{m-1}$ son diferentes. Llamaremos T al conjunto de los elementos diferentes de $\langle a \rangle$

$$\mathrm{T} = \{e, a, a^2, \ldots, a^{m-1}\}.$$

Si a^t es cualquier elemento de $\langle a \rangle$, dividiendo a t entre m obtenemos $t = mq + r$ donde $0 \leq r < m$, luego:

$$a^t = a^{mq+r} = (a^m)^q a^r = e^q a^r = a^r$$

y como $r < m$ entonces el elemento a^r está en T. En conclusión $\mathrm{T} = \langle a \rangle$.

Para cada entero positivo n la anterior estructura la llamaremos el grupo $(Z_n, +)$. Representaremos habitualmente esta estructura con el conjunto

$$Z_n = \{0, 1, 2, 3, 4, , \ldots (n-1)\}$$

y la operación la definiremos por

$$a + b = res\left(\frac{a \oplus b}{n}\right)$$

donde la operación $\oplus$ es la suma habitual de números enteros y $res\left(\frac{a \oplus b}{n}\right)$ significa tomar el residuo de la división de la suma usual de a con b entre n.

En particular $(Z_6, +)$ es generado por $\{1\}$ y $\{5\}$, pero también es generado por $\{2, 3\}$ puesto que $2 + 3 = 5$. También es generado por $\{3, 4\}$, $\{2, 3, 4\}$, $\{1, 3\}$ y $\{3, 5\}$ pero no es generado por $\{2\}$, pues $\langle 2 \rangle = \{0, 2, 4\}$.

3.5.2. Los grupos de permutaciones

Sea X $= \{0, 1, 2, \ldots, n-1\}$, el conjunto de las funciones biyectivas de X en X con la operación composición forman un grupo de orden $n!$ que notamos S_n. Cada una de esas funciones recibe el nombre de permutación y podemos representarla mediante una matriz $2 \times n$ cuya primera fila son los elementos de X y cuya segunda fila está formada por las imágenes de los elementos de la primera.

Ejemplo

El conjunto de las funciones biyectivas de $\{0, 1, 2\}$ en $\{0, 1, 2\}$, cuyos elementos son

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

junto con la composición habitual de funciones, forman el grupo S_3

$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_5	f_0	f_4	f_3	f_1
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_3	f_1	f_2	f_5	f_0
f_5	f_5	f_2	f_3	f_1	f_0	f_4

Tabla 22

Ahora, si llamamos

$$a = f_5 \qquad b = f_2 \qquad e = f_0$$

notamos que

$$a^2 = f_4 \qquad ab = f_3 \qquad a^2b = f_1$$

por tanto,

$$S_3 = \{e, a, a^2, b, ab, a^2b\}$$

y si asumimos que formamos un grupo con las condiciones:

$$a^3 = e$$
$$b^2 = e$$
$$a^2b = ba$$

obtenemos la tabla:

$\circ$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Tabla 23

3.5.2.1. Una representación matricial de S_3

El conjunto de matrices[12] con entradas en el campo Z_3

$$G = \{a, b, c, d, e, f\}$$

donde

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, d = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, e = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \text{ y } f = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$$

con la multiplicación usual de matrices, tiene como tabla

$\times$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

Tabla 24

y es isomorfo con el grupo S_3.

[12]DIXON, John. Problems in group theory. New York: Dover, 1973. p. 23.

3.5.3. Los grupos diedros

Para cada número par $n = 2k$, con k un entero mayor que 2, podemos formar un grupo con n elementos, que notamos D_{2k}, partiendo de dos elementos a y b tales que:

1. $b^k = a^2 = e$, $b^m \neq e$ si $0 < m < k$ y $a \neq e$,
2. $ba = ab^{-1}$,

los elementos de D_{2k} son de la forma $b^m a^i$ donde $0 \leq m < k$ e $i = 0$ o 1.

Ejemplos

1. Un ejemplo de grupo diedro, para $k = 3$ esta dado por el grupo G generado por los elementos x e y, tales que $x^3 = y^2 = (xy)^2 = 1$, donde 1 es el elemento idéntico.

   Como $x^3 = 1$, $y^2 = 1$, y $(xy)^2 = (xy)(xy) = 1$ entonces si operamos a cada lado de la igualdad $(xy)(xy) = 1$ por y, teniendo en cuenta que la operación es asociativa y que 1 es el elemento neutro, se tiene

   $$(xy)x = y$$

   de aquí, multiplicando por x^2, obtenemos

   $$yx = x^2y.$$

   De manera análoga llegamos a que $yx^2 = xy$, concluyendo así que

   $$\mathrm{G} = \{1, x, y, x^2, xy, x^2y\}$$

   y que la operación esta dada por

$*$	1	x	y	x^2	xy	x^2y
1	1	x	y	x^2	xy	x^2y
x	x	x^2	xy	1	x^2y	y
y	y	x^2y	1	xy	x^2	x
x^2	x^2	1	x^2y	x	y	xy
xy	xy	y	x	x^2y	1	x^2
x^2y	x^2y	xy	x^2	y	x	1

Tabla 25

Notemos que $xy = yx^2 = yx^{-1}$. En este caso podemos reemplazar la condición 2. de la definición de grupo diedro, $xy = yx^{-1}$, por la condición $(xy)^2 = 1$ y caracterizar la estructura con dos sistemas de axiomas.

Si notamos a 1, x, y, x^2, xy y x^2y, como a, b, c, d, e y f, respectivamente, la operación esta dada por la tabla

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	d	e	a	f	c
c	c	f	a	e	d	b
d	d	a	f	b	c	e
e	e	c	b	f	a	d
f	f	e	d	c	b	a

Tabla 26

En esta tabla, a es el elemento idéntico, y las condiciones (adicionales a ser un grupo) que definen la estructura son: $a^2 = a$, $bd = a$, $c^2 = a$, $db = a$, $e^2 = a$ y $f^2 = a$. Además, la operación $*$ es elástica.

2. Otro ejemplo de grupo diedro es el correspondiente a $k = 4$, que esta dado por el grupo G generado por dos elementos a y b tales que

   i. $b^4 = a^2 = e$

   ii. $ba = ab^3$

   donde e es el elemento idéntico.

   Si establecemos la correspondencia

$$e \to 4$$
$$a \to 2$$
$$b \to 6$$
$$b^2 \to 3$$
$$b^3 \to 0$$
$$ab \to 5$$
$$ab^2 \to 7$$
$$ab^3 \to 1$$

la tabla que resulta de las condiciones dadas es:

•	0	1	2	3	4	5	6	7
0	3	2	5	6	0	7	4	1
1	7	4	6	5	1	3	2	0
2	1	0	4	7	2	6	5	3
3	6	5	7	4	3	1	0	2
4	0	1	2	3	4	5	6	7
5	2	3	0	1	5	4	7	6
6	4	7	1	0	6	2	3	5
7	5	6	3	2	7	0	1	4

Tabla 27

3.5.3.1. Una representación matricial de D_8

El conjunto de matrices con entradas en los números enteros

$$\mathrm{M} = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

donde

$$2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad 6 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad 3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad 4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$5 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 7 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ y } \quad 0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

con la multiplicación usual de matrices es isomorfo con D_8.

Ejercicios

1. *Demuestre que el grupo diedro D_6 es isomorfo con el grupo de permutaciones de tres elementos S_3.*

2. *Demuestre que M con la multiplicación usual de matrices es una representación del grupo diedroD_8.*

3.5.4. El grupo de los cuaternios

El grupo de los cuaternios que notamos Q es el grupo de ocho elementos que podemos caracterizar de las siguientes maneras:

1. Un grupo generado por dos elementos a y b que cumplen las siguientes relaciones:
$$a^4 = e,\ b^2 = a^2,\ b^{-1}ab = a^{-1}.$$

2. Un grupo generado por cuatro elementos w, x, y y z, tales que
$$w^2 = x^2 = y^2 = z,\ z^2 = 1, wx = y,\ xy = w \text{ e } yw = x$$
donde 1 el elemento idéntico.

3. Un grupo generado por dos elementos i, j tales que
$$ij = -ji = k$$
con
$$i^2 = j^2 = k^2 = -1$$
y
$$ij = -ji, ik = -ki, jk = -kj.$$

4. Un grupo generado por las matrices $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ y $b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ con entradas en los números complejos y la multiplicación usual de matrices.

Las caracterizaciones 1 y 2 son equivalentes mediante la biyección

$$\begin{aligned} a &\to x \\ b &\to w \\ a^2 &\to z \\ e &\to 1 \\ a^{-1} &\to y \end{aligned}$$

pues

$$a^4 = x^4 = (x^2)^2 = z^2 = 1 = e$$
$$b^2 = w^2 = x^2 = z = a^2$$

y como la condición $b^{-1}ab = a^{-1}$ es equivalente a $aba = b$, entonces

$$aba = a(ba) = x(wx) = xy = w = b.$$

Las caracterizaciones 2 y 3 son equivalentes mediante la biyección

$$\begin{aligned} j &\to x \\ i &\to w \\ 1 &\to 1 \\ k &\to y \\ -1 &\to z \end{aligned}$$

como es fácilmente verificable.

Las caracterizaciones 1 y 4 son equivalentes mediante la biyección

$$\begin{aligned} a &\to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ b &\to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \end{aligned}$$

pues

$$\begin{aligned} a^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e, \\ b^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = a^2 \end{aligned}$$

y se cumple que $b^{-1}ab = a^{-1}$ donde

$$a^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{y} \qquad b^{-1}\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Ejercicios

1. *Demuestre que el grupo diedro D_8 no es isomorfo con el grupo de los cuaternios.*

2. *Construya el grupo $Z_2 \times Z_4$ y encuentre unas condiciones que lo caractericen.*

3. *Construya el grupo $Z_2 \times Z_2 \times Z_2$ y encuentre unas condiciones que lo caractericen.*

4. *¿El grupo $Z_2 \times Z_4$ es isomorfo con el grupo $Z_2 \times Z_2 \times Z_2$? ¿Y cada uno de ellos con el grupo D_8? ¿Y con el grupo de los cuaternios?*

3.5.5. Un grupo con 12 elementos

Un ejemplo de un grupo H, con doce elementos, generado por dos elementos x e y, que satisfacen la primera condición para los grupos diedros, $x^3 = y^2 = 1$, pero la segunda la sustituimos por $(xy)^3 = 1$, es

$$\mathrm{H} = \{1,\ x,\ y,\ x^2,\ xy,\ x^2y,\ yx,\ yx^2,\ xyx,\ yxy,\ xyx^2,\ x^2yx\}$$

y teniendo en cuenta que de tales condiciones se deduce que $yx^2y = xyx$, $(yx)^2 = x^2y$, $(xy)^2 = yx^2$, $x^2yx^2 = yxy$, la tabla de la operación es:

$*$	1	x	y	x^2	xy	x^2y	yx	yx^2	xyx	yxy	xyx^2	x^2yx
1	1	x	y	x^2	xy	x^2y	yx	yx^2	xyx	yxy	xyx^2	x^2yx
x	x	x^2	xy	1	x^2y	y	xyx	xyx^2	x^2yx	yx^2	yxy	yx
y	y	yx	1	yx^2	yxy	xyx	x	x^2	x^2y	xy	x^2yx	xyx^2
x^2	x^2	1	x^2y	x	y	xy	x^2yx	yxy	yx	xyx^2	yx^2	xyx
xy	xy	xyx	x	xyx^2	yx^2	x^2yx	x^2	1	y	x^2y	yx	yxy
x^2y	x^2y	x^2yx	x^2	yxy	xyx^2	yx	1	x	xy	y	xyx	yx^2
yx	yx	yx^2	yxy	y	xyx	1	x^2y	x^2yx	xyx^2	x^2	xy	x
yx^2	yx^2	y	xyx	yx	1	yxy	xyx^2	xy	x	x^2yx	x^2	x^2y
xyx	xyx	xyx^2	yx^2	xy	x^2yx	x	y	yx	yxy	1	x^2y	x^2
yxy	yxy	x^2y	yx	x^2yx	x^2	xyx^2	yx^2	y	1	xyx	x	xy
xyx^2	xyx^2	xy	x^2yx	xyx	x	yx^2	yxy	x^2y	x^2	yx	1	y
x^2yx	x^2yx	yxy	xyx^2	x^2y	yx	x^2	xy	xyx	yx^2	x	y	1

Tabla 28

Si denotamos a $1, x, y, x^2, xy, x^2y, yx, yx^2, xyx, yxy, xyx^2$ y x^2yx, como a, b, c, d, e, f, g, h, i, j, k y l respectivamente, la operación dada por la tabla

$*$	a	b	c	d	e	f	g	h	i	j	k	l
a	a	b	c	d	e	f	g	h	i	j	k	l
b	b	d	e	a	f	c	i	k	l	h	j	g
c	c	g	a	h	j	i	b	d	f	e	l	k
d	d	a	f	b	c	e	l	j	g	k	h	i
e	e	i	b	k	h	l	d	a	c	f	g	j
f	f	l	d	j	k	g	a	b	e	c	i	h
g	g	h	j	c	i	a	f	l	k	d	e	b
h	h	c	i	g	a	j	k	e	b	l	d	f
i	i	k	h	e	l	b	c	g	j	a	f	d
j	j	f	g	l	d	k	h	c	a	i	b	e
k	k	e	l	i	b	h	j	f	d	g	a	c
l	l	j	k	f	g	d	e	i	h	b	c	a

Tabla 29

donde a es el elemento neutro, las condiciones $c^2 = k^2 = l^2 = a$, $bd = db = a$, $eh = he = a$, $fg = gf = a$, $ij = ji = a$, definen la misma estructura.

Ejercicios

1. *Construya el grupo $Z_2 \times Z_2 \times Z_3$ y encuentre unas condiciones que lo caractericen.*

2. *Construya el grupo $Z_2 \times S_3$ y encuentre unas condiciones que lo caractericen.*

3. *¿El grupo $Z_2 \times S_3$ es isomorfo con el grupo $Z_2 \times Z_2 \times Z_3$? ¿Y cada uno de ellos con el grupoH?*

4. *Construya la tabla de la operación que se obtiene, si en el ejemplo anterior, cambiamos las condiciones que deben cumplir x e y, por*

   a) $x^3 = y^2 = (xy)^4 = 1$
   b) $x^4 = y^2 = (xy)^2 = 1$
   c) $x^2 = y^5 = (yx)^3 = 1$

   y en cada caso, solamente aseguramos que la operación es asociativa. ¿Se obtiene una estructura de grupo?, ¿cuáles propiedades cumplen las nuevas operaciones?

5. *Determine cuántos elementos distintos tiene el grupo generado por los elementos x e y, que cumplen las relaciones $xy^2 = y^3x$ y $yx^3 = x^2y$, y construya la tabla de la operación.*

3.6. Retículos

En el capítulo dos estudiamos algunos retículos con dos y con tres elementos, veamos otros ejemplos de retículos finitos[13]:

Ejemplos

1. El retículo N_5 con 5 elementos, cuyo diagrama es:

[13]DUBREIL, Paul y DUBREIL, Marie Louise. Lecciones de álgebra moderna. México: Reverte, 1965. p. 200-201.

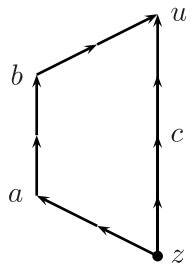


Figura 2

no es distributivo, puesto que

$$a \vee (b \wedge c) = a \vee z = a$$

$$(a \vee b) \wedge (a \vee c) = b \wedge u = b$$

y $a \neq b$.

Como consecuencia de no ser distributivo, el retículo N_5 no es únicamente complementado, aunque sí es complementado, cada elemento tiene un complemento, por ejemplo c y z son complemento de b, puesto que

$$b \wedge c = z \qquad b \vee c = u$$

y

$$b \wedge z = z \qquad b \vee z = u.$$

2. El retículo M_3 cuyo diagrama de Hasse es

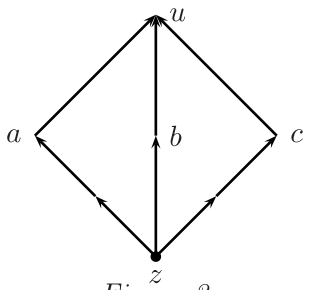


Figura 3

no es distributivo, ya que

$$a \vee (b \wedge c) = a \vee z = a$$

$$(a \vee b) \wedge (a \vee c) = u \wedge u = u$$

pero $a \neq u$ y también

$$a \wedge (b \vee c) = a \wedge u = a$$

$$(a \wedge b) \vee (a \wedge c) = z \vee z = z$$

y $a \neq z$.

En M_3 también cada elemento tiene un complemento, pero no es único.

3. Los retículos de 5 elementos dados por

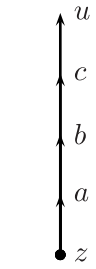


Figura 4

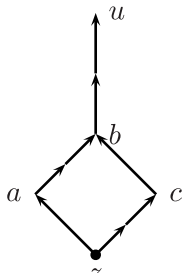


Figura 5

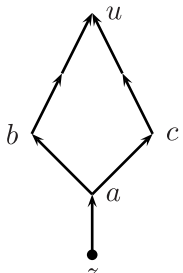


Figura 6

son distributivos.

Ejercicios

1. *Construya las tablas de* $\wedge$ *y* $\vee$ *para los retículos* M_3 y N_5.

2. *Estudie si para cada y en* N_5*, las funciones*

$$\begin{aligned} f_y : \mathrm{N}_5 &\to \mathrm{N}_5 \\ x &\mapsto f_y(x) = y \wedge x \end{aligned}$$

tienen adjunta a derecha.

3. *Demuestre que los retículos mencionados en el numeral 3 de los ejemplos anteriores son distributivos.*

4. *Demuestre que el retículo*

es un álgebra de Heyting.

5. *Estudie los retículos con seis elementos y dé un ejemplo de uno distributivo y uno no distributivo.*

6. *Construya una lógica con cinco elementos.*

CAPÍTULO 4

Estructuras infinitas enumerables

A. ¿Qué cosa es el número?
B. Una cosa.
A. Pero, ¿qué cosa?
B. La que se te antoje.
A. Entonces yo puedo reemplazar
en una ecuación el "1"por lo que se me antoje.
B. Del mismo modo que en $(x + x) - x = x$
puedes reemplazar a x por cualquier número.
A. ¿Puedo reemplazar "1"por la "luna"en $1 + 1 = 2$?

(*Kenny, Anthony*; *Introducción a Frege*)

Hasta el siglo XIX, los números naturales eran usados familiarmente y sin mayores dificultades, los matemáticos los habían aceptado sin preocupación y los empleaban en todos sus estudios. A comienzos del siglo XIX, la aparición de las geometrías no euclidianas condujo a que los matemáticos buscaran los fundamentos de las matemáticas en la aritmética; se consideraba que los números naturales podían ser la base de esta disciplina y se empezó a trabajar en su formalización. Al respecto, Kline[1] señala que el interés por fundamentar la aritmética

> (...) fue el deseo de asegurar la verdad de la matemática. Como consecuencia de la creación de las geometrías no euclidianas, la geometría había perdido su status de verdad, pero parecía

[1]KLINE, Morris. El pensamiento matemático de la antigüedad a nuestros días. Madrid: Alianza, 1972. v. 3. p. 1293.

> todavía que la matemática construida sobre la aritmética ordinaria debía ser una realidad incuestionable en cierto sentido filosófico.

Otra razón que motivó a los matemáticos a cuestionarse frente a la estructura de los números naturales, fue el desarrollo del álgebra y el análisis durante el siglo XIX, incluida la búsqueda de una estructuración clara y precisa de los números reales, que permitiera justificar en forma detallada y suficiente, teoremas y demostraciones relacionadas con ellos. A finales del siglo XIX, específicamente en 1872, aparecieron las teorías formales sobre los números reales, desarrolladas por Charles Méray, Karl Weierstrass, Eduard Heine, Georg Cantor y Richard Dedekind, basadas en algunas propiedades de los números racionales y sus operaciones, los cuales, a su vez, se definen en términos de los números naturales; pero, no se tenía una fundamentación sólida para estos, en términos de Boyer[2] "Todo el mundo cree que sabe lo que es, por ejemplo, el número 3, hasta que intenta definirlo y explicar su significado..." se hizo necesario, entonces, definir los números naturales a partir de algo más básico.

Frente a esta cuestión, surgen diferentes alternativas: algunos matemáticos, estaban confiados en la pureza y simplicidad de los números naturales, señalando que la sucesión ilimitada $1, 2, 3, \ldots$ es la intuición más digna de confianza que le fue dada al hombre; pues, al fin y al cabo, como decía Kronecker, "Dios hizo los enteros; todo lo demás es obra del hombre". De alguna manera, se consideraba que los números naturales brotan en el sentido interno por una especie de intuición originaria del acto de contar.

Entre los matemáticos que buscaban bases más precisas para la aritmética, fue Grassmann el primero en proponer una fundamentación lógica de la aritmética en 1861, empleando el concepto de sucesor y el método de inducción para definir las operaciones y demostrar sus propiedades. Esta línea sería seguida, años después, por Dedekind y Peano.

Otra propuesta fue desarrollada por el alemán Gottlob Frege, quien, a partir de una reflexión sobre la naturaleza de la aritmética y del número hace un balance histórico y filosófico de los resultados conocidos hasta ese momento, y apoyado en las teorías de Boole y Cantor, introdujo una definición para *número cardinal* de un conjunto, identificándolo con la clase de todos los conjuntos que son equivalentes al conjunto dado, es decir, todos los conjuntos cuyos elementos puedan ponerse en correspondencia biunívoca con un conjunto dado. Esta definición apareció en 1884

[2]BOYER, Carl. Historia de la Matemática. Madrid: Alianza Universidad, 1987. p. 733.

en el libro *Die Grundlagen der Arithmetik, eine logischemathematische Untersuchung über den Begriff der Zahl.*

Aunque la idea de clase es muy antigua, según menciona este mismo autor, esta se vislumbra desde la época de Galileo, en 1638, quien presenta en su obra *Diálogo sobre dos nuevas ciencias*[3], una equivalencia una clase y una parte propia de ella[4], en este caso, Galileo planteó una equivalencia entre una clase y una parte propia de ella. Leibniz también presentó un ejemplo de equivalencia entre clases, él planteó que la clase de los números pares y la de los naturales son equivalentes; aunque hubo un error en su conclusión, que luego Cantor subsanó. Bolzano distinguió entre clases finitas e infinitas, fundamental para el desarrollo de la teoría que, con posterioridad, Cantor haría. De hecho, fue George Cantor, quien en 1895 definió clase: "entendemos por clase (Menge) toda reunión (Zusammenfassung) en un solo conjunto de objetos bien distinguidos de nuestra intuición (Anschauung) o de nuestro pensamiento (Denkens)"[5]. Cantor también diferencia entre números cardinales y ordinales, lo cual es indistinguible para clases finitas pero no para las clases infinitas; de este modo se encuentra en la teoría de clases un campo donde es posible definir los números naturales.

Sin embargo, la paradoja de Russell de la clase de todas las clases que no son miembros de sí mismas, pareció hacer fracasar la teoría de clases de Frege, como él mismo lo manifiestó en 1903 con la publicación del segundo volumen de su obra: "No hay nada menos apetecible para un hombre de ciencia que cuando está a punto de terminar su obra se le derrumben los cimientos. En esta situación me pone una carta del señor Bertrand Russell recibida cuando la obra estaba a punto de salir de la imprenta."[6]; esto llevó a la búsqueda de otros cimientos libres de contradicciones para las matemáticas, desde un razonamiento lógico más estricto.

La paradoja de Russell, tuvo varias consecuencias, entre ellas, la inconsistencia de la teoría de conjuntos hasta ahora desarrollada; sin embargo, tal paradoja no hacía que la teoría de conjuntos se invalidará, pero eran necesarias alternativas de solución; una fue planteada por el mismo Russell, la teoría de tipos, y otra, la axiomática de Zermelo, que luego Skolem y Von

[3]GALILEI, Galileo. Diálogo sobre dos nuevas ciencias. En : Hawking, Stephen. A Hombros de Gigantes. Barcelona: Crítica, 2003. p. 376.

[4]Galileo afirma que hay tantas raíces como cuadrados y tantas raíces como números naturales; en palabras actuales, la clase de los números naturales es equivalente con la clase de los cuadrados de los números naturales.

[5]BELL, Eric. Historia de las Matemáticas. México: Fondo de Cultura Económica, 2002. p. 286.

[6]Ibid., p. 293.

Neumann retomarían; la axiomática de Zermelo se constituyó después en una base para definir los números naturales desde la óptica conjuntista.

La axiomatización de los números naturales más conocida es la de Giuseppe Peano, presentada en 1889, en *Arithmetices principia nova método exposita*. Tal desarrollo se fundamenta en una teoría de los números enteros propuesta por Dedekind en 1888, basado, a su vez, en las ideas conjuntistas de Cantor. La intención de Peano era desarrollar un lenguaje formalizado para las matemáticas, libre de ambigüedades e intuiciones, y para el caso de la aritmética, abordó el trabajo de reducirla a un conjunto de postulados, necesarios y suficientes para todas las demostraciones y libres de hipótesis implícitas. Para ello, usó tres conceptos primitivos (número natural, número uno y ser sucesor), cinco axiomas y la idea de definición recursiva para las operaciones, con lo cual caracterizó por completo la noción de número natural, estableció y demostró las propiedades de los números naturales respecto a las operaciones.

En este capítulo presentaremos una parte de la forma original del trabajo de Peano y un desarrollo de sus ideas siguiendo los lineamientos de Edmund Landau, cambiando el 1 por el 0 como primer elemento, donde demostramos que las operaciones de suma y multiplicación y el orden se deducen de los axiomas. Seguidamente mostramos una versión moderna de los axiomas de Peano y comparamos algunas demostraciones con las versiones iniciales.

Luego abordamos otras propuestas, incluso anteriores a la de Peano, que también formalizan el concepto de número natural. El norteamericano Charles Peirce presentó en 1881 un sistema de axiomas para los números naturales en el artículo *On the logic of number, publicado en la revista The American journal of mathematics*. Su intención de axiomatizar la aritmética se nota en las primeras frases del artículo:

> "Nadie puede poner en duda las propiedades elementales concernientes al número: las que no son manifiestamente verdaderas a primera vista se verifican mediante las demostraciones usuales. Pero aunque vemos que son verdaderas, no vemos tan fácilmente con precisión por qué son verdaderas; tanto es así que un lógico inglés de renombre ha abrigado la duda si serían verdaderas en todo el universo. El objetivo de este artículo es mostrar que ellas son consecuencias estrictamente silogísticas de unas pocas proposiciones primarias"[7].

[7]PEIRCE, C. On the Logic of Number. Citado por BEDOYA, Lina. Peano, Lawvere,

En su teoría toma como términos indefinidos: un conjunto N y *una relación* R *de orden* en este conjunto, propone cuatro axiomas y define las operaciones en forma recursiva, con lo cual demuestra las propiedades de estas. Luego amplía las pruebas de estas propiedades para abarcar otros números considerando, por ejemplo, la infinitud en ambas direcciones. Estudiamos la versión de Peirce y demostramos que es equivalente a la de Peano.

Enseguida vemos que también es posible caracterizar a los números naturales utilizando una estructura algebraica de semigrupo naturalmente ordenado y demostramos que esta versión es equivalente a la de Peirce y por lo tanto a la de Peano.

A continuación estudiamos una propuesta radicalmente diferente propuesta por el norteamericano F. William Lawvere en 1945, que consiste en traducir los axiomas de Peano al lenguaje de objetos y morfismos propio de la teoría de categorías, de donde obtenemos la noción de objeto *números naturales* esta versión también es equivalente a la de Peano.

Finalmente incluimos la teoría de los números naturales en una teoría más general, la teoría de conjuntos, deducimos de ella los axiomas de Peano y construimos los números naturales como ciertos conjuntos bien ordenados, lo que en un capítulo posterior conduce a los números ordinales como una generalización de los números naturales.

4.1. La estructura de los números naturales

4.1.1. ¿Qué es un número natural?

A esta pregunta podemos darle varias respuestas:

1. Según John Stuart Mill, los números son generalizaciones de agrupaciones de objetos de los que tenemos conciencia como cosas, y no como solo signos. Cuando resolvemos una ecuación algebraica aplicamos en cada paso a a, b y x proposiciones como: *cosas iguales añadidas a cosas iguales hacen cosas iguales, y que cosas iguales sustraídas de cosas iguales dejan cosas iguales.*

Frege refuta esta idea diciendo que hay números no representables por objetos físicos[8] y que el concepto de número también se aplica a colecciones

Peirce: Tres Axiomatizaciones de los Números Naturales. Ibagué, 2003, 54 p. Trabajo de grado (Profesional en matemáticas con énfasis en estadística) Universidad del Tolima. Facultad de Ciencias. Departamento de Matemáticas y Estadística. p. 23.

[8]El número total de átomos del universo conocido no supera 10^{100}.

de cosas abstractas; además, suponer que la suma de números naturales corresponde a una adición física se contradice mezclando algunos líquidos, en los que suceda alguna reacción química, donde la suma es menor que las partes.

Afirma, que un número no puede ser un objeto físico ni una propiedad de los objetos físicos, pues los objetos físicos tienen propiedades de naturaleza muy diversa como el color, el tamaño, la forma, la contextura, la cantidad de moléculas, etc. La mayoría de estas propiedades están bien definidas, no así lo numérico. Además, cada objeto físico o agregado de objetos físicos muestra diferentes números: número de caras, de lados, de vértices, de moléculas, de átomos, de componentes, etc. No hay una cosa que se muestre únicamente como dos o como uno o como tres.

2. Un número es un objeto puramente formal, son signos sin contenido expreso (formalismo), la aritmética, desde este punto de vista, es un juego con signos vacíos, sin significado (números), que se combinan de acuerdo a unas reglas preestablecidas. Frege también rechaza esta posición, afirmando que si los números son solo signos vacíos no tendrían aplicación posible, esto equivale a confundir los símbolos que representan a los números con los números.

3. Un número es una imagen mental, es una idea, una intuición. Y de nuevo Frege refuta:

> "Si el número fuera una representación, la aritmética sería psicología. La aritmética es tan escasamente psicología como por ejemplo lo es la astronomía. Así como ésta no se ocupa de la representación de los planetas, sino de los planetas mismos, de la misma manera el objeto de la aritmética no es representación alguna. Si el dos fuera una representación, esta sería la mía por lo pronto. La representación de otro, sería en cuanto tal, otra representación. De esta manera tal vez tendríamos muchos millones de doses[9] ".

4.1.1.1. La respuesta de Frege

Frege (1848-1925) da una respuesta en 1884, afirma que un número no es una colección de cosas, ni una propiedad de tal colección, ni tampoco el producto subjetivo de un proceso mental, sino que un enunciado numérico afirma algo objetivo acerca de un concepto. Los números son objetos

[9]FREGE, Gottlob. Los fundamentos de la Aritmética, México: Universidad Nacional Autónoma de México, 1972. p. 142.

lógicos que caen bajo determinados conceptos. Un concepto es una función proposicional y cada número tiene una función proposicional que le corresponde.

Por ejemplo, 0 es el número que pertenece al concepto *no idéntico a sí mismo*, que en símbolos es $\exists x(\neg x = x)$; el número de objetos que caen bajo este concepto es cero. El concepto *no idéntico a sí mismo* viene de la lógica donde está definida la identidad y la negación.

1 es el número correspondiente al concepto *idéntico a 0*, solo hay un número que es idéntico a 0 el cual es el 0.

El concepto de *relación biyectiva* es la función proposicional[10]
$\phi(\varphi, a, b, c, d, e, f) = \psi(\varphi, a, b, c)$ y $\eta(\varphi, d, e, f)$, donde
$\psi(\varphi, a, b, c) \equiv$ Si $\varphi(a, b)$ y $\varphi(a, c)$ entonces $b = c$
$\eta(\varphi, d, e, f) \equiv$ Si $\varphi(d, f)$ y $\varphi(e, f)$ entonces $d = e$.

El concepto *F es equinumeroso con el concepto G*, es la función proposicional: *existe una relación biyectiva φ que relaciona las entidades que caen bajo el concepto F con las entidades que caen bajo el concepto G.*

Con esto, *el número que corresponde al concepto F* es la función proposicional *x es equinumeroso a F* y finalmente *n es un número natural o cardinal* es la función proposicional *existe un concepto F tal que n es el número que corresponde al concepto F.*

Lo que Frege intentó en los *Grundlagen der Arithmetik* fue reducir la aritmética a la lógica pero Bertrand Rusell descubrió un error en uno de los principios básicos de su lógica, también numerado el quinto, como el número del famoso postulado de Euclides sobre las paralelas. Así como el quinto postulado dio origen a las geometrías no euclidianas, el mejoramiento del quinto postulado de Frege dio origen a la moderna teoría de conjuntos. Esta misma debilidad señalada por Russell era aplicable también a la teoría de Cantor.

Las teorías de Frege y Cantor son contradictorias pero, es posible trabajar con ellas y obtener muy buenos resultados. La paradoja de Russell hizo que el proyecto fracasara.

Frege al conocer la paradoja insertó en el segundo volumen de *Grundgesetze der Arithmetik* un apéndice en el que debilitaba algunos de sus axiomas pretendiendo eliminar las contradicciones, pero Stanislaw Lesniewski probó, luego de muerto Frege, que incluso su modificación llevaba a con-

[10]PÉREZ, Jesús Hernando. La aritmética según Gottlob Frege. Un ejemplo de matemáticas elementales. En : Memorias XIII Encuentro de Geometría y I de Aritmética. Vol. 1. (jun. 2002); p. 19-33.

tradicción. Su error se basaba en asumir las conclusiones sobre teoría de conjuntos de Cantor sin previa revisión.

En conclusión, Frege fracasó en su intento de derivar la aritmética de la lógica, y fracasó en su intento de mostrar que la naturaleza del número consiste en ser un objeto lógico.

4.1.1.2. La respuesta de Russell

Russell, (1872-1970), no se desanimó con el fracaso de Frege, por el contrario junto con Alfred North Whitehead dedicó sus esfuerzos a encontrar una forma adecuada para axiomatizar las matemáticas que permitiera eliminar las paradojas, así que vuelve a tratar el asunto en 1901.

Inicialmente discute[11] si las palabras que designan un número natural son sustantivos, o adjetivos o ambas cosas, por ejemplo en la frase

Ese conjunto tiene **tres elementos**

la palabra *tres* se usa como adjetivo, pero en la frase

tres **más cinco es igual a ocho**

tres es un sustantivo.

Russell propuso definir *tres* como un adjetivo, es decir precisar qué significa que un conjunto tenga tres (3) elementos y luego definir el sustantivo en términos del adjetivo, de la siguiente forma:

Decimos que un conjunto S tiene tres elementos si y solo si

$$\exists(x, y, z \in S) \text{ tales que } ((x \neq y, y \neq z, x \neq z) \text{ y}$$

$$(\forall w \in \mathrm{S})(w = x \text{ ó } w = y \text{ ó } w = z).$$

o de forma equivalente si y sólo si:

$$(\exists x)(\exists y)(\exists z)\{x \in \mathrm{S} \wedge y \in \mathrm{S} \wedge z \in \mathrm{S} \wedge x \neq y \wedge x \neq z \wedge y \neq z \wedge (\forall w) \\ [w \in \mathrm{S} \rightarrow w = x \vee w = y \vee w = z]\}$$

La fórmula dice que en S existen tres elementos diferentes y solo tres, Henri Poincaré no estuvo de acuerdo con ella, objetando que para escribirla es necesario saber de antemano lo que significa tres para contar las variables

[11] LUQUE, Carlos. El concepto de número natural según Giusseppe Peano. En : Memorias del XIII Encuentro de Geometría y I de Aritmética. Vol 1. (jun. 2002); p. 45-85.

que colocamos en la fórmula; es decir que es necesaria la noción intuitiva aritmética de 3, para que la definición lógica dada tenga sentido; si alguien no supiera contar y no supiera que el conjunto $\{x, y, z\}$ tiene tres elementos, no sabría si la definición es correcta o no.

Russell, por su parte, replicó que no estaba interesado en si las nociones lógicas son *psicológicamente* anteriores a las nociones aritméticas, sino en un sentido estrictamente lógico, la aritmética es reducible a la lógica y la teoría de conjuntos, su definición es buena en el lenguaje de la lógica y la teoría de conjuntos, pues la definición dada caracteriza la propiedad de tener tres elementos.

Russell da una definición de número cardinal que coincide con la de Frege si identificamos la noción de rango[12] de Frege con la suya de clase: un número es una clase de clases equivalentes. También logra *definir* las ideas primitivas de Peano *cero, sucesor y número natural* incluyendo también la inducción matemática como definición y no como un axioma, veamos:

Definiciones

Una *propiedad* se llamará *hereditaria* en los números naturales cuando la cumpla el sucesor de n siempre que la cumpla n. Similarmente una *clase* se dirá *hereditaria* cuando $n + 1$ sea uno de sus elementos siempre que lo sea n.

Una *propiedad* se dirá *inductiva* cuando sea una propiedad hereditaria que la cumpla el cero, y de manera análoga se define una clase inductiva.

La *posteridad* de un número natural con respecto a la relación *antecesor inmediato* es la totalidad de aquellos elementos que pertenecen a toda clase hereditaria a la que el número dado pertenece[13].

Según lo anterior, la posteridad de 0 se compondrá de aquellos términos que pertenezcan a toda clase inductiva y por lo tanto los *números naturales* son la posteridad de 0 respecto de la relación *ser predecesor inmediato de*.

Basado en esta definición de número natural y en la definición de número, que enuncia: "*Un número es todo aquello que sea el número de alguna clase*"[14], determina que: *Cero* es la clase cuyo único miembro es la clase nula. El *sucesor* del número de términos de la clase α es el número de términos de la clase compuesta por α y x, siendo x cualquier término que no pertenece a la clase α. De esta manera los tres términos no definidos de Peano quedan convertidos en tres definiciones.

[12]El rango de la función proposicional que define el concepto.

[13]RUSSELL, Bertrand. Introducción a la filosofía matemática. Barcelona: Paidos, 1988. p. 29.

[14]Ibid., p. 25.

A manera de ejemplo, ¿qué es el número tres desde el punto de vista de Russell? Según él, un número particular no es idéntico a ningún conjunto de términos que tengan este número: el número 3 no es idéntico a un trío particular de personas. El número tres es algo que todos los tríos tienen en común y que los distinguen de otros conjuntos, es decir, los que tienen este número.

Russell se refiere a clases para definir los conjuntos de números. Dos cosas están en la misma clase si tienen el mismo número de términos. Y para determinar cuando dos cosas están en la misma clase Russell plantea: "Cuenta cuántos miembros tiene cada una, si tienen el mismo número entonces están en la misma clase". Sin embargo, para que esto sea posible tendríamos que haber definido los números y suponer que sabemos cómo descubrir cuántos miembros tiene un conjunto.

Russell sostiene que estamos tan adecuados a contar que esto fácilmente lo podemos pasar por alto. Esta afirmación es válida para las clases finitas, y para la clase de los números naturales plantea la definición de clases por extensión o por comprensión. En la primera se nombran uno a uno sus elementos, en la segunda se caracterizan todos mediante alguna afirmación; una definición extensiva puede siempre ser reducida a una comprensiva pero a menudo la comprensiva no puede ser reducida ni tan solo teóricamente a la extensiva. También se dan casos donde la definición comprensiva no es única. Por ejemplo si queremos referirnos a la clase $\{2\}$ que tiene como único elemento al número 2, podemos definirla por comprensión como: la clase cuyo único elemento es el menor número primo, o el único primo par.

