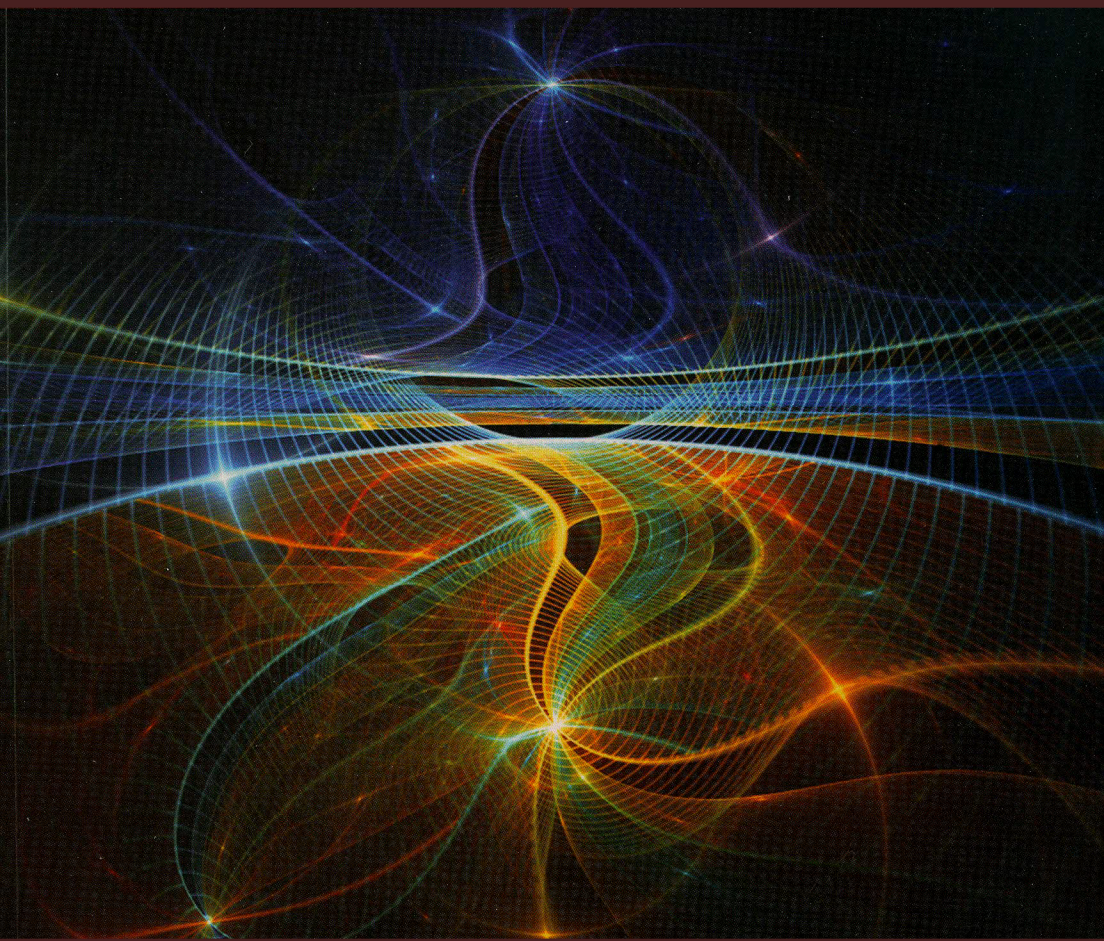
Fundamentos de matemática avanzada



Dr. René Piedra

INSTITUTO TECNOLOGICO DE SANTO DOMINGO

René Piedra

Nació en La Habana, Cuba, el 14 de septiembre de 1952 y se nacionalizó dominicano en el 1998. Se graduó por la Universidad de La Habana de licenciado en Matemática Pura en el 1976. Posteriormente realizó diversos estudios de postgrado, culminando su maestría de Matemática en 1977 y el doctorado en Ciencias Físico-Matemáticas en 1990. En su tesis doctoral, logró situar la Teoría de Aproximantes Simultáneos a un mismo nivel en el contexto de la interpolación de funciones analíticas mediantes fracciones racionales con denominador de grado prefijado.

Desde que se graduó hasta enero del año 1992 fue profesor en la Universidad de la Habana, Cuba. En 1993 llega a República Dominicana, desde esa fecha y hasta mayo de 2007, se desempeña como profesor de la Pontificia Universidad Católica Madre y Maestra, Recinto Santo Tomás de Aquino. Allí fue director del Departamento de Matemáticas y Física desde 1999 hasta 2006 y coordinador de la Maestría en Matemática Educativa hasta el 2007.

Fue consultor en el área de matemática de la Dirección General de Currículo de la SEE. Desde el 2007 es profesor de INTEC y, además, funge como coordinador de la carrera de licenciatura en Matemática con concentración en Estadística y Ciencias Actuariales; es miembro del Comité de Postgrado del INTEC y director del Centro de Investigación Matemática y Educación Matemática (CIMEM-INTEC) y coordinador del foro académico MAT-INTEC.

FUNDAMENTOS DE MATEMÁTICA AVANZADA

Dr. René Piedra

FUNDAMENTOS DE MATEMÁTICA AVANZADA

Instituto Tecnológico de Santo Domingo
Santo Domingo, 2012

Piedra, René
Fundamentos de matemática avanzada / René Piedra .— Santo Domingo : Instituto Tecnológico de Santo Domingo, 2012
274 p. : il.

1. Matemáticas I. Título

510
P613f

CEP/INTEC

INSTITUTO TECNOLÓGICO DE SANTO DOMINGO

ISBN: 978-9945-472-14-1

Revisión de contenido:
Félix Lara

Edición al cuidado de Fari Rosario

Diseño de portada:
Alejandro de Jesús Nivar

Diagramación:
Jesús Alberto de la Cruz

Impresión:
Editora Búho, S.R.L.
Tels.: 809 686 2241 | 809 686 2243
Fax: 809 687 6239
E-mail: editorabuho@yahoo.com

Impreso en la República Dominicana
Printed in Dominican Republic

Agradecimientos

Quiero agradecer a Dios por todas las bendiciones que me ha dado, a mi madre, la Dra. Graciella de la Torre, quien me dio la vida y fue mi maestra, a mi profesor y amigo el Dr. Miguel Jimenez Pozo –quien además de la amistad me honra con la escritura del prólogo de este libro–. A mi profesor y amigo, quien fue el tutor científico de mi investigación doctoral, el Dr. Guillermo López Lagomasino.

También agradezco el apoyo que me han brindado las autoridades del INTEC, en particular al decano de la Facultad de Ciencias Básicas y Ambientales, mi amigo, MSc. Félix Lara, y a todos mis profesores y profesoras, a mis alumnos y alumnas.

A mi esposa, Lizette, quien me ha acompañado, apoyado y aguantado durante más de 37 años, a mis hijas Lissette y Lisbell, a mi yerno, *Mandy*, quien es mi hijo varón, a mi adolecente nieta, Susette, mi nietecito Jorge David y a la nietecita, Amanda Michelle, quien debe nacer muy pronto con la gracia de Dios: ellos son mi alegría y la razón de mi existencia.

El autor

Contenido

3. CONJUNTOS, RELACIONES Y FUNCIONES

4. ESTRUCTURAS ALGEBRAICAS

5. CONJUNTOS NUMÉRICOS

Prólogo

La Matemática es, contrariamente a lo que algunas personas creen, como un gigantesco edificio en permanente y acelerado crecimiento, cuyos cimientos no son tan sólidos como lo es su propia estructura. Esto debe justificarse al menos brevemente. Pero hay que dejar en claro que escribir sobre los fundamentos de esta ciencia, justo de lo que trata de hacer este libro, deviene en una tarea compleja y difícil.

Hablamos de crecimiento permanente, porque es una ciencia que se enriquece día a día con resultados que responden a problemas que se encontraban pendientes por solucionarse o problemas nuevos que provienen de otras ciencias: que provienen de la vida práctica o de las exigencias de la misma Matemática. Estas exigencias corresponden a diferentes motivaciones, como pueden ser la unificación de teorías matemáticas mediante abstracciones más generales o el estudio de problemas nuevos que surgen precisamente cuando se cuenta con resultados novedosos.

Diríase que nuestro conocimiento es como una gran mancha cuya frontera es lo desconocido o lo que hay que investigar. Mientras más

conocemos, más aumenta esta mancha y consecuentemente su frontera. Es decir, crecen los problemas a investigar.

El crecimiento es acelerado, porque el volumen de artículos contentivos de resultados matemáticos nuevos crece cada año. Son cientos de miles de páginas publicadas anualmente en revistas especializadas, con resultados matemáticos nuevos, acabaditos de hornear, escritos de manera concisa. Hace ya muchas décadas que no hay y seguramente no habrá nuevamente, un matemático conocedor de toda la Matemática existente en su momento de vida. El crecimiento no es solo en la Matemática sino en todas las ciencias, a lo que debe sumarse el surgimiento de otras nuevas. Todas, incluyendo las sociales y no solamente la Física como antes ocurría, reclaman ahora respuesta matemática a sus problemas particulares.

Se sabía que la aplicación de la Matemática a los diversos problemas industriales, biológicos, económicos, etc., redundaría en extraordinarios beneficios. Pero estas aplicaciones carecían de sentido práctico, pues los cálculos a las soluciones de los modelos correspondientes podrían necesitar más tiempo que la vida misma. Incluso y sin exagerar, la sucesión de varias vidas. Repentinamente nos encontramos con un desarrollo vertiginoso de los cómputos electrónicos que posibilitan estos cálculos en tiempos increíblemente breves. Es así como la Computación facilitó la aparición de la llamada Matemática Industrial, cuya utilización en los últimos treinta o cuarenta años ha sido tan espectacular, que sin exageración alguna puede ser considerada como revolucionaria.

Si bien este crecimiento agigantado podría sorprender a quienes han pensado que en Matemática todo está hecho; la sorpresa verdadera llega cuando afirmamos que sus cimientos no son tan sólidos como su estructura aparenta. En efecto, el edificio matemático es fuerte porque el rigor empleado en el trabajo ha ido evolucionando de manera tal, que si bien siempre continuará evolucionando y será perfectible, hoy en día es aceptado como bueno y los problemas de antaño han sido redefinidos y

contestados con este nuevo rigor. Es fuerte porque cada artículo arroja resultados nuevos que aparecen publicados en las revistas de investigación matemática y se supone que ha sido previamente sometido a un arbitraje internacional severo. Es fuerte porque su aplicación diaria a las múltiples necesidades humanas es siempre exitosa. Y sin embargo clamamos que este sólido edificio se sustenta en una base tambaleante.

La afirmación anterior es compartida por todos los matemáticos, por supuesto. Pero sería bueno que ilustremos un tanto las causas para un público menos versado en el tema. La Matemática debe apoyarse en conceptos primarios, como son nuestro propio lenguaje, que es la forma material del pensamiento abstracto. Se apoya, por así decirlo, en la noción de conjunto, pertenencia y función, en las ideas geométricas, las nociones de cantidad y de otras mediciones como áreas y volúmenes. ¿Y qué sucede? La noción intuitiva de conjunto ha sido fuente de innumerables paradojas y contradicciones. Si todas las cosas materiales o abstractas tuviesen la posibilidad de ser elementos de un conjunto, ¿por qué no puede existir matemáticamente el conjunto de todos los conjuntos? Solamente un limitado número de especialistas en los fundamentos de la Matemática conocen con relativa claridad el terreno resbaladizo que pisan al tratar con la Teoría de Conjuntos, originada en los trabajos del célebre matemático alemán Georg Cantor. ¿Podríamos fiarnos de nuestra intuición geométrica? Hace mucho que sabemos de la existencia de superficies con una sola cara, de curvas que llenan todo un espacio, de que no existen prácticamente funciones derivables en el conjunto de funciones continuas. En cantidades (o cardinales, para ser más precisos), sabemos que casi no hay números racionales o algebraicos en comparación con los irracionales trascendentes, a pesar de que son relativamente pocos números trascendentes los que hemos identificado. También conocemos la imposibilidad de asignar volúmenes a todos los subconjuntos del espacio tridimensional, si deseamos mantener un mínimo de propiedades geométricamente razonables. Estas y otras sorpresas y contradicciones con nuestro pensamiento, originaron históricamente períodos de crisis

en la Matemática. Estas crisis, sin embargo, constituyeron siempre motores impulsores para cambios de ese pensamiento, remodelando teorías, perfeccionando el rigor.

¡Sí, pero no! El lector tiene derecho a plantearse y a valorar la Matemática que, al fin y al cabo, ha ido remodelándose, adaptándose a las necesidades nuevas asociadas al desarrollo del conocimiento humano. Pero lamentablemente es la propia Lógica Matemática la que, atacándose a sí misma, demuestra rigurosamente sus limitaciones. Fue un eminente especialista de origen checo, de nombre Kurt Gödel, quien hacia 1931 borró de un plumazo los sueños de todos los matemáticos. Por decirlo de alguna manera aunque sea informal, Gödel demostró rigurosamente que cualquier esfuerzo para probar que los axiomas que sustentan la aritmética están libres de contradicciones, será siempre baldío.

Sus conclusiones, más generales que las expuestas de manera muy simple en la oración anterior, son realmente tan profundas, que originaron un libro no dirigido a cualquier lector. El mismo no buscaba explicar el trabajo de Gödel sino tan solo dar una idea de en qué consiste ese trabajo.

Lo expuesto hasta aquí, aunque realmente de manera muy informal y breve, debe sustentar, espero, la afirmación hecha desde el primer párrafo de este prólogo, relativa a la dificultad y complejidad de escribir un libro sobre los fundamentos de la Matemática, sin que sea un tratado para especialistas y que mantenga un rigor lógico relativo y pueda ser aprovechado por lectores de diversos niveles. Pero no conforme con lograr ese objetivo con este libro, el Dr. Piedra se esfuerza todavía en sistematizar y promover el razonamiento deductivo del lector, aplicándolo a la formación de los conjuntos numéricos, un tema de trascendental importancia. Es también un esfuerzo en la didáctica, en la enseñanza de la Matemática, donde lamentablemente abundan maestros que no tienen el dominio requerido; pues si algo está claro, es que para enseñar cualquier tema

hace falta ante todo dos requisitos: dominar el tema y tener la vocación. ¡Qué bueno que el Dr. Piedra satisface ambos!

Respecto a los conjuntos numéricos que ocupan una parte sustancial del libro que prologamos, debemos detenernos en su relevancia. De las mil y una maneras en que podríamos estudiar el desarrollo de la humanidad, una de ellas podría ser atendiendo a la idea que tenían de los números en cada estadio. Los primeros individuos sociales, obviamente, tenían suficiente con los números naturales para satisfacer sus necesidades. Después, es de esperarse, necesitaron las fracciones positivas. Se documenta históricamente que ya los babilonios y después los antiguos egipcios, manejaban fracciones y las representaban con símbolos especiales. Más adelante y, aunque parezca hoy de manera tan natural, la creación y utilización del cero no como elemento posicional para la escritura de cifras sino como cantidad propiamente, fue considerada por los indios y por los mayas alrededor de la época de Cristo. Tenemos así los números naturales y poco a poco la introducción de los enteros y de los racionales. Pero los procesos de desarrollo usualmente no marchan linealmente, el salto a los reales requirió de siglos y tuvo su inicio con los griegos y el célebre teorema de Pitágoras, pues se deduce del mismo que la longitud de la hipotenusa de cualquier triángulo rectángulo con dos lados iguales, no es racionalmente proporcional a la longitud de estos. Es decir, la hipotenusa de un triángulo rectángulo de longitud 1, tendría como longitud un número cuyo cuadrado fuese 2, no existente en el terreno de los números racionales. La aparición de los números imaginarios y de los cuaterniones, corresponde a períodos relativamente muy recientes.

Si estudiamos la historia de los números, en cierto sentido estaríamos estudiando la evolución de la Matemática; pero no totalmente desde el punto de vista de sus fundamentos. Los números, en efecto, inicialmente fueron aceptados como conceptos abstractos primarios, aunque esta denominación no se usare. La pregunta de cómo definir los números rigurosamente vino con el célebre matemático y filósofo inglés Bertrand

Russell, ya en el siglo xx, quien reconoció la necesidad de una respuesta adecuada al problema. Aunque su respuesta finalmente no fuese totalmente exacta, abrió el camino hacia ese objetivo. Para que el lector tenga una idea de los problemas que se plantean, podría tratar –como ejercicio recreativo inicialmente y de complejidad insuperable después– de definir rigurosamente el número 1. Pues el 1 es el 1, una cosa solamente, diría dentro de un círculo vicioso cualquier persona. Tan complejo es este problema que el célebre matemático alemán Leopold Kronecker, doctorado en 1845 en Berlín, precisamente en temas de números, sentenció que Dios había hecho el número 1 y los hombres los demás.

Por último, desearía detenerme unos instantes en las características personales del autor. La vida da vueltas. Unas veces nos pone de un lado y en otras, de cabeza. La madre del autor del libro, la Dra. Graciella de la Torre, fue mi profesora justamente en Teoría de Conjuntos y en Topología, en la Universidad de La Habana durante un curso que tomé en el 1967/68 cuando cursaba mi año de la Licenciatura en Matemática. Eran tantas las interrogantes, las contradicciones "aparentes" en los fundamentos del material estudiado, que me parecían incorrectos y los rechazaba por ilógicos. Así de mal andaba yo en aquella época estudiantil. Así de sorprendentes son los resultados de la Teoría de Conjuntos. Más adelante, siendo yo profesor titular en dicha universidad, tuve entre mis alumnos de pregrado al hoy profesor y doctor René Piedra, autor de este libro como ya sabemos. Y luego –así ocurrió– todos: la Dra. Graciella, el Dr. René y yo fuimos compañeros de trabajo en un mismo departamento docente de la Facultad de Matemática y Computación de la Universidad de La Habana, durante muchos años. Juntos trabajamos, juntos impartimos cursos. Creo que estos antecedentes me avalan, me autorizan a expresar, mi opinión positiva sobre la capacidad matemática del autor.

Recomiendo la lectura y el estudio de este libro porque me parece correctamente escrito, porque independientemente de los aciertos y deficiencias

que a la postre pudiesen detectarse en el mismo, el autor logra a mi juicio –y a través de su entusiasmo contagioso– abrir el prisma multicolor de la motivación; premisa fundamental de la educación.

Puebla, México, 18 de junio de 2012

Dr. & Dr. Scient. Miguel A. Jiménez Pozo
Profesor-Investigador Titular
Facultad de Ciencias Físico Matemáticas
Benemérita Universidad Autónoma de Puebla
Puebla, México

Introducción

Lo deseable debería ser que el Sistema Educativo de cada país garantice que en la enseñanza de la matemática se combine la abstracción con el cálculo y la geometría. En ese sentido, el conocido matemático español Enrique Zuazua afirma:

> La naturaleza está llena de formas geométricas a las que no podemos escapar y el cálculo es doblemente imprescindible, primero a la hora de resolver problemas concretos y, en segundo lugar, porque el cálculo reiterado de manera sistemática conduce a la abstracción, es como si el sistema neuronal necesitara repetir muchas veces las mismas operaciones para sintetizarlas, automatizarlas y dar el salto a la abstracción. Pero también es cierto que los problemas con los que se encuentra el ciudadano exigen, de manera creciente, de una cierta simbolización y abstracción, pues la complejidad que entrañan muchos de ellos en cualquier ámbito de nuestra actividad, económica o industrial, hacen materialmente imposible un abordaje con técnicas meramente calculísticas. (2007: 127).

En un artículo titulado "Enseñando y utilizando técnicas matemáticas para hacer demostraciones", escribe el matemático Daniel Solow: "La incapacidad para comunicar demostraciones de una manera comprensible

ha sido perjudicial para estudiantes y profesores en todas las ramas de las matemáticas". (citado por Hilton, 2005: 7).

En el prólogo del libro *Cómo entender y hacer demostraciones en Matemáticas* escrito por Solow, el matemático Peter Hilton (2005: 7) destaca lo siguiente:

> Todos aquellos que han tenido la experiencia de enseñar matemáticas y la mayoría de aquellos que han tratado de aprenderlas, deben coincidir seguramente en que entender una demostración matemática es una traba para la mayoría de los estudiantes y muchos de ellos tratan de salvar este obstáculo evadiéndolo, confiando en la indulgencia del profesor para que no incluya demostraciones en los exámenes. Esta confabulación entre estudiantes y profesor evita algunas de las consecuencias desagradables, tanto para el alumno como para el profesor, producidas por la falta de dominio del tema por parte del estudiante, pero esto no modifica el hecho de que un elemento clave de las matemáticas, probablemente su característica más notable no ha entrado en el repertorio del estudiante. El doctor Solow cree que es posible enseñar al estudiante a entender la naturaleza de las demostraciones sistematizándolas.

Aunque quizás no deba aceptarse como absolutamente cierto este último planteamiento, sí creo que hay aspectos de esa sistematización que deben ayudar al estudiante a desarrollar la capacidad de entender y de hacer demostraciones matemáticas, es por ello que decidí incluir en este libro un capítulo 1, de carácter introductorio, para abordar el proceso de sistematización propuesto por el doctor Solow. Posteriormente, en el segundo capítulo, estudiaremos los fundamentos de esa sistematización.

La importancia de la Matemática, como fundamento de una gran parte de las ciencias y de la tecnología, no lo es solo por ella tratar del espacio y de la cantidad, y por ello servir de herramienta para modelar la realidad, sino mucho más esencialmente lo es por ella constituir el conjunto de sistemas hipotéticos deductivos y sus aplicaciones. Por esta razón, en la Enseñanza de la Matemática debe priorizarse su valor formativo y, más importante que el estudio de casos particulares para aplicar fórmulas

matemáticas, lo es la obtención de nuevos métodos y la suma de experiencias mentales con que se enriquece nuestra facultad de razonamiento lógico, pues la adquisición de una disciplina mental racional es lo más valioso de una educación científica.

Toda teoría científica se construye a partir de un conjunto de conceptos, llamados conceptos primarios, los cuales no se definen, sino que sirven para definir otros conceptos de la teoría, así como de un conjunto de proposiciones, cuya veracidad se acepta sin demostración, las cuales son llamadas axiomas o postulados y sirven, en esa teoría, para hacer las demostraciones de la veracidad o falsedad de otras proposiciones. Ante esta aseveración, inmediatamente nos debemos preguntar: ¿qué se entiende por una demostración válida de la veracidad o falsedad de una proposición dada dentro de una teoría específica?

Debe ser claro que para la validez de una demostración se necesitará de la construcción de un argumento que haga dicha prueba.

En los fundamentos de la Matemática, vistos como actualmente se ven, se encuentra la estructura del pensamiento racional dada, en primer lugar, mediante elementos de la Lógica, donde la teoría de la demostración mediante argumentos válidos y la metodología en la deducción de teoremas a partir de axiomas u otros teoremas ya demostrados son de gran importancia y, en segundo lugar, mediante elementos de la teoría de conjuntos, los cuales le ofrecen el soporte para su construcción y lenguaje.

Elementos de Lógica Matemática y de Teoría de Conjuntos se estudian en el segundo y tercer capítulo. En el segundo se formula una teoría de inferencia que se adecúa a todos los ejemplos típicos del razonamiento deductivo en Matemática y en las ciencias empíricas. Además se hace énfasis en la traducción a simbología lógica de textos en español, como base para la comprensión racional de estos.

En el tercer capítulo, mediante la aceptación de un cierto conjunto de axiomas, se ejemplifica la construcción de otros conjuntos y las operaciones fundamentales entre ellos, y se relacionan con la estructura de la lógica estudiada en el segundo. Además se estudian las relaciones y funciones, lo cual es fundamental para la comparación de conjuntos y para definir otras estructuras, como la de conjunto cociente y la de conjunto ordenado.

En el cuarto capítulo se estudia el concepto de operación binaria y se introducen algunas estructuras algebraicas, las cuales son esenciales para la comprensión de una definición matemática formal del concepto de número.

Las definiciones más importantes en la Matemática, por ser creadoras de nuevos conceptos, son las que se dan por axiomas, por recurrencia, o por abstracción, en el quinto capítulo se pone esto de manifiesto, mediante las cuatro partes que lo componen.

En la primera parte se define el número natural por axiomas y sus operaciones por recurrencia. En la segunda, tercera y cuarta parte se definen por abstracción respectivamente, los enteros, los racionales y los reales. Se destacan las inmersiones entre ellos y se concluye con la representación decimal de un número real y la demostración de que un número real es racional, si y sólo si, su representación decimal infinita es periódica.

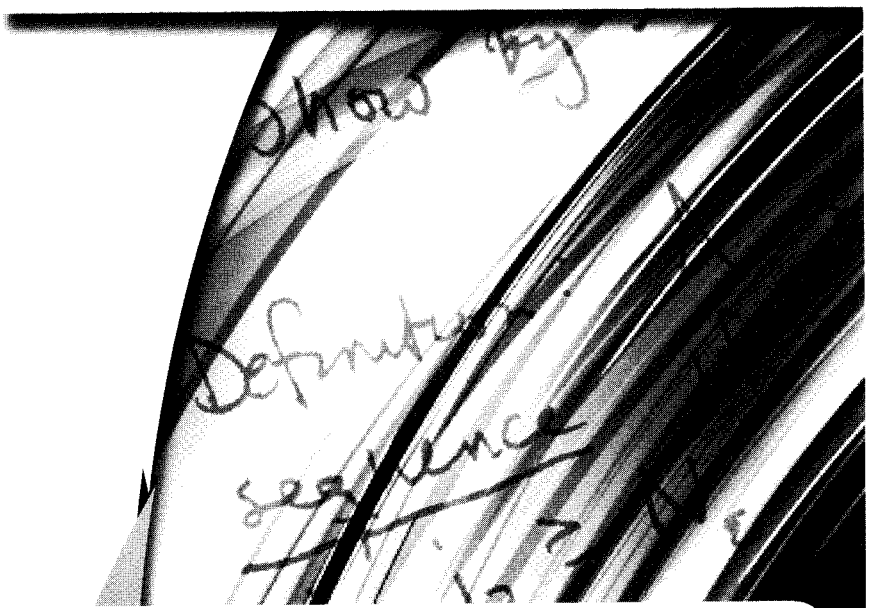
Con este libro pretendemos llenar un vacío en la literatura de la Matemática en nuestro país y en otros muchos, fundamentalmente, de habla hispana, pues analiza elementos esenciales de los fundamentos de la Matemática, en particular, los que tienen que ver con el desarrollo del pensamiento racional y abstracto, el razonamiento hipotético deductivo y la teoría de formación de los conjuntos numéricos en un lenguaje asequible que, aunque sea riguroso, no peque de un excesivo formalismo y sea lo

suficientemente sencillo en presentación y contexto, para que permita una fácil comprensión del lector interesado en la temática.

El texto puede servir de consulta tanto en cursos de capacitación de maestros y profesores de nivel medio o superior, como en asignaturas de formación matemática de diversos niveles y para diversos perfiles. Puede resultar provechoso para el área de ciencias y tecnología. En definitiva, espero que este libro sea una lectura provechosa para todos aquellos que les guste la Matemática y deseen o necesiten conocer sus fundamentos.

1 La sistematización

Como método para entender y hacer demostraciones matemáticas



Introducción

El método de sistematización que se propone a continuación fue sugerido por Daniel Solow (1992) como una metodología apropiada para explicar las matemáticas abstractas y las técnicas que se utilizan en una demostración. Esta metodología, en mi opinión, es muy válida cuando se inician estos estudios.

Lo primero que se debe destacar es que para entender o hacer demostraciones en Matemática es indispensable aprender un nuevo idioma y una forma nueva de razonar, para lo cual se requiere mucha práctica. El objetivo que tenemos en este capítulo es que el lector adquiera los elementos básicos sobre el idioma y la forma de razonar.

1.1. El método progresivo-regresivo

El método progreso-regresivo para hacer una demostración en matemática es posiblemente la técnica más usual en el razonamiento hipotético deductivo. Esta técnica se emplea para hacer una demostración en matemática del tipo $A \rightarrow B$.

Un cuadro que corresponde a este método es:

Proceso regresivo: $B_n \rightarrow B_{n-1} \rightarrow \ldots \rightarrow B_1 \rightarrow B$
Proceso progresivo: $A \rightarrow A_1 \rightarrow \ldots \rightarrow A_m$
Para concluir: $A_m \rightarrow B_n$

El método progresivo-regresivo. Para demostrar $A \rightarrow B$ podemos suponer que A es verdadero y debemos obtener, como conclusión, la veracidad de B. Cuando tratamos de determinar cómo llegar a la conclusión estamos usando un proceso regresivo, cuando tratamos de usar la información contenida en A estamos usando un proceso progresivo.

El proceso regresivo debe iniciarse preguntando: ¿cómo o cuándo puedo concluir que B es verdadera?, esta pregunta debe formularse en forma abstracta, es decir, independiente de las particularidades del caso, símbolos, notación, etc, y tiene que contestarse para iniciar el proceso. Esa pregunta Solow la llama "pregunta de abstracción". Cuando respondemos esa pregunta de abstracción y la particularizamos para nuestro caso, obtenemos una proposición B_1 que, de ser verdadera, tendría

que ser verdadera B_1, es decir, tal que B_1 implica a B, esto se simboliza como $B_1 \rightarrow B$.

En el proceso progresivo tratamos de obtener una proposición A_1 que pueda deducirse de A, es decir, que de A ser verdadera, tendría que ser verdadera A_1, lo cual se simboliza como antes $A \rightarrow A_1$.

Veamos el siguiente ejemplo, ampliamente analizado por Solov (1992: 23-30).

Ejemplo 1

Supongamos que dado un triángulo rectángulo XYZ de lados x y y e hipotenusa z, deseamos demostrar que si el triángulo XYZ tiene área $\frac{Z^2}{4}$ entonces el triángulo XYZ es isósceles.

¿Cuál pregunta puede formularse en forma abstracta para iniciar el proceso regresivo?

Proceso regresivo.

¿Sería correcta la pregunta?:
¿Cómo podemos demostrar que el triángulo XYZ es isósceles?

La pregunta de abstracción correcta es:

¿Cómo podemos demostrar que un triángulo es isósceles?

Es decir, en la pregunta de abstracción no debe aparecer si el triángulo se llama XYZ o ABC o de otra manera.

Después de hacernos la pregunta de abstracción, debemos contestarla. Si bien puede haber diversas respuestas, debemos escoger una adecuada a la información que tenemos. Una adecuada sería: **probando que tie-**

nen dos lados de igual longitud. Aplicada esa respuesta a nuestra situación, significa probar que $x = y$. Esta proposición será B_1 del proceso regresivo en el cuadro que corresponde al método progresivo-regresivo.

¿Cuál pregunta puede formularse en forma abstracta para continuar el proceso regresivo?

Una pregunta de abstracción adecuada sería:

¿Cómo podemos demostrar que dos números reales son iguales?

Una adecuada respuesta ahora sería **probando que la diferencia es cero.** Aplicada esa respuesta a nuestra situación, significa **probar que** $x - y = 0$. Esta proposición será B_2 en nuestro cuadro.

Pasemos ahora a desarrollar un proceso progresivo:

En nuestro caso A nos afirma que el triángulo rectángulo XYZ de lados x y y, e hipotenusa z, tiene área $\frac{Z^2}{4}$

Sabiendo que el triángulo XYZ es rectángulo, con hipotenuisa z y los otros dos lados x y y, tenemos que $x^2 + y^2 = z^2$ y que su área es $\frac{xy}{2}$. Por tanto de A se deduce que $\frac{xy}{2} = \frac{Z^2}{4} = \frac{x^2 + y^2}{4}$. Luego podemos tomar a $\frac{xy}{2} = \frac{x^2 + y^2}{4}$ como el A_1 en el proceso progresivo de nuestro cuadro.

Usando ahora propiedades de los números reales podemos obtener: A_2 como $x^2 - 2xy + y^2 = 0$ y, luego A_3, como $(x - y)^2 = 0$.

Ahora es evidente que: $A_3 \rightarrow B_2$ quedando cerrado el cuadro progresivo-regresivo.

Una demostración matemática de esta proposición, sin hacer uso de esta descripción, consiste sólo en destacar que:

El área del triágulo XYZ es $\frac{xy}{4}$ por ser un triángulo rectángulo y, por Pitágoras $z^2 = x^2 + y^2$. Ahora, inmediatamente se obtiene que $\frac{xy}{2} = \frac{x^2 + y^2}{4}$, de donde $(x - y)^2 = 0$ y por tanto $x = y$, es decir, el triángulo XYZ es isósceles.

Antes de hacer una demostración matemática, creo que presentar en algunos casos, una descripción del proceso como hicimos antes, así como hacer preguntas para que los estudiantes hagan ese proceso por sí solos: puede ayudar a una mejor comprensión de la demostración y a desarrollar habilidades para hacerlas.

1.2. Cuantificadores, los métodos de demostración por construcción y por selección

Cuantificador existencial. Cuando en una proposición se comienza afirmando la existencia de algún objeto que cumple algo se dice que la proposición correspondiente está encabezada por el cuantificador existencial.

El método de demostración por construcción

En ocasiones la proposición $\boldsymbol{B}$ que se quiere deducir de $\boldsymbol{A}$, en $\boldsymbol{A \rightarrow B}$ está encabezada por el cuantificador existencial. Es natural que en ese caso una pregunta de abstracción natural puede ser: ¿cómo puedo probar la existencia de algún objeto con tal propiedad?

Durante el proceso regresivo, si alguna vez se encuentra en esa situación, una respuesta posible sería: construyéndolo, aunque ésta no es la única. La idea es generar (adivinar, producir, idear un algoritmo para producir, etc) el objeto deseado. Todo depende del problema en particular, pero en cualquier caso, la información de A será usada para hacer el trabajo.

Cuantificador universal. Cuando en una proposición se comienza afirmando que cada objeto o que todos los objetos cumplen algo se dice que la proposición correspondiente está encabezada por el cuantificador universal.

El método de demostración por selección

En ocasiones la proposición B que se quiere deducir de A, en $A \rightarrow B$, está encabezada por el cuantificador universal. Cuando queremos probar B, es decir, que todos los elementos de un cierto conjunto satisfacen una propiedad, si el conjunto tiene pocos elementos podríamos probar, para cada elemento, que la propiedad requerida es satisfecha. Sin embargo, cuando el conjunto tiene muchos elementos o una cantidad infinita de ellos, no podríamos hacerlo o nos demoraríamos demasiado, en ese caso podemos tener presente que para definir el conjunto dado debe haber alguna propiedad que lo caracterice. Precisamente el método de selección consiste en tomar un elemento arbitrario de ese conjunto y usando solo la propiedad que caracteriza al conjunto, probar que entonces también cumple la propiedad que queríamos probar que cumplen todos los elementos de dicho conjunto.

Ejemplo 2

Supongamos que queremos probar que el sistema de ecuaciones dado a continuación tiene solución:

$$ax + by = e$$
$$cx + dy = f$$

Donde a, b, c, d, e, f son números reales y $ad - bc \neq 0$. Note que lo que hay que concluir, supuesta las condiciones sobre los números reales anteriores, es que existen x y y que satisfacen las ecuaciones dadas. Se puede llegar fácilmente, usando propiedades conocidas, a **construir** esos números, $x = \frac{ed - bf}{ad - bc}$ y $y = \frac{ce - af}{cb - ad}$, usando la condición $ad - bc \neq 0$.

Ejemplo 3

Sea dada una función $y = f(x)$, continua en un intervalo $[a, b]$ y diferenciable en (a, b), donde a y b son números reales y $a < b$. Supongamos que queremos encontrar, si existen, su valor máximo, su valor mínimo y los puntos del intervalo [a, b] donde se alcanzan.

Es natural que una pregunta de abstracción posible sea: **¿cuándo una función dada tiene máximo/mínimo en $[a, b]$?**, es decir, **¿cuándo una función tiene valor máximo y/o valor mínimo en $[a, b]$?**

Si bien hay varias respuestas posibles a esta pregunta de abstracción; la primera puede ser usando la definición de valor máximo y de valor mínimo, la más adecuada en la situación planteada es usando el teorema de extremo, es decir, **cuando la función es continua en $[a, b]$**. Al particularizar la respuesta a nuestro caso obtenemos inmediatamente que la respuesta sea afirmativa.

Para encontrar esos valores, satisfecha la existencia de ellos, una pregunta de abstracción natural es: **¿cómo puedo encontrar los valores máximo y mínimo de una función en [a, b] en el caso que sabemos que existen?**

Si bien hay varias respuestas posibles a esta pregunta de abstracción, la más adecuada en este caso debe ser: encontrando todos los posibles puntos en $[a, b]$ donde se alcancen esos valores y escogiendo, como valor máximo, el mayor de las evaluaciones de esos puntos en la función y, análogamente, el correspondiente como valor mínimo.

Naturalmente esa respuesta infiere que sabemos o podemos encontrar esos posibles puntos. Si en un punto de (a, b) la función alcanza uno de esos valores extremos, entonces también en ese punto se alcanza un extremo local (esto debe haberse analizado cuando se estudia el tema) y, por el teorema de Fermat, en ese punto, si la función es diferenciable, la derivada debe ser cero. En nuestro caso la función es diferenciable en (a, b).

Por tanto, los puntos del intervalo $[a, b]$ donde se pueden alcanzar esos extremos son: a, b y los puntos x de (a, b) donde $f'(x) = 0$.

Evaluando la función en cada uno de esos puntos encontramos el valor máximo y el mínimo de la función en $[a, b]$, así como los puntos donde se alcanzan esos valores.

Observación: Los libros que usualmente se usan en el país como texto para impartir los cursos de Cálculo Diferencial no incluyen la demostración del teorema de extremos que hemos usado, solo aparece su enunciado para ser utilizado.

- **¿Cuál es la dificultad que tiene su demostración?**

- **¿Deben los profesores dominar esa demostración?**

Siendo tan importante ese teorema,

- ***¿Debe estudiarse su demostración en los cursos de Cálculo universitarios?***

La respuesta a la primera pregunta es conocida, la dificultad está en que se debe dominar una definición matemática del concepto de conjunto de números reales. La respuesta a las otras dos preguntas depende de las siguientes preguntas respectivamente:

- ***¿Deben los profesores dominar una definición matemática del concepto de conjunto de números reales?***

- ***¿Debe estudiarse una definición matemática del concepto de conjunto de números reales en los cursos de Cálculo universitarios o antes de estos?***

Ejemplo 4

Sea dada una función $y = f(x)$ continua y diferenciable en el conjunto de números reales, la cual satisface que $f(-1) \cdot f(1) < 0$ y que $\lim_{x \to -\infty} f(x) = \lim_{x \to \infty} f(x) = 0$. Supongamos que queremos encontrar, si existen, su valor máximo, su valor mínimo y los puntos en el conjunto de números reales donde se alcanzan.

Es natural que una pregunta de abstracción posible es: **¿cuándo una función como la dada tiene máximo/mínimo en el conjunto de números reales?**, es decir, **¿cuándo una función como la dada tiene valor máximo y/o valor mínimo en R?**

Si bien hay varias respuestas posibles a esta pregunta de abstracción, una puede ser usando la definición de valor máximo y de valor mínimo, la más adecuada en la situación planteada es: si existe un intervalo $[a, b]$, donde la función alcance sus valores extremos en ese intervalo y se pueda garantizar que el valor máximo que se alcanza en ese intervalo es mayor que el valor que toma la función en cualquier punto del

conjunto $\mathbf{R} - [a, b]$ y, análogamente, el valor mínimo es menor que el valor que toma la función en cualquier punto de ese conjunto complementario en **R** del intervalo $[a, b]$.

Teniendo en cuenta que nuestra función es continua en **R**, y por tanto la función restringida a cualquier intervalo del tipo $[a, b]$ alcanza su máximo y su mínimo en ese intervalo, basta preguntarnos si existe un intervalo $[a, b]$ tal que el valor que toma la función en cualquier punto de $\mathbf{R} - [a, b]$ es menor que el que toma en algún punto de $[a, b]$ y mayor que el que toma en otro punto de $[a, b]$.

Usando que $f(-1) \cdot f(1) < 0$ y la definición de que $\lim_{x \to -\infty} f(x) = \lim_{x \to \infty} f(x) = 0$, se puede lograr garantizar la existencia de ese intervalo. El lector deberá hacerlo.

Usando ahora que la función es diferenciable en **R** obtenemos que los posibles puntos donde se pueden alcanzar esos valores extremos son puntos donde $f'(x) = 0$. Evaluando la función en cada uno de esos puntos encontramos el valor máximo y el mínimo de la función en **R** y los puntos donde se alcanzan esos valores.

Observación: El método de selección es usado frecuentemente en la demostración de teoremas como, por ejemplo:

- El que dice que toda función real diferenciable es continua, donde uno considera una función real diferenciable arbitraria y prueba que ella es continua.
- El teorema de extremo anteriormente utilizado, donde uno toma una función continua arbitraria en un intervalo arbitrario $[a,b]$ y prueba que ella alcanza sus valores extremos.