Russell afirma que es más simple descubrir si dos conjuntos tienen el mismo número de términos que definir lo que es número. Finalmente declara que:

> "Un número es una clase de clases equivalentes[15]: esta definición nos permite la deducción de todas las propiedades usuales de los números, ya sean finitos o infinitos, y es la única que es posible (hasta donde conozco) para expresar en términos de los conceptos fundamentales de la lógica general."[16]

Como vemos la discusión puede alargarse y profundizarse, sobre todo si acudimos a la opinión de los filósofos[17].

[15]En la parte final de este capítulo trataremos más en detalle este concepto.
[16]RUSSELL, Op. cit., 1988, p. 116.
[17]FREGE, Op. cit., p. 165-189.

4.1.1.3. La respuesta de Peano

En 1889 Giuseppe Peano, no se interesa en ¿qué es un número natural? sino en la manera como ellos se relacionan entre sí; son las reglas del juego de sus interacciones las que determinan su naturaleza, no los objetos en sí.

Como en el juego del ajedrez no tiene sentido la pregunta de cuál es el verdadero sentido de la reina o cuál es su aspecto real, sino cuál es su naturaleza dentro del juego, y solo allí tiene existencia; está definida por la manera como ella se mueve, de manera que podemos jugar con una reina deforme, o una muy bella, o incluso podemos jugar sin fichas, abstraerlas y jugar a ciegas.

Este punto de vista, tan antiguo como Eudoxo o Euclides, conocido como el *método axiomático*, conduce a determinar cuáles son las reglas del juego que definen la naturaleza de los números naturales; esto es, un sistema axiomático para los números naturales.

Euclides en el año 300 a.C, presentó la geometría como un conjunto de proposiciones que se deducen de unas fundamentales llamados *axiomas*, mediante una forma preestablecida de razonar.

En las presentaciones axiomáticas se parte de unos términos no definidos, se enuncian unas relaciones entre ellos, que aceptamos como ciertas (los axiomas), estos no tienen que ser evidentes o universalmente aceptados; se presume una forma correcta de razonar, usualmente la lógica bivalente clásica, y con esto se deducen otras afirmaciones que llamamos teoremas. Los teoremas son ciertos en la medida de que los axiomas lo sean y que los razonamientos sean correctos.

La axiomática no se ocupa de explicar la naturaleza de los objetos matemáticos que forman parte de la teoría, sino las propiedades y las relaciones entre ellos.

En particular, la axiomática de Peano, supone que existen los números naturales y pretende encontrar un sistema simple de axiomas que los caractericen y que nos permitan deducir a partir de ellos[18] las propiedades de los números naturales, utilizando las reglas de la lógica.

La propuesta de Peano de 1889 no fue la única, como ya mencionamos, pero sí la que más rápido se popularizó. Mientras Peano se interesaba por axiomatizar la Aritmética, Hilbert proponía en su libro *Grundlagen der*

[18]En 1931 Kurt Gödel demostró que no existe una teoría matemática que incluya la aritmética y que sea consistente (no es posible deducir de la teoría una proposición p y su negación $\neg p$) y completa, en el sentido de que toda afirmación formulada en términos de la teoría sea demostrable o refutable.

Geometrie de 1899, una axiomatización para la geometría, que no dependía de lo que significaran los términos: punto, recta, y plano.

Peano demostró que los cinco axiomas para los números naturales eran independientes y desarrolló un modelo para demostrar independencia de un sistema de axiomas. En 1898 cambió los axiomas comenzando con el cero en lugar del uno.

La versión de 1889, es la primera versión suya de una axiomatización de las matemáticas en un lenguaje simbólico, en su libro usa la lógica de Boole, Schöder y C. S. Peirce estableciendo una analogía entre operaciones geométricas y algebraicas con las operaciones de la lógica e introduce innovaciones: por ejemplo, usa diferentes símbolos para las operaciones lógicas y matemáticas, distingue entre las proposiciones categóricas y las condicionales, formula una teoría de cuantificación (Frege ya había avanzado en estas direcciones, pero Peano no conocía su trabajo) y fija prácticamente toda su simbología; esta es más manejable que la de Frege, y se hizo popular entre los matemáticos, junto con algunas modificaciones realizadas por Whitehead y Russell, convirtiéndose así en el lenguaje común de la lógica matemática.

En la parte aritmética reconoce los aportes de Dedekind y Grassmann. Su trabajo influyó en Hilbert en su formulación de la geometría y en Whitehead y Russell en su tratamiento de la lógica matemática.

En teoría, el libro consiste de un prefacio y 10 secciones:

1. Números y adición
2. Sustracción
3. Máximos y mínimos
4. Multiplicación
5. Potenciación
6. División
7. Teoremas varios
8. Razones de números
9. Sistemas de racionales e irracionales
10. Sistemas de cantidades.

La primera sección es tratada con cierto nivel de detalle, la segunda, cuarta, quinta y sexta solo dan explicaciones y definiciones, las demás las omite. Una versión completa de la axiomática de Peano fue elaborada por Edmund Landau[19] en 1929.

Las demostraciones en *Arithmetices Principia Nova Método Exposita* son una lista de fórmulas, cada una relacionada con la siguiente, pero no pruebas formales, puesto que no enuncia reglas de inferencia.

La noción del condicional $a \supset b$ que Peano interpreta como "de a se deduce b", permanece vaga en el texto y no usa valores de verdad.

Inicialmente presenta una lista de las nociones aritméticas iniciales (que él llama explicaciones): número, uno, sucesor y "es igual a", para cada una de ellas dice respectivamente:

El signo N significa *número* (entero positivo).
El signo 1 significa *Unidad*
El signo $x + 1$ significa el *sucesor* de x o x más 1
El signo $=$ significa "*igual a*".

En seguida formula nueve axiomas, que relacionan estas nociones:

1. $1 \in \mathrm{N}$
2. $x \in \mathrm{N} \supset x = x$
3. $x, y \in \mathrm{N} \supset x = y. = .y = x.$
4. $x, y, z \in \mathrm{N} \supset x = y.y = z \supset x = z.$
5. $x = y.y \in \mathrm{N} \supset x \in \mathrm{N}$
6. $x \in \mathrm{N} \supset x + 1 \in \mathrm{N}$
7. $x, y \in \mathrm{N} \supset x = y. = .x + 1 = y + 1.$
8. $x \in \mathrm{N} \supset x + 1 \neq 1.$
9. $k \in K \therefore 1 \in k \therefore x \in \mathrm{N}.x \in k \supset x + 1 \in k ::\supset N = \mathrm{k}.$

Los axiomas 2, 3, 4 y 5, se refieren a la igualdad, los restantes cinco axiomas son conocidos como *los axiomas de Peano.*

El axioma 6 establece que para cada número natural existe un sucesor en los números naturales y el axioma 7 afirma que el sucesor de cada número

[19]LANDAU, Edmund. Foundations of Analisys, The Arithmetic of whole, rational, irrational and complex numbers. New York: Chelsea Publishing Company, 1966. p. 1-13.

natural es único y que dos números distintos tienen diferente sucesor. El axioma 8 afirma que 1 no es el sucesor de algún número natural, es decir que es el primero.

El axioma 9, es una traducción del principio de inducción matemática, está formulado en términos de clases y contiene una clase variable "k"e incluye también una clase de todas las clases, K.

A continuación, comienza a introducir nuevos términos en la teoría; es decir, a hacer definiciones; por ejemplo define el número dos como $2 = 1+1$ y demuestra que $2 \in \mathrm{N}$ de la siguiente forma:

$\mathrm{P1} \supset 1 \in \mathrm{N}$ (1)

$1[x](\mathrm{P6}) \supset 1 \in \mathrm{N} \supset 1+1 \in \mathrm{N}$ (2)

$(1)(2) \supset 1+1 \in \mathrm{N}$ (3)

$\mathrm{P10} \supset 2 = 1+1 \in \mathrm{N}$ (4)

$(4).(3).(2, 1+1)[x, y](\mathrm{P5}) \supset 2 \in \mathrm{N}$ (5)

que podemos parafrasear como:

Del primer axioma podemos concluir que $1 \in \mathrm{N}$ (1)

Si aplicamos el axioma 6 reemplazando x por 1, concluimos que $1+1 \in \mathrm{N}$ (2)

De (1) y (2) concluimos que $1+1 \in \mathrm{N}$ (3)

Por la definición[20] de 2 inferimos que $2 = 1+1 \in \mathrm{N}$ (4)

De (4), (3) y de aplicar el axioma 5 a (2, 1 + 1) como $[x, y]$ concluimos que $2 \in \mathrm{N}$. (5)

Luego introduce la adición, multiplicación y potenciación como definiciones; para la adición expresa:

$$x, y \in \mathrm{N} \supset x + (y+1) = (x+y) + 1$$

Esto significa que si x, y son números y si $(x+y)$ es un número, $(x+y)+1$ existe y es un número, definimos $x + (y+1)$ como el sucesor de $(x+y)$.

En la proposición 19 demuestra que

$$x, y \in \mathrm{N} \supset (x+y) \in \mathrm{N}$$

La proposición 22 afirma que

$$x, y, z \in \mathrm{N} \supset x = y \text{ implica que } x + z = y + z$$

[20]En el libro de Peano la proposición 10 (P10) es la definición de $2 = 1+1, 3 = 2+1$, etc.

En la segunda sección introduce los símbolos $-$, $<$ y $>$ y define la sustracción pero no enuncia teorema alguno.

La multiplicación la define, en la cuarta sección, en dos pasos:

1. $x \in \mathrm{N} \supset x \times 1 = x$
2. $x, y \in \mathrm{N} \supset x \times (y + 1) = x \times y + x$

y lo mismo hace con la potenciación:

1. $x \in \mathrm{N} \supset x^1 = x$
2. $x, y \in \mathrm{N} \supset x^{y+1} = x^y \times x$

Como vemos estas definiciones son recursivas, en el sentido de que se define para un primer número y luego se define para el sucesor de un número cualquiera con base en el número; pero no hay justificación para este tipo de definiciones en el sistema de Peano, pues su criterio de definición es que el lado derecho de una ecuación de definición es un *agregado de signos que tienen un significado* y tampoco afirmó que estas definiciones fueran eliminables o deducibles de la teoría[21].

4.1.1.3.1. Algunos teoremas de la aritmética de Peano

En esta sección presentamos con mayor detalle lógico lo hecho en el capítulo 7 de LUQUE, Carlos; MORA, Lyda y PÁEZ, Jorge. Actividades matemáticas para el desarrollo de procesos lógicos: Contar e Inducir. Bogotá: Universidad Pedagógica Nacional, 2002; incluyendo las definiciones de suma y multiplicación como teoremas y el orden como una consecuencia de los axiomas; seguiremos la secuencia de teoremas presentada en el libro de Landau[22] modificando un poco la notación, iniciando en 0 suponiendo que existe un conjunto de número naturales que notaremos N y usando los siguientes axiomas:

A1. 0 es un número natural

A2. Para cada x existe exactamente un número natural, llamado el sucesor de x, que notaremos x^+.

A3. Para todo x se tiene que $x^+ \neq 0$.

[21] El sistema propuesto por Dedekind en 1888 si tiene un teorema (el 126) que permite justificar las definiciones recursivas.

[22] LANDAU, Op. cit., p. 1-13.

A4. Si $x^+ = y^+$ entonces $x = y$.

A5. Si un subconjunto A de los números naturales tiene las siguientes propiedades:

I. 0 pertenece a A

II. Si x pertenece a A entonces x^+ pertenece a A
podemos concluir que A = N.

Enunciamos y demostramos a continuación algunos teoremas:

Teorema L1: si $x \neq y$ entonces $x^+ \neq y^+$.

Prueba: supongamos que $x^+ = y^+$, entonces por el axioma A4 tendríamos que $x = y$, lo cual contradice la hipótesis de que $x \neq y$.

Teorema L2: $x^+ \neq x$.

Prueba: sea M el conjunto de todos los x para los cuales es cierta la afirmación.

I) Por los axiomas A1 y A3 tenemos que $0^+ \neq 0$; por consiguiente, 0 pertenece a M.

II) Si x pertenece a M, entonces $x^+ \neq x$, y aplicando el teorema L1 tenemos que $(x^+)^+ \neq x^+$, por lo que x^+ pertenece a M.

Por el axioma A5, M es igual al conjunto de todos los números naturales, es decir, tenemos que para todo x, $x^+ \neq x$.

Teorema L3: si $x \neq 0$ existe un (y por consiguiente, por el axioma A4, exactamente uno) u tal que $x = u^+$.

Prueba: sea M el conjunto al que pertencen el número 0 y todos aquellos x para los cuales existe tal u. (por el axioma A3, para cualquier x se tiene que $x \neq 0$).

I) 0 pertenece a M.

II) Si x pertenece a M, entonces, existe u tal que $x = u^+$, por el axioma A2 tenemos que $x^+ = (u^+)^+$, de modo que x^+ pertenece a M.

Por el axioma A5, M=N; entonces, para cada $x \neq 0$, existe un u tal que $x = u^+$.

Teorema L4 y a la vez **definición 1:** a cada par de números naturales x, y, asignamos un único número natural, notado $x + y$, tal que:

1. $x + 0 = x$ para todo x en N.

2. $x + y^+ = (x + y)^+$ para cada x y cada y en N.

$x + y$ es llamado *la suma* de x y de y, o el número obtenido por la *adición* de y a x.

Prueba: (A) Primero mostraremos que para cada número natural x fijo pero arbitrario[23] existe a lo más una posibilidad de definir $x + y$ para todo número natural y de tal manera que $x + 0 = x$ y $x + y^+ = (x + y)^+$.

Sean a_y y b_y definidos para todo y, de forma que

$$a_0 = x,\ b_0 = x,\ a_{y^+} = (a_y)^+,\ b_{y^+} = (b_y)^+.$$

Sea M el conjunto de todos los y para los cuales $a_y = b_y$.

I) $a_0 = x = b_0$; por consiguiente 0 pertenece a M.

II) Si y pertenece a M, entonces $a_y = b_y$, luego por el axioma A2, $(a_y)^+ = (b_y)^+$, por consiguiente $a_{y^+} = (a_y)^+ = (b_y)^+ = b_{y^+}$; así que y^+ pertenece a M.

Por tanto, $M = \text{N}$ es decir, que para cada y tenemos $a_y = b_y$.

(B) Ahora debemos mostrar que para cada número natural x es posible definir $x + y$ para todo número natural y, de tal manera que $x + 0 = x$ y $x + y^+ = (x + y)^+$.

Sea M el conjunto de todos los x para los cuales es esto posible (de exactamente una manera, por la parte (A)).

I) Para $x = 0$, el número

$$x + y = y$$

cumple las condiciones, puesto que

$$x + 0 = 0 = x$$

$$x + y^+ = y^+ = (x + y)^+$$

por tanto, 0 pertenece a M.

[23]Cuando hacemos una afirmación para cada x fijo pero arbitrario de un conjunto cualesquiera, la afirmación es válida para todos los elementos del conjunto. (ZEHNA y JOHNSON, Op. cit., p. 25-26).

II) Sea x que pertenece a M, luego existe un $x+y$ para todo y tal que $x+0=x$ y $x+y^+=(x+y)^+$. Entonces el número

$$x^+ + y = (x+y)^+$$

es el número requerido para el numero x^+, pues

$$x^+ + 0 = (x+0)^+ = x^+$$

y

$$\begin{aligned} x^+ + y^+ &= (x+y^+)^+ \\ &= ((x+y)^+)^+ \\ &= (x^+ + y)^+ \end{aligned}$$

por tanto x^+ pertenece a M, y por A5 $M=N$.

Corolario L1: (existencia de elemento idéntico para la adición)

$$x+0=0+x=x$$

Corolario L2: $x^+ + y = (x+y)^+$

Teorema L5: (ley asociativa de la adición)

$$(x+y)+z = x+(y+z)$$

Prueba: fijemos x y y, y denotemos por M al conjunto de todos los z para los cuales la afirmación del teorema es cierta.

I) $(x+y)+0 = x+y = x+(y+0)$, por tanto 0 pertenece a M.

II) Sea z un elemento de M, entonces

$$(x+y)+z = x+(y+z)$$

luego

$$\begin{aligned} (x+y)+z^+ &= ((x+y)+z)^+ \\ &= (x+(y+z))^+ \\ &= x+(y+z)^+ \\ &= x+(y+z^+) \end{aligned}$$

por lo cual z^+ pertenece a M.

De esta manera la afirmación es válida para todo número natural z.

Teorema L6: (ley conmutativa de la adición)

$$x + y = y + x$$

Prueba: fijemos y, y sea M el conjunto de todos los x para los cuales la afirmación es verdadera.

I) Tenemos que $y + 0 = y$, y por el corolario L1, $0 + y = y$, luego $0 + y = y + 0$, por tanto 0 pertenece a M.

II) Si x pertenece a M, entonces $x + y = y + x$, por consiguiente

$$(x + y)^+ = (y + x)^+ = y + x^+.$$

Por el corolario L2, tenemos que

$$x^+ + y = (x + y)^+$$

de donde

$$x^+ + y = y + x^+$$

así que x^+ pertenece a M.

Y la afirmación es válida para todo número natural x.

Teorema L7: si $x \neq 0$, entonces $y \neq x + y$.

Prueba: fijemos x, y sea M el conjunto al que pertencen el número 0 y todos los y para los cuales la afirmación es valida.

I) 0 pertenece a M.

II) Si y pertenece a M, entonces

$$y \neq x + y$$

de donde

$$y^+ \neq (x + y)^+$$

es decir

$$y^+ \neq x + y^+$$

lo que conlleva a que y^+ pertenezca a M y por consiguiente la afirmación es válida para todo número natural y.

Este teorema usualmente se presenta como: si $x + y = y$ entonces $x = 0$.

Teorema L8: (ley cancelativa de la adición) si $y \neq z$ entonces $x + y \neq x + z$.

Prueba: consideremos un número natural y fijo, y un número natural z fijo tal que $y \neq z$, y sea M el conjunto de todos los x para los cuales $x + y \neq x + z$.

I) Como $y \neq z$, tenemos que $0 + y \neq 0 + z$, por tanto 0 pertenece a M.

II) Si x pertenece a M, entonces $x + y \neq x + z$, de donde

$$(x + y)^+ \neq (x + z)^+$$

o sea

$$x^+ + y \neq x^+ + z$$

luego x^+ pertenece a M.

Por consiguiente la afirmación es verdadera para todo número natural x.

La ley cancelativa habitualmente se presenta como: si $x + y = x + z$ entonces $y = z$.

Teorema L9: dados números naturales x y y solo sucede uno de los siguientes casos:

1. $x = y$.
2. Existe un número natural $u \neq 0$ (exactamente uno, por el teorema L8) tal que $x = y + u$.
3. Existe un un número natural $v \neq 0$ (exactamente uno, por teorema L8) tal que $y = x + v$.

Prueba:

A) Los casos 1 y 2 son contradictorios, pues si $x = y$ y $x = y + u$ con $u \neq 0$ entonces $y = y + u$, lo que contradice el teorema L7. El mismo argumento muestra que 1 y 3 son incompatibles. Veamos que 2 y 3 también son incompatibles: Si $x = y + u$, $u \neq 0$ y $y = x + v$, $v \neq 0$ entonces $x = (x+v)+u = x+(v+u)$ y por el teorema L8 concluimos que $v + u = 0$. Como $u \neq 0$, por el teorema L3 existe z en N tal que $z^+ = u$ y por tanto $v + u = v + z^+ = (v + z)^+ = 0$, lo que contradice el axioma A3.

Por consiguiente podemos tener a lo sumo uno de los casos 1, 2 o 3.

B) Sea x fijo, y sea M el conjunto de todos los y para los cuales uno (por la parte A), exactamente uno de los casos 1, 2 o 3 se tiene.

I) Para $y = 0$, tenemos que ó $x = 0 = y$ (caso 1) o por el teorema L3 existe u en N tal que

$$x = u^+ = (0 + u)^+ = 0 + u^+ = y + u^+ \quad \text{(caso 2)},$$

Por tanto 0 pertenece a M.

II) Sea y que pertenece a M. entonces ó $x = y$ de donde $y^+ = x^+ = (x + 0)^+ = x + 0^+$ (caso 3 para y^+).

O $x = y + u$, con $u \neq 0$; por el teorema L3 existe w en N tal que $u = w^+$ y como

$$x^+ = (y + u)^+ = y^+ + u = y^+ + w^+ = (y^+ + w)^+$$

de donde $x = y^+ + w$ (caso 2 para y^+). En particular si $w = 0$, tenemos que $x = y^+$ (caso 1 para y^+).

O $y = x + v$ con $v \neq 0$; luego $y^+ = (x + v)^+ = x + v^+$ (caso 3 para y^+).

En cualquier caso, y^+ pertenece a M. Y por consiguiente siempre tenemos uno de los casos 1, 2 o 3.

Orden en los números naturales

Definición 2: si $x = y + u$ con $u \neq 0$, entonces $x > y$. ($>$ léase "es mayor que")

Definición 3: si $y = x + v$ $v \neq 0$, entonces $x < y$. ($<$ léase "es menor que")

Teorema L10: para cualesquiera x, y dados, se tiene exactamente uno de los casos.

$$x = y, \quad x > y, \quad x < y$$

Prueba: aplicando el teorema L9, la definición 2 y la definición 3.

Teorema L11: si $x > y$ entonces $y < x$.

Prueba: como $x > y$ existe $u \neq 0$ en N tal que $x = y + u$ y como $y < x$ significa que existe $v \neq 0$ en N tal que $x = y + v$, si hacemos $u = v$ conseguimos la conclusión.

Teorema L12: si $x < y$ entonces $y > x$.

Prueba: análoga a la del teorema L11.

Definición 4: $x \geq y$ significa $x > y$ o $x = y$. (léase "mayor o igual que")

Definición 5: $x \leq y$ significa $x < y$ o $x = y$. (léase "menor o igual que").

Teorema L13: si $x \geq y$ entonces $y \leq x$.

Prueba: consecuencia directa del teorema L11.

Teorema L14: si $x \leq y$ entonces $y \geq x$.

Prueba: consecuencia directa del teorema L12.

Teorema L15: si $x < y$, $y < z$, entonces $x < z$.

Prueba: como $x < y$ existe $v \neq 0$ en N tal que $y = x + v$ y como $y < z$ existe $w \neq 0$ en N tal que $z = y + w$ de donde

$$z = (x + v) + w = x + (v + w),$$

lo que significa que

$$x < z.$$

Teorema L16: si ($x \leq y$, $y < z$) o ($x < y$, $y \leq z$), entonces $x < z$.

Prueba: si en la hipótesis vale alguna igualdad, obtenemos la conclusión o si no aplicamos el teorema L15.

Teorema L17: (propiedad transitiva del orden) si $x \leq y$, $y \leq z$, entonces $x \leq z$.

Prueba: si en la hipótesis valen dos igualdades obtenemos la conclusión, si no aplicamos el teorema L16.

Teorema L18: si $y \neq 0$ entonces $x + y > x$.

Prueba: la conclusión se sigue de la igualdad $x + y = x + y$ y de la definición 2.

Teorema L19: (ley de monotonía de la adición) si $x > y$, o $x < y$, entonces $x + z > y + z$, o $x + z < y + z$, respectivamente.

Prueba:

1. Si $x > y$, entonces existe $u \neq 0$ en N tal que

   $$x = y + u,$$

   y por lo tanto

$$\begin{aligned} x + z &= (y + u) + z \\ &= (u + y) + z \\ &= u + (y + z) \\ &= (y + z) + u, \end{aligned}$$

luego

$$x + z > y + z.$$

2. Si $x < y$, entonces $y > x$, de donde, por 1), $y + z > x + z$, es decir, $x + z < y + z$.

Teorema L20: si $x + z > y + z$, o $x + z < y + z$, entonces $x > y$ o $x < y$, respectivamente.

Prueba:

1. Si $x + z > y + z$, entonces existe $u \neq 0$ en N tal que

$$\begin{aligned} x + z &= (y + z) + u \\ &= y + (z + u) \\ &= y + (u + z) \\ &= (y + u) + z \end{aligned}$$

Y por el teorema L8 $x = y + u$, por lo tanto $x > y$.

2. Si $x + z < y + z$, entonces $y + z > x + z$, de donde, por 1), $y > x$, es decir, $x < y$.

Teorema L21: si $x > y$, $z > u$, entonces $x + z > y + u$.

Prueba: por el teorema L19, tenemos que como $x > y$ entonces $x + z > y + z$ y como $z > u$ entonces $z + y > u + y$, luego

$$y + z = z + y > u + y = y + u$$

de donde, por el teorema L15

$$x + z > y + u.$$

Teorema L22: si ($x \geq y$, $z > u$), o ($x > y$, $z \geq u$), entonces $x + z > y + u$.

Prueba: si en la hipótesis vale una igualdad aplicamos el teorema L19, si no aplicamos el teorema L21.

Teorema L23: si $x \geq y$, $z \geq u$, entonces $x + z \geq y + u$.

Prueba: si en la hipótesis valen dos igualdades obtenemos la conclusión, si no aplicamos el teorema L22.

Teorema L24: $x \geq 0$.

Prueba: o $x = 0$ o por el teorema L3, $x = u^+ = (0+u)^+ = 0+u^+$ luego $x > 0$.

Teorema L25: si $y > x$ entonces $y \geq x^+$.

Prueba: como $y > x$ entonces existe $u \neq 0$ en N tal que $y = x+u$. Por el teorema L3 existe w en N tal que $w^+ = u$, luego $y = x + w^+ = (x + w)^+ = x^+ + w$. Si $w = 0$ entonces $y = x^+$, si $w \neq 0$ entonces $y > x^+$.

Teorema L26: si $y < x^+$ entonces $y \leq x$.

Prueba: supongamos que $y > x$, entonces por el teorema L25, $y \geq x^+$ lo que contradice la hipótesis.

Teorema L27: (propiedad reflexiva del orden) $x \leq x$.

Prueba: se tiene la igualdad $x = x$.

Teorema L28: (propiedad antisimétrica del orden) si $x \leq y$ y $y \leq x$ entonces $x = y$.

Prueba: por la definición 5 tenemos que

$$(x < y \text{ o } x = y) \text{ y } (y < x \text{ o } x = y)$$

esto es equivalentes a tener los siguientes cuatro casos:

1. $x < y$ y $y < x$
2. $y < x$ y $x = y$
3. $x < y$ y $y = x$
4. $x = y$ y $y = x$

Los tres primeros casos contradicen el teorema L10. Por tanto se cumple que $x = y$.

Teorema L29: (principio de buen orden) en cada conjunto no vacío de números naturales existe un *mínimo* (es decir, uno que es menor que cualquier otro número del conjunto).

Prueba: sea R un subconjunto no vacío de números naturales y sea M el conjunto de todos los x tales que $x \leq y$ para todo y de R.

Por el teorema L24, el número 0 pertence a M. No todo número natural x pertenece a M pues para cada y de R el número y^+ no pertenece a M, puesto que $y^+ > y$.

Por consiguiente existe un m en M tal que m^+ no pertenece a M; podemos afirmar que $m \leq n$ para todo n de R y que es un elemento de R, pues si m no perteneciera a R, entonces para cada n de R tendríamos $m < n$, de donde, por el teorema L25, $m^+ \leq n$; así m^+ pertenecería a M, contradiciendo la condición con la cual m fue introducida. Luego R tiene elemento mínimo.

Teorema L30 y al mismo tiempo **definición 6:** para cada par de números naturales x, y hay exactamente una manera de asignarle un número natural, notado xy, tal que

$x0 = 0$ para todo número natural x.

$xy^+ = (xy) + x$ para todo x y todo y.

xy es llamado el *producto* de x y y, o el número obtenido de la *multiplicación* de x por y.

Prueba: (palabra por palabra igual que el teorema L4):

A) Primero mostraremos que para cada número natural x fijo existe a lo más una posibilidad de definir xy para todo número natural y de tal manera que $x0 = 0$ y $xy^+ = (xy) + x$ para todo y.

Sean a_y y b_y definidos para todo y, tal que $a_0 = 0$, $b_0 = 0$, $a_{y^+} = a_y + x$, $b_{y^+} = b_y + x$ para todo y.

Sea M el conjunto de todos los y para los cuales $a_y = b_y$.

I) $a_0 = 0 = b_0$, por tanto 0 pertenece a M.

II) Si y pertenece a M, entonces $a_y = b_y$, de donde $a_y + x = b_y + x$ y por tanto $a_{y^+} = b_{y^+}$, por consiguiente y^+ pertenece a M.

Luego $M = N$, es decir, para todo y tenemos que $a_y = b_y$.

B) Ahora debemos mostrar que para cada número natural x, es posible definir xy para todo y de tal manera que $x0 = 0$ y $xy^+ = (xy) + x$ para todo y.

Sea M el conjunto de todos los x para los cuales esto es posible (de exactamente una manera, por la parte (A)).

I) Para $x = 0$, el número

$$xy = 0$$

cumple las condiciones, puesto que

$$x0 = 0 = x,$$

y

$$xy^+ = 0 = xy + 0 = (xy) + x.$$

Por lo tanto 0 pertenece a M.

II) Sea x que pertenece a M, entonces existe un xy para todo y tal que $x0 = 0$ y $xy^+ = (xy) + x$. Entonces el número

$$x^+y = (xy) + y$$

es el número requerido para x^+, pues

$$x^+0 = x0 + 0 = 0$$

y

$$\begin{aligned} x^+y^+ &= (xy^+) + y^+ \\ &= ((xy) + x) + y^+ \\ &= (xy) + (x + y^+) \\ &= (xy) + (x + y)^+ \\ &= (xy) + (x^+ + y) \\ &= (xy) + (y + x^+) \\ &= ((xy) + y) + x^+ \\ &= (x^+y) + x^+. \end{aligned}$$

Por lo tanto x^+ pertenece a M y la afirmación es válida para todo número natural.

Corolario L3: $0x = 0$

Corolario L4: $x^+y = (xy) + y$

Teorema L31: (ley conmutativa de la multiplicación)

$$xy = yx$$

Prueba: fijemos y, y sea M el conjunto de todos los x para los cuales la afirmación es cierta.

I) Tenemos $y0 = 0$ y por el corolario L3, $0y = 0$, de donde $0y = y0$, así que 0 pertenece a M.

II) Si x pertenece a M, entonces $xy = yx$, de donde

$$xy + y = yx + y = yx^+$$

Por el corolario L4, tenemos que

$$x^+y = xy + y$$

de donde

$$x^+y = yx^+$$

y en consecuencia x^+ pertenece a M. La afirmación es verdadera para todo número natural x.

Teorema L32: (ley distributiva de la multiplicación con respecto a la suma)

$$x(y + z) = xy + xz$$

Prueba: fijemos x y y; sea M el conjunto de todos los z para los cuales la afirmación es verdadera.

I) $x(y + 0) = xy = xy + 0 = xy + x0$; por lo que 0 pertenece a M.

II) Si z pertenece a M, entonces

$$x(y + z) = xy + xz$$

luego

$$\begin{aligned} x(y + z^+) &= x((y + z)^+) \\ &= x(y + z) + x \\ &= xy + (xz + x) \\ &= xy + xz^+, \end{aligned}$$

así que z^+ pertenece a M. Por consiguiente, la afirmación es verdadera.

Teorema L33: (ley asociativa de la multiplicación)

$$(xy)z = x(yz)$$

Prueba: fijamos x y y; sea M el conjunto de todos los z para los cuales la afirmación es verdadera.

I) $(xy)0 = 0 = x(y0)$; por lo que 0 pertenece a M.

II) Sea z que pertenece a M. Entonces

$$(xy)z = x(yz)$$

luego

$$\begin{aligned}(xy)z^+ &= (xy)z + xy \\ &= x(yz) + xy\end{aligned}$$

y por el teorema L32,

$$\begin{aligned}(xy)z^+ &= x(yz + y) \\ &= x(yz^+).\end{aligned}$$

Así que z^+ pertenece a M y por lo tanto, $M = \mathrm{N}$.

Teorema L34: (ley de monotonía de la multiplicación) si $x > y$ o $x = y$ o $x < y$, y $z \neq 0$ entonces $xz > yz$, $xz = yz$ o $xz < yz$, respectivamente.

Prueba:

1. Si $x > y$ entonces existe $u \neq 0$ en N tal que $x = y + u$, luego

   $$xz = (y + u)z = yz + uz,$$

   y como $u \neq 0$ y $z \neq 0$ entonces $uz \neq 0$, puesto que si $z \neq 0$, existe w en N tal que $w^+ = z$, por tanto $uz = uw^+ = uw + u \neq 0$. Debido a esto y al teorema L18, concluimos que $xz > yz$.

2. Si $x = y$ entonces $xz = yz$.

3. Si $x < y$ entonces $y > x$, y por 1), $yz > xz$, luego $xz < yz$.

Teorema L35: si $(xz > yz)$ o $(xz = yz)$ o $(xz < yz)$ con $z \neq 0$, entonces $(x > y)$, o $(x = y)$, o $(x < y)$, respectivamente.

Prueba: Dados x y y números naturales, por el teorema L10, tenemos que se tiene solo uno de los siguientes casos:

1. $(x < y)$: por L34 se cumple que $xz < yz$.

2. $(x > y)$: por L34 se cumple que $xz > yz$.

3. $x = y$: por L34 se cumple que $xz = yz$.

I) Si suponemos que $(xz > yz)$, los casos 1 y 3 no se pueden dar pues implican una contradicción con la hipótesis. Luego se cumple que $x > y$.

II) Si suponemos que $(xz < yz)$, los casos 2 y 3 no se pueden dar pues implican una contradicción con la hipótesis. Luego se cumple que $x < y$.

III) Si suponemos que $(xz = yz)$, los casos 1 y 2 no se pueden dar pues implican una contradicción con la hipótesis. Luego se cumple que $x = y$. Este caso se conoce como la **ley cancelativa de la multiplicación**.

Teorema L36: si $x > y$, $z > u$, entonces $xz > yu$.

Prueba: por el teorema L34, tenemos que $xz > yz$ y $zy > uy$, como $yz = zy > uy = yu$, luego por el teorema L15 concluimos que $xz > yu$.

Teorema L37: si $(x \geq y,\ z > u)$ con $x \neq 0$ o $(x > y,\ z \geq u)$ con $z \neq 0$, entonces $xz > yu$.

Prueba: si en la hipótesis hay una igualdad aplicamos el teorema L34; si no, aplicamos el teorema L36.

Teorema L38: si $x \geq y$, $z \geq u$ entonces $xz \geq yu$.

Prueba: si en la hipótesis hay dos igualdades de signos el resultado es inmediato; si no, se sigue del teorema L37.

4.1.1.3.2. Otra forma de presentar la axiomática de Peano

La presentación axiomática de los números naturales hecha inicialmente por Peano en 1889 tiene como primer número natural al 1, en 1898 formuló otra axiomática donde el primer número natural es 0 y aunque los dos conjuntos de números naturales resultantes de cada axiomática no son isomorfos desde el punto de vista algebraico, pues uno es un semigrupo y el otro es un monoide, si lo son como conjuntos ordenados.

Presentaremos ahora una versión más moderna de la axiomática que asume al 1 como primer número natural[24], posteriormente la compararemos con otras versiones axiomáticas para los números naturales. En esta versión suponemos la existencia de un conjunto no vacío N, cuyos elementos son

[24]Numeraremos de la misma forma los axiomas y teoremas que se derivan en la versión con 1 como primer elemento, pero para diferenciarlos usaremos primas, por ejemplo: A3 y A3′, L1 y L1′.

los números naturales, de una función $\sigma : \mathrm{N} \to \mathrm{N}$ en la que el elemento $\sigma(n)$, para cada $n \in \mathrm{N}$, es el *sucesor* de n y como *axiomas*:

AF1. σ es inyectiva es decir, cada numero natural m es sucesor de a lo más un número natural.

AF2. El conjunto $\sigma(\mathrm{N})$ de los elementos de N que son sucesores de algún elemento de N, es un subconjunto propio de N, es decir, existe un $n_0 \in \mathrm{N}$ tal que $\sigma(n) \neq n_0$ para todo $n \in \mathrm{N}$. Equivalentemente: $\mathrm{N}_0 = \mathrm{N} - \sigma(\mathrm{N}) \neq \varnothing$.

AF3. (**Principio de inducción**). Si un conjunto $A \subseteq \mathrm{N}$ tal que:

- $A \cap (\mathrm{N} - \sigma(\mathrm{N})) \neq \varnothing$
- $\sigma(A) \subseteq A$,

entonces $A = \mathrm{N}$.

El axioma AF3 dice que si los elementos de N_0 pertenecen a un conjunto A y además todos los sucesores de los elementos de A están en A, entonces dicho conjunto es igual al de los números naturales.

Las demostraciones siguen las líneas de razonamiento presentadas en la sección anterior, realizando los cambios necesarios para que el primer número natural no sea 0, por ejemplo el teorema L2 se traduce en:

Teorema L2′: para todo numero natural m se tiene $\sigma(m) \neq m$.

Prueba: sea

$$M_0 = \{m \in N; \sigma(m) \neq m\}$$

Por el axioma AF2 existe $n_0 \in M_0$, es decir,

$$M_0 \cap (\mathrm{N} - \sigma(N)) \neq \varnothing.$$

Además, si $m \in M_0$ entonces $\sigma(m) \neq m$ y como σ es inyectiva $\sigma(\sigma(m)) \neq \sigma(m)$ entonces $\sigma(m) \in M_0$, por lo tanto, $\sigma(M_0) \subseteq M_0$ y por el axioma AF3, $M_0 = \mathrm{N}$.

El conjunto $\mathrm{N}_0 = \mathrm{N} - \sigma(\mathrm{N})$ es un conjunto unitario, pues si suponemos que $\mathrm{N}_0 = \{n_0, n_1\}$ entonces el conjunto $A = \{n_0, \sigma(n_0), \sigma(\sigma(n_0)), \ldots\}$ sería igual al conjunto de los números naturales pues satisface las condiciones del axioma AF3, pero $n_1 \in \mathrm{N}$ y no pertenece a A, pues $n_0 \neq n_1$ y $\sigma(n) \neq n_1$ para todo n en N. Al único número natural en $\mathrm{N}_0 = \mathrm{N} - \sigma(\mathrm{N})$ lo notamos 1.

Con esta notación tenemos que para todo $m \in \mathrm{N}$, $m \neq 1$ hay un único número natural m_1 tal que $\sigma(m_1) = m$; y el principio de inducción queda en la forma: todo conjunto no vacío de números naturales al que pertenezca el 1 y al que pertenezca el sucesor de cada uno de sus elementos, es igual al conjunto de los números naturales.

Teorema L4′: existe una única función $f : \mathrm{N} \times \mathrm{N} \to \mathrm{N}$ que cumple:

1. $f(n, 1) = \sigma(n)$.
2. $f(n, \sigma(m)) = \sigma(f(n, m))$, para todo $n, m \in \mathrm{N}$.

Esta única función se llama *suma* y $f(n, m)$ se denota $n + m$.

Prueba:

a) Unicidad: sean

$$f, g : \mathrm{N} \times \mathrm{N} \to \mathrm{N}$$

dos funciones que satisfacen las condiciones 1) y 2). Sea $n \in \mathrm{N}$ y

$$M = \{m \in \mathrm{N} : f(n, m) = g(n, m)\}$$

Por hipótesis,

$$f(n, 1) = \sigma(n) = g(n, 1)$$

por lo tanto $1 \in M$. Además, si $m \in M$ entonces $f(n, m) = g(n, m)$, luego

$$f(n, \sigma(m)) = \sigma(f(n, m)) = \sigma(g(n, m)) = g(n, \sigma(m))$$

es decir, $\sigma(m) \in M$. Por tanto, $M = \mathrm{N}$, es decir $f = g$.

b) Existencia: sea

$\mathrm{L} = \{n \in \mathrm{N}$: existe $f : \mathrm{N} \times \mathrm{N} \to \mathrm{N}$ que satisface las condiciones 1) y 2)

para todo $m \in \mathrm{N}\}$

Definamos primero la función $f : \mathrm{N} \times \mathrm{N} \to \mathrm{N}$ de la siguiente manera:

$$(1, m) = \sigma(m) \text{ para todo } m \in \mathrm{N}$$
$$f(\sigma(n), m) = \sigma(f(n, m)) \text{ para todo } m \in \mathrm{N}$$

Tenemos que $1 \in L$, pues

$$f(1, 1) = \sigma(1)$$

y

$$f(1, \sigma(m)) = \sigma(\sigma(m)) = \sigma(f(1, m)).$$

Si $n \in L$ entonces $f(n, m)$ satisface las condiciones 1) y 2) para todo $m \in \mathrm{N}$, además $\sigma(n)$ satisface que:

$$f(\sigma(n), 1) = \sigma(f(n, 1)) = \sigma(\sigma(n))$$

y

$$f(\sigma(n), \sigma(m)) = \sigma(f(n, \sigma(m))) = \sigma(\sigma(f(n, m))) = \sigma(f(\sigma(n), m))$$

por tanto, $\sigma(n) \in \mathrm{L}$. Entonces $\mathrm{L} = \mathrm{N}$.

Teorema L27′: (principio del buen orden) sea M un subconjunto no vacío de N, entonces $M - \sigma(M)$ no es vacío. Es decir, en cada conjunto no vacío M de números naturales hay al menos un elemento que no es sucesor de algún número en M.

Prueba: supongamos que $M \neq \varnothing$ y que $M - \sigma(M) = \varnothing$, entonces todo elemento de M es sucesor de algún elemento de M, o sea $M \subseteq \sigma(M)$; luego

$$\mathrm{N} - \sigma(\mathrm{N}) \subseteq \mathrm{N} - \sigma(M) \subseteq \mathrm{N} - M$$

Pero $M \cap (\mathrm{N} - M) = \varnothing$ y por lo tanto $\sigma(M) \cap \sigma(\mathrm{N} - M) = \varnothing$, pues si $x \in \sigma(M)$ y $x \in \sigma(\mathrm{N} - M)$, existen $y \in M$ y $z \in \mathrm{N} - M$ tales que $\sigma(y) = \sigma(z)$, pero como σ es inyectiva, esto es absurdo. Entonces

$$\sigma(\mathrm{N} - M) = \mathrm{N} - \sigma(M) \subseteq \mathrm{N} - M$$

Es decir, $\mathrm{N} - M$ satisface el axioma de inducción y se tiene que $\mathrm{N} - M = N$. Luego M debe ser vacío, contradiciendo la hipótesis.

Ejercicio

Defina la operación multiplicación y demuestre que la multiplicación de números naturales distribuye con respecto a la suma ya definida.

4.1.1.4. La respuesta de Peirce

En 1881, varios años antes que Peano, en el artículo *On the Logic of Number*[25] C.S. Peirce presentó una axiomatización de los números naturales, describiendolos como un sistema de cantidad simple, discreto, semilimitado; llamando

[25]PEIRCE, Charles. On the Logic of Number. En : American Journal Mathematics, Vol. 4, (1881); p. 85-95.

1. Un sistema de cantidad simple a un conjunto totalmente ordenado.
2. Un sistema semi-limitado si tiene un elemento mínimo pero no máximo.
3. Un sistema discreto en el que para todo número x, mayor que otro, es el sucesor inmediato de algún número.
4. Un sistema es infinito si del hecho de que una proposición sea verdadera para algún número es verdadera para el sucesor inmediato, se puede inferir que si esta proposición es cierta para algún número es cierta para todo número mayor.

En términos modernos postula la existencia de un conjunto N y una *relación de orden* en N, que satisfacen los siguientes axiomas:

AP1. N es un conjunto totalmente ordenado. (Notamos $\leq$ al orden).

AP2. Existe en N el *primer* número, el elemento mínimo de N, (el cual denotamos por 1); esto es, para todo $m \in$ N se tiene que $1 \leq m$ y N no posee elemento máximo.

AP3. Todo elemento x de N distinto del mínimo posee un *antecesor inmediato* x'.

AP4. *Principio de inducción*: si S es un subconjunto de N que satisface:
$n \in$ S implica que $n + 1 \in$ S
entonces
$n \in$ S implica que $m \in$ S, para todo $m > n$.

Las operaciones suma $x + y$ y producto xy los define por recursión:

- Si x carece de antecesor inmediato ($x = 1$), entonces $x + y$ se define como y^+, el sucesor inmediato de y, y si x tiene antecesor inmediato x', $x + y$ se define como el sucesor inmediato de $x' + y$.

De manera similar, si x carece de antecesor inmediato, xy se define como y; en caso contrario, se define como y; en caso contrario, se define como $y + x'y$.

En símbolos, podemos expresar la suma como:

$$1 + y = y^+$$

$$(1 + x) + y = 1 + (x + y)$$

donde si $z = 1 + x$, entonces z es sucesor inmediato de x y x es antecesor inmediato de z. La multiplicación asume la forma:

$$1y = y$$

$$(1 + x)y = y + xy.$$

Las pruebas consisten en mostrar primero que la proposición es verdadera para el número uno, y luego que si es verdadera para el número n, es verdadera para el número $1+n$, sucesor inmediato de n; veamos algunos ejemplos:

Teorema P.1: (ley asociativa de la adición) para cualesquier números naturales x, y y z

$$(x + y) + z = x + (y + z).$$

Prueba: elegimos y y z elementos fijos pero arbitrarios de N, y hacemos inducción sobre x.

i. Verificamos para $x = 1$; y la afirmación:

$$(1 + y) + z = 1 + (y + z)$$

es cierta por la segunda parte de la definición de adición.

ii. Debemos probar que si es cierto para $x = n$, es cierto para $x = 1+n$; esto es, si

$$(n + y) + z = n + (y + z)$$

entonces

$$((1 + n) + y) + z = (1 + n) + (y + z).$$

Y como

$$\begin{aligned}((1 + n) + y) + z &= (1 + (n + y)) + z && \text{por la definición de la adición}\\ &= 1 + ((n + y) + z) && \text{por la definición de la adición}\\ &= 1 + (n + (y + z)) && \text{por hipótesis}\\ &= (1 + n) + (y + z) && \text{por la definición de la adición}\end{aligned}$$

Teorema P.2: (ley conmutativa de la adición) para cualesquier números naturales x, y

$$(x + y) = (y + x).$$

Prueba: hacemos inducción sobre y.

i. Para $y = 1$ hacemos inducción sobre x. Si $x = 1$ obtenemos una identidad.

Si la afirmación es verdadera para $x = n$, esto es

$$n + 1 = 1 + n,$$

debemos probar que es verdadera para $x = 1 + n$, o sea que

$$(1 + n) + 1 = 1 + (1 + n).$$

Como

$$\begin{aligned} (1+n)+1 &= 1+(n+1) && \text{por la ley asociativa de la adición} \\ &= 1+(1+n) && \text{por hipótesis.} \end{aligned}$$

ii. Ahora suponemos que la afirmación es verdadera para $y = n$, o sea que

$$x + n = n + x$$

donde x es un elemento fijo pero arbitrario de N, debemos probar que es verdadera para $y = 1 + n$, o sea que

$$x + (1 + n) = (1 + n) + x.$$

$$\begin{aligned} \text{Como } x+(1+n) &= (x+1)+n && \text{por la ley asociativa de la adición} \\ &= (1+x)+n && \text{por la parte } i. \text{ de esta demostración} \\ &= 1+(x+n) && \text{por la definición de adición} \\ &= 1+(n+x) && \text{por hipótesis} \\ &= (1+n)+x && \text{por la definición de adición.} \end{aligned}$$

y la prueba está completa.

Teorema P.3: (ley distributiva de la multiplicación con respecto a la adición) para cualesquier números naturales x, y, z

$$(x + y)z = xz + yz$$

y

$$z(x + y) = zx + zy.$$

Prueba: para probar la primera igualdad elegimos y y z elementos fijos pero arbitrarios de N, y hacemos inducción sobre x.

i. Verificamos para $x = 1$

$$\begin{aligned}(1+y)z &= z + yz && \text{Por la definición de multiplicación}\\ &= 1z + yz && \text{Por la definición de multiplicación}\end{aligned}$$

ii. Supongamos que la afirmación es verdadera para $x = n$, esto es

$$(n+y)z = nz + yz,$$

debemos probar que es verdadera para $x = 1 + n$, o sea que

$$((1+n)+y)z = (1+n)z + yz$$

Como

$$\begin{aligned}((1+n)+y)z &= (1+(n+y))z && \text{Por la definición de adición}\\ &= z + (n+y)z && \text{Por la definición de multiplicación}\\ &= z + (nz + yz) && \text{Por hipótesis}\\ &= (z + nz) + yz && \text{Por la ley asociativa de la adición}\\ &= (1+n)z + yz && \text{Por la definición de multiplicación.}\end{aligned}$$

Ejercicio

Con la axiomática de Peirce demuestre las siguientes propiedades:

1. $x(y+z) = xy + xz$
2. $(xy)z = x(yz)$
3. $xy = yx$.

4.1.1.5. Equivalencia entre las Axiomatizaciones

Probaremos ahora que los números naturales definidos en las axiomatizaciones de Peirce y Peano (iniciando en 1) son los mismos; para ello, como tenemos un mismo conjunto de objetos, si queremos demostrar que los axiomas de Peano implican los de Peirce debemos construir una relación de orden y probar que satisface los axiomas de Peirce; en sentido contrario debemos construir la función sucesor y probar los axiomas de Peano.

4.1.1.5.1. Los axiomas de Peano implican los de Peirce

Si usamos la versión de Landau[26] de la axiomática de Peano iniciando en 1, la definición 5′:

$$x \leq y \quad \text{significa } x < y \text{ o } x = y.$$

donde la definición 3′ es

$$x < y \quad \text{si y solo si existe } u \text{ en N tal que } y = x + u$$

nos da una relación de orden y el teorema L10′ que coincide con el teorema L10, nos dice que el orden es total y con esto hemos demostrado el primer axioma AP1 de Peirce.

Veamos con más detalle la propiedad antisimétrica: si $a \leq b$ y $b \leq a$ entonces $a = b$. Para ello, supongamos que $a \neq b$ y como $a \leq b$ y $b \leq a$, por la definición 5′, existen p, $q \in$ N tales que $a + p = b$ y $b + q = a$; por lo cual:

$$a + (p + q) = (a + p) + q = b + q = a,$$

pero esto contradice el teorema L18′ ($x + y > x$).

Para probar el axioma AP2 veamos que N tiene elemento mínimo, para esto veamos que $1 \leq a$ para todo número natural a. Si $a = 1$ se tiene una igualdad, si $a \neq 1$, por el teorema L3′ (Si $x \neq 1$ existe un u tal que $x = u^+$), existe $b \in$ N tal que $a = b^+$, interpretando b^+ como $b + 1$, concluimos que $1 < a$.

Ahora probemos que N no tiene elemento máximo; como por A2′ que coincide con A2, dado un número natural a este tiene un sucesor a^+ y por el teorema L2′ $a^+ \neq a$, luego interpretando $a^+ = a + 1$, tenemos que para todo número natural a, se cumple que $a < a^+$, lo que significa que ningún a en N es máximo.

El Axioma AP3 de Peirce se colige del hecho de que para un b arbitrario en N, no existe $c \in$ N, de manera que $c \neq b$, $c \neq b^+$ y $b < c < b^+$; pues si existiera, deberían existir p, $q \in$ N, tales que $c = b + p$ y $b^+ = c + q$, de donde

$$b^+ = c + q = (b + p) + q = b + (p + q)$$

[26]Los axiomas, definiciones y teoremas correspondientes a esta versión los numeraremos de igual forma que los correspondientes a la versión que inicia en 0 y que desarrollamos en la sección 4.1.1.3.1. Para diferenciarlos incluiremos una comilla, por ejemplo el axioma correspondiente a A1 lo llamaremos A1′ y el teorema correspondiente a L3 lo notaremos L3′.

pero

$$1 < p < (p + q)$$

por el teorema L18′ y según el teorema L3′, existe $r \in$ N tal que $p+q = r^+$. Ahora

$$b^+ = b + (p + q) = b + r^+ = (b + r)^+$$

y por el teorema L1′ que coincide con L1, concluimos que $b = b + r$, lo cual contradice el teorema L7′ ($y \neq x + y$). Por lo tanto dado un número natural $b \neq 1$, por el teorema L3′ existe a en N tal que $b = a^+$, luego b es el *antecesor inmediato* de a.

Probemos ahora el axioma AP4: Sea S un subconjunto de N tal que $n \in$ S implica que $n + 1 \in$ S. Luego,

i. Si $n = 1 \in$ S, por el axioma A5′ tenemos que $S =$ N, es decir, $m \in$ S para todo m con $m > 1$.

ii. Si $n \in$ S, $n \neq 1$, por el teorema L3′ existe $j \in N$ tal que $n = j + 1$ y definimos un nuevo subconjunto S' como sigue:

$$S' = \{i \in N | j + i \in S\}.$$

Puesto que $n = j + 1$ y $n \in S$, entonces $1 \in S'$. Si $k \in S'$ entonces $j + k \in S$ de donde, por hipótesis $(j + k) + 1 \in S$ pero

$$(j + k) + 1 = j + (k + 1)$$

luego $k + 1 \in S'$ y por el axioma A5′ es $S' = N$.

Sea $m \in N$ con $m > n$, como $n \neq m$, existe $p \in N$ tal que $n + p = m$ de donde

$$m = (j + 1) + p = j + (1 + p)$$

pero $1 + p \in N = S'$ luego $j + (1 + p) \in S$, es decir, $m \in S$.

4.1.1.5.2. Los axiomas de Peirce implican los de Peano

Debemos ahora garantizar la existencia de sucesores con la noción de antecesores inmediatos.

Para demostrar el axioma A2′ (Todo elemento n en N tiene un único sucesor inmediato n^+), supongamos que algún elemento n no posee sucesor inmediato. Esto implica que no existe algún elemento cuyo antecesor inmediato es n y que el conjunto unitario $S = \{n\}$ satisface la condición

"para cada k, si el antecesor inmediato de k pertenece a S entonces k pertenece a S", porque no hay algún elemento k cuyo antecesor inmediato sea n. Como $n \in S$ implica que $n+1 \in S$, por el axioma AP4 de Peirce, se sigue para todo $m > n$, $m \in S$ y debido a que S es unitario, el único sucesor de n es el mismo n y esto significa que n es el elemento máximo de N, pues el orden es lineal. Lo cual contradice el axioma AP2. Por tanto todo elemento n en N posee sucesor inmediato que es único y lo notamos n^+.

El axioma A1′ (1 es un número natural), se deduce del hecho de que 1 es el mínimo de N.

El axioma A4′ (Si $x^+ \neq y^+$ entonces $x \neq y$), se obtiene debido a que si $x = y$, entonces $x + 1 = y + 1$.

Debido a que el elemento mínimo no puede ser sucesor inmediato de algún elemento, obtenemos el axioma A3′ (Para todo x se tiene que $x^+ \neq 1$).

La demostración del axioma A5′ (Si un subconjunto A de los números naturales tiene las siguientes propiedades: 1 pertenece a A y si x pertenece a A entonces x^+ pertenece a A, entonces A = N), la desarrollamos como sigue:

Sea A un subconjunto de N, tal que 1 pertenece a A y si x pertenece a A entonces x^+ pertenece a A, por el axioma AP4, para todo $m > 1$, m pertenece a A y como 1 el mínimo de N, entonces A = N.

4.1.1.6. La respuesta de Warner

Otra alternativa[27] para presentar los números naturales es asumir la existencia de un conjunto N, una operación + y una relación de orden en N que conforman una estructura conocida como *semigrupo naturalmente ordenado*, esto es: un semigrupo ordenado[28] $(E, +, \leq)$ que satisface las siguientes condiciones:
$(NO1)$ El orden $\leq$ es un buen orden[29].
$(NO2)$ La operación + es cancelativa.
$(NO3)$ Para todo $m, n \in E$, si $m \leq n$, entonces existe $p \in E$ tal que $m + p = n$.
$(NO4)$ Existe $m \in E$ y $n \in E$ tal que $m \neq n$.

[27]Esta versión aparece en: WARNER, Op. cit., p. 100-167.

[28]Un *semigrupo ordenado* es un semigrupo (E, Δ) donde está definida una relación de orden $\leq$ *compatible con la operación*; es decir, que para todo x, y, $z \in E$ si $x \leq y$, entonces $x \Delta z \leq y \Delta z$ y $z \Delta x \leq z \Delta y$.

[29]Una relación $\leq$ en un conjunto E es un *buen orden* si es un orden total y cada subconjunto no vacío de E tiene un elemento mínimo.

Las cuatro condiciones son independientes, es decir, ninguna de ellas puede ser deducida de las demás.

Aceptamos como postulado que:

Existe un semigrupo naturalmente ordenado.

Es posible probar[30] que dos semigrupos naturalmente ordenados son isomorfos como semigrupos ordenados y por lo tanto, salvo isomorfismos, hay exactamente un semigrupo naturalmente ordenado (N, +, $\leq$); a los elementos de N los llamamos *números naturales*.

El conjunto $E = \{0\}$ con la única operación y la única relación de orden definibles en E es un semigrupo ordenado conmutativo que satisface los axiomas $(NO1) - (NO3)$, pero no es naturalmente ordenado.

Como (N, +, $\leq$) es un semigrupo naturalmente ordenado, en particular es bien ordenado, luego existe un elemento mínimo en N, que llamaremos 0 y denotamos al complemento de $\{0\}$ como N^*. Por $(NO4)$, $\mathrm{N}^* \neq \varnothing$ y también posee un elemento mínimo que denotamos 1. Veamos algunos teoremas propios de esta estructura:

Teorema W.1: el número natural 0 es el elemento neutro para la operación +.

Prueba: como 0 es el número natural más pequeño, $0 \leq p$ para todo $p \in \mathrm{N}$, en particular $0 \leq 0 + 0$ y $0 \leq 0$, luego por $(NO3)$ existe $s \in \mathrm{N}$ tal que $0 + s = 0$, también $0 \leq s$ y debido a la compatibilidad del orden con la suma tenemos que:

$$0 + 0 \leq 0 + s = 0.$$

En conclusión, $0 + 0 = 0$. Y para cada número natural n,

$$(n + 0) + 0 = n + (0 + 0) = n + 0,$$

y por $(NO2)$ concluímos que $n + 0 = n$, y de manera análoga,

$$0 + (0 + n) = (0 + 0) + n = 0 + n$$

por $(NO2)$ obtenemos $0 + n = n$. Por lo tanto 0 es el elemento neutro para la suma en N.

Teorema W.2: si m y n son números naturales, entonces $m \leq n$ si y solo si existe un número natural p tal que $m + p = n$.

[30] Teorema 16.15 de WARNER, Op. cit., p. 129.

Prueba: la condición es necesaria por $(NO3)$. Pero también es suficiente, ya que si $m + p = n$, entonces por el teorema W.1 y la compatibilidad del orden con la suma,

$$m = m + 0 \leq m + p = n.$$

Teorema W.3: el elemento p que identificamos en el teorema W2 es único.

Prueba: sea $m \leq n$, luego existe un número natural p tal que $m+p = n$, supongamos que existe otro número natural q tal que $m + q = n = m + p$, entonces por $(NO2)$, $q = p$.

Si $m \leq n$, denotaremos al único número natural p tal que $m + p = n$ como $n - m$. Así si $m \leq n$, entonces por definición

$$m + (n - m) = n = (n - m) + m.$$

Teorema W.4: si m, n y p son números naturales, entonces $m < n$ si y solo si

$$m + p < n + p.$$

Prueba: supongamos que $m < n$, entonces por la compatibilidad del orden con respecto a la suma

$$m + p \leq n + p$$

pero no es posible que $m + p = n + p$, pues por $(NO2)$ $m = n$, lo que contradice la hipótesis. Luego debe ser

$$m + p < n + p.$$

Recíprocamente, si $m + p < n + p$, como $\leq$ es un orden total se tiene que $m < n$, pues de lo contrario sería $m \geq n$ y de la compatibilidad del orden con respecto a la suma resultaría que

$$m + p \geq n + p$$

contradiciendo la hipótesis.

Teorema W.5: si n y p son números naturales, entonces

a. $n < n + 1$.

b. $n < p$ si y solo si $n + 1 \geq p$.

Prueba:
a. Como $0 < 1$, por el teorema W.4

$$n = n + 0 < n + 1.$$

b. Si $n < p$, por el teorema W.1 tenemos que $p - n \neq 0$, así $1 \leq p - n$ por ser 1 el elemento mínimo del conjunto de los naturales diferentes de 0, y por consiguiente

$$n + 1 \leq n + (p - n) = p.$$

Recíprocamente, si $n + 1 \leq p$, entonces $n < p$ puesto que $n < n + 1$.

Teorema W.6: (principio de inducción matemática) sea S un subconjunto de N tal que $0 \in S$ y para todo número natural n, si $n \in S$, entonces $n + 1 \in S$. Entonces $\mathrm{N} = S$.

Prueba: supongamos que $S \neq \mathrm{N}$. Entonces el complemento S^c de S no es el conjunto vacío y por $(NO1)$ tiene un elemento mínimo a. Por hipótesis, $a \neq 0$, y por lo tanto $a \geq 1$.

Como $(a - 1) + 1 = a$, por el teorema W.5 tenemos que, $a - 1 < a$, en consecuencia $a - 1 \notin S^c$ pues a es el elemento mínimo de S^c, entonces $a - 1 \in (S^c)^c = S$, y por lo tanto $a \in S$ pues $a = (a - 1) + 1$ por hipótesis, lo que es una contradicción. En conclusión, $S = \mathrm{N}$.

Teorema W.7: (conmutatividad de la operación +) el semigrupo naturalmente ordenado $(N, +, \leq)$ es conmutativo.

Prueba: vamos a demostrar que para todo par de elementos a, b de N, $a + b = b + a$:

Para cada elemento $a \in \mathrm{N}$, formamos el conjunto

$$\mathrm{H}_a = \{b \in \mathrm{N} : a + b = b + a\}$$

y observemos que por ser 0 el elemento neutro para + en N (teorema W.1.), tenemos que $a + 0 = 0 + a$; de ahí, $0 \in \mathrm{H}_a$.

Demostremos, utilizando el principio de inducción (teorema W.6), que $\mathrm{H}_a - \{0\} = \mathrm{N}^*$:

i. Veamos que $1 \in \mathrm{H}_a - \{0\}$, esto es $a+1 = 1+a$: Para esto demostremos por inducción que para cualquier $b \in \mathrm{N}^*$, $1 + b = b + 1$:

   a. $1 + 1 = 1 + 1$, si no fuera así, tendríamos $1 + 1 < 1 + 1$ y por el teorema W.2 existe un número natural p tal que $(1+1)+p = 1+1$; aplicando la propiedad asociativa de la operación + y el axioma NO2 obtendríamos $p = 0$ y como 0 es el elemento neutro de la suma concluiríamos que $1 + 1 = 1 + 1$.

b. Supongamos que b cumple que $1 + b = b + 1$, demostremos que $1 + (b + 1) = (b + 1) + 1$.
Por asociatividad de la operación + en N, tenemos que

$$1 + (b + 1) = (1 + b) + 1$$

y aplicando hipótesis de inducción obtenemos que

$$1 + (b + 1) = (b + 1) + 1.$$

ii. Supongamos que $n \in \mathrm{H}_a - \{0\}$, demostremos que $n + 1 \in \mathrm{H}_a - \{0\}$:
Demostrar que $n + 1 \in \mathrm{H}_a - \{0\}$, es equivalente a demostrar que

$$a + (n + 1) = (n + 1) + a.$$

Supongamos que $a + (n + 1) \neq (n + 1) + a$, luego por ser N totalmente ordenado,

$$a + (n + 1) < (n + 1) + a$$

o

$$a + (n + 1) > (n + 1) + a.$$

Si partimos de que $a + (n + 1) < (n + 1) + a$, entonces por el teorema W.2 existe un $p \in \mathrm{N}$, tal que

$$(a + (n + 1)) + p = (n + 1) + a$$

por la asociatividad de la operación + en N

$$(a + n) + (1 + p) = (n + 1) + a$$

y por ser n un elemento de H_a, entonces $a + n = n + a$ y

$$(n + a) + (1 + p) = (n + 1) + a$$

nuevamente por la asociatividad de la operación + en N y por ser n cancelable en N (axioma $NO2$), tenemos que

$$a + (1 + p) = 1 + a$$

y como por la parte *i*. tenemos que $a + 1 = 1 + a$, usando las propiedades asociativa y cancelativa de + en N, concluimos que $p = 0$ lo que implica que

$$a + (n + 1) = (n + 1) + a$$

y conseguimos una contradicción. De manera análoga obtenemos una contradicción si asumimos que

$$a + (n + 1) > (n + 1) + a.$$

Entonces podemos concluir que $n + 1 \in \mathrm{H}_a - \{0\}$, por tanto $\mathrm{H}_a - \{0\} = \mathrm{N}^*$ y $\mathrm{H}_a = \mathrm{N}$.

4.1.1.6.1. Los axiomas de Warner implican los de Peirce

Identificaremos N^* con el conjunto de los números naturales de Peirce, con lo cual los axiomas AP1 y la primera parte de AP2, se deducen del axioma NO1, quedando pendiente probar que N^* no posee elemento máximo, esto es, no existe un elemento $m \in \mathrm{N}^*$ tal que $n \leq m$ para todo $n \in \mathrm{N}^*$; pues si existiera, se tendría que $m \geq m + 1$ lo que contradice el teorema W5.

El axioma AP3 se demuestra probando que el elemento $n - 1$ es el antecesor inmediato de n con $n \neq 1$. Es decir, veamos que no existe un $z \in \mathrm{N}^*$ tal que $n < z < n + 1$, pues de lo contrario, existirían $p \neq 0$ y $s \neq 0$ tales que $n + p = z$ y $z + s = n + 1$, pero como $n < n + 1$ implica que existe un único t tal que $n + t = n + 1$, por el axioma NO2 concluimos que $t = 1$, luego

$$n + t = z + s = (n + p) + s = n + (p + s)$$

y por el axioma NO2, tenemos que $t = p + s$, es decir, $1 = p + s$.

Por otro lado, como $p, s \in \mathrm{N}^*$ y por ser 1 el elemento mínimo de N^*, tenemos que $1 \leq p$ y $1 \leq s$ y por el teorema W5 y por ser N un semigrupo ordenado, $1 < 1 + 1 \leq s + p$ consiguiendo una contradicción.

Para completar la demostración de que la axiomática de Warner implica la de Peirce nos falta demostrar el axioma AP4: Sea S un subconjunto de N^* tal que $n \in \mathrm{S}$ implica que $n + 1 \in \mathrm{S}$. Luego,

i. Si $n = 1 \in \mathrm{S}$, por el teorema W6 tenemos que $S = \mathrm{N}^*$, es decir, $m \in S$ para todo m con $m > 1$.

ii. Si $n \in \mathrm{S}$, $n \neq 1$, entonces $1 < n$, luego por el axioma NO3, existe $j \in \mathrm{N}^*$ tal que $n = j + 1$ y definimos un nuevo subconjunto S' como sigue:

$$S' = \{i \in \mathrm{N}^* | j + i \in S\}.$$

Puesto que $n = j + 1$ y $n \in S$, entonces $1 \in S'$. Si $k \in S'$ entonces $j + k \in S$ de donde, por hipótesis $(j + k) + 1 \in S$ pero

$$(j+k)+1 = j+(k+1)$$

luego $k+1 \in S'$ y por el teorema W6, $S' = \mathrm{N}^*$.

Sea $m \in \mathrm{N}^*$ con $m > n$, como $n \neq m$, existe $p \in \mathrm{N}^*$ tal que $n+p = m$ de donde

$$m = (j+1)+p = j+(1+p)$$

pero $1+p \in \mathrm{N}^* = S'$ luego $j+(1+p) \in S$, es decir, $m \in S$.

4.1.1.6.2. Los axiomas de Peirce implican a los de Warner

Identificaremos el conjunto de los números naturales de Warner con $\mathrm{N} = \mathrm{N}^* \cup \{0\}$, donde N^* es el conjunto de los números naturales de Peirce y 0 es un elemento que se introduce con las condiciones $0 < 1$ y para todo $x \in \mathrm{N}$, $x + 0 = x$.

En primera instancia, se cumple el axioma $NO4$ de Warner, puesto que en N están el 0, por construcción y el elemento mínimo de N^*, por el axioma AP2.

Ahora, por el axioma AP1, N es totalmente ordenado por la relación "$\leq$", además tal relación es un buen orden, ya que todo subconjunto S no vacío de N tiene elemento mínimo, como lo garantiza el teorema L27′ ya que éste se deduce de la axiomática de Peano iniciando en 1 y esta axiomática es equivalente a la de Peirce[31]; con lo que obtenemos el axioma $NO1$.

Por otra parte, se cumple el axioma $NO2$, garantizado por el teorema L8′ en la forma: para todo $x, y, z \in \mathrm{N}$, si $x + y = x + z$ entonces $y = z$.

Finalmente, se cumple el axioma $NO3$, que enuncia para cualquier par de elementos x e y de N, si $x \leq y$ entonces, existe un p en N tal que $x + p = y$; pues si $x = y$ entonces $p = 0$. Y si $x \neq y$ y $x < y$ entonces la existencia de p se garantiza por el teorema L9′ y la definición 3′.

En el libro de Warner se demuestra seguidamente la validez de las definiciones por recurrencia y se aplica este resultado para definir y demostrar las propiedades básicas de la multiplicación y la potenciación. No las presentaremos aquí pero recomendamos su lectura para estudiar un punto de vista moderno.

[31] Todos los teoremas demostrados dentro de la axiomática de Peano iniciando en 1, son válidos en la axiomática de Peirce y viceversa, puesto que estas axiomáticas son equivalentes.

4.1.1.7. La respuesta de Lawvere

Hasta ahora hemos caracterizado el conjunto de los números naturales de manera analítica, es decir en términos de sus elementos, comenzando con el 0 y sus sucesores definimos las operaciones y el orden entre ellos; William Lawvere[32] en 1964 presentó una forma radicalmente opuesta, caracterizándolo sintéticamente como un objeto que se relaciona con otros objetos mediante flechas (morfismos) y diagramas conmutativos dentro del lenguaje de la teoría de categorías[33]. Observó que la sucesión

$$a, f(a), f(f(a)), f(f(f(a))), \ldots$$

donde f es una función de un conjunto arbitrario X en sí mismo y a es un elemento arbitrario de X, se puede escribir por recurrencia, notándola (s_n), como:

$$s_0 = a$$

$$s_{n+1} = f(s_n)$$

y como una sucesión en un conjunto X es una función $s : \mathrm{N} \to X$, la condición

$$s(n+1) = f(s(n))$$

puede expresarse como $s(\sigma(n)) = f(s(n))$ o como $s\sigma(n) = (fs)(n)$, siendo $\sigma : \mathrm{N} \to \mathrm{N}$ la función sucesor mencionada en la sección 4.1.1.3.2. De otro lado, la igualdad de funciones $s\sigma = fs$ puede expresarse afirmando que el diagrama siguiente conmuta

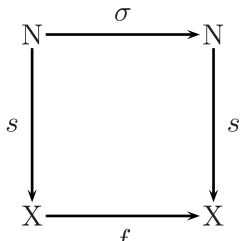


Figura 1

Por otra parte, una forma de elegir un elemento a de un conjunto arbitrario X es mediante una función $\boldsymbol{a} : T \to X$ de un conjunto unitario T en X, de forma que al único elemento en T se le asigna el elemento a en X y por lo tanto la condición $s(0) = a$ puede expresarse eligiendo el elemento 0 en N y el elemento a en X y afirmar que el diagrama

[32]LAWVERE, William. An Elementary Theory of the Category of Sets. Proc. Nat. Acad. Sci. 52. 1964. p. 1506-1511.

[33]Esta sección está basada fundamentalmente en: BEDOYA, Op. cit., p. 10-18.

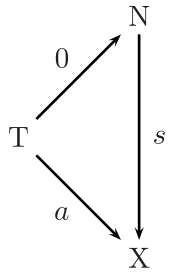


Figura 2

conmuta, o lo que es lo mismo $s0 = \boldsymbol{a}$.

Los dos diagramas anteriores pueden integrarse en uno solo, en la forma

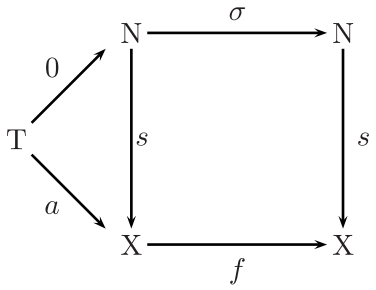


Figura 3

Una terna (N, σ, $\mathbf{0}$) tal que para cualquier terna $(X, f, \boldsymbol{a})$ existe una única función $s : \mathrm{N} \to X$ que hace conmutativo este diagrama, es lo que caracteriza al *conjunto de números naturales*. En realidad como en esta definición solo intervienen flechas y diagramas conmutativos, ella tiene sentido en los contextos de la teoría de categorías donde el conjunto de números naturales se reemplaza por un objeto números naturales[34].

En la axiomatización de los números naturales según Lawvere tenemos

Términos no definidos: un conjunto N, una función σ de N en N, una constante 0 en N.

Axioma: para cada conjunto X, cada función $f : X \to X$ y cada elemento $a \in X$, existe una única función $s : N \to X$ tal que:

$$s(0) = a$$

$$s\sigma = fs$$

[34]El nombre *objeto números naturales* combina singular y plural porque es un objeto en una categoría pero corresponde al conjunto de los números naturales en la categoría de los conjuntos y no a un número natural.

En diagramas, esta axiomatización la podemos presentar como:
Asumimos que existe la terna (N, σ, $\mathbf{0}$)

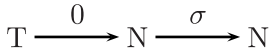


Figura 4

donde T es un conjunto unitario. Para cualquier terna $(X, f, \boldsymbol{a})$

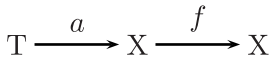


Figura 5

Existe una única función $s : \mathrm{N} \to X$ tal que el diagrama

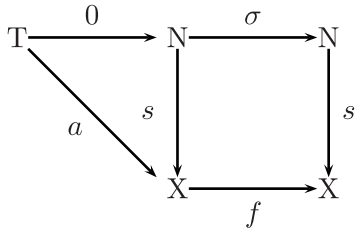


Figura 6

conmuta.

4.1.1.8. Equivalencia de Lawvere y Peano

En las axiomatizaciones de los números naturales por Peano y Lawvere los términos son los mismos, luego la equivalencia se prueba demostrando los axiomas de Peano en el sistema de Lawvere y, a continuación, demostrando el axioma de Lawvere en la aritmética de Peano.

4.1.1.8.1. El axioma de Lawvere implica los axiomas de Peano

Asumimos la existencia de una terna (N, σ, $\mathbf{0}$) que satisface el axioma de Lawvere.

Teorema F.1: si $t : \mathrm{N} \to \mathrm{N}$ es una función que satisface $t(0) = 0$ y $t\sigma = \sigma t$ entonces $t = i_N$ (función idéntica en N).

Prueba: por el axioma de Lawvere, para el conjunto N con la función $\sigma : \mathrm{N} \to \mathrm{N}$ y el elemento $0 \in \mathrm{N}$ existe una única función $s : \mathrm{N} \to \mathrm{N}$ con $s(0) = 0$ y $\sigma s = s\sigma$. Es decir el diagrama

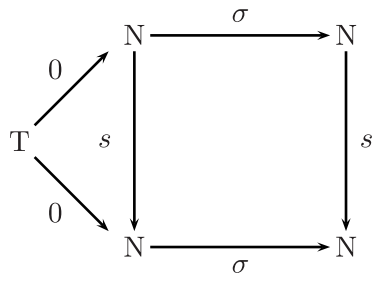


Figura 7

es conmutativo.

Por hipótesis $t(0) = 0$ y $\sigma t = t\sigma$ y como s única, entonces $t = s$. También tenemos que $i_N(0) = 0$ y $\sigma i_N = i_N \sigma$ por tanto $i_N = s$ pues s es única. En conclusión $t = i_N$.

Teorema F.2: σ es inyectiva.

Prueba: consideremos el conjunto $X = \mathrm{N}\times\mathrm{N}$, el elemento $(0,0) \in \mathrm{N} \times \mathrm{N}$ y la función $f : \mathrm{N} \times \mathrm{N} \to \mathrm{N} \times \mathrm{N}$ definida como

$$f(m,n) = (n, \sigma(n)).$$

Por el axioma de Lawvere, existe una única función $s : \mathrm{N} \to \mathrm{N} \times \mathrm{N}$ tal que $s(0) = (0,0)$ y $s\sigma = fs$. Como el codominio de la función s es $\mathrm{N} \times \mathrm{N}$, podemos escribirla como $s(n) = (g(n), h(n))$ donde g, h son funciones de N en N. En un diagrama:

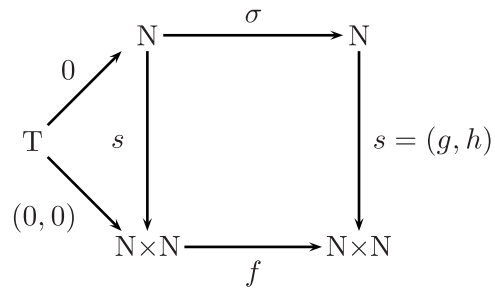


Figura 8

Como $(0,0) = s(0) = (g(0), h(0))$ entonces $g(0) = 0$ y $h(0) = 0$. Adicionalmente,

$$(s\sigma)(n) = s(\sigma(n)) = (g(\sigma(n)), h(\sigma(n))) = ((g\sigma)(n), (h\sigma)(n))$$

y

$$(fs)(n) = f(s(n)) = f(g(n), h(n)) = (h(n), \sigma(h(n))) = (h(n), (\sigma h)(n)).$$

Luego, para cada $n \in N$

$$(g\sigma)(n) = h(n) \qquad \text{y} \qquad (h\sigma)(n) = (\sigma h)(n)$$

es decir,

$$g\sigma = h, \qquad \text{y} \qquad h\sigma = \sigma h.$$

Puesto que $h(0) = 0$ y $h\sigma = \sigma h$ se sigue del teorema F.1. que $h = i_N$. Por tanto, $g\sigma = i_N$ y si suponemos que $\sigma(p) = \sigma(q)$ con p, q en N, entonces $(g\sigma)(p) = (g\sigma)(q)$, es decir, $i_N(p) = i_N(q)$ de donde $p = q$, en consecuencia, σ es inyectiva.

Teorema F.3: $0 \notin \sigma(\mathrm{N})$.

Prueba: sea X un conjunto no vacío y $f : X \to X$ una función no sobreyectiva; luego existe $a \in X$ que no pertenece a $f(x)$, es decir, $f(x) \neq a$ para todo $x \in X$.

Por el axioma de Lawvere, existe una única función $s : \mathrm{N} \to X$ con

$$s(0) = a \qquad \text{y} \qquad fs = s\sigma.$$

Supongamos que 0 pertenece a $\sigma(\mathrm{N})$, es decir, $\sigma(n) = 0$ para algún $n \in N$. Entonces $s(\sigma(n)) = s(0)$, luego $f(s(n)) = s(\sigma(n)) = s(0) = a$, lo cual contradice la hipótesis, por tanto, $0 \notin \sigma(\mathrm{N})$

Teorema F.4: si un subconjunto $S \subseteq N$ satisface

- $0 \in S$
- para cada $n \in \mathrm{N}$, si $n \in S$ entonces $\sigma(n) \in S$

entonces $S = \mathrm{N}$.