1.3. Los métodos de demostración por contradicción y contrapositivo

Para demostrar $\boldsymbol{A \rightarrow B}$ podemos suponer que A es verdadero y debemos obtener, como conclusión, la veracidad de B. En el método por contradicción suponemos que A es verdadero y que B es falso, y se procura demostrar que se cumple la veracidad y falsedad de alguna proposición, lo cual es una contradicción al hecho que toda proposición en la lógica bivalente sólo tiene un valor de verdad posible, o verdadero o falso. Así, como no es posible que A sea verdadero y que B sea falso, se podría concluir que $\boldsymbol{A \rightarrow B}$ es verdadero.

En el método contra positivo sólo se supone que $\boldsymbol{B}$ es falso y se procura demostrar, como consecuencia, que $\boldsymbol{A}$ es falso, lo cual prueba que $\boldsymbol{A \rightarrow B}$ es verdadero, pues $\boldsymbol{A \rightarrow B}$ sólo es falso, si $\boldsymbol{B}$ es falso y $\boldsymbol{A}$ es verdadero.

Hay muchas situaciones donde se utiliza alguno de esos métodos, por ejemplo, a veces cuando se quiere demostrar la unicidad de que un elemento satisface algo, se supone que existan dos diferentes y se logra, bajo ese supuesto, alguna contradicción.

En el ejemplo 2, si $(x_1, y_1) \neq (x_2, y_2)$ son soluciones del sistema dado, se obtiene que, por ser soluciones del sistema, satisfacen:

$$a(x_2 - x_1) - b(y_2 - y_1) = 0$$
$$c(x_2 - x_1) - d(y_2 - y_1) = 0$$

Multiplicando ahora la primera ecuación por d, la segunda por b y restando, obtenemos que: $(ad - bc)(x_2 - x_1) = 0$. Y, multiplicando la primera ecuación por c, la segunda por a y restando, obtenemos que: $(ad - bc)(y_2 - y_1) = 0$

Si $(x_1, y_1) \neq (x_2, y_2)$ se obtiene que $(ad - bc) = 0$ y, esto es una contradicción a la suposición de que $ad - bc \neq 0$.

Otra situación, en que se usa comúnmente el método por contradicción o el contrapositivo, es cuando se quiere probar la veracidad de una proposición que se encabeza con el cuantificador universal, $\forall x, P(x)$; para ello se supone lo contrario, es decir, la existencia de x ocurriendo la negación de $P(x)$, y llegando a una contradicción.

Ejemplo 5. Probemos que: "$\forall n \in N$, *si* n^2 *es par, entonces n es par*".

Supongamos que exista un número natural n tal que n^2 sea par pero n sea impar. Si n es impar, existe $k \in Z$ tal que $n = 2k + 1$, por definición de impar. Entonces $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ y, como $2k^2 + 2k$ es un entero si k lo es, entonces n^2 es impar, lo cual contradice la suposición de que es par. Por tanto, como no puede existir ese número natural se concluye que es cierta la proposición enunciada al no poder ser cierta su negación.

Debe destacarse que muchos estudiantes tienen dificultad para expresar correctamente la negación de proposiciones en que se usan cuantificadores. En el próximo capítulo se profundiza en su estudio.

Solow (1992) destaca en su libro, que existen cuatro términos en matemática que se encuentran frecuentemente cuando se tratan con demostraciones: proposición, teorema, lema y corolario. Así mismo recuerda que existen proposiciones que se aceptan sin demostración: los *axiomas*. Análogamente recuerda qué es una definición formal de un concepto matemático, así como la existencia de conceptos que se aceptan sin definición, los llamados conceptos primarios.

Nota: El conocimiento que tengamos de las definiciones de los conceptos matemáticos, así como de la teoría precedente que estamos estudiando, será lo que nos ayudará a hacernos preguntas de abstracción adecuadas y nos permitirá responderlas correctamente.

Por todo lo dicho anteriormente no nos podemos conformar con la "comprensión" de un concepto matemático, debemos poderlo definir.

1.4. Resumen y ejercicios propuestos

La metodología de sistematizar las diversas técnicas generales de demostración que se usan en matemática, es un recurso muy útil para el que comienza a estudiar la matemática en ese nivel y para el maestro que quiere ayudar a sus estudiantes a entender y hacer demostraciones matemáticas.

En los siguientes capítulos daremos fundamento a lo visto aquí y desarrollaremos otras técnicas muy usadas en demostraciones matemáticas

Ejercicios propuestos

Diga cuáles técnicas de demostración usted utilizaría para demostrar cada una de las siguientes proposiciones y explique por qué, posteriormente desarróllelas en forma sistemática destacando cada aspecto en su demostración.

a) La suma de dos enteros pares es un entero par.

b) El producto de dos enteros es impar si y sólo si ambos enteros son impares.

c) Para cualesquiera números enteros a,b,c, si "a divide a b" y "b divide a c", entonces "a divide a c".

d) Para cualesquiera números reales x, y, z si $x^2 + y^2 + z^2 = 1$, entonces el máximo valor de $xy + yz + zx$ es 1.

e) Para todo número real x, si $x > 2$ entonces existe un único número real y, tal que $y < 0$ y $x = \dfrac{2y}{1 + y}$

f) Para todo entero par n y entero impar m, 4 divide a mn o 4 no divide n.

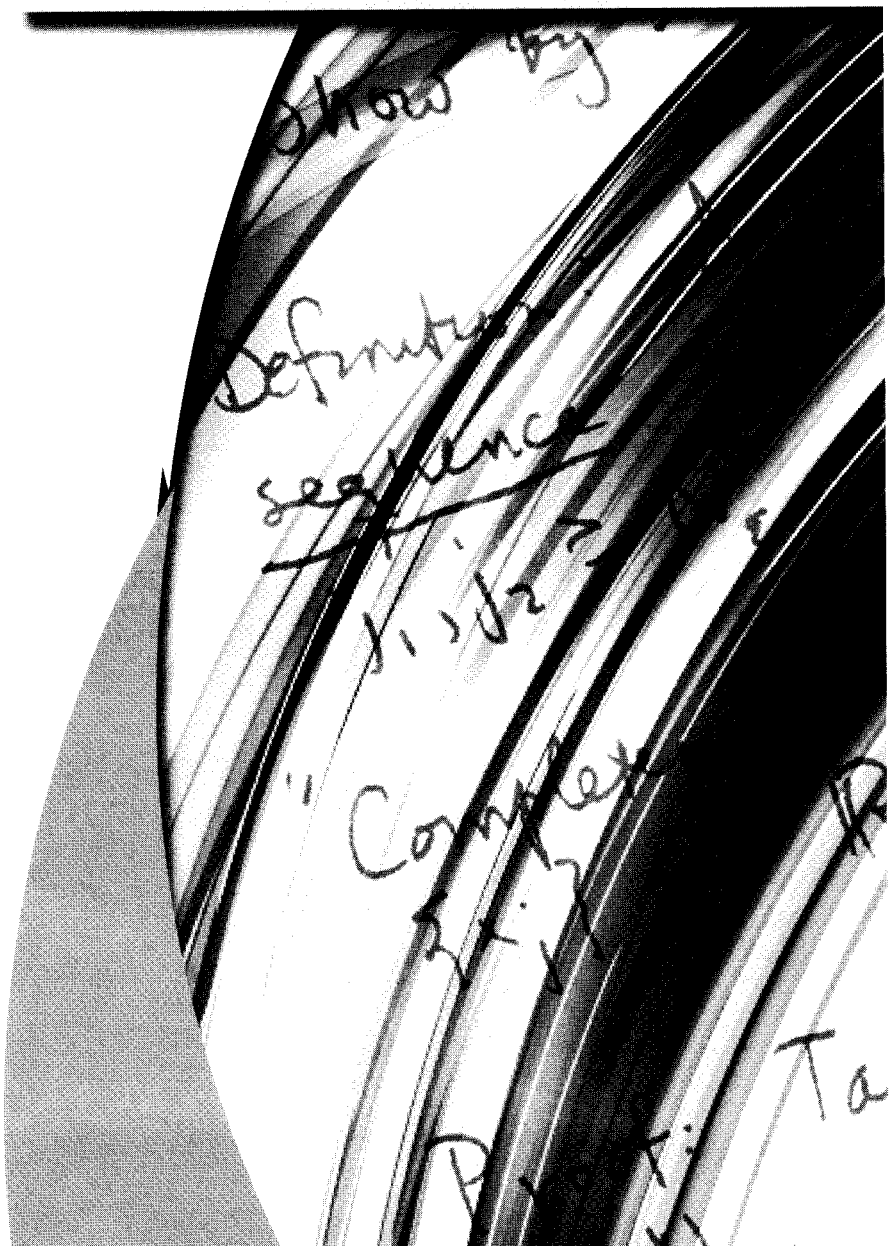
g) Dadas tres líneas rectas l_1, l_2 y l_3 coplanares, si l_1 y l_2 y son perpendiculares a l_3, entonces son paralelas entre sí.

h) En una fiesta en que hay 53 personas, al menos dos de ellas cumplen años en la misma semana.

i) Para todo entero m y todo natural n, m es congruente a n módulo n si y sólo si n divide a m.

j) Existe $m \in N$ tal que para todo $n \in N$, $\dfrac{1}{2n + 1} > \dfrac{1}{mn}$

2 Introducción a la lógica matemática



2. Introducción

La Matemática es una disciplina compleja: es usada para describir y modelar los objetos del mundo real y las leyes que lo rigen, es utilizada como una herramienta fundamental para resolver problemas, en todas las ciencias y en la tecnología, se establece como una abstracta ciencia deductiva y además como un arte donde se crean y desarrollan bellas teorías y demostraciones.

La deducción matemática y la lógica se encuentran muy cercanas entre sí relativamente, ya que el lenguaje de la deducción es requerido para ser preciso, y los símbolos de la lógica le quitan ambigüedad a nuestro lenguaje.

Modernamente la lógica se ha convertido en una materia no solo profunda, sino de gran amplitud y aplicación a otras ciencias. Por otro lado, en la medida en que usted avanza en sus estudios, necesita usar cada vez más correctamente el lenguaje matemático para poder seguir avanzando. Cuando usted explica algo, construye un argumento para ello. Elementos básicos para analizar y usar el lenguaje matemático, así como la misma estructura para la construcción de argumentos sean matemáticos o no, se encuentran en la lógica simbólica.

El estudio de la lógica se remonta al siglo IV a.c. cuando Aristóteles la puso a la cabeza de su sistema filosófico como materia indispensable para cualquier ciencia. La lógica aristotélica se mantuvo casi inalterable hasta el siglo XVI, cuando prácticamente es ignorada y se mantiene sin jugar ningún papel relevante en el desarrollo de las ciencias hasta el siglo XIX.

La Lógica Matemática, como hoy la entendemos, se fundamenta inicialmente en los trabajos de Frege y Peano. Un aspecto muy importante de estos trabajos fue que surgieron como una necesidad en el proceso de formalización de la Matemática, pues el Cálculo Infinitesimal, que Newton y Leibniz trazaron con gran imaginación y que después desarrollaron Cauchy, Gaus y otros, tuvo que ser precisado en la medida que se usaban conceptos más generales y abstractos.

Dedekind, Riemann, Weierstrauss y otros fueron sistematizando la Matemática hasta el punto de dejarla "construida", esencialmente teniendo como principio los números naturales y las propiedades elementales de conjuntos. Cantor, por su parte, desarrolló la base de la Teoría de Conjuntos, la cual inició llena de contradicciones que confirmaron la necesidad de la lógica, como herramienta de la matemática, y parte esencial de sus fundamentos.

En el desarrollo de la lógica matemática también estuvieron presentes grandes dificultades: el sistema de Frege, mediante el cual se pretendía regular el razonamiento matemático, tenía contradicciones. Con el tiempo se fueron haciendo modificaciones, como los Principia Matemática de Whitehead y Russel, de gran complejidad lógica, a la cual le siguieron muchas teorías, destacándose entre ellas "La Teoría de Conjuntos" de Zérmelo y Fraenkel, así como la de von Neumann-Bernays-Godel. Ambas constan de unos principios básicos, axiomas, y unas reglas precisas de demostración, que permiten deducir los teoremas conocidos hasta el momento de la Matemática sin contradicción.

No se puede poner en duda la importancia en la Matemática de la Teoría de la Demostración y de la Metodología para la deducción de teoremas a partir de axiomas. Con el desarrollo de la destreza en los razonamientos deductivos se puede proporcionar la base para estudios de Matemática más profundos y penetrantes, sin embargo, solo han tenido un interés secundario en muchos planes de enseñanza.

En este segundo capítulo, donde se hace una introducción de la Lógica Matemática, estudiamos el álgebra de proposiciones, los cuantificadores, el cálculo de predicados, un conjunto de reglas llamadas reglas de inferencia, la inferencia con cuantificadores y diversas técnicas o métodos de prueba. Además hacemos énfasis en un uso correcto del lenguaje, en una simbolización adecuada y en estrategias generales para hacer una demostración.

2.1. El álgebra de proposiciones

En lógica una oración declarativa es una **proposición**, la cual se le llama **atómica** si es simple lo que asevera y, **compuesta o molecular** si no lo es. Las **proposiciones compuestas** se construyen usando un conjunto fijo de palabras que conectan proposiciones tanto atómicas como compuestas.

2.1.1. Conectivos lógicos

Una de las contribuciones de la lógica a la economía y claridad de los discursos matemáticos, es la paternidad en encontrar, que las oraciones matemáticas pueden ser clasificadas usando un conjunto pequeño de palabras conectivas, las cuales llamaremos, como es usual, **conectivos lógicos**. Los conectivos lógicos más usados en Matemática son: **y, o, no, si...entonces, si y sólo si.**

Para comprender **cómo la proposición compuesta está formada por sus partes atómicas,** usamos la técnica de simbolizar lógicamente la proposición y analizar su forma estructural independiente de su contenido. Para esto usamos letras mayúsculas para las proposiciones,

llamadas proposiciones variables, y símbolos especiales para establecer los conectivos. La expresión que se obtiene es llamada: **fórmula proposicional.**

En la lógica clásica, que es la que estamos estudiando, una proposición tiene que ser o falsa, o verdadera, lo cual constituye su **valor de verdad.** La tabla que se forma, atendiendo a todas las combinaciones posibles de los valores de verdad de las partes atómicas de una fórmula proposicional, se denomina "tabla de verdad" de dicha fórmula.

2.1.2.1 Tablas de verdad de las fórmulas proposicionales compuestas más simples que se obtienen con los conectivos lógicos, las cuales definen a los conectivos

Conjunción (y). El símbolo que se usa para la conjunción es $\wedge$.

P	Q	P∧Q
V	V	V
V	F	F
F	V	F
F	F	F

Disyunción (o). El símbolo que se usa para la disyunción es $\vee$.

P	Q	P∨Q
V	V	V
V	F	V
F	V	V
F	F	F

Negación (no). El símbolo que se usa para la negación es $\neg$.

P	$\neg$P
V	F
F	V

Condicional (si...entonces). El símbolo que se usa para la condicional es $\rightarrow$.

P	Q	P$\rightarrow$Q
V	V	V
V	F	F
F	V	V
F	F	V

P se llama el antecedente y Q el consecuente en la condicional P$\rightarrow$Q.

Bicondicional (si y sólo si). La bicondicional se simboliza por $\leftrightarrow$

P	Q	P$\leftrightarrow$Q
V	V	V
V	F	F
F	V	F
F	F	V

2.1.2. Agrupamiento y paréntesis, computación del valor de verdad

Es frecuente encontrar proposiciones que tienen más de un conectivo. Los conectivos pueden ser usados con proposiciones compuestas de la misma forma que con atómicas. En todos los casos habrá uno que es el **"mayor"**, a ese se le llama **dominante**, ya que actúa sobre toda la proposición.

Una proposición con la forma ( ) $\wedge$ ( ) es una conjunción, no importa si el contenido de cada paréntesis es atómico o compuesto. Por ejemplo: $(P \vee Q) \wedge R$ es una conjunción a pesar que una de las partes que la componen sea una disyunción.

Los paréntesis son los símbolos de puntuación de la lógica. Las proposiciones en que no aparecen conectivos lógicos no requieren de paréntesis.

Adoptando algunas reglas simples acerca de la "potencia" de los conectivos lógicos, se pueden eliminar algunos de los paréntesis en las proposiciones simbolizadas:

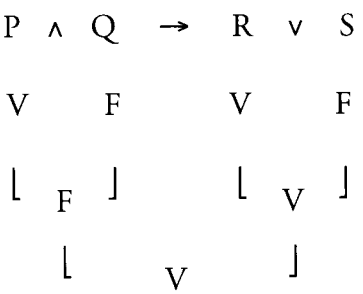
- **Regla 1:** El $\rightarrow$ es el más potente de los conectivos lógicos.
- **Regla 2:** El signo de negación $\neg$ es más débil que cualquiera de los otros cuatro.
- **Regla 3:** Tienen igual potencia: a) $\wedge$ y $\vee$
  b) $\leftrightarrow$ y $\rightarrow$

Ejemplo:

Analicemos la fórmula proposicional: $(P \wedge Q) \rightarrow (R \vee S)$. Suponemos que los valores de verdad de P y R son verdaderos y los de Q y S son falsos.

Primeramente notamos que los paréntesis no son necesarios atendiendo a las reglas dadas anteriormente, en particular la regla 1, por lo que podemos reescribir esa proposición en forma equivalente como $P \wedge Q \rightarrow R \vee S$.

Para encontrar el valor de verdad sólo necesitamos una línea de su tabla de verdad, la computación puede ser organizada en la forma de un diagrama como sigue:



Notemos que la proposición, la cual es una condicional, con los valores de verdad supuestos es verdadera.

2.1.3. El álgebra de proposiciones

Al introducir las fórmulas proposicionales, nosotros hemos abstraído la forma de la proposición respecto a su contenido. En esta sección veremos que las fórmulas proposicionales pueden ser manipuladas algebraicamente y que sus propiedades pueden ser aplicadas a oraciones matemáticas muy útilmente.

Comencemos identificando las que tienen valor de verdad constante.

Definición de tautología. Sea F una fórmula proposicional. Entonces F es llamada una tautología, si y sólo si, F tiene valor de verdad verdadero para toda posible combinación de valores de verdad de sus proposiciones variables componentes.

Ejemplos. Son tautologías las siguientes fórmulas:

- $P \rightarrow P$
- $P \vee \neg P$
- $P \leftrightarrow P$

Definición de equivalencia lógica. Sean F y G dos fórmulas proposicionales. Se dice que F y G son equivalentes, y esto se denota por $F \Leftrightarrow G$, si $F \leftrightarrow G$ es una tautología.

Ejemplos:

- P y $\neg\neg P$ son equivalentes, es decir, $P \Leftrightarrow \neg\neg P$
- $P \rightarrow Q$ y $\neg P \vee Q$ son equivalentes, es decir, $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$

Definición de implicación lógica. Sean F y G dos fórmulas proposicionales. Se dice que F implica lógicamente a G, y esto se denota por $F \Rightarrow G$, si $F \rightarrow G$ es una tautología.

Ejemplos. Son implicaciones lógicas las siguientes:

- $P \wedge Q \Rightarrow P$
- $P \Rightarrow P \vee Q$

El siguiente teorema recoge algunas de las propiedades básicas de los conectivos lógicos. Los nombres de estas propiedades son similares a

los correspondientes para las propiedades de la adición y multiplicación de números reales.

Teorema 2.1.4.1. (Propiedades algebraicas de los conectivos lógicos)

Sean P, Q y R fórmulas proposicionales. Entonces se tienen las siguientes equivalencias:

1. $P \wedge Q \Leftrightarrow Q \wedge P$,	conmutatividad de la conjunción.
2. $P \vee Q \Leftrightarrow Q \vee P$,	conmutatividad de la disyunción.
3. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$,	asociatividad de la conjunción.
4. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$,	asociatividad de la disyunción.
5. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$,	Distributividad de la disyunción respecto a la conjunción.
6. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$,	Distributividad de la conjunción respecto a la disyunción.
7. $P \Leftrightarrow \neg\neg P$	Doble negación.

Las demostraciones de estas propiedades pueden hacerse usando tablas de verdad.

Nota. Hemos visto que probar a través de la definición, usando la definición de dos fórmulas proposicionales que son equivalentes, se reduce a probar que la bicondicional entre ellas es una tautología. Para ello, según su definición, basta hacer su tabla de verdad, y comprobar que cada una de todas sus filas concluye en verdadera.

Atendiendo al carácter transitivo de la equivalencia de proposiciones, es decir, si $P \Leftrightarrow Q$ y $Q \Leftrightarrow R$, entonces $P \Leftrightarrow R$, podemos obtener otra forma de probar que dos proposiciones son equivalentes.

Ejemplo:

Supongamos que se probó, en el ejemplo de equivalencia lógica, que $P \rightarrow Q$ y $\neg P \vee Q$ son equivalentes.

Probemos ahora que $P \vee Q$ y $\neg P \rightarrow Q$ también lo son:

Se tiene que $P \vee Q \Leftrightarrow \neg\neg P \vee Q$, por doble negación, y esta última equivale a $\neg P \rightarrow Q$, por lo supuesto probado en el ejemplo.

Ahora podemos concluir, por la transitividad de ($\Leftrightarrow$), que $P \vee Q \Leftrightarrow \neg P \rightarrow Q$.

Teorema 1.1.4.2. (formas relativas de una condicional)

Sean P y Q fórmulas proposicionales, entonces:

1. $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
2. $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$.

Demostremos 2:

$\neg Q \rightarrow \neg P \Leftrightarrow \neg\neg Q \vee \neg P$ por 1

$\Leftrightarrow Q \vee \neg P$ por doble negación

$\Leftrightarrow \neg P \vee Q$ por conmutatividad

$\Leftrightarrow P \rightarrow Q$ por 1.

Nota: La equivalencia 2 fundamenta el método contrapositivo de demostración, ¿por qué?

Teorema 1.1.4.3. (de la bicondicional)

Sean P y Q fórmulas proposicionales, entonces:
$P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$.

La demostración se puede hacer, y es inmediata, mediante tablas de verdad.

Teorema 1.1.4.4. (sobre negación) (leyes de Morgan)

Sean P y Q fórmulas proposicionales, entonces:

1. $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
2. $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

La demostración se puede hacer, y es inmediata, mediante tablas de verdad.

El siguiente resultado es muy usado en la construcción de demostraciones en matemática.

Teorema 1.1.4.5. (de transportación de antecedentes)

Sean P, Q, R fórmulas proposicionales, entonces: $P\rightarrow(Q\rightarrow R) \Leftrightarrow (P\wedge Q)\rightarrow R$

Demostración.

$P\rightarrow(Q\rightarrow R) \Leftrightarrow \neg P\vee(Q\rightarrow R)$		por 1 de formas relativas de una condicional
	$\Leftrightarrow \neg P\vee(\neg Q\vee R)$	por 1 de formas relativas de una condicional
	$\Leftrightarrow (\neg P\vee\neg Q)\vee R$	por asociatividad de la disyunción
	$\Leftrightarrow \neg(P\wedge Q)\vee R$	por ley de Morgan
	$\Leftrightarrow P\wedge Q\rightarrow R$	por 1 de formas relativas de una condicional

Por tanto, $P\rightarrow(Q\rightarrow R) \Leftrightarrow P\wedge Q\rightarrow R$ atendiendo a la transitividad de ($\Leftrightarrow$).

2.1.4. Ejercicios resueltos

1. Desarrollar la tabla de verdad de la fórmula proposicional $P \wedge Q \rightarrow P \vee R$. ¿Qué puede concluir?

Solución

P	Q	R	$P \wedge Q$	$P \vee R$	$P \wedge Q \rightarrow P \vee R$
V	V	V	V	V	V
V	V	F	V	V	V
V	F	V	F	V	V
V	F	F	F	V	V
F	V	V	F	V	V
F	V	F	F	F	V
F	F	V	F	V	V
F	F	F	F	F	V

La fórmula proposicional $P \wedge Q \rightarrow P \vee R$ es una tautología.

2. Diga qué tipo de proposición es $\neg P \wedge Q \rightarrow R \vee S$ atendiendo al signo dominante y luego use paréntesis para formar, con los elementos de la función proposicional anterior una nueva proposición que sea:

   a) Una negación
   b) Una conjunción
   c) Una disyunción

Solución:

La proposición inicial es una condicional, pues el conectivo dominante es $\rightarrow$

- $\neg(P \wedge Q \rightarrow R \vee S)$ es una negación.
- $\neg P \wedge (Q \rightarrow R \vee S)$ es una inclusión.
- $(\neg P \wedge Q \rightarrow R) \vee S$, también se logra en $\neg(P \wedge Q \rightarrow R) \vee S$, son disyunciones.

3. Pruebe que $P \rightarrow Q$ y $\neg P \vee Q$ son equivalentes.

Solución:

P	Q	$\neg P$	$P \rightarrow Q$	$\neg P \vee Q$	$(P \rightarrow Q) \leftrightarrow \neg P \vee Q$
V	V	F	V	V	V
V	F	F	F	F	V
F	V	V	V	V	V
F	F	V	V	V	V

Como la bicondicional entre ellas es una tautología, entonces son equivalentes.

4. Pruebe que $P \rightarrow (Q \rightarrow R) \Leftrightarrow \neg(P \wedge \neg R) \vee \neg Q$

Solución:

$P \rightarrow (Q \rightarrow R) \Leftrightarrow P \wedge Q \rightarrow R$ Transportación de antecedentes

$\Leftrightarrow \neg R \rightarrow \neg(P \wedge Q)$ 2 de formas relativas de una condicional

$\Leftrightarrow \neg R \rightarrow \neg P \vee \neg Q$ ley de Morgan

$\Leftrightarrow \neg\neg R \vee (\neg P \vee \neg Q)$ 1 de formas relativas de una condicional

$\Leftrightarrow R \vee (\neg P \vee \neg Q)$ Doble negación

$\Leftrightarrow (R \vee \neg P) \vee \neg Q$ Asociatividad de la disyunción

$\Leftrightarrow \neg\neg(R \vee \neg P) \vee \neg Q$ Doble negación

$\Leftrightarrow \neg(\neg R \wedge \neg\neg P) \vee \neg Q$ ley de Morgan

$\Leftrightarrow \neg(\neg R \wedge P) \vee \neg Q$ Doble negación

$\Leftrightarrow \neg(P \wedge \neg R) \vee \neg Q$ Conmutatividad de la conjunción

Por tanto, se ha probado la equivalencia.

2.1.5. Ejercicios propuestos

1. Construya una tabla de verdad para probar que cada fórmula proposicional dada es una tautología:

   a) $P \wedge Q \rightarrow P$, b) $P \rightarrow P \vee Q$, c) $[P \wedge (P \rightarrow Q)] \rightarrow Q$

2. Construya una tabla de verdad para probar que las siguientes pares de formas proposicionales son equivalentes:

   a) $P \vee (Q \wedge R)$ y $(P \vee Q) \wedge (P \vee R)$,
   b) $P \wedge (Q \vee R)$ y $(P \wedge Q) \vee (P \wedge R)$

3. Use el álgebra de proposiciones para probar cada una de las siguientes equivalencias lógicas:

   a) $P \leftrightarrow Q \Leftrightarrow \neg P \leftrightarrow \neg Q$,
   b) $\neg(P \leftrightarrow Q) \Leftrightarrow (P \wedge \neg Q) \vee (Q \wedge \neg P)$,

c) $\neg[\neg Q \rightarrow \neg P] \Leftrightarrow P \wedge \neg Q$,
d) $(P \rightarrow R) \wedge (Q \rightarrow R) \Leftrightarrow (P \vee Q) \rightarrow R$,
e) $\neg(P \wedge Q) \Leftrightarrow P \rightarrow \neg Q$, f) $\neg(P \leftrightarrow Q) \Leftrightarrow P \leftrightarrow \neg Q$.

4. Forme la negación de cada proposición usando, si es necesario, las leyes de Morgan para encontrar la forma más usada o útil.

   a) Todos los números m,n, y k son enteros,
   b) El número 3 es impar y primo,
   c) El número n es un cuadrado perfecto o es primo,
   d) El número 9 es impar, pero no es primo,
   e) Si a.b=0, entonces a=0 o b=0,
   f) Si a>0 y b<0, entonces a+b>0 sólo si $a>|b|$
   g) Si a es impar, entonces su cuadrado es impar, e inversamente.

2.2. Cuantificadores. Cálculo de predicados

En el estudio de la estructura interna de muchas proposiciones no es suficiente el cálculo de proposiciones estudiado hasta ahora, y se requiere introducir algún lenguaje que lo permita. Por ejemplo: todos los números reales que son menores que 1 son menores que 2. ¿Cómo, aceptando la veracidad de la proposición anterior, se puede hacer una demostración formal lógica para probar que al ser $0 < 1$ entonces $0 < 2$?

Para estudiar la estructura interna de proposiciones como la del párrafo de arriba, vamos a introducir los conceptos de predicado y de cuantificador.

2.2.1. Predicados

Una oración como "*n* es un número primo", en la cual el sujeto no está especificado, es llamada un **predicado** en lógica. La letra "*n*", la cual establece el sujeto de la oración, es llamada un objeto variable.

Un predicado simple, llamado predicado variable, se simboliza en lógica mediante una letra mayúscula seguida de uno o más objetos variables en una lista entre paréntesis. Por ejemplo, P(x) puede representar al predicado: "x es menor que 1", (x<1).

Predicados compuestos son representados usando los símbolos usuales para los conectivos lógicos, junto con las variables del predicado. Por ejemplo: P(x) → Q(x) puede representar el predicado compuesto "si x<1 entonces x<2".

La proposición "2 es un número primo", la cual se obtiene de sustituir n por 2 en el predicado "n es un número primo", tiene un valor de verdad que dependió de la sustitución que se realizó.

En general se requiere de un conjunto cuyos elementos son los posibles sustitutos de los objetos variables del predicado. Este conjunto es llamado el Universo de Discurso. Un conjunto apropiado para ser el Universo de Discurso, en el predicado anterior, es el conjunto de números naturales.

Conjuntos numéricos muy usados en el campo de las matemáticas son:

- conjunto de números complejos, $\boldsymbol{C}$
- conjunto de números reales, $\boldsymbol{R}$
- conjunto de números racionales, $\boldsymbol{Q}$
- conjunto de números enteros, $\boldsymbol{Z}$
- conjunto de números naturales, $\boldsymbol{N}$

Para simbolizar que un elemento x pertenece al conjunto A usamos el símbolo $\in$ y leemos que x pertenece a A cuando escribimos $x \in A$.

2.2.2. El Cuantificador Universal

Es fácil ver que diferentes sustituciones en un predicado como "n es un número primo", pueden dar como resultado proposiciones con diferentes valores de verdad.

Cuando nosotros describimos el predicado $(x+1)^2 = x^2+2x+1$ como una identidad en álgebra, entendemos que cualquier sustitución que se haga de la x por un elemento específico del universo de discurso, lo convierte en una proposición verdadera, esto es así cuando el universo de discurso es uno cualquiera de los conjuntos numéricos anteriores, por ejemplo $\boldsymbol{R}$. Esta es la condición para que la proposición, "Para todo número real x, $(x+1)^2 = x^2+2x+1$", sea verdadera.

En lógica necesitamos una regla precisa que determine el valor de verdad de este tipo de proposiciones.

Definición de Cuantificador Universal. Sea P(x) un predicado con universo de discurso U. Entonces, "Para todo x, P(x)", denotada por "$\forall$x, P(x)", es una proposición cuyo valor de verdad es verdadero si para cualquier sustitución del objeto variable x que hagamos en P(x) por un elemento a$\in$U, la proposición resultante P(a) es verdadera y, la proposición "$\forall$x, P(x)", es una proposición cuyo valor de verdad es falso, en cualquier otro caso.

El símbolo "$\forall$" se lee "para todo" y denota al símbolo llamado "el cuantificador universal". En "$\forall$x, P(x)" decimos que el objeto variable x ha sido cuantificado en el predicado P(x) por el cuantificador universal.

Otras frases en español que se utilizan para leer el cuantificador universal son: "cualquiera sea", "para cada", etc.

Ejemplo:

"Todos los números reales que son menores que 1 son menores que 2", se puede expresar como: "$\forall x,\ x < 1 \rightarrow x < 2$".

Si denotamos "P(x): x<1 y Q(x): x<2", entonces, sin usar simbología matemática, nos queda: "$\forall$x, P(x) $\rightarrow$ Q(x)".

Aquí no aparece explícitamente el universo de discurso en la expresión dada en términos lógicos, esto ocurre cuando se está asumiendo uno por algún tipo de acuerdo anterior en el contexto, por ejemplo, si estamos estudiando o trabajando con el conjunto de números reales, cuando asumimos que el universo de discurso es el conjunto de los números reales, no necesitamos escribirlo explícitamente.

2.2.3. El Cuantificador Existencial

La proposición "la ecuación x-1=0 tiene solución real" es verdadera matemáticamente. En el contexto de nuestro análisis de predicados, decimos que al menos una sustitución del objeto variable en el predicado x-1=0 por un elemento del universo de discurso, el conjunto de números reales R, dá como resultado una proposición verdadera.

Otra vez nosotros tenemos formada una proposición donde se cuantifica un predicado.

Definición del Cuantificador Existencial. Sea P(x) un predicado con universo de discurso U. Entonces "existe al menos un x, tal que P(x)",

denotada por: "$\exists x$, P(x)", es verdadera, si al menos P(a) es verdadera para alguna sustitución $a \in U$ del objeto variable x en el predicado P(x) y, "$\exists x$, P(x)" es falsa, en cualquier otro caso.

El símbolo $\exists$, se lee existe y es usado para denotar el cuantificador existencial; en "$\exists x$, P(x)" decimos que el objeto variable x ha sido cuantificado en el predicado P(x) por el cuantificador existencial.

Otras frases usadas en español que expresan el cuantificador existencial son: "hay al menos un", "hay un", "existe al menos un", "para algún", etc.

Ejemplo:

Si el predicado P(x) viene definido por x-1=0, entonces la proposición: "$\exists x$, P(x)" es verdadera, pues P(1) es verdadera. Aquí, igual que antes, hemos asumido que el universo de discurso es el conjunto de números reales, aunque éste no aparece explícitamente en la expresión en términos lógicos.

2.2.4. Predicados con dos o más objetos variables

Si dos o mas variables ocurren en un predicado, cada una de ellas puede ser cuantificada por el cuantificador universal o el existencial. Es indispensable usar tantos cuantificadores como variables haya para transformar el predicado en una proposición o en una función proposicional.

Las reglas para determinar el valor de verdad de la proposición resultante son aplicadas de izquierda a derecha.

Ejemplos:

1. "$(\forall x)(\exists y)$, P(x,y)" será verdadera si la proposición "$\exists y$, P(a,y)" es verdadera para cada valor "a" arbitrario que se le asigne a la variable "x" en su universo de discurso. Esto último ya sabemos lo que significa. Notemos que el valor "b" que debe tomar la variable "y" en su universo de discurso para hacer verdadera P(a,b) depende del valor "a", es decir, a diferentes valores que se le asigne a la variable "x", en general, serán diferentes los valores que debe tomar la variable "y".

2. "$(\exists y)(\forall x)$, P(x,y)" será verdadera si al menos hay un valor fijo "b" en el universo de discurso de la variable "y" para el cual la proposición "$\forall x$, P(x,b)" es verdadera. Notemos que ese valor "b" de la variable "y" no depende del valor que tome la variable "x", es decir, debe servir el mismo valor "b" para todos los valores que pueda tomar la variable "x" en su universo de discurso.

Observaciones:

1. En el caso que dos variables tengan el mismo universo de discurso, y ambas se vayan a cuantificar por el mismo cuantificador, se puede usar el cuantificador una sola vez y escribir a continuación ambas variables separadas por comas. Por ejemplo, es lo mismo decir:

   i) $(\forall x,y)$, $P(x,y)$ y $(\forall x)(\forall y)$, $P(x,y)$,
   ii) $(\exists x,y)$, $P(x,y)$ y $(\exists x)(\exists y)$, $P(x,y)$

2. Si queremos destacar explícitamente el universo de discurso U, lo podemos hacer, respectivamente para cada cuantificador, de la siguiente forma: $(\forall x \in U), P(x)$ y $(\exists x \in U), P(x)$

2.2.5. Negación de proposiciones encabezadas por cuantificadores

Recalcamos que una proposición es verdadera si y sólo si su negación es falsa; lo cual se deduce inmediatamente del hecho que el valor de verdad de una proposición es siempre el opuesto al de su negación.

Atendiendo a lo anterior se obtiene el siguiente resultado.

Teorema 2.2.5.1. (de negación de cuantificadores)

Sea P(x) un predicado con universo de discurso U. Entonces son equivalentes las siguientes pares de proposiciones:

- $\neg(\forall x, P(x))$ y $\exists x, \neg P(x)$
- $\neg(\exists x, P(x))$ y $\forall x, \neg P(x)$

La demostración es una reiteración del significado de cada proposición.

Ejemplos:

1. Es lo mismo decir que no todas las personas son valientes, a decir que existe al menos una persona que no es valiente.

2. $\neg(\exists x, x^2=-1)$, es lo mismo que decir, $\forall x, x^2 \neq -1$

2.2.6. Ejercicios resueltos

1. Simbolice completamente, destacando un universo de discurso, U, adecuado:

   a) Todos los gorriones son pájaros.
   b) Ningún tirano es una persona justa.
   c) Sólo las personas son racionales.
   d) Todos los pájaros y todos los peces son animales.
   e) No todos los hombres son inteligentes.

Respuestas de 1:

a) G(x): x es un gorrión
   P(x): x es un pájaro
   U: el conjunto de animales $\quad \forall x,\ G(x) \rightarrow P(x)$

b) T(x): x es un tirano
   J(x): x es justo
   U: el conjunto de personas $\quad \forall x,\ T(x) \rightarrow \neg J(x)$

c) P(x): x es persona
   R(x): x es racional
   U: el conjunto de seres vivos $\quad \forall x,\ R(x) \rightarrow P(x)$

d) P(x): x es un pájaro
   F(x): x es un pez
   A(x): x es un animal
   U: el conjunto de seres vivos $\quad \forall x,\ [P(x) \rightarrow A(x)] \wedge [F(x) \rightarrow A(x)]$

e) H(x): x es un hombre
   I(x): x es inteligente
   U: el conjunto de seres vivos $\quad \neg(\forall x,\ H(x) \rightarrow I(x))$

■ *Nota.* $\neg(\forall x, H(x) \rightarrow I(x))$ *equivale a decir* $\exists x, H(x) \wedge \neg I(x)$

La equivalencia anterior se obtiene inmediatamente usando la negación de cuantificadores y que:

$\neg(H(x) \rightarrow I(x)) \Leftrightarrow \neg(\neg H(x) \wedge I(x))$ por 1 de teorema 2.1.4.2.
$\Leftrightarrow H(x) \wedge \neg I(x)$ por teorema 2.1.4.4. (leyes de Morgan)

En español se diría: existen hombres que no son inteligentes, lo cual equivale a decir que no todos los hombres son inteligentes.

2.2.7. Ejercicios propuestos

1. Asuma que ser particular, ser eficiente, ser artístico y ser bonito tienen significado matemático en el conjunto de números naturales y use el diccionario siguiente en lo que sigue:

   P(x): x es particular
   E(x): x es eficiente
   A(x): x es artístico.
   B(x): x es bonito.

   A. Traduzca cada proposición en símbolos lógicos, usando como universo de discurso el conjunto de números naturales:

      a) Todo número eficiente es artístico.
      b) Hay números artísticos que son bonitos
      c) Hay números particulares que no son artísticos.
      d) Hay números que son bonitos y son eficientes, pero no todos los eficientes son bonitos.
      e) Todo número es artístico o particular

B. Traduzca cada proposición al español, teniendo en cuenta el diccionario anteriormente dado.

a) $(\forall x \in N)[P(x) \rightarrow B(x)]$
b) $(\exists x \in N)\{[P(x) \wedge B(x)] \wedge \neg E(x)\}$
c) $(\forall x \in N)[A(x) \vee E(x) \rightarrow B(x) \vee P(x)]$

2. Forme la negación de cada uno de los enunciados del ejercicio anterior, tanto en forma simbólica como en español, y empleé las propiedades que necesite para expresar esa negación en la forma mas usada o útil.

3. Forme la negación de cada una de las siguientes proposiciones y decida, usando sus conocimientos aritméticos y algebraicos, sus valores respectivos de verdad.

a) $(\exists x, y \in R)[\sqrt{x^2 + y^2} = x + y]$
b) $(\forall x, y \in R)[\sqrt{x^2 + y^2} = x + y]$
c) $(\forall x, y \in R)[x + y = 0 \rightarrow x = 0 \wedge y = 0]$
d $(\exists x \in R)[x^2 < x]$
e) $(\forall x, y \in R)[x^2 + y^2 \geq 2y]$

2.3. Reglas de inferencia

En este punto estudiaremos las reglas básicas que se siguen para establecer un razonamiento o argumento desde el punto de vista de su estructura, es decir, haciendo abstracción de su contenido. Paralelamente veremos la estructura de una demostración lógica formal, la cual es, en esencia,

la estructura de una demostración en matemática. Por último veremos algunas técnicas de demostración.