Prueba: la segunda hipótesis significa que la función σ puede restringirse a S, es decir, existe la función restringida $\hat{\sigma} : S \to S$ definida como $\hat{\sigma}(n) = \sigma(n)$ para cada $n \in S$.

Si $j : S \to N$ la función inclusión, o sea ($j(n) = n$ para cada $n \in S$, entonces

$$(j\hat{\sigma})(n) = j(\sigma(n)) = \sigma(n) = \sigma(j(n)) = (\sigma j)(n)$$

para cada $n \in S$, es decir, $j\hat{\sigma} = \sigma j$.

Por el axioma de Lawvere, para el conjunto S, la función $\hat{\sigma} : S \to S$ y $0 \in S$ existe una única función $s : N \to S$ tal que $s(0) = 0$ y $s\sigma = \hat{\sigma}s$. En resumen tenemos que el siguiente diagrama es conmutativo:

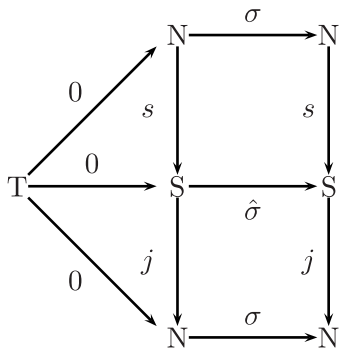


Figura 9

lo que significa que $(js)(0) = j(s(0)) = j(0) = 0$ y $(js)\sigma = j(s\sigma) = j(\hat{\sigma}s) = (j\hat{\sigma})s = (\sigma j)s = \sigma(js)$.

Y por el teorema F.1. concluimos que $js = i_N$ y como para cada $r \in N$ existe $s(r) \in N$ con $j(s(r)) = js(r) = i_N(r) = r$ lo que demuestra que j es sobreyectiva, es decir, $S = N$.

Los teoremas F.2., F.3. y F.4. demuestran que el axioma de Lawvere implica los axiomas de Peano según la versión presentada en la sección 4.1.1.3.2.

4.1.1.8.2. Los axiomas de Peano implican el axioma de Lawvere

Ahora asumimos válidos los axiomas de Peano presentados en la sección 4.1.1.3.2. y consideramos un conjunto arbitrario X, una función $f : X \to X$ y un elemento $a \in X$, debemos probar la existencia y unicidad de una función $s : \mathrm{N} \to X$ tal que $s(0) = a$ y $fs = s\sigma$.

Definimos la función s como sigue:

- $s(0) = a$
- Suponemos conocido $s(n)$ y definimos $s(\sigma(n)) = f(s(n))$.

Teorema F.5: la función s está definida en todo N.

Prueba: sea D el dominio de s, $0 \in D$ porque definimos $s(0) = a$. Ahora si suponemos que $n \in D$, tenemos que $s(n)$ está definido y por definición $s(\sigma(n)) = f(s(n))$, luego $\sigma(n) \in D$. Por el axioma AF3 de Peano, $D = \mathrm{N}$.

Teorema F.6: la función s es única.

Prueba: supongamos que existe otra función $t : \mathrm{N} \to X$ tal que $t(0) = a$, $ft = t\sigma$. Sea C el subconjunto de N donde s y t coinciden, es decir,

$$C = \{n \in N | s(n) = t(n)\}.$$

$0 \in C$ porque $s(0) = a$ y $t(0) = a$. Si suponemos que $n \in C$, $s(n) = t(n)$, entonces

$$s(\sigma(n)) = f(s(n)) = f(t(n)) = t(\sigma(n))$$

por tanto $\sigma(n) \in C$ y por el axioma AF3 de Peano, $C = \mathrm{N}$ luego s, t son iguales.

4.1.1.9. La respuesta de Zermelo - Fraenkel - Skolem

Otra salida para construir el conjunto de números naturales es fundamentarlo en una teoría más general de cuyos axiomas podamos deducir los axiomas de Peano. Elegimos la versión[35] de la teoría de conjuntos propuesta inicialmente por Zermelo, en la que se evitan las paradojas a costa de limitarla un poco en su generalidad.

En la teoría de conjuntos de Zermelo-Fraenkel-Skolem[36] se usan tres nociones primitivas: *conjunto, elemento* y la *relación de pertenencia* $\in$, además una colección de objetos abstractos B; los objetos se representan mediante letras, y la igualdad $a = b$ significa que los símbolos *ayb* designan la misma cosa.

4.1.1.9.1. Los axiomas de la teoría de conjuntos

La teoría asume como axiomas[37]:

1. **Axioma de extensionalidad:** dos conjuntos son iguales si y solo si tienen los mismos elementos, en símbolos:

$$(\forall x)(\forall y)((\forall z)(z \in x \leftrightarrow z \in y) \rightarrow (x = y)).$$

2. **Axioma del conjunto vacío:** existe un conjunto sin elementos

$$(\exists x)(\forall z)(\neg(z \in x)).$$

[35]Existen otras versiones, una conocida como teoría de clases, debida a J. von Neumann y modificada por P. Bernays y K, Gödel y una versión de Russell y Whitehead, conocida como teoría de tipos, propuesta en 1910, aunque esta última es poco usada. Una versión más reciente basada en la noción de categoría está expuesta en: LAWVERE, William. ROSEBRUGH, Robert. Sets for Mathematicians. Cambridge: Cambridge University Press, 2003. p. 154-165.

[36]Propuesto por E. Zermelo en 1908, y modificada por A. Fraenkel y T. Skolem en 1922, para adecuarla a la aritmética ordinal transfinita.

[37]Seguimos la numeración de: MUÑOZ, José. Introducción a la teoría de conjuntos. 4 ed. Bogotá: Universidad Nacional de Colombia, 2002. p. 49-52; 134.

3. **Esquema axiomático de separación:** a todo conjunto a y a toda condición $p(x)$ corresponde un conjunto b cuyos elementos son precisamente los x de a para los cuales se cumple $p(x)$.

4. **Axioma de pares no ordenados:** si x e y son conjuntos, el par (no ordenado) $\{x, y\}$ es un conjunto.

$$(\forall x)(\forall y)(\exists z)(\forall w)(w \in z \leftrightarrow ((w = x) \vee (w = y))).$$

5. **Axioma de la unión:** sea x un conjunto de conjuntos, la unión de todos sus elementos es un conjunto.

$$(\forall x)(\exists y)(\forall z)((z \in y) \leftrightarrow (\exists w)((z \in w) \wedge (w \in x))).$$

6. **Axioma del conjunto potencia:** para cada conjunto x existe un conjunto y de subconjuntos de x.

$$(\forall x)(\exists y)(\forall z)((z \in y) \leftrightarrow (z \subseteq x)).$$

7. **Axioma del infinito:** existe un conjunto x que contiene al conjunto vacío y es tal que si y pertenece a x entonces la unión de y y el conjunto $\{y\}$ también pertenece a x. Este axioma garantiza la existencia de conjuntos infinitos.

$$(\exists x)((\varnothing \in x) \wedge (\forall y)((y \in x) \rightarrow (y \cup \{y\} \in x))).$$

8. **Axioma de elección:** para toda familia no vacía de conjuntos no vacíos y disyuntos dos a dos, existe una función que permite escoger un solo elemento de cada conjunto de manera que se pueda formar con ellos un nuevo conjunto.

4.1.1.9.2. La construcción de los números naturales como conjuntos bien ordenados

En el axioma 2 de la teoría se establece que *existe un conjunto sin elementos.* Comúnmente lo llamamos *conjunto vacío*, y como no tiene elementos es un buen candidato para representar al número natural *cero*, hagamos entonces:

$$0 = \varnothing.$$

Si queremos que el sucesor de 0 sea un conjunto con un elemento, es natural la elección:

$$1 = \{\varnothing\}.$$

Para construir el sucesor de 1 tenemos varias opciones; por ejemplo, Zermelo propuso que:

$$2 = \{1\} = \{\{\varnothing\}\}$$

y que el sucesor de n fuera:

$$n + 1 = \{n\}$$

o sea, que n es 0 encerrado entre n pares de corchetes. Esta idea funciona bien con conjuntos finitos, pero presenta problemas en los conjuntos infinitos[38].

Usando una idea de Frege, J. Von Neumann propuso que cada número natural fuera el conjunto de los números naturales menores que él, es decir:

$$\begin{aligned} 0 &= \varnothing \\ 1 &= \{0\} = \{\varnothing\} \\ 2 &= \{0, 1\} = \{\varnothing, \{\varnothing\}\} \\ 3 &= \{0, 1, 2\} \ldots, \text{etc.} \end{aligned}$$

En esta versión, el número natural n es un conjunto que tiene exactamente n elementos.

Respetando la idea, de que el sucesor de un número natural una unidad más adelante, el sucesor de un conjunto debe ser un conjunto con un elemento más; por esto definimos, el sucesor de un conjunto x como:

$$x^+ = x \cup \{x\}$$

Con esto obtenemos el conjunto:

$$\mathrm{N} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \ldots\}.$$

De manera general, un conjunto A lo llamamos *inductivo*[39] si $\varnothing \in$ A y el sucesor de todo elemento de A también pertenece a él. Además, un conjunto x lo llamamos *número natural* si pertenece a todo conjunto inductivo.

El conjunto de los números naturales, que identificamos con la intersección no vacía de conjuntos inductivos, es el más pequeño de los conjuntos inductivos, lo que está garantizado por el siguiente teorema.

Teorema Z1: la intersección de una colección no vacía de conjuntos inductivos es un conjunto inductivo.

[38]SMULLYAN Raymond, FITTING, Melvin. Set theory and the continuum problem. Oxford: Clarendon Press, 1996. p. 29.

[39]La existencia de por lo menos un conjunto inductivo lo garantiza el axioma 7.

Prueba: sea C es una colección no vacía de conjuntos inductivos, entonces por la definición de conjunto inductivo, para todo elemento A de la colección se tiene que $\varnothing \in$ A, o sea que $\varnothing$ es un elemento de la intersección de todos los A de C; además, si x es un elemento de tal intersección, por ser cada A inductivo, también x^+ pertenece a la intersección. De ahí, se concluye que el conjunto intersección, K, de todos los conjuntos inductivos A de C, es inductivo.

Teorema Z2: ningún número natural es subconjunto de alguno de sus elementos.

Prueba: definamos el conjunto H de todos los números naturales que no son subconjunto de alguno de sus elementos

$$\mathrm{H} = \{n \in \mathrm{N} : (\forall x)(x \in n) \rightarrow (\neg(n \subseteq x))\}$$

$\varnothing \in$ H, pues no tiene elementos; dado $n \in$ H veamos que $n^+ \in$ H:

Como $n \in$ H, entonces $(\forall x)(x \in n) \rightarrow (\neg(n \subseteq x))$, en particular si $x = n$ entonces $(n \in n) \rightarrow (\neg(n \subseteq n)$ pero $n \subseteq n$ y por tanto $n \notin n$.

Sea $y \in n^+$, luego como $n^+ = n \cup \{n\}$ entonces $y \in n$ o $y \in \{n\}$; si $y \in n$, entonces como $n \in$ H, $\neg(n \subseteq y)$ por tanto $(\neg(n^+ \subseteq y)$, pues si $n^+ \subseteq y$ tendríamos que $n \subseteq n^+ \subseteq y$ que es una contradicción y por lo tanto $n^+ \in$ H.

Si $y \in \{n\}$, entonces $y = n$, como $n \in n^+$ y $n \notin n$, concluimos que $\neg(n^+ \subseteq n = y)$ y por tanto $n^+ \in$ H. Como N es el menor conjunto inductivo, se concluye que H = N.

Teorema Z3: ningún número natural es elemento de sí mismo.

Prueba: supongamos que existe un natural n tal que $n \in n$, como $n \subseteq n$ entonces n sería subconjunto de sí mismo contradiciendo el teorema Z2.

Teorema Z4: todo elemento de un número natural es subconjunto propio de dicho natural.

Prueba: sea

$$\mathrm{T} = \{n \in \mathrm{N} : (\forall x)(x \in n) \rightarrow (x \subset n)\}$$

$\varnothing \in$ T pues no hay elementos en $\varnothing$ que no cumplan la condición.

Supongamos que $n \in$ T y sea $x \in n^+ = n \cup \{n\}$, entonces $x \in n$ o $x = n$. Si $x = n$ tenemos que $x \subset n^+$ y si $x \in n$, como $n \in$ T entonces $x \subset n \subset n^+$, por lo tanto $n^+ \in$ T. Como N es el menor conjunto inductivo, se concluye que T = N.

Teorema Z5: la relación de pertenencia es transitiva.

Prueba: sea $m \in n$ y $n \in k$ entonces por el teorema Z4, $n \subset k$ por lo tanto $m \in k$.

4.1.1.9.3. Los axiomas de la teoría de conjuntos implican los axiomas de Peano

Veamos que el conjunto de los números naturales construido satisface los axiomas de Peano[40]:

Por definición de conjunto inductivo, $0 = \varnothing$ es un número natural y todo número natural tiene un único sucesor; además, el principio de inducción matemática se tiene por ser N el menor conjunto inductivo (teorema Z1), puesto que, si $\mathrm{H} \subseteq \mathrm{N}$ y satisface que $0 \in \mathrm{H}$ y que para todo elemento $n \in \mathrm{H}$ se cumple que $n^+ \in \mathrm{H}$, entonces H es inductivo, pero como N es el menor entonces $\mathrm{N} \subseteq \mathrm{H}$, o sea que $\mathrm{N} = \mathrm{H}$.

Por otro lado, $\varnothing$ no es sucesor de algún número natural, ya que como $n \notin \varnothing$ y $n \in n \cup \{n\} = n^+$, para todo número natural n, entonces $\varnothing \neq n^+$.

Para demostrar que $n^+ = m^+$ implica $n = m$, suponemos que $n^+ = m^+$, entonces $m \in m^+ = n^+$ y $n \in n^+ = m^+$, lo que significa que $m \in n$ o $m = n$, y que $n \in m$ o $n = m$, respectivamente, en símbolos

$$(m \in n \vee m = n) \wedge (n \in m \vee n = m)$$

Por la distributividad de $\vee$ con respecto a $\wedge$ y por ser la igualdad una relación simétrica, tenemos que

$$(m \in n \wedge n \in m) \vee (m = n)$$

Pero si suponemos que $(m \in n \wedge n \in m)$ por el teorema Z5, concluimos que $m \in m$ contradiciendo el teorema Z3, por lo tanto $m = n$, lo que termina la demostración.

[40] En esta sección consideraremos a 0 como el primer número natural.

CAPÍTULO 5

Representaciones de N

Lo fundamental no es qué sabemos, sino cómo lo sabemos
Aristóteles

En el capítulo anterior estudiamos diferentes presentaciones axiomáticas equivalentes de los números naturales, en este capítulo nos dedicaremos a construir representaciones de ellas; en la construcción de representaciones de estructuras finitas contábamos con una tabla que nos permitía abstraer la estructura, o recíprocamente con los axiomas construimos la tabla; en el caso de los números naturales no podemos hacer tablas, pues es un conjunto infinito; por tanto, debemos construir modelos que satisfagan los axiomas que definen a los números naturales.

Usaremos la versión de Peano con 0 como primer elemento, o sea:

A1′. 0 es un número natural.

A2′. El sucesor de cualquier número natural n es un número natural n^+.

A3′. Dos números naturales diferentes no tienen el mismo sucesor, es decir que si $k \neq n$ entonces $k^+ \neq n^+$.

A4′. 0 no es el sucesor de número alguno.

A5′. Si un subconjunto A de los números naturales tiene las siguientes propiedades:

a. 0 pertenece a A

b. Si x pertenece a A entonces x^+ pertenece a A podemos concluir que A = N.

Construiremos primero la representación más conocida, que llamaremos *representación usual* y de ella, con pequeñas variaciones, construiremos sucesiones infinitas de números naturales, partiendo de un primer número (no necesariamente 0) y adicionándole otro número fijo para conseguir progresiones aritméticas; luego a partir de un primer número multiplicamos por otro fijo y obtenemos progresiones geométricas; después cambiamos el número fijo que se adiciona por una progresión aritmética obteniendo sucesiones cuadráticas, y repitiendo la secuencia adicionamos una sucesión cuadrática a un primer número para obtener sucesiones cúbicas y así sucesivamente.

En seguida estudiamos algunas sucesiones definidas por recurrencia a partir de dos elementos y en un caso particular expresamos esto como una sucesión no recurrente. En el siguiente paso construimos sucesiones sumando los primeros términos de otra sucesión obteniendo las series aritméticas y geométricas. Si en lugar de sumar, restamos obtenemos las series telescópicas.

Nuestra siguiente actividad se dirige a copiar la estructura de los números naturales a conjuntos más grandes en el sentido de que los naturales sean un subconjunto de ellos, tomando como ejemplo el conjunto subyacente a los números enteros.

5.1. La representación usual

Si buscamos un conjunto que satisfaga los axiomas A1′ y A2′ nos basta con el conjunto $\{0\}$ si definimos que el sucesor de 0 sea el mismo 0, pero esto contradice el axioma A4′.

Si definimos como sucesor de un número, el número que está a la derecha de él en la secuencia:

$$0, 1, 2, 3, 4, 5, 3$$

El conjunto obtenido cumple los axiomas A1′, A2′ y A4′; pero no cumple el axioma A3′, por lo tanto debemos impedir ciclos de dos o más elementos.

Un conjunto que satisface los cinco axiomas[1] lo construimos partiendo de un número cero que notamos 0 y agregamos su sucesor notado 0^+ y

[1]NEWMAN, James. Sigma el Mundo de las Matemáticas. Barcelona: Grijalbo, 1997. v. 5. p. 7-22.

luego el sucesor de éste y así sucesivamente, con esto obtenemos

$$\mathrm{N} = \{0, 0^{+}, 0^{++}, 0^{+++}, \ldots\}$$

Y si notamos $0^{+} = 1$, $0^{++} = 2$, $0^{+++} = 3$, etc., obtenemos el conjunto:

$$\mathrm{N} = \{0, 1, 2, 3, \ldots\}.$$

A este conjunto lo llamaremos la *representación usual de los números naturales*[2].

Si consideramos el conjunto

$$\mathrm{H} = \mathrm{N} \cup \{\mathrm{X}\}$$

donde incluimos un elemento X que no pertenece a N y es su propio sucesor, vemos que H cumple los 4 primeros axiomas, pero no el axioma A5′.

5.2. Cambio de símbolos

De la misma forma que en la primera actividad, podemos cambiar los símbolos para conseguir otras representaciones de los números naturales, *eligiendo* otro símbolo[3], digamos a como *primer* elemento y así el conjunto de los números naturales lo podemos representar como:

$$\mathrm{N}' = \{a, a^{+}, a^{++}, a^{+++}, \ldots\}$$

y si escogemos otros símbolos, como en el capítulo 2 de "*Actividades matemáticas para el desarrollo de procesos lógicos: contar e Inducir*[4]"para representar:

$$\begin{aligned} a^{+} &= \oplus \\ a^{++} &= \varnothing \\ a^{+++} &= \text{®} \\ a^{++++} &= \text{©} \end{aligned}$$

[2]JIMÉNEZ, Rafael; GORDILLO, Enrique y RUBIANO, Gustavo. Teoría de Números para Principiantes. Bogotá: Universidad Nacional de Colombia, 1999. p. 1-11.

[3]Aquí podemos incluir como ejemplos los sistemas de representación de los números hechos por los egipcios, los babilonios, los chinos, los mayas, etc.

[4]LUQUE, MORA y PÁEZ, Op. cit., p. 43.

y así sucesivamente reemplazando cada sucesor por un nuevo símbolo, entonces obtenemos

$$\mathrm{N}' = \{a, \oplus, \varnothing, ®, ©, \ldots\}$$

Por supuesto este conjunto tiene las mismas propiedades[5] que el conjunto de los naturales con primer elemento 0 (cero).

Si quisiéramos demostrar algún teorema, que es válido para los números naturales en su representación usual, en la nueva representación, vemos que *no aportamos algo nuevo a la discusión*, pues la demostración es la misma cambiando 0 por a en los axiomas y teoremas. Esta es solo otra *representación* de los números naturales. Por ejemplo:

Teorema: si $x \neq a$ existe un único u en N' tal que $x = u^+$.

Prueba: sea M el conjunto cuyos elementos son el número a y todos aquellos x en N' para los cuales existe tal u. Por el axioma A4 N', (reemplazando el 0 por a) para cualquier x se tiene que $x \neq a$.

I) a pertenece a M.

II) Si x pertenece a M, entonces, existe u en N' tal que $x = u^+$. Por el axioma A2′ $x^+ = (u^+)^+$ entonces $(u^+)^+$ pertenece a M y esto significa que x^+ pertenece a M.

Por el axioma A5′ (reemplazando el 0 por a), a M pertenecen todos los números naturales; entonces, para cada $x \neq a$ en N', existe un u en $\mathrm{N}\,'$ tal que $x = u^+$. La unicidad de u la garantiza el axioma A3′.

[5]Los egipcios idearon algoritmos para efectuar operaciones aritméticas que empleaban en la solución de diversos problemas. La aritmética egipcia fue esencialmente aditiva; para las sumas y las restas usuales se limitaban a combinar o a cancelar los diferentes símbolos hasta llegar al resultado concreto. La multiplicación y la división también se reducían a procesos aditivos, pero el cálculo era un poco más complicado. Se evidencia en los algoritmos de las operaciones el reconocimiento de que la suma y la multiplicación son *conmutativas*, en el sentido que empleaban las dos opciones indistintamente, y que la multiplicación es distributiva respecto a la suma, dado que es uno de los elementos considerados en el algoritmo para la multiplicación.

5.3. Con los mismos símbolos usuales pero con otros significados

5.3.1. Sucesiones infinitas de números naturales

Si escogemos los mismos símbolos de la representación usual pero le damos un significado diferente; por ejemplo, podemos iniciar en 5 e incluir todos sus sucesores, para obtener:

$$\mathrm{N}'' = \{5, 6, 7, 8, 9, \ldots\}$$

O modificamos la idea común de sucesor para que el sucesor de n no sea $n + 1$, sino por ejemplo $n + 2$, o $n + k$ para cualquier número k de la representación usual, obtenemos otras representaciones de los números naturales como:

$$\mathrm{N}''' = \{7, 9, 11, 13, 15, \ldots\}$$

$$\mathrm{N}'^{v} = \{0, 3, 6, 9, 12, 15, \ldots\}$$

$$\mathrm{N}^{v} = \{1, 3, 5, 7, 9, 11, \ldots\}$$

$$\mathrm{N}^{v\prime} = \{2, 4, 6, 8, 10, 12, \ldots\}$$

Todos estos conjuntos satisfacen los axiomas de Peano, como puede verificarse fácilmente. Por ejemplo, podemos construir un conjunto S de números que tenga como primer elemento a 8 y el sucesor de un número n es $n + 3$, así:

$$\mathrm{S} = \{8, 11, 14, 17, \ldots\}$$

Este conjunto satisface las siguientes condiciones:
$8 \in \mathrm{S}$
8 no es sucesor de algún número en S
Todo número de S tiene un solo sucesor
Cada número es sucesor de solo un número de S
Si $\mathrm{A} \subseteq \mathrm{S}$, es tal que $8 \in \mathrm{A}$ y cada vez que $k \in \mathrm{A}$, $k^+ \in \mathrm{A}$ entonces $\mathrm{A} = \mathrm{S}$.

La adición en S la definimos de la misma forma como:

i. $n + 8 = n$

ii. $n + k^+ = (n + k)^+$.

Para cualquier número n y $k \in \mathrm{S}$.

La existencia de un elemento idéntico para la adición se demuestra de forma completamente análoga a como hicimos en N:

Teorema: para todo número n en S se cumple que

$$n + 8 = 8 + n = n$$

Prueba: sea $M = \{x \in S : x + 8 = 8 + x = x\}$. 8 pertenece a M puesto que $8 + 8 = 8$ por la parte $i.$ de la definición de suma.

Si x pertenece a M, entonces $x + 8 = 8 + x = x$, por la parte $ii.$ de la definición de suma tenemos que

$$8 + x^+ = (8 + x)^+ = x^+,$$

por la parte $i.$ de la definición de suma tenemos que $x^+ + 8 = x^+$, luego $x^+ + 8 = 8 + x^+ = x^+$, por lo tanto x^+ pertenece a M. Por el axioma A5′, $M = S$.

De nuevo, estamos repitiendo los razonamientos, el símbolo 0 podemos reemplazarlo por el símbolo 8, o por cualquier otro pero todo sigue esencialmente igual. Tendremos resultados aparentemente curiosos como

$$11 + 8 = 11, 14 + 17 = 23, \text{ etc.}$$

Pero si cambiamos de nuevo los nombres de los números, por ejemplo hacemos que:

$$8 = 0', 11 = 1', 14 = 2', 17 = 3', 20 = 4', 23 = 5', \text{ etc.}$$

Volvemos a la normalidad

$$1' + 0' = 1', \ 2' + 3' = 5', \text{ etc.}$$

En general podemos formar distintas representaciones de N asignando a cada valor $n \in$ N un único elemento, bien sea del mismo N o de cualquier otro conjunto infinito obteniendo una sucesión infinita.

De hecho lo que estamos haciendo es definir una función sucesor que sea inyectiva del conjunto

$$\text{N} = \{0, 1, 2, 3, \ldots\}$$

en sí mismo; como ya sabemos las operaciones entre los nuevos símbolos están definidas mediante la función sucesor.

Ejemplos

1. El conjunto subyacente a los números pares como representación de los números naturales

Tomemos como base la representación usual de los números naturales

$$\mathrm{N} = \{0, 1, 2, 3, \ldots\}$$

y a partir de ella construyamos otras, cambiándole el nombre a cada número natural n por el doble de él, obteniendo el conjunto:

$$\mathrm{P} = \{0, 2, 4, 6, 8, \ldots\}$$

donde 0 es el primer elemento y el sucesor de cualquier n en P es $n + 2$; la suma la notaremos $\oplus$, y la definimos de la misma manera:

i. $n \oplus 0 = n$

ii. $n \oplus k^+ = (n \oplus k)^+$.

Así obtenemos que:

$$\begin{aligned} &2 \oplus 0 = 2 \\ &2 \oplus 2 = 2 \oplus 0^+ = (2 \oplus 0)^+ = 2^+ = 4 \\ &2 \oplus 4 = 2 \oplus 2^+ = (2 \oplus 2)^+ = 4^+ = 6 \end{aligned}$$

y así sucesivamente, con los mismos resultados que en la representación usual.

Gráficamente:

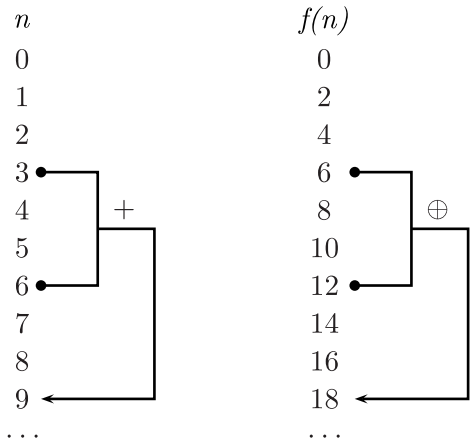


Figura 1

La función que define esta representación, a partir de la usual, es

$$\begin{aligned} f : \mathrm{N} &\to \mathrm{P} \\ n &\mapsto 2n \end{aligned}$$

esta función es biyectiva y su inversa es

$$\begin{aligned} f^{-1} : \mathrm{P} &\to \mathrm{N} \\ a &\mapsto \frac{a}{2} \end{aligned}$$

La operación $\oplus$ puede ser expresada en términos de la suma $+$ de la representación usual, mediante la expresión:

$$a \oplus b = f(f^{-1}(a) + f^{-1}(b))$$

obteniendo:

$$\begin{aligned} a \oplus b &= f(f^{-1}(a) + f^{-1}(b)) \\ &= 2\left(\frac{a}{2} + \frac{b}{2}\right) \\ &= a + b \end{aligned}$$

como ya sabíamos.

Eso significa, que la operación $\oplus$ se efectúa de la misma forma que $+$, por ejemplo:

$$6 \oplus 12 = 6 + 12 = 18$$

y a la suma $a + b$ entre dos números naturales, le corresponde mediante f la suma de los pares $f(a) \oplus f(b)$, en símbolos:

$$f(a + b) = f(a) \oplus f(b)$$

La multiplicación la copiamos de igual manera, pero el resultado ya no es el mismo:

$$\begin{aligned} a \otimes b = &\ f(f^{-1}(a) \times f^{-1}(b)) \\ = &\ 2\left(\frac{a}{2} \times \frac{b}{2}\right) \\ = &\ \frac{a \times b}{2} \end{aligned}$$

Ahora

$$4 \otimes 8 = \frac{4 \times 8}{2} = 16$$

A pesar de que la multiplicación no se efectúa de la misma forma, se sigue manteniendo la relación:

$$f(a \times b) = f(a) \otimes f(b)$$

gráficamente:

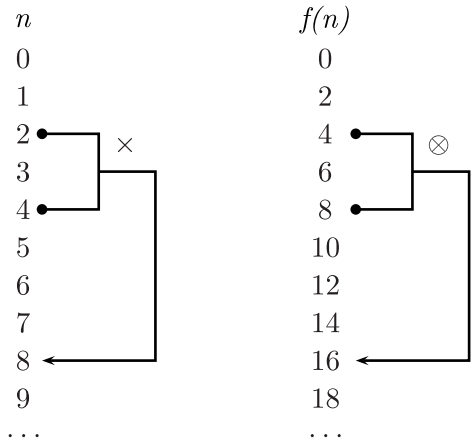


Figura 2

2. El conjunto subyacente a los números impares como representación de los números naturales

Como sabemos la suma de dos números pares es un número par y por eso no nos sorprendería mucho que lográramos con facilidad interpretar cada número par como un número natural; pero si consideramos el conjunto subyacente a los números impares, y los notamos I, en la representación usual de los números naturales, la suma de dos de ellos no es impar; pero podemos hacer una copia de los números naturales en el conjunto subyacente a los impares de manera que la *nueva* suma entre ellos sí dé como resultado uno de ellos, esto se logra con la función biyectiva:

$$\begin{aligned} f : \mathrm{N} &\to \mathrm{I} \\ n &\mapsto 2n + 1 \end{aligned}$$

y su inversa

$$\begin{aligned} f^{-1} : \mathrm{I} &\to \mathrm{N} \\ a &\mapsto \frac{a-1}{2}. \end{aligned}$$

La nueva suma entre elementos de I está dada por

$$a \oplus b = f(f^{-1}(a) + f^{-1}(b))$$

o sea

$$\begin{aligned} a \oplus b &= f(f^{-1}(a) + f^{-1}(b)) \\ &= 2\left(\frac{a-1}{2} + \frac{b-1}{2}\right) + 1 \\ &= a + b - 1 \end{aligned}$$

en particular,

$$5 \oplus 9 = 13.$$

Ejercicio

Copie la multiplicación de los números naturales en su representación usual al conjunto subyacente a los números impares usando la función biyectiva f definida anteriormente.

3. Progresiones Aritméticas como representaciones de los números naturales

Generalizando los dos ejemplos anteriores, podemos construir otras representaciones de N, a partir de la usual, escogiendo en ella un número a_0 como *primer término* y sumándole a él un número fijo d llamado *razón*, para obtener el sucesor, y repitiendo el proceso, obtener cada uno de los términos siguientes, para conseguir lo que conocemos como una *progresión aritmética*[6]:

$$\mathrm{A} = \{a_0,\ \ a_0 + d,\ \ a_0 + 2d,\ \ a_0 + 3d,\ \ \ldots\}$$

El *término n-ésimo* de esta progresión, notado a_n, está dado por:

$$a_n = a_0 + nd$$

para $n > 0$, por ejemplo para formar

$$\mathrm{N}'' = \{5, 6, 7, 8, 9, \ldots\}$$

[6]Los pitagóricos en el siglo VI a. de C., estudiaron estas progresiones y en el libro VII de los *Elementos* de Euclides también aparecen con el nombre de *números en proporción continua*. En el siglo VI d.C. el libro hindú *Aryabhatiya* incluye un estudio de las progresiones aritméticas, reglas para hallar el último término y para hallar la suma, pero sin justificación alguna.

el término n-ésimo es:

$$a_n = 5 + n$$

En una progresión aritmética los términos entre el primero y el n-ésimo término se llaman *términos diferenciales* o *medios aritméticos* entre a_0 y a_n.

El modelo también funciona con números negativos, racionales, reales o complejos, o cualquier otro tipo de número, por ejemplo si $a_0 = -9$ y $d = 4$, obtenemos:

$$\mathbf{X} = \{-9, -5, -1, 3, 7, \ldots, -9 + 4n, \ldots\}$$

Una progresión aritmética conocida aparece al calcular el *interés simple* de un capital inicial P, por ejemplo si el dinero se invierte al interés simple del $8\,\%$ anual, entonces en n años la cantidad de dinero inicial P se ha convertido en

$$P_n = P + n(0,08)P$$

Las operaciones de suma y multiplicación en estas representaciones se pueden calcular a partir de las operaciones de la representación usual mediante la función

$$\begin{aligned} f : \mathrm{N} &\to \mathrm{A} \\ n &\mapsto a_0 + nd \end{aligned}$$

y su inversa

$$\begin{aligned} f^{-1} : \mathrm{A} &\to \mathrm{N} \\ m &\mapsto \left(\frac{m - a_0}{d}\right). \end{aligned}$$

Pero debido a que sus expresiones se tornan cada vez más enredadas y menos dicientes las dejamos de lado ya que solo con las imágenes de las sucesiones tenemos bastante por hacer.

4. Progresiones geométricas como representaciones de números naturales

El proceso descrito en el ejemplo anterior lo podemos modificar, cambiando la suma por multiplicación, obteniendo las progresiones geométricas[7], partiendo de un número a y multiplicando por otro número k (que puede ser igual a a), por ejemplo

$$\{5, 25, 125, 625, \ldots\}$$

[7]En el libro VII de los *Elementos* de Euclides estas progresiones se llaman *números en proporción doble continua.*

Una *progresión geométrica* es una sucesión $\mathrm{B} = \{a_0,\, a_0r,\, a_0r^2,\, a_0r^3, \ldots\}$, en la cual el cociente de cada término y el anterior es constante, esto es, $\dfrac{a_n}{a_{n-1}} = r$, con r constante. El valor r se llama *razón* de la progresión geométrica.

Las progresiones geométricas también pueden ser de números negativos, por ejemplo si $r = -1$ y $a = 2$, la progresión es

$$2, -2, 2, -2, 2, \ldots$$

O una progresión decreciente de fracciones, por ejemplo

$$\frac{1}{3},\ \frac{1}{3^2},\ \frac{1}{3^3},\ \frac{1}{3^4},\ \frac{1}{3^5},\ \cdots$$

5. Sucesiones cuadráticas

En los ejemplos anteriores de sucesiones, obtuvimos el término siguiente a partir del anterior sumándole o multiplicándole *un mismo número*, ahora sumaremos a cada término una cantidad diferente.

Empecemos el proceso con una secuencia simple, iniciemos con un número cualquiera, digamos 3, le sumamos 1, al resultado le sumamos 2, al resultado le sumamos 3, y así sucesivamente; obteniendo la sucesión:

$$3, 4, 6, 9, 13, 18, \ldots$$

nos preguntamos, ¿cuál es el término general?

Por la forma como la construimos, vemos que:

$$\begin{array}{ll} 0 & 3 \\ 1 & 3+1 \\ 2 & 3+1+2 \\ 3 & 3+1+2+3 \\ \vdots & \vdots \end{array}$$

y ¡claro!, el término n-ésimo es:

$$3 + 1 + 2 + 3 + \cdots + n$$

pero la suma que sigue al primer término ya la conocemos[8]

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

[8]LUQUE, MORA y PÁEZ, Op. cit., p. 173-194.

y el término n-ésimo de la sucesión es:

$$3 + \frac{n(n+1)}{2}.$$

Análogamente, si construimos una sucesión sumando a un número fijo la lista de los pares o los impares, encontraremos fórmulas de segundo grado. Por ejemplo si partimos de 5 y le sumamos consecutivamente cada uno de los números pares, tenemos:

$$\begin{array}{lll} 0 & 5 & = 5 \\ 1 & 5+2 & = 7 \\ 2 & 5+2+4 & = 11 \\ 3 & 5+2+4+6 & = 17 \\ \vdots & \vdots & \vdots \\ k & 5+2+4+6+\cdots+2k & = 5+k(k+1) = k^2+k+5 \end{array}$$

pues la suma

$$\sum_{k=1}^{n} 2k = 2+4+6+\cdots+2n = n(n+1)$$

De la misma forma, podemos usar la suma de los números impares:

$$\sum_{k=1}^{n} (2k-1) = 1+3+5+\cdots+(2n-1) = n^2$$

para obtener funciones cuadráticas que nos permitan cambiarles la cara a los números naturales. Con estas funciones podemos copiar las operaciones, pero de nuevo no nos interesamos de manera directa en esa tarea, porque aparte de ser engorrosas, no aportan algo nuevo a nuestra discusión.

Ejercicios

1. *Encontrar el término n-ésimo de las siguientes sucesiones:*

$$\{7, 9, 13, 19, 27, \ldots\}$$

$$\{9, 12, 17, 24, 33, 44, \}$$

2. *Generalice el procedimiento anterior sumando una progresión aritmética a un número fijo. ¿Obtiene una sucesión cuadrática?*

3. *¿Todas las sucesiones cuadráticas se obtienen de esta forma?*

6. Sucesiones cúbicas

Reiteramos el proceso anterior, pero ahora sumamos la secuencia de los números triangulares, o cuadrados y obtenemos funciones biyectivas (sobre la imagen de la función) de tercer grado, por ejemplo

$$6, 7, 10, 16, 26, \ldots$$

que se obtiene partiendo de 6 y sumando consecutivamente cada uno de los números triangulares T_k, de la forma:

0	6	6
1	$6+1$	7
2	$6+1+3$	10
3	$6+1+3+6$	16
$\vdots$	$\vdots$	$\vdots$
k	$6+1+3+6+\cdots+T_k$	

y como

$$\sum_{k=1}^{n} T_k = T_1 + T_2 + T_3 + \cdots + T_n = \frac{n(n+1)(n+2)}{6}$$

obtenemos para el término k-ésimo de la sucesión:

$$6 + \frac{k(k+1)(k+2)}{6}$$

De manera análoga, obtenemos fórmulas cúbicas sumando números cuadrados, usando:

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Ejercicios

1. *Encontrar el término n-ésimo de las siguientes sucesiones:*

$$\{9, 10, 14, 23, 39, \ldots\}$$

$$\{12, 22, 37, 58, 86, \ldots\}$$

2. *Generalice el procedimiento anterior sumando una sucesión cuadrática a un número fijo. ¿obtiene una sucesión cúbica?*

3. *¿Todas las sucesiones cúbicas se obtienen de esta forma?*

Si sumamos números cúbicos y usamos

$$\sum_{k=1}^{n} k^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

obtenemos funciones de grado cuatro y así sucesivamente.