Un razonamiento o argumento en lógica está compuesto por un conjunto de proposiciones, llamadas premisas y una proposición, llamada conclusión. El conjunto de premisas debe ser **consistente**, es decir, **debe poder existir una asignación de certeza mediante la cual todas ellas sean verdaderas.**

Una demostración lógica de que un argumento es válido está formada por un conjunto ordenado de proposiciones, cada una de las cuales para ser incluida en dicho conjunto ordenado tiene que cumplir con alguna cierta regla que le permite su inclusión en ese orden y, donde la última proposición es la conclusión del razonamiento o argumento.

Las **reglas de inferencia** son las reglas que permiten incluir proposiciones en una demostración lógica de un argumento, es decir, en el conjunto ordenado de proposiciones que conforman la demostración lógica de su validez.

Recordemos que como estamos haciendo abstracción de los contenidos de las proposiciones, aunque digamos proposiciones debe sobreentenderse que estamos diciendo fórmulas proposicionales.

Por supuesto, un principio básico que deben poseer estas reglas es que si las premisas de un argumento son todas verdaderas y el argumento es válido, entonces la conclusión tiene que ser verdadera.

2.3.1. Reglas básicas de inferencia

A continuación vamos a enunciar un conjunto de reglas, las cuales en nuestro contexto son las reglas de inferencia básicas que vamos a considerar como válidas para su uso en las demostraciones lógicas.

- **Regla de la Premisa.** Sea P una fórmula proposicional. Entonces, si P es una premisa, P puede ser incluida en la demostración.

- **Regla de la Tautología.** Sea P una fórmula proposicional. Entonces, si P es una tautología, P puede ser incluida en cualquier demostración.

- **Regla de la Equivalencia.** Sean P y Q fórmulas proposicionales y $P \Leftrightarrow Q$. Entonces, si P ha sido incluido en una demostración, Q puede ser incluido.

- **Regla del Modus Poniendo Ponens (PP).** Sean P y Q fórmulas proposicionales. Entonces, si P y $P \rightarrow Q$ han sido incluidas en una demostración, Q puede ser incluido también.

- **Regla del Modus Tolliendo Ponens o de la disjunción (TP).** Sean P y Q fórmulas proposicionales. Entonces, si $P \vee Q$ y $\neg P$ han sido incluidas en una demostración, Q puede ser incluida también.

- **Regla del Modus Tolliendo Tollens (TT).** Sean P y Q fórmulas proposicionales. Entonces, si $P \rightarrow Q$ y $\neg Q$ han sido incluidas en una demostración, $\neg P$ puede ser incluida también.

- **Regla de la Simplificación (S).** Sean P y Q fórmulas proposicionales. Entonces, si $P \wedge Q$ ha sido incluida en una demostración, tanto P como Q pueden ser incluidas también.

- **Regla de la Adjunción (A).** Sean P y Q fórmulas proposicionales. Entonces, si P y Q han sido incluidas en una demostración, $P \wedge Q$ puede ser incluida también.

- **Regla de la Adición (LA).** Sean P y Q fórmulas proposicionales. Entonces, si P ha sido incluida en una demostración, $P \vee Q$ puede ser incluida también.

- **Regla de la simplificación disyuntiva (DP).** Sea P una fórmula proposicional. Entonces, si $P \vee P$ ha sido incluida en una demostración, P puede ser incluida también.

> *Nota. Notemos que le estamos llamando reglas, pues no estamos interesados en que sean independientes unas de otras, es decir, algunas de las reglas que estamos dando pueden ser deducidas de otras que aparecen en dicho conjunto de reglas dado.*

Si estuviéramos haciendo un desarrollo formal de la lógica tendríamos que tener mucho más cuidado para definir los axiomas correspondientes de la teoría, los cuales harían el papel que para nosotros hacen las reglas.

2.3.2. Técnicas de demostración

En muchas ocasiones, en el argumento que queremos demostrar que es válido, la conclusión es una condicional, es decir, tiene la forma $P \rightarrow Q$.

Atendiendo al principio básico de la validez de un argumento, "si cada vez que las premisas son todas verdaderas la conclusión también tiene que ser verdadera", la regla llamada, "la prueba de la condicional", que

a continuación se describe, nos brinda un procedimiento o técnica para hacer tal tipo de demostraciones.

- **Prueba de la condicional (CP).** Sean P y Q fórmulas proposicionales. Si de introducir P como premisa, a un conjunto de premisas dados de un argumento, se logra incluir lógicamente a Q en una demostración, entonces se puede incluir, como consecuencia de las premisas originales del argumento, a $P \rightarrow Q$ en la demostración de su validez.

Ejemplos:

1. Sean P, Q y R fórmulas proposicionales. El argumento que tiene a $P \rightarrow Q$ y $Q \rightarrow R$ como premisas y a $P \rightarrow R$ como conclusión, es un argumento válido. **(Llamado: Regla del silogismo hipotético).**

Demostración:

1) $P \rightarrow Q$		Premisa
2) $Q \rightarrow R$		Premisa
3)	P	Premisa Introducida.
4)	Q	PP 1 y 3
5)	R	PP 2 y 4
6) $P \rightarrow R$		CP 3 y 5.

2. Sean P, Q, R, S y M fórmulas proposicionales. El argumento que tiene a $S \wedge (\neg P \vee M)$ y $M \rightarrow Q \vee R$ como premisas y a $P \rightarrow (\neg Q \rightarrow R)$ como conclusión, es un argumento válido.

Demostración:

1) $S \wedge (\neg P \vee M)$	Premisa
2) $M \rightarrow Q \vee R$	Premisa

3) ¬PvM			S 1
4)	P		Premisa Introducida
5)	¬¬P		Equivalencia 4
6)	M		TP 3 y 5
7)		¬Q	Premisa Introducida
8)		QvR	PP 2 y 6
9)		R	TP 7 y 8
10)	¬Q→R		CP 7 y 9
11) P→(¬Q→R)			CP 4 y 10.

Nota. Notemos que cada vez que se incluye una premisa introducida en la demostración, es decir, una premisa que no formaba parte de las premisas del argumento, la proposición que se incluye, y las subordinadas a ella, deben ocupar otra columna a la derecha. Así se van formando bloques de demostraciones subordinadas, pero al aplicar la prueba de la condicional logramos incluir, en el bloque principal de la demostración, una proposición del tipo P→Q.

Por otro lado, una fórmula proposicional como P∧¬P, la cual es siempre falsa, es llamada una **contradicción**. Como una contradicción es siempre falsa, no puede ser deducida de un conjunto de premisas que sea consistente. Esto justifica la siguiente regla, la cual es una técnica de demostración, llamada prueba indirecta o por contradicción.

- **Prueba Indirecta, (IP).** Sea P una fórmula proposicional. Si por introducirse como premisa la negación de P a un conjunto de premisas de un argumento para la demostración de su validez, se puede incluir lógicamente como consecuencia una contradicción, entonces P se deduce lógicamente del conjunto de premisas del argumento y, por tanto, puede incluirse en la demostración de que dicho argumento es válido.

Ejemplos:

1. Sean P, Q, R y S fórmulas proposicionales. El argumento que tiene a $P \vee Q$, $P \rightarrow R$ y $Q \rightarrow S$ como premisas, y a $R \vee S$ como conclusión, es un argumento válido. (llamada Regla del silogismo disyuntivo)

Demostración:

1)	$P \vee Q$	Premisa
2)	$P \rightarrow R$	Premisa
3)	$Q \rightarrow S$	Premisa
4)	$\neg(R \vee S)$	Premisa Introducida
5)	$\neg R \wedge \neg S$	Ley de Morgan en 4
6)	$\neg R$	S 5
7)	$\neg S$	S 5
8)	$\neg P$	TT 2 y 6
9)	$\neg Q$	TT 3 y 7
10)	$\neg P \wedge \neg Q$	A 8 y 9
11)	$\neg(P \vee Q)$	Ley de Morgan en 10
12)	$P \vee Q) \wedge \neg(P \vee Q)$	A 1 y 11
13)	$R \vee S$	IP o Contradicción 4 y 12.

Así queda demostrada la regla del sigolismo disyuntivo.

2. Se desea probar que P se sigue lógicamente de las premisas $\neg Q \vee R$, $\neg P \rightarrow \neg R$ y Q.

Demostración:

1)	$\neg Q \vee R$	Premisa
2)	$\neg P \rightarrow \neg R$	Premisa
3)	Q	Premisa
4)	$\neg P$	Premisa Introducida

5)	$\neg R$	PP 2 y 4
6)	$\neg Q$	TP 1 y 5
7)	$Q \wedge \neg Q$	A 3 y 6
8) P		IP o Contradicción 4 y 7.

2.3.3. Reglas con predicados y con cuantificadores

En lógica y en matemática se usa el símbolo = para conectar diferentes nombres de un mismo objeto. Esto motiva tener la siguiente regla:

- **Regla de la Sustitución.** Sea S un predicado que contiene el objeto variable o fijo x, y supongamos que x=z. Entonces, si S ha sido incluido en una demostración, el predicado que se forma de sustituir a x por z, en una o mas ocurrencias en S, puede ser incluido también.

  Las reglas de inferencia básicas estudiadas no incluyen el uso de cuantificadores. Para cada cuantificador veremos dos reglas o leyes: la de especificación y la de generalización.

- **Ley de Especificación Universal (UE).** Sea P(x) un predicado con universo de discurso U y $z \in U$. Entonces, si $\forall x$, P(x) ha sido incluido en una demostración, P(z) también puede ser incluido en ella.

Ejemplos:

1. El argumento que tiene a las proposiciones: todo número divisible por 2 es par, 4 es impar o divisible por 2 y 4 no es impar, como premisas, y que tiene a 4 es par como conclusión; es un argumento válido.

Primero simbolicemos:
P(x): x es divisible por 2, Q(x): x es par, R(x): x es impar.

Demostración:

1. $\forall x, P(x) \rightarrow Q(x)$	Premisa
2. $R(4) \vee P(4)$	Premisa
3. $\neg R(4)$	Premisa
4. $P(4) \rightarrow Q(4)$	Especificación Universal $4/x$ en 1.
5. P(4)	TP 2 y 3
6. Q(4)	PP 4 y 5.

2. El argumento que tiene a las proposiciones: todos los santiagueros son cibaeños, todos los cibaeños son dominicanos, y Miguel es santiaguero, como premisas, y a Miguel es dominicano como conclusión; es un argumento válido.

Primero simbolicemos:
P(x): x es santiaguero, Q(x): x es cibaeño, R(x): x es dominicano

Demostración:

1) $\forall x, P(x) \rightarrow Q(x)$	Premisa
2) $\forall x, Q(x) \rightarrow R(x)$	Premisa
3) P(Miguel)	Premisa
4) $P(Miguel) \rightarrow Q(Miguel)$	Especificación Universal $^{Miguel}/_{x}$ en 1.
5) Q(Miguel)	PP 3 y 4
6) $Q(Miguel) \rightarrow R(Miguel)$	Especificación Universal $^{Miguel}/_{x}$ en 2.
7) R(Miguel)	PP 5 y 6.

- **Ley de Generalización Universal (UG)**. Sea P(x) un predicado con universo de discurso U. Si y es un elemento general o arbitrario de U, es decir, no tiene especiales especificaciones, y P(y) ha

sido incluido en una demostración, entonces, $\forall x$, P(x) puede ser incluido también.

Ejemplos:

1. El argumento que tiene como premisas a $\forall x$, $x<1 \rightarrow x<2$ y $\forall x$, $x<2 \rightarrow x<3$, y tiene como conclusión a $\forall x$, $x<1 \rightarrow x<3$, es un argumento válido.

Demostración:

1) $\forall x$, $x<1 \rightarrow x<2$	Premisa
2) $\forall x$, $x<2 \rightarrow x<3$	Premisa
3) $x<1 \rightarrow x<2$	Especificación Universal x/x en 1.
4) $x<2 \rightarrow x<3$	Especificación Universal x/x en 2.
5) $x<1 \rightarrow x<3$	Silogismo hipotético 3 y 4.
6) $\forall x$, $x<1 \rightarrow x<3$	Generalización Universal en 5.

2. Todos los pájaros son animales, todos los ruiseñores son pájaros; por tanto, todos los ruiseñores son animales.

Simbolicemos:
P(x): x es un ruiseñor, Q(x): x es un pájaro, R(x): x es un animal

Demostración:

1) $\forall x$, $Q(x) \rightarrow R(x)$	Premisa
2) $\forall x$, $P(x) \rightarrow Q(x)$	Premisa
3) $P(x) \rightarrow Q(x)$	Especificación Universal x/x en 2
4) $Q(x) \rightarrow R(x)$	Especificación Universal x/x en 1
5) $P(x) \rightarrow R(x)$	Silogismo hipotético 3 y 4
6) $\forall x$, $P(x) \rightarrow R(x)$	Generalización Universal en 5.

Ley de la generalización existencial (EG). Sea P(x) un predicado y z un elemento de su universo de discurso. Entonces, si P(z) ha sido incluido en una demostración, $\exists x$, P(x), puede ser incluido también.

Ejemplos:

1. Sea P(x) un polinomio de variable x. Suponga que P(5)=0 es cierto. Entonces usted puede asumir como cierto que $\exists x$, P(x)=0.

2. Si en una graduación José se graduó con honores, podemos concluir que en esa graduación hubo al menos un graduado con honores.

Ley de especificación existencial (EE). Sea P(x) un predicado con universo de discurso U, Entonces, si ($\exists x$, P(x)) ha sido incluido en una demostración, P(a) puede ser incluida para algún $a \in U$ con propiedades especiales, no un miembro general de U.

Ejemplos:

1. En cálculo se prueba que existen funciones que son continuas pero que no son derivables en cero. Entonces un encabezamiento que diga "sea f una función continua y no derivable en cero" es posible y tiene sentido hacerse.

2. Si la proposición: "En esta graduación existen estudiantes que se graduaron con honores" es cierta, sabemos que en el predicado "x se graduó con honores", podemos sustituir la x por algún nombre que hace a la proposición resultante verdadera.

Prueba por casos.- Una técnica de demostración, muy usada en matemática, es la llamada prueba por casos, la cual está sustentada en la regla de inferencia que dice: si $P \vee Q$, $P \rightarrow R$ y $Q \rightarrow R$ han sido incluidos en una demostración, también puede ser incluida R.

Esta regla se puede deducir aplicando primero la regla del silogismo disyuntivo, mediante la cual se incluye a $R \vee R$, y después la simplificación disyuntiva con la que podemos concluir e incluir a R.

Ejemplo:

Sabemos que todo número entero es par o impar, es decir:

$$(\forall n \in Z)(\exists k \in Z),\ (n = 2k \vee n = 2k + 1)$$

Probemos que: $(\forall n \in Z)(\exists k \in Z),\ (n^2 = 4k \vee n^2 = 4k + 1)$ y para ello, haremos una demostración por casos como se haría en matemática:

Caso 1. Si n es par, entonces existe un entero k tal que $n = 2k$ y, por tanto, $n^2 = (2k)^2 = 4k^2$

Caso 2. Si n es impar entonces existe un entero k tal que $n = 2k + 1$ y, por tanto, $n^2 = (2k + 1)^2 = 4(k^2 + k) + 1$

Como k^2 y $k^2 + k$ son números enteros, queda probado que:
$(\forall n \in Z)(\exists k \in Z),\ (n^2 = 4k \vee n^2 = 4k + 1)$

2.3.4. La inducción matemática

Una técnica de demostración de la validez de un argumento de la forma $\forall n \in N,\ P(n)$, se basa en la propiedad inductiva de los naturales, la cual será estudiada con detenimiento en el capítulo V.

Esta propiedad dice: Sea $S \subseteq N$ cumpliendo con las propiedades siguientes:

1) $1 \in S$ y 2) Para todo n, si $n \in S$ entonces $n + 1 \in S$

Entonces se puede concluir que: $S = N$

Nota. La técnica consiste en probar que $P(1)$ *es verdadero y, que la proposición,* $\forall n \in N$, $P(n) \rightarrow P(n + 1)$ *también es verdadera; pues en dicho caso, habríamos probado que el conjunto* $S = \{n \in N: P(n)$ *es verdadero*$\}$ *coincide con todo el conjunto de números naturales, como una consecuencia de la propiedad inductiva enunciada más arriba.*

Ejemplo: Probemos que: $\left(1 + \frac{1}{n+2}\right)^{n+2} < n + 2$ para todo número natural n.

Demostración. Para $n = 1$, es verdadera, pues:

$$\left(1 + \frac{1}{1+2}\right)^{1+2} = \left(1 + \frac{1}{3}\right)^{3} = \left(\frac{4}{3}\right)^{3} = \frac{64}{27} = 2 + \frac{10}{27} < 3 = 1 + 2.$$

Supongamos que: $\left(1 + \frac{1}{n+2}\right)^{n+2} < n + 2$

Como $1 + \frac{1}{n+3} < 1 + \frac{1}{n+2}$, entonces:

$$\left(1 + \frac{1}{n+3}\right)^{n+3} < \left(1 + \frac{1}{n+2}\right)^{n+3} = \left(1 + \frac{1}{n+2}\right)^{n+2} \left(1 + \frac{1}{n+2}\right)$$

$$< (n+2)\left(1 + \frac{1}{n+2}\right) = n + 3.$$

La última desigualdad se sigue por la suposición de la validez de $P(n)$.

Por tanto, hemos probado $P(1)$ y que es verdadera la proposición $\forall n \in N$, $P(n) \rightarrow P(n+1)$. **Luego queda demostrada que**

$$\left(1 + \frac{1}{n+2}\right)^{n+2} < n + 2$$ **para todo número natural** n.

Una variante de la técnica de inducción matemática es la llamada inducción **completa**.

La prueba de la veracidad de $\forall n \in N$, $P(n)$, se obtiene mediante inducción completa si:

1) Se demuestra que $P(1)$ es verdadera y

2) De asumir que $P(j)$ es verdadera para $j \in N$ y $1 \leq j \leq n$, se deduce que $P(n+1)$ es verdadero también.

Ejemplo de demostración por inducción completa:

Supongamos que la sucesión (a_n) viene definida en forma recurrente por:

$$a_1 = 1,\ a_2 = 3,\ \text{y}\ a_{n+2} = 3a_{n+1} - 2a_n,\ \text{para todo}\ n \in N.$$

Encontremos el patrón de formación de a_n, es decir, una manera de expresar a_n explícitamente en función de n, y luego demostremos, usando inducción completa, que ese patrón es válido.

Al escribir los primeros cinco términos obtenemos: 1,3,7,15, y 31, y encontramos así que un patrón para esos cinco primeros términos es $a_n = 2^n - 1$.

Demostremos que ese patrón es válido para todo $n \in N$. Sabemos que $a_1 = 1 = 2^1 - 1$, por tanto se cumple para $n = 1$.

Vamos a demostrar que si se cumple que $a_j = 2^j - 1$, para $1 \leq j \leq n + 1$, entonces también se cumple para a_{n+2}.

Notemos que en este caso debe probarse que la proposición se cumple tanto para $n = 1$ como para $n = 2$. **¿Por qué?**

También se cumple para $n = 2$ pues $a_2 = 3 = 2^2 - 1$

Supongamos que $a_j = 2^j - 1$, para $j \in N$ y $1 \leq j \leq n + 1$, entonces:

$$a_{n+2} = 3a_{n+1} - 2a_n = 3(2^{n+1} - 1) - 2(2^n - 1) = 3.2^{n+1} - 3 - 2^{n+1} + 2 = 2^{n+2} - 1.$$

Aquí probamos que $P(1)$ y que $P(2)$ son verdaderas y, que si $P(j)$ es verdadera para $j \in N$ y $1 \leq j \leq n + 1$, entonces $P(n + 2)$ también lo es; lo cual equivale a haberse probado por inducción completa que $P(n)$ es verdadera para todo $n \in N$.

Por tanto $a_n = 2^n - 1$, para todo número natural n.

En el capítulo IV se hará un estudio más profundo de la inducción matemática y de las definiciones recursivas.

2.3.5. Ejercicios resueltos

1. Demostrar ¬B, si se tienen las siguientes premisas: J∧B → S, ¬S∨T, ¬T y J.

1) J∧B→S		Premisa
2) ¬S∨T		Premisa
3) ¬T		Premisa
4) J		Premisa
5)	B	Premisa Introducida
6)	J∧B	A 4 y 5
7)	S	PP 1 y 6
8)	¬S	TP 2 y 3
9)	S∧¬S	A 7 y 8
10) ¬B		IP o Contradicción 5 y 9.

2. Demostrar ¬D, si se tienen las siguientes premisas: D→W, A∨¬W y ¬(D∧A).

1) D→W		Premisa
2) A∨¬W		Premisa
3) ¬(D∧A)		Premisa
4) ¬D∨¬A		ley de Morgan
5)	D	Premisa Introducida
6)	W	PP 1 y 5
7)	A	TP 2 y 6

8)	¬A	TP 4 y 5
9)	A∧¬A	A 7 y 8
10) ¬D		IP o Contradicción 5 y 9.

3. Demostrar D→C, si se tienen las siguientes premisas:
A→(B→C), ¬D∨A y B.

1) A→(B→C)		Premisa
2) ¬D∨A		Premisa
3) B		Premisa
4)	D	Premisa Introducida
5)	A	TP 2 y 4
6)	B→C	PP 1 y 5
7)	C	PP 3 y 6
8) D→C		CP 4 y 7

4. Demostrar P→(¬Q→R), si se tienen las siguientes premisas:
S∧(¬P∨M) y M→Q∨R.

1) S∧(¬P∨M)		Premisa
2) M→Q∨R		Premisa
3) ¬P∨M		S 1
4)	P	Premisa Introducida
5)	M	TP 3 y 4
6)	Q∨R	PP 2 y 5
7)	¬Q→R	1 de relativa a la condicional
8) P→(¬Q→R),		CP 4 y 7

5. Demostrar $\forall x, F(x) \rightarrow \neg D(x)$, si se tienen como premisas: $\forall x, D(x) \rightarrow M(x)$ y $\forall x, F(x) \rightarrow \neg M(x)$.

1) $\forall x, F(x) \rightarrow \neg M(x)$	Premisa
2) $\forall x, D(x) \rightarrow M(x)$	Premisa
3) $F(x) \rightarrow \neg M(x)$	UE. x/x en 1
4) $D(x) \rightarrow M(x)$	UE. x/x en 2
5) $F(x)$	Premisa Introducida
6) $\neg M(x)$	PP 1 y 5
7) $\neg D(x)$	TT 4 y 6
8) $F(x) \rightarrow \neg D(x)$	CP 5 y 7
9) $\forall x, F(x) \rightarrow \neg D(x)$	UG 8

2.3.6. Ejercicios propuestos

1. Asuma las propiedades y definiciones del álgebra elemental y pruebe en forma matemática las propiedades dadas. Exprese como premisas las definiciones y propiedades usadas en cada demostración matemática, y simbolice y demuestre la validez del argumento correspondiente en forma lógica.

   a) La suma de dos enteros pares es un entero par.
   b) El producto de dos enteros es impar si y sólo si ambos enteros son impares.
   c) Para cualesquiera números enteros a, b, y c, si "a divide a b" y "b divide a c", entonces "a divide a c".
   d) Para todo entero x y todo natural n, x es congruente a n módulo n si y sólo si n divide a x.
   e) Existe $m \in N$ tal que para todo $n \in N$, $\dfrac{1}{2n+1} > \dfrac{1}{mn}$

2. Asuma las propiedades y definiciones del álgebra elemental. Pruebe en forma matemática, o dé un contraejemplo en el caso de ser falsa. Exprese como premisas las definiciones y propiedades usadas en cada demostración matemática, simbolice y demuestre, en el caso de ser válido, en forma lógica la validez del argumento correspondiente.

   a) Para todo número natural n, $n^2 - n + 41$ es un número primo.
   b) Para todo número real a, $|a| \geq a$.
   c) Para todo número real x, $|x+3| \geq |x+2|$.
   d) Para todo entero n, $n^2 + n + 1$ es impar.

3. Simbolice completamente y luego demuestre que el argumento es válido.

   a) El agente que encontró el arma estaba en el apartamento. Cualquiera que estuviera en el apartamento estaba en la ciudad. Si alguien estaba en Bávaro no estaba en la ciudad. José estaba en Bávaro. Por tanto, José no es el agente que encontró el arma.
   b) Todos los números positivos son mayores que cero. Tres es un número positivo. Tres es igual a dos mas uno. Por tanto, dos mas uno es mayor que cero.
   c) Todos los miembros del comité viven en la ciudad de Santiago. El presidente de la sociedad es un miembro del comité. La señorita López es la presidente de la sociedad. Por tanto, la señorita López vive en la ciudad de Santiago.
   d) Jorge pudo haber visto el auto en que uyó el asesino. Pedro fue el primer testigo de la defensa. Jorge estaba en la fiesta o Pedro dio testimonio falso. Nadie en la fiesta pudo ver el auto en que uyó el asesino. Por tanto, el primer testigo de la defensa dio testimonio falso.
   e) Daniel Rey era matemático. Ningún matemático ignora los temas que estudia el cálculo infinitesimal. Don King escribió sobre

todas las cosas que el no ignoraba. Don King era Daniel Rey. Por tanto, si las sucesiones de Cauchy es un tema que estudia el cálculo infinitesimal, entonces Don King escribió sobre ellas.

f) Todos los miembros de nuestro grupo trabajan en la obra teatral o en la preparación de ella. Los que trabajan en la obra teatral están ensayando. Los que trabajan en la preparación de ella están pintando el salón. Por tanto, si Julio es miembro de nuestro grupo, entonces está ensayando o pintando el salón.

g) Cada chico es mas joven que su padre. Carlos es un chico que no es mas joven que Raúl. Cualquiera que esté casado con Margarita es el padre de Carlos. Por tanto, Raúl no está casado con Margarita.

h) Todas las niñas de la familia Martínez están en el cuadro de honor de la Escuela. Eva es una niña de la familia Martínez. El que recibió el premio de matemática no estaba en el cuadro de honor de la Escuela. Por tanto, Eva no recibió el premio de matemática.

i) Cada tema en esta lección es una parte de la Topología. Cada persona que puede resolver problemas en una parte de la Topología tiene mentalidad matemática. María es una persona que puede resolver problemas sobre Espacios de Banach y los Espacios de Banach es un tema en esta lección. Por tanto, María tiene mentalidad matemática.

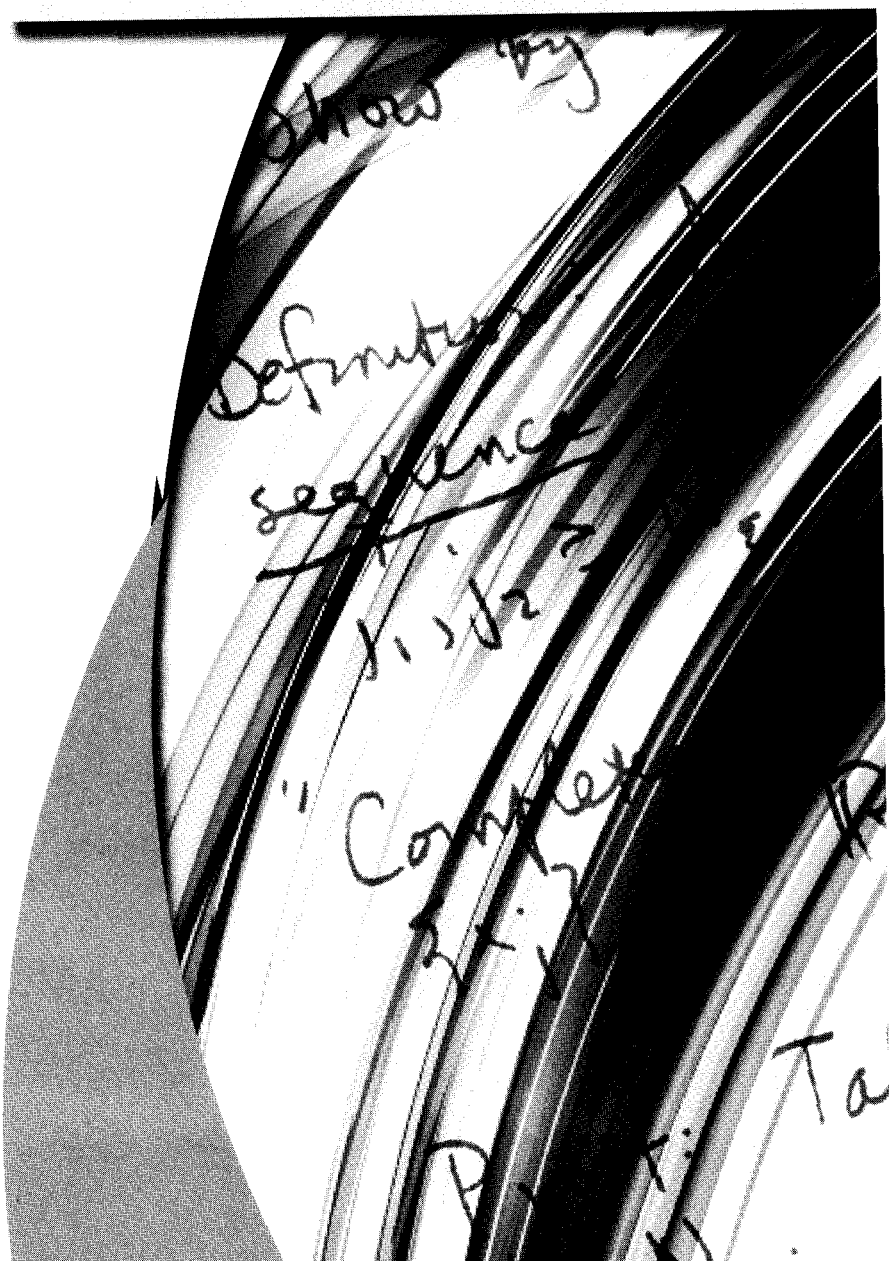
j) Todo aquel que quiera a José escogerá a Abel para su equipo. Abel no es amigo de nadie que sea amigo de Julio. Luis no escogerá a nadie que no sea amigo de Carlos para su equipo. Por tanto, si Carlos es amigo de Julio, entonces Luis no quiere a José.

4. ¿Cuál es el error en el argumento de la siguiente demostración de la proposición, la cual es evidentemente falsa: "En cualquier conjunto de n personas todas tienen el mismo sexo"?

   Demostración: Para $n = 1$ es evidentemente cierto. Suponemos que es cierto para $n \geq 1$. Si tengo un conjunto de $n + 1$ personas, formo

un subconjunto de n personas, por hipótesis de inducción en ese conjunto todas la personas tienen el mismo sexo, luego formo otro subconjunto de n personas que incluya la persona del conjunto de $n + 1$ personas que no estaba en el subconjunto de personas que había formado primero, en ese nuevo conjunto, también por hipótesis de inducción todas tienen el mismo sexo, por tanto la persona que no estaba en el primer subconjunto que había formado de n personas tiene el mismo sexo que el de esas persona, por tanto, en el conjunto de $n + 1$ personas, todas tienen el mismo sexo. Por inducción podemos concluir que es verdadera la proposición enunciada.

3 Conjuntos, Relaciones y Funciones



3. Introducción

Para entender con precisión conceptos como límite y continuidad, los matemáticos del siglo XIX encontraron necesario agregar una descripción axiomática del sistema de números reales.

Como la lógica de proposiciones es intuitivamente clara y precisa, y como las reglas para combinar conjuntos se basan en las correspondientes para combinar proposiciones, Gottlob Frege (1848-1925) apreció que el conjunto de números reales puede ser construido partiendo de una primera definición de cada número natural como un conjunto.

Un axioma de la teoría de conjuntos propuesto por Frege es: "el axioma de abstracción", el cual evidenciaría la conexión natural entre un predicado y un conjunto: "para cualquier predicado P(x) debe haber un conjunto de objetos para el cual P(x) es verdadero". Justo antes que el segundo volumen de los trabajos de Frege fuera publicado en 1919, Bertrand Russell (1872-1970) mostró que el axioma de abstracción llevaba directamente a una contradicción, como lo muestra el siguiente ejemplo: Sea P(x) el predicado "x no es miembro de si mismo", y sea el A el conjunto de todos los objetos que hacen P(x) verdadero; si A es miembro de si mismo entonces P(A) es falso y A no es miembro de si mismo, análogamente, si A no es miembro de si mismo entonces P(A) es verdadero y A es miembro de si mismo. Es por ello que no se puede hablar del conjunto o familia de todos los conjuntos, sino que siempre debemos referirnos a un universo dado cuando estemos desarrollando los elementos de esta teoría. Esto fue conocido como la paradoja de Russell.

Una forma modificada del axioma de abstracción es llamada "axioma de especificación": Dado un conjunto existente B y un predicado P(x), existe un subconjunto de B para el cual P(x) es verdadero.

Otros axiomas han sido adaptados para regular los tipos de conjuntos que son asumidos a existir. Un sistema de axiomas, que aparece para dar la fundamentación suficiente para el desarrollo de las matemáticas elementales, y en el cual no hay paradojas como la de Russell, es el de Zermelo-Fraenkel, nombrado así por los matemáticos Ernst Zermelo (1871-1956) y Abraham Fraenkel (1891-1965). Nosotros nos referiremos informalmente a algunos de ellos para justificar nuestra suposición de existencia de ciertos tipos de conjuntos.

Si bien la lógica nos da la estructura del pensamiento matemático en lo que se refiere a razonamiento deductivo, la teoría de conjuntos nos da la maquinaria para poder desarrollarlo. Conceptos básicos de esta teoría, como los de relaciones y funciones, aparecen en todas las ramas de la Matemática. Por ello podemos afirmar que la Teoría de Conjuntos se encuentra en los Fundamentos de la Matemática.

3.1. Conjuntos

3.1.1. Propiedades de conjuntos

El lenguaje de conjuntos puede ser remitido al lenguaje de la lógica en forma natural si se entiende que cualquier conjunto particular está contenido en un conjunto universal del cual todos sus miembros son tomados.

El predicado $x \in A$ significa que x es un elemento de A, o que x es un miembro del conjunto A. El predicado $x \notin A$ significa que x no es elemento del conjunto A.

Para que el conjunto A esté bien definido tiene que ser posible decidir cuando la proposición $x \in A$ es verdadera o falsa para cada elemento x del conjunto universal.

Si es posible listar los elementos de un conjunto A, podemos escribir la lista de sus elementos entre llaves y separados por comas para representar al conjunto. Por ejemplo: Si $A = \{1,2,3\}$, entonces $1 \in A$, pero $4 \notin A$.

Otra forma de describir ese conjunto A es a través de un predicado P(x) con universo U, mediante la forma: $A = \{x / P(x)\}$. Ejemplo: Si U = *N* es el conjunto de números naturales, $A = \{ x / x<4\}$.

Sea $A = \{1\}$, entonces $1 \in A$ es verdadero, pero el objeto 1 es diferente del conjunto unitario {1}, luego $\{1\} \notin A$. Si $B = \{\{1\}\}$, entonces A y B tienen diferentes elementos.

Uno de los axiomas del sistema de Zermelo-Fraenkel es que existe un conjunto que no tiene elementos, al que llamamos conjunto nulo o vacío y lo representamos por el símbolo ϕ.

Por ejemplo: si U=*R* es el conjunto de números reales, y el predicado P(x) viene definido por $x^2 + 1 = 0$, como sabemos que ese predicado es falso para cada número real, el conjunto $\{x / P(x)\}$ no tiene elementos, es decir, coincide con el conjunto vacío ϕ.

- **Relacionando conjuntos.-** Dos conjuntos son iguales si tienen exactamente los mismos elementos. Igualdad de conjuntos se define formalmente usando la bicondicional de lógica.

- **Definición de igualdad de conjuntos.** Sean U el conjunto universal y A, B conjuntos. Decimos que A es igual a B, denotado por A = B, si y sólo si, A y B tienen exactamente los mismos miembros, más precisamente, en símbolos lógicos, si y sólo si, la proposición $\forall x, (x \in A \leftrightarrow x \in B)$ es verdadera. Esto equivale a: $A = B \Leftrightarrow \forall x, (x \in A \leftrightarrow x \in B)$.

- **Definición de inclusión de conjuntos.** Sean U el conjunto universal y A, B conjuntos. Decimos que A está incluido en B, o que A es subconjunto de B, y lo denotamos por $A \subset B$, si y sólo si, cada miembro de A es también un miembro de B; en símbolos lógicos: $A \subset B \Leftrightarrow \forall x, (x \in A \rightarrow x \in B)$.

Nota.- Probando teoremas sobre conjuntos es una buena forma de practicar las técnicas estudiadas en el primer capítulo.

Una aplicación en el lenguaje de conjuntos de una **prueba directa** para probar que $A \subset B$ es:

- Sea x un miembro general de U
- Asumir que $x \in A$ como premisa introducida
- Probar que $x \in B$ se sigue mediante un razonamiento lógico
- Obtener $x \in A \rightarrow x \in B$ por la prueba de la condicional
- Aplicar la ley de Generalización Universal y de ahí por equivalencia deducir que $A \subset B$.

Y, de una **prueba indirecta**, es:

- Sea x un miembro general de U
- Asumir que $x \in A$ y que $x \notin B$
- Deducir una contradicción mediante un razonamiento lógico.

- Se obtiene así la negación de lo que se asumió
- Se obtiene $x \in A \rightarrow x \in B$ por ley de Morgan y equivalencia 1 de formas relativas de una condicional.
- Aplicar la ley de Generalización Universal y de ahí, por equivalencia, deducir que $A \subset B$.

Ejemplo 1. (Teorema sobre propiedades de la inclusión)

Sean U el conjunto universal y, A, B, y C conjuntos. Entonces:

1) $\phi \subset A$
2) $A \subset A$
3) $(A \subset B \wedge B \subset C) \Rightarrow A \subset C$. Es decir si $A \subset B$ y $B \subset C$, entonces $A \subset C$.
4) $(A \subset B \wedge B \subset A) \Rightarrow A = B$.

Demostración:

1) Por prueba indirecta: si $\phi \not\subset A$, entonces existe $x \in \phi$ y $x \not\in A$, pero ϕ no tiene elementos, por lo que x no puede pertenecer al ϕ, lo cual contradice lo supuesto. $\therefore \phi \subset A$.
2) Trivial
3) Si $x \in A$, por ser $A \subset B$ entonces $x \in B$, y por ser $B \subset C$, entonces $x \in C$. Se obtiene entonces que $x \in A \rightarrow x \in C$ y, de ahí que, $A \subset C$. $\therefore (A \subset B \wedge B \subset C) \Rightarrow A \subset C$.
4) Se obtiene inmediatamente del hecho que $(x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)$ equivale a $x \in A \leftrightarrow x \in B$.

3.1.2. Operaciones con conjuntos. El álgebra de conjuntos

Cada uno de los conectivos lógicos puede ser expresado en el lenguaje de conjuntos. La condicional y la bicondicional son usados en la definición de la relación de subconjuntos y en la de igualdad de conjuntos. Cada forma lógica de disyunción, inclusión y negación está relacionada con una operación de conjuntos que provoca un nuevo conjunto.

- **Definición de unión.-** Sean U el conjunto universal y A, B conjuntos. Entonces la unión de A y B es denotada por $A \cup B$ y definida por:

$$A \cup B = \{x / x \in A \vee x \in B\}.$$

- **Definición de intersección.-** Sean U el conjunto universal y A, B conjuntos. Entonces la intersección de A y B se denota por $A \cap B$ y se define como:

$$A \cap B = \{x / x \in A \wedge x \in B\}.$$

Decimos que dos conjuntos A y B son disjuntos si $A \cap B = \emptyset$

- **Definición de complemento.-** Sean U el conjunto universal y A un conjunto. Entonces el complemento de A se denota como A' y se define por:

$$A' = \{x / x \notin A\}.$$

Ejemplo 2: Sea U = N, A = {x/ x<5}, y B = {x/ x>2}. Entonces:

1) $A \cup B = N$
2) $A \cap B = \{3,4\}$
3) $A' = \{ x/ x \geq 5\}$

Teorema 3.1.2.1. (de propiedades de las operaciones de conjuntos)

Sean U el conjunto universal y A, B, C conjuntos. Entonces:

1) $A \cup B = B \cup A$	conmutativa de la unión
2) $A \cap B = B \cap A$	conmutativa de la intersección
3) $A \cup (B \cup C) = (A \cup B) \cup C$	asociativa de la unión
4) $A \cap (B \cap C) = (A \cap B) \cap C$	asociativa de la intersección
5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributiva
6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributiva
7) $A'' = A$	Doble negación
8) $(A \cup B)' = A' \cap B'$	ley de Morgan
9) $(A \cap B)' = A' \cup B'$	ley de Morgan
10) $A \cup A = A$	idempotente de la unión
11) $A \cap A = A$	idempotente de la intersección
12) $A \subset (A \cup B)$	
13) $A \cap B \subset A$	
14) $(A \cup B) \cap B = B$	
15) $(A \cap B) \cup B = B$	

Demostración. Se deja como ejercicio.

A modo de ejemplo veamos la demostración de 8. Por la ley de Morgan se obtiene que: $\neg(x \in A \vee x \in B) \Leftrightarrow (x \notin A \wedge x \notin B)$, de donde inmediatamente se obtiene: $(A \cup B)' = A' \cap B'$.

Teorema 3.1.2.2. (de propiedades de las operaciones donde intervienen el universo o el conjunto vacío)

Sean U el conjunto universal y A un conjunto. Entonces:

1) $A \cup \phi = A$
2) $A \cap \phi = \phi$
3) $A \cup A' = U$
4) $A \cap A' = \phi$
5) $A \cap U = A$
6) $A \cup U = U$
7) $\phi' = U$
8) $U' = \phi$

Demostración; Se deja como ejercicio.

- **El álgebra de conjuntos.** En el álgebra de proposiciones, nosotros usamos las propiedades básicas de los conectivos lógicos para verificar equivalencias lógicas por sustitución en fórmulas lógicamente equivalentes. En el álgebra de conjuntos nosotros usamos las propiedades correspondientes de las operaciones de conjuntos para verificar identidades que envuelven conjuntos.

Por ejemplo, definimos el complemento relativo de un conjunto con respecto a otro en términos de las operaciones complemento e intersección.

- **Definición de complemento relativo a un conjunto.** Sean U el conjunto universal y A, B conjuntos. Entonces el complemento relativo de B en A, lo denotamos por A-B, y es definido como: $A-B = A \cap B'$. Es decir, consiste en todos los miembros de A que no lo son de B.

Teorema 3.1.2.3. (de propiedades del complemento relativo a un conjunto)

Sean U el conjunto universal y A, B, C conjuntos. Entonces:

1) $A-\phi = A$
2) $\phi-A = \phi$
3) $U-A = A'$
4) $A-U = \phi$
5) $A \cup (B-A) = A \cup B$
6) $A-(B \cup C) = (A-B) \cap (A-C)$
7) $A-(B \cap C) = (A-B) \cup (A-C)$
8) $(A-B)-C = (A-C)-(B-C)$

Demostración: Se deja como ejercicio.

El siguiente teorema lista alguna de las relaciones más complejas entre conjuntos y sus operaciones.

Teorema 3.1.2.4.- (de algunas equivalencias complejas entre conjuntos y sus operaciones)

Sean U el conjunto universal y A, B, C conjuntos. Entonces:

1) $(A \subset B \wedge C \subset B) \Leftrightarrow A \cup C \subset B$
2) $(A \subset B \wedge A \subset C) \Leftrightarrow A \subset B \cap C$
3) Las siguientes condiciones son todas equivalentes:
   3.1. $A \subset B$
   3.2. $A \cup B = B$
   3.3. $A \cap B = A$
   3.4. $B' \subset A'$

Demostración: Demostremos 1 a modo de ejemplo.

$\Rightarrow$)

$x \in A \cup C \rightarrow x \in A \vee x \in C$	por definición
$\rightarrow x \in B \vee x \in B$	por suposición $(A \subset B \wedge C \subset B)$
$\rightarrow x \in B$	por simplificación disyuntiva

Es decir, $A \cup C \subset B$

$\therefore (A \subset B \wedge C \subset B) \Rightarrow A \cup C \subset B$

$\Leftarrow$)

$x \in A \rightarrow x \in A \vee x \in C$	por la regla de la adición
$\leftrightarrow x \in A \cup C$	por definición de unión
$\rightarrow x \in B$	por suposición $A \cup C \subset B$

luego, $A \subset B$

$x \in C \rightarrow x \in A \vee x \in C$	por la regla de la adición
$\leftrightarrow x \in A \cup C$	por definición de unión
$\rightarrow x \in B$	por suposición $A \cup C \subset B$

luego, $C \subset B$

y por adjunción $A \subset B \wedge C \subset B$

$\therefore A \cup C \subset B \Rightarrow (A \subset B \wedge C \subset B)$

y podemos concluir que:

$$\therefore (A \subset B \wedge C \subset B) \Leftrightarrow A \cup C \subset B.$$

3.1.3. Construcción de conjuntos

Aunque un desarrollo de la teoría axiomática de conjuntos no es objetivo nuestro aquí, debemos reconocer que la existencia de los tipos de conjuntos que introducimos, es parte de una teoría general. En teoría de conjuntos, el término conjunto es un concepto primario y por tanto no se define.

Una lista estándar de los axiomas de Zermelo-Fraenkel incluye generalmente nueve axiomas, de los cuales nosotros consideraremos seis para mostrar en algunos ejemplos como son usados en la construcción de conjuntos.

Axiomas de Zermelo-Fraenkel

- **Axioma de extensión.-** Dos conjuntos son iguales si y sólo si ellos tienen los mismos elementos.

- **Axioma del conjunto vacío.-** Hay un conjunto que no tiene elementos.

- **Axioma de especificación.-** Dados un conjunto X y un predicado P(x) cualesquiera, existe un subconjunto A de X para el cual, para todo x elemento de A, P(x) es verdadero.

- **Axioma de Pareo.-** Para cualesquiera conjuntos X e Y existe un conjunto cuyos elementos son X e Y.

- **Axioma de Unión.-** Para cualquier conjunto X cuyos miembros son conjuntos, existe un conjunto cuyos elementos son los elementos de los miembros de X.

- **Axioma del conjunto Potencia.-** Para cualquier conjunto X existe un conjunto cuyos elementos son todos los subconjuntos de X.

Observaciones.

1) La definición de igualdad de conjuntos se basa en el axioma de extensión.
2) El axioma del conjunto vacío garantiza la existencia de conjuntos.
3) Los otros cuatro axiomas justifican la construcción de conjuntos a partir de conjuntos existentes.
   Por ejemplo:
   - el axioma de pareo junto con el de existencia del conjunto vacío garantizan la existencia de un conjunto con elemento el conjunto vacío.
   - el axioma de pareo con el de unión juntos garantizan que la unión de conjuntos es un conjunto;
   - el de especificación implica que la intersección de dos conjuntos A y B es un conjunto, pues sus miembros pueden ser especificados de un conjunto existente, el de la unión de ellos.

- **Definición de conjunto potencia.-** Sea A un conjunto. Entonces el conjunto potencia de A, denotado por $\boldsymbol{P}(\mathbf{A})$, es definido por: $\boldsymbol{P}(\mathbf{A}) = \{B: B \subset A\}$ Es decir, el conjunto de todos los subconjuntos de **A**, el cual es un conjunto por el axioma seis.

Teorema 3.1.3.1. (sobre la potencia de conjuntos finitos)

Sea A un conjunto finito y $n \in \mathbb{N} \cup \{0\}$ su cantidad de elementos, entonces P(A) es finito y tiene 2^n elementos.

Demostración.

Supuesto A y n como en las hipótesis, como

$2^n=(1+1)^n=\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{n}$ y cada $\binom{n}{r}$

es el número de subconjuntos de A con r elementos, se obtiene la tesis.

Teorema 3.1.3.2. (propiedades de la Potencia).

Sean A y B conjuntos, entonces:

- $A\in P(A)$
- $\phi\in P(A)$
- Si $A\subset B$ entonces $P(A)\subset P(B)$

La demostración es inmediata.

¿Qué usted opina?

¿Será en general verdadera la igualdad $P(A\cup B)=P(A)\cup P(B)$?

- **Definición de par ordenado y producto cartesiano.** Los pares ordenados (a,b) y (c,d) son iguales, si y sólo si, a=c y b=d.

En el par ordenado (a,b), **a** es llamada la primera componente y **b** es llamada la segunda componente.

En un desarrollo formal de la Teoría de Conjuntos, si $a\in A$ y $b\in B$, entonces se define y se denota el par ordenado (a,b) como el conjunto: $(a,b)=\{\{a\},\{a,b\}\}$, el cual está bien definido, pues $\{a\},\{a,b\}\in P(A\cup B)$ y, por tanto, de la definición de conjunto potencia, se obtiene inmediatamente que $\{\{a\},\{a,b\}\}\subset P(A\cup B)$.

Así, el **producto cartesiano de A y B(AXB)**, cuando tanto **A** como **B** son conjuntos diferentes del conjunto vacío, se define, por **especificación** en **P(P(A∪B))**, por: **AXB = {(x,y)/ x∈A ∧ y∈B}** .

En el caso de que uno de los conjuntos sea el conjunto vacío notemos que el producto cartesiano es también el conjunto vacío, pues al no existir elementos de uno de los conjuntos no se puede formar ningún par ordenado.

Teorema 3.1.3.3. (sobre propiedades de los productos cartesianos)

Sean A, B, C y D conjuntos no vacíos. Entonces:

- AX(B∪C) = (AXB) ∪ (AXC).
- AX(B∩C) = (AXB) ∩ (AXC).
- Si A⊂C y B⊂D entonces AXB ⊂ CXD.
- AXϕ = ϕ.
- Si AXB = ϕ, entonces A=ϕ ∨ B=ϕ.
- Si AXB = AXC y A≠ϕ, entonces B=C.
- Si A≠ϕ, B≠ϕ y AXB = BXA, entonces A=B.

La demostración de cada una de estas propiedades se deja como ejercicio, pero hacemos la última a modo de ejemplo.

Demostración de la última propiedad:

Supongamos que A≠B. Sin perdida de generalidad sea A⊄B, entonces existe x, x∈A y x∉B. Como B≠ϕ, existe y∈B, pero y≠x , pues x no pertenece a B.

Así (x,y)∈AXB, pero (x,y)∉BXA , pues x∉B. Esto contradice la hipótesis **AXB = BXA. Por tanto: A = B.**

Conjuntos indizados

Una **familia** de conjuntos es un conjunto cuyos miembros son conjuntos. Una manera de construir una familia de conjuntos es mediante el conjunto potencia de un conjunto. Otro camino es asociar un conjunto a cada miembro de un ***conjunto de índices.***

Sea S un conjunto no vacío, y supongamos que para cada $x \in S$ hay un correspondiente conjunto A_x. Decimos entonces que el conjunto:

$$F = \{ A_x : x \in S \}$$

es una **familia de conjuntos indizados** y cada miembro de S es llamado un **índice.**

Definición de unión e intersección sobre una familia de conjuntos.- Sea F una familia de conjuntos. La unión sobre F es denotada por $\bigcup_{B \in F} B$ y es definida como: $\bigcup_{B \in F} B = \{x:(\exists B \in F)\ (x \in B)\}$. La intersección sobre **F** es denotada por $\bigcap_{B \in F} B$ y es definida como:

$$\bigcap_{B \in F} B = \{x:(\forall B \in F)\ (x \in B)\}$$

Si F es la familia de conjuntos indizadas, $F = \{ A_x : x \in S \}$, entonces la unión y la intersección sobre F son denotadas y definidas respectivamente como:

$$\bigcup_{x \in S} A_x = \{y: (\exists x \in S: (y \in A_x))\} \qquad y \qquad \bigcap_{x \in S} A_x = \{y: (\forall x \in S: (y \in A_x))\}$$

Sea F una familia de conjuntos. Decimos que F es disjunta por parejas si, y sólo si, la intersección de cualquier par de miembros de F es el vacío.

Teorema 3.1.3.4.- (sobre propiedades en las familias de conjuntos indizados)

Sean $\boldsymbol{F} = \{ A_x : x \in S \}$ una familia de conjuntos indizados y B un conjunto. Entonces:

1. Para cada z∈S, $A_z \subset \bigcup_{x \in S} A_x$.
2. Para cada z∈S, $\bigcap_{x \in S} A_x \subset A_z$.
3. $B \cap (\bigcup_{x \in S} A_x) = \bigcup_{x \in S} (B \cap A_x)$
4. $B \cup (\bigcap_{x \in S} A_x) = \bigcap_{x \in S} (B \cup A_x)$
5. $\left(\bigcup_{x \in S} A_x\right)' = \bigcap_{x \in S} A_x'$
6. $\left(\bigcap_{x \in S} A_x\right)' = \bigcup_{x \in S} A_x'$

La tercera y la cuarta son las leyes distributivas, y las dos últimas son las leyes de Morgan. Dejamos las demostraciones como ejercicio.

3.1.4. Ejercicios propuestos

1. Sean U el conjunto universal y A, B, C conjuntos. Pruebe que:

1) $A \cup B = B \cup A$	conmutativa de la unión
2) $A \cap B = B \cap A$	conmutativa de la intersección
3) $A \cup (B \cup C) = (A \cup B) \cup C$	asociativa de la unión
4) $A \cap (B \cap C) = (A \cap B) \cap C$	asociativa de la intersección
5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributiva

6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ Distributiva
7) $A'' = A$ Doble negación
8) $(A \cup B)' = A' \cap B'$ ley de Morgan
9) $(A \cap B)' = A' \cup B'$ ley de Morgan
10) $A \cup A = A$ idempotente de la unión
11) $A \cap A = A$ idempotente de la intersección
12) $A \subset (A \cup B)$
13) $A \cap B \subset A$
14) $(A \cup B) \cap B = B$
15) $(A \cap B) \cup B = B$

2. Sean U el conjunto universal y A un conjunto. Pruebe que:

1) $A \cup \phi = A$
2) $A \cap \phi = \phi$
3) $A \cup A' = U$
4) $A \cap A' = \phi$
5) $A \cap U = A$
6) $A \cup U = U$
7) $\phi' = U$
8) $U' = \phi$

3. Sean U el conjunto universal y A, B, C conjuntos. Pruebe que:

1) $A - \phi = A$
2) $\phi - A = \phi$
3) $U - A = A'$
4) $A - U = \phi$
5) $A \cup (B - A) = A \cup B$
6) $A - (B \cup C) = (A - B) \cap (A - C)$
7) $A - (B \cap C) = (A - B) \cup (A - C)$
8) $(A - B) - C = (A - C) - (B - C)$

4. Sean U el conjunto universal y A, B, C conjuntos. Pruebe que:

   1) $(A \subset B \wedge A \subset C) \Leftrightarrow A \subset B \cap C$
   2) Las siguientes condiciones son todas equivalentes:
      2.1 $A \subset B$
      2.2 $A \cup B = B$
      2.3 $A \cap B = A$
      2.4 $B' \subset A'$

5. Sean A, B, C, y D conjuntos no vacíos. Pruebe que:

   1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
   2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
   3) Si $A \subset C$ y $B \subset D$ entonces $A \times B \subset C \times D$.
   4) $A \times \phi = \phi$.
   5) Si $A \times B = \phi$, entonces $A = \phi \vee B = \phi$.
   6) Si $A \times B = A \times C$ y $A \neq \phi$, entonces $B = C$.
   7) Si $A \neq \phi$, $B \neq \phi$ y $A \times B = B \times A$, entonces $A = B$.

6. Sean $\mathbf{F} = \{ \mathbf{A}_x : x \in \mathbf{S} \}$ una familia de conjuntos indizados y B un conjunto. Pruebe que:

   1) Para cada $z \in S$, $\mathbf{A}_z \subset \bigcup_{x \in S} \mathbf{A}_x$.

   2) Para cada $z \in S$, $\bigcap_{x \in S} \mathbf{A}_x \subset \mathbf{A}_z$.

   3) $B \cap (\bigcup_{x \in S} A_x) = \bigcup_{x \in S} (B \cap A_x)$.

   4) $B \cup (\bigcap_{x \in S} A_x) = \bigcap_{x \in S} (B \cup A_x)$.

   5) $\left(\bigcup_{x \in S} A_x \right)' = \bigcap_{x \in S} A_x'$.

6) $\left(\bigcap_{x\in S} A_x\right)^{|} = \bigcup_{x\in S} A_x^{|}$.

3.2. Relaciones

3.2.1. Definición y propiedades de las relaciones

Los conjuntos son usados para expresar algunos conceptos matemáticos muy importantes. En particular, el producto cartesiano de dos conjuntos juega un importante rol en ese sentido.

- **Definición de relación.-** Sean A y B dos conjuntos no vacíos. Entonces decimos que una **relación de A en B** es un subconjunto de AXB.

Una **relación sobre A** es un subconjunto de AXA.

Si R es una relación de A en B, decimos que **x es R-relativo a y,** si y sólo si, $(x,y)\in R$, en cuyo caso escribimos xRy.

El dominio, Dom(R), y el recorrido, rango o imagen, Rec(R), Ran(R) o Im(R), de la relación R son respectivamente los subconjuntos de A y B definidos por:

$DomR = \{x: (\exists y)\ [(x,y)\in R]\}$

$Ran(R)=ImR = \{y: (\exists x)\ [(x,y)\in R]\}$

Sea A un conjunto no vacío. **La relación identidad sobre A** se define por:

$$I_A = \{(x,x) \in AXA\}.$$

Propiedades de la igualdad

De la multitud de relaciones sobre un conjunto, ciertas de ellas tienen propiedades especialmente útiles en matemática.

Por ejemplo para resolver ecuaciones en el sistema de números reales son muy usadas las siguientes propiedades de la igualdad:

1. Para todo a, a=a
2. Para todo a y b, si a=b entonces b=a
3. Para todo a, b y c, si a=b y b=c, entonces a=c.

Esas tres propiedades son llamadas respectivamente: **reflexiva, simétrica y transitiva.** Relaciones que poseen las tres propiedades anteriores son llamadas relaciones de equivalencia.

Definiciones (relaciones reflexivas, simétricas y transitivas)

Sea R una relación sobre el conjunto no vacío A. Nosotros decimos que:

1. **R es reflexiva** si, y sólo si, para todo x∈A, xRx.
2. **R es simétrica** si, y sólo si, para todo x y todo y, si xRy entonces yRx.
3. **R es transitiva si**, y sólo si, para todo x, todo y, y todo z, si xRy y yRz, entonces xRz.

Relaciones que cumplen las tres condiciones, es decir, que son reflexivas, simétricas y transitivas, son llamadas relaciones de equivalencia.

El lector debe escribir, como ejercicio, las definiciones de ser:

R no reflexiva, R no simétrica, y R no transitiva,

que se derivan al hacer las negaciones lógicas correspondientes.

Propiedades de desigualdades

Cuando se resuelven inecuaciones en el sistema de números reales se asumen las siguientes propiedades:

1. Para todo x, $x \leq x$.
2. Para todo x, y, z, si $x \leq y$ y $y \leq z$, entonces $x \leq z$.
3. Para todo x, y, si $x \leq y$ y $y \leq x$, entonces $x = y$.

En otras palabras la relación $\leq$, en el conjunto de números reales, es reflexiva y transitiva. La tercera es conocida como la **propiedad antisimétrica.**

Relaciones que tienen las tres propiedades anteriores son llamadas: **relaciones de orden.**

- **Definición de relación antisimétrica.** Sea R una relación sobre el conjunto no vacío A. Nosotros decimos que R es antisimétrica, si y sólo si, para todo x y todo y, si xRy y yRx, entonces $x=y$.

- **Definición de relación Inversa.-** Sea R una relación del conjunto no vacío A en el conjunto no vacío B. La relación inversa de R, denotada por $\mathbf{R}^{-1}$, es definida por: $R^{-1}=\{(x,y): (y,x)\in R\}$.

Teorema 3.2.1.1. (propiedades que R^{-1} hereda de R)

Sea R una relación sobre el conjunto no vacío A. Entonces:

1. Si R es reflexiva, entonces R^{-1} es también reflexiva.
2. Si R es simétrica, entonces también R^{-1} es simétrica.
3. Si R es transitiva, entonces también R^{-1} es transitiva.
4. Si R es antisimétrica, entonces también R^{-1} es antisimétrica.

Probemos la última (la 4) a modo de ejemplo: Si $xR^{-1}y$ y yR^{-1} x, entonces yRx y xRy, por definición de R^{-1} ; y por tanto, bajo el supuesto que R sea antisimétrica, obtenemos que x=y. Es decir, si R es antisimétrica, también R^{-1} lo es.

- **Definición de composición de relaciones.-** Sean A, B, C conjuntos no vacíos, S una relación de A en B y R una relación de B en C. La relación compuesta de R con S, denotada por RoS, es definida por: $RoS=\{(x,z):(\exists y)[xSy \wedge yRz]\}$.

Teorema 3.2.1.2.- (propiedades de la relación compuesta)

Sean R, S, T relaciones sobre un conjunto no vacío A. Entonces:

1. $Ro(SoT)=(RoS)oT$.
2. $I_A oR=R$.
3. $(RoS)^{-1} = S^{-1}oR^{-1}$.

A modo de ejemplo demostremos la 3. $(x,y) \in (RoS)^{-1}$ si, y sólo si, $(y,x) \in RoS$ por definición de inversa; esto último equivale, por definición de compuesta a que existe z , tal que ySz y zRx ; lo cual, a su vez equivale, por definición de inversa, a que existe z , tal que "$xR^{-1}z$" y

"$zS^{-1}y$"; y finalmente, por definición de compuesta, esto último equivale a que $(x,y) \in S^{-1}oR^{-1}$.

3.2.2. Relaciones de equivalencia

- **Definición de relación de equivalencia.-** Sea A un conjunto no vacío y E una relación sobre A. Decimos que E es una **relación de equivalencia** si, y sólo si, E es **reflexiva**, E es simétrica, y E **es transitiva.**

Para cada $x \in A$, **la clase de equivalencia de x** es denotada y definida por:

$$\bar{x} = \{ y \in A: xEy\}$$

El conjunto de todas las clases de equivalencia, denotado por **A/E**, es llamado **A módulo E.**

Teorema 3.2.2.1.- (sobre clases de equivalencia)

Sea E una relación de equivalencia sobre el conjunto no vacío A, y sean $x,y \in A$.

Entonces: $\bar{x} = \bar{y}$ si sólo si $x \, E \, y$

Demostración.

Primera parte ($\Rightarrow$).- Supongamos que $\bar{x} = \bar{y}$.

Como $x \in \bar{x}$ y $y \in \bar{y}$ por definición de clase y ser E reflexiva, entonces, bajo el supuesto de la igualdad entre ambos conjuntos, $\bar{y} \in \bar{x}$ y, nuevamente por definición de clase de equivalencia, x E y.

Segunda parte ($\Leftarrow$).- Supongamos que x E y.

Probemos que $\bar{x} \subseteq \bar{y}$.

Si z $\in \bar{x}$ entonces, por definición de clase, xEz. Por otro lado, como por hipótesis, xEy, entonces y E x, pues E es simétrica. Luego, por transitividad, yEz, y por tanto z $\in \bar{y}$. Es decir, $\bar{x} \subseteq \bar{y}$.

Análogamente se prueba que $\bar{y} \subseteq \bar{x}$ y de ambas inclusiones obtenemos la igualdad.

- **Definición de partición.** Sea A un conjunto no vacío y sea ***P*** una familia de conjuntos. Decimos que ***P*** es una **partición de A**, si y sólo si, las siguientes tres condiciones se cumplen:

  1. Para todo B, si B $\in$ P, entonces B$\neq\emptyset$.

  2. Para todo B y C, si B $\in$ ***P*** y C $\in$ P, entonces o B=C o B$\cap$C=$\emptyset$.

  3. $\bigcup_{B \in P} B = A$

Si E es una relación de equivalencia sobre A, entonces la familia de sus clases de equivalencia, **A/E**, es una partición de A, llamada la **partición inducida de A por E.**

Teorema 3.2.2.2. (A/E es una partición de A)

Sea E una relación de equivalencia sobre el conjunto no vacío A. Entonces se cumplen las siguientes tres condiciones:

1. Para todo x∈A, $\bar{x} \neq \emptyset$
2. Para cualesquiera x,y∈A $\bar{x} = \bar{y}$ o $\bar{x} \cap \bar{y} = \emptyset$
3. $\bigcup_{x \in S} \bar{x} = A$

La demostración se deja como ejercicio

Teorema 3.2.2.3. (toda partición induce una relación de equivalencia de la cual ella es la partición inducida)

Sea ***P*** una partición del conjunto no vacío A. Si se define la relación Q por xQy si y sólo si, existe B∈P tal que x∈B y y∈B, entonces Q es una relación de equivalencia sobre A y P = A/Q.

Demostración.

Q es reflexiva.- Si x∈A entonces existe B∈***P*** tal que x∈B por la condición 3 de partición, y por tanto, xQx. Es decir Q es reflexiva.

Q es simétrica.- Evidente de la definición de Q.

Q es transitiva.- Si xQy y yQz entonces existen B y C en ***P*** tales que x,y∈B y y,z∈C. Por tanto, y∈ B∩C, y de la condición 2 de partición, se deduce B=C.

Luego x,z∈B=C y xQz. Luego Q es transitiva.

Hemos demostrado que Q es una relación de equivalencia sobre A.

Probemos ahora que: $P = A/Q$.

Primera parte: $P \subseteq A/Q$.- Sea $B \in P$, como P es una partición de A, entonces $B \neq \emptyset$ y existe $x \in B$. Probemos que $\bar{x} = B$ y así $B \in A/Q$.

Sea $y \in \bar{x}$ luego xQy y existe $C \in P$ tal que, $x \in C$ y $y \in C$. De ahí que $x \in B \cap C$ ya que $x \in B$ y, por la condición 2 de partición, B=C. Por tanto, $y \in B$ al pertenecer a C, luego $\bar{x} \subseteq B$. Sea $y \in B$, como $x \in B$ tenemos que $x,y \in B$, y así, xQy, es decir, $y \in \bar{x}$, luego $B \subseteq \bar{x}$. Por tanto, $P \subseteq A/Q$.

Segunda parte: $A/Q \subseteq P$.- Sea $\bar{x} \in A/Q$. Sabemos que $x \in \bar{x}$, por ser Q reflexiva. Probemos que: $\bar{x} \in P$. Como $\bigcup_{B \in P} B = A$, existe $B \in P$ tal que $x \in B$. Si $y \in \bar{x}$ entonces xQy, luego existe $C \in P$ tal que $x,y \in C$. Como P es disjunto por parejas, B=C. Así obtenemos que B contiene a $\bar{x}$. Veamos que también B está contenido en $\bar{x}$ y, por tanto, que son iguales. Si $y \in B$ entonces $x,y \in B$ y por definición de Q, xQy, luego $y \in \bar{x}$. Por tanto, B está contenido en $\bar{x}$. Luego: $\bar{x} = B \in P$. Por tanto, $A/Q \subseteq P$.

Se sigue inmediatamente, que: $P = A/Q$.

Ejemplo:

Sea Z el conjunto de números enteros y $n \in N$ un número natural. Definamos la relación congruencia módulo n en **Z** por: Para todo $x,y \in Z$ $x \equiv y \bmod(n)$, es decir, x es congruente a y módulo n, si y sólo si, existe $k \in Z$ tal que $x - y = k \cdot n$.

Probemos que la congruencia módulo n es una relación de equivalencia:

1) Es reflexiva, pues para todo $x \in Z$, $x - x = 0 = 0 \cdot n$

2) Es simétrica, pues si $x - y = k \cdot n$, entonces $y - x = (-k) \cdot n$.
3) Es transitiva, pues si $x - y = k \cdot n$ y $y - z = m \cdot n$, entonces $x - z = (k + m) \cdot n$.

El espacio cociente de **Z** por la relación de equivalencia congruencia módulo n, se acostumbra a denotar por Z_n. Por ejemplo donde $Z_2 = \{\overline{0}, \overline{1}\}$ donde $\overline{0} = \{2k : k \in Z\}$ y $\overline{1} = \{2k + 1 : z \in Z\}$.

En general Z_n es un conjunto con n elementos: $Z_n = \{\overline{j} : j = 0,1 \ldots n - 1\}$ donde $\overline{j} = \{j + nk : k \in Z\}$

3.2.3. Relaciones de orden

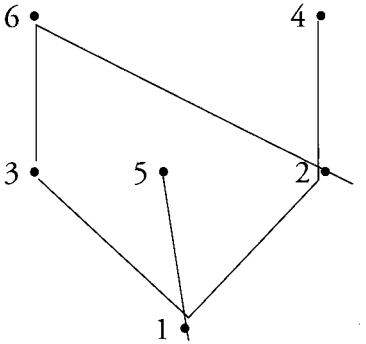
Cuando se ilustra el conjunto de números reales por una recta orientada estamos usando la información contenida en la relación $x \leq y$ para organizar los puntos que representan a los números reales.

En general, relaciones que tienen las propiedades de reflexividad, transitividad y antisimetría imponen algún orden sobre el conjunto.

- **Definición (de orden parcial).** Sean A un conjunto no vacío y R una relación sobre A. Decimos que **R es un orden parcial sobre A** si y sólo si R es reflexiva, transitiva y antisimétrica. También decimos que **A está parcialmente ordenado por R**.

El orden impuesto en un conjunto por una relación puede ser ilustrado con un diagrama llamado **diagrama de Hasse**, donde los elementos del conjunto son representados por puntos conectados por líneas atendiendo al orden.

Por ejemplo si consideramos el conjunto { 1,2,3,4,5,6 } ordenado por la relación x|y, x divide a y, un diagrama de Hasee asociado a esa relación sería:



Definición (de orden total). Sea R una relación de orden parcial sobre el conjunto no vacío A. Decimos que **R es un orden total sobre A,** si y sólo si, para cualesquiera x,y∈A, se tiene que xRy o yRx. Decimos también que **A está totalmente ordenada por R.**

Si un conjunto A está parcialmente ordenado por una relación R, podemos encontrar subconjuntos de A que están totalmente ordenados por R. Tales subconjuntos son llamados **cadenas**.

Si el conjunto A está totalmente ordenado por R entonces todos sus elementos están organizados como una **cadena simple**.

- **Definición (de cadena).** Sea R una relación de orden parcial sobre el conjunto no vacío A, y sea B un subconjunto de A. Decimos que B es una **cadena**, si y sólo si, B está totalmente ordenado por R.

En el ejemplo anterior, son cadenas del conjunto { 1,2,3,4,5,6 } ordenado por la relación x|y, las siguientes: { 1,2,4 }, { 1,3,6 }, { 1,5 }, y cualquier subconjunto no vacío de estos conjuntos.

- **Definición (de elementos minimales y maximales).** Sea R un orden parcial sobre el conjunto A, y $a \in A$, entonces decimos que

  a) a es minimal, si y sólo si, para todo $x \in A$, $xRa \Rightarrow x=a$.
  b) a es maximal, si y sólo si, para todo $x \in A$, $aRx \Rightarrow x=a$.

En el ejemplo anterior: 1 es un elemento minimal y tanto 4, 5, como 6, son maximales.

- **Definición (de mínimo y máximo).** Sea R un orden parcial sobre el conjunto A, y $a \in A$, entonces decimos que:

  a) a es el elemento mínimo de A, si y sólo si, para todo $x \in A$, aRx.
  b) a es el elemento máximo de A, si y sólo si, para todo $x \in A$, xRa.

En el ejemplo anterior: 1 es el mínimo de A según esa relación, y no tiene máximo.

En un conjunto parcialmente ordenado pueden existir elementos minimales o maximales y no ser únicos, pero, si tiene elemento mínimo o máximo, entonces éste es único.

Teorema 3.2.3.1. (unicidad del mínimo y el máximo)

Sea R un orden parcial sobre el conjunto A. Entonces, si existe elemento mínimo (máximo) de A por R, es único.

Demostración: Suponemos que a y b son elementos mínimos. Entonces aRb y bRa. Usando la propiedad antisimétrica que posee R, al ser una relación de orden, se sigue que a=b. Por tanto, no pueden existir mínimos diferentes.

En forma análoga se obtiene la unicidad del máximo.

Teorema 3.2.3.2. (relación entre elementos extremales y extremos)

1) Sea R un orden parcial sobre el conjunto A, si A tiene elemento mínimo (máximo) entonces ese elemento es minimal (maximal).

2) Sea R un orden total sobre el conjunto A, si A tiene elemento minimal (maximal) entonces ese elemento es el mínimo (el máximo).

Demostración de 1: Si para todo $x \in A$ se tiene que aRx, entonces, si xRa se tendría, por la propiedad antisimétrica de R, que a=x. Por tanto: si a es mínimo, entonces a es minimal. Análogamente se obtiene que si a es máximo, entonces a es maximal.

Demostración de 2: Sea "a" un elemento minimal. Como A está totalmente ordenado por R, se tiene que, para todo $x \in A$, aRx o xRa. Pero, al ser "a" minimal, se tiene que, si xRa entonces x=a. Así obtenemos que, si x es diferente de "a", entonces aRx. Como adicionalmente aRa, pues la relación es reflexiva, podemos concluir que para todo $x \in A$, aRx, es decir, que a es el elemento mínimo de A. Análogamente se obtiene que: si a es maximal, entonces a es el elemento máximo de A.

- **Definición (de conjunto bien ordenado).** Sea R un orden total sobre el conjunto A. Entonces decimos que A está bien ordenado por R, si y sólo si, todo subconjunto no vacío B de A contiene elemento mínimo, es decir, para todo subconjunto no vacío B de A, existe $b \in B$, tal que para todo $x \in B$, se tiene que bRx.

Ejercicios propuestos

1. Sea R una relación sobre el conjunto no vacío A. Pruebe que:

   - Si R es reflexiva, entonces R^{-1} es también reflexiva.
   - Si R es simétrica, entonces también R^{-1} es simétrica.
   - Si R es transitiva, entonces también R^{-1} es transitiva.

2. Sean R, S, T relaciones sobre un conjunto no vacío A. Pruebe que:

   - $Ro(SoT)=(RoS)oT$.
   - $I_A oR=R$.

3. Sean R y S dos relaciones sobre el conjunto no vacío A. Pruebe, o dé un contrajemplo, de las siguientes aseveraciones:

   - Si R y S son reflexivas sobre A, entonces $R \cup S$ es reflexiva sobre A.
   - Si R y S son simétricas, entonces $R \cup S$ es simétrica.
   - Si R y S son transitivas, entonces $R \cup S$ es transitiva.
   - Si R y S son antisimétricas, entonces $R \cup S$ es antisimétrica.
   - Si R y S son reflexivas sobre A, entonces $R \cap S$ es reflexiva sobre A.
   - Si R y S son simétricas, entonces $R \cap S$ es simétrica.
   - Si R y S son transitivas, entonces $R \cap S$ es transitiva.
   - Si R y S son antisimétricas, entonces $R \cap S$ es antisimétrica.
   - $Dom(R \cup S) = Dom(R) \cup Dom(S)$.
   - $Dom(R \cap S)$ $Dom(R) \cap Dom(S)$.

4. Sea E una relación de equivalencia sobre el conjunto no vacío A. Pruebe que se cumplen las siguientes tres condiciones:

   - Para todo $x \in A$, $\overline{x} \neq \emptyset$
   - Para cualesquiera $x,y \in A$, $\overline{x}=\overline{y}$ o $\overline{x} \cap \overline{y}=\emptyset$
   - $U_{x \in A} \overline{x} = A$

5. Sean A={1,2,3,4}, P={{1,4},{2,3}}, y E={(1,1),(2,2),(3,3),(4,4), (1,3),(3,1)}.

   - Encuentre las clases de equivalencia de A respecto a **E**.
   - Encuentre la partición de A inducida por **E**.
   - Encuentre la relación de equivalencia **Q** tal que $\boldsymbol{P = A/Q}$.

6. Sea E una relación sobre el conjunto no vacío A. Pruebe las siguientes aseveraciones:

   - **E** es una relación de equivalencia sobre A si y sólo si, **E** es reflexiva y para todo a,b,c $\in A$ si a**E**b y b**E**c, entonces c**E**a.
   - Si **E** es simétrica y transitiva y dom(**E**)=A, entonces **E** es una relación de equivalencia sobre A.
   - Si **E** es una relación de equivalencia sobre A, entonces E^{-1} es una relación de equivalencia sobre A y $A/E^{-1} = A/\mathbf{E}$.

7. Sea A = {1, 2, 3}.

   - Encuentre dos órdenes parciales sobre A que no sean órdenes totales.
   - Encuentre dos órdenes totales diferentes sobre A.
   - ¿Cuántos órdenes totales diferentes sobre A hay?
   - Encuentre dos cadenas diferentes en el conjunto potencia, $\boldsymbol{P}$**(A),** ordenado por la inclusión $\subset$
   - Ilustre la relación entre los elementos de ($\boldsymbol{P}$**(A)**, $\subset$) mediante un diagrama de Hasse.
   - Encuentre todos los elementos minimales y maximales de ($\boldsymbol{P}$**(A)**, $\subset$).
   - ¿Tiene ($\boldsymbol{P}$**(A)**, $\subset$) elemento mínimo?, ¿tiene elemento máximo?

8. Explique por qué cada conjunto, dado a continuación, está totalmente ordenado, o no, por la relación "a divide a b" (a|b).

   - A = {1, 2, 3, 4, 6, 8, 12, 24}
   - A = {1, 2, 4,12, 24}
   - A = {3n: n $\in N$}
   - A = {3^n: n $\in N$}.

9. Pruebe o desapruebe en cada caso si la relación es un orden parcial sobre el conjunto dado y analice, en el caso de que sea un orden parcial, si es o no es, un orden total.

   - La relación sobre $N \times N$ definida por: $(a,b)R(c,d) \Leftrightarrow a \leq c \wedge b \leq d$
   - La relación sobre $N \times N$ definida por: $(a,b)R(c,d) \Leftrightarrow a = c \wedge (b \leq d \vee a < d)$
   - La relación sobre N definida por:
     $aRb \Leftrightarrow [(a+b \text{ es par}) \wedge a \leq b) \vee (a+b \text{ es impar}) \wedge a \text{ es par})]$

10. Sea R un orden parcial sobre el conjunto no vacío A, y $a \in$A. Use definiciones apropiadas para dar la forma lógica de las negaciones de las siguientes aseveraciones:

    - a es minimal.
    - a es maximal.
    - a es el mínimo de A.
    - a es el máximo de A.

11. Pruebe las siguientes aseveraciones:

    - Pruebe que si R es un orden parcial sobre el conjunto no vacío A, y A tiene máximo (mínimo), entonces el máximo (mínimo) es único y es un elemento maximal (minimal).

- Pruebe que si R es un orden total sobre el conjunto no vacío A, y A tiene elemento maximal (minimal), éste es único y es el máximo (mínimo) de A.

- Pruebe que si R es un orden total (buen orden) sobre A, y B es un subconjunto de A, entonces B está totalmente ordenado (bien ordenado) por R.

12. Pruebe que el conjunto de números naturales está totalmente y es bien ordenado por la relación de orden ($\leq$).

3.3. Funciones

3.3.1. Propiedades de las funciones

En matemática el término función siempre ha indicado una dependencia, y en diversas épocas se ha considerado definida priorizando algunos de sus aspectos. En la actualidad su esencia queda descrita por su definición como cierto subconjunto de pares ordenados, es decir, como una relación que satisface ciertas condiciones.

- **Definición de función.** Sea f una relación del conjunto A en el conjunto B. Nosotros decimos que f es una función, o que dicha relación es funcional, si y sólo si:
  $\forall x \in A, \forall y,z \in B, (x,y) \in f \wedge (x,z) \in f \Rightarrow y = z$

Si $Dom(f) = A$, y $ran(f) \subset B$, se dice que f se aplica de A en B y que f es una aplicación o función de A en B, y lo denotamos por: $f: A \rightarrow B$

El rango de una función f, $ran(f)$, tambien se le llama imagen de f o recorrido de f en cuyo caso la denotaciones respectivas usadas son $Im(f)$ y $R(f)$.

Notemos que las definiciones respectivas de dominio y rango de una función correponden a las definiciones respectivas de f como relación.

Sea f una función y $x \in Dom(f)$. Decimos que y **es el valor de** f en x, o la imagen de x por f, y lo denotamos por $y = f(x)$ si y sólo si $(x,y) \in f$. En este caso también decimos que x es la preimagen de y.

Teorema 3.3.1.1. (de igualdad de funciones)

Sean f y g funciones. Entonces f=g si y sólo si $Dom(f) = Dom(g)$ y para todo $x \in Dom(f), f(x) = g(x)$

La demostración es una consecuecia inmediata de la igualdad de conjuntos, a partir de la definición de función como una relación que satisface ciertas condiciones. Se deja como ejercicio.

Ejemplos de funciones:

1) Sea A un subconjunto del conjunto Universal U. La **función característica de A** se define y se denota por $I_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$

2) Sea **E** una relación de equivalencia sobre el conjunto no vacío A, y $A/_E$ el conjunto A módulo **E**, es decir, el conjunto de las clases de equivalencia determinadas en A por **E**. La función que a cada $x \in A$ le hace corresponder su clase $\bar{x}$ en $A/_E$, es llamada **la aplicación canónica de A sobre** $A/_E$.