7. Sucesiones por recurrencia

No siempre debemos iniciar con un valor numérico y de él obtener los demás, podemos por ejemplo iniciar con *dos* valores y a partir de ellos definir un sucesor, uno de los más célebres ejemplos de este método es la *sucesión de Fibonacci*

$$\{1, 1, 2, 3, 5, 8, 13, \ldots\}.$$

Está sucesión la definimos partiendo de los números 1 y 1, calculando el siguiente término con la suma de los dos anteriores, esto es:

$$x_n = x_{n-1} + x_{n-2} \quad \text{para} \quad n \geq 2 \quad \text{y} \quad x_0 = 1 \quad \text{y} \quad x_1 = 1.$$

Esta sucesión está presente en la naturaleza; por ejemplo, las pipas de girasol forman espirales en sentidos contrarios y el número de espirales que hay en cada sentido son términos consecutivos de la sucesión de Fibonacci, siendo las combinaciones más frecuentes: 21 y 34, 34 y 55, 89 y 144. También se da este crecimiento en las piñas de las coníferas y los números de espirales más habituales en cada sentido son las parejas de términos: 5 y 8, 8 y 13.

Pero estas sucesiones podemos reducirlas a las anteriores expresando el valor de x_n, no en forma recursiva, sino en términos de la variable n, suponiendo que:

$$x_n = c\alpha^{n+1} + d\beta^{n+1}$$

para algún valor de c y d que debemos calcular. Como debe cumplirse con la condición de recurrencia:

$$c\alpha^{n+1} + d\beta^{n+1} = c\alpha^n + d\beta^n + c\alpha^{n-1} + d\beta^{n-1}$$

o

$$c(\alpha^{n+1} - \alpha^n - \alpha^{n-1}) = d\ (\beta^n + \beta^{n-1} - \beta^{n+1})$$

entonces

$$c\alpha^{n-1}(\alpha^2 - \alpha - 1) = d\beta^{n-1}(-\beta^2 + \beta + 1)$$

igualdad que se tiene, si los paréntesis valen cero, es decir:

$$\alpha^2 - \alpha - 1 = 0$$

y

$$-\beta^2 + \beta + 1 = 0$$

pero estas dos ecuaciones son equivalentes, y por lo tanto tienen las mismas soluciones:

$$\beta = \frac{1+\sqrt{5}}{2} \qquad \text{y} \qquad \alpha = \frac{1-\sqrt{5}}{2}.$$

Sabemos que

$$\alpha\beta = -1$$
$$\alpha + \beta = 1$$

y si elegimos, como términos iniciales de la sucesión (podemos hacer cualquier otra elección)

$$x_0 = c\alpha + d\beta = 1$$
$$x_1 = c\alpha^2 + d\beta^2 = 1$$

obtenemos un sistema de dos ecuaciones con dos incógnitas, cuya solución es:

$$c = \frac{\beta - 1}{-1 - \alpha^2} \quad \text{y} \quad d = \frac{1-\alpha}{\beta^2 + 1}$$

Reemplazando α y β obtenemos $c = \dfrac{-1}{\sqrt{5}},\ d = \dfrac{1}{\sqrt{5}}$ y por lo tanto:

$$x_n = c\alpha^{n+1} + d\,\beta^{n+1} = \frac{\beta^{n+1} - \alpha^{n+1}}{\sqrt{5}}$$

lo que nos da el término n-ésimo de la sucesión de Fibonacci.

Si elegimos: $x_0 = 7$ y $x_1 = 10$ como términos iniciales con la misma condición de recurrencia $x_n = x_{n-1} + x_{n-2}$ para $n \geq 2$, obtenemos como término n-ésimo:

$$x_n = \left(\frac{15 - 11\sqrt{5}}{10}\right)\alpha^{n+1} + \left(\frac{15 + 11\sqrt{5}}{10}\right)\beta^{n+1}.$$

Ahora si escogemos como condición de recurrencia

$$x_n = 2x_{n-1} + 3x_{n-2} \quad \text{para} \quad n \geq 2$$

con términos iniciales $x_0 = 4$ y $x_1 = 7$, obtenemos la sucesión

$$4,\ 7,\ 26,\ 73, \ldots$$

el término n-ésimo lo calculamos suponiendo

$$x_n = c\alpha^{n+1} + d\beta^{n+1}$$

y usando la condición de recurrencia obtenemos que $\alpha = 3$ y $\beta = -1$ y con estos valores encontramos que

$$c = \frac{11}{2} \qquad \text{y} \qquad d = \frac{5}{4}$$

Así, el término n-ésimo de la sucesión es

$$x_n = c\alpha^{n+1} + d\beta^{n+1} = \frac{11}{2}\alpha^{n+1} - \frac{5}{4}\beta^{n+1}.$$

Podría pensarse que si una sucesión *es construida con algún criterio lógico*, de manera que su término n-ésimo esté bien determinado, debe ser siempre posible encontrar una fórmula algebraica para escribirlo, pero esto no es cierto; podemos formar sucesiones con criterios definidos, pero que no sea posible o por lo menos inmediato encontrar una fórmula para ella, por ejemplo, la sucesión finita:

$$\{0, 5, 4, 2, 9, 8, 6, 7, 3, 1\}$$

fue formada de manera que los números del 0 al 9 fueran escritos de acuerdo al orden alfabético de su nombre en español. La secuencia

$$\{1, 8, 7, 4, 5, 6, 3, 2, 9\}$$

está formada por la última cifra de los cubos de los primeros nueve números naturales: $1, 8, 27, 64, 125, 216, \ldots, 729$. La sucesión

$$\{6, 8, 62, 63, 66, 72, 73, 76, 81, 84, \ldots\}$$

está formada por números cuyos nombres en español empiezan y terminan con la misma letra.

En algunos casos, los términos de la sucesión *son el resultado de un procedimiento algebraico*, pero no es posible escribir una fórmula para ellos, por ejemplo la sucesión:

$$\{8, 10, 13, 18, 25, 36, \ldots\}$$

se obtiene a partir del 8, sumando consecutivamente los números primos.

Ejercicios

1. *Estudie las secuencias definidas por*[9]

$$A_n(p, q) = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

en donde α y β son las soluciones de la ecuación $x^2 - px + q = 0$, con p y q números enteros diferentes de cero. En particular, ¿cuáles secuencias se obtienen si $p = 1$ y $q = -1$?

2. *Desarrolle el ejercicio anterior con secuencias definidas por la fórmula*

$$B_n(p, q) = \alpha^n + \beta^n$$

[9] A estas secuencias se les denomina *sucesiones de Lucas*. Para más información ver: CLAWSON, Calvin. Misterios matemáticos. Magia y belleza de los números. México: Diana, 1999.

5.3.2. Series

Otra manera de obtener sucesiones es sumando los primeros términos de una sucesión dada $\{a_n\}$. Llamamos *serie* a la sucesión de sumas parciales

$$\begin{aligned} s_0 &= a_0 \\ s_1 &= a_0 + a_1 \\ s_2 &= a_0 + a_1 + a_2 \\ &\vdots \\ s_n &= a_0 + a_1 + \cdots + a_n \\ &\vdots \end{aligned}$$

y la notamos $\sum_{k=0}^{\infty} a_k$. La n-ésima suma parcial de la serie es s_n.

Ejemplos

1. Series Aritméticas

La sucesión de las sumas parciales de los términos de una sucesión aritmética se llama *serie aritmética*. Si

$$\mathrm{s}_n = a_0 + (a_0 + d) + \cdots + [a_0 + (n-1)d] + [a_0 + nd]$$

e invertimos el orden de la suma obtenemos:

$$\mathrm{s}_n = [a_0 + nd] + [a_0 + (n-1)d] + \cdots + (a_0 + d) + a_0$$

y si ahora sumamos ambas igualdades observamos que:

$$2\mathrm{s}_n = [2a_0 + nd] + [2a_0 + nd] + [2a_0 + nd] + \cdots + [2a_0 + nd]$$

donde el sumando se repite n veces, es decir que:

$$2\mathrm{s}_n = n[2a_0 + nd]$$

o sea que

$$\mathrm{s}_n = \frac{n[2a_0 + nd]}{2}$$

y si sustituimos $a_0 + nd$ por a_n obtenemos que

$$\mathrm{s}_n = \frac{n[a_0 + a_n]}{2}.$$

Casos particulares de esta fórmula son las correspondientes a la suma de los primeros números naturales, la de los números pares, la de los impares, etc.

2. Series Geométricas

Si s_n representa la suma de los $n+1$ primeros términos de una progresión geométrica[10],

$$s_n = a_0 + a_0 r + a_0 r^2 + a_0 r^3 + \cdots + a_0 r^n$$

y multiplicamos por r ambos lados de la igualdad, obtenemos:

$$r s_n = a_0 r + a_0 r^2 + a_0 r^3 + \cdots + a_0 r^n + a_0 r^{n+1}$$

ahora restamos ambas sumas y obtenemos

$$s_n - r s_n = a_0 - a_0 r^{n+1}$$

o lo que es lo mismo

$$s_n = \frac{a_0 - a_0 r^{n+1}}{1 - r} \qquad \text{con} \quad r \neq 1$$

o de otra forma

$$s_n = \frac{a_0 (1 - r^{n+1})}{1 - r} \qquad \text{con} \quad r \neq 1$$

Si una progresión geométrica es decreciente, la razón es una fracción menor que 1, y sus potencias serán cada vez menores cuanto mayor sea el exponente, si n aumenta indefinidamente, $a_0 r^{n+1}$ tiende a 0 y el valor de la suma es:

$$S = \frac{a_0}{1 - r}$$

Este resultado es fundamental para asegurar la existencia de números n-males periódicos[11] y es la primera ocasión en que encontramos que una suma de infinitos términos tiene un resultado finito. En estos casos se dice que la serie es *convergente*[12].

[10] En algunas tablillas babilónicas se encuentran adiciones como: $1 + 2 + 2^2 + 2^3 + 2^4 + \cdots + 2^9$ y $1^2 + 2^2 + 3^3 + 4^4 + \cdots + 9^9$ aunque, como las tablillas solo incluían casos concretos, no se tiene información sobre si los babilonios conocían expresiones generales para calcular estas sumas.

[11] LUQUE, Carlos y MORA, Lyda. Una aproximación a los números racionales positivos. Bogotá: Universidad Pedagógica Nacional, 2001. p. 1-35.

[12] La teoría básica de la convergencia fue estudiada alrededor de 1820 por el matemático francés Agustin Louis Cauchy.

Algunos ejemplos donde se usan series geométricas son:

1. Arquímedes (287-212 a. de C.) en su obra *La cuadratura de la parábola*, usa la serie infinita

$$T + \frac{T}{4} + \frac{T}{4^2} + \cdots + \frac{T}{4^n} + \cdots = \frac{4T}{3}$$

para el cálculo del área de un segmento parabólico, en este caso $r = \frac{1}{4}$ y $a_0 = 1$. Una visualización de que la suma

$$\frac{1}{4} + \frac{1}{4^2} + \cdots + \frac{1}{4^n} + \cdots = \frac{1}{3}$$

la tenemos en la siguiente figura

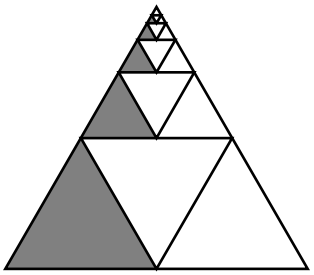


Figura 3

2. La paradoja de Aquiles y la tortuga descrita por Zenón tiene que ver con la serie:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} + \ldots$$

cuya suma es 1.

3. En base 10 la serie:

$$0,999999\ldots = 0,\overline{9} = 9\left(\frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots + \frac{1}{10^n + \cdots}\right) = 1$$

Podríamos inferir que si la cantidad que se agrega en cada paso se va haciendo cada vez más pequeña, llegará el momento en que no aporta a la suma y esta converge, pero la *serie armónica:*

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \cdots + \frac{1}{n} + \cdots$$

nos contradice esta hipótesis, puesto que el término n-ésimo de la sucesión $\left\{\frac{1}{n}\right\}$ es cada vez más pequeño y sin embargo la n-ésima suma parcial crece indefinidamente ya que:

$$\frac{1}{2} = \frac{1}{2}$$
$$\frac{1}{3} + \frac{1}{4} > \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$
$$\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} > \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}$$
$$\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} >$$
$$\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} = \frac{1}{2}$$

y así sucesivamente podemos agrupar, cada vez el doble de términos logrando que la suma de la izquierda forme la serie armónica y la de la derecha sea la suma de infinitas veces $\frac{1}{2}$, que crece sin límite.

3. Series aritmético-geométricas

Combinando sucesiones aritméticas y geométricas obtenemos series de la forma:

$$a + (a + d)\, r + (a + 2d)\, r^2 + \cdots + (a + nd)\, r^n$$

Ejercicio

Estudie el valor de esta suma dando inicialmente valores particulares para d y r. Luego generalice.

4. Series telescópicas

Otra forma de conseguir sucesiones a partir de otras, es hacer la sucesión de las diferencias entre un término y el anterior o viceversa, si $\{a_n\}$ es una sucesión cualquiera, $\{a_n\}'$ es la sucesión de sus diferencias, que llamamos sucesión *derivada* de la anterior:

$$\{a_n\}' = \{b_n\}$$

donde

$$b_n = a_{n+1} - a_n$$

y la n-ésima suma parcial de la sucesión $\{b_n\}$ es

$$s_n = (a_1 - a_0) + (a_2 - a_1) + (a_3 - a_2) + \cdots + (a_{n+1} - a_n)$$

es decir,

$$s_n = a_{n+1} - a_0$$

o alternativamente

$$b_n = a_n - a_{n+1}$$

cuya n-ésima suma parcial es

$$s_n = (a_0 - a_1) + (a_1 - a_2) + (a_2 - a_3) + \cdots + (a_n - a_{n+1})$$

o sea,

$$s_n = a_0 - a_{n+1}.$$

Si el término general de la sucesión $\{a_n\}$ se hace cada vez más pequeño, tiende a 0, entonces la suma es el primer término o su inverso aditivo.

Por ejemplo si

$$\{a_n\} = \{0,\ 1,\ 4,\ 9,\ \ldots n^2,\ \ldots\}$$

la sucesión derivada[13] es

$$\{a_n\}' = \{1,\ 3,\ 5,\ 7,\ \ldots 2n-1,\ \ldots\}$$

Para la sucesión

$$\{d_n\} = \{2,\ 3,\ 6,\ 11,\ \ldots n^2+2,\ \ldots\}$$

la sucesión derivada es

$$\{d_n\}' = \{1,\ 3,\ 5,\ 7,\ \ldots 2n-1,\ \ldots\}$$

y para

$$\{f_n\} = \{-1,\ 0,\ 3,\ 8,\ \ldots n^2-1,\ \ldots\}$$

la sucesión derivada es

$$\{f_n\}' = \{1,\ 3,\ 5,\ 7,\ \ldots 2n-1,\ \ldots\}$$

[13]En el caso en que la sucesión $\{a_n\}$ sea creciente escogeremos como su derivada $b_n = a_{n+1} - a_n$, si es decreciente la escogemos como $b_n = a_n - a_{n+1}$.

En general si

$$\{a_n\} = \{0 + a,\ 1 + a,\ 4 + a,\ 9 + a,\ \ldots n^2 + a,\ \ldots\}$$

la sucesión derivada es, en todos los casos, la misma

$$\{a_n\}' = \{1,\ 3,\ 5,\ 7, \ldots 2n - 1,\ \ldots\}.$$

O sea que para cualquier sucesión $\{a_n\}$ y para cualquier número fijo a, las sucesiones

$$\{a_n\} \quad \text{y} \quad \{a_n + a\}$$

tienen la misma derivada.

Si hacemos la suma de la sucesión derivada, desde el primer término hasta el término n-esimo obtenemos, en todos los casos:

$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$$

Aquí está la semilla del teorema fundamental del cálculo.

Ejercicios

1. *Lea el artículo: Imaz, C., (1996). Una alternativa teórica del Cálculo, en Investigaciones en educación matemática. México. D.F.: Grupo editorial Iberoamérica. p. p. 17-26. Estudie relaciones entre series de números infinitesimales e integrales.*

2. *Si primero derivamos y luego sumamos no regresamos a la sucesión original ¿Habrá algún camino para lograr esto? Dada una sucesión, ¿es posible encontrar sucesiones de las que ella sea derivada?*

Leibniz usó con maestría estas series, llamadas *telescópicas* para, deducir resultados sorprendentes; por ejemplo, consideró la sucesión:

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \cdots, \frac{1}{n}, \cdots$$

sumó la sucesión de sus diferencias[14]

$$\left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \left(\frac{1}{4} - \frac{1}{5}\right) + \left(\frac{1}{5} - \frac{1}{6}\right) + \left(\frac{1}{6} - \frac{1}{7}\right) + \cdots = 1$$

[14]Debemos tener cuidado al aplicar procedimientos que conocemos válidos para sumas finitas a series infinitas.

y obtuvo:

$$\frac{1}{2}+\frac{1}{6}+\frac{1}{12}+\frac{1}{20}+\frac{1}{30}+\frac{1}{42}+\cdots+\frac{1}{n(n+1)}+\cdots=1$$

multiplicó término a término esta sucesión por 2 y consiguió:

$$\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\frac{1}{10}+\cdots+\frac{2}{n(n+1)}+\cdots=2$$

que es ¡*la serie de los inversos de los números triangulares*!

Luego sumó la sucesión de las diferencias de la sucesión

$$\frac{1}{2},\ \frac{1}{6},\ \frac{1}{12},\ \frac{1}{20},\ \frac{1}{30},\ \frac{1}{42},\ \cdots,\ \frac{1}{n(n+1)},\ \cdots$$

con el resultado:

$$\left(\frac{1}{2}-\frac{1}{6}\right)+\left(\frac{1}{6}-\frac{1}{12}\right)+\left(\frac{1}{12}-\frac{1}{20}\right)+\left(\frac{1}{20}-\frac{1}{30}\right)+\left(\frac{1}{30}-\frac{1}{42}\right)+\left(\frac{1}{42}-\frac{1}{56}\right)$$
$$+\cdots=\frac{1}{2}$$

es decir que

$$\frac{1}{3}+\frac{1}{12}+\frac{1}{30}+\frac{1}{60}+\cdots+\frac{2}{n(n+1)(n+2)}+\cdots=\frac{1}{2}$$

Para construir una sucesión cuya suma sea $\frac{1}{3}$ hacemos la sucesión de las diferencias de esta sucesión,

$$\frac{1}{3},\ \frac{1}{12},\ \frac{1}{30},\ \frac{1}{60},\ \cdots,\ \frac{2}{n(n+1)(n+2)},\ \cdots$$

y obtenemos

$$\frac{1}{4}+\frac{1}{20}+\cdots+\frac{2\times 3}{n(n+1)(n+2)(n+3)}+\cdots$$

y así sucesivamente, obtenemos sucesiones cuya suma es $\frac{1}{4},\ \frac{1}{5},\ \frac{1}{6},$ etc.

Con ellas Leibniz formó un triángulo similar al triángulo de Pascal, llamado *triángulo armónico:*

$$
\begin{array}{ccccccccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \cdots & \frac{1}{n} & \cdots & \\
\frac{1}{2} & \frac{1}{6} & \frac{1}{12} & \frac{1}{20} & \frac{1}{30} & \frac{1}{42} & \cdots & \frac{1}{n(n+1)} & \cdots & & \\
\frac{1}{3} & \frac{1}{12} & \frac{1}{30} & \frac{1}{60} & & \cdots & & \frac{2}{n(n+1)(n+2)} & \cdots & & \\
\frac{1}{4} & \frac{1}{20} & \frac{1}{60} & & \cdots & & & \frac{2\times 3}{n(n+1)(n+2)(n+3)} & \cdots & & \\
\vdots & & & & & & & & & &
\end{array}
$$

consiguiendo sucesiones infinitas de números racionales, *que no son series geométricas* cuya suma es un número racional; también decimos que la serie converge a un número racional.

Ejercicio

Encontrar el término n-ésimo para la k-ésima fila del triángulo armónico.

5. Series p

Luego de encontrar la suma de los inversos de los números triangulares es natural la pregunta ¿la serie de los inversos de los cuadrados

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots+\frac{1}{n^2}+\cdots$$

Converge[15]?

Jacob Bernoulli usó la desigualdad

$$2n^2 \geq n(n+1),$$

en la forma

$$\frac{1}{k^2} \leq \frac{1}{k\cdot\dfrac{(k+1)}{2}}$$

para comparar

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots+\frac{1}{n^2}+\cdots \leq 1+\frac{1}{3}+\frac{1}{6}+\frac{1}{10}+\cdots+\frac{1}{n\dfrac{(n+1)}{2}}$$

[15]Este problema, conocido como el *problema de Basilea*, fue planteado por Pietro Mengoli (1625-1686), en 1684, a Jacob Bernoulli (1654-1705), y fue expuesto a la comunidad matemática en 1698.

y como la suma de los inversos de los triangulares converge a 2, concluyó que

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots+\frac{1}{n^2}+\cdots\leq 2$$

El mismo argumento sirve para afirmar que como

$$\frac{1}{n^p}\leq\frac{1}{n^2}\quad\text{para todo } p\geq 2,$$

la serie

$$1+\frac{1}{2^p}+\frac{1}{3^p}+\cdots+\frac{1}{k^p}+\cdots$$

converge para $p=3,4,5,\ldots$

Estas series[16] son conocidas como series p. Ni Jacob Bernoulli, ni Leibniz pudieron con el caso $p=2$, Euler encontró que si $p=2$

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots=\frac{\pi^2}{6},$$

si $p=4$ la serie converge a $\dfrac{\pi^2}{90}$. Ahora tenemos ¡series de números racionales que convergen a números irracionales!

Ejercicio

Sabemos que la serie de los inversos de los números triangulares tiene una suma finita, pero la de los inversos de todos los naturales no ¿qué sucede con la serie de los inversos de los números pares y con la de los inversos de los impares?

5.3.3. El conjunto subyacente a los números enteros como una representación de los números naturales

En lo que hemos hecho hasta ahora hemos conseguido representaciones de los números naturales en subconjuntos propios de ellos, o en algunos subconjuntos de números racionales definidos por subconjuntos de números naturales (inversos de triangulares, de cuadrados, etc.) y vimos que podemos copiar su estructura; estudiaremos ahora la posibilidad de construir

[16] La serie $1+\dfrac{1}{2^p}+\dfrac{1}{3^p}+\cdots+\dfrac{1}{k^p}+\cdots$ define para todo valor *real* $p>1$ una función conocida como la función ζ de Riemann, una de las más importantes de la teoría de números.

representaciones de los números naturales en un conjunto donde estos están contenidos como subconjunto, por ejemplo en el conjunto subyacente a los números enteros.

Como objeción podríamos decir que los naturales son la mitad de los enteros, en el sentido de que uno de cada dos son naturales, que los enteros no tienen un primer número, y además que los enteros son un conjunto de números que tiene su propia estructura: es un grupo abeliano con la suma y junto con la multiplicación forma un anillo conmutativo, y los números naturales no tienen esa estructura. Pero podemos hacer *una copia aumentada* de los naturales en el conjunto subyacente a los números enteros, definiendo la función biyectiva:

$$f : \mathrm{N} \to \mathrm{Z}$$

$$n \mapsto f(n) = \begin{cases} -\dfrac{n}{2} & \text{si } n \text{ es par} \\ \dfrac{n+1}{2} & \text{si } n \text{ es impar} \end{cases}$$

que ordena al conjunto subyacente a los números enteros en la forma:

$$0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 4,\ -4,\ \ldots$$

y, también podemos copiar tanto la suma como el producto de los números naturales, para definir dos nuevas operaciones $\oplus$ y $\otimes$ entre los elementos del conjunto descrito anteriormente, como

$$a \oplus b = f(f^{-1}(a) + f^{-1}(b))$$

y

$$a \otimes b = f(f^{-1}(a) \times f^{-1}(b))$$

o más explícitamente[17]

$$z \oplus w = \begin{cases} z + w & \text{si } z \leq 0 \text{ y } w \leq 0 \\ 1 - z - w & \text{si } z > 0 \text{ y } w > 0 \\ z - w & \text{si } z > 0 \text{ y } w \leq 0 \\ w - z & \text{si } z \leq 0 \text{ y } w > 0 \end{cases}$$

y

$$z \otimes w = \begin{cases} -2 \times z \times w & \text{si } z \leq 0 \text{ y } w \leq 0 \\ 2 \times z \times w - (z + w) + 1 & \text{si } z > 0 \text{ y } w > 0 \\ 2 \times z \times w - w & \text{si } z > 0 \text{ y } w \leq 0 \\ 2 \times z \times w - z & \text{si } z \leq 0 \text{ y } w > 0 \end{cases}$$

[17] Con $+$, $-$ y $\times$ representando la suma, la resta y el producto usual de números enteros.

haciendo que el conjunto de los símbolos que representan usualmente a los números enteros con las nuevas operaciones, forme una estructura isomorfa a la de los números naturales.

En particular, vemos que el sucesor de -1 es 2 que corresponde a $(-1) \oplus 1 = 1 - (-1) = 2$; el sucesor de 2 es $2 \oplus 1 = -2$ y así sucesivamente. En general el sucesor de un elemento x en Z es $x \oplus 1$, puesto que $x \oplus 1 = f(f^{-1}(x) + f^{-1}(1)) = f(f^{-1}(x) + 1)$ y $f^{-1}(x) + 1$ es el sucesor de $f^{-1}(x)$.

Si definimos una relación de orden "$\underline{\leq}$" en Z, como

$$a \underline{\leq} b \quad \text{si y sólo si} \quad f^{-1}(a) \leq f^{-1}(b)$$

con a y b elementos de Z. Es inmediato comprobar que la relación $\underline{\leq}$ es de orden y es total, pues la relación $\leq$ en N es de orden y es total y f es biyectiva. De manera general, todas las propiedades que cumple la relación $\leq$ en N también se cumplen en la relación $\underline{\leq}$ en Z.

CAPÍTULO 6

Equivalencia (o equipotencia) de conjuntos

El Álgebra es generosa, a menudo da más de lo que le preguntamos
D´Alembert

En este capítulo definimos equivalencia de conjuntos, estudiamos sus propiedades y las usamos para definir conjuntos finitos e infinitos. La noción de equivalencia no tiene mayor dificultad si nos referimos a conjuntos finitos y aún a conjuntos como el de los números naturales; sin embargo, en general esta noción genera muchos problemas vinculados con la paradoja de Russell. Quizá por esto, resulta ser muy poderosa cuando se remedian los problemas que genera; ella da lugar al concepto de número cardinal que no solo incluye a los números naturales sino que aplicada a otros conjuntos infinitos produce los números cardinales transfinitos, una de las más bellas teorías construidas por George Cantor.

Inicialmente suponemos la existencia de los números naturales y los usamos para definir los conjuntos finitos y estudiar sus propiedades, luego los comparamos con otros conjuntos no finitos, y para ello definimos la enumerabilidad y mostramos que la unión finita o enumerable y el producto cartesiano de conjuntos enumerables es enumerable, resultados que usamos para demostrar que los números racionales y los algebraicos son conjuntos enumerables. Al final presentamos someramente a los números cardinales y ordinales transfinitos, definimos operaciones entre ellos y mostramos algunas de sus propiedades.

6.1. Definición y propiedades

Dos conjuntos A y B son *equivalentes* (ó *equipotentes*) si existe una función biyectiva de A en B, lo notamos: A $\sim$ B. La equipotencia cumple las siguientes propiedades:

i) Dado A un conjunto, A $\sim$ A, pues la función idéntica definida de A en A por: $f(x) = x$ para todo $x \in$ A, es biyectiva.

ii) Dados A y B conjuntos, si A $\sim$ B entonces B $\sim$ A, porque si A $\sim$ B existe un función biyectiva f de A en B y por lo tanto existe la función f^{-1} de B en A, inversa de f que también es biyectiva, lo que significa que B $\sim$ A.

iii) Dados A, B y C conjuntos si A $\sim$ B y B $\sim$ C entonces A $\sim$ C. Esto es consecuencia de que si A $\sim$ B y B $\sim$ C existen funciones biyectivas g de A en B y h de B en C, de forma que la función compuesta $h \circ g$ es una función biyectiva de A en C, es decir que A $\sim$ C.

6.1.1. Estabilidad de la equivalencia con el producto cartesiano

La equivalencia de conjuntos es estable o compatible con el producto cartesiano; esto significa que si A, B, C y D son conjuntos y

$$\mathrm{A} \sim \mathrm{B} \quad \text{y} \quad \mathrm{C} \sim \mathrm{D},$$

entonces

$$\mathrm{A} \times \mathrm{C} \sim \mathrm{B} \times \mathrm{D}.$$

Como A $\sim$ B existe una función biyectiva g de A en B y como C $\sim$ D existe una función biyectiva h de C en D, entonces la función producto:

$$\begin{aligned} \mathrm{F} : \mathrm{A} \times \mathrm{C} &\to \mathrm{B} \times \mathrm{D} \\ (x, y) &\mapsto \mathrm{F}(x, y) = (g(x), h(y)) \end{aligned}$$

también es una función biyectiva. Es inyectiva porque si $\mathrm{F}(x, y) = \mathrm{F}(z, w)$ entonces

$$(g(x), h(y)) = (g(z), h(w))$$

lo que implica que $g(x) = g(z)$, $h(y) = h(w)$ y como g y h son inyectivas concluimos que $x = z$, $y = w$.

Ejercicio

Pruebe que la función F *es sobre.*

Sin embargo, el comportamiento de la equivalencia de conjuntos con la unión y con la intersección de conjuntos no es tan noble, por ejemplo: si $\mathrm{A} = \{0, 1\}$, $\mathrm{B} = \{a, b\}$, $\mathrm{C} = \{0\}$ y $\mathrm{D} = \{c\}$ tenemos que $\mathrm{A} \sim \mathrm{B}$ y $\mathrm{C} \sim \mathrm{D}$, pero $\mathrm{A} \cup \mathrm{C}$ no es equivalente a $\mathrm{B} \cup \mathrm{D}$, ni $\mathrm{A} \cap \mathrm{C}$ es equivalente a $\mathrm{B} \cap \mathrm{D}$.

Pero si A y B son *conjuntos disyuntos*, C y D *son también disyuntos* entonces

$$\mathrm{A} \sim \mathrm{C} \text{ y } \mathrm{B} \sim \mathrm{D} \text{ implica que } \mathrm{A} \cup \mathrm{B} \sim \mathrm{C} \cup \mathrm{D}.$$

Para demostrarlo, construyamos una función biyectiva T de $\mathrm{A} \cup \mathrm{B}$ en $\mathrm{C} \cup \mathrm{D}$, definida por:

$$\mathrm{T}(x) = \begin{cases} f(x) & \text{si } x \in \mathrm{A} \\ g(x) & \text{si } x \in \mathrm{B} \end{cases}$$

donde f y g son las funciones biyectivas definidas de A en C y de B en D respectivamente.

Ejercicios

1. *Pruebe que la función* T *es biyectiva.*

2. *¿Qué sucede con la intersección, la diferencia y las otras 13 operaciones entre pares de conjuntos en relación con la equivalencia de conjuntos?*

3. *Pruebe que dados* A, B *y* C *conjuntos,*

   a) $\mathrm{A} \times \mathrm{B} \sim \mathrm{B} \times \mathrm{A}$.

   b) $\mathrm{A} \times \{x\} \sim \mathrm{A}$.

   c) $\mathrm{A} \times (\mathrm{B} \times \mathrm{C}) \sim (\mathrm{A} \times \mathrm{B}) \times \mathrm{C}$.

6.1.2. Conjuntos finitos

Si comparamos dos subconjuntos no vacíos de números naturales de la forma:

$$\{1, 2, 3, \ldots, m\} \text{ y } \{1, 2, 3, \ldots, n\}$$

intuitivamente aceptamos que son equivalentes si y solamente si $m = n$.

Veamos que esta intuición resulta cierta o se puede demostrar. Si $m = n$ la función idéntica es la biyección que los hace equivalentes; si suponemos que son equivalentes entonces existe una biyección

$$f : \{1, 2, 3, \ldots, m\} \to \{1, 2, 3, \ldots, n\}$$

y como f es inyectiva, $f(m)$ es un único número natural entre 0 y n; si quitamos del dominio de f al elemento m y en el codominio a su imagen $f(m)$ los conjuntos resultantes también son equivalentes:

$$\{1, 2, 3, \ldots, (m-1)\} \sim \{1, 2, 3, \ldots, n\} - \{f(m)\}$$

pero si del conjunto

$$\{1, 2, 3, \ldots, n\}$$

quitamos el elemento k, el conjunto resultante es equivalente a

$$\{1, 2, 3, \ldots, (n-1)\}$$

ya que la función

$$h : \{1, 2, 3, \ldots, k, \ldots, n\} \to \{1, 2, 3, \ldots, k, \ldots, n\}$$

$$x \to h(x) = \begin{cases} k & \text{si } x = n \\ n & \text{si } x = k \\ x & \text{si } x \neq k \text{ y } x \neq n \end{cases}$$

es biyectiva y por esto $h(n) = k$ es un único número natural entre 1 y n; si quitamos del dominio de h al elemento n y en el codominio a su imagen k los conjuntos resultantes son equivalentes:

$$\{1, 2, 3, \ldots, (n-1)\} \sim \{1, 2, 3, \ldots, n\} - \{k\}.$$

Por la propiedad *iii*) de la equivalencia, concluimos que:

$$\{1, 2, 3, \ldots, (m-1)\} \sim \{1, 2, 3, \ldots, (n-1)\}.$$

Suponiendo que $m \geq n$, reiteramos este proceso de quitar un elemento en cada conjunto hasta obtener la equivalencia:

$$\{1, \ldots, m - (n-1)\} \sim \{1\}$$

de donde concluimos que

$$m - (n-1) = 1$$

o sea que

$$m = n$$

que es lo que queríamos mostrar.

Decimos que un conjunto A es *finito*[1] o que A *tiene m elementos* si existe un número natural m, que notamos $\#(\mathrm{A})$ y lo llamamos el *cardinal* del conjunto A, de forma tal que A es equivalente con el conjunto $\{1, 2, 3, \ldots, m\}$. Definimos el cardinal del conjunto vacío como el número natural 0. Con esto *cada número natural es el cardinal de un conjunto finito.*

En conclusión *dos conjuntos finitos son equivalentes si y solo si tienen el mismo número de elementos*; en símbolos:

$$\mathrm{A} \sim \mathrm{B} \text{ si y solo si } \#(\mathrm{A}) = \#(\mathrm{B}).$$

Notemos que el número de elementos de un conjunto no depende de la forma de contar sus elementos.

6.1.2.1. Propiedades de los conjuntos finitos

1. Sean A, B dos conjuntos finitos disyuntos de m y k elementos respectivamente, entonces $\mathrm{A} \cup \mathrm{B}$ tiene $m + k$ elementos.

Prueba:

Como A es finito existe un número natural m tal que

$$\mathrm{A} \sim \{1, 2, 3, \ldots, m\}$$

y como B es finito existe un número natural k tal que

$$\mathrm{B} \sim \{1, 2, 3, \ldots, k\}.$$

También tenemos que los conjuntos

$$\mathrm{P} = \{1, 2, 3, \ldots, k\} \quad \text{y} \quad Q = \{m+1, m+2, m+3, \ldots, m+k\}$$

son equivalentes por la función biyectiva

$$\begin{aligned} f : P &\to \mathrm{Q} \\ s &\mapsto m + s \end{aligned}$$

y por la propiedad *iii*) de la equivalencia, tenemos que

$$\mathrm{B} \sim \{m+1, m+2, m+3, \ldots, m+k\}.$$

[1] También es posible una definición de conjunto finito independiente del concepto de número natural; por ejemplo Dedekind en 1888 (y Peirce independientemente por la misma época) propuso: un conjunto es finito si no es equivalente con alguno de sus subconjuntos propios. Y una definición que no requiere el concepto de equivalencia, propuesta en 1942, es debida a Tarski: un conjunto A es finito si y sólo si toda familia de subconjuntos de A tiene elemento mínimo.

Entonces

$$A \cup B \sim \{1, 2, 3, \ldots, m, m+1, m+2, m+3, \ldots, m+k\}$$

porque A y B son disyuntos y debido a que $m+1$ es el sucesor de m y cada uno de los demás elementos es sucesor del anterior y por el teorema L2 del capítulo 4, que enuncia: para todo número natural x, se cumple que $x^+ \neq x$; entonces A $\cup$ B tiene $m+k$ elementos.

2. Si un conjunto A es finito, todo subconjunto B de A también es finito[2] y #(B) $\leq$ #(A).

3. Si un conjunto A es finito, entontes A $\cap$ B y A $-$ B son finitos.

4. Si B es un subconjunto propio no vacío de un conjunto finito A, entonces #(B) $<$ #(A).

Prueba: Si B es un subconjunto propio no vacío de A, equivalente con A, entonces como A $-$ B es disyunto con B y A = B $\cup$ (A $-$ B) tenemos que

$$\#(\mathrm{A}) = \#(B) + \#(\mathrm{A} - \mathrm{B})$$

como B es no vacío,

$$\#(\mathrm{A}) > \#(\mathrm{B}),$$

de donde concluimos que A y B no son equivalentes contra lo supuesto.

5. La unión de un número finito de conjuntos finitos es un conjunto finito.

Prueba: Consideremos la unión de dos conjuntos finitos A y B sin contar dos veces los elementos comunes entre ellos, es decir,

$$\mathrm{A} \cup \mathrm{B} = \mathrm{A} \cup (\mathrm{B} - \mathrm{A})$$

y como A y (B $-$ A) son conjuntos finitos y disyuntos, entonces

$$\#(\mathrm{A} \cup \mathrm{B}) = \#(\mathrm{A}) + \#(\mathrm{B} - \mathrm{A})$$

y A $\cup$ B es finito.

Haciendo inducción sobre el número de conjuntos, demostramos que la unión finita de conjuntos finitos es un conjunto finito.

Ejercicio

Demuestre por inducción la propiedad 5.

[2]Una prueba de esta afirmación se encuentra en HRBACEK, Karel y JECH, Thomas. Introduction to set theory. 3 ed. New York: Marcel Dekker, 1999. p. 70-71.

6. Si A y B son conjuntos finitos y $\#(\mathrm{A}) = n$, $\#(\mathrm{B}) = m$, para cada $n, m \in \mathrm{N}$, entonces $\#(\mathrm{A} \times \mathrm{B}) = nm$.

Prueba: Haciendo inducción sobre n, con m fijo pero arbitrario. Para $n = 0$, $\mathrm{A} = \varnothing$, y $\varnothing \times \mathrm{B} = \varnothing$, por lo tanto

$$\#(\mathrm{A} \times \mathrm{B}) = \#(\varnothing \times \mathrm{B}) = \#(\varnothing) = 0$$

y como

$$0m = 0$$

la proposición es válida.

Supongamos que para algún $n = k$,

$$\#(\mathrm{A} \times \mathrm{B}) = \#(\mathrm{A})\#(\mathrm{B}) = km.$$

Debemos probar que se cumple para $n = k + 1$; sea A un conjunto con k elementos y w tal que $w \notin A$. El conjunto $\mathrm{A} \cup \{w\}$ es un conjunto con $k + 1$ elementos, por consiguiente:

$$\begin{aligned}
(\mathrm{A} \cup \{w\}) \times \mathrm{B} &= \{(a, b) | a \in (\mathrm{A} \cup \{w\}) \wedge b \in \mathrm{B}\} \\
&= \{(a, b) | (a \in \mathrm{A} \vee a \in \{w\}) \wedge b \in \mathrm{B}\} \\
&= \{(a, b) | (a \in \mathrm{A} \wedge b \in \mathrm{B}) \vee (a \in \{w\} \wedge b \in \mathrm{B})\} \\
&= \{(a, b) | a \in \mathrm{A} \wedge b \in \mathrm{B}\} \cup \{(a, b) | a \in \{w\} \wedge b \in \mathrm{B}\} \\
&= (\mathrm{A} \times \mathrm{B}) \cup (\{w\} \times \mathrm{B}).
\end{aligned}$$

Como $\mathrm{A} \times \mathrm{B}$ y $\{w\} \times \mathrm{B}$ son conjuntos disyuntos, entonces tenemos que

$$\begin{aligned}
\#((\mathrm{A} \cup \{w\}) \times \mathrm{B}) &= \#(\mathrm{A} \times \mathrm{B}) + \#(\{w\} \times \mathrm{B}) \\
&= km + m \\
&= (k + 1)m \\
&= \#(\mathrm{A} \cup \{w\})\#(\mathrm{B})
\end{aligned}$$

lo que concluye la demostración.