3) Sea $f: A \rightarrow B$, donde A y B son conjuntos no vacíos. Sea $C \subseteq A, C \neq \emptyset$. Entonces se define y se denota la función restricción de f a C por:

$$f/_C : C \rightarrow B \quad \text{tal que} \quad f/_C (x) = f(x)$$

- **Definición de función sobre o epiyectiva.-** Sea A un conjunto no vacío y f una función que aplica A en B. Diremos que f es sobre o epiyectiva si $Im(f) = B$. En este caso diremos que f aplica A sobre B.

Por ejemplo, la aplicación canónica de A sobre $A/_E$, que a cada $x \in A$ le hace corresponder su clase $\bar{x}$, es sobre.

Toda función es una relación y por tanto la composición de funciones está definida como composición de relaciones. Probemos que dicha composición es también una función.

Teorema 3.3.1.2. (la composición de funciones es una función)

Sean A, B, y C conjuntos no vacíos, $g : A \rightarrow B$ y $f: B \rightarrow C$. Entonces $f \circ g$ es una función y $f \circ g : A \rightarrow C$. Además, para todo $x \in A$, $f \circ g\,(x) = f(g(x))$

Demostración:

De las propiedades de las relaciones sabemos que $(f \circ g) \subseteq$ A y que $ran(f \circ g) \subseteq$ C. Debemos probar que:

- A$\subset Dom(f \circ g)$, es decir, para todo $x \in A$, existe $y \in C$, tal que $(x,y) \in f \circ g$

- $f \circ g$ es función, es decir, para todo, x,y,z, si $(x,y) \in f \circ g$ y $(x,z) \in f \circ g$ entonces $y = z$.

- Para todo $x \in A$, $f \circ g\,(x) = f(g(x))$

Si $x \in A$ entonces existe $b \in B$ tal que $(x,y) \in g$, por ser $g : A \to B$, y para ese $b \in B$ existe $y \in C$ tal que $(b,y) \in f$, y por tanto $(x,y) \in f \circ g$. Así queda demostrado que $A \subset Dom(f \circ g)$.

Si $(x,y) \in f \circ g$ y $(x,z) \in f \circ g$, entonces existen $b_1, b_2 \in B$ tales que $(x,b_1) \in g$, $(x,b_2) \in g$, $(b_1,y) \in f$ y $(b_2,z) \in f$. Luego, por ser $g : A \to B$, se tiene que $b_1 = b_2$ y de aquí, por ser $f : B \to C$, se sigue que $y = z$. Por tanto, $f \circ g$ es función.

Para todo $x \in A$, existe $y \in C$, tal que $(x,y) \in f \circ g$, donde $f \circ g\,(x) = y$, por ser $f \circ g$ función. Además existe $b \in B$ tal que $(x,b) \in g$, por ser $g : A \to B$, y para ese $b \in B$ existe $z \in C$ tal que $(b,z) \in f$, por ser $f : B \to C$. Se sigue que $(x,z) \in f \circ g$, de donde $g(x) = b$ y $f(b) = z$. Ya probamos que $f \circ g$ es función, por tanto $y = z$. Luego, $f \circ g\,(x) = f(g(x))$.

Es fácil probar, y se deja como ejercicio, que, si $g : A \to B$, y $f : B \to C$ son sobre, entonces, $f \circ g : A \to C$ también lo es.

- **Definición.- (de inyectiva, de biyectiva)** Sea $f : A \to B$. Decimos que f es inyectiva, si y sólo si, para todo $x,y \in A$, si $f(x) = f(y)$, entonces $x = y$. Tales funciones son conocidas también como inyecciones, o simplemente se dicen que son uno a uno. Decimos que f es **biyectiva**, o que es una **biyección**, si es inyectiva y sobre.

En general, dada $f : A \to B$, siempre existe f^{-1} como relación inversa de la relación f. Pero,

¿Cuándo f^{-1} es función?

¿Cuándo $f^{-1} : B \to A$?

Teorema 3.3.1.3. (de inversa como función)

Sea $f: A \rightarrow B$.

1. Entonces $f^{-1}: B \rightarrow A$ sólo si $f: A \rightarrow$ B es una biyección.
2. Entonces $f^{-1}: B \rightarrow A$ es una biyección si $f: A \rightarrow B$ es una biyección.

Demostración.

Demostración de 1: Debemos demostrar que si $f: A \rightarrow B$ y $f^{-1}: B \rightarrow A$, entonces $f: B \rightarrow A$ es una biyección. Por la hipótesis sabemos que:

$Dom(f)$ = A, $Im(f) \subseteq B$, $Dom(f^{-1}) = B$ y $Im(f^{-1}) = A$

Debemos probar entonces, que $B = Im(f)$ y, que para todo $x,y \in A$, si $f(x) = f(y)$ entonces $x = y$. Lo primero se sigue de $f^{-1}: B \rightarrow A$, pues $ran(f) = Dom(f^{-1})$, luego $B = ran(f)$

Además, para todo $x,y \in A$, si $f(x) = f(y)$, entonces $(x,z), (y,z) \in f$ para algún z, por lo que $(x,z), (y,z) \in f^{-1}$ y, como $f^{-1}: B \rightarrow A$, f^{-1} es función, y por tanto, $x = y$

Demostración de 2: Si $f: A \rightarrow B$ es una biyección, entonces f es uno a uno y es sobre. Debemos probar que f^{-1} es función, y que $f^{-1}: B \rightarrow A$ es una biyección. Como $ran(f) = B$ entonces $Dom(f^{-1}) = B$. Si $(z,x), (z,y) \in f^{-1}$, entonces $(x,z), (y,z) \in f$ y, por ser f una función uno a uno, entonces x=y. Por tanto, f^{-1} es función y $f^{-1}: B \rightarrow A$. Falta sólo probar que f^{-1} es sobre, es decir que $ran(f^{-1})$=A. Esto se sigue inmediatamente pues, $ran(f^{-1})=Dom(f)=A$, ya que $f: A \rightarrow B$. El **teorema está probado.**

La demostración del siguiente teorema se sigue inmediatamente, y se deja como ejercicio.

Teorema 3.3.1.4

Sea $f: A \to B$ una biyección. Para todo $x \in A$, $y \in B$ se tiene que:

$$f(x) = y \Leftrightarrow f^{-1}(y) = x.$$

- **Definición.- (de imagen e imagen inversa)** Sea $f: A \to B$, $X \subseteq A$ y $Y \subseteq B$, entonces **la imagen de X, denotada por** $f(X)$, y **la imagen inversa de Y, denotada por** $f^{-1}(Y)$, están definidas respectivamente por:

$$f(X) = \{f(x): x \in X\} \quad \text{y} \quad f^{-1}(Y) = \{x \in Dom(f): f(x) \in Y\}.$$

Note que $f^{-1}(Y)$ tiene sentido como imagen inversa aunque f^{-1} no sea función.

Teorema 3.3.1.5. (sobre composición de biyecciones)

Sean $g: A \to B$ y $f: B \to C$ biyecciones. Entonces:

1. $f \circ g: A \to C$ es una biyección.
2. $g^{-1} \circ f^{-1}: C \to A$ es una biyección y $g^{-1} \circ f^{-1} = (f \circ g)^{-1}$

Demostración

Demostración de 1. Probemos que $f \circ g : A \to C$ es sobre:

Sea $z \in C$, entonces existe $y \in B$ tal que $z = f(y)$, pues f es sobre, y como también g es sobre, existe $x \in A$ tal que $y = g(x)$, de donde $z = f(g(x))$, es decir, $z=(f \circ g)(x)$. Por tanto $f \circ g$ es sobre.

Probemos que $f \circ g : A \to C$ es uno a uno: Para todo $x,y \in A$, si $(f \circ g)(x) = (f \circ g)(y)$, entonces $f(g(x)) = f(g(y))$ por la definición de composición, de donde $g(x) = g(y)$ por ser f inyectiva, y como consecuencia de ser g también inyectiva, $x = y$; luego $f \circ g$ es uno a uno.

Finalmente podemos concluir que $f \circ g : A \to C$ es una **biyección** al ser sobre y uno a uno.

Demostración de 2. Ya se probó que la inversa de una biyección es también una biyección. Luego, de 1, podemos concluir que $g^{-1} \circ f^{-1} : C \to A$ es una biyección. Veamos que: $g^{-1} \circ f^{-1} = (f \circ g)^{-1}$.

Sabemos que: $Dom(g^{-1} \circ f^{-1}) = Dom((f \circ g)^{-1}) = C$

Basta probar que: Para todo $x \in C$, $(g^{-1} \circ f^{-1})(x) = (f \circ g)^{-1}(x)$

Sea $x \in C$, entonces existe $y \in A$ tal que $(g^{-1} \circ f^{-1})(x) = g^{-1}(f^{-1}(x))=y$

Aplicando el teorema anterior de más arriba tenemos que:

$$g(y) = f^{-1}(x), \text{ y que } f(g(y)) = x$$

De donde $(f \circ g)(y) = f(g(y)) = x$, y así, $(f \circ g)^{-1}(x) = y$

Por tanto: Para todo $x \in C$, $(g^{-1} \circ f^{-1})(x) = (f \circ g)^{-1}(x)$

Luego tenemos que: $g^{-1} \circ f^{-1} = (f \circ g)^{-1}$

Nota.- Es fácil probar ahora que si $f: A \to B$ *es una biyección, entonces:* $f \circ f^{-1} = I_B$ *y* $f^{-1} \circ f = I_A$, *donde* I_B *y* I_A *son las identidades de B y A respectivamente.*

Esto se deja como ejercicio.

3.3.2. Conjuntos equipotentes o equivalentes

Nuestro uso de la palabra "tamaño" aplicado a conjuntos, nos indicaría que conjuntos como A={1,2,3} y B={a,b,c} tienen el mismo tamaño, y que ambos conjuntos tienen mayor tamaño que el conjunto C={1,2}. Pero no sabríamos diferenciar el tamaño entre conjuntos con una cantidad infinita de elementos.

- **Definición (de conjuntos equipotentes, equivalentes o de igual cardinal o tamaño).-** Sean A y B conjuntos. Diremos que A y B son conjuntos equivalentes, equipotentes o de igual cardinal, si existe una función biyectiva $f: A \to B$. Cuando esto ocurra escribiremos: A≡B

Teorema 3.3.2.1. (la equivalencia de conjuntos en una familia de conjuntos dada es una relación de equivalencia sobre dicha familia de conjuntos)

Sean A, B, y C conjuntos arbitrarios de una familia de conjuntos dada. Entonces se cumple:

1. A≡A
2. Si A≡B entonces B≡A.
3. Si A≡B y B≡C entonces A≡C.

La demostración es inmediata, ya que:

Para 1, basta considerar la función identidad de A;

Para 2, basta considera la función inversa de la biyección de A a B;

Para 3, basta hacer la composición de funciones biyectivas correspondiente.

Notemos que para hablar de que (≡) es una relación de equivalencia, es necesario definir la relación sobre una familia de conjuntos determinada, pues como sabemos, hablar del conjunto o familia de todos los conjuntos lleva a una paradoja, la paradoja de Russell.

- **Definición. (de conjunto finito y de cardinal, o número cardinal, de los conjuntos finitos)**

Diremos que el conjunto A es finito, si y sólo si, A=ø o $A \equiv N_m$ para algún $m \in N$, *donde* $N_m = \{k \in N : k \leq m\}$.

Si A es un conjunto finito, el cardinal de A será denotado por card(A) y es definido por: card(A)=0 si A=ø y card(A)=m si $A \equiv N_m$

Teorema 3.3.2.2. (sobre el cardinal de la unión de dos conjuntos finitos disjuntos)

Sean A y B conjuntos finitos y disjuntos. Entonces:

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B).$$

Demostración:

Sea m_A =card(A) y m_B =card(B).

Entonces existen $f: A \to N_{m_A}$, y $g: B \to N_{m_B}$

Sea el conjunto de números naturales dado por:

$$C= \{k \in N : m_A + 1 \leq k \leq m_A + m_B\},$$

y sea $h : N_{m_A} \to C$, definida por $h(x) = x + m_A$, la cual es evidentemente una biyección.

Entonces la función $p : A \cup B \to N_{m_A+m_B}$ definida por:

$$p(x)= \left\{ \begin{array}{ll} f(x) & si \quad x \in A \\ h(g(x)) & si \quad x \in B \end{array} \right\}$$

es biyectiva. Demuéstrelo como ejercicio.

- **Definición. (de conjunto infinito)** Sea A un conjunto. Decimos que A es infinito, si no es finito.

Ejemplo:

El conjunto de números naturales es infinito. Aunque esto es evidente, veamos como se podría demostrar.

Si N fuera finito, como no es el conjunto vacío, existiría un número natural m tal que $N \equiv N_m$ y por tanto una biyección $f: N_m \to N$.

Pero $n=1+\sum_{i=1}^{m} f(i) \in N$ es mayor que cualquier elemento de la imagen de f, luego $f: N_m \rightarrow N$ no es sobre, y no puede existir tal biyección.

Como N no es finito, entonces es infinito.

- **Definición (de conjunto numerable).** Sea A un conjunto. Diremos que A es numerable, si A es finito o $A \equiv N$. En el caso $A \equiv N$ diremos que A es infinito numerable y que el card(A)=card(N).

Sea P = $\{2n: n \in N\}$ el conjunto de números naturales pares, y sea I = $\{2n\text{-}1: n \in N\}$ el conjunto de números naturales impares.

Sabemos que $N = P \cup I$, y que $g: N \cap I = \Phi$

Es fácil probar que $f: N \rightarrow P$, y $g: N \rightarrow I$ definidas respectivamente por:

$$f(n) = 2n, \quad y \quad g(n) = 2n \rightarrow 1,$$

son biyecciones.

Observación.

Notemos que el conjunto números naturales pares y el conjunto de números naturales impares son subconjuntos propios del conjunto de números naturales, sin embargo, ambos poseen el mismo cardinal que el de los naturales.

Esto no es posible en el caso de conjuntos finitos, si A es un subconjunto propio del conjunto finito B entonces el cardinal de A tiene que ser menor que el cardinal de B, **¡pruébelo!**

Teorema 3.3.2.3. (sobre la unión de dos conjuntos infinito numerables y disjuntos)

Sean A y B conjuntos disjuntos y cada uno de ellos infinito numerable. Entonces su unión es un conjunto infinito numerable.

Demostración.

Sean $f: A \to N$, $y\, g: B \to N$ biyecciones. Entonces la función $h: A \cup B \to N$ definida por:

$$h(x) = \left\{ \begin{array}{ll} 2f(x) & si \quad x \in A \\ 2g(x) - 1 & si \quad x \in B \end{array} \right\}$$

es una biyección.

¡Pruébelo!

Teorema 3.3.2.4. (sobre el cardinal de subconjuntos del conjunto de números naturales)

Sea $A \subset N$. Entonces A es finito o infinito numerable.

Demostración.

Supongamos que A no es finito. Como $(N, \leq)$ está bien ordenado, entonces A tiene elemento mínimo según $(\leq)$.

Si definimos por $f(1)$ a ese elemento mínimo, y si, suponiendo definido a $f(n)$, definimos al conjunto A_n por $A_n=\{m \in N: \quad m > f(n)\}$, y al mínimo de A_n, por $f(n+1)$, entonces la aplicación así definida $f: N \rightarrow A$ está bien definida y es una biyección.

¡Pruébelo!

Una consecuencia inmediata de este teorema es que:

Corolario.- Si B es infinito numerable y A es subconjunto de B, entonces A es finito o infinito numerable.

Demostración.-

Sea $f: B \rightarrow N$ una biyección, la cual existe pues B es infinito numerable, y consideremos $A \neq \Phi$, ya que si A es el conjunto vacío es trivial.

Entonces, la función restricción de f a A $f/_A : A \rightarrow f(A)$, es evidentemente una biyección. Como $f(A) \subseteq N$, por el teorema anterior obtenemos que $f(A)$ es finito o infinito numerable y, como por definición, el conjunto A tiene el mismo cardinal que el conjunto $f(A)$, pues existe una biyección entre ambos conjuntos, podemos concluir que el conjunto A es finito o infinito numerable.

Nota:

1) Sean A y B disjuntos, A finito y B infinito numerable. Es fácil probar que su unión es infinito numerable, y su prueba es:

Hay dos casos posibles $A = \Phi$ o $A \neq \Phi$.

Si A es el conjunto vacío, la unión de A y B es B, luego su unión es infinito numerable.

En el otro caso $A \neq \Phi$, de ser finito A, existe $n \in N$ tal que $f: A \rightarrow N_n$ es una biyección. Además, existe una biyección $h : B \rightarrow N$, por ser B infinito numerable.

Basta definir:

$$g = A \cup B \rightarrow N, \qquad \text{como} \qquad g(x) = \left\{ \begin{array}{ll} f(x) & si \quad x \in A \\ h(x)+n & si \quad x \in B \end{array} \right\}$$

la cual será también una biyección.

Por tanto, también en este caso, la unión de A y B es un conjunto infinito numerable.

2) Notemos ahora que, en los resultados anteriores, la condición de ser disjuntos no era necesaria, pues:

$$A \cup B = (A\text{-}(A \cup B)) \cup B$$

Es decir, la unión de un conjunto finito y un conjunto infinito numerable es un conjunto infinito numerable.

3) $N \times N$ un conjunto infinito numerable.

Basta considerar la aplicación $f: N \times N \rightarrow N$ definida por $f((n,m)) = 2^n.3^m$, la cual está bien definida y es inyectiva, pues la descomposición en factores primos da un único número natural. Luego, es una biyección sobre su imagen.

Así, $N \times N$ tiene el mismo cardinal que un subconjunto de N, pero como $N \times N$ evidentemente no es finito, entonces es un conjunto infinito numerable.

Teorema 3.3.2.5.- (cardinal del conjunto de números racionales)

El conjunto de números racionales Q es un conjunto infinito numerable,

Demostración:

Probemos primero que el conjunto de números racionales positivos Q^+, es un conjunto infinito numerable.

Sea F el conjunto de expresiones fraccionarias de la forma $^{p}/_{q}$, donde p y q son números naturales. Es claro que $Q^+ \subseteq$ F y que Q^+ no es finito.

Sea $f: F \rightarrow N \times N$, definida por $f\left(^{p}/_{q}\right) = (p,q)$. La función $f: F \rightarrow N \times N$ es uno a uno y aplica F sobre $N \times N$

Por tanto F es un conjunto infinito numerable y como $Q^+ \subseteq$ F no es finito, entonces también es infinito numerable, pues es equivalente a un subconjunto infinito del conjunto numerable $N \times N$.

Después de probado esto, se obtiene inmediatamente que Q es un conjunto infinito numerable, pues $Q = Q^+ \cup Q^- \cup \{0\}$, donde Q^-, conjunto de números racionales negativos, es un conjunto infinito numerable al serlo Q^+, pues $f: Q^- \rightarrow Q^+$ definida por $f(x) = -x$ es una biyección.

Por tanto $Q = Q^+ \cup Q^- \cup \{0\}$ también es un conjunto infinito numerable, al ser una unión de dos conjuntos infinitos numerables y un conjunto finito.

Así tenemos que: card(Q)=card(N)

Teorema 3.3.2.6. (sobre el cardinal de R)

El conjunto de números reales **R** es un conjunto infinito no numerable.

Demostración

Sabemos que todo número real x del intervalo (0,1) tiene una única representación de la forma $x = 0.x_1\, x_2 \ldots$ donde $x_n \in \{0,1,2,3,4,5,6,7,8,9\}$ para todo $n \in N$ es el dígito en el lugar n de la representación decimal de x, asumiendo que la parte decimal no contiene una sucesión infinita de nueves repetidos; por ejemplo escribiendo $0.30\overline{0}$ por $0.29\overline{9}$.

Supongamos que exista una biyección $f: N \rightarrow (0,1)$, y llegaremos a una contradicción.

Sea $b = 0.b_1\, b_2\, b_3 \ldots$ donde $b_n = 2$ si el dígito en el lugar n de la representación decimal de f(n) es 1, y $b_n = 1$ si el dígito en el lugar n de la representación decimal de f(n) es diferente de 1.

Entonces $b \neq f(n)$ para todo $n \in N$, luego $f: N \rightarrow (0,1)$ no es sobre. Por tanto, se contradice que sea una biyección.

Hemos obtenido así que el intervalo (0,1) no es un conjunto infinito numerable. Pero es infinito, luego es un infinito no numerable.

Es fácil definir una aplicación biyectiva $g: (0,1) \rightarrow R$, por ejemplo:

$$g(x) = \tan\left(\pi x - \frac{\pi}{2}\right)$$

Por tanto, el conjunto de números reales tiene el mismo cardinal que el intervalo (0,1), luego es un conjunto infinito no numerable.

3.3.3. Aplicaciones que preservan el orden

Dado un conjunto A y una relación de orden parcial R sobre A, es decir, una relación que es reflexiva, simétrica y transitiva sobre A, decimos que el par (A,R) es un conjunto parcialmente ordenado.

El estudio de aplicaciones que preservan esta estructura de orden juega un importante rol en el análisis de los objetos de la matemática.

- **Definición.- (de aplicación que preserva el orden)** Sean (A,R) y (B,S) conjuntos parcialmente ordenados. Nosotros decimos que la aplicación $f: A \rightarrow B$ preserva el orden dado, si y sólo si:

$$\forall x,y \in A,\ (x,y) \in R \Leftrightarrow (f(x), f(y)) \in S$$

También decimos que f es una función que preserva el orden.

Sabemos que $(R,\leq)$ es un conjunto ordenado parcialmente, (lo es totalmente).

Definimos que una función $f: R \rightarrow R$ es creciente, si para todo $x,y \in Dom(f)$ se tiene que:

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

Es fácil probar que $f: R \to R$ es creciente, si y sólo si, preserva el orden ($\leq$).

- **Definición. (de isomorfismo de orden)** Sean (A,R) y (B,S) conjuntos parcialmente ordenados. Decimos que A y B son **isomorfos de orden,** si y sólo si, existe una biyección $f: A \to B$ que preserva el orden.

En dicho caso decimos que la aplicación $f: A \to B$ es un **isomorfismo de orden.**

Una propiedad se dice que es una **propiedad de orden,** siempre que: cada vez que la propiedad la posea un conjunto parcialmente ordenado (A,R) cualquiera, entonces también la poseen todos los conjuntos parcialmente ordenados que sea isomorfos de orden de (A,R).

Teorema 3.2.3.1. (propiedades de orden)

Sean (A,R) y (B,S) conjuntos parcialmente ordenados y la aplicación $f: A \to B$ un isomorfismo de orden. Entonces:

1) La aplicación inversa $f^{-1} : B \to A$ es un isomorfismo de orden.
2) Si el conjunto A está totalmente ordenado por R entonces el conjunto B también está totalmente ordenado por S.
3) Si X es una cadena en (A,R) entonces $f(X)$ es una cadena en (B,S).
4) Si "a" es elemento minimal (maximal) en (A,R), entonces $f(a)$ es un elemento minimal (maximal) en (B,S).
5) Si "a" es el mínimo (máximo) en (A,R), entonces $f(a)$ es el mínimo (máximo) en (B,S).
6) Si A está bien ordenado por R, entonces B está bien ordenado por S.

Demostración.

• Demostración de 1

La aplicación inversa $f^{-1} : B \to A$ es una biyección, pues $f: A \to B$ lo es.

Sean $u, v \in B$ y $x = f^{-1}(u)$, $y = f^{-1}(v)$

Entonces, $f(x) = u$, $f(y) = v$ y, como $f: A \to B$, es un isomorfismo de orden

$$(u,v) = (f(x), f(y)) \in S \Leftrightarrow (x,y) = (f^{-1}(u), f^{-1}(v)) \in R$$

Por tanto, f^{-1} mantiene el orden.

Por tanto, la aplicación inversa $f^{-1} : B \to A$ es un isomorfismo de orden.

• Demostración de 2.

Sean $b_1, b_2 \in B$, entonces existen $a_1, a_2 \in A$, tales que $f(a_1) = b_1$, y $f(a_2) = b_2$, pues $f: A \to B$ es sobre, al ser una biyección.

Como el conjunto A está totalmente ordenado por R, entonces

$$(a_1, a_2) \in R, \text{ o } (a_2, a_1) \in R,$$

y como $f: A \to B$ preserva el orden, entonces:

$$(f(a_1), f(a_2)) \in R, \text{ o } (f(a_2), f(a_1)) \in R,$$

es decir, $(b_1, b_2) \in S$, o $(b_2, b_1) \in S$.

Por tanto, el conjunto *B* está totalmente ordenado por *S*, si el conjunto A lo está por *R*.

• **Demostración de 3.-** Inmediata de 2, se deja como ejercicio.

• **Demostración de 4.-** Demostremos el caso minimal; el caso maximal es similar, y se deja como ejercicio.

Sea a un elemento minimal de (A,R). Probemos que $f(a)$ es minimal en (B,S)

Si $(y, f(a)) \in S$, entonces $y \in B$, y como $f: A \to B$ es sobre, al ser una biyección, existe $x \in A$, tal que $f(x) = y$; así $(f(x), f(a)) \in S$.

Pero, como $f^{-1} : B \to A$ preserva el orden, entonces $(x,a) \in R$, lo que implica, al ser a un elemento minimal de (A,R), que $x = a$.

Se sigue que, $f(x) = y = f(a)$

Por tanto, $f(a)$ **es un elemento minimal en** (B,S).

• **Demostración de 5.-** Se deja como ejercicio

• **Demostración de 6.-** Sea $B_1 \subseteq B$, $B_1 \neq \Phi$. Probemos que si (A,R) está bien ordenado, entonces B_1 tiene mínimo.

Como $f: A \to B$ es sobre, al ser una biyección, existe $A_1 \subseteq A$, $A_1 \neq \Phi$, tal que $f(A_1) = B_1$.

Si (A,R) está bien ordenado, existe $a_1 \in A_1$, tal que, $\forall a \in A_1\ (a_1,a) \in R$,

Pero, como $f: A \to B$ preserva el orden, entonces $\forall a \in A_1, (f(a_1), f(a)) \in S$, es decir, $\forall b \in B$, $(f(a_1), b) \in S$.

Por tanto $f(a_1)$ es el mínimo de B_1.

Es decir, hemos probado que todo subconjunto no vacío de B tiene elemento mínimo, si eso ocurre con A.

Luego, hemos probado que si (A,R) está bien ordenado, entonces (B,S) también lo está.

3.3.4. Ejercicios propuestos

1) Sean f y g funciones. Pruebe que: $f = g$, si y sólo si, $Dom(f) = Dom(g)$ y para todo $x \in Dom(f)$, se tiene que $f(x) = g(x)$.

2) Pruebe que: si $g : A \to B$, y $f : B \to C$ son sobre, entonces, $f \circ g : A \to C$ también lo es.

3) En general, dada $f: A \to B$, existe f^{-1} como relación inversa de la relación f. ¿Cuándo f^{-1} es función? ¿Cuándo $f^{-1} : B \to A$?

4) Sea $f: A \to B$ una biyección. Pruebe que:

   - para todo $x \in A$ y todo $y \in B$, se tiene que, $f(x) = y \Leftrightarrow f^{-1}(y) = x$
   - $f \circ f^{-1} = I_B$ y $f^{-1} \circ f = I_A$, donde I_B y I_A son las identidades de B y A respectivamente.

5) Complete la demostración del teorema sobre la cardinalidad de la unión de dos conjuntos finitos y disjuntos.

6) Pruebe que si B es un conjunto finito y A es un subconjunto propio de B, entonces el $card(A) < card(B)$.

7) Complete la demostración sobre la unión de dos conjuntos infinito-numerables y disjuntos.

8) Complete la demostración en el teorema sobre el cardinal de los subconjuntos del conjunto de números naturales.

9) Complete la demostración del teorema sobre las propiedades de orden.

10) ¿Es la aplicación canónica $f: Z \rightarrow Z_6$ uno a uno? Justifique su respuesta.

11) Sea A un conjunto con $card(A) = 60$. Pruebe que hay la misma cantidad de subconjuntos de A con 40 elementos, que subconjuntos de A con 20 elementos.

12) Sean A y B conjuntos finitos tales que $card(A) = n$, y n es diferente de cero. Pruebe que:

- Si $B \equiv A$, entonces $card(B) = n$.
- Si $x \in A$, entonces $card(A - \{x\}) = n - 1$.
- $card(A \times \{x\}) = n$.

13) Pruebe que cada uno de los siguientes conjuntos es infinito numerable:

- El conjunto de matrices de orden 2×2 cuyas entradas son números naturales.
- El conjunto de todos los subconjuntos del conjunto de números naturales que contienen cuatro elementos.
- El conjunto de todas las funciones lineales $p(x) = ax + b$, donde a y b son números enteros.
- $A \times A$, si el conjunto A es infinito numerable.

14) Pruebe que $(a,\infty) \equiv R$, *para todo* $a \in R$.

15) ¿Es el conjunto de números irracionales infinito numerable? Justifique su respuesta.

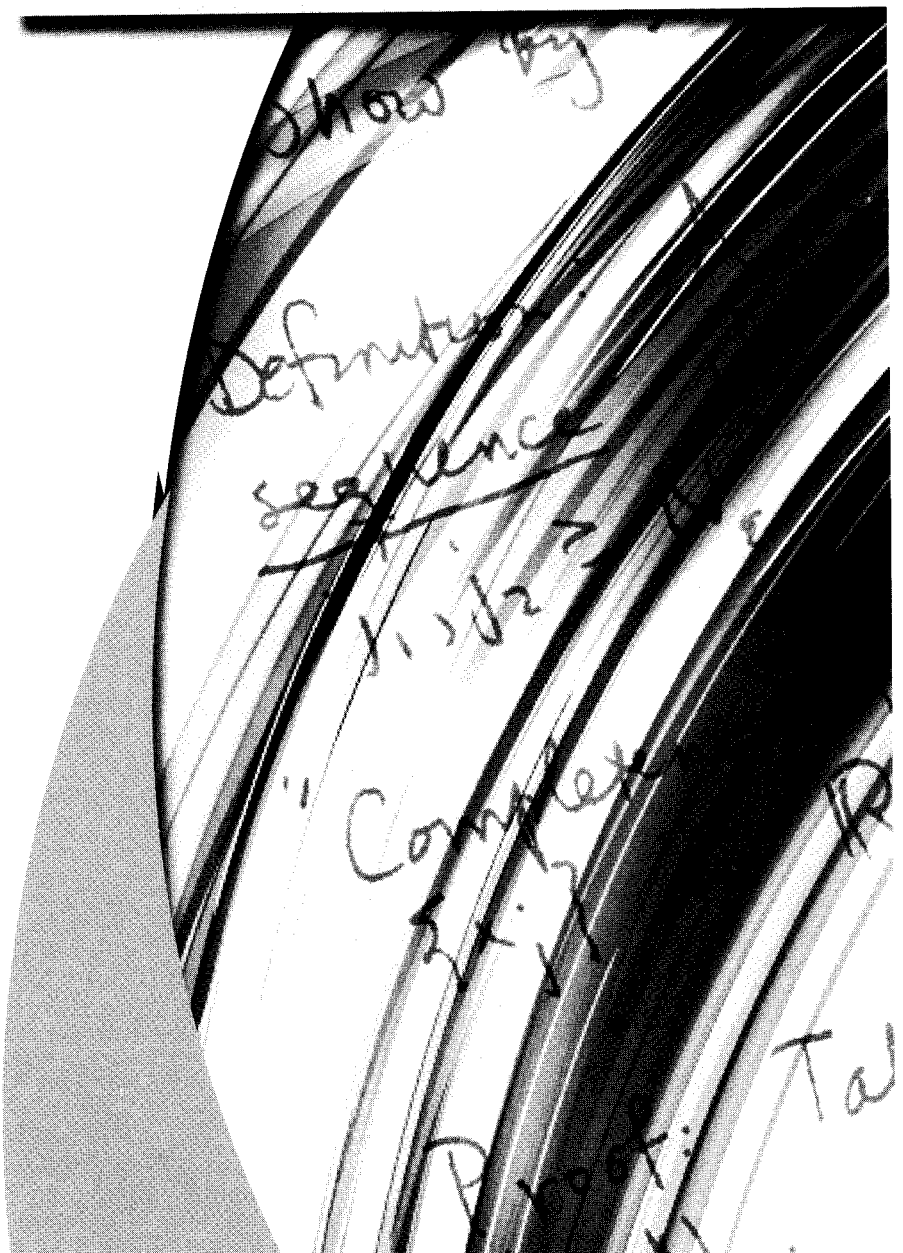
16) ¿Es $Q \times Q$ infinito numerable? Justifique su respuesta.

17) Pruebe que $(Q^+,\leq)$ *y* $(Q^-,\geq)$ son isomorfos de orden.

18) Sea A, el conjunto de todos los factores positivos de 30, y B el conjunto de todos los factores primos de 30. Pruebe que $(A,|)$ es isomorfo a $(P(B),\subseteq)$. Aquí (|) es la relación de equivalencia "divide", y **P**(B) es el conjunto potencia de B.

19) Pruebe que no hay dos conjuntos parcialmente ordenados entre $(N, \leq)$, $(Z,\leq)$, $(Q,\leq)$ y $(R,\leq)$ que sean isomorfos de orden entre sí.

4 Estructuras Algebraicas



4. Introducción

Uno de los grandes logros de los matemáticos del siglo XIX fue la identificación de las propiedades algebraicas fundamentales o reglas, tales como: asociatividad, conmutatividad, distributividad, etc, que gobiernan el comportamiento, en este sentido, de los números reales. El reconocimiento que otros objetos, diferentes a los números reales, puedan tener algunas de estas propiedades o reglas, eventualmente motivó el desarrollo del álgebra abstracta.

Nuestro objetivo en este capítulo no es el desarrollo del álgebra abstracta, sino la presentación de las reglas fundamentales que gobiernan los números desde este punto de vista, y la ejemplificación, en un contexto más general, de ciertos tipos de estructuras o sistemas algebraicos.

Para ello estudiaremos primeramente el concepto de operación binaria, que generaliza los conceptos de adición y multiplicación de números, así como otros ejemplos.

Posteriormente haremos el estudio de algunas estructuras algebraicas simples, sus propiedades y ejemplos.

Luego consideraremos los isomorfismos algebraicos para mas tarde estudiar algunas estructuras algebraicas no simples.

Por último propondremos un grupo de ejercicios para que el lector, con su realización, logre el dominio de los temas estudiados.

4.1. Operaciones binarias

Cuando sumamos y multiplicamos números, ¿qué estamos haciendo?. Estamos aplicando, en cada caso, una regla determinada, mediante la cual le estamos asignando, a un par de elementos de un conjunto, (a un par de números), un elemento del conjunto, (un número).

- **Definición. (de operación binaria)** Sea S un conjunto no vacío y sea $*$ una función. Diremos que $*$ es una operación binaria sobre S, si, y sólo si, $* : S \times S \rightarrow S$

En el caso que $*$ es una operación binaria sobre S, diremos que la imagen de (a,b) por $*$ es su producto, y lo denotaremos por: $* (a,b) = a * b$

Ejemplo 1. La adición, y la multiplicación de números reales, son operaciones binarias sobre el conjunto de números reales.

Por convenio, en este caso, al resultado de la adición de los números "a" y "b" se le llama: suma de "a" y "b", y se reserva la palabra producto, para el resultado de la multiplicación de "a" y "b".

Ejemplo 2. La adición y la multiplicación de matrices de orden 2X2 con entradas números reales son operaciones binarias sobre el conjunto de estas matrices.

Por convenio, al igual que en el caso real, se dice la suma de las matrices A y B, al resultado de la adición de dichas matrices y, se reserva la palabra producto, para el resultado de la multiplicación de A y B.

Ejemplo 3. Dado un conjunto A, la unión y la intersección de conjuntos, son operaciones binarias sobre el conjunto potencia de A, $\boldsymbol{P}$(A).

Por convenio, al resultado de la unión (intersección) de los conjuntos B y C se le llama: unión (intersección) de B y C.

- **Definición. (de operación binaria cerrada en un conjunto)** Sea $*$ una operación binaria sobre el conjunto no vacío S, y $A \subseteq S$. Se dice que $*$ es cerrada en A, si y sólo si, $x * y \in A$, *para todo* $x, y \in A$

Ejemplo. La adición y multiplicación de números reales son operaciones binarias cerradas en el conjunto de números naturales, en el conjunto de números enteros y en el conjunto de números racionales.

Nota. *En lo que sigue diremos simplemente operación, en vez de operación binaria.*

- **Definición. (de operación conmutativa)** Sea $*$ una operación sobre el conjunto no vacío S. Diremos que $*$ es conmutativa si, y sólo si, $a * b = b * a$, *para todo* $a,b \in S$

Ejemplo 1. La adición y la multiplicación de números reales son operaciones conmutativas.

Ejemplo 2. La adición de matrices, de orden 2X2 con entradas reales, es conmutativa, pero la multiplicación no.

- **Definición. (de operación asociativa)** Sea $*$ una operación sobre el conjunto no vacío S. Diremos que $*$ es asociativa, si y sólo si, $a * (b * c) = (a * b) * c$, *para todo* $a,b,c \in S$

Ejemplo 1. La adición y la multiplicación de números reales son asociativas.

Ejemplo 2. La adición y la multiplicación de matrices, de orden 2X2 con entradas reales, son asociativas.

- **Definición. (de elemento identidad)** Sea $*$ una operación sobre el conjunto no vacío S. Diremos que $e \in S$ es un elemento identidad para la operación $*$ si, y sólo si, $e * a = a * e = a$, *para todo* $a \in S$

Ejemplo 1. La adición y la multiplicación de números reales tienen elemento identidad, 0 y 1, respectivamente.

Ejemplo 2. La adición y la multiplicación de matrices, de orden 2X2 con entradas reales tienen elemento identidad $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ y $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ respectivamente.

4.1.1. Ejercicios propuestos sobre operaciones binarias

1) Sea la operación $*$ definida sobre Z por: $x * y = xy - y$
   Evalúe las siguientes expresiones:
   a) $(2 * 3) * (3 * 2)$ b) $3 * (1 * (5 * 0))$

2) Defina la operación $*$ sobre $A = \{a,b,c\}$ mediante la siguiente tabla de doble entrada:

$*$	a	b	c
a	c	a	b
b	c	c	b
c	a	a	c

Evalúe cada una de las siguientes expresiones:

- $(a * b) * (b * a)$,

- $a * (a * a), (a * a) * a,$
- $(c * a) * (a * b).$

3) Defina la operación $\oplus$ sobre $A = \{0,1,2\}$ por: $x \oplus y = r$ donde r es el residuo de dividir la suma ordinaria de x y y por 3. Represente $\oplus$ mediante una tabla de doble entrada.

4) Defina la operación $\otimes$ sobre $A = \{0,1,2\}$ por: $x \otimes y = r$ donde r es el residuo de dividir el producto ordinario de x y y por 3. Represente $\otimes$ mediante una tabla de doble entrada.

5) Sea la operación $*$ definida sobre el conjunto de números reales R por: $x * y = x + y - xy$ Pruebe la veracidad o falsedad de las siguientes aseveraciones:

   - $*$ es asociativa.
   - $*$ es conmutativa.
   - tiene elemento identidad en el conjunto de números reales.

6) Sea Ω el conjunto de todas las matrices de orden 2×2 con entradas números reales. Sabemos que la adición y multiplicación en Ω son respectivamente operaciones binarias. Pruebe la veracidad o falsedad de las siguientes aseveraciones:

   - La adición en Ω es conmutativa.
   - La multiplicación en Ω es conmutativa.
   - La adición en Ω es asociativa.
   - La multiplicación en Ω es asociativa.
   - La adición en Ω tiene elemento identidad.
   - La multiplicación en Ω tiene elemento identidad.

7) Sea X un conjunto no vacío y $\mathfrak{F}$ el conjunto de todas las funciones $f: X \to X$:

- Explique porqué la composición es una operación binaria sobre $\mathfrak{F}$.
- ¿Es la composición asociativa sobre $\mathfrak{F}$? Explique.
- ¿Es la composición conmutativa sobre $\mathfrak{F}$? Explique.
- ¿Tiene la composición elemento identidad sobre $\mathfrak{F}$? Explique.

4.2. Sistemas algebraicos simples

En el capítulo anterior estudiamos las estructuras de orden. Una manera de organizar la inmensa cantidad de posibles operaciones que pueden definirse sobre conjuntos no vacíos, es mediante las llamadas estructuras algebraicas. Una estructura algebraica es un conjunto no vacío junto con una o mas operaciones definidas sobre el, la cual es simple, cuando es una sola operación.

Al igual que hicimos con las estructuras de orden, si tenemos un conjunto no vacío S y una operación binaria $*$ sobre él, diremos que el par $(S,*)$ es un sistema algebraico simple. En lo que sigue no destacaremos el hecho de ser simple y diremos sólo estructura algebraica.

Podemos clasificar distintos sistemas algebraicos a partir del cumplimiento de ciertas propiedades en ellos, llamadas axiomas de la estructura algebraica correspondiente, y así dar nuevas definiciones de estructuras algebraicas específicas, mediante los axiomas que las definen.

4.2.1. Semigrupos

La estructura de semigrupos es una de las estructuras algebraicas más simple, es aquella estructura en que se cumple la propiedad asociativa.

- **Definición.- (de semigrupo)** El sistema algebraico $(S,*)$ es un semigrupo, si la operación $*$ es asociativa.

Los ejemplos dados antes de operaciones asociativas forman estructuras de semigrupo.

Teorema 4.2.1.1.- (fundamental de semigrupo)

Sean $(S,*)$ un semigrupo y $x_i \in S$, *para todo* $i \in N$. Entonces queda unívocamente determinado el elemento $y_n = x_1 * x_2 *... * x_n$ para todo $n \in N$ como elemento de S. (La definición matemática de y_n, es decir, de los puntos suspensivos, se hace por recurrencia: $y_1 = x_1$ para $n = 1$, y supuesto definido y_n, se define $y_{n+1} = y_n * x_{n+1}$, así queda, por inducción matemática, definido y_n, *para todo* $n \in N$; el hecho que pueden eliminarse los paréntesis es consecuencia de la propiedad asociativa, que es lo que se está destacando en el teorema)

Demostración

Sea $(S,*)$ un semigrupo, $x_i \in S$, *para todo* $i \in N$.

Es claro que $x_1 * x_2$ es un elemento único de S cualesquiera sean x_1, $x_2 \in S$, pues $* : S \times S \rightarrow S$. Luego queda unívocamente determinado el producto de dos elementos de S. Por tanto, la proposición:

si $x_i \in S$ *para todo* $i \in N$, entonces queda unívocamente determinado el elemento $y_n = x_1 * x_2 * ... * x_n$ como elemento de S.

Está probada que es cierta para $n = 2$. Es trivialmente cierta para $n = 1$.

Supongamos que el producto de cualquier combinación de j elementos de S con $2 \leq j \leq n$ queda determinado unívocamente, entonces

$$y_{n+1} = (y_n) * x_{n+1} = (y_{n-1} * x_n) * x_{n+1} = (y_{n-1}) * (x_n * x_{n+1}),$$

donde esta última igualdad se obtiene por la asociatividad en el semigrupo, luego está unívocamente determinado, no dependiendo de cómo se asocie, pues siempre se puede igualar, por asociatividad, al producto de dos elementos que están unívocamente determinados, pues y_n y y_{n-1} están unívocamente determinados por hipótesis de inducción completa, y el producto de dos elementos de S también.

Ahora tiene sentido definir la potencia enésima de un elemento.

- **Definición. (de potencia enésima)** Sea $(S,*)$ un semigrupo y $a \in S$. La enésima potencia de a es denotada por a^n, y definida en forma recurrente por: $a^1 = a$ y, para todo número natural n, con $n > 1$, $a^n = a^{n-1} * a$

Ejemplo. Sabemos que $(R,\cdot)$ y $(R,+)$ son semigrupos. En el primer caso la potencia enésima de $a \in R$, se denota como usualmente en las estructuras de semigrupo en general, por a^n; sin embargo, en el segundo caso, en el aditivo, la potencia enésima de $a \in R$, no se le llama así usualmente, y se denota por na *o* $n \cdot a$.

Si en una estructura algebraica $(S,*)$ dada, la operación satisface el axioma de conmutatividad, se dirá que dicha estructura es conmutativa.

Teorema 4.2.1.2.- (de la potencia enésima de un producto)

Sea $(S,*)$ un semigrupo conmutativo, Entonces:

$$\forall x, y \in S, \forall n \in N, (x * y)^n = x^n * y^n.$$

Demostración:

Hacemos la demostración por inducción. Sean $x,y \in S$ arbitrarios, entonces: $(x * y)^1 = x * y$ por definición; si suponemos que $(x * y)^n = x^n * y^n$, entonces:

$$\begin{aligned}
(x * y)^{n+1} &= (x * y)^n * (x * y), && \text{por definición} \\
&= (x^n * y^n) * (x * y), && \text{por hipótesis de inducción} \\
&= \Big((x^n * y^n) * y\Big) * y, && \text{por asociatividad} \\
&= \Big(x^n * (y^n * x)\Big) * y, && \text{por asociatividad} \\
&= \Big(x^n * (x * y^n)\Big) * y, && \text{por conmutatividad} \\
&= \Big((x^n * x) * y^n\Big) * y, && \text{por asociatividad} \\
&= \Big((x^n * x) * (y^n * y)\Big), && \text{por asociatividad} \\
&= x^{n+1} * y^{n+1}, && \text{por definición.}
\end{aligned}$$

Luego, está demostrada la propiedad

4.2.2. Monoide

El hecho de que un semigrupo posea elemento identidad, por su importancia, va a caracterizar una nueva estructura algebraica.

- **Definición. (de monoide)** Sea $(S,*)$ un semigrupo. Si esta estructura satisface el axioma de existencia de elemento identidad, es decir, si existe $e \in S$, tal que $e * x = x * e = x$, *para todo* $x \in S$, diremos que $(S,*)$ es un monoide.

Ejemplo 1. $(R,+)$ y $(R,\cdot)$ son monoides con identidades 0 y 1 respectivamente.

Ejemplo 2. El conjunto de matrices de orden 2×2 con entradas de números reales, con la adición y con la multiplicación de matrices, son monoides con identidades $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ y $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ respectivamente.

La existencia de elemento identidad en una estructura algebraica garantiza su unicidad.

Teorema 4.2.2.1. (de unicidad del elemento identidad)

Sea $(S,*)$ un sistema algebraico con identidad. Entonces el elemento identidad es único.

Demostración:

Inmediata, se asume que existen dos elementos identidades y aplicando la definición de elemento identidad a cada uno de ellos, se obtiene que tienen que ser iguales.

En el estudio de ecuaciones algebraicas, la existencia de "elemento inverso" es esencial.

- **Definición. (de elemento inversible)** Sea $(S,*)$ una estructura algebraica con elemento identidad "e". Sea $x \in S$. Diremos que x es inversible si, y sólo si, existe $y \in S$ tal que $x * y = y * x = e$.

A tal y se le llama inverso de x, y se denota por: $y = x^{-1}$

Teorema 4.2.2.2. (el inverso, en un monoide, es único)

Sea $(S,*)$ un monoide con elemento identidad "e". Sean $x,y \in S$. Si x es inversible y $x * y = e$ *o* $y * x = e$, entonces $y = x^{-1}$.

Demostración:

Supongamos que $y * x = e$, entonces, como x es inversible existe x^{-1}, y

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

Notemos que en la tercera igualdad se requirió la asociatividad.

En forma análoga, se puede probar que $y = x^{-1}$, si $x * y = e$.

Por tanto, queda probada la propiedad.

Nota: *En el caso de la estructura* $(S,+)$, *el inverso de* $x \in S$, *se le llama usualmente inverso aditivo u opuesto de* x, *y se le denota por* $-x$.

Teorema 4.2.2.3. (el inverso del inverso de un elemento, es el propio elemento)

Sea $(S,*)$ un monoide con elemento identidad "e". Sea $x \in S$. Si x es inversible en $(S,*)$, entonces x^{-1} también lo es, y $(x^{-1})^{-1} = x$.

Demostración:

Como x es inversible, por su definición, x^{-1} también lo es, y $x * x^{-1} = e$.

Luego, por el teorema anterior,

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

Teorema 4.2.2.4. (la identidad es inversible en un monoide)

Sea $(S,*)$ un monoide con elemento identidad "e". Entonces e es inversible.

Demostración:

Inmediata, basta aplicar la definición de elemento identidad aplicada al propio e, y obtenemos que es inversible y su inverso es el mismo, es decir, $e^{-1} = e$

Teorema 4.2.2.5.- (del inverso del producto de dos elementos inversibles)

Sea $(S,*)$ un monoide con elemento identidad "e". Sean $x,y \in S$. Si x e y son inversibles entonces: $x * y$ es inversible y $(x * y)^{-1} = y^{-1} * x^{-1}$.

Demostración:

$$(x * y) * (y^{-1} * x^{-1}) = x * \left(y * (y^{-1} * x^{-1})\right) \quad \text{Por asociatividad}$$

$$= x * \left((y * y^{-1}) * x^{-1}\right) \quad \text{Por asociatividad}$$

$$= x * (e * x^{-1}) \quad \text{Por inverso}$$

$$= x * x^{-1} \quad \text{Por identidad}$$

$$= e \quad \text{Por inverso.}$$

En forma análoga se prueba que: $(y^{-1} * x^{-1}) * (x * y) = e$ Por tanto, $x * y$ es inversible, y por la unicidad del inverso: $(x * y)^{-1} = y^{-1} * x^{-1}$

4.2.3. Grupo

Para muchos, la estructura de grupo es la estructura algebraica mas importante, entre las simples. En ella se generalizan las propiedades de la estructura de $(R,+)$.

- **Definición de grupo.-** El sistema algebraico $(G,*)$ es llamado un grupo, si y sólo si, se satisfacen las siguientes propiedades, llamadas axiomas de grupo:

  1) $*$ es una operación asociativa
  2) $(G,*)$ tiene elemento identidad, e
  3) Todo elemento de G es inversible.

En otras palabras $(G,*)$ es un grupo, si y sólo si, es un monoide en que todos sus elementos son inversibles. Si un grupo $(G,*)$ satisface el axioma de conmutatividad, es decir, que $x * y = y * x$, *para todo* $x,y \in G$, entonces decimos que el grupo es abeliano o conmutativo.

Ejemplo 1.- $(R,+)$ y $(R\text{-}\{0\},\cdot)$ son grupos. Pero $(R,\cdot)$ no es un grupo pues 0 no es inversible.

Ejemplo 2.- El conjunto de matrices de orden 2×2, con entradas reales y con la operación de adición de matrices, es un grupo, pues es un monoide, y toda matriz $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ tiene inversa aditiva que es: $-A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$

Sin embargo, con la operación de multiplicación de matrices, no es un grupo, pues hay muchas matrices que no tienen inversas según la multiplicación (todas las que tienen determinante 0).

Si el conjunto G es un conjunto finito con n elementos, y $(G,*)$ es un grupo, entonces se dice que $(G,*)$ es un grupo finito de orden n.

Ejemplo 3.- Sea Z_n el conjunto de los enteros congruentes módulo n, para n un número natural cualquiera, y definamos la operación de adición en Z_n por:

$\overline{x} + \overline{y} = \overline{x + y}$, donde la suma $x + y$ es la usual en Z.

Debemos probar que la operación de adición está bien definida en Z_n, es decir, que el resultado de esta operación no depende de los elementos que representan las clases involucradas. Esto significa probar que si $\overline{x}_1 = \overline{x}_2$ y $\overline{y}_1 = \overline{y}_2$ entonces $\overline{x_1 + y_1} = \overline{x_2 + y_2}$

Supongamos que $\bar{x}_1 = \bar{x}_2$ y $\bar{y}_1 = \bar{y}_2$, luego existen $k,m \in Z$, tales que $x_1 - x_2 = kn$ y $y_1 - y_2 = mn$.

Entonces, aplicando las propiedades de la adición de enteros,

$(x_1 + y_1) - (x_2 + y_2) = (k + m)\, n$, y por tanto, $\overline{x_1 + y_1} = \overline{x_2 + y_2}$

Es evidente, por las propiedades correspondientes de los enteros, que $(Z_n,+)$ es un grupo finito y conmutativo de orden n.

Teorema 4.2.3.1.- (sobre la solución de ciertas ecuaciones en un grupo)

Sea $(G,*)$ un grupo, y sean a, b , $x \in G$. Entonces:

$$1)\ a * x = b \quad \text{si y sólo si } x = a^{-1} * b$$

y en forma análoga

$$2)\ x * a = b \quad \text{si y sólo si } x = b * a^{-1}.$$

Demostración:

Demostremos la primera, pues la segunda se hace en forma análoga, y la dejamos como ejercicio.

$x = e * x = (a^{-1} * a) * x = a^{-1} * (a * x) = a^{-1} * b$. Por tanto, si $a * x = b$, entonces $x = a^{-1} * b$.

Por otro lado, si $x = a^{-1} * b$, entonces $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$.

Por tanto, está demostrada la doble implicación.

Teorema 4.2.3.2. (sobre la propiedad cancelativa en los grupos)

Sea $(G,*)$ un grupo y sean $a,b,c \in G$. Si $a * b = a * c$ o $b * a = c * a$, entonces $b = c$. Es decir, la operación en un grupo, tiene la propiedad cancelativa.

Demostración:

Supongamos que $a * b = a * c$. Entonces:

$b = e * b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = (a^{-1} * a) * c = e * c = c$.

En forma análoga se obtiene el resultado si $b * a = c * a$, y se deja como ejercicio.

Por tanto, está probada la propiedad cancelativa en los grupos.

Teorema 4.2.3.3. (sobre la potencia enésima en grupos finitos)

Sea $(G,*)$ un grupo finito, y sea $a \in G$ un elemento de G arbitrario. Entonces existe $n \in N$, tal que, $a^n = e$

Demostración:

Como G es finito y toda potencia de a tiene que estar en G, se tiene que existen potencias distintas que dan el mismo elemento, pues como

el conjunto de números naturales es infinito, si no ocurriera así sería también infinito. Por tanto, existen $p,q \in N$, $p \neq q$ y $a^p = a^q$.

Sin perdida de generalidad podemos suponer que $p < q$. Entonces:

$$e = (a^p)^{-1} * a^p = (a^p)^{-1} * a^q = (a^p)^{-1} * (a^p * a^{q-p}) = \left((a^p)^{-1} * a^p\right) * a^{q-p} = e * a^{q-p} = a^{q-p}$$

Basta ahora tomar $n = q - p$, que es un número natural pues es un entero positivo.

- **Definición del orden de un elemento de un grupo finito.** Sea $(G,*)$ un grupo finito, y sea $a \in G$ un elemento de G arbitrario. Diremos que n es el orden de a, si y sólo si, $n = min\ \{ m \in N : a^m = e\}$

Notemos que este mínimo siempre existe pues, $\{ m \in N : a^m = e\} \neq \Phi$ y N está bien ordenado por $(\leq)$.

Ejemplo 4. Sea A un conjunto finito de n elementos, con $n \in N$. Entonces el conjunto de todas las biyecciones sobre A, con la operación de composición de funciones, forma un grupo, ¡pruébelo!, y es llamado el grupo de permutaciones de n elementos.

- **Definición. (de subgrupo).** Sea $(G,*)$ un grupo, y $H \subseteq G$. Entonces $(H,*)$ es llamado un subgrupo de $(G,*)$, si y sólo si, $(H,*)$ es un grupo.

  Nota.- Como la operación en un grupo es asociativa, entonces la expresión a^n está bien definida para todo $n \in N$, cuando $(G,*)$ es un grupo y $a \in G$. Además, en un grupo también se cumplen las leyes de los exponentes, es decir:

  $$\forall n, m \in N,\ \forall a \in G,\ a^n * a^m = a^{n+m} \quad y \quad a^{n \cdot m} = (a^n)^m.$$

- **Definición. (de grupo cíclico)** Un grupo $(G,*)$ se dice que es cíclico, si existe un elemento $a \in G$, tal que cualquier elemento de G se puede expresar como una potencia de a.

Ejemplo 5. $(Z_3,+)$ es un grupo cíclico de tres elementos. En él se cumplen las siguientes igualdades:

$$(\overline{1})^1 = \overline{1}, \qquad (\overline{1})^2 = \overline{1} + \overline{1} = \overline{2}, \qquad (\overline{1})^3 = \overline{1} + \overline{1} + \overline{1} = \overline{3} = \overline{0}.$$

4.2.4. Ejercicios propuestos sobre estructuras algebraicas simples

1) Pruebe que cada una de las siguientes estructuras algebraicas es un semigrupo:

   - $(N,*)$, donde $x * y$ es el mínimo en $\{x,y\}$.
   - $(N,*)$, donde $x * y$ es el máximo común divisor de x y y.
   - $(P(A),\cap)$, donde A es un conjunto arbitrario y $P(A)$ es su potencia.
   - $(N,*)$, donde $x * y$ es el máximo en $\{x,y\}$.
   - $(N,*)$, donde $x * y$ es el mínimo común múltiplo de x y y.

2) ¿Cuáles de los semigrupos dados a continuación es también un monoide?

   - $(N,*)$, donde $x * y$ es el mínimo en $\{x,y\}$.
   - $(N,*)$, donde $x * y$ es el máximo común divisor de x y y.
   - $(P(A),\cap)$, donde A es un conjunto arbitrario y $P(A)$ es su potencia.
   - $(N,*)$, donde $x * y$ es el máximo en $\{x,y\}$.
   - $(N,*)$, donde $x * y$ es el mínimo común múltiplo de x y y.

3) ¿Cuáles de las matrices dadas a continuación son inversibles respecto a la multiplicación?

- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$
- $\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$

4) Asuma que $(S,*)$ es un monoide con identidad e y que x y y son elementos inversibles en S. Pruebe que:

- $x * y = (x * y^{-1}) * y^2$.
- $(x * y)^{-1} * x = y^{-1}$.
- $(x^2)^{-1} * x = x^{-1}$.

5) Sea A un conjunto finito de n elementos, con n un número natural, sea P_n el conjunto de todas las biyecciones $f: A \to A$, y sea $\circ$ la composición de funciones. Demuestre que $(P_n, \circ)$ es un grupo, el cual, como dijimos antes, es llamado el grupo de permutaciones de n elementos.

6) Represente en una tabla de operación el grupo de permutaciones de tres elementos.

7) Demuestre que para cada $n \in N$, $(Z_n, +)$ es un grupo conmutativo.

8) Construya la tabla de doble entrada de $(Z_6, +)$ y encuentre el orden de cada uno de sus elementos.

9) Sea $(S,*)$ un monoide y sea A el conjunto de todos los elementos inversibles de $(S,*)$. Pruebe que $(A,*)$ es un grupo.

10) Construya la tabla de doble entrada del grupo cíclico de orden 5, y encuentre el orden de cada uno de sus elementos.

11) Decida, en cada caso, si el sistema algebraico dado es un grupo o no. Justifique su respuesta:

- $\left(P(A),\Delta\right)$, donde donde A es un conjunto arbitrario, $P(A)$ es su potencia, y Δ es la diferencia simétrica de conjuntos.
- $(R-\{1\},*)$, donde $x * y = x + y - xy$.
- $(H,\circ)$, donde H es el conjunto de todas las funciones $f: R \to R$, de la forma $f(x) = ax + b$ para $a,b \in R$, y $\circ$ representa la composición de funciones.

12) ¿Es el grupo de permutaciones de tres elementos un grupo cíclico?. Justifique su respuesta.

13) Explique porqué un grupo cíclico finito tiene que ser abeliano.

4.2.5. Isomorfismos algebraicos entre estructuras algebraicas simples

En el capítulo anterior, cuando estudiamos conjuntos ordenados, definimos los isomorfismos de orden como biyecciones entre estructuras de orden que preservan sus órdenes. Además, definimos que una propiedad es de orden, cuando la propiedad se mantiene por isomorfismos de orden entre dos estructuras de orden isomorfas cualesquiera.

Es natural ahora, al estudiar estructuras algebraicas, definir lo que entendemos como isomorfismos algebraicos. Estos deben ser biyecciones entre estructuras algebraicas que preservan sus estructuras desde el punto de vista algebraico, es decir, preservan la operación; y así mismo

las propiedades algebraicas deben definirse como las propiedades que se mantienen por isomorfismos entre estructuras algebraicas isomorfas.

- **Definición. (de homomorfismo algebraico)** Sean $(A,*)$ y $(B,\otimes)$ dos sistemas algebraicos. Entonces la aplicación $f: A \to B$ se dice que preserva la estructura algebraica o la operación, si y sólo si,

$$\forall x, y \in A, f(x * y) = f(x) \otimes f(y).$$

En ese caso decimos que f aplica $(A,*)$ en $(B,\otimes)$, lo que se representa por $f: (A,*) \to (B,\otimes)$, y además que f es un homomorfismo de $(A,*)$ en $(B,\otimes)$.

- **Definición. (de estructuras algebraicas isomorfas)** Sean $(A,*)$ y $(B,\otimes)$ dos sistemas algebraicos. Nosotros decimos que $(A,*)$ es isomorfa a $(B,\otimes)$, y lo denotamos por $(A,*) \cong (B,\otimes)$, si y sólo si, existe una biyección $f: A \to B$, que preserva la operación, es decir, que es un homomorfismo algebraico. En ese caso, nosotros también decimos que f es un isomorfismo algebraico o simplemente isomorfismo de $(A,*)$ en $(B,\otimes)$.

Teorema 4.2.5.1. (sobre propiedades algebraicas)

Sean $(A,*)$ y $(B,\otimes)$ dos sistemas algebraicos, tales que $(A,*) \cong (B,\otimes)$.

Entonces:

1. Si $*$ es asociativa, entonces $\otimes$ también lo es.
2. Si $*$ es conmutativa, entonces $\otimes$ también lo es.
3. Si $(A,*)$ tiene elemento identidad, entonces $(B,\otimes)$ también lo tiene.

4. Si cada elemento de A es inversible en $(A,*)$, entonces cada elemento de B es inversible en $(B,\otimes)$.
5. $\forall m,n \in N$, si $(A,*)$ es un grupo finito con m elementos de orden n, entonces $(B,\otimes)$ es un grupo finito con m elementos de orden n.
6. Si $(A,*)$ es un grupo cíclico, entonces $(B,\otimes)$ es un grupo cíclico también.

Demostración.

Sea f: $(A,*) \rightarrow (B,\otimes)$ un isomorfismo.

Demostración de 1:

Supongamos que $*$ es asociativa.

Sean $y_1, y_2, y_3 \in B$, entonces existen $x_1, x_2, x_3 \in A$, tales que

$f(x_1) = y_1$, $f(x_2) = y_2$, $f(x_3) = y_3$, por ser f sobre, al ser biyectiva.

Entonces:

$$y_1 \otimes (y_2 \otimes y_3) = f(x_1) \otimes \Big(f(x_2) \otimes f(x_3) \Big) = f(x_1) \otimes f(x_2 * x_3) =$$

$$f\Big(x_1 * (x_2 * x_3)\Big) = f\Big((x_1 * x_2) * x_3\Big) = f(x_1 * x_2) \otimes f(x_3) =$$

$$\Big(f(x_1) \otimes f(x_2) \Big) \otimes f(x_3) = (y_1 \otimes y_2) \otimes y_3.$$

Luego, $\otimes$ es asociativa también.

Por tanto, si $*$ es asociativa, entonces $\otimes$ también lo es.

Demostración de 2:

Supongamos que $*$ es conmutativa.

Sean $y_1, y_2 \in B$, entonces existen $x_1, x_2 \in A$, tales que:

$$f(x_1) = y_1 \ , \quad f(x_2) = y_2.$$

Luego: $y_1 \otimes y_2 = f(x_1) \otimes f(x_2) = f(x_1 * x_2) = f(x_2 * x_1) = f(x_2) \otimes f(x_1) = y_2 \otimes y_1$

Por tanto, si $*$ es conmutativa, entonces $\otimes$ también lo es.

Demostración de 3:

Supongamos que $(A,*)$ tiene elemento identidad "e".

Sea y un elemento arbitrario de B. Entonces existe $x \in A$, tal que $f(x) = y$, luego:

$$y \otimes f(e) = f(x) \otimes f(e) = f(x * e) = f(x) = y.$$

En forma análoga, se obtiene que $f(e) \otimes y = y$.

Así, hemos probado que $(B, \otimes)$ tiene elemento identidad y es $f(e)$.

Por tanto, si $(A,*)$ tiene elemento identidad e, entonces $(B, \otimes)$ también tiene elemento identidad, y es $f(e)$.

Demostración de 4:

Supongamos que cada elemento de A es inversible en $(A,*)$.

Sea $y \in B$ arbitrario; luego existe $x \in A$, tal que $f(x) = y$. Como x es inversible, sea x^{-1} su inverso. Sea e el elemento identidad en $(A,*)$, y ya probamos, en el punto anterior, que $f(e)$ es el elemento identidad en $(B,\otimes)$.

Entonces: $y \otimes f(x^{-1}) = f(x) \otimes f(x^{-1}) = f(x * x^{-1}) = f(e)$ y, en forma análoga, se obtiene que: $f(x^{-1}) \otimes y = f(e)$.

Luego, y es inversible y $y^{-1} = f(x^{-1})$.

Por tanto, si cada elemento de A es inversible en $(A,*)$, entonces cada elemento de B es inversible en $(B,\otimes)$.

Demostración de 5:

Supongamos que $n,m \in N$ son arbitrarios, y que $(A,*)$ es un grupo finito con m elementos de orden n.

Como f es una biyección de A en B y A es finito, entonces B es finito y $card(A) = card(B)$. Por 1,3, y 4 demostrados anteriormente, si $(A,*)$ es un grupo, entonces $(B,\otimes)$ es un grupo. Por tanto, si $(A,*)$ es un grupo finito de orden n, entonces $(B,\otimes)$ es también un grupo finito de orden n.

Sea $a \in A$ un elemento de orden n, probemos $f(a)$ tiene orden n también.

Sea $e \in A$, la identidad de $(A,*)$, sabemos, por 3, que $f(e)$ es la identidad de $(B,\otimes)$. Ahora, $\left(f(a)\right)^n = f(a^n) = f(e)$

Luego el orden de $f(a)$ es menor o igual que n. Probemos que no puede ser menor. Sea $k \in N$, $k < n$ y supongamos que k es el orden de $f(a)$. Entonces:

$$f(e) = \Big(f(a)\Big)^k = f(a^k).$$

Esto cual implica que $a^k = e$, contradiciendo que el orden de a es n.

Por tanto, el orden de $f(a)$ en $(B,\otimes)$ es n al igual que el orden de a en $(A,*)$.

Pero, como f es una biyección, no puede haber elementos en $(B,\otimes)$ de orden n que no sean imágenes de elementos de A, los cuales tiene que tener orden n en $(A,*)$, por lo visto anteriormente.

Por tanto, *para cualesquiera* $m,n \in N$, si $(A,*)$ es un grupo finito con m elementos de orden n, entonces $(B,\otimes)$ es un grupo finito con m elementos de orden n.

Demostración de 6:

Sea $(A,*)$ un grupo cíclico. Supongamos sea $a \in A$ tal que para todo $x \in A$, existe $n \in N$, tal que $x = a^n$, el cual existe por ser $(A,*)$ un grupo cíclico.

Sea $y \in B$ arbitrario, luego existe $x \in A$, tal que $y = f(x)$, por ser f sobre. Entonces $y = f(x) = f(a^n) = \Big(f(a)\Big)^n$ y, por tanto, existe $b = f(a) \in B$ que cumple: "para todo $y \in B$ existe $n \in N$, tal que $b^n = \Big(f(a)\Big)^n = y$", es dedir, $(B,\otimes)$ es cíclico.

Por tanto, hemos demostrado que si $(A,*)$ **es un grupo cíclico, entonces** $(B,\otimes)$ **es un grupo cíclico también.**

En el epígrafe 3.3.2 probamos que la relación $A \equiv B$ es una relación de equivalencia sobre cualquier familia de conjuntos dada. Ahora podemos probar que el isomorfismo define una relación, que es de equivalencia sobre cualquier familia de sistemas algebraicos dados.

Teorema 4.2.5.2.- (sobre la equivalencia en una familia de sistemas algebraicos dados).

Sean $(A,*)$, $(B,\otimes)$ y $(C,\oplus)$ sistemas algebraicos. Entonces:

1) $(A,*) \cong (A,*)$.

2) Si $(A,*) \cong (B,\otimes)$ entonces $(B,\otimes) \cong (A,*)$.

3) Si $(A,*) \cong (B,\otimes)$ y $(B,\otimes) \cong (C,\oplus)$, entonces$(A,*) \cong (C,\oplus)$.

La demostración es trivial y se deja como ejercicio.

4.2.6. Ejercicios propuestos sobre estructuras algebraicas simples isomorfas

1) Demuestre el teorema sobre la equivalencia en una familia de sistemas algebraicos.

2) Decida cuáles de las siguientes funciones preservan la operación y justifique su decisión:

- f: $(\mathrm{R},+) \to (\mathrm{R}^+,\cdot)$, definida por $f(x) = e^x$.
- $f: \left([-\pi,\pi],+\right) \to \left([-1,1],+\right)$, definida por $f(x) = senx$.
- f: $(\mathrm{R},+) \to (\mathrm{R}^+,+)$, definida por $f(x) = |x|$.
- f: $(\mathrm{R},\cdot) \to (\mathrm{R}^+,\cdot)$, definida por $f(x) = |x|$.

- f: (R,+) → (R,+), definida por $f(x) = ax + b$, donde a y b son números reales fijos arbitrarios.

- f: (R,·) → (R,·), definida por $f(x) = ax + b$, donde a y b son números reales fijos arbitrarios.

3) Sea $A = \{0,1\}$.

   a) ¿Cuántas operaciones binarias diferentes sobre A hay? ¿Cuántas operaciones pueden definirse sobre A que sean asociativas y cuántas que tengan elemento identidad?

   b) Separe los posibles sistemas algebraicos $(A,*)$ en clases de equivalencia respecto a isomorfismos. ¿Cuántos grupos no-isomórficos de orden dos hay?

4) Explique porqué el grupo de permutaciones sobre tres elementos no es isomórfico al grupo cíclico de orden seis.

4.3. Estructuras algebraicas no simples

Hasta ahora, los sistemas algebraicos que hemos estudiado están formados por un conjunto no vacío y una operación binaria definida sobre el. El estudio de los sistemas numéricos nos indica la importancia de considerar estructuras formadas con dos operaciones binarias.

En este epígrafe veremos dos ejemplos de estas estructuras: los anillos y los campos o cuerpos.

En lo que sigue, denotaremos por "+" a una operación que llamaremos la operación de adición, y al producto por esta operación se le dará el

nombre de suma; así mismo, denotaremos por " $\cdot$ " a una operación que llamaremos multiplicación, y al producto por esta operación se la dará el nombre de producto.

4.3.1. Anillos

- **Definición de anillo**

Sea A un conjunto no vacío y, + y $\cdot$ operaciones binarias definidas sobre A. Diremos que $(A,+,\cdot)$ es un anillo, si las operaciones de adición "+", y de multiplicación "$\cdot$", definidas sobre A, cumplen con las siguientes propiedades, que son los axiomas de anillo:

1) $(A,+)$ es un grupo abeliano o conmutativo.

2) La multiplicación es asociativa, es decir, $(A,\cdot)$ es un semigrupo.

3) *Para cualesquiera* $x, y, z \in A$, se cumplen la ley distributiva izquierda y la ley distributiva derecha, es decir,
$x(y+z) = x\cdot y + x\cdot z$, y $(x+y)\cdot z = x\cdot y + y\cdot z$, respectivamente.

Un anillo $(A,+,\cdot)$ en el cual la multiplicación es conmutativa, se dice que es un anillo conmutativo.

Si $B \subset A$ y $(B,+,\cdot)$ es un anillo, decimos que $(B,+,\cdot)$ es un subanillo de $(A,+,\cdot)$.

Ejemplos. $(Z,+,\cdot)$, $(Q,+,\cdot)$ y $(R,+,\cdot)$ son anillos conmutativos, $(Z,+,\cdot)$ es un subanillo de $(Q,+,\cdot)$ y también lo es de $(R,+,\cdot)$. Además, $(Q,+,\cdot)$ es un subanillo de $(R,+,\cdot)$.

El elemento identidad de + se denotará en lo que sigue por 0, y se le llamará cero o identidad aditiva. De igual modo, al inverso del elemento a según +, se denotará por $-a$, y se le llamará inverso aditivo u opuesto de a.

Teorema 4.3.1.1. (algunas propiedades en un anillo)

Sea $(A,+,\cdot)$ un anillo con identidad aditiva 0. Entonces, para cualesquiera sean $x,y \in A$, se tiene que:

1) $0 \cdot x = x \cdot 0 = 0$

2) $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$

3) $(-x) \cdot (-y) = x \cdot y$

Demostración:

Demostración de 1: Sea $x \in A$. Usando que 0 es el neutro aditivo, y la propiedad distributiva, tenemos que $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Luego, por la propiedad cancelativa de +, $x \cdot 0 = 0$

En forma análoga se obtiene que $0 \cdot x = 0$.

Demostración de 2: Sean $x,y \in A$. Usando la propiedad distributiva, que $-x$ es el inverso aditivo de x, y lo demostrado en 1, tenemos que $(-x) \cdot y + x \cdot y = (-x + x) \cdot y = 0 \cdot y = 0$. Por tanto, de la definición de inverso aditivo, se obtiene que: $(-x) \cdot (y) = -(x \cdot y)$

En forma análoga, se obtiene que: $x \cdot (-y) = -(x \cdot y)$

Demostración de 3: Sabemos que el inverso aditivo de $-x$, es decir, el inverso aditivo del inverso aditivo de x, es el propio x.

Por lo demostrado en 2, sabemos que: $(-x) \cdot y$ es el inverso aditivo de $x \cdot y$, y que $(-x)\cdot(-y)$ es el inverso aditivo de $(-x) \cdot y$. Por tanto, $(-x)\cdot(-y) = x \cdot y$.

Al igual que en las estructuras algebraicas simples, en las que no son simples se tiene el concepto de isomorfismo y de estructuras isomorfas.

- **Definición de isomorfismo de anillos y de anillos isomorfos.** Sean $(A,+,\cdot)$ y $(B,\oplus,\otimes)$ dos anillos. Si $f: A \to B$ es una biyección que satisface, para cualesquiera sean $x,y \in A$, las propiedades:

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

  2) $f(x \cdot y) = f(x) \otimes f(y)$

Diremos entonces que $f: A \to B$ es un isomorfirmo entre el anillo $(A,+,\cdot)$ y el anillo $(B,\oplus,\otimes)$. En el caso que existe un isomorfismo de anillos entre dos anillos dados, diremos que estos anillos son isomorfos.

Al igual que antes, las propiedades algebraicas de un anillo son comunes entre todos los anillos isomorfos.

Por ejemplo: Si $(A,+,\cdot)$ y $(B,\oplus,\otimes)$ son anillos isomorfos y $(A,+,\cdot)$ es conmutativo ($x \cdot y = y \cdot x$, para todo $x, y \in A$), entonces $(B,\oplus,\otimes)$ es también conmutativo, ($u \otimes v = v \otimes u$, para todo $u, v \in B$)

4.3.2. Cuerpos o Campos

- **Definición de cuerpo o campo.-** Sea $(F,+,\cdot)$ un anillo conmutativo. Diremos que $(F,+,\cdot)$ es un cuerpo o campo si, y sólo si, $(F-\{0\},\cdot)$ es un grupo, es decir, si a los axiomas de anillo conmutativo, se le adicionan los axiomas de existencia de unidad o neutro de la multiplicación y el de la existencia de inverso multiplicativo para todo elemento de F, con la excepción del neutro de la adición o 0.

En todo lo que sigue, excepto que se especifique lo contrario, denotaremos por 0 y 1 respectivamente, a los neutros de la adición y la multiplicación de un cuerpo cualquiera.

Nota: Por supuesto que todas las propiedades que tienen los anillos, también las tienen los cuerpos.

Demostremos la siguiente propiedad de los cuerpos:

Propiedad de cuerpo.- Sea $(F,+,\cdot)$ un cuerpo y 1 la identidad o neutro de la multiplicación. Entonces para todo $x \in F$ se tiene que $-x = (-1)\cdot x$.

La demostración de esta propiedad se reduce a probar que $(-1)\cdot x$ es el inverso aditivo de x, y para ello basta probar que $(-1)\cdot x + x = 0$.

Usando el axioma de la identidad multiplicativa, la propiedad distributiva, el axioma del inverso aditivo y la propiedad 1 del teorema sobre propiedades de anillos, obtenemos inmediatamente lo que se quiere probar, y esto es:

$$(-1)\cdot x + x = (-1)\cdot x + 1\cdot x = (-1+1)\cdot x = 0\cdot x = 0.$$

Ejemplos de cuerpos: $(Q,+,\cdot)$, y $(R,+,\cdot)$ son cuerpos. Y, análogamente al caso de los anillos, $(Q,+,\cdot)$ es un subcuerpo de $(R,+,\cdot)$.

Un ejemplo de cuerpo finito lo es $(Z_3,+,\cdot)$

- **Definición de diferencia y cociente.-** Sea $(F,+,\cdot)$ un cuerpo, y $x,y \in F$ arbitrarios. Entonces:

  1) la diferencia de x y y se denota, y viene definida por: $x - y = x + (-y)$ donde $-y$ es el inverso aditivo de y.

  2) Si $y \neq 0$, el cociente de x y y se denota, y viene definido por:

  $$x \div y = \frac{x}{y} = x \cdot (y^{-1})$$ donde y^{-1} es el inverso multiplicativo de y.

Teorema 4.3.2.1.- (algunas propiedades de los cuerpos)

Sea $(F,+,\cdot)$ un cuerpo.

1) Sean $a,b \in F$, $a \neq 0$. Entonces la ecuación $a \cdot x + b = 0$ tiene solución única $x = a^{-1} \cdot (-b)$.
2) Cualesquiera sean $x,y \in F$, si $x \cdot y = 0$, entonces $x = 0$ o $y = 0$.
3) Cualesquiera sean $x,y,z \in F$, $x \cdot (y - z) = x \cdot y - x \cdot z$

Demostración:

Demostración de 1. $a \cdot x + b = 0$, si y sólo si, $a \cdot x$ es el inverso aditivo de b, es decir, si y sólo si, $a \cdot x = -b$. Pero $a \cdot x = -b$, equivale a que $a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (-b)$, luego usando la asociatividad, el axioma de inverso multiplicativo, y el de identidad multiplicativa, esto último equivale a que: $x = a^{-1} \cdot (-b)$.

Al probarse que *para todo* $x \in F$ $a \cdot x + b = 0$ si y sólo si $x = a^{-1} \cdot (-b)$, queda probada también la unicidad de la solución.

Demostración de 2. Supongamos que $x \neq 0$. Si $x \cdot y = 0$, entonces $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$, y ahora, usando la asociatividad, el axioma del inverso multiplicativo, y el de identidad multiplicativa, así como la propiedad 1 del teorema correspondiente a las propiedades de anillos, se obtiene que $y = 0$.

En forma análoga se demuestra que, si $y \neq 0$, entonces $x = 0$.

Demostración de 3. Se obtiene en forma inmediata usando la definición de diferencia, la propiedad distributiva, y la propiedad 2 del teorema correspondiente a las propiedades de anillos.

- **Definición de cuerpo ordenado.** Sea $(F,+,\cdot)$ un cuerpo. Se dice que $(F,+,\cdot)$ es un cuerpo ordenado, si y sólo si, existe un subconjunto no vacío $P \subset F$, cuyos elementos diremos que son los elementos positivos de F, que satisface las siguientes propiedades, llamados axiomas de cuepo ordenado:

  1) $0 \notin P$.
  2) P es cerrado por la adición y la multiplicación, es decir, la suma y el producto de elementos de P es un elemento de P.
  3) Para todo $x \in F$, si $x \neq 0$ y $x \notin P$, entonces $-x \in P$.

Los elementos de F diferentes de 0, y que no pertenecen a P, es decir, que no son positivos, se les llama negativos.

Teorema 4.3.2.2. (el producto de elementos negativos es positivo)

Sea $(F,+,\cdot)$ un cuerpo ordenado, y $x,y \in F-\{0\}$ elementos negativos arbitrarios. Entonces $x \cdot y$ es positivo.

Demostración:

Usando la propiedad 3 del teorema sobre propiedades de anillos obtenemos que $x \cdot y = (-x) \cdot (-y)$. Por tanto, si $x,y \in F-\{0\}$ son negativos, su producto es el producto de los elementos $-x$ y $-y$, los cuales son positivos por el axioma 3 de la definición de cuerpo ordenado, y este producto es positivo por el correspondiente axioma 2.

- **Definición. (de <)** Sea $(F,+,\cdot)$ un cuerpo ordenado, sea P el conjunto de elementos positivos de F, y sean $x,y \in F$ arbitrarios. Decimos que x es menor que y, y lo denotamos por $x < y$, si y sólo si, $y - x \in P$

Decir que $x < y$ equivale a decir que y es mayor que x, lo cual se denota por $y > x$.

Las reglas que usamos en álgebra elemental para resolver inecuaciones, conforman un teorema sobre propiedades de orden en los cuerpos ordenados.

Teorema 4.3.2.3. (propiedades de <)

Sea $(F,+,\cdot)$ un cuerpo ordenado, y sean $x,y \in F$ arbitrarios. Entonces se cumplen las siguientes aserciones:

1. Exactamente una de la siguientes proposiciones es verdadera: $x < y$, $x = y$, o $y < x$
2. Si $x < y$ y $y < z$, entonces $x < z$.
3. Si $x < y$, entonces $x + z < y + z$.
4. Si $x < y$ y $0 < z$, entonces $x \cdot z < y \cdot z$.