Ejercicio

Demuestre que para todo $n \in N$ se cumple que $\#(\wp(A)) = 2^n$ donde $\#(A) = n$.

7. Para todo $n, m \in \mathrm{N}$ se cumple que $\#(\mathrm{A}^{\mathrm{B}}) = n^m$ donde $\#(\mathrm{A}) = n$, $\#(\mathrm{B}) = m$ y A^{B} es el conjunto de todas las funciones de B en A.

Prueba: Por inducción sobre n dejando m fijo pero arbitrario; si $n = 0$ entonces $\mathrm{A} = \varnothing$ y el conjunto de todas las funciones de B en A es vacío puesto que la única relación de B en A (la relación vacía) no es función, entonces $\#(\mathrm{A}^{\mathrm{B}}) = 0 = 0^m$.

Supongamos que se cumple para algún $n = k$, es decir que $\#(\mathrm{A}^{\mathrm{B}}) = k^m$, debemos probar que se cumple para $n = k+1$. Sea $w \notin \mathrm{A}$, entonces $\mathrm{A} \cup \{w\}$ es un conjunto con $k+1$ elementos, estudiemos el número de funciones de B en $\mathrm{A} \cup \{w\}$.

Primero tomemos las funciones en las que w no es imagen de algún elemento, es decir k^m funciones por la hipótesis de inducción. Contemos ahora las funciones de B en $\mathrm{A} \cup \{w\}$ en las cuales w es imagen de un solo elemento de B, como B tiene m elementos, existen m funciones con esta condición y por cada una de estas funciones quedan $m-1$ elementos en B, que deben tener como imagen algún elemento de A, y como A tiene k elementos, por la hipótesis de inducción hay k^{m-1} funciones, luego el número de funciones de B en $\mathrm{A} \cup \{w\}$ en las cuales w es imagen de un sólo elemento de B, es mk^{m-1}.

Con un procedimiento análogo encontramos que el número de funciones de B en $\mathrm{A} \cup \{w\}$ que tienen a w como imagen de 2 elementos de B es $\binom{m}{2}k^{m-2}$ y así hasta contar las funciones en las cuales w es imagen de todos los elementos de B. Por lo tanto, el número de funciones de B en $\mathrm{A} \cup \{w\}$ es:

$$k^m + mk^{m-1} + \binom{m}{2}k^{m-2} + \binom{m}{3}k^{m-3} + \cdots + 1$$

y por el teorema del binomio

$$k^m + mk^{m-1} + \binom{m}{2}k^{m-2} + \binom{m}{3}k^{m-3} + \cdots + 1 = (k+1)^m,$$

luego

$$\#((\mathrm{A} \cup \{w\})^{\mathrm{B}}) = (k+1)^m.$$

En conclusión, la proposición es válida para todo número natural.

6.1.3. Conjuntos infinitos

Buena parte de lo que hemos desarrollado para conjuntos finitos puede extenderse a conjuntos no finitos, que llamaremos *conjuntos infinitos*; pero primero debemos probar[3] que *existen conjuntos infinitos*, y por supuesto el conjunto de los números naturales N es nuestro candidato inicial.

Si N fuera finito existiría un número natural m tal que

$$\mathrm{N} \sim \{1, 2, 3, \ldots, m\}$$

y podríamos aplicarle el procedimiento de quitarle números hasta conseguir que

$$\mathrm{N} - \{1, 2, 3, \ldots, m\} \sim \{1\}.$$

Pero esto no es posible porque el conjunto

$$\mathrm{N} - \{1, 2, 3, \ldots, m\}$$

no puede ser unitario, ya tiene al menos dos elementos distintos: $m + 1$ y su sucesor.

6.1.3.1. Conjuntos enumerables

Decimos que un conjunto A es *enumerable* si $\mathrm{A} \sim \mathrm{N}$ y que es *contable* si es *finito* o *enumerable*. Por definición, todos los conjuntos enumerables tienen el mismo *cardinal* que llamaremos *aleph sub cero* y que notamos $\aleph_0$, este es el primer *cardinal transfinito*.

Si un conjunto A es enumerable existe una función biyectiva entre A y N de manera que los elementos de $\mathrm{A} = \{a_1, a_2, a_3, \ldots, a_n, \ldots\}$, se pueden marcar con subíndices naturales, de manera que $a_i \neq a_j$ si y solo si $i \neq j$.

Ejemplos

1. Los números pares P y los impares I son enumerables, como lo mostramos en el capítulo 5.

2. Los números enteros también son enumerables.

[3] Dentro de la teoría de conjuntos de Zermelo - Fraenkel - Skolem esto se supone como axioma.

6.1.3.2. Propiedades de los conjuntos infinitos

1. Todo conjunto que contenga como subconjunto a los números naturales debe ser también infinito, pues si $\mathrm{N} \subseteq \mathrm{A}$ y A fuera finito entonces por la propiedad 2 de los conjuntos finitos, N sería finito.

2. Un conjunto es infinito si tiene subconjuntos infinitos, porque si fuera finito todos sus subconjuntos serían finitos.

3. Todo conjunto infinito tiene un subconjunto equivalente al conjunto de los números naturales N.

Prueba: Supongamos que A es un conjunto infinito, A no es vacío, por lo tanto, existe un elemento de A, digamos a_1.

$\mathrm{A} - \{a_1\}$ no es vacío (si lo fuera A sería finito, contra la hipótesis). Entonces existe un elemento de $\mathrm{A} - \{a_1\}$, digamos a_2; y así sucesivamente, el conjunto

$$\mathrm{A} - \{a_1, a_2, \ldots, a_n\}$$

no es vacío, luego existe $a_{n+1} \in \mathrm{A} - \{a_1, a_2, \ldots, a_n\}$. y así para cada número natural k, pero el conjunto $\{a_1, a_1, a_3, \ldots\}$ es equivalente a N y

$$\{a_1, a_2, a_3, \ldots\} \subset \mathrm{A}.$$

4. Contrario a lo que sucede con los conjuntos finitos, *si un conjunto* A *es infinito entonces* A *es equivalente a alguno de sus subconjuntos propios.*

Prueba: Como A tiene un subconjunto enumerable,

$$\mathrm{B} = \{b_1, b_2, b_3, \ldots\} \subseteq \mathrm{A}$$

definimos la función

$$f : \mathrm{A} \to \mathrm{B}$$
$$x \mapsto f(x) = \begin{cases} x & \text{si } x \in (\mathrm{A} - \mathrm{B}) \\ b_{2n} & \text{si } x = b_n \end{cases}$$

f es inyectiva y su recorrido es

$$\mathrm{C} = (\mathrm{A} - \mathrm{B}) \cup \{b_2, b_4, b_6, \ldots\}$$

que es un subconjunto *propio* de A, luego A es equivalente a C.

5. Un resultado fácil de sospechar es que la unión de dos conjuntos enumerables es enumerable.

Prueba: Si A y B son disyuntos, los podemos representar:

$$\mathrm{A} = \{a_1, a_2, a_3, \ldots\}, \quad \mathrm{B} = \{b_1, b_2, b_3, \ldots\}$$

con $a_i \neq b_i$ para todo i en N, y su unión la enumeramos en la forma:

$$\mathrm{A} \cup \mathrm{B} = \{a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n, \ldots\},$$

lo que muestra que $\mathrm{A} \cup \mathrm{B}$ es enumerable. Si A y B no son disyuntos consideramos

$$\mathrm{A} \cup \mathrm{B} = \mathrm{A} \cup (\mathrm{B} - \mathrm{A})$$

y aplicamos el razonamiento anterior.

6. También es de esperarse que la unión de un número finito de conjuntos enumerables sea enumerable.

7. El producto cartesiano $\mathrm{A} \times \mathrm{B}$ de dos conjuntos enumerables es enumerable.

Prueba: Como A y B son enumerables son ambos equivalentes a N, tomemos dos copias diferentes de N, pero equivalentes, por ejemplo:

$$N \sim \{2^n : n \in N\} \quad \text{y} \quad \mathrm{N} \sim \{5^k : k \in \mathrm{N}\}.$$

Por la propiedad *iii*) de la equivalencia podemos hacer equivalentes a una de ellas con A y a la otra con B y así:

$$\mathrm{A} \times \mathrm{B} \sim \{(2^n, 5^k) : n, k \in \mathrm{N}\} \sim \{2^n \times 5^k : n, k \in N\}$$

pero $\{2^n \times 5^k : n, k \in \mathrm{N}\}$ es un subconjunto enumerable de N, por lo tanto $\mathrm{A} \times \mathrm{B}$ es enumerable.

8. El producto cartesiano de un número finito de conjuntos enumerables es enumerable.

Ejercicio

Demuestre las propiedades 6 y 8 para conjuntos enumerables.

Ya hemos desarrollado herramientas para demostrar ¡*sin mostrar alguna función biyectiva*! que:

i. El conjunto Q de todos los números racionales es enumerable, pues Q es equivalente a un subconjunto de $\mathrm{N} \times \mathrm{N}$.

ii. En R^2 (ó en R^n) el conjunto de todos los puntos de coordenadas racionales es enumerable.

9. Un resultado sorprendente es que la unión de un número enumerable de conjuntos enumerables es enumerable.

Prueba: Debemos probar que si $\{\mathrm{A}_j\}_{j\in N}$ es una colección enumerable de conjuntos enumerable, entonces la unión $\bigcup_{j=1}^{\infty} \mathrm{A}_j$ es enumerable.

Para ello supongamos que A_j es enumerable para todo $j \in \mathrm{N}$ y que los conjuntos $\mathrm{A}_1, \mathrm{A}_2, \mathrm{A}_3, \ldots$ son disyuntos, dos a dos, entonces podemos enumerar cada uno de ellos en la forma

$$\mathrm{A}_j = \{a_{j1}, a_{j2}, a_{j3}, \ldots a_{jn}, \ldots\}, j \in \mathrm{N}.$$

Definimos la función

$$\begin{aligned} f : \bigcup_{j=1}^{\infty} \mathrm{A}_j &\to \mathrm{N} \times \mathrm{N} \\ a_{jn} &\mapsto f(a_{jn}) = (j, n) \end{aligned}$$

f es biyectiva y por lo tanto

$$\bigcup_{j=1}^{\infty} \mathrm{A}_j \sim \mathrm{N} \times \mathrm{N} \sim \mathrm{N}.$$

Si los conjuntos no son disyuntos dos a dos, definimos

$$\begin{aligned} \mathrm{B}_1 &= \mathrm{A}_1 \\ \mathrm{B}_2 &= \mathrm{A}_2 - \mathrm{A}_1 \\ \mathrm{B}_3 &= \mathrm{A}_3 - (\mathrm{A}_1 \cup \mathrm{A}_2) \\ &\vdots \\ \mathrm{B}_n &= \mathrm{A}_n - (\mathrm{A}_1 \cup \mathrm{A}_2 \cup \ldots \cup \mathrm{A}_{n-1}) \end{aligned}$$

y con esto cada B_i es disyunto con cada B_j si $i \neq j$ y

$$\bigcup_{n=1}^{\infty} \mathrm{A}_n = \bigcup_{n=1}^{\infty} \mathrm{B}_n$$

B_1 es enumerable y cada B_i con $i \geq 2$ es finito o enumerable, entonces se tiene que $\bigcup_{n=1}^{\infty} \mathrm{B}_n$ es enumerable y en consecuencia $\bigcup_{n=1}^{\infty} \mathrm{A}_n$ es enumerable.

Una bonita consecuencia del resultado anterior es que *el conjunto S de todos los polinomios de coeficientes racionales es enumerable.*

Prueba: Si llamamos S_n al conjunto de todos los polinomios con coeficientes racionales de grado n, entonces

$$\mathrm{S}_n \sim \mathrm{Q}^{n+1}$$

porque un polinomio de grado n tiene $n+1$ coeficientes racionales y

$$\mathrm{Q}^{n+1} \sim \mathrm{N}^{n+1}$$

porque Q es equivalente a N, pero

$$\mathrm{N}^{n+1} \sim \mathrm{N}$$

porque el producto cartesiano de un número finito de conjuntos enumerables es enumerable. Finalmente,

$$S = \bigcup_{n=1}^{\infty} \mathrm{S}_n \sim \mathrm{N}$$

por ser una unión enumerable de conjuntos enumerables.

Como consecuencia de estos resultados, una perla! *El conjunto de los números algebraicos*[4] *es enumerable.*

La prueba es inmediata si utilizamos el teorema fundamental del álgebra que afirma que una ecuación polinómica de grado n tiene a lo más n raíces y como hay un número enumerable de ecuaciones polinómicas, entonces hay un número enumerable de soluciones, es decir de números algebraicos. De nuevo, no hemos definido función biyectiva alguna[5].

La condición de biyectividad puede debilitarse un poco con base en el teorema de Schröder-Bernstein[6] que nos garantiza que si existen dos funciones inyectivas $h : \mathrm{A} \to \mathrm{B}$ y $g : \mathrm{B} \to \mathrm{A}$, entonces existe una biyección $f : \mathrm{A} \to \mathrm{B}$.

Podemos usar este teorema para demostrar de otra forma que los números racionales no negativos son enumerables, encontrando una función inyectiva de los números racionales no negativos en los naturales, pues la otra es obvia.

La manera habitual es hacer una sucesión de la siguiente tabla escogiendo los números en diagonal:

[4]Un número es algebraico si es la solución de una ecuación polinómica con coeficientes racionales.

[5]BREUER, J. Iniciación a la Teoría de Conjuntos. Madrid: Paraninfo, 1972. p. 44-52.

[6]SUPPES, Patrick. Teoría axiomática de conjuntos. Cali: Norma, 1968. p. 60-61.

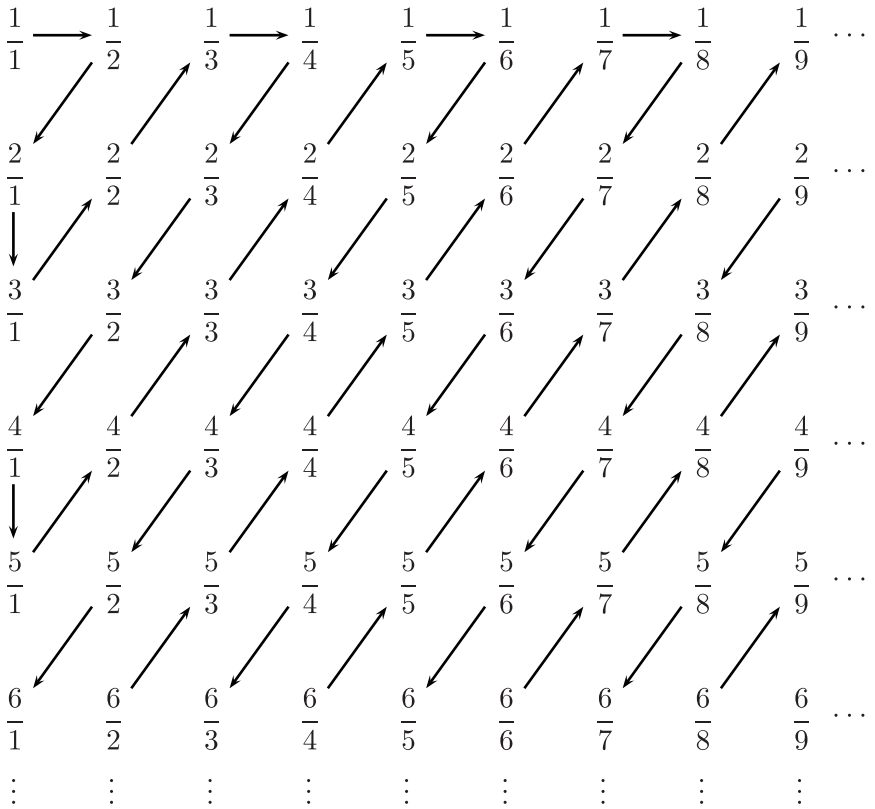


Tabla 1

para obtener:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \ldots$$

Lo que nos sugiere definir la función inyectiva

$$f : N \times (\mathrm{N} - \{0\}) \to \mathrm{N}$$
$$(a, b) \mapsto f((a, b)) = \frac{1}{2}(a + b - 1)(a + b - 2) + b$$

que puede expresarse en términos de números triangulares T_n como

$$f((a, b)) = T_{(a+b-2)} + b.$$

Si identificamos a los números racionales no negativos[7] que notamos Q, con las clases de equivalencia $[(a,b)]$ según la relación $(a,b) \sim (c,d)$ si y sólo si $ad = bc$, la función

$$h : \mathrm{Q} \to \mathrm{N} \times (\mathrm{N} - \{0\})$$
$$[(a,b)] \mapsto h([(a,b)]) = (a,b)$$

es inyectiva y la composición

$$f \circ h : Q \to N$$

también es inyectiva, lo que demuestra que los números racionales no negativos son enumerables.

Ejercicio

Demuestre que la función f es inyectiva.

6.2. Generalizaciones de la noción de número natural

Hasta ahora hemos supuesto la existencia de los números naturales y con ellos definimos el cardinal de un conjunto finito o enumerable; vamos ahora a tomar la noción de cardinalidad como primitiva para asignarle a cada conjunto infinito un cardinal dentro de la teoría de Zermelo-Fraenkel-Skolem, y para ello es necesario agregar el axioma:

> *A cada conjunto le corresponde un número cardinal de manera que dos conjuntos equivalentes tienen el mismo cardinal.*

6.2.1. Los números cardinales transfinitos

Ya conocemos el cardinal de los números naturales $\aleph_0$, debemos encontrar ahora otros números cardinales infinitos, y una fuente de ellos está en otro descubrimiento de Cantor; él demostró[8] que un conjunto cualquiera E no puede ser puesto en correspondencia biunívoca con el conjunto de

[7] LUQUE, MORA y TORRES, Op. cit., 2005, p. 115 - 128.

[8] Una demostración de este teorema se encuentra en: KURATOWSKI, Kazimierz. Introducción a la teoría de conjuntos y a la topología. Barcelona: Vinces-Vives, 1966. p. 63.

sus partes[9] $\wp$(E) y por tanto el conjunto $\wp(\wp(\mathrm{E}))$ no puede ser puesto en biyección con $\wp$(E) y así sucesivamente.

Esto significa que dado un cardinal infinito o cardinal transfinito, por ejemplo $\aleph_0$, siempre existe uno mayor y en consecuencia hay una infinidad de números transfinitos diferentes[10].

6.2.1.1. Operaciones entre números cardinales transfinitos

Entre los números cardinales transfinitos también podemos definir las operaciones aritméticas básicas como suma, multiplicación y potenciación que comparten algunas propiedades con las operaciones definidas para los números naturales.

La *suma* de dos números cardinales transfinitos α y β la definimos[11], usando una relación válida entre conjuntos finitos, como el *cardinal de la unión de dos conjuntos disyuntos A y B cuyos cardinales son α y β respectivamente*; esta operación es conmutativa y asociativa; pero a diferencia de los números cardinales finitos, es idempotente, o sea que para todo cardinal transfinito α

$$\alpha + \alpha = \alpha.$$

La definición de sustracción[12] de números cardinales transfinitos no podemos hacerla como el cardinal de la diferencia conjuntista entre ellos, puesto que el resultado no es único; por ejemplo, si hacemos la diferencia entre el conjunto de los números naturales, cuyo cardinal es $\aleph_0$, y él mismo, obtenemos al conjunto vacío; pero si hacemos la diferencia entre el conjunto de los números naturales, cuyo cardinal es $\aleph_0$, y el conjunto de los números impares, cuyo cardinal también es $\aleph_0$, nos resulta el conjunto de los números pares cuyo cardinal es el mismo $\aleph_0$.

También la *multiplicación de dos cardinales transfinitos* α y β, la definimos extendiendo la del caso finito como el *cardinal del producto cartesiano de dos conjuntos A y B cuyos cardinales son α y β respectivamente.* Esta operación también es conmutativa, asociativa, idempotente y distributiva

[9] También llamado *conjunto potencia* de E.

[10] De estas consideraciones surge un problema ¿cuál es el cardinal del conjunto de todos los conjuntos con distintos cardinales? éste debería ser mayor que cualquier cardinal, incluso él mismo. La solución de este problema se consiguió posteriormente limitando el concepto de conjunto para evitar que la colección de los conjuntos con distintos cardinales fuera un conjunto.

[11] Una versión detallada y no tan abstrusa de la aritmética cardinal y ordinal transfinita se encuentra en: KURATOWSKI, Op. cit., p. 59-87. O una más elaborada en: SUPPES, Op. cit., p. 58-99.

[12] La sustracción de números cardinales no está definida.

con respecto a la suma antes definida. Además si uno de los factores es el conjunto vacío, el producto también es vacío.

6.2.2. Los números ordinales infinitos

Otro desarrollo hecho por Cantor entre 1879 y 1884, fue la teoría de los *números ordinales*; en ella diferenció los términos *número cardinal* y *número ordinal*, diciendo que el primero, está vinculado a contar los elementos de un conjunto sin tener en cuenta el orden; el segundo, sí lo tiene en cuenta; las dos nociones coinciden en el caso finito, puesto que no importa cómo se numeren los elementos de un conjunto finito, el último elemento enumerado coincide con el cardinal del conjunto.

Para la definición de números ordinales, Cantor utiliza conjuntos totalmente ordenados; esto es conjuntos ordenados donde cualquier par de elementos x e y del conjunto son comparables, es decir, se tiene que

$$x \leq y \quad \text{o} \quad y \leq x.$$

y define que dado un conjunto X, dos subconjuntos A y B de X, totalmente ordenados son *semejantes* si existe entre los dos un isomorfismo de conjuntos ordenados, es decir si existe una función biyectiva f *que respeta el orden*, o sea que si:

$$x \leq y \text{ entonces } f(x) \leq f(y).$$

Ejercicio

Demuestre que la relación de semejanza es de equivalencia.

Los conjuntos semejantes son equivalentes, pero los conjuntos equivalentes no son siempre semejantes. Sin embargo, si entre los conjuntos totalmente ordenados elegimos los conjuntos *bien ordenados*, o sea aquellos cuyos subconjuntos no vacíos tienen siempre elemento mínimo, obtenemos los *números ordinales*, de manera que

Dos conjuntos bien ordenados semejantes tienen el mismo número ordinal.

El conjunto vacío se asume que está bien ordenado y en el caso de los conjuntos finitos su número ordinal coincide con el cardinal, puesto que los órdenes totales que se pueden definir en un conjunto A con n elementos son buenos órdenes y difieren a lo más en una permutación de los elementos del conjunto A, es decir que cada permutación, que es una función biyectiva,

induce un buen orden en A y todos estos órdenes son isomorfos, por lo que definen un solo número ordinal, el n-esimo.

Ejercicios

Demuestre que:

1. *Todo subconjunto de un conjunto bien ordenado está bien ordenado.*
2. *Todo conjunto ordenado, que es semejante a un conjunto bien ordenado, está bien ordenado.*
3. *Todo conjunto finito está bien ordenado.*

En 1904, Ernst Zermelo demostró[13] que *todo conjunto puede ser bien ordenado*. Para ello utilizó el axioma de elección[14] que, como ya dijimos, establece que de cualquier colección no vacía de conjuntos no vacíos, es posible elegir en cada uno de ellos un elemento para formar un nuevo conjunto.

El teorema de Zermelo implica que puede cambiarse el orden de cualquier conjunto de forma que sea un conjunto bien ordenado. Este teorema garantiza la existencia de un buen orden pero no ofrece la forma de construirlo.

Para definir los primeros números ordinales podemos elegir un representante de cada clase de conjuntos bien ordenados semejantes, como lo hicimos en el capítulo 4, en la forma:

$$0 = \varnothing, \qquad 1 = \{0\}, \qquad 2 = \{0, 1\}, \ldots,$$

el $(n+1)$-*ésimo* ordinal lo definimos por recursión como

$$n + 1 = \{0, 1, 2, 3, \ldots, n\}.$$

Y hasta aquí la coincidencia con los números cardinales, porque ahora introducimos el *primer número ordinal transfinito*, el ordinal de los números naturales con orden creciente:

$$\omega = \{0, 1, 2, 3, \ldots\}$$

y sus sucesores:

$$\omega + 1 = \{0, 1, 2, 3, \ldots, \omega\}$$

[13]Una demostración del teorema de Zermelo se encuentra en KURATOWSKI, Op. cit., p. 84-85.

[14]El Axioma de elección, el teorema de buena ordenación y el hecho de que los cardinales de dos conjuntos cualesquiera son comparables son afirmaciones equivalentes.

$$\omega + 2 = \{0, 1, 2, 3, \ldots, \omega, \omega + 1\}$$

$$\vdots$$

$$\omega + \omega = 2\omega = \{0, 1, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$$

y así sucesivamente.

El número ordinal del conjunto de los números naturales pero en orden decreciente lo notamos ${}^*\omega$.

Ejercicio

Demuestre que $\omega \neq^* \omega$, es decir, que los números naturales con el orden creciente no es semejante con los números naturales con el orden decreciente.

6.2.2.1. Operaciones entre números ordinales

Definimos la *suma de números ordinales* como el ordinal del conjunto que se obtiene posponiendo al primero el segundo de los conjuntos dados, manteniendo en cada uno de ellos el orden original (a este orden se le llama *orden suma*) y asumiendo que todo elemento del primer conjunto es menor que todo elemento del segundo conjunto; por ejemplo $\omega + 3$ es el ordinal del conjunto formado por todos los naturales seguido de ω, $\omega + 1$ y $\omega + 2$ en este orden.

Más generalmente, si X, Y son conjuntos bien ordenados, su *suma ordinal* está definida por

$$\mathrm{X} + \mathrm{Y} = (\mathrm{X} \amalg \mathrm{Y}, \leq).$$

O mejor

$$(\mathrm{X}, \leq_{\mathrm{X}}) + (\mathrm{Y}, \leq_{\mathrm{Y}}) = (\mathrm{X} \amalg \mathrm{Y}, \leq_{\mathrm{X} \amalg \mathrm{Y}})$$

donde $\amalg$ representa a la unión disyunta de X e Y, y el *orden suma* se define:

$$x \leq_{\mathrm{X} \amalg \mathrm{Y}} y \quad \text{si } x \in \mathrm{X} \quad \text{y} \quad y \in \mathrm{Y}$$

y si comparamos elementos de X, o de Y, lo hacemos con su orden particular. Por ejemplo, si

$$\mathrm{X} = \{\underset{a}{\bullet} \to \underset{b}{\bullet}\}$$

$$\mathrm{Y} = \{\underset{0}{\bullet} \to \underset{1}{\bullet} \to \underset{2}{\bullet}\}$$

entonces

$$\text{X+Y} = \{\underset{a}{\bullet} \to \underset{b}{\bullet} \to \underset{0}{\bullet} \to \underset{1}{\bullet} \to \underset{2}{\bullet}\}.$$

Como vemos, esta suma *no es conmutativa*, por ejemplo como $\omega = \{0, 1, \ldots\}$, entonces

$$\omega + 1 = \{0, 1, \ldots, \omega\}$$

pero

$$1 + \omega = \{\omega, 0, 1, 2, \ldots\} \equiv \omega$$

porque si cambiamos de nombre

$$\omega \to 0, 0 \to 0', \ldots\ p \to p', \text{etc.}$$

obtenemos

$$1 + \omega = \{0, 0', 1', 2', \ldots\} = \omega.$$

El ordinal de los números enteros con su orden natural es ${}^*\omega + \omega$.

En el conjunto de los números ordinales también se definen las operaciones de multiplicación y potenciación como se detalla en las referencias citadas.

Por último queremos mencionar que los números ordinales también están ordenados, según la secuencia:

$$0, 1, 2, \ldots, \omega, \omega+1, \omega+2, \ldots, \omega+\omega = 2\omega, 2\omega+1, 2\omega+2 \ldots, \omega^2 = \omega \times \omega \ldots,$$

donde ω es el primer *ordinal infinito* pero ω y $\omega + \omega$ no son sucesores de algún número, por lo que son llamados *ordinales límite*.

También podemos usar el orden para clasificar los números ordinales como sigue:

En la primera clase notada O_1 están los *ordinales finitos*. En la segunda clase O_2 están los ordinales

$$\omega, \omega + 1, \omega + 2, \ldots, 2\omega, 2\omega + 1, \ldots, 3\omega, 3\omega + 1, \ldots, \omega \times \omega = \omega^2, \omega^3, \ldots \omega^\omega, \ldots$$

donde $\omega \times \omega$ es un conjunto formado por ω copias de ω. Cada uno de estos ordinales es *el ordinal de un conjunto cuyo cardinal es* $\aleph_0$.

El conjunto de los ordinales que hay en O_2 no es enumerable, Cantor introdujo para su cardinal el símbolo $\aleph_1$; y demostró que es el primer cardinal después de $\aleph_0$.

Los ordinales de tercera clase O_3 son

$$\Omega, \Omega + 1, \Omega + 2, \ldots, \Omega + \Omega, \ldots$$

Estos son números ordinales de conjuntos bien ordenados, cada uno de los cuales tiene $\aleph_1$ elementos. El cardinal de O_3 es mayor que $\aleph_1$ y lo denotamos $\aleph_2$ y así sucesivamente construimos nuevos cardinales y ordinales.

Entre números cardinales no es posible establecer en general una relación de orden, pero si los cardinales son de conjuntos bien ordenados, Cantor demostró que sí son comparables.

En 1897, Cesare Burali-Forti mostró que el conjunto bien ordenado de todos los números ordinales, debería tener como número ordinal el mayor de todos los números ordinales; pero entonces este número ordinal sería mayor que todos los números ordinales planteándose así una paradoja, que ya Cantor había notado en 1885. Para eliminar esta paradoja un grupo de matemáticos entre ellos Hilbert y Russell distinguieron entre clases y conjuntos y establecieron que la clase de todos los ordinales no es un conjunto.

CAPÍTULO 7

Otros conjuntos enumerables de números

A fin de alcanzar la verdad es necesario, una vez en la vida, poner todo en duda.
Descartes

Por lo hecho hasta ahora, podríamos pensar que todos los conjuntos enumerables de números son isomorfos a los números naturales y esto es así si definimos las operaciones de suma y multiplicación por recurrencia como lo hemos hecho, pero podemos definir otras estructuras sobre conjuntos enumerables como lo veremos enseguida.

7.1. Los números enteros

En *Actividades matemáticas para el desarrollo de procesos lógicos: Clasificar, medir e invertir*[1] se presentaron varias representaciones de los números enteros y una construcción de ellos como parejas de números reales positivos, cuando ellas se restringen a los números naturales; esa exposición corresponde a la construcción realizada por Russell utilizando relaciones entre números naturales.

En este capítulo presentamos algunos hechos históricos que llevaron a considerar a los números enteros, particularmente los negativos, como objetos que surgieron por una necesidad teórica en la historia de las matemáticas,

[1]LUQUE, MORA y TORRES, Op. cit., 2005, p. 231-281.

mostramos la construcción de Russell y las axiomatizaciones de Padoa basada en las ideas de sucesor y simétrico, la de Le Veque basada en la estructura algebraica de dominio de integridad ordenado y demostramos la equivalencia de las dos últimas.

Seguidamente hacemos un breve repaso histórico de representaciones de los números racionales y dos caracterizaciones para ellos, una de Weierstrass y otra de Dedekind.

Con respecto a los números algebraicos, no conocemos axiomatización alguna, y solo damos de ellos una somera descripción.

7.1.1. Los números negativos: objetos inaceptables en la historia de las matemáticas

El principal foco de atención en la historia de los números enteros está en la aparición y uso de los números negativos, objetos que no aparecieron como el producto de procesos naturales como es el caso de los números naturales y fraccionarios y, que fueron aceptados como números mucho tiempo después de que fueran formuladas algunas de las leyes que gobiernan su comportamiento.

Uno de los antecedentes al uso de números enteros negativos puede observarse en las civilizaciones antiguas (babilónica, egipcia y china) a través de las operaciones en donde se realizaban sustracciones y se distinguían los sustraendos de alguna forma, por ejemplo, utilizando varillas de color rojo como lo hacían los chinos hacia el primer siglo de nuestra era. Sin embargo, no puede afirmarse que en dichas civilizaciones se concibiera a los enteros negativos como números[2], ya que ni en los enunciados ni en las soluciones de sus problemas aparecen estos entes y tampoco se conocen reglas que hayan sido formuladas para desarrollar cálculos con estos números.

Los griegos, aunque tampoco concebían a los enteros negativos como números, abordaron procedimientos geométricos que los llevaron a obtener equivalencias entre áreas que hoy podemos escribir como

$$(a-b)^2 = a^2 - 2ab + b^2$$

y

$$(a-b)(a+b) = a^2 - b^2$$

en las cuales implícitamente está la idea de multiplicar dos números negativos o un número negativo y uno positivo. No obstante, fue Diofanto en

[2]SMITH, David. History of mathematics. New York: Dover, 1958. v. 2. p. 257

su Aritmética quien dio un paso decisivo para poder trabajar con números negativos, pues él propone un nuevo objeto llamado *deficiencia* y postula, de manera axiomática, algunas reglas para operar con este objeto y con los números positivos que son objetos que denotan *disponibilidad*, a saber[3]: *deficiencia multiplicada por deficiencia da disponibilidad* (el producto de dos números negativos da positivo) y *deficiencia multiplicada por disponibilidad da deficiencia* (el producto de un número negativo por uno positivo da negativo). Para la adición y sustracción de estos nuevos objetos Diofanto no da explícitamente reglas, pero en sus escritos se puede observar cómo al restar ciertos números obtiene números negativos.

Aunque Diofanto trató de caracterizar la estructura de los números enteros, debemos mencionar que solamente uso números negativos como herramienta para realizar cálculos intermedios en el desarrollo de un problema en el que los datos y la solución eran números positivos.

El siguiente vestigio de los números enteros en la historia de las matemáticas aparece en la India, donde personajes como Brahmagupta, hacia el año 628, y Mahavira, hacia el año 825, utilizan números negativos para indicar *deudas* mientras que los números positivos se utilizan para representar *activos*[4]. Brahmagupta, por su parte, en una de sus obras establece reglas para realizar sumas, restas, multiplicaciones y divisiones entre los activos, las deudas y la nada, es decir entre números positivos, negativos y el cero, por ejemplo dice "Una deuda restada de la nada se convierte en un bien, un bien restado de la nada se convierte en una deuda".

Hacia el año 850 aparece una obra del matemático Mahavira en la que se recopilan todas estas reglas para realizar operaciones con números negativos[5]. Posteriormente, estas reglas pueden encontrarse en todos los escritos indios en los que se aborde el tema.

El matemático Indio Bhaskara en el siglo XII, acepta, aunque con cierta prudencia, los números negativos, pues por un lado establece que la raíz cuadrada de un número positivo tiene dos valores, un positivo y otro negativo, pero también afirma que si 50 y -5 son soluciones de un problema, entonces -5 no podrá ser tenido en cuenta ya que es inadecuado y las personas no aceptan soluciones negativas[6].

[3]BASHMAKOVA, I. G. y SMIRNOVA, G. S. The birth of literal Algebra. En: The American Mathematical Monthly. Vol. 106, No. 1. (1999); p. 57-66.

[4]KLINE, Morris. El pensamiento matemático de la antigüedad a nuestros días. Madrid: Alianza Universidad, 1972. v. 1. p. 251.

[5]SMITH, Op. cit., p. 258.

[6]KLINE, Op. cit., p. 251.

El aporte de los árabes al desarrollo del concepto de número negativo es dado particularmente por al-Khowârizmî hacia el año 825 en su obra titulada Al-jabrw'almuqâbala, donde realiza cálculos con cantidades añadidas y sustraídas, que adquieren su carácter de aditivo o sustractivo al margen del calculo que se desea desarrollar[7]; así, para él no existen cantidades positivas o negativas, sino cantidades que se suman o restan a otras. En su obra se dan reglas para operar con estas cantidades, así por ejemplo enuncia[8]:

> "si se tiene diez menos uno por diez menos uno, el diez por el diez es cien; y el uno substraído por el diez es diez substractivo, y el uno también substraído por el diez es diez substractivo. Esto es ochenta. Y el uno substraído por el uno substraído, uno aditivo. Esto es pues ochenta y uno".

De esta forma, al-Khowârizmî da las reglas básicas para realizar las cuatro operaciones con cantidades añadidas y substraídas, o lo que hoy llamaríamos números positivos y negativos, pero, la idea de que tales cantidades substraídas se constituyan en números es inexistente, y expresiones como "menos la cantidad", "menos la cosa" en las que aparece la palabra menos solo pueden interpretarse como indicadores de una sustracción a realizar.

En la edad media y en el renacimiento las cantidades negativas no han sido aceptadas aun como números, y su uso sigue aferrado al tratamiento de ecuaciones. Así, por ejemplo, Cardano obtiene números negativos como raíces de ecuaciones, pero tales soluciones las considera imposibles y las tilda de *ficticias* en tanto que a las raíces positivas las denomina *reales*[9]. Además, propone una de las primeras notaciones para las cantidades negativas anteponiendo "m:" a un número.

Stifel, hacia 1544, relaciona los números negativos con cantidades menores que cero y muestra reglas para operar con ellos. Bonbellí, por su parte denota las cantidades negativas con el prefijo "m." y trata de enunciar las reglas dadas por Diofanto para operar con dichas cantidades de una manera más simple, de la siguiente forma[10]:

[7]PUIG, Luis. Historias de al-Khwârizmî (6.ª entrega). El cálculo con la cosa. En: Suma. Vol. 67. (jun. 2011); p. 101-110.

[8]Ibid., p. 103.

[9]KLINE, Op. cit., p. 338.

[10]DERBYSHIRE, John. Unknown Quantity. A real and imaginary history of Algebra. Washington: Joseph Henry Press, 2006. p. 83.

più̇viapiù fa più
meno viapiù fa meno
più̇via meno fa meno
meno via meno fa più

donde *più* significa positivo, *meno* negativo, *via* veces y *fa* es.

Entre los primeros matemáticos que aceptaron los números negativos están Descartes, Thomas Harriot, Stevin y Girard. Descartes aceptó parcialmente los números negativos al decir que las raíces negativas de una ecuación eran falsas ya que pretendían representar números menores que la nada, pero que las ecuaciones que tenía raíces negativas podían transformarse para obtener ecuaciones cuyas soluciones fueran mayores que las de la original en una cantidad predeterminada. Un clásico resultado que muestra su aceptación de los números negativos aparece en su famosa regla de los signos, en la cual observa la variación de signos en la ecuación para predecir la cantidad posible de raíces negativas o positivas.

Para Harriot, era concebible que un número negativo apareciera como parte de una ecuación, Stevin utilizaba números negativos como coeficientes de una ecuación y al igual que Girard, en su L'Inventionnouvelle en l'algèbre de 1629, los aceptaba como soluciones de una ecuación.