Demostración:

Demostración de 1. Sabemos que, $x = y$ equivale a que $y \cdot x = 0$, para ello basta sumar a ambos miembros de la igualdad el inverso aditivo de x, y usar las propiedades correspondientes. Luego, si $x = y$ entonces $y - x \notin P$ y, por tanto, $x < y$ es falso. En forma análoga se tiene que $x = y$ equivale a que $x - y = 0$, de donde se obtiene que, si $x = y$ entonces $y < x$ es también falso.

Si $x \neq y$, entonces $y - x \neq 0$, y usando el axioma 3 de cuerpo ordenado, se obtiene que si $x < y$ es falso entonces $y < x$ es verdadero, y viceversa. En forma análoga, usando la equivalencia de $x \neq y$ con $x - y \neq 0$, si $y < x$ es falso, entonces $x < y$ es verdadero, y viceversa.

Si $x < y$ y $y < x$ son verdaderos, entonces $y - x \in P$ y $x - y \in P$, de donde la suma $(y - x) + (x - y) = 0 \in P$, lo que es una contradicción.

Como todo elemento de F es cero o diferente de cero, queda probada 1.

Demostración de 2. Se obtiene inmediatamente usando el hecho de que P es cerrado para la adición.

Demostración de 3. Se obtiene inmediatamente del hecho evidente de que $y - x \in P$ equivale a que $(y + z) - (x + z) \in P$

Demostración de 4. Se obtiene inmediatamente usando el hecho de que P es cerrado para la multiplicación.

- **Definición. (de ≤)** Sea $(F,+\cdot)$ un cuerpo ordenado y $x,y \in F$ arbitrarios, decimos que x es menor o igual que y, y lo denotamos por $x \leq y$, si y sólo si, $x < y$ *o* $x = y$.

Ahora se puede enunciar el siguiente teorema, cuya demostración es evidente y se deja como ejercicio.

Teorema 4.3.2.4.- (cuerpo ordenado como conjunto totalmente ordenado)

Sea $(F,+\cdot)$ un cuerpo ordenado. Entonces $(F,\leq)$ es un conjunto totalmente ordenado.

4.3.3. Ejercicios propuestos

1) Sean $(A,+,\cdot)$ y $(B,\oplus,\otimes)$ dos anillos isomorfos. Demuestre que:

   - Si $(A,+,\cdot)$ es conmutativo, entonces $(B,\oplus,\otimes)$ también lo es.
   - Si $(A,+,\cdot)$ tiene neutro o unidad multiplicativa, entonces $(B,\oplus,\otimes)$ también la tiene.
   - Si $(A,+,\cdot)$ cumple con los axiomas de cuerpo, entonces $(B,\oplus,\otimes)$ también los cumple.

2) Sea $(G,+)$ un grupo abeliano o conmutativo. Pruebe que $(G,+,\cdot)$ es un anillo, donde $\cdot$ está definida por: $x \cdot y = 0$, *para todo* $x,y \in G$

3) Sea $nZ = \{nz : z \in Z\}$. Pruebe que $(nZ, +, \cdot)$, donde $+$ y $\cdot$ son la adición y multiplicación usuales, es un anillo *para todo* $n \in N$.

4) Pruebe que los anillos $(2Z, +, \cdot)$ y $(3Z, +, \cdot)$ no son isomorfos.

5) Dé un ejemplo de un anillo con unidad multiplicativa, y de un subanillo de este anillo con unidad multiplicativa diferente a la del anillo. Demuestre que en el caso de los campos esto no es posible, es decir, la unidad multiplicativa de todo subcampo de un campo dado, es la unidad del campo.

6) Sea $(A, +, \cdot)$ un anillo. Si a y b son elementos de A diferentes de 0 tales que $a \cdot b = 0$, entonces decimos que a y b son divisores de 0; a es un divisor izquierdo y b lo es derecho. Demuestre que en el anillo $(Z_n, +, \cdot)$ los divisores de 0 son aquellos elementos que no son primos relativos con n.

7) Pruebe que si p es primo, entonces $(Z_p, +, \cdot)$ es un cuerpo o campo.

8) Pruebe que la identidad aditiva en un cuerpo no tiene inverso multiplicativo.

9) Pruebe que si x es un elemento de un cuerpo, y $x^2 = x \cdot x = 0$, entonces $x = 0$.

10) ¿Si x y y son elementos de un cuerpo y $x^2 + y^2 = 0$, es necesario que $x = y = 0$? Explique su respuesta.

11) ¿Tiene solución la ecuación $x^2 = a$ para todo valor de a, en el cuerpo $(Z_5, +, \cdot)$? Explique su respuesta.

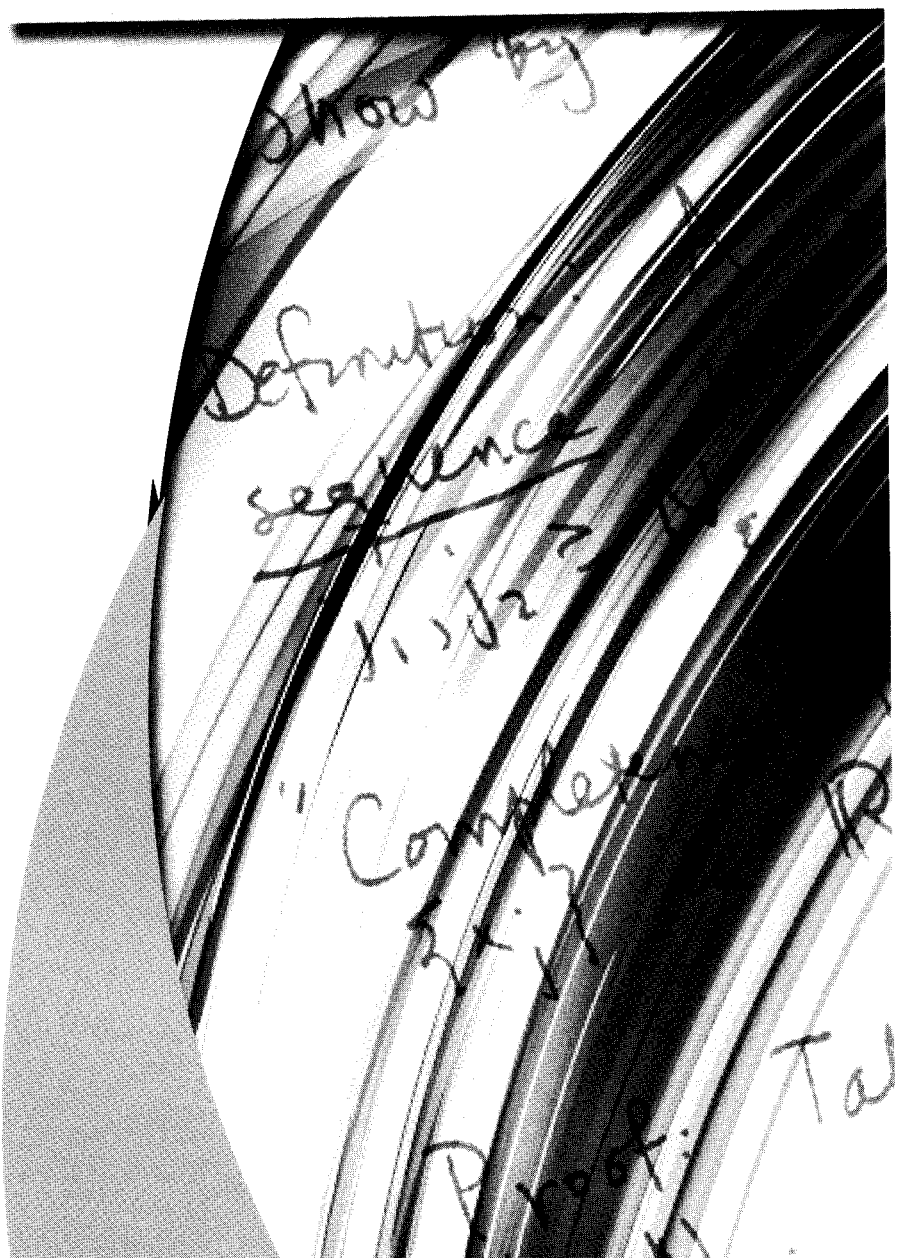
12) Sean $(F,+,\cdot)$ un cuerpo ordenado, P el conjunto de sus elementos positivos, y $x,y \in F-\{0\}$. Pruebe cada una de las siguientes proposiciones:

- Si $x \in P$ y $y \notin P$, entonces $x \cdot y \notin P$.
- $x \cdot (-x) \notin P$.
- $x^2 \in P$.
- $1 \in P$.
- Si $x \in P$, entonces $x^{-1} \in P$.

13) Sean $(F,+,\cdot)$ un cuerpo ordenado y P el conjunto de sus elementos positivos. Pruebe cada una de las proposiciones siguientes:

- $1 + 1 \neq 0$.
- Para todo $x \in F$, $x < x + 1$.
- Para todo $x \in P$, $-x < x$.
- Para todo $x \in F$, $x \in P$, si y sólo si $0 < x$.
- Para todo $x \in F-\{0\}$, $0 < x^2$.

5 Conjuntos Numéricos



5. Introducción: Sobre el concepto de número

El concepto de número es un resultado del desarrollo de la Matemática y fue formado en el transcurso de un largo y prolongado proceso histórico. Todavía hoy en día algunos confunden el número, cuyo concepto es abstracto e independiente del sistema de numeración que se emplee, con el símbolo que se utiliza para representarlo.

En la estructura de la Matemática, además de las proposiciones y teoremas, están los conceptos sobre los que éstos se sustentan. La extensión de los conceptos matemáticos es infinita, por lo que la manera de definir un concepto matemático no es por extensión sino por comprensión. Otras dos características de la Matemática que la distinguen de las Ciencias Naturales y la acercan a la Lógica son: que sus razonamientos son hipotético-deductivos y sus definiciones son nominales, no reales.

Muchas veces vemos que se definen los números naturales, los enteros, y posteriormente los racionales mediante los símbolos que los representan, u operaciones no definidas entre estos símbolos y luego, haciendo una referencia en el sistema de numeración decimal, "distinguen" teóricamente sin base razonada alguna, los irracionales de los racionales, en los reales.

Aunque el tratamiento del concepto de número mediante la simbología que se usa para representarlo no es la forma matemática de hacerlo, debe ser considerada adecuada en el nivel básico, pues los niños no tiene desarrolladas las estructuras cerebrales para hacer abstracción y pueden,

sin embargo, acercarse así al concepto por las propiedades de sus operaciones aunque sea sin rigor. No obstante, ya en el nivel medio, donde se debe desarrollar el pensamiento abstracto, racional y crítico en nuestros estudiantes, el maestro de matemática debe dominar sus fundamentos, en particular los correspondientes al concepto de número y la teoría de números.

En la primera parte del capítulo se hace el estudio, en forma esquemática, del concepto de número natural teniendo como base los axiomas de Peano. En la segunda parte se define el número entero por abstracción y se prueba que el conjunto de números naturales está inmerso en el de los enteros.

En la tercera parte se vuelve a dar una definición por abstracción, ahora del concepto de número racional, y también se justifica como una necesidad de tipo algebraica, se vuelven a extender las definiciones de adición y multiplicación, en este caso a los racionales, y se prueba que el conjunto de los enteros está inmerso en el de los racionales.

En la cuarta parte se construyen los números reales por abstracción usando clases de sucesiones contiguas. Aquí se justifica la necesidad de la creación de este nuevo campo numérico, no por una necesidad de tipo algebraica, sino para poder darle carácter de continuo al nuevo campo mediante un isomorfismo con los puntos de una recta ordenada. Se vuelven a extender las definiciones de adición y multiplicación a este campo, y se prueba que el conjunto de los racionales está inmerso en el de los reales.

5.1 PRIMERA PARTE: NÚMERO NATURAL

5.1.0. Introducción a la primera parte

El concepto de número es un resultado del desarrollo de la Matemática y fue formado en el transcurso de un largo y prolongado proceso histórico. Las raíces de este concepto se pueden encontrar en la necesidad de contar o en la necesidad de relacionar conjuntos según la cantidad de sus elementos, las cuales se remontan a épocas anteriores a la existencia de escritura y de las que sólo existen datos indirectos proporcionados por la lingüística y la etnografía.

Posiblemente no se logre nunca conocer con precisión como era que pensaba el hombre primitivo, pero parece lógico aceptar que la necesidad de expresarse y de pensar ocurrieron simultáneamente, y junto con ella debe haber estado presente en algún grado la de contar, medir longitudes, áreas y volúmenes, la de estimar el peso de algunos cuerpos y, muy importante, la del concepto de orden. Inicialmente el hombre utilizó diversos objetos para contar: dedos, piedras, etc, y con el uso de más y más "números", surgieron símbolos para representarlos.

Una característica de los primeros períodos de la historia de la cultura humana es la diversidad de sistemas de símbolos para representar los números y, con la necesidad de hacer operaciones con ellos la creación de diversos Sistemas de Numeración. Gradualmente, en el transcurso de un largo proceso histórico, se perfeccionaron y unificaron los sistemas de numeración, hasta la aceptación universal del Sistema de Numeración Decimal, el cual es utilizado actualmente por todos los países.

Todavía hoy en día algunos confunden el número, cuyo concepto es abstracto e independiente del sistema de numeración que se emplee, con el símbolo que se utiliza para representarlo. La historia y el perfeccionamiento del concepto de número están íntimamente relacionados con la historia de la matemática en general.

La matemática fue vista por mucho tiempo como una ciencia que representa directamente a la realidad, y su motor para el desarrollo fue la Física. Actualmente es un bello Arte al mismo tiempo que es Ciencia, y ella misma genera su propio motor para desarrollarse, ya sea a través de la obtención de nuevos resultados o teoremas con bellas demostraciones en teorías conocidas o, mediante la creación de nuevas teorías matemáticas modernas, donde las relaciones y formas se presentan de manera abstracta mediante conjuntos de elementos cuyas propiedades y reglas de operación se dan con ayuda de un sistema de axiomas.

En Matemática los tipos de conceptuación que más interesan, por ser creadoras de nuevos conceptos, son las definiciones por abstracción, por recurrencia y las definiciones axiomáticas, ya que las definiciones explícitas sólo son clasificatorias, en ellas sólo se usan palabras o símbolos nuevos para conceptos ya definidos.

En esta primera parte del capítulo se hace el estudio, en forma esquemática, del concepto de número natural teniendo como base los axiomas de Peano.

Muchos maestros discuten sobre si el cero debe ser considerado un número natural o no. Históricamente hablando, el cero no había sido creado aún cuando ya otros números lo habían sido.

Si se asume la posición de introducir el concepto de número natural para resolver el problema de contar y, teniendo en cuenta que se comienza a contar por el uno, el cero no debería ser considerado un número natural. Es decir, los números naturales introducidos como ordinales deben empezar en uno. Sin embargo, si se asume la posición de introducir el concepto de número natural para relacionar los conjuntos por las cantidades de los elementos que poseen, a través del concepto de cardinal, y por tanto, tratarlo como un concepto derivado de la Teoría de Clases, entonces el cero debería ser considerado como el primer número natural atendiendo a que es el cardinal del conjunto vacío.

Estimo que no reviste importancia, desde un punto de vista conceptual, que posición se asume en la discusión anterior, la cual creo que es estéril pues es un simple asunto clasificatorio y tomar un criterio.

La distinción entre introducir el concepto de número natural mediante su consideración ordinal o cardinal, no sólo debe diferenciar si el cero se va a considerar natural o no, lo cual como dijimos sólo tiene importancia clasificatoria, sino que conduce a dos aspectos del concepto de número natural que corresponden a dos vías diferentes para fundamentarlo, y esto sí es importante. Para los conjuntos finitos ambas vías llevan al mismo resultado, sin embargo, para los conjuntos infinitos no es así y la diferencia es esencial, pues según sea el orden elegido para contar, resulta un número ordinal diferente.

Si el número natural se introduce por su aspecto ordinal, entonces es considerado como un concepto primitivo, y se fundamenta axiomáticamente. Esta fue la vía seguida por Peano, Hilbert, etc. Si se introduce por su aspecto cardinal entonces es un concepto derivado del cálculo de clases, y así lo hicieron Cantor y Frege, siendo perfeccionado sobre todo por Russell.

El Sistema de Peano es axiomático y ordinal en sus inicios, pasando posteriormente a desarrollar la teoría cardinal; mientras Russell desarrolla primero la aritmética cardinal como un capítulo de la Teoría de Clases, para después introducir el número ordinal.

El desarrollo completo de cualquiera de ambos procedimientos es largo y tedioso y para muchos no es, en ninguno de ellos, completamente satisfactorio. No obstante, nadie debe dudar de la importancia del concepto de número, este concepto constituye la máxima dificultad de los fundamentos de la Matemática, pero es la base de toda ella. Así se muestra en lo dicho por el famoso matemático L. Kronecker: "Dios creó el número natural, lo demás es obra del hombre".

En esta primera parte del capítulo se hace el estudio, en forma esquemática y sintética, del concepto de número natural teniendo como base los axiomas de Peano.

5.1.1. El Sistema de Axiomas de Peano

En el sistema de Peano los términos: "número natural", un elemento llamado "uno", y una relación "sucesor de" son tomados como no definidos, es decir como conceptos primarios, los cuales, mediante "los axiomas de Peano" , quedan definidos axiomáticamente por las reglas que determinan estos axiomas.

Uno puede definir axiomáticamente los números naturales mediante otro conjunto de axiomas que no sean los de Peano, pero éstos son posiblemente los que más corresponden al concepto intuitivo de contar que se quiere formalizar.

Axiomas de Peano:

1. Uno es un número natural,$(1 \in N)$
2. Para todo número natural n existe un número natural llamado sucesor de n, que denotamos por suc(n), el cual es un número natural y está unívocamente determinado por:
   $((\forall n \in N, \exists suc(n) \in N) \wedge (\forall n \in N, \forall m \in N, n = m \Rightarrow suc(n) = suc(m))))$
3. Uno no es sucesor de otro número natural, $(\forall n \in N, suc(n) \neq 1)$
4. Para todo m y n números naturales si el sucesor de n es igual al sucesor de m entonces n es igual a m, $(\forall n \in N, \forall m \in N)\ (suc(n) = suc(m) \Rightarrow n = m)$
5. Propiedad inductiva. Si un conjunto de números naturales S cumple que:
   - $1 \in S$
   - $\forall n \in S, suc(n) \in S$

   entonces S contiene a todos los números naturales, $(S = N)$

Estos cinco axiomas son proposiciones que caracterizan esencialmente la llamada sucesión numérica natural, o conjunto ordenado de números naturales, y puede tomarse como definición implícita de los mismos. El sistema $(N, suc, 1)$, donde N, suc, y 1 vienen definidos mediante los axiomas de Peano anteriores, es conocido como un modelo del sistema de axiomas de Peano.

Para definir ahora las operaciones aritméticas conocidas entre números naturales se utiliza el concepto de operación binaria. Recordemos que dados A y B conjuntos no vacíos, se define el producto cartesiano A por B, y se denota $A \times B$, como $A \times B = \{\{\{a\},\{a,b\}\} / a \in A \wedge b \in B\}$. Así mismo, el conjunto $\{\{a\},\{a,b\}\}$ como elemento de $A \times B$, se denota por (a,b), donde a es llamada la primera componente y b la segunda componente del par (a,b). Ya sabemos que una operación binaria sobre A, formalmente hablando, no es mas que una aplicación de $A \times A$ en A.

Ahora podemos definir la operación de adición de números naturales mediante una definición por recurrencia.

5.1.2. La adición de números naturales (+)

A todo par de números naturales (n,m) se le asigna un número natural, llamado suma de m y n, el cual es denotado por $m + n$, y viene definido en forma recurrente por:

N1.- $m + 1 = suc(m)$, *para todo* $m \in N$

N2.- $m + (n + 1) = suc(m + n)$, *para todo* $m \in N$

Veamos que está bien definida como operación binaria sobre N.

Sea $A = \{n \in N : \forall m \in N,\ m + n \in N\}$. Es inmediato, usando el quinto axioma de Peano, que A coincide con el conjunto de los números naturales y, por tanto, que está bien definida la adición como operación binaria sobre *N*. (1 pertenece a A por N1 y el segundo axioma de los números naturales; además, de n pertenecer a A se obtiene, usando N2, que el sucesor de n también está por N1)

Nota.- Como n+1=suc(n), usando el quinto axioma de Peano se obtiene que 1+n=n+1.

Demostración:

Sea A el conjunto de números naturales n para los cuales 1+n=n+1.

Es evidente que 1 pertenece a A.

Por N2, 1+suc(n)=suc(1+n), pero suc(1+n)=suc(n+1) si n pertenece a A y el segundo axioma de Peano. Como suc(n+1)= (n+1)+1 y n+1=suc(n) por N1, obtenemos que 1+suc(n)=suc(n)+1. Usando el quinto axioma de Peano A=N.

Ahora podemos concluir con el siguiente teorema que valida las propiedades más importantes de la adición de números naturales.

Teorema 5.1.2.1. (propiedades de la adición)

1. $(\forall x \in N, \forall y \in N, \forall n \in N)\ (x + y) + n = x + (y + n)$
   Propiedad asociativa de +.

2. $(\forall x \in N, \forall n \in N)\ (x + n = n + x)$
   Propiedad conmutativa de la +.

3. $(\forall x \in N, \forall y \in N, \forall n \in N)\ (x + n = y + n) \Rightarrow x = y$
   Propiedad de cancelación de la +.

Demostración.

1. Sea $A = \{n \in N / (x + y) + n = x + (y + n), \forall x, y \in N\}$. Probemos que A es el conjunto de todos los números naturales aplicando el quinto axioma de Peano.

$$\begin{aligned} (x + y) + 1 &= suc(x + y) && por\ \ N1 \\ &= x + suc(y) && por\ \ N2 \\ &= x + (y + 1) && por\ \ N1 \end{aligned}$$

Por tanto $1 \in A$.

Probemos que si $n \in A$, entonces $suc(n) \in A$.

Supongamos que $n \in A$ y sean x,y números naturales arbitrarios.

$$\begin{aligned} (x + y) + suc(n) &= suc\Big((x + y) + n\Big) && por\ \ N2 \\ &= suc\Big(x + (y + n)\Big) && por\ \ n \in N \\ &= x + suc(y + n) && por\ \ N2 \\ &= x + \Big(y + sus(n)\Big) && por\ \ N2 \end{aligned}$$

Por tanto, si $n \in A$, entonces $suc(n) \in A$.

Luego, por el quinto axioma de Peano, podemos concluir que $A = N$

2. Sea $A = \{n \in N / (\forall x \in N)\ (x + n = n + x)\}$. Se procede en forma análoga a como en 1 y se obtiene similarmente que $A = N$.

3. $A = \{n \in N / (\forall x \in N, \forall y \in N)\ (x + n = y + n) \Rightarrow x = y\}$. Se procede en forma análoga a como en 1 y se obtiene similarmente que $A = N$.

Análogamente a como se hizo con la adición se puede definir el producto de números naturales por recurrencia.

5.1.3. La multiplicación de números naturales (·)

A todo par de números naturales (m,n) se le asigna un número natural llamado producto de m y n, el cual es denotado por $m \cdot n$, y viene definido en forma recurrente por:

P1.- $m \cdot 1 = m$, *para todo* $m \in N$
P2.- $m \cdot suc(n) = m \cdot n + m$, *para todo* $m \in N$

Veamos que está bien definida como operación binaria sobre N

Sea $A = \{n \in N : (\forall m \in N)\ (m \cdot n \in N)\}$. Es fácil e inmediato, usando el quinto axioma de Peano como antes, probar que A coincide con el conjunto de los números naturales, y por tanto, que está bien definida la multiplicación como operación binaria sobre N, ya que: 1 pertenece a A por P1, y si n está en A, se obtiene por P2 y ser la adición una operación binaria sobre N, que $suc(n)$ también está.

En lo que sigue y cuando no haya lugar a dudas escribiremos mn por $m \cdot n$ para denotar el producto de la multiplicación de los números m y n.

Teorema 5.1.3.1. (propiedades de la multiplicación)

1. $(\forall x \in N, \forall y \in N, \forall n \in N)\ (x + y)\ n = xn + yn$
   propiedad distributiva de $\cdot$ respecto a $+$.

2. $(\forall n \in N)\ (1n = n)$
   1 es el neutro de la $\cdot$.

3. $(\forall x \in N, \forall n \in N)\ (xn = nx)$
   propiedad conmutativa de la $\cdot$.

4. $(\forall x \in N, \forall y \in N, \forall n \in N)\ \Big((xy)n = x(yn)\Big)$
   propiedad asociativa de la $\cdot$.

Demostración.

1. Sea $A = \Big\{n \in N / (\forall x,y \in N)\ \Big((x + y)\ n = xn + yn\Big)\Big\}$. Probemos que A es el conjunto de todos los números naturales aplicando el quinto axioma de Peano.

Es trivial que $1 \in A$, por P1 y ser $x + y$ un número natural.

Probemos ahora que si $n \in A$, entonces $suc(n) \in A$.

Supongamos que $n \in A$. Sean $x,y \in N$ arbitrarios. Entonces:

$$\begin{aligned}
(x + y)suc(n) &= (x + y)n + (x + y) && por\ \ P2\\
&= (xn + yn) + (x + y) && por\ \ n \in A\\
&= \big((xn + yn) + x\big) + y && por\ \ asoc.\ de + .\\
&= \big(xn + (yn + x)\big) + y && por\ \ asoc.\ de + .\\
&= \big(xn + (x + yn)\big) + y && por\ \ conm.\ de + .\\
&= \big((xn + x) + yn\big) + y && por\ \ asoc.\ de + .
\end{aligned}$$

$$= (xn + x) + (yn + y) \qquad por \quad asoc.\ de + .$$
$$= xsuc(n) + ysuc(n) \qquad por \quad P2.$$

Por tanto, si $n \in A$, entonces $suc(n) \in A$.

Luego, por el quinto axioma de Peano, obtenemos que $A = N$ y queda probado que:

$$(\forall x \in N, \forall y \in N, \forall n \in N)\ \big((x + y)\ n = xn + yn\big).$$

2. Sea $A = \{n \in N / 1n = n\}$. Probemos que A es el conjunto de todos los números naturales aplicando el quinto axioma de Peano.

   Es trivial que $1 \in A$ por P1 para $m = 1$.

Probemos ahora que si $n \in A$, entonces $suc(n) \in A$.

Supongamos que $n \in A$

$$1 \cdot (n + 1) = 1 \cdot n + 1 \qquad por \quad P2$$
$$= n + 1 \qquad por \quad n \in A$$
$$= suc(n) \qquad por \quad N1 \text{ para } m = n$$

Por tanto, si $n \in A$, entonces $suc(n) \in A$.

Luego, por el quinto axioma de Peano, podemos concluir que $A = N$y queda probado que:

$1 \cdot n = n$, para todo número natural n.

3. Sea $A = \{n \in N / (\forall x \in N)\ (xn = nx)\}$. Probemos que A es el conjunto de todos los números naturales aplicando el quinto axioma de Peano.

$1 \in A$, pues se probó en 2.

Probemos que si $n \in A$, entonces $suc(n) \in A$.

Supongamos que $n \in A$, y sea $x \in N$ arbitrario. Entonces:

$$\begin{aligned} x \cdot suc(n) &= x \cdot n + x && \textit{por P2} \\ &= x \cdot n + 1 \cdot x && \textit{por } n \in A \textit{ y prueba en 2} \\ &= (n + 1) \cdot x && \textit{probado en } 1 \\ &= \big(suc(n)\big) \cdot x && \textit{por } N1 \text{ para } m = n \end{aligned}$$

Por tanto, si $n \in A$, entonces $suc(n) \in A$.

Luego, por el quinto axioma de Peano, podemos concluir que $A = N$ y

$$(\forall x \in N, \forall n \in N)\ (xn = nx)$$

4. Sea $A = \{n \in N / (\forall y \in N)\ ((xy)n = x(yn))\}$. Probemos que A es el conjunto de todos los números naturales aplicando el quinto axioma de Peano.

$1 \in A$, por P1 aplicado para $m = xy$ en el término izquierdo de la igualdad, obtenemos que $(xy)1 = xy$, y aplicado para $m = y$ en el término derecho, obtenemos que $x(y1)1 = xy$. Por tanto, se tiene la igualdad correspondiente y así, que $1 \in A$.

Probemos que si $n \in A$, entonces $suc(n) \in A$.

Supongamos que $n \in A$ y sean $x,y \in N$ arbitrarios. Entonces:

$$
\begin{aligned}
(xy)suc(n) &= (xy)n + xy && \textit{por } P2\\
&= x(yn) + xy && \textit{por } n \in A\\
&= (yn)x + yx && \textit{probado en 3}\\
&= (yn + y)x && \textit{probado en 1}\\
&= x(yn + y) && \textit{probado en 3}\\
&= x(ysuc(n)) && \textit{por } P2
\end{aligned}
$$

Por tanto, si $n \in A$, entonces $suc(n) \in A$.

Luego, por el quinto axioma de Peano, podemos concluir que $A = N$ y queda probado que:

$$(\forall x \in N, \forall y \in N, \forall n \in N)\ ((xy)n = x(yn))$$

5.1.4. El orden de los números naturales

Definición

Para cualesquiera m y n números naturales, diremos que m es menor que n, y lo denotamos por $m < n$, si existe un número natural k, tal que $n = m + k$.

Teorema 5.1.4.1. (propiedades del orden (<) en los naturales)

1. Para todo número natural n, $n < n + 1$

2. Para cualesquiera a, b, y c números naturales, si $a < b$ y $b < c$, entonces $a < c$. (transitividad)

3. Para cualesquiera a y b números naturales, si $a < b$, entonces $suc(a) = b$ o $suc(a) < b$.

4. Para cualesquiera a y b números naturales hay exactamente una sola proposición verdadera de las siguientes tres proposiciones:

$$a < b,\ b < a,\ a = b.$$

5. Para cualesquiera a, b, y c números naturales se tiene que $a < b$, si y sólo si, $a + c < b + c$

6. Para cualesquiera a, b, y c números naturales se tiene que $a < b$, si y sólo si, $ac < bc$.

7. Para cualesquiera a, b, c, y d números naturales, si $a < b$ y $c < d$, entonces $a + c < b + d$.

8. Para cualesquiera a, b, y c números naturales, si $ac = bc$, entonces $a = b$.

Demostración

1. Trivial, pues $n + 1 = n + 1$.

2. Si $a < b$ y $b < c$ existen $p, q \in N$, tales que $b = a + p$ y $c = b + q$. Entonces $c = (a + p) + q$ y, por asociatividad, $c = a + (p + q)$.

   Ahora, como $p + q$ es un número natural, podemos concluir que $a < c$.

3. Si $a < b$, existe $m \in N$, tal que $b = a + m$. Hay dos casos posibles: $m = 1$ o $m \neq 1$. En el primer caso, si $m = 1$, entonces $b = suc(a)$. En el segundo caso, si $m \neq 1$, entonces existe un número natural n tal

que $suc(n) = m$. Esto es una consecuencia inmediata de probar que el conjunto:

$$A = \{m \in N : (m = 1) \vee (\exists n \in N)\ ((xy)n = x(yn))\}$$

coincide con el conjunto de los números naturales, y esta coincidencia se consigue rápidamente aplicando el quinto axioma de Peano, lo cual se deja como ejercicio.

Ahora, obtenemos que:

$$b = a + m = a + suc(n) = a + (n + 1) = a + (1 + n) = (a + 1) + n = suc(a) + n$$

por tanto, $suc(a) < b$. Y hemos probado que si $a < b$, entonces $suc(a) = b$ o $suc(a) < b$.

4. Sea $A = \{n \in N : ((\forall b \in N)\ (n = b) \vee (n < b) \vee (b < n))\}$.

Probemos que $1 \in A$: Sea $b \in N$ arbitrario. Hay dos casos posibles $b = 1$, o $b \neq 1$. Si $b \neq 1$, entonces $b = suc(c)$, para algún $c \in N$. Luego, $b = c + 1 = 1 + c$ y $1 < b$ Por tanto, $\forall b \in N,\ 1 = b \vee 1 < b$ y así hemos probado que $1 \in A$.

Probemos ahora que si $n \in A$, entonces $suc(n) \in A$.

Sea $b \in N$ arbitrario y supongamos que $n \in A$

Si $n \in A$, entonces $n = b \vee n < b \vee b < n$.

Caso 1: ($n = b$). Entonces $b < n + 1$ por 1, es decir, $b < suc(n)$
Por tanto, $suc(n) \in A$

Caso 2: ($n < b$). Entonces, de 3, obtenemos que $b = suc(n) \vee suc(n) < b$. Por tanto, $suc(n) \in A$

Caso 3: ($b < n$). Sabemos por 1 que $n < suc(n)$ y entonces, por la transitividad demostrada en 2, obtenemos que $b < suc(n)$. Por tanto, $suc(n) \in A$

Es decir, en cualquier caso, si $n \in A$, entonces $suc(n) \in A$.

Por tanto, por el quinto axioma de Peano, podemos concluir que $A = N$.

Supongamos ahora que existen a y b números naturales tales que dos de las proposiciones $a = b$, $a < b$ o $b < a$ son verdaderas y veamos que en cualquier caso llegamos a una contradicción.

Si $a = b$ y $a < b$ entonces $a < a$.

Si $a < b$ y $b < a$, entonces de 2 se obtiene $a < a$.

Por tanto, en cualquier caso de suponer que se cumplen dos de las proposiciones anteriores, se obtiene que $a < a$..

Si existe $a \in N$, tal que $a < a$, entonces existe un número natural n tal que $a = a + n$, luego $a + 1 = (a + n) + 1 = a + (n + 1)$, y por la propiedad de cancelación de la adición $1 = n + 1 = suc(n)$ para ese número natural n, lo cual no es posible, pues 1 no es sucesor de ningún número natural.

Esto es una contradicción a la suposición de que existan dos números naturales para los cuales sean verdaderas dos de las proposiciones: $a = b$, $a < b$, o $b < a$.

Como ya habíamos probado que al menos una de ella es verdadera para cualesquiera sean los números naturales a y b, ahora podemos concluir

que: **una y sólo una de las proposiciones, $a = b$, $a < b$ o $b < a$, es verdadera.**

5. Sean a y b números naturales arbitrarios.
   Si $a < b$, entonces existe $n \in N$ tal que $b = a + n$ por definición. Luego, si c es un número natural arbitrario, entonces

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

Y, por tanto, $a + c < b + c$

Sean a, b, c números naturales arbitrarios.

Si $a + c < b + c$, entonces existe un número natural n tal que:

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

Por la propiedad de cancelación, entonces $b = a + n$ para ese número natural n y, por tanto, $a < b$.

Luego hemos probado que, para cualesquiera a, b y c números naturales $a < b$, si y sólo si, $a + c < b + c$.

6. Si $a < b$, entonces existe $n \in N$, tal que $b = a + n$. Luego,
   $bc = (a + n)c = ac + nc$, y como $nc \in N$, se sigue que $ac < bc$

Si $ac < bc$, veamos que $a < b$, usando 4, al no poder ser cierto $a = b$ ni $b < a$. Si $a = b$, entonces se tendría que $ac = bc$, lo cual no puede ser por 4 si $ac < bc$; si $b < a$, entonces ya probamos que $bc < ac$, lo cual no puede ser cierto por 4 si tenemos que $ac < bc$.

Luego, podemos concluir por 4, que: $a < b$ si $ac < bc$.

Por tanto hemos demostrado que, para cualesquiera *a, b* y *c* números naturales *a* < *b*, si y sólo si, *ac* < *bc*.

7. Supongamos que $a < b$ y $c < d$. Luego existen $n,m \in N$, tales que, $b = a + n$ y $d = c + m$. Entonces:

$$\begin{aligned} b + d &= (a + n) + (c + m) \\ &= \big((a + n) + c\big) + m \\ &= \big(a + (n + c)\big) + m \\ &= \big(a + (c + n)\big) + m \\ &= \big((a + c) + n\big) + m \\ &= (a + c) + (n + m) \end{aligned}$$

Luego, $a + c < b + d$

Por tanto, hemos probado 7.

8. Sean $a,b,c \in N$ arbitrarios tales que $ac < bc$. Se prueba fácil, como antes, que a no puede ser igual a b, ni tampoco ser mayor que b. Así se concluye, de 4, que $a < b$.

Teorema 5.1.4.2.

Sea a un número natural arbitrario. Entonces no existe ningún número natural b, tal que $a < b$ y $b < suc(a)$.

La demostración de este teorema se obtiene inmediatamente suponiendo la existencia del número natural b cumpliendo las condiciones $a < b$ y

$b < suc(a)$, y llegando a una contradicción al aplicar 3 y 4 del teorema anterior.

- **Definición. (≤)**

Dados a y b números naturales, decimos que a es menor o igual a b, y lo denotamos por $a \leq b$, si y sólo si, $a < b$ o $a = b$.

Es ahora trivial la demostración de las propiedades enunciadas en el siguiente teorema:

Teorema 5.1.4.3. (propiedades de (≤) en los naturales)

Sean a, b, c números naturales cualesquiera, entonces:

1. $a \leq a$.
2. Si $a \leq b$ y $b \leq a$, entonces $a = b$.
3. Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.
4. $a \leq b$ o $b \leq a$.

5.1.5. Ejercicios propuestos

1. Demuestre que si $n \in N$, entonces:

   - $n = 1$ o $n = suc(m)$ para algún $m \in N$.
   - $n \neq suc(n)$.

2. Sean $(N,suc,1)$ y $(B,\&,e)$ dos modelos del sistema de axiomas de Peano. Demuestre que existe una biyección $f: N \rightarrow B$ tal que:

   - $f(1) = e$
   - $(\forall n \in N)\ (\ f(suc(n)) = \&(f(n))\ )$

3. Complete la demostración del teorema sobre propiedades de la adición.

4. Complete la demostración del teorema que dice: Sea a un número natural arbitrario. Entonces no existe un número natural b tal que $a < b$ y $b < suc(a)$.

5. Complete la demostración del teorema sobre propiedades de $\leq$ en los naturales.

6. Sea P(n) un predicado. Asuma que P(1) es verdadero y que P($suc(n)$) es verdadero siempre que P(n) lo sea. Pruebe que P(n) es verdadero para todo $n \in N$. (esto significa probar que el método de inducción matemática, es un método válido de demostración)

7. Explique cómo usted resuelve, en el sistema de números naturales, la ecuación $3x + 7 = 19$.

8. Pruebe que no existe $n \in N$ tal que $2n = 5$.

9. Pruebe que para todo $a,b \in N$, si $a < b$, entonces existe un único $c \in N$ tal que $b = a + c$. (Tal c es llamado diferencia de b y a, y es denotado por $c = b - a$)

10. Explique por qué la diferencia de dos números naturales no es una operación binaria sobre N.

5.2 SEGUNDA PARTE: NÚMERO ENTERO

5.2.0. Introducción a la segunda parte

En la enseñanza básica, después de definir los números naturales mediante los símbolos 1,2,3,.....,etc; se acostumbra a motivar la necesidad de otro campo numérico para representar mediante números "el debo" versus "el tengo", y "el no tengo ni debo". Muchas veces también se utiliza como motivación la necesidad de tener un campo numérico donde la resta esté bien definida. A continuación se introducen los símbolos $-1,-2,-3,...,$etc para resolver "el debo" versus "el tengo", y se les llama enteros negativos y el 0 para resolver "el no tengo ni debo" y se le llama cero. A los naturales entonces le llaman enteros positivos.

En la primera parte del capítulo se hizo el estudio, en forma esquemática, del concepto de número natural teniendo como base los axiomas de Peano. En esta segunda parte se define, usando elementos de la Teoría de Conjuntos, el número entero por abstracción, además se definen las operaciones usuales de enteros, y se prueban sus propiedades fundamentales, así como que el conjunto de números naturales está inmerso en el de los enteros.

Como se puede apreciar, el concepto de Número Entero, al igual que el de Número Natural, no depende del simbolismo que se use para su representación.

5.2.1. Definición por abstracción de número entero

Para ello primeramente definimos la relación $\equiv$ sobre $N \times N$ como sigue:

- **Definición de $\equiv$ sobre $N \times N$**

$(a,b) \equiv (c.d) \Leftrightarrow a + d = b + c$

Así definida, $\equiv$ es una relación de equivalencia sobre $N \times N$, como se enuncia en el siguiente teorema cuya demostración es trivial.