A lo largo de los siglos XVII y XVIII los números negativos continuaron siendo utilizados como los coeficientes de una ecuación, herramientas de cálculo necesarias para resolver la ecuación y eventualmente eran aceptados como las raíces de la ecuación, sin embargo, todavía no eran entendidos. Por ejemplo, Wallis aceptaba los números enteros, pero creía que ellos tenían que ser números mayores que infinito y menores que cero pues, como afirma[11] en su *Arithmeticainfinitorum* de 1665, si a es un número positivo y b un número negativo la razón a/b debería ser mayor que infinito ya que $a/0$ es infinito.

De manera análoga, Euler durante la segunda mitad del siglo XVIII creía que los números negativos eran mayores que infinito.

Los matemáticos de finales del siglo XVIII y comienzos del siglo XIX comenzaron a cuestionarse sobre la validez de las reglas que sus predecesores dieron para trabajar con números negativos, así, por ejemplo Euler trata de justificar la validez de la conocida identidad $(-a)(-c) = ac$ remitiéndose a mostrar que no podía ser igual a $(-a)c$.

Uno de los trabajos más importantes en relación con este aspecto fue el *Treatise of Algebra* de Peacock, en donde su comparación entre álgebra

[11]KLINE, Op. cit., p. 339.

aritmética y álgebra simbólica le permite establecer que las operaciones aritméticas deben ceñirse a las leyes del álgebra simbólica, y estas últimas no necesitan alguna referencia a objetos específicos y simplemente deben establecerse. Por ejemplo, él dice que[12] como en álgebra aritmética si $b > a$ y $d > c$ se tiene $(b - a)(d - c) = bd + ac - ad - bc$, entonces en álgebra simbólica tal identidad debe cumplirse sin imponer restricciones sobre a, b, c y d, lo que permite concluir que $(-a)(-c) = ac$, si $b = d = 0$.

En síntesis, la idea que tenía Pecock sobre álgebra simbólica puede resumirse así[13]:

> En álgebra simbólica, las reglas determinan el significado de las operaciones... podríamos llamarlas suposiciones arbitrarias, ya ellas son impuestas arbitrariamente sobre una ciencia de símbolos y sus combinaciones, las cuales podrían ser adaptadas a cualquier otro sistema asumido de reglas consistentes.

De ahí, que el álgebra deba ser entendida como una ciencia deductiva, a la manera de la geometría, en la que los procesos tienen que estar basados sobre enunciados bien formulados en términos de las operaciones, operaciones que a su vez no tienen otro significado que aquel determinado por los axiomas o leyes declaradas.

En concordancia con esta última idea, Hamilton en su obra *Preliminary and Elementary Essay on Algebra as the Science of Pure Time* de 1835, enfatiza en la necesidad de entender el álgebra como un álgebra práctica en la que se establecen las leyes que permiten manipular las expresiones algebraicas y se definen los objetos en un dominio formal en el que debe evitarse acudir a interpretaciones físicas. Específicamente, en el prefacio él enuncia[14]:

> No se requiere escepticismo especial para dudar, o incluso para desmentir, la doctrina de negativos e imaginarios, cuando declaramos (como comúnmente se ha hecho) cuatro principios como estos: que una *magnitud mayor puede ser substraída de una menor*, y que lo restante es *menor que nada*; que *dos números negativos* o números que denotan magnitudes menores que nada, pueden *multiplicarse* el uno por el otro, y que el producto sea un número *positivo*, o un número que denota un magnitud mayor que la nada; y que *el cuadrado de un número*, o el

[12]KLEINER, Israel. A history of abstract algebra. Boston: Birkhäuser, 2007. p. 13.
[13]Ibid., p. 14.
[14]Ibid., p. 150.

> producto obtenido de multiplicar un número por sí mismo, es además *siempre positivo*, cuando el número sea positivo o negativo, aunque los números, llamados imaginarios, puedan ser encontrados o concebidos o determinados, y operados bajo todas las reglas de los números positivos o negativos, como si ellos estuvieran sujetos a tales reglas, *aunque ellos tengan cuadrados negativos*, y no puedan ser supuestos números negativos, positivos o cero, de tal forma que las magnitudes que ellos denotan no puedan ser mayores que nada, o menores que nada, o incluso iguales a nada.

En 1867 HermannHankel, en el libro *Theorie der KomplexenZahlensysteme*, establece que[15]: "La condición para establecer una aritmética universal es por lo tanto la de una matemática puramente intelectual, separada de todo tipo de percepciones sensibles". En tal sentido, aceptar que un objeto puede ser concebido como un número en matemáticas está únicamente condicionado a que su definición sea posible lógicamente bajo una teoría, en la cual se caracterice claramente el objeto, es decir sin contradicciones, a partir de un conjunto de leyes que determinen su comportamiento.

D'alembert escribe en su *Encyclopéie* que[16]: "las reglas algebraicas de operación con números negativos son admitidas generalmente por todos y reconocidas como exactas, cualquiera que sea la idea que tengamos sobre estas cantidades".

A mediados del siglo XIX el álgebra fue consolidándose como una ciencia de símbolos sin interpretación y sus leyes de combinación, y los diferentes tipos de números comenzaban a ser caracterizados por las propiedades que cumplían las operaciones que entre ellos se definían.

Así, se puede observar que en la historia de las matemáticas, los números negativos, y en sí los números enteros, fueron utilizados como herramientas de cálculo en la solución de ecuaciones pero no fueron aceptados como números hasta que los matemáticos establecieron que las matemáticas son una construcción humana y que los objetos que se estudian en las matemáticas deben caracterizarse a través de las leyes que definen una teoría.

[15]BOYER, Op. cit., p. 693.

[16]KLINE, Morris. El pensamiento matemático de la antigüedad a nuestros días. Madrid: Alianza Universidad, 1972. v. 2. p. 789.

7.1.2. La construcción de Russell

Russell, tratando de derivar toda la matemática de la lógica, define los números enteros, evitando referencias a intuiciones geométricas de segmentos dirigidos y a argumentos algebraicos como suponer soluciones a ecuaciones como $a+x=b$, como relaciones asimétricas de números naturales[17].

En su formulación
$+1$ es la relación R definida para todo $x, y \in$N por:

$$x\mathrm{R}y \quad \text{si y solo si} \quad x = y + 1$$

o en otros términos

$$+1 = \{(m+1, m) : m \in \mathrm{N}\} = \{(1,0), (2,1), (3,2), \dots\}$$

-1 es la relación recíproca de la anterior, tal que para todo $x, y \in$N:

$$x\mathrm{R}'y \quad \text{si y solo si} \quad x + 1 = y$$

o sea

$$-1 = \{(m, m+1) : m \in \mathrm{N}\} = \{(0,\,1), (1,\,2), (2,\,3)\ \dots\}$$

2 es la compuesta de R consigo misma, R^2, definida para todo $x, y \in N$ por:

$$x\mathrm{R}^2y \quad \text{si y solo si} \quad x = y + 2.$$

Y para cada número natural k, R^k es el número positivo $+k$ y R'^k es el número negativo $-k$. Es decir que en general

$$+k = \{(m+k, m) : m \in \mathrm{N}\}$$

$$0 = \{(m, m) : m \in \mathrm{N}\}$$

$$-k = \{(m, m+k) : m \in \mathrm{N}\}.$$

Si $x = \{(m,k) : m, k \in \mathrm{N}\}$ e $y = \{(n,p) : n, p \in \mathrm{N}\}$ son números enteros definimos la suma como[18]

$$x + y = \{(m+n, k+p) : m, n, k, p \in \mathrm{N}\}$$

y la multiplicación como

$$xy = \{(mn+kp, mp+kn) : m, n, k, p \in \mathrm{N}\}.$$

[17]RUSSELL, Bertrand. Introduction to mathematical philosophy. New York: Dover, 1993. p. 64.

[18]FALK, Mary. Introducción a la matemática contemporánea. Bogotá: Universidad Nacional de Colombia, 1992. p. 76 - 79.

7.1.3. La axiomática de Padoa

Alessandro Padoa (1868-1937), un alumno de Peano, define los números enteros como elementos de un conjunto Z no vacío, que satisface:

1. Para cada $a \in Z$ existe un único elemento de Z que denominamos el *siguiente* de a y que notaremos a^+.
2. Para cada $a \in$ Z existe un único elemento de Z que denominamos el *simétrico* de a y notaremos $(-a)$.
3. El simétrico del simétrico de a es a. En símbolos, $a = (-(-a))$.
4. El simétrico de a es igual al siguiente del simétrico del siguiente de a. En símbolos, $-a = (-(a^+))^+$.
5. Existe un elemento en Z que se llama cero y se nota 0 y es el simétrico de sí mismo.
6. Todo elemento distinto de 0 es distinto de su simétrico.
7. Si A es un subconjunto de Z no vacío tal que:

   a) si $a \in$ A entonces $a^+ \in$ A
   b) si $a \in$ A y $a = b^+$ implica que $b \in$ A,

   entonces A = Z.

En el caso de que $a = b^+$ se dice que b es el *antecesor inmediato* de a y se nota $'a$.

La suma la define como:

$$a + 0 = a$$
$$a + b^+ = (a + b)^+$$
$$a + {}'b = {}'(a + b)$$

y la multiplicación por

$$a \times 0 = 0;$$
$$a \times b^+ = a \times b + a$$
$$a \times {}'b = a \times b + (-a).$$

Ejercicios

Demuestre las propiedades asociativa, conmutativa, existencia de elemento idéntico de la suma y la multiplicación de números enteros usando la axiomática de Padoa.

7.1.4. La axiomática de Le Veque

Otro sistema axiomático para los números enteros, presentado por Le Veque[19] es el siguiente:

I. Cada pareja de enteros a y b tiene una suma única $a+b$ y un producto único $a \cdot b$ o ab, de tal manera que se cumplen las siguientes leyes:

   Ley asociativa: $a + (b + c) = (a + b) + c$ $\quad a(bc) = (ab)c$

   Ley conmutativa: $a + b = b + a$ $\quad ab = ba$

   Ley distributiva: $a(b + c) = ab + ac$.

II. Los enteros distintos 0 y 1 tienen las propiedades: $a+0 = a$ y $1 \cdot a = a$ para todo número entero a.

III. Para cada entero a, la ecuación $a + x = 0$ tiene una solución única x, llamada $-a$.

IV. Si $c \neq 0$ y $ca = cb$, entonces $a = b$.

V. Existe un subconjunto de enteros, llamados enteros positivos, con las siguientes propiedades: la suma y el producto de enteros positivos son positivos y, cualquier entero a diferente de cero tiene la propiedad de que solamente uno de los dos números a o $-a$ es positivo.

   Definición: se dice que a es menor que b y se escribe $a < b$ si $b - a$ es un entero positivo y se escribe $a \leq b$ si $a < b$ o $a = b$.

VI. Todo conjunto de enteros positivos que contenga al menos un elemento, contiene un elemento mínimo. Es decir, existe un entero a en el conjunto tal que $a \leq b$ para todo elemento b en el conjunto.

Ejercicio

Demuestre que entre 0 y 1 no hay números enteros usando la axiomática de Le Veque.

[19]LE VEQUE, William. Teoría elemental de los números. México: Herrero Hermanos, Sucesores, 1968. p. 10 - 12.

7.2. Equivalencia entre los sistemas axiomáticos de Padoa y de Le Veque

7.2.1. Los axiomas de Le Veque implican los de Padoa

Primero definimos para cada entero a su sucesor a^+ como $a+1$, por el axioma I de Le Veque se garantiza la unicidad. Con esto demostramos el axioma 1 de Padoa.

El elemento simétrico $(-a)$ de a que se asegura en el axioma 2, puede definirse por el axioma III, como el elemento x solución de la ecuación $a+x=0$, con lo que queda demostrado el axioma 2.

Para demostrar el axioma 3 partamos de la igualdad $a+(-a)=0$, del axioma III, la cual es equivalente a $(-a)+a=0$, por la conmutatividad de la suma en Z (axioma I), y nuevamente por el axioma III tenemos que $a=-(-a))$, que era lo deseado.

Para demostrar el axioma 4 partimos de

$$(-(a+1))+(a+1)=0$$

según los axiomas III y I.

Por el axioma I,

$$(-(a+1))+(1+a)=0$$

entonces

$$(-(a+1)+(1+a))+(-a)=0+(-a).$$

Así, de acuerdo con los axiomas I, II y III,

$$-(a+1)+1=(-a).$$

Ahora, por el axioma II, $0+0=0$ y por el axioma III tenemos que $-0=0$, esto demuestra el axioma 5 de Padoa; la existencia del 0 la demuestra el axioma II.

Para demostrar el axioma 6 de Padoa, suponemos que $a\neq 0$ y $a=-a$ entonces a y $-a$ son ambos positivos o ambos negativos lo que contradice el axioma V, luego $a\neq(-a)$.

Ejercicio

Demuestre el axioma 7 de Padoa dentro de la axiomática de Le Veque.

7.2.2. Los axiomas de Padoa implican los de Le Veque

Para demostrar el axioma I de Le Veque, observemos que las definiciones de suma y de producto presentadas en la axiomática de Padoa, garantizan que para cada par de elementos a y b de Z, existe un valor $a+b$ y $a\times\ b$ de Z que representan su suma y producto respectivamente; además, por el axioma 1, estos valores son únicos.

Debemos demostrar ahora, que la suma y multiplicación de enteros es asociativa y conmutativa, y que se tiene la distributividad de la multiplicación con respecto a la suma:

Asociatividad de la suma: Para todo $x, y, z \in Z$, se cumple $(x+y)+z = x+(y+z)$.

Fijemos x y y, y denotemos por A al conjunto de todos los z para los cuales la afirmación es cierta,

$$\mathrm{A} = \{z \in \mathrm{Z} : (x+y)+z = x+(y+z)\}$$

Tenemos que $\mathrm{A} \neq \emptyset$, ya que por la definición de suma, $0 \in \mathrm{A}$; además:

i. Si suponemos que $a \in \mathrm{A}$, entonces $(x+y)+a = x+(y+a)$ y teniendo en cuenta la defínción de suma

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

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

pero como

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

concluimos que

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

es decir $a^+ \in \mathrm{A}$.

ii. Si $a \in \mathrm{A}$ y $a = b^+$, entonces por hipótesis se cumple que

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

Como

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

y

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

entonces

$$((x+y)+b)^+ = (x+(y+b))^+$$

y como $x^+ = y^+$ implica que $x = y$, tenemos que $(x+y)+b = x+(y+b)$, es decir $b \in$A.

Finalmente, por el axioma 7, concluimos que A = Z, lo que significa que para todo entero z, se tiene que $(x+y)+z = x+(y+z)$.

Ejercicio

Dentro de la axiomática de Padoa demuestre que para todo x, y en Z

$$x^+ = y^+ \quad \textit{implica que} \quad x = y.$$

Antes de demostrar la conmutatividad de la suma, vamos a demostrar que para todo a en Z, se cumple que $a+1 = 1+a$, donde $1 = 0^+$:

Sea A $= \{z \in \text{Z} : z+1 = 1+z\}$, A no es vacío, ya que $0 \in$ A, pues

$$0+1 = 0+0^+ = (0+0)^+ = 0^+ = 1 = 1+0.$$

i. Si $a \in$ A, entonces $a+1 = 1+a$, luego

$$1+a^+ = (1+a)^+ = (a+1)^+ = a+1^+$$

Pero como para todo x en Z, $x^+ = x+1$, $a+1^+ = a+(1+1)$, de donde por la asociatividad de la suma tenemos que $a+(1+1) = (a+1)+1 = a^+ + 1$. Por tanto $1+a^+ = a^+ + 1$, con lo que demostramos que $a^+ \in$ A.

ii. Si $a \in$ A y $a = b^+$, entonces

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

y como

$$(1+b)^+ = 1+a = a+1 = b^+ + 1 = (b^+)^+,$$

concluimos que

$$1+b = b^+ = b+1,$$

es decir $b \in$ A.

Por el axioma 7, concluimos que A = Z, lo que significa que para todo entero a, $a + 1 = 1 + a$, o en otras palabras que $a + 1 = a^+ = 1 + a$.

Conmutatividad de la suma: para todo $x, y \in$ Z, se cumple $x+y = y+x$.

Fijemos y, y sea H $= \{x \in \text{Z} : x + y = y + x\}$. H no es vacío, ya que $0 \in$ H.

i. Si $x \in$ H, entonces $x + y = y + x$, luego

$$y + x^+ = (y + x)^+ = (x + y)^+ = x + y^+,$$

como para todo entero a, se cumple que $a + 1 = a^+ = 1 + a$, tenemos que

$$x + y^+ = x + (1 + y),$$

y por la asociatividad de la suma,

$$x + (1 + y) = (x + 1) + y = x^+ + y,$$

con lo que demostramos que

$$y + x^+ = x^+ + y,$$

es decir $x^+ \in$ H.

ii. Dado $x \in$ H y $x = z^+$, entonces por hipótesis se cumple que

$$x + y = y + x$$

pero como

$$y + x = y + z^+ = (y + z)^+$$

y

$$x + y = z^+ + y = z + y^+ = (z + y)^+,$$

tenemos que

$$(y + z)^+ = (z + y)^+$$

por lo tanto

$$y + z = z + y,$$

lo que significa que $z \in$ H.

Por el axioma 7, H = Z, es decir que para todo x en Z, $x + y = y + x$.

Ejercicios

1. *Demuestre las propiedades asociativa y conmutativa de la multiplicación.*

2. *Demuestre la propiedad distributiva de la multiplicación con respecto a la suma.*

Para demostrar que 0 y 1 son distintos usamos que $x^+ \neq x$ para todo x en Z. $a + 0 = a$ lo garantiza la definición de suma; demostraremos que para todo a en Z, $1 \cdot a = a$:

Sea $\mathrm{H} = \{x \in \mathrm{Z} : 1 \cdot x = x\}$. H no es vacío, ya que $0 \in \mathrm{H}$, pues por la definición de multiplicación $1 \cdot 0 = 0$.

i. Si $a \in \mathrm{H}$, entonces $1 \cdot a = a$ y $1 \cdot a = a \cdot 1$ por la ley conmutativa de la multiplicación, luego

$$1 \cdot a^+ = 1 \cdot a + 1 = a + 1 = a^+$$

Lo que significa que $a^+ \in H$.

ii. Dado $a \in \mathrm{H}$ y $a = b^+$, entonces por hipótesis se cumple que $1 \cdot a = a$,

$$b^+ = 1\ b^+ = 1 \cdot b + 1 = (1 \cdot b)^+$$

luego $1 \cdot b = b$, es decir, $b \in \mathrm{H}$.

Por el axioma 7, $\mathrm{H} = \mathrm{Z}$. De acuerdo a lo anterior, podemos concluir que el axioma II se cumple.

Para demostrar el axioma III, usamos el esquema presentado en los casos anteriores:

Sea $\mathrm{A} = \{z \in \mathrm{Z} : z + (-z) = 0\}$, A no es vacío ya que $0 \in \mathrm{A}$, pues por el axioma 5 y la definición de suma,

$$0 + (-0) = 0 + 0 = 0.$$

i. Si $a \in \mathrm{A}$, entonces $a + (-a) = 0$, por el axioma 4 tenemos que $(-a) = -(a^+) + 1$, luego

$$\begin{aligned} a + (-a) &= a + (-(a^+) + 1) \\ &= a + (1 + (-(a^+))) \\ &= a^+ + (-(a^+)) \end{aligned}$$

por tanto $a^+ + (-(a^+)) = 0$, con lo que demostramos que $a^+ \in \mathrm{A}$.

ii. Si $a \in \mathrm{A}$ y $a = b^+$, entonces

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

y como $b^+ + (-(b^+)) = b + (-b)$, tenemos que $b \in \mathrm{A}$. Y por el axioma 7, $\mathrm{A} = \mathrm{Z}$.

Hemos demostrado que para cada a en Z, la ecuación $a + x = 0$ tiene solución y es $x = (-a)$.

Ejercicio

Demuestre que la solución de la ecuación $a + x = 0$ es única.

Dado el conjunto

$$\mathrm{Z}^+ = \{0^+, (0^+)^+, ((0^+)^+)^+, \ldots\},$$

si a y b son elementos de Z^+, también lo serán $a+b$ y $a \times b$ por la definición de la suma y el producto en la axiomática de Padoa. Con esto definimos una relación de orden "$\leq$", así:

$$a \leq b \quad \text{si y solo si} \quad b + (-a) \in \mathrm{Z}^+ \ \text{ o } \ a = b.$$

Si $b + (-a) \in \mathrm{Z}^+$, escribimos $a < b$. Si $a \neq 0$, entonces $a \in \mathrm{Z}^+$, o $(-a) \in \mathrm{Z}^+$, pero no ambos, pues si así fuera $a + (-a) = 0 \in \mathrm{Z}^+$, lo que es una contradicción. Con esto demostramos el axioma V de Le Veque.

Ejercicios

1. *Demuestre que "$\leq$"es una relación de orden.*
2. *Demuestre que si $a \neq b$, entonces o bien $a > b$ o bien $b > a$.*

Para demostrar el axioma IV de Le Veque, partimos de $ca = cb$ con $c \neq 0$ y suponemos que $a \neq b$, luego tenemos que o $b > a$ o $a > b$.

Si $b > a$, entonces $h = b + (-a) \in \mathrm{Z}^+$, de manera que $a + h = b$. Como $ca = cb$, tenemos que

$$ca = c(a + h) = ca + ch$$

y si sumamos $(-ca)$ en ambos lados de la igualdad, obtenemos que $0 = ch$ y como $c \neq 0$, $h = 0$, lo cual contradice nuestra hipótesis de que $b > a$. De

manera análoga, obtenemos una contradicción si suponemos que $a > b$. Por lo tanto $a = b$.

Ejercicios

1. *En la demostración anterior concluimos que* $h = 0$*, cuando* $0 = ch$ *y* $c \neq 0$*. Demuestre este hecho.*

2. *Demuestre el axioma VI de Le Veque, con base en los axiomas de Padoa.*

3. *Busque otras axiomatizaciones para los números enteros.*

4. *Busque otras representaciones para los números enteros.*

7.3. Los números racionales

En *Actividades matemáticas para el desarrollo de procesos lógicos: Clasificar, medir e invertir*[20] se muestran varias representaciones de los números racionales: como números $n-$ males, como fracciones continuas simples finitas, y como familias de parejas de números naturales, representaciones que son resultado de un desarrollo histórico y cultural, como veremos en los siguientes apartados.[21]

Los inicios del concepto de número racional corresponden al uso de la noción de fracción[22], desde diferentes interpretaciones y contextos determinados por las necesidades de cada civilización o época. Su formalización se debió al interés por fundamentar teóricamente los números reales.

7.3.1. Sistemas de representación de fracciones en algunas culturas

Las fracciones surgieron relativamente tarde, en relación con los números naturales, ya que las culturas primitivas evitaron el uso de este tipo de números al crear unidades más pequeñas, por lo menos, en relación con las

[20]LUQUE, MORA y TORRES, Op. cit., 2005, p. 60-136.

[21]Narrados en la misma secuencia histórica que en libro MORA, Lyda y TORRES Johana. Concepciones de estudiantes de Licenciatura en Matemáticas sobre números reales. Bogotá: Universidad Pedagógica Nacional, 2007. p. 73 - 80.

[22]Del latín *fractío - ôni* que significa romper, quebrar.

medidas que realizaban; por ejemplo los romanos establecieron un sistema de medidas con submúltiplos para no utilizar los números fraccionarios[23].

Uno de los primeros indicios del uso de fracciones se corresponde con una interpretación de estas como parte-todo, y aparece en las tablillas babilónicas, donde se evidencia una extensión de su sistema de numeración para los números naturales a las fracciones sexagesimales. Allí por ejemplo, bajo su principio de notación posicional, que presenta algunas ambigüedades por la falta de un símbolo para la posición vacía, representaron la fracción sexagesimal[24] $\frac{61}{30}$ (es decir, $2 + 2 \cdot 60^{-1}$) como $\curlyvee \curlyvee \curlyvee\curlyvee$ o la fracción[25] $171\frac{1}{2}$ como se muestra a continuación:

 $= 2 \cdot (60) + 5 \cdot 10 + 1\frac{1}{2} = 171\frac{1}{2}$

Para los Babilonios las fracciones $\frac{1}{2}$, $\frac{1}{3}$ y $\frac{2}{3}$ que eran consideradas como totalidades (unidades) y no como partes de la unidad[26], tenían una representación diferente a las demás, así usaban el símbolo  para $\frac{1}{2}$,  para $\frac{1}{3}$ y para $\frac{2}{3}$.

Con respecto a las operaciones entre fracciones, aparecen varias tablas con problemas de álgebra que las involucraban. Por ejemplo, el primer problema de la tablilla 4652 de YBC[27], enuncia: *Yo encontré una piedra. No la pesé. Un séptimo agregué. Un undécimo que agregué. Yo lo pesé. 1 maná. ¿Cuál fue el peso original de la piedra? El peso de la piedra era* $\frac{2}{3}$ *maná 8 gin* $22\frac{1}{2}$*še*[28].

Algunos autores como Kline[29] señalan que los babilonios desarrollaron tablas que contenían representaciones sexagesimales finitas de los inversos multiplicativos de los números naturales de la forma $2^a 3^b 5^c$ y aproximaciones a fracciones como $\frac{1}{7}$, $\frac{1}{11}$ y $\frac{1}{13}$, ..., que eran utilizadas de forma sistemática para realizar divisiones entre números naturales.

[23]La unidad principal era el *as*, $\frac{1}{12}$ del *as* era llamado *uncia* cuyo símbolo era $-$, $\frac{2}{12}$, era *sextans*, representado por $=$; entre otros. (SMITH, Op. cit., p. 208).

[24]BOYER, Carl. Historia de la Matemática. Madrid: Alianza Universidad, 1987. p. 51.

[25]SMITH, Op. cit., p. 38.

[26]KLINE, Op. cit., p. 22

[27]Yale Babylonian Collection

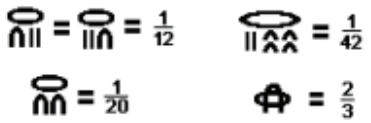
[28]MELVILLE, Duncan. An Old Babylonian Problem Text. En: Mesopotamiam Mathematics [En linea]. (2002). [consultado 10 enero 2007]. Disponible en <http://it.stlawu.edu/ %7Edmelvill/mesomath/tablets/Stones.html>

[29]KLINE, Op. cit., p. 24.

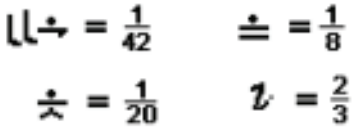
Según autores como Boyer y Smith, una idea cercana a la de fracción apareció por primera vez en Egipto, en las sociedades cazadoras de carácter comunitario y en las de carácter agrícola-comercial, a partir del reparto de piezas de carne, cosechas de grano, campos o tributos; así, la fracción no era vista como un número susceptible de ser generalizado, sino como la expresión de una acción de reparto donde solo eran admisibles las fracciones unitarias (fracciones cuyo numerador es uno) y excepcionalmente, la fracción $\frac{2}{3}$ que aparece como un operador para obtener la equivalencia en *khar* (unidad de medida de la capacidad de grano) de codos cúbicos (1 codo cúbico $= \frac{2}{3}$ khar) y $\frac{3}{4}$ que se usó con carácter descriptivo pero no operativo.

Ejercicio

A partir de las siguientes fracciones egipcias escritas en notación jeroglífica, indique ¿qué significado tiene el ovalo?, ¿cuáles son las reglas de escritura de las fracciones unitarias?



Los egipcios utilizaron otro sistema de numeración, el hierático, en el que un punto reemplazaba al óvalo en el sistema jeroglífico[30]. En este, las fracciones unitarias eran escritas de manera un poco distinta, como podemos ver:



En el *Papiro de Rhind* aparece una tabla en la que se representan las fracciones de numerador 2 y denominador un número impar entre 5 y 101, como sumas de fracciones unitarias de distintas formas, por ejemplo:

[30]El punto fue usado como un símbolo para la fracción aún en la época moderna, tal como se encuentra en copias de libros ingleses del siglo XVIII, en los cuales $\frac{1}{2}$ y $\frac{1}{4}$ se representaban como $\dot{\frac{}{2}}$ y $\dot{\frac{}{4}}$ respectivamente.

$$\begin{aligned}\frac{2}{43} &= \frac{1}{42}+\frac{1}{86}+\frac{1}{129}+\frac{1}{301}\\ &= \frac{1}{24}+\frac{1}{258}+\frac{1}{1032}\\ &= \frac{1}{30}+\frac{1}{86}+\frac{1}{645}\end{aligned}$$

En este papiro, se observa que ellos desarrollaron diversas reglas para expresar fracciones como sumas de fracciones unitarias; sin embargo, no existe una aplicable a todos los casos[31]; y utilizarlas a la hora de realizar las cuatro operaciones aritméticas entre fracciones. Además, aunque no se hace explícita la aparición de propiedades de las operaciones, sí se observa la posibilidad de asociar, para reducir un conjunto de símbolos, y conmutar, por cuanto solían ordenar los números de forma decreciente.

Por ejemplo, en el problema 9 del papiro de Rhind se realiza la multiplicación $\frac{1}{2}+\frac{1}{14}\times 1+\frac{1}{2}+\frac{1}{4}$ de la siguiente manera[32]:

1	1/2 1/14
1/2	1/4 1/28
1/4	1/8 1/56
1 1/2 1/4	1/2 1/4 1/8 1/14 1/28 1/56

El resultado de la operación que aparece en el último renglón de la segunda columna es una suma de 6 fracciones de numerador 1 y denominador creciente que el escriba reduce de la siguiente forma: primero suma la columna $1/14+1/28+1/56$ alcanzando el valor de 1/8, con lo cual la serie se transforma en 1/2 1/4 1/8 1/8; ahora realiza sumas equivalentes para seguir el procedimiento de reducción:

$$\begin{array}{c}1/2\ \ 1/4\ \ 1/8\ \ 1/8\\ 1/2\ \ 1/4\ \ 1/4\\ 1/2\ \ 1/2\\ 1\end{array}$$

de donde concluye que la respuesta a la multiplicación inicial es 1.

[31]Por ejemplo reglas equivalentes a las fórmulas $\frac{2}{bc}=\frac{1}{b\frac{b+c}{2}}+\frac{1}{c\frac{b+c}{2}}$.

[32]La notación 1/2 1/4 corresponde a $\frac{1}{2}+\frac{1}{4}$

Ejercicio

A partir del ejemplo dado describa el proceso utilizado por ellos para multiplicar fracciones y dé otros ejemplos.

En Grecia aparecieron dos interpretaciones de las fracciones; por un lado en el periodo clásico las fracciones representaban razones entre números enteros y no provenían de alguna forma de reparto, en tanto para los alejandrinos las fracciones eran trabajadas como números[33].

Al parecer, los griegos siguieron los métodos egipcios para representarlas; Herón y otros, por ejemplo, descomponían las fracciones comunes en fracciones unitarias y hasta inicios del siglo X esta tradición se mantenía, según lo muestra el Papiro de Akhmin (que data, aproximadamente del siglo VIII) y escritos hebreos de Rabbi Sa´adia ben Joseph al-Fayyumî[34].

El simbolismo utilizado para las fracciones empleaba las letras de su alfabeto; escribían, por ejemplo, $\frac{1}{3}$ como $\overset{ov}{\Gamma}$ o $\overset{II}{\Gamma}$, donde Γ es el símbolo griego[35] para el tres, o $\frac{1}{4}$ como $^{II}\Delta$ y para las fracciones comunes, escribían la fracción a la inversa; es decir, $\frac{4}{19}$ para $\frac{19}{4}$, como lo hacían Herón y Diofanto (275?); otros escritores griegos, como Aristarco (260 a.C.?), escribían la palabra para el numerador y el símbolo del número para el denominador, otros repetían el numeral para el denominador; esto es, para $\frac{2}{5}$, en símbolos modernos, $2'5''5''$; sin embargo, cuando los científicos griegos necesitaban un sistema preciso de aproximación acudían al sistema sexagesimal como lo hacía Ptolomeo.

Nuestra simbología actual para las fracciones es debida a los hindúes, aunque ellos no usaban la raya horizontal; al parecer, fueron los árabes quienes la introdujeron, pero solo se usó de manera general hasta el siglo XVI[36].

El uso de las fracciones en la civilización India, se remonta al siglo V, no se encuentran detalladas las maneras de representar las fracciones, aunque se sabe que las usaban, pues se encuentran en el planteamiento o en las soluciones a problemas de la época en libros como *Kavanagh* y *Lilavati*[37], como se observa en estos ejemplos:

[33]KLINE, Op. cit., p. 184.

[34]SMITH, Op. cit., p. 212.

[35]Los símbolos griegos usados son modernos.

[36]La barra oblicua es el resultado del deseo por simplificar la escritura y las formas impresas, se cuenta que fue De Morgan quien la instituyó en 1845.

[37]Uno de los capítulos de la obra del matemático hindú Bhaskara, que lleva el nombre de su hija.

> "Un tercio de una colección de ninfeas es ofrecida a Mahadev, un quinto a Huri, un sexto al Sol, un cuarto a Devi, y seis que permanecen son representadas al espiritual que enseña. Requerido el número entero de ninfeas.
>
> Un quinto de una colmena de abejas voló a la flor de Kadamba; un tercio voló al Silandhara; tres veces la diferencia de estos dos números voló a un árbol; y una abeja continuó volando atraída por la fragancia del Ketaki y el Malati. ¿Cuál fue el número de las abejas?"

Otro uso de las fracciones se encuentra en el libro de astronomía *Aryabhatiya*, escrito por *Aryabhata* en el año 499. Allí se plantea la manera de solucionar una regla de tres simple: *En la regla de tres, multiplicar el fruto por el deseo y dividir por la medida; el resultado es el fruto del deseo.*

En términos modernos:

$$\frac{a}{b} = \frac{c}{x} \qquad \text{es equivalente a} \qquad x = \frac{b \cdot c}{a}$$

donde a es llamada *la medida*; b es *el fruto*; c es *el deseo*, y x es *el fruto del deseo.*

Un problema del mismo libro es: Si dos y un medio medidas de azafrán cuestan 3/7 de una moneda ¿Cuántas medidas de azafrán se podrán comprar con nueve monedas? *En terminología india: 5/2 es el fruto, 9 es el deseo, 3/7 es la medida; el fruto del deseo será:*

$$\frac{9\dfrac{5}{2}}{\dfrac{3}{7}} = 52\ \frac{1}{2}$$

Aunque no se encuentran registros de las operaciones entre fracciones, autores como Wussing H. señalan que "el conocimiento de las propiedades aritméticas del cero estaba totalmente consolidado en la matemática hindú, así como métodos algorítmicos correctos para el tratamiento de los números negativos, del cálculo de fracciones, de las raíces cuadradas y a modo de empleo la regla de tres"[38]; de hecho, el conocimiento que tuvieron sobre las fracciones llevó hasta considerarlas como exponentes de ciertas bases, interpretando $x^{2/3}$ *como el lado del cubo del cuadrado de una fracción.*

[38] WUSSING, Hans. Lecciones de historia de las matemáticas. Madrid: Siglo XXI, 1998. p. 80

En manuscritos árabes de matemáticos como Al-Khowarizmi, aparecen fracciones (números audibles) en el planteamiento y solución de algunos problemas, pero sin cuestionarse frente al concepto o propiedades de estas, aunque se observa un tratamiento natural sobre las fracciones y sus operaciones, como en los hindúes.

Fibonacci (1180-1250), aunque usaba con propiedad el sistema decimal derivado de los numerales hindú-arábigos, extrañamente escribía las fracciones como sexagesimales y usaba preferencialmente las fracciones unitarias para problemas mercantiles y las sexagesimales para problemas matemáticos teóricos. Esto es evidente en los problemas expuestos en el *Liber Abaci*, donde se hace una explicación de algoritmos aritméticos basados en los procedimientos propuestos por los hindúes y los árabes y se presentan mecanismos para representar la parte fraccionaria como una yuxtaposición de fracciones unitarias, a la manera de los egipcios.

Los chinos, por su parte, también usaron las fracciones sin dificultad desde épocas remotas. El Chou Pei (aprox. 1105 a. C.) contiene problemas que involucran números como $247\frac{933}{1460}$, no escrito simbólicamente, pero sí verbalmente[39], y en *Los nueve capítulos*, se muestran métodos para desarrollar operaciones entre fracciones, similares a los realizados en la actualidad, interpretando la fracción como una acción de reparto asociada a una división inexacta: "Cuando el dividendo tiene un resto, lo nombramos con ayuda del divisor: el divisor se toma como denominador [mu, la madre], el resto del dividendo como numerador [zi, los hijos]", de manera que al realizar una división inexacta el resultado se da en forma de número mixto de la forma

$$\frac{D}{d} = c + \frac{r}{d},$$

donde c es el cociente y r el residuo.

En otros problemas de la misma obra, la fracción se asocia a procesos de medida, aunque conservando la interpretación de parte-todo, como el siguiente: *"Existe un campo de 4/7 de bu de ancho y 3/5 de bu de largo. Encontrar el área. Respuesta: 12/35 de bu"*, para los cuales aparecen reglas de solución como: multiplicar los denominadores para obtener el divisor, multiplicar los numeradores para obtener el dividendo, dividir el dividendo entre el divisor y, en algunos casos, un procedimiento auxiliar para simplificar las fracciones, semejante al algoritmo de Euclides para encontrar el máximo común divisor entre dos números.

[39]SMITH, Op. cit, p. 215

Los chinos fueron los pioneros de las fracciones decimales (siglo XIV a.C.), tal vez, derivadas de su sistema de numeración y del sistema decimal de pesos y medidas que usaban, pues la transformación de monedas y medidas era el contexto más frecuente de aparición de fracciones. En un comentario a *Los nueve capítulos* (segundo milenio a.C. aprox.) realizado en el primer siglo de esta era, hay algunas reglas que son hoy consideradas como precursoras de la invención de las fracciones decimales, estas son[40]:

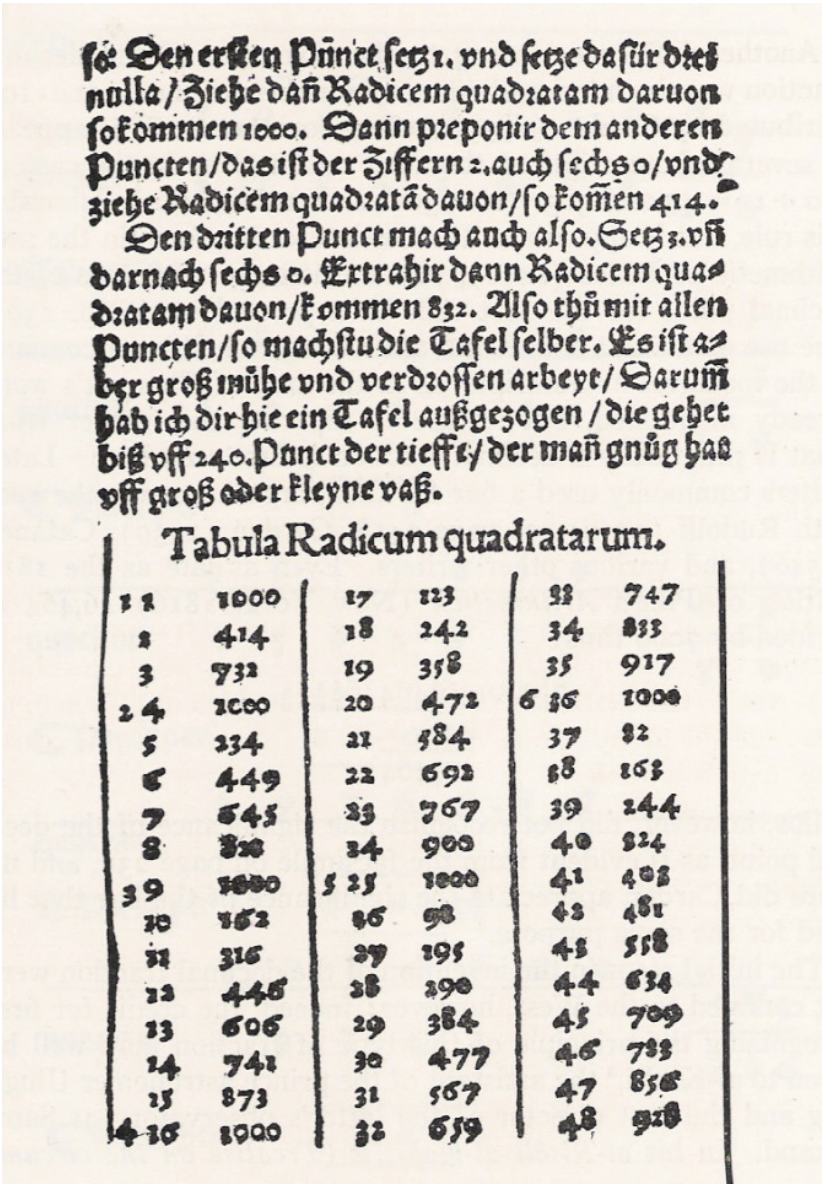
$$\sqrt{a} = \frac{\sqrt{100a}}{10} \quad \text{y} \quad \sqrt[3]{a} = \frac{\sqrt[3]{1000a}}{10}$$

Estas reglas se usaron en el siglo XV y XVI para la extracción de la raíz cuadrada y fueron resumidas posteriormente en una sola: $\sqrt[n]{a} = \frac{\sqrt[n]{a \cdot 10^{kn}}}{10^k}$; la consecuencia más importante de esta regla, en relación con la fracción decimal, es su uso para la elaboración de tablas con muy buenas aproximaciones de algunas raíces cuadradas como puede verse en la tabla de la figura 1 de Adam Riese´s Rechnung auff der Linien und Federn (1522).