Teorema 5.2.1.1. ($\equiv$ es una relación de equivalencia sobre $N \times N$)

La relación $\equiv$ es una relación de equivalencia sobre $N \times N$, es decir:

1. Es reflexiva $\left(\forall (a,b) \in N \times N,\ (a,b) \equiv (a,b)\right)$
2. Es simétrica, es decir:
   $\left(\forall (a,b), (c,d) \in N \times N\right)$, *si* $(a,b) \equiv (c,d)$ *entonces* $(c,d) \equiv (a,b)$
3. Es transitiva, es decir:
   $\left(\forall (a,b), (c,d), (e,f) \in N \times N\right)$ $\left(si\ (a,b) \equiv (c,d)\ y\ (c,d) \equiv (e,f)\right.$, entonces $\left.(a,b) \equiv (e,f)\right)$

Consideramos ahora el espacio cociente $N \times N / \equiv$, cuyos elementos son las clases de equivalencia definidas por $\equiv$.

La clase de equivalencia del par (a,b), se denota y viene definida por

$$\overline{(a,b)} = \left\{(m,n) \in N \times N / (a,b) \equiv (m,n)\right\}$$

Se define ahora como número entero a cada clase de equivalencia y, como conjunto de números enteros, a $N \times N / \equiv$, el cual se simboliza por Z.

A continuación vamos a definir la adición de enteros.

5.2.2. La adición de números enteros

A cada par de números enteros $\overline{(a,b)}$, $\overline{(c,d)}$, se le asigna un número entero, llamado suma de $\overline{(a,b)}$ y $\overline{(c,d)}$, el cual es denotado y definido por:

$\overline{(a,b)} + \overline{(c,d)} = \overline{(a + c, b + d)}$ donde la suma $(a + c)$ y $(b + d)$ es la suma de naturales.

Para que esta operación esté bien definida, debe probarse que dicha suma no depende del elemento que representa cada clase para su suma, es decir, si $\overline{(a_1, b_1)} = \overline{(a_2, b_2)}$ y $\overline{(c_1, d_1)} = \overline{(c_2, d_2)}$ entonces

$$\overline{(a_1 + c_1, b_1 + d_1)} = \overline{(a_2 + c_2, b_2 + d_2)}$$

Esto es trivial, pues si $a_1 + b_2 = b_1 + a_2$ y $c_1 + d_2 = d_1 + c_2$, entonces se tiene, evidentemente, usando las propiedades asociativa y conmutativa de la adición de números naturales, que $(a_1 + c_1) + (b_2 + d_2) = (b_1 + d_1) + (a_2 + c_2)$.

Por tanto, la adición de enteros está bien definida.

Teorema 5.2.2.1 (propiedades de la adición de enteros)

Sean x,y,z números enteros arbitrarios. Entonces:

1. $(x + y) + z = x + (y + x)$, propiedad asociativa de la adición de enteros.
2. $x + y = y + x$, propiedad conmutativa de la adición de enteros.
3. $x + \overline{(1,1)} = x$ existencia de elemento neutro para la adición de enteros.
4. Si $x = \overline{(a,b)}$ entonces $x + \overline{(b,a)} = \overline{(1,1)}$ existencia del inverso aditivo.

Demostración:

1. Se obtiene inmediatamente haciendo $x = \overline{(a,b)}$, $y = \overline{(c,d)}$, $z = \overline{(e,f)}$ y aplicando la definición de suma de enteros y la propiedad asociativa de la adición de números naturales.
2. Análogo a 1 y aplicando la propiedad conmutativa de la adición de números naturales, pues por la propiedad de cancelación en la adición de números naturales se tiene que:
   $(a + 1, b + 1) \equiv (a,b)$ y así $\overline{(a,b)} = \overline{(a + 1, b + 1)}$
3. Si $x = \overline{(a,b)}$, entonces $x + \overline{(b,a)} = \overline{(a + b,b + a)} = \overline{(a + b,a + b)} = \overline{(1,1)}$

A continuación definimos la resta o diferencia de enteros como una suma con el inverso aditivo, es decir, $\overline{(a,b)} - \overline{(c,d)} = \overline{(a,b)} + \overline{(d,c)} =$ Esta definición justifica las notaciones $\overline{(d,c)} = -\overline{(c,d)}$ por las propiedades 2 y 3, y la de $\overline{(1,1)} = -\overline{(1,1)}$

5.2.3. La multiplicación de Enteros

Sean $\overline{(a,b)}$, $\overline{(c,d)}$ números enteros, la multiplicación de estos enteros se define y se denota por: $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac + bd, ad + bc)}$ donde la adición y la multiplicación $ac + db$ y $ad + bc$ son las correspondientes a la adición y multiplicación de números naturales.

Para que esta operación esté bien definida sobre los enteros no debe depender, el resultado, del elemento que represente cada clase en la multiplicación, es decir, si $\overline{(a_1,b_1)} = \overline{(a_2,b_2)}$ y $\overline{(c_1,d_1)} = \overline{(c_2,d_2)}$, entonces

$$\overline{(a_1,b_1)} \cdot \overline{(c_1,d_1)} = \overline{(a_2,b_2)} \cdot \overline{(c_2,d_2)}$$

Esta última igualdad equivale a:

$$\overline{(a_1c_1 + b_1d_1 , a_1d_1 + b_1c_1)} = \overline{(a_2c_2 + b_2d_2 , a_2d_2 + b_2c_2)}$$

La cual, para obtenerla debemos probar que:

$$(a_1c_1 + b_1d_1) + (a_2,d_2 + b_2,c_2) = (a_1d_1 + b_1c_1) + (a_2c_2 + b_2d_2)$$

Del hecho que $a_1 + b_2 = a_2 + b_1$ y $c_1 + d_2 = c_2 + d_1$, obtenemos que:

$$c_1(a_1 + b_1) = c_1(a_2 + b_1) \quad ; \quad b_2(c_2 + d_1) = b_2(d_2 + c_1) \quad ;$$

$$a_2(d_2 + c_1) = a_2(c_2 + d_1) \quad ; \quad d_1(a_2 + b_1) = d_1(b_2 + a_1) \quad .$$

Ahora igualando la suma de los cuatro primeros términos en estas igualdades con la suma de los cuatro segundos términos, y aplicando las propiedades de la adición y multiplicación de números naturales se puede concluir la igualdad:

$$(a_1c_1 + b_1d_1) + (a_2d_2 + b_2c_2) = (a_1d_1 + b_1c_1) + (a_2c_2 + b_2d_2)$$

Y, por tanto, que la multiplicación de enteros está bien definida.

Al igual que con los números naturales, cuando no haya lugar a confusión, escribiremos xy en vez de $x \cdot y$ para representar el producto de la multiplicación de dos némeros enteros x,y.

Teorema 5.2.3.1. (propiedades de la multiplicación de enteros)

Cualesquiera sean x,y,z números enteros, se satisfacen:

1. $(xy)z = x(yz)$
   propiedad asociativa

2. $xy = yx$
   propiedad conmutativa.

3. $x(y + z) = xy + xz$
   propiedad distributiva de la multiplicación respecto a la adición.

4. $x\overline{(2,1)} = x$
   propiedad del elemento neutro para la multiplicación.

5. $x\overline{(1,1)} = \overline{(1,1)}$
   propiedad de la multiplicación por el neutro aditivo o cero.

6. Si $x \neq \overline{(1,1)}$ y $xy = xz$ entonces $y = z$
   propiedad de cancelación de la multiplicación.

7. $xy = \overline{(1,1)}$, si y sólo si, $x = \overline{(1,1)}$ o $y = \overline{(1,1)}$
   propiedad de la multiplicación con resultado cero.

Demostración

Sean $x = \overline{(a,b)}$, $y = \overline{(c,d)}$, $x = \overline{(e,f)}$, para $a,b,c,d,e,f \in N$, entonces

1. $(xy)z = (\overline{(a,b)} \cdot \overline{(c,d)}) \cdot \overline{(e,f)} = \overline{(ac + bd,\ ad + bc)} \cdot \overline{(e,f)}$,

$$= \overline{((ac + bd)e + (ad + bc)f,\ (ac + bd)f + (ad + bc)e)}$$

$$= \overline{(a(ce + df) + b(de + cf),\ a(cf + de) + b(df + ce))}$$

$$= \overline{(a,b)} \cdot \overline{(ce + df,\ de + cf)} = \overline{(a,b)} \cdot (\overline{(c,d)} \cdot \overline{(e,f)}) = x(yz)$$

2. Análogo a 1 y usando la propiedades correspondientes de los naturales.

3. Análogo a 1 y usando la propiedades correspondientes de los naturales.

4. Sea $x = \overline{(a,b)}$. Entonces:

$$x \cdot \overline{(2,1)} = \overline{(a,b)} \cdot \overline{(suc(1),\ 1)} = \overline{(a \cdot suc(1) + b \cdot 1,\ a \cdot 1 + b \cdot suc(1))}$$

$$= \overline{((a \cdot 1 + a) + b,\ a + (b \cdot 1 + b))} = \overline{(a + (a + b),\ (a + b) + b)}$$

$$= \overline{(a,b)} = x$$

5. Análogo a 4.

6. Si $x \neq \overline{(1,1)}$, entonces $a \neq b$ y, si $xy = xz$ se tiene que:

$\overline{(ac + bd,ad + bc)} = \overline{(ae + bf,\ af + be)}$, de donde

$(ac + bd) + (af + be) = (ad + bc) + (ae + bf)$

Y, de aquí,

$$a(c+f)+b(d+e)=a(d+e)+b(c+f). \quad (*)$$

Como $a \neq b$, entonces $a < b$ o $a > b$. Supongamos, sin perdida de generalidad, que $a < b$ (en el otro caso se procede en forma análoga).

Si $a < b$, entonces existe $m \in N$, tal que $b = a + m$.

Sustituyendo ahora b por $a + m$ en $(*)$, obtenemos que:

$$a(c+f)+(a+m)(d+e)=a(d+e)+(a+m)(c+f),$$

y de aquí, utilizando las propiedades de la adición y multiplicación de números naturales, se sigue que:

$$m(d+e)=m(c+f).$$

Ahora podemos concluir, por la propiedad de cancelación de números naturales, que:

$d + e = c + f$, es decir, $y = \overline{(c,d)} = \overline{(e,f)} = z$

7. Si $xy = \overline{(1,1)}$, entonces $\overline{(ac+bd,ad+bc)} = \overline{(1,1)}$ lo que significa que: $ac + bd + 1 = ad + bc + 1$ y, por cancelación, $ac + bd = ad + bc$ $(**)$

Supongamos ahora que $x \neq \overline{(1,1)}$ lo cual significa que $a \neq b$, vamos a obtener entonces que $y = \overline{(1,1)}$ es decir, $c = d$.

Análogamente se puede obtener que $x = \overline{(1,1)}$ $(a = b)$, si $y \neq \overline{(1,1)}$ $(c \neq d)$

Si $a \neq b$, entonces $a < b$ o $a > b$. Supongamos ahora que $a < b$, si fuera $a > b$, se procedería en forma similar.

Sea entonces, $b = a + m$ para algún $m \in N$. Sustituyendo ahora en $(**)$ tenemos que: $ac + (a + m)d = ad + (a + m)c$ de donde $md = mc$ y, por cancelación $d = c$, es decir, $y = \overline{(1,1)}$

Recíprocamente, si $x = \overline{(1,1)}$ o $y = \overline{(1,1)}$, entonces

$xy = \overline{(ac + bd,ad + bc)} = \overline{(c + d,c + d)} = \overline{(1,1)}$ o

$xy = \overline{(ac + bd,ad, + bc)} = \overline{(a + b,a + b)} = \overline{(1,1)}$

5.2.4. El orden de los enteros

Sean $\overline{(a,b)}$ y $\overline{(c,d)}$ números enteros, entonces decimos que $\overline{(a,b)} < \overline{(c,d)}$ (leemos menor que) si y sólo si $a + d < b + c$, donde aquí el orden $(<)$ es el definido en los naturales.

Para que esté bien definido este orden en los enteros, es necesario probar que no depende de los elementos que representan las clases correspondientes. Es decir, debe probarse que:

Si $\overline{(a_1,b_1)} = \overline{(a_2,b_2)}$, $\overline{(c_1,d_1)} = \overline{(c_2,d_2)}$ y $\overline{(a_1,b_1)} < \overline{(c_1,d_1)}$, entonces $\overline{(a_2,b_2)} < \overline{(c_2,d_2)}$

Si $\overline{(a_1,b_1)} = \overline{(a_2,b_2)}$, $\overline{(c_1,d_1)} = \overline{(c_2,d_2)}$ y $\overline{(a_1,b_1)} < \overline{(c_1,d_1)}$, entonces $a_1 + b_2 = b_1 + a_2$, $c_1 + d_2 = d_1 + c_2$ y $a_1 + d_1 < b_1 + c_1$

Entonces, de la última desigualdad, $b_1 + c_1 = a_1 + d_1 + m$ para algún $m \in N$.

Luego $b_1 + c_1 + b_2 + c_2 = a_1 + d_1 + b_2 + c_2 + m$ y, sustituyendo obtenemos:

$$b_1 + c_1 + b_2 + c_2 = a_2 + d_2 + b_1 + c_1 + m.$$

Ahora, cancelando, tenemos que $b_2 + c_2 = a_2 + d_2 + m$, es decir, que $a_2 + d_2 < b_2 + c_2$. Esto significa que $\overline{(a_2, b_2)} < \overline{(c_2, d_2)}$

Por tanto está probado que está bien definido la relación (<) entre enteros.

Teorema 5.2.4.1. (propiedades de (<) en los enteros)

Sean $x,y,z \in Z$, entonces:

1. Si $x < y$ y $y < z$ entonces $x < z$ (propiedad transitiva de <)

2. Hay exactamente una y sólo una proposición verdadera entre $x < y$, $y < x$, $x = y$ (propiedad de tricotomía)

Demostración:

Sean $x = \overline{(a,b)}$, $y = \overline{(c,d)}$, $z = \overline{(e,f)}$

1. Si $\overline{(a,b)} < \overline{(c,d)}$ y $\overline{(c,d)} < \overline{(e,f)}$, entonces $a + d < b + c$ y $c + f < d + e$. Se sigue, por propiedad 7 de (<) en los naturales, que $a + d + c + f < b + c + d + e$ Y, por la propiedad 5, obtenemos que:

$$a + f < b + e, \text{ es decir, } \overline{(a,b)} < \overline{(e,f)}$$

2. Decir que exactamente una sola de las proposiciones siguientes es verdadera, $\overline{(a,b)} < \overline{(c,d)}$, $\overline{(c,d)} < \overline{(a,b)}$, $\overline{(a,b)} < \overline{(c,d)}$ equivale a decir que

exactamente una sola de las proposiciones: $a + d < b + c$, $b + c < a + d$, $a + d = b + c$ es verdadera. Esto es consecuencia de la propiedad de tricotomía en los naturales.

Análogamente a como se hizo en los naturales se define, en el caso de los enteros, que $x \leq y$ si y sólo si $x < y$ o $x = y$.

Usando las propiedades correspondientes de los naturales se obtiene, en forma inmediata, las siguientes propiedades de orden de los enteros.

Teorema 5.2.4.2 (propiedades de (≤) en los enteros)

Sean $x,y,z \in Z$, entonces:

1. $x \leq x$
2. Si $x \leq y$ y $y \leq x$, entonces $x = y$.
3. Si $x \leq y$ y $y \leq z$, entonces $x \leq z$.
4. $x \leq y$ o $y \leq x$

5.2.5. Inmersión de *N* en *Z*. Notación usual

- **Definición (de enteros positivos)**

Diremos que el entero $x = \overline{(a,b)}$ es un número entero positivo si y sólo si $b < a$. Si el conjunto de números enteros lo denotamos por Z entonces, al de enteros positivos, lo denotamos por Z^+.

Teorema 5.2.5.1. (Cerradez de la adición (+) y la multiplicación (·) en Z^+)

Las operaciones de adición y multiplicación de enteros son operaciones cerradas en Z^+, es decir, la suma y producto de enteros positivos es un entero positivo.

Demostración.

Si $x = \overline{(a,b)}$ y $y = \overline{(c,d)}$ son enteros positivos, es decir, $b < a$ y $d < c$, entonces:

- $x + y = \overline{(a,b)} + \overline{(c,d)}$ es también un entero positivo, pues $b + d < a + c$. Esto se obtiene inmediatamente usando la propiedad 7 de (<) en los naturales.
- $x \cdot y = \overline{(a,b)} \cdot \overline{(c,d)}$ es también un entero positivo. Si $b < a$ y $d < c$, entonces existen n y m números naturales tales que: $a = b + m$ y $c = d + n$. Así $ac = bc + mc$, $ac = ad + an$ y $ac = bd + bn + dm + mn$, luego $ac + ac = bc + ad + mc + an$ e, inmediatamente

$$\begin{aligned} ac + bd + bn + dm + mn &= bc + ad + m(d + n) + (b + m)n \\ &= bc + ad + md + mn + bn + mn \end{aligned}$$

De donde, $ac + bd = bc + ad + mn$, es decir $bc + ad < ac + bd$, lo cual significa que $x \cdot y$ es un entero positivo.

Teorema 5.2.5.2 (de la inmersión de $(N,+,\cdot,\leq)$ en $(Z,+,\cdot,\leq)$

Los conjuntos N y Z^+ son isomorfos respecto a la adición, respecto a la multiplicación y respecto al orden ($\leq$), es decir, existe una biyección $f: N \rightarrow Z^+$, que cumple:

1. $(\forall n, m \in N)\left(f(n+m) = f(n) + f(m)\right)$

2. $(\forall n, m \in N)\left(f(nm) = f(n)\ f(m)\right)$

3. $(\forall n, m \in N)\left(n \leq m\right) \Rightarrow f(n) \leq f(m)\big)$

Esto significa que el conjunto de los números naturales está inmerso en el de los enteros y que $f: N \rightarrow Z^+$ es una inmersión de N en Z

Demostración.

Definimos $f(n) = \overline{(suc(n), 1)}$

La función f **es uno a uno**, pues si $f(n) = f(m)$, entonces $\overline{(suc(n), 1)} = \overline{(suc(m), 1)}$, $suc(n) + 1 = suc(m) + 1$ e, imediatamente $m = n$.

La función f **es sobre**, pues si $(a,b) \in Z^+$, entonces $a = b + n$ para algún $n \in N$, de donde $f(n) = \overline{(suc(n), 1)} = \overline{(a,b)}$

1. $f(n + m) = \overline{(suc(n + m), 1)}$

$= \overline{(n + m + 1,1)}$

$= \overline{(n + m + suc(1), suc(1))}$

$= \overline{((n + 1) + (m + 1), 1+1)}$

$= \overline{(n + 1,1)} + \overline{(m + 1,1)}$

$= f(n) + f(m)$

2. $f(nm) = \overline{(suc(nm),1)}$

$= \overline{(nm + 1,1)}$

$= \overline{(nm + n + m + 1 + 1, n + m + 1 + 1)}$

$$= \overline{(n + 1,1)}\ \overline{(m + 1,1)}$$

$$= f(n)\ f(m)$$

3. Si $n \leq m$, entonces $suc(n) \leq suc(m)$, luego $suc(n) + 1 \leq suc(m) + 1$. Por tanto $(suc(n),1) \leq (suc(m),1)$, es decir, $f(n) \leq f(m)$

Este resultado nos permite considerar a N inmerso en Z mediante este isomorfismo con Z^+, y así, para todo $n \in N$ hacer las siguientes notaciones:

1. $\overline{(suc(n),1)} = n$
2. $\overline{(1,suc(n))} = -n$
3. $(1,1) = 0$

Nota. *Observemos que todo número entero queda así representado, pues si* $x = \overline{(a,b)} \in Z = N \times N / \equiv$, *entonces exactamente una y sólo una de las tres posibilidades siguientes es verdadera:*

- $a = b$, en cuyo caso $x = \overline{(a,b)} = \overline{(1,1)} = 0$;
- $b < a$, en cuyo caso $x = \overline{(a,b)} = \overline{(b + n,b)} = \overline{(suc(n),1)} = n$, para algún $n \in N$.
- $a < b$, en cuyo caso $x = \overline{(a,b)} = \overline{(a,a + n)} = -\overline{(a + n,a)} = -\overline{(suc(n),1)} = -n$, para algún $n \in N$

Teorema 5.2.5.3 (sobre Z^+ y <)

Sea $x \in Z$, entonces:

1. $x \in Z^+$ si, y sólo si, $0 < x$

2. Exactamente una sola de las siguientes proposiciones es verdadera: $x = 0$, $x \in Z^+$, o , $-x \in Z^+$

Demostración.

1. $x \in Z^+$ si sólo si $1 < suc(x)$ considerado $x \in N$, lo cual ocurre si, y sólo si, $1 + 1 < suc(x)+1$ lo cual equivale a $(1,1) < (suc(x),1)$, es decir, a: $0 < x$ considerado $x \in Z$.

2. Si $x \in Z$, entonces, o $x = \overline{(1,1)}$, $(x = 0)$ o, una de las dos condiciones siguientes se cumple: $x = \overline{(suc(n),1)}$ o $x = \overline{(1, suc(n))}$, para algún $n \in N$. Pero, esto último equivale a que $x \in Z^+$ o que $-x = \overline{(suc(n),1)} \in Z^+$. Por otro lado, $\forall n \in N$, $\overline{(suc(n),1)} \neq \overline{(1, suc(n))}$ y por tanto, exactamente sólo una puede ser verdadera.

Nota: *Ahora podemos decir: para cualesquiera $x,y \in Z$, $x \leq y$ si y sólo si $y - x \geq 0$.*

Consideremos los siguientes símbolos para representar los números siguientes: el símbolo 1 para el número natural uno como ya hemos estado haciendo, 2 para suc(1), 3 para suc(2), 4 para suc(3), 5 para suc(4), 6 para suc(5), 7 para suc(6), 8 para suc(7), 9 para suc(8), 10 para suc(9), y además el 0 para el entero cero, como ya hicimos y destacamos antes.

Para todo $n \in N$, consideremos el símbolo, dado por la cadena de símbolos $a = a_n a_{n-1} \ldots a_1$, donde $a_j \in \{0,1,2,3,4,5,6,7,8,9\}$ para todo j, $1 \leq j \leq n$. Cuando pueda haber confusión entre el símbolo nm y el

producto nm, se acostumbra, en el caso de la multiplicación de n y m, usar uno de los siguientes símbolos para su producto:

$$n \cdot m,\ (n)(m),\ \text{o}\ n \times m.$$

Diremos que el símbolo $a = a_n a_{n-1} \ldots a_1$ equivale al símbolo $b = b_m b_{m-1} \ldots b_1$ donde n y m son números naturales cualesquiera y para todo $j,i,\ 1 \leq j \leq n,\ 1 \leq i \leq m$ se tiene que $a_j \in \{0,1,2,3,4,5,6,7,8,9\}$ y $b_i \in \{0,1,2,3,4,5,6,7,8,9\}$, si y sólo si,

$$\exists k \in N / \left(\forall j,i\ (a_j = b_i = 0\ si\ k \leq j \leq n \wedge k \leq i \leq m)\right) \wedge \left(\forall j\ (a_j = b_j\ \ si\ 1 \leq j \leq k)\right) \qquad (*)$$

Notemos que podemos establecer una relación entre cada símbolo $a = a_n a_{n-1} \ldots a_1$ y el conjunto $N \cup \{0\}$ mediante

$$a = a_n(10)^{n-1} + a_{n-1}(10)^{n-2} \ldots + a_2(10) + a_1$$

para cada $a \in N \cup \{0\}$, donde $(10)^j$ es el producto $(10)(10)...(10)$ j veces, la cual puede probarse que es una biyección entre el conjunto de las clases de símbolos equivalentes, al que representamos por uno de sus elementos y el conjunto $N \cup \{0\}$.

Generalmente se toma $a = a_k a_{k-1} \ldots a_1$ como el elemento representativo de su clase tomando el valor $k \in N$ correspondiente a cuando $a_k \neq 0$ para $k \neq 1$. En ese caso, por el isomorfismo existente, todo número de $N \cup \{0\}$ se representa unívocamente como $a = a_k a_{k-1} \ldots a_1$ y a dicha representación la consideramos como el número que ella representa.

Si procedemos en forma análoga con los símbolos $a = -a_n a_{n-1} \ldots a_1$ e identificamos los símbolos 0 y −0, obtenemos la representación usada de los números enteros no positivos, y finalmente la correspondiente de todos los enteros.

Definiendo la suma y multiplicación de los símbolos como la suma y multiplicación de los enteros que representan, se podrían construir los algoritmos de la adición y de la multiplicación de enteros para esta representación, los cuales son los que se estudian en la enseñanza básica y, sencillamente llamarles números enteros a los símbolos correspondientes, tal y como se hace usualmente.

5.2.6. Descomposición en factores primos

Sean p y q son números enteros, si $p = mq$ para algún $m \in Z$, entonces decimos que q es un divisor de p o que p es un múltiplo de q, y escribimos $q \mid p$ (se lee: q divide a p).

Un entero p es primo si $p > 1$ y si los únicos divisores positivos de p son 1 y p. Decimos que p es compuesto si $p > 1$ y p no es primo. El entero 1 no es primo ni compuesto.

Es fácil probar que:

Teorema 5.2.6.1.- (de descomposición en factores primos)

Sea p un entero y $p > 1$. Entonces p es primo o producto de primos.

Demostración:

La demostración se hará por inducción completa.

Evidentemente para $p = 2$ es cierta, pues 2 es primo.

Supongamos que es cierta para todo entero k, con $2 \leq k < p$.

Si p no es primo, entonces admite un divisor m, con $1 < m < p$; luego $p = nm$ para algún entero n, con $1 < n < p$. Por hipótesis de inducción completa tanto n como m son primos o producto de primos, y por tanto se sigue la veracidad de la proposición para p, con lo que se concluye la demostración.

Nota: *Si se tiene que* $d \mid a$ *y que* $d \mid b$ *diremos que* d *es un divisor común de* a y b.

Teorema 5.2.6.2 (de divisores comunes)

Cada par de enteros a y b admite un divisor común d de la forma: $d = ax + by$ donde x y y son enteros. Además cada divisor común de a y b divide a d.

Demostración

Supongamos primeramente que $a \geq 0$ y $b \geq 0$. En este caso la demostración se hará por inducción completa sobre $n = a + b$.

Si $n = 0$ entonces $a = b = 0$ y basta tomar $d = 0$ con $x = y = 0$.

Supongamos que se cumpla la proposición para $0 \leq k \leq n - 1$.

Por simetría, sin perdida de generalidad, podemos suponer que $a \geq b$.

Si $b = 0$, entonces $d = a$, $x = 1$, $y = 0$.

Si $b \geq 1$, entonces podemos aplicar la hipótesis de inducción completa a $a - b$, b, pues su suma es $a = n - b \leq n - 1$; por tanto existe un divisor común d de $a - b$ y b de la forma $d = (a - b)x + by$.

Como d divide a $a - b$ y a b, divide a su suma $(a - b) + b = a$, por tanto es divisor común de a y b; además $d = ax + b(y - x)$ es combinación lineal de a y b.

Para completar la demostración en el caso $a \geq 0$ y $b \geq 0$, debemos probar que cada divisor común de a y b divide a d, pero esto es inmediato pues un divisor común de a y b también divide a la combinación lineal $d = ax + b(y - x)$.

Si a o b fueran negativos, basta aplicar el resultado anterior a $|a|$ y $|b|$.

Nota: *Si d es un divisor común de a y b de la forma $d = ax + by$, entonces $-d$ es también un divisor común de la misma forma $-d = a(-x) + b(-y)$. De estos dos divisores comunes, el no negativo se denomina el máximo común divisor de a y b, y se denota por $mcd(a,b)$.* Si $mcd(a,b) = 1$, *se dice que a y b son primos entre sí.*

Teorema 5.2.6.3 (lema de Euclides)

Si $a|bc$ y $mcd(a,d) = 1$, entonces $a|c$.

Demostración

Como $mcd(a,d) = 1$, entonces podemos escribir $ax + by = 1$, luego $c = acx + bcy$. Pero $a|acx$ y, como $a|bc$, también $a|bcy$. Por tanto, podemos concluir que $a|c$.

Teorema 5.2.6.4 (corolario del lema de Euclides)

Si un número primo p divide a ab, entonces $p|a$ o $p|b$. En general, si un número primo p divide a un producto de enteros $a_1 \cdot a_2 \cdot \ldots \cdot a_n$, entonces divide, al menos, a uno de los factores.

Demostración.

Sea p un número primo. Supongamos que $p|ab$ y que p no divide a a. Como p es primo, $mcd(a,p) = 1$ o $mcd(a,p) = p$; pero, como p no divide a a, entonces $mcd(a,p)$ no puede ser p. Por tanto $mcd(a,p) = 1$ y, por el lema de Euclides $p|b$.

El caso de la afirmación más general se puede demostrar por inducción en el número de factores n, y se deja como ejercicio.

Teorema 5.2.6.5.- (de unicidad de la descomposición)

Cada entero $n > 1$ puede ser representado como producto de factores primos, y si se prescinde del orden de los factores, la descomposición es única.

Demostración

Lo único que falta por probar es la unicidad de descomposición. Su demostración se hará por inducción completa en el número entero n.

Para $n = 2$ se tiene inmediatamente, pues 2 es primo.

Supongamos que el teorema es verdadero para k, con $2 \leq k \leq n-1$. Si n es primo no hay nada que demostrar. Supongamos que n es compuesto y que admite dos descomposiciones en factores primos:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_t \cdot \begin{pmatrix} * \\ * \end{pmatrix}$$

Debemos probar que $s = t$ y que cada p es igual a algún q.

De $\begin{pmatrix} * \\ * \end{pmatrix}$ se tiene que p_1 divide a $q_1 \cdot q_2 \cdot \ldots q_t$, luego divide a alguno de los factores. Hacemos, de hacer falta, un reordenamiento de los factores de modo que el factor que p_1 divide sea q_1. Ahora $p_1 \mid q_1$ y, como p_1 y q_1 son primos $p_1 = q_1$.

Simplificamos p_1 en $\begin{pmatrix} * \\ * \end{pmatrix}$ y obtenemos:

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdot \ldots \cdot p_s = q_2 \cdot q_3 \cdot \ldots \cdot q_t$$

Como n es compuesto $1 < \frac{n}{p_1} < n$, luego, por hipótesis de inducción completa, las descomposiciones anteriores son únicas si se prescinde del orden y, por tanto, lo son también las descomposiones en $\begin{pmatrix} * \\ * \end{pmatrix}$. Con esto queda demostrado el teorema.

5.2.7. Ejercicios propuestos

1) Pruebe el teorema: **(La relación $\equiv$ definida en esta sección es una relación de equivalencia sobre $N \times N$)**

2) Complete la demostración del teorema 5.2.2.1: **propiedades de la adición de enteros.**

3) Complete la demostración del teorema 5.2.3.1: **propiedades de la multiplicación de enteros.**

4) Complete la demostración del teorema 5.2.4.2: **propiedades de $\leq$ en los enteros.**

5) Pruebe que:

- $(Z^+,+) \cong (N,+)$.
- $(Z^+,\cdot) \cong (N,\cdot)$.
- $(Z^+,\leq) \cong (N,\leq)$ son isomórficos de orden.

6) Pruebe que: $(\forall x,y,z \in Z)\ (x + z < y + z \Leftrightarrow x < y)$

7) Sea Z^- el conjunto de todos los enteros $\overline{(a,b)}$ tales que $a < b$, llamados enteros negativos. Pruebe o desapruebe que:

- La adición de enteros es cerrada en Z^-
- La multiplicación de enteros es cerrada en Z^-
- $x \in Z^-$ si y sólo si $x < 0$
- Exactamente una sola de las siguientes proposiciones es verdadera: $x = 0$, $x \in Z^-$, o , $-x \in Z^-$
- $(Z^-,+) \cong (N,+)$.
- $(Z^-,\cdot) \cong (N,\cdot)$.
- $(Z^-,\leq) \cong (N,\leq)$ son isomórficos de orden.
- $(Z^-,\geq) \cong (N,\geq)$ son isomórficos de orden.

8) Pruebe que para todo $x \in Z$:

- si $x \neq 0$, entonces $x^2 \in Z^+$.
- $x(-x) \notin Z^+$.
- $-x = (-1)x$.

9) Pruebe que para cualesquiera $x,y \in Z$:

- si $x \in Z^+$ y $y \notin Z^+$, entonces $xy \notin Z^+$.
- si $xy = 1$, entonces $x = y = 1$ *o* $x = y = -1$.

10) Complete la demostración del corolario del lema de Euclides (teorema 5.2.6.4) para el caso más general.

5.3 TERCERA PARTE: NÚMERO RACIONAL

5.3.0. Introducción a la tercera parte

Usualmente se motiva el concepto de número racional mediante la necesidad, ya sea de la existencia de números que representen las fracciones de la unidad, o de un campo numérico donde tenga solución la ecuación $bx = a$, para a y b números enteros con $b \neq 0$. Se define entonces el número racional como el cociente de dos enteros con denominador diferente de cero. El problema que tiene esta definición está en las definiciones de "el cociente de dos enteros" y de "el denominador de ese cociente", las cuales, en forma no matemática, se dan muchas veces por la simbología que se usa: el cociente de los enteros y se escribe como $\frac{a}{b}$, donde b es su denominador.

En la primera y segunda parte de este capítulo se hizo el estudio, en forma esquemática, del concepto de número natural teniendo como base los axiomas de Peano y el de número entero por abstracción y se probó que el de los naturales está inmerso en el de los enteros.

En esta tercera parte se define el conjunto de los números racionales por abstracción, y se prueba que el conjunto de los números enteros está inmerso en el de los racionales.

5.3.1. Número Racional

Consideremos el conjunto de enteros que no contiene al cero y lo denotamos por Z^*

Al igual que hicimos en el caso de los enteros, la definición de número racional se hará por abstracción.

Para ello definimos la siguiente relación ($\equiv$) sobre $Z \times Z^*$:

$$(x,y) \equiv (u,v) \Leftrightarrow xv = yu$$

Es trivial probar que ($\equiv$) define una relación de equivalencia sobre $Z \times Z^*$. ¡Pruébelo!.

Denotamos a la clase de equivalencia, determinada por ($\equiv$) en $Z \times Z^*$, del elemento $(x,y) \in Z \times Z^*$ por $\overline{(x,y)}$ y, al conjunto, $Z \times Z^* / \equiv$ de todas dichas clases de equivalencia, por: Q

Los elementos de Q serán llamados números racionales, y así Q será el conjunto de números racionales. Para que estas denominaciones tengan sentido, será necesario darle a Q una estructura de campo de números.

5.3.2. La adición y la multiplicación de números racionales (+) y (·)

Definición de suma y producto de números racionales (+) y (·)

1. A cada par de números racionales $\overline{(x,y)}$ y $\overline{(u,v)}$ se le asigna el número racional, llamado su suma, que viene definido y se denota por: $\overline{(x,y)} + \overline{(u,v)} = \overline{(xv + uy,yv)}$

2. A cada par de números racionales $\overline{(x,y)}$ y $\overline{(u,v)}$ se le asigna el número racional, llamado su producto, que viene definido y se denota por: $\overline{(x,y)} \cdot \overline{(u,v)} = \overline{(xu,yv)}$

Nota. Las operaciones de adición y multiplicación de números racionales están bien definidas. *Evidentemente* $\overline{(xv + uy,yv)}$ *y* $\overline{(xu,yv)}$ *son números racionales pues las sumas y productos de números enteros son números enteros y el producto de números enteros es cero sólo si alguno de los factores que lo componen es cero. Para que las operaciones de adición y multiplicación estén bien definidas sobre* $\mathcal{Q}$ *debe probarse, además, que los resultado de las operaciones no dependen de los elementos que representan las clases que se suman y multiplican decir: si* $\overline{(x_1,y_1)} = \overline{(x_2,y_2)}$ *y* $\overline{(u_1,v_1)} = \overline{(u_2,v_2)}$ *entonces:* $\overline{(x_1,y_1)} + \overline{(u_1,v_1)} = \overline{(x_2,y_2)} + \overline{(u_2,v_2)}$ *y* $\overline{(x_1,y_1)} \cdot \overline{(u_1,v_1)} = \overline{(x_2,y_2)} \cdot \overline{(u_2,v_2)}$

Lo cual se traduce a probar que: si $x_1y_2 = x_2y_1 \wedge u_1v_2 = u_2v_1$ entonces $(x_1v_1 + y_1u_1)y_2v_2 = (x_2v_2 + y_2u_2)y_1v_1$ y $x_1u_1y_2v_2 = x_2u_2y_1v_1$, lo cual se obtiene inmediatamente de las propiedades de las operaciones de adición y multiplicación de enteros.

Podemos concluir que ambas operaciones están bien definidas sobre $\mathcal{Q}$. Al igual que antes, eliminaremos el punto en la operación de multiplicación cuando no haya lugar a dudas, y escribiremos simplemente $\overline{(x,y)}\ \overline{(u,v)}$ por $\overline{(x,y)} \cdot \overline{(u,v)}$. En todo lo que sigue denotamos al número racional

$\overline{(x,y)}$ como $\frac{x}{y}$. Teniendo en cuenta esta notación, y las definiciones dadas, la suma y el producto de los racionales $\frac{x}{y}$ y $\frac{u}{v}$ quedan determinados por:

$$\frac{x}{y} + \frac{u}{v} = \frac{xv + yu}{yv} \quad \text{y} \quad \frac{x}{y} \times \frac{u}{v} = \frac{xu}{yv}$$

5.3.3. Propiedades de la adición y la multiplicación de números racionales. La diferencia y división de racionales

Teorema 5.3.3.1.- (propiedades de la adición y multiplicación de números racionales)

1. La adición y la multiplicación de números racionales es asociativa
2. La adición y la multiplicación de números racionales es conmutativa
3. La multiplicación es distributiva respecto a la adición
4. La adición y la multiplicación de números racionales tiene elemento identidad o neutro, los cuales son respectivamente $\frac{0}{1}$ y $\frac{1}{1}$
5. Todo número racional $\frac{x}{y}$ tiene inverso aditivo o recíproco $\frac{-x}{y}$

6. Todo número racional $\frac{x}{y}$ diferente de $\frac{0}{1}$ tiene inverso multiplicativo $\frac{y}{x}$

7. $\frac{0}{1} \neq \frac{1}{1}$.

Sólo haremos la demostración de la propiedad 7, las demás también son consecuencia inmediata de la definición y de las propiedades de la adición y la multiplicación de enteros.

Demostración de 7

Si $\frac{0}{1} = \frac{1}{1}$ entonces $(0)(1)=(1)(1)$ y el entero 0 es igual al entero 1, lo cual es una contradicción. Por tanto, $\frac{0}{1} \neq \frac{1}{1}$

- **Definición. (de resta o diferencia de racionales)** De forma similar ha como hicimos con los enteros, se define y se denota la resta o diferencia de los números racionales $x = \frac{a}{b}$, $y = \frac{c}{d}$ por: $x - y = \frac{a}{b} - \frac{c}{d} = \frac{a}{b} + \frac{-c}{d}$

- **Definición. (de división de racionales)** Ahora podemos definir la división (÷) de números racionales con divisor diferente de $\frac{0}{1}$, mediante la multiplicación con el inverso multiplicativo, es decir, se define y se denota la división de los números racionales $x = \frac{a}{b}$, $y = \frac{c}{d}$ con $\frac{c}{d} \neq \frac{0}{1}$, por: $x \div y = \frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c}$

Si $x = \frac{a}{b} \neq \frac{0}{1}$ entonces, su inverso multiplicativo $x^{-1} = \frac{b}{a}$ se denota por: $x^{-1} = \frac{1}{x}$

- **Definición (de los números racionales positivos)**

Se dice que un número racional $\frac{x}{y}$ es positivo si, y sólo si, el producto de los enteros xy es positivo, es decir, si $xy > 0$.

> ***Nota.*** *Notemos que el hecho de ser positivo un número racional está bien definido, lo que significa que el hecho de ser positivo no depende del elemento que represente la clase: Si* $x = \frac{a}{b} = \frac{c}{d}$ *entonces* $ad = bc$, *luego* $abdd = bbcd$, *y como* b *y* d *son diferentes de 0, inmediatamente se obtiene que:* $ab > 0$ *si, y sólo si,* $cd > 0$.

El conjunto de números racionales positivos se denota por Q^+.

Teorema 5.3.3.2. (de propiedades de Q^+)

1. $\frac{0}{1} \notin Q^+$
2. La suma y el producto de números racionales positivos es un número racional positivo.
3. Para todo número racional x, si $x \notin Q^+$ y $x \neq 0$, entonces $-x \in Q^+$.

Demostración

1. Pues, (0)(1)=0 y 0 no es mayor que 0.

2. Si $\frac{a}{b}, \frac{c}{d} \in Q^+$, entonces $ab > 0$, $cd > 0$ por definición.

Como $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ y $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$, debemos probar que: $(ad + bc)bd > 0$ y $achd > 0$. Estas desigualdades se obtienen inmediatamente del hecho que la suma y el producto de enteros positivos es un entero positivo.

3. Sea $x = \frac{a}{b} \in Q$ y $x \neq 0$. Si $x \notin Q^+$ entonces, por la propiedad de tricotomía de los enteros, $ab \leq 0$ pero, como $ab \neq 0$ pues $x \neq