La segunda influencia más importante en el desarrollo de la fracción decimal fue la regla para dividir números de la forma $a \cdot 10^n$, atribuido a Regiomontano (1436 -1476), por el matemático italiano Girolamo Cardano (1501-1576) y que en la obra de Chuquet (1484) aparecen algunos ejemplos como $470 \div 10 = 47$ y $503 \div 10 = 50\frac{3}{10}$ y en la de Pellos (1492), quien usa el punto decimal, por primera vez, para separar un entero de la fracción decimal pero sin comprender la naturaleza de los decimales, como se ve en la figura 2.

El uso del punto decimal propuesto por Pellos no tomó trascendencia, pues escritores posteriores a él utilizaban una línea vertical para este propósito, como Rudolff (1530), Cardano (1539), Cataneo (1546), Viète (1579), entre otros; el primero de estos, Christoph Rudolff (1500-1545?), trabajó sistemáticamente con fracciones decimales y sus operaciones pero no escribió teoría sobre ellas (véase figura 3), y es debido a esto que algunos historiadores como Klein y Smith, consideran que este hombre es el inventor de las fracciones decimales ya que su obra Coss (1525) es una de las primeras impresiones donde aparecen las fracciones decimales.

[40]BOYER, Op. cit., p. 264.



ſe: Den erſten Punct ſetz 1. vnd ſetze dafür drey nulla / Ziehe dañ Radicem quadratam daruon ſo kommen 1000. Dann preponir dem anderen Puncten / das iſt der Ziffern 2. auch ſechs 0 / vnd ziehe Radicem quadratã dauon / ſo komẽ 414.

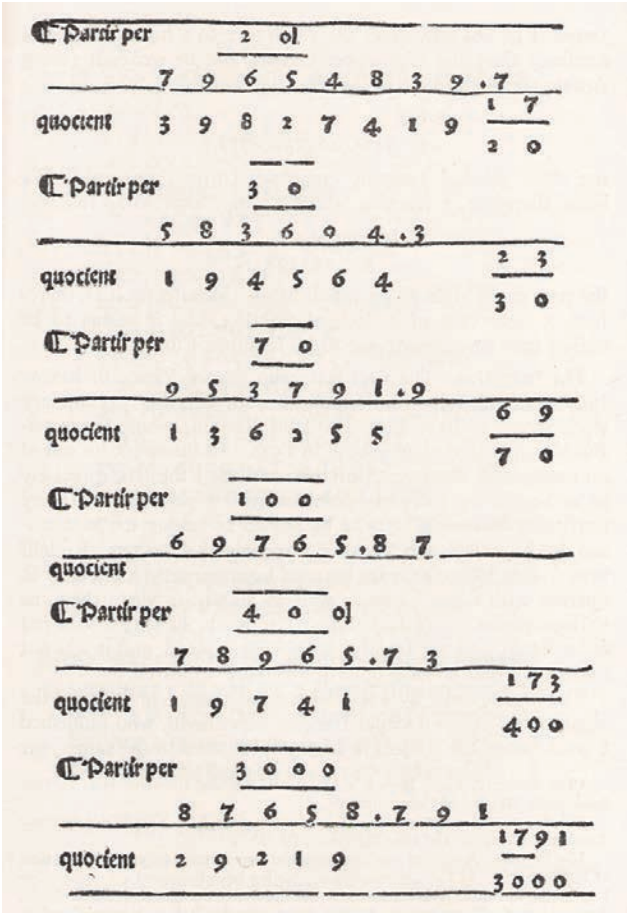
Den dritten Punct mach auch alſo. Setz 3. vñ darnach ſechs 0. Extrahir dann Radicem quadratam dauon / kommen 832. Alſo thũ mit allen Puncten / ſo machſtu die Tafel ſelber. Es iſt aber groß mühe vnd verdroſſen arbeyt / Darumb hab ich dir hie ein Tafel außgezogen / die gehet biß vff 240. Punct der tieffe / der mañ gnůg hat vff groß oder kleyne vaß.

Tabula Radicum quadratarum.

1	1	1000	17	123	33	747	
	2	414	18	242	34	833	
	3	732	19	358	35	917	
2	4	1000	20	472	6	36	1000
	5	234	21	584	37	82	
	6	449	22	692	38	163	
	7	645	23	767	39	244	
	8	828	24	900	40	324	
3	9	1000	5	25	1000	41	403
	10	162	26	98	42	481	
	11	316	27	195	43	558	
	12	446	28	290	44	634	
	13	606	29	384	45	709	
	14	741	30	477	46	783	
	15	873	31	567	47	856	
4	16	1000	32	659	48	928	

Tomada de SMITH, Op. cit. p. 237

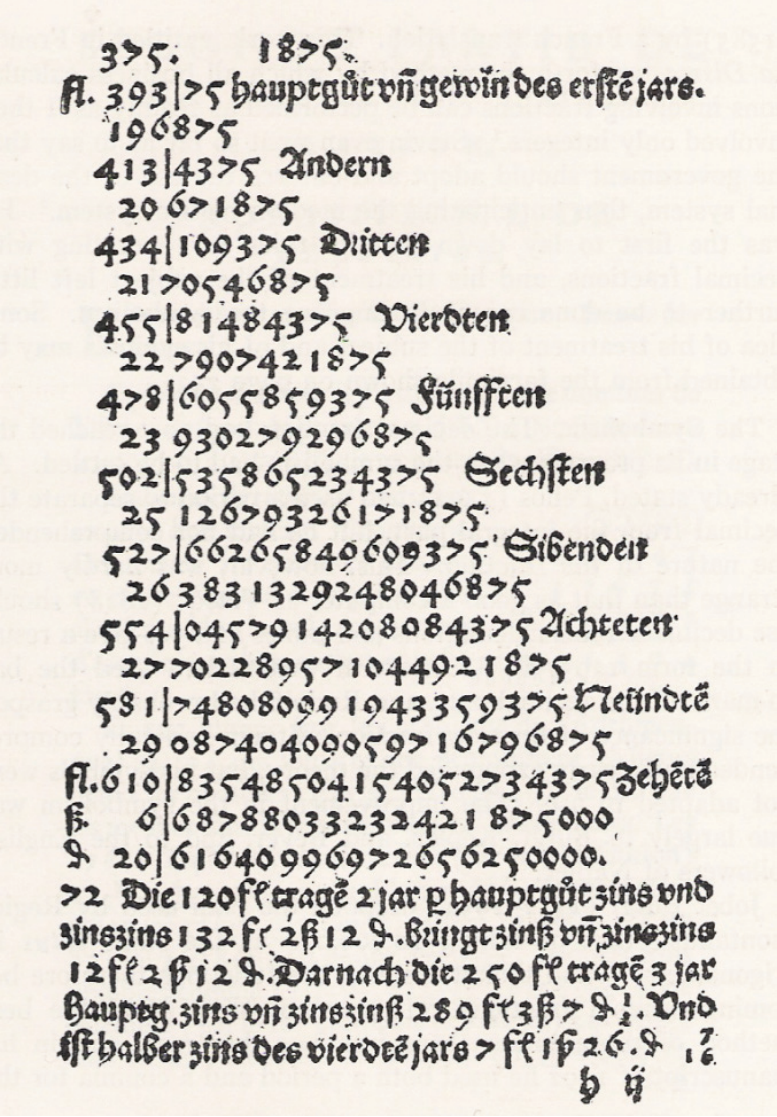
Figura 1



Tomada de SMITH, Op. cit. p. 239
Figura 2

Viète fue uno de los más prominentes defensores del uso de las fracciones decimales en vez de las sexagesimales como lo manifiesta en su obra *Canon-mathematicus* (1579): "Los sexagesimales y los sesentas han de ser usados raramente o nunca en la matemática, mientras que los milésimos y los miles, los centésimos y los cientos, los décimos y los dieces, y las progresiones semejantes, ascendentes y descendentes, deben usarse frecuentemente y aún exclusivamente"[41] y utilizó tanto números en negrita como barras horizontales y verticales para notar las fracciones decimales; por ejemplo, escribía 314.159. $\frac{26536}{100000}$ o **314.159**.265.36 o **99.946**|458.75.

[41]Ibid., p. 386.



Tomada de SMITH, Op. cit. p. 241
Figura 3

No obstante, en Oriente se usaba, un poco antes de Pellos, la fracción decimal. Al-Kashi (aprox. 1436) se auto consideró el inventor de las fracciones decimales ya que, aunque utilizaba principalmente fracciones sexagesimales, atribuía a las decimales la misma exactitud que las primeras y las usó para dar un valor de π, así:

Sah−hah

3 1415926535898732

lo cual, en nuestros símbolos actuales corresponde a 3,1415926535898732; que como puede verse es una muy buena aproximación de este número irracional.

Lo que si es conocido por muchos es que hasta 1585 aparece un libro que contiene por primera vez toda la teoría sobre las fracciones decimales y este es *De Thiende*, titulado así en flamenco, pero más célebre como *La Disme* y escrito por Simon Stevin de Brujas (1548-1620), quien obviamente, no fue el inventor de los números decimales ni mucho menos el que desarrolló un mejor simbolismo para estos, pero sí quizás quien los comprendió totalmente.

Su reconocimiento es debido a que, por una parte, mediante su cuadernillo, explica de manera sencilla cómo usar la notación decimal y su operatividad sin recurrir a los fraccionarios, y lo hace accesible a cualquier comerciante de la época, que era lo que pretendía Stevin, difundir los decimales entre las personas corrientes para que fuesen utilizados en la ejecución de problemas prácticos de manera similar a como manejaban los números naturales, en palabras de Kline

Stevin "(. . .) pone su experiencia en la práctica comercial, financiera e ingenieril al servicio de sus preocupaciones "teóricas"e inversamente, su "teoría"se pone en marcha dentro de su "actividad práctica"[42].

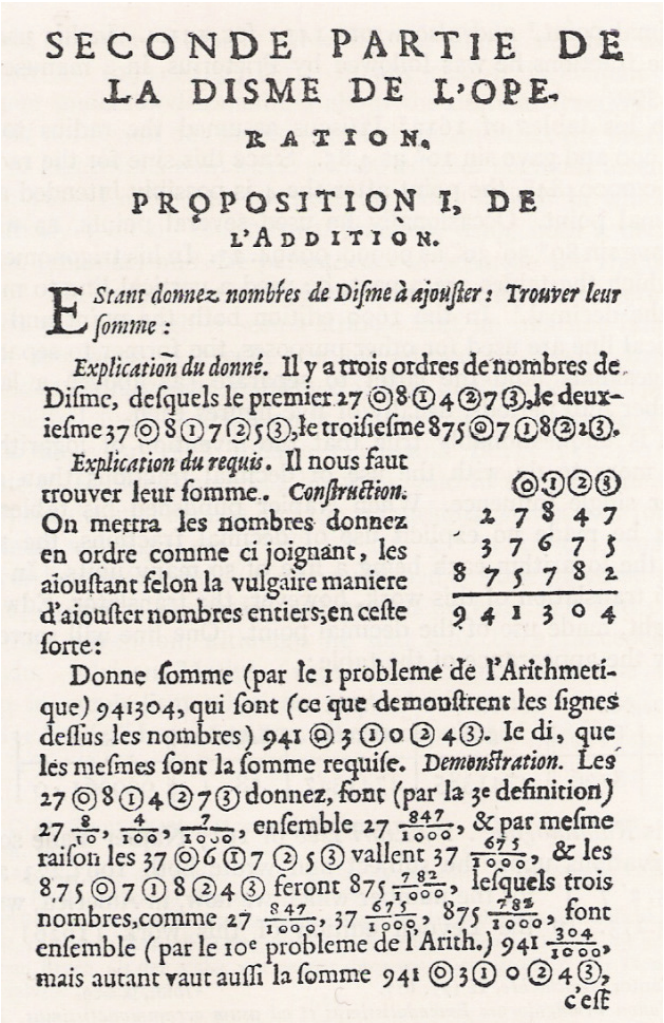
Y por otra, Stevin contribuyó a un cambio en la concepción de la matemática, más específicamente en la concepción de número, identificando en un solo concepto las magnitudes continuas y las cantidades discretas.

Como se señaló anteriormente, el simbolismo usado por Stevin para los decimales fue tan pobre como elemental; para representar las posiciones de cada número, escribía al lado o sobre cada numeral la potencia que 10 debía llevar en el denominador si fuese representado como fraccionario; así, Stevin notaba, por ejemplo, 27,847 de la siguiente manera

⓪	①	②	③
27	8	4	7

o 2 7 ⓪ 8 ① 4 ② 7 ③, como puede observarse en la figura 4.

[42]KLINE, Jacob. Greek Mathematical Thought and the Origin of Algebra. New York: Dover Publications, 1968. p. 186



SECONDE PARTIE DE LA DISME DE L'OPERATION.

PROPOSITION I. DE L'ADDITION.

Estant donnez nombres de Disme à ajouster : Trouver leur somme :

Explication du donné. Il y a trois ordres de nombres de Disme, desquels le premier 27 ⓪8①4②7③, le deuxieſme 37 ⓪8①7②5③, le troiſieſme 875 ⓪7①8②2③.

Explication du requis. Il nous faut trouver leur ſomme. *Conſtruction.* On mettra les nombres donnez en ordre comme ci joignant, les aiouſtant ſelon la vulgaire maniere d'aiouſter nombres entiers, en ceſte ſorte:

⓪	①	②	③
	2	7	8 4 7
	3	7	6 7 5
8	7	5	7 8 2
9	4	1	3 0 4

Donne ſomme (par le 1 probleme de l'Arithmetique) 941304, qui ſont (ce que demonſtrent les ſignes deſſus les nombres) 941 ⓪3①0②4③. Ie di, que les meſmes ſont la ſomme requiſe. *Demonſtration.* Les 27 ⓪8①4②7③ donnez, ſont (par la 3e definition) $27\ \frac{8}{10}, \frac{4}{100}, \frac{7}{1000}$, enſemble $27\ \frac{847}{1000}$, & par meſme raiſon les 37 ⓪6①7②5③ vallent $37\ \frac{675}{1000}$, & les 875 ⓪7①8②4③ feront $875\ \frac{782}{1000}$, leſquels trois nombres, comme $27\ \frac{847}{1000}$, $37\ \frac{675}{1000}$, $875\ \frac{782}{1000}$, ſont enſemble (par le 10e probleme de l'Arith.) $941\ \frac{304}{1000}$, mais autant vaut auſſi la ſomme 941 ⓪3①0②4③, c'eſt

Tomada de SMITH, Op. cit. p. 243
Figura 4

Como es de suponerse, este simbolismo no fue utilizado por mucho tiempo; el mejoramiento en la notación decimal fue debido a matemáticos posteriores como Jobst Bürgi[43] (1552-1632), G. A. Magini (1555-1617), Christoph Clavius[44] (1537-1612) y Johann Hartman Beyer[45] (1563-1625).

[43] A quien Kepler, en su obra de 1616 atribuyó la fracción decimal.

[44] El uso del punto decimal se le atribuye a Magini o a Clavius, ambos amigos de Kepler (BOYER, Op. cit., p. 386).

[45] Beyer, en una carta a Kepler escribió 314, $1'5''9'''2''''6'''''5'''''''$ para 314.15926 (SMITH, Op. cit., p. 245).

Pero John Napier (1550-1617), fue quien popularizó el uso del punto decimal en sus tablas de logaritmos; aunque él inicialmente no lo usó, en la edición de su obra, hecha en 1616 por Edward Wright, aparecen los números decimales tal como los escribimos en la actualidad. Además en la obra *Rhabdologiae* de 1617, Napier hace referencia a los decimales de Stevin y propone usar punto o coma para indicar separación entre la parte entera y la decimal; sin embargo, en escritos posteriores se encuentra multitud de representaciones para los números decimales[46] y aún, en nuestros días no hay acuerdo entre el punto decimal, la coma o superíndices subrayados para la escritura de números decimales.

7.3.2. Caracterizaciones de los números racionales

Hemos presentado algunas formas de representar fracciones y números decimales o sexagesimales, pero ellos no representan la estructura de los números racionales. Esta estructura debe estar caracterizada por un conjunto de axiomas o por una construcción basada en otra estructura axiomatizada como la de los números enteros.

No presentaremos axiomáticas que definan formalmente a los números racionales, sino dos caracterizaciones de estos formuladas por Weierstrass y Dedekind donde muestran algunos componentes fundamentales de su estructura, veamos:

7.3.2.1. La propuesta de Weierstrass

Weierstrass caracteriza los números racionales positivos con base en la idea de partes exactas de la unidad y en la de una relación de equivalencia, así:

1. $1/n$ es la n-ésima parte exacta de la unidad si y solo si $n(1/n) = 1$.

2. Un número racional es una combinación lineal de partes de la unidad con coeficientes enteros.

3. Define igualdad entre racionales usando las siguientes transformaciones: n elementos de la forma $1/n$ pueden ser reemplazados por la unidad y todo número racional puede ser reemplazado por sus partes exactas.

[46] SMITH, Op. cit., p. 246.

4. Un número racional será representado por un agregado entendido como una lista de fracciones positivas cuya suma es el número representado. Así por ejemplo 4/3 puede ser representado por

   $a = \{1/3, 1/3, 1/3, 1/3\}$ o
   $b = \{1/6, 1/6, 1/6, 1/6, 1/6, 1/6, 1/6, 1/6\}$[47]

En esta caracterización, podemos observar la influencia que tuvo el tratamiento egipcio de las fracciones sobre la idea de número racional planteada por Weierstrass, pues él extiende la idea de representar fracciones como combinaciones lineales de fracciones unitarias (partes exactas de la unidad), para definir un número racional como una de tales combinaciones. Ahí, al parecer, Weierstrass implícitamente da por sentadas las operaciones de suma entre racionales y de producto entre un número natural y uno racional, sin embargo, no se incluye explícitamente alguna propiedad que estas operaciones deban cumplir.

Por otro lado, Weierstrass con la idea intuitiva de componer una unidad con n partes n-ésimas exactas de esta, además de definir una relación de igualdad entre los racionales, presenta una noción incipiente de inversos multiplicativos.

Finalmente, notemos que las características 3 y 4, muestran que existen diferentes formas de representar a un mismo número racional, dependiendo de las partes exactas de la unidad que se incluyan en el conjunto; con ello, podemos observar que un número racional puede concebirse como una familia de agregados, y que existe una relación de equivalencia entre agregados que permite definir tal familia. No obstante, aunque hay noción de igualdad entre racionales, no la hay para el orden.

7.3.2.2. La propuesta de Dedekind

Dedekind, por su parte, supone elaborada la aritmética de los números racionales y señala que forman un cuerpo de números con unas propiedades relacionadas con el orden. Esto lo resume en las siguientes propiedades:

1. Las cuatro operaciones fundamentales están definidas para todo par de números racionales con excepción de la división por cero.

2. Dados dos números racionales cualesquiera está definido un orden entre ellos, de manera que el sistema constituye un dominio unidi-

[47] SÁNCHEZ, Clara. La construcción de los números reales. En : XIV Coloquio Distrital de Matemáticas y Estadística (1997). p. 8.

mensional bien ordenado, infinito en dos direcciones opuestas. Esto se traduce en que

"Si a y b representan un mismo número racional, se pondrá tanto $a = b$ y $b = a$. Que dos números racionales sean diferentes se muestra en que la diferencia $a - b$ tiene un valor positivo o negativo. En el primer caso, se dice que a es mayor que b y b menor que a, lo que se indicará a través de los signos $a > b$ y $b < a$, en el segundo caso $b > a$ y $a < b$. Respecto a esta doble posibilidad de ser diferente, se valen las siguientes leyes:

i. Si $a > b$ y $b > c$, entonces $a > c$. Siempre que a, c sean dos números distintos y que b sea mayor que uno de ellos y menor que el otro, queremos expresarlo, sin temor a la reminiscencia de representaciones geométricas, diciendo: b está entre los números a y c.

ii. Si a y c son números distintos, existen siempre infinitos números b que están entre a y c.

iii. Si a es un número determinado, todos los números[48] del sistema $\mathbf{R}$ se descomponen en dos clases, A_1 y A_2, cada una de las cuales contiene infinitos individuos; la primera clase A_1 abarca todos los números a_1 que son menores que a, la segunda clase A_2 abarca todos los números a_2 que son mayores que a; el número a puede asignarse arbitrariamente a la primera o a la segunda clase, y de acuerdo con ello es o bien el mayor número de la primera clase o el menor de la segunda. En cada caso la división del sistema $\mathbf{R}$ en las dos clases A_1 y A_2 es tal que todo número de la primera clase A_1 es menor que cada número de la segunda clase A_2[49]."

En esta caracterización de los números racionales, Dedekind da por sentadas las cuatro operaciones fundamentales de la aritmética, y no expone las propiedades que estas deben cumplir en el nuevo conjunto, exalta la relación de orden definida para tal conjunto, relacionándola con la propiedad de interestancia de los puntos en una recta, y de manera especial menciona la densidad como una característica relevante.

Según Ferreirós (1998), en su introducción al libro *¿Qué son y para qué sirven los números?*, Dedekind en algunos manuscritos de 1850, construye los números enteros a partir de los números naturales y los números racionales a partir de los números enteros, definiéndolos como clases de

[48]Sistema $\mathbf{R}$ hace referencia al dominio de los números racionales.

[49]DEDEKIND, Richard. ¿Qué son y para qué sirven los números?: y otros escritos sobre los fundamentos de las matemáticas.Madrid: Alianza Editorial, 1998. p. 81 - 82.

equivalencia de pares de números naturales y enteros, respectivamente, y definiendo las operaciones entre estas parejas de números, de manera análoga a la usada por Hamilton para los números complejos; consiguiendo así, que los números racionales formen una estructura de cuerpo. Este desarrollo fue publicado en 1890 con el título *La extensión del concepto de número sobre la base de la serie de los números naturales.*

7.3.3. Representaciones de los números racionales

Construidos los números racionales como clases de equivalencia de parejas de números enteros, o a partir de los números racionales positivos como se presenta en el libro *Actividades matemáticas para el desarrollo de procesos lógicos: Clasificar, medir e invertir*[50], sabemos que forman un campo enumerable, totalmente ordenado y denso. Allí se muestran cuatro representaciones de ellos, a saber:

- Los números n-males: extendimos la idea de número decimal y la forma de definir tanto las relaciones de igualdad y orden como las operaciones de suma y producto, para trabajar números de este tipo en otras bases, y así tener que para cada base n, los números con un número finito de cifras n-males y los periódicos son una representación de los números racionales positivos.

- Las familias de fracciones equivalentes: definimos las fracciones positivas y el 0, como parejas números naturales, las operaciones de suma y producto entre ellas, y a partir de la relación de equivalencia dada por

$$\frac{a}{b} = \frac{c}{d} \quad \text{si y sólo si} \quad ad = cb$$

  interpretamos la colección de las clases o de familias de parejas de números naturales como una representación de los números racionales positivos y si cambiamos los números naturales por enteros obtenemos una representación de todos los racionales.

- Las fracciones continuas simples y finitas: definimos las fracciones continuas finitas y simples como expresiones de la forma

[50]LUQUE, MORA y TORRES, Op. cit., 2005, p. 53 - 113, 129 - 136.

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 \ldots + \cfrac{1}{a_n}}}}}$$

con a_i números naturales, intentamos establecer mecanismos para operar entre ellas y demostramos que toda fracción continua simple y finita representa un racional y que todo racional puede ser representado por medio de una de tales fracciones.

- Las familias de parejas de números naturales: elaboramos una construcción oficial de los números racionales, con base en parejas ordenadas de números naturales y en la relación de equivalencia dada por

$$(a, b) \approx (c, d) \quad \text{si y sólo si} \quad ad = cb.$$

Concluimos que un número racional es una clase o familia de tales parejas equivalentes, definiendo las operaciones de suma y producto, las relaciones de igualdad y orden, comprobando las propiedades algebraicas y de orden que caracterizan a esta estructura.

Ahora bien, todas estas representaciones de los números racionales positivos podemos extenderlas para construir representaciones de los números racionales, permitiéndonos así determinar la estructura en común.

7.4. Los números algebraicos

El otro conjunto enumerable que enunciamos en el capítulo anterior es el de los números algebraicos, ellos son una generalización de los números racionales, definidos como la soluciones de alguna ecuación polinómica con coeficientes racionales.

La suma y el producto de números algebraicos es algebraico y aún más, forman un campo[51] totalmente ordenado[52]. No conocemos una axiomatización para los números algebraicos.

[51] Una demostración de esta afirmación se encuentra en: NIVEN, Ivan y ZUCKERMAN, Herbert. Introducción a la teoría de los números. México: Limusa, 1976. p. 191 - 193.

[52] Un tratamiento detallado sobre números algebraicos se encuentra en: POLLARD, Harry. The theory of algebraic numbers. New Jersey: John Wiley and Sons, 1965. p. 44-56.

Con lo que hemos desarrollado hasta aquí podríamos esperar que todos los conjuntos de números fueran finitos o enumerables pero en esto no es así, en el libro: LUQUE, Carlos., MORA, Lyda y TORRES, Johana. *Actividades matemáticas para el desarrollo de procesos lógicos: representar estructuras no enumerables*. Bogotá. Universidad Pedagógica Nacional, 2009., se hace una presentación de estas estructuras.

Bibliografía

[1] AABOE, Asger. Matemáticas: Episodios históricos. Cali: Norma, 1964.

[2] ALBERT, Adrian. Quasigroups I. Trans. Amer. Math. Soc, 1943. v. 54.

[3] ALFONSO, Hernando. Geometría plana y del espacio desde un punto de vista euclidiano. Bogotá: Universidad Pedagógica Nacional, 1997.

[4] BASHMAKOVA, I. G. y SMIRNOVA, G. S. The birth of literal Algebra. En: The American Mathematical Monthly. Vol. 106, No. 1. (1999); p. 57-66.

[5] BEDOYA, Lina. Peano, Lawvere, Peirce: Tres Axiomatizaciones de los Números Naturales. Ibagué, 2003, 54 p. Trabajo de grado (Profesional en matemáticas con énfasis en estadística) Universidad del Tolima. Facultad de Ciencias. Departamento de Matemáticas y Estadística.

[6] BELL, Eric. Historia de las Matemáticas. México: Fondo de Cultura Económica, 2002.

[7] BIRKHOFF, Garrett. Lattice Theory. Providence (Rhode Island): AMS, 1940.

[8] BOL, Gerrit. Gewebe und Gruppen, Math. Ann. 1937. v. 114.

[9] BOYER, Carl. Historia de la Matemática. Madrid: Alianza Universidad, 1987.

[10] _____A history of mathematics. 2 ed. New York: John Wiley & Sons, 1991.

[11] BRAUNSS, Günter & ZUBROD, Heinz. Einführung in die Booleschen Algebren. Frankfurt am Main: Akademische Verlagsgesellschaft, 1974.

[12] BREUER, J. Iniciación a la Teoría de Conjuntos. Madrid: Paraninfo, 1972.

[13] CAICEDO, Xavier. Elementos de lógica y calculabilidad. Bogotá: Una Empresa Docente, Universidad de los Andes, 1990.

[14] CLAWSON, Calvin. Misterios matemáticos. Magia y belleza de los números. México: Diana, 1999.

[15] DEDEKIND, Richard. ¿Qué son y para qué sirven los números?: y otros escritos sobre los fundamentos de las matemáticas.Madrid: Alianza Editorial, 1998.

[16] DERBYSHIRE, John. Unknown Quantity. A real and imaginary history of Algebra. Washington: Joseph Henry Press, 2006.

[17] DEVLIN, Keith. The Joy of sets. New York: Springer, 1993.

[18] DIXON, John. Problems in group theory. New York: Dover, 1973.

[19] DUBREIL, Paul y DUBREIL, Marie Louise. Lecciones de álgebra moderna. México: Reverte, 1965.

[20] EUCLIDES. Elementos. Libros I - XIII. Madrid: Gredos, 1991.

[21] FALK, Mary. Introducción a la matemática contemporánea. Bogotá: Universidad Nacional de Colombia, 1992.

[22] FRALEIGH, John. A first course in abstract Algebra. 6 ed. New York: Addison-Wesley, 1999.

[23] FREGE, Gottlob. Los fundamentos de la Aritmética, México: Universidad Nacional Autónoma de México, 1972.

[24] GALILEI, Galileo. Diálogo sobre dos nuevas ciencias. En: Hawking, Stephen. A Hombros de Gigantes. Barcelona: Crítica ,2003. p. 376.

[25] GOLDBLATT, Robert. Topoi, The categorical análisis of Logic. Amsterdam: North Holland, 1984.

[26] GONZÁLEZ, José., et al. Números enteros. Madrid: Síntesis, 1990.

[27] GRIFFITHS, David. Introduction to Quantum Mechanic. New Yersey: Prentice Hall, 1994.

[28] HERSTEIN, Israel. Álgebra moderna. México: F. Trillas, 1970.

[29] HRBACEK, Karel y JECH, Thomas. Introduction to set theory. 3 ed. New York: Marcel Dekker, 1999.

[30] ILSE, Dieter; LEHMANN, Ingmar & SCHULZ, Wolfgang. Gruppoide und Funktionalgleichungen. Berlín: VEB Deutscher Verlag der Wissenschaften, 1984.

[31] JAMMER, Max. Conceptual development of quantum mechanics. New York: John Willey & Sons, 1974.

[32] JIMÉNEZ, Rafael; GORDILLO, Enrique y RUBIANO, Gustavo. Teoría de Números para Principiantes. Bogotá: Universidad Nacional de Colombia, 1999.

[33] KLEINER, Israel. A history of abstract algebra. Boston: Birkhäuser, 2007.

[34] KLINE, Jacob. Greek Mathematical Thought and the Origin of Algebra. New York: Dover Publications, 1968.

[35] KLINE, Morris. El pensamiento matemático de la antigüedad a nuestros días. Madrid: Alianza Universidad, 1972. v. 1.

[36] _____El pensamiento matemático de la antigüedad a nuestros días. Madrid: Alianza, 1972. v. 2.

[37] _____El pensamiento matemático de la antigüedad a nuestros días. Madrid: Alianza, 1972. v. 3.

[38] KURATOWSKI, Kazimierz. Introducción a la teoría de conjuntos y a la topología. Barcelona: Vinces-Vives, 1966.

[39] LANDAU, Edmun. Foundations of Analisys, The Arithmetic of whole, rational, irrational and complex numbers. New York: Chelsea Publishing Company, 1966.

[40] LAWVERE, William. An Elementary Theory of the Category of Sets. Proc. Nat. Acad. Sci. 52. 1964.

[41] LAWVERE, William y ROSEBRUGH, Robert. Sets for Mathematicians. Cambridge: Cambridge University Press, 2003.

[42] LENTIN, André y RIVAUD, Jacques. Álgebra Moderna. Madrid: Aguilar, 1971.

[43] LE VEQUE, William. Teoría elemental de los números. México: Herrero Hermanos, Sucesores, 1968.

[44] LUKASIEWICZ, Jan. Selected Works. Amsterdam: North Holland Publishing, 1970.

[45] LUNA, Joaquín. El concepto de número natural según Bertrand Russell. En: Memorias XIII Encuentro de Geometría y I de Aritmética. Vol. 1. (jun. 2002); p. 35 - 44.

[46] LUQUE, Carlos; DONADO, Alberto y PAÉZ, Jorge. H-conjuntos (una generalización de la noción de conjunto). XIV Coloquio Distrital de Matemáticas y Estadística. Bogotá: Universidad Pedagógica Nacional, 1997.

[47] LUQUE, Carlos. El concepto de número natural según Giusseppe Peano. En: Memorias XIII Encuentro de Geometría y I de Aritmética. Vol. 1. (jun. 2002); p. 45 - 85.

[48] LUQUE, Carlos y MORA, Lyda. Una aproximación a los números racionales positivos. Bogotá: Universidad Pedagógica Nacional, 2001.

[49] LUQUE, Carlos; MORA, Lyda y PÁEZ, Jorge. Actividades matemáticas para el desarrollo de procesos lógicos: Contar e Inducir. Bogotá: Universidad Pedagógica Nacional, 2002.

[50] LUQUE, Carlos; MORA, Lyda y TORRES, Johana. El proceso matemático de representar. XX Coloquio Distrital de Matemáticas y Estadística. Bogotá: Universidad Pedagógica Nacional, 2004.

[51] _____ Actividades matemáticas para el desarrollo de procesos lógicos: clasificar, medir e invertir. Bogotá: Universidad Pedagógica Nacional, 2005.

[52] _____ Estructuras análogas a los números reales. Bogotá: Universidad Pedagógica Nacional, 2006.

[53] MELVILLE, Duncan. An Old Babylonian Problem Text. En: Mesopotamian Mathematics [en línea]. (2002). [consultado 10 enero 2007]. Disponible en <http://it.stlawu.edu/%7Edmelvill/mesomath/tablets/Stones.html>

[54] MORA, Lyda y TORRES Johana. Concepciones de estudiantes de Licenciatura en matemáticas sobre números reales. Bogotá: Universidad Pedagógica Nacional, 2007.

[55] MOSTOW, George; SAMPSON, Joseph. y MEYER, Jean-Pierre. Fundamental Structures of Algebra. New York: McGraw Hill, 1963.

[56] MUÑOZ, José. Introducción a la teoría de conjuntos. 4 ed. Bogotá: Universidad Nacional de Colombia, 2002.

[57] NIVEN, Ivan y ZUCKERMAN, Herbert. Introducción a la teoría de los números. México: Limusa, 1976.

[58] NEWMAN, James. Sigma el Mundo de las Matemáticas. Barcelona: Grijalbo, 1997. v. 5.

[59] OOSTRA, Arnold. Lógicas de Lukasiewicz y sus álgebras. En: _____ Huellas en los encuentros de Geometría y Aritmética. Bogotá: Universidad Pedagógica Nacional, 2005.

[60] _____ Huellas en los encuentros de Geometría y Aritmética. Bogotá: Universidad Pedagógica Nacional, 2005.

[61] PEIRCE, Charles. On the Logic of Number. En: American Journal Mathematics. Vol. 4. (1881); p. 85-95.

[62] PÉREZ, Jesús Hernando. La aritmética según Gottlob Frege. Un ejemplo de matemáticas elementales. En: Memorias XIII Encuentro de Geometría y I de Aritmética. Vol. 1. (jun. 2002); p. 19 - 33.

[63] POLLARD, Harry. The theory of algebraic numbers. New Jersey: John Wiley and Sons, 1965.

[64] PUIG, Luis. Historias de al-Khwârizmî (6ª entrega). El cálculo con la cosa. En: Suma. Vol. 67. (jun. 2011); p. 101-110.

[65] RUIZ, Carlos. Teoría de la adjunción. Trabajo de año sabático. Bogotá: Universidad Nacional, 1989.

[66] RUSSELL, Bertrand. La evolución de mi pensamiento Filosófico. Madrid: Alianza Editorial, 1976.

[67] _____ Introduction to mathematical philosophy. New York: Dover, 1993.

[68] _____ Introducción a la filosofía matemática. Barcelona: Paidos, 1988.

[69] SÁNCHEZ, Clara. La construcción de los números reales. En: XIV Coloquio Distrital de Matemáticas y Estadística (1997).

[70] SCHRÖDER, Ernst. Lehrbuch der arithmetik und algebra fuer lehrer und studierende, Band 1, Leipzig: Teubner, 1873.

[71] SMITH, David. History of mathematics. New York: Dover, 1958. v. 2.

[72] SMULLYAN Raymond, FITTING, Melvin. Set theory and the continuum problem. Oxford: Clarendon Press, 1996.

[73] STEIN, Sherman. On the foundations of quasigroups, Trans. Amer. Math. Soc. 85, 1957.

[74] SUPPES, Patrick. Teoría axiomática de conjuntos. Cali: Norma, 1968.

[75] TAKAHASHI, Alonso. Las nociones matemáticas IV. Giusseppe Peano (La axiomática). En: Boletín de Matemáticas. Vol. 6, No. 5. (1972); p. 33 - 45.

[76] TAKEUCHI, Yu. Conjuntos Ordenados - Fundamentos de Análisis. En: IV Coloquio Distrital de Matemáticas y Estadística. (1987).

[77] WANG, Hao. Reflections on Kurt Gödel. Massachusetts: Massachusetts institute of Technology, 1987.

[78] WARNER, Seth. Modern Algebra. New York: Dover, 1990.

[79] WUSSING, Hans. Lecciones de historia de las matemáticas. Madrid: Siglo XXI, 1998.

[80] YAGLOM, Isaak. Elementary geometry, then and now. En: COXETER, Harold. The geometry vein. New York: Springer, 1981. p. 253 - 269.

[81] ZALAMEA, Fernando. Una jabalina lanzada hacia el futuro: anticipos y aportes de C. S. Peirce a la lógica matemática del siglo XX. En: Mathesis 9. (1993). p. 391 - 404.

[82] ZEHNA, Peter y JOHNSON, Robert. Elements of set theory. Boston: Allyn and Bacon, 1972.

Índice alfabético

En el estudio de las matemáticas los procesos de abstraer y representar permiten formalizar los conceptos dentro de teorías mediante lenguajes especializados y permiten construir modelos que ejemplifiquen dichas teorías en universos particulares; no obstante, es común que en dicha actividad estos procesos no sean identificados y aún más, que no sea usual el diseño de actividades y situaciones que favorezcan su desarrollo.

En este libro se sugieren algunas actividades enfocadas en el desarrollo de dichos procesos matemáticos, especialmente en el trabajo con estructuras algebraicas finitas y enumerables. El tratamiento que se hace parte de algunas representaciones de estructuras algebraicas finitas para abstraer su estructura, para luego caracterizarla vía axiomas necesarios y suficientes; en las estructuras algebraicas infinitas pero enumerables, como la de los números naturales, se estudian varias de sus axiomáticas, se comparan y se construyen representaciones.

ISBN 978-958-8650-53-1
9 789588 650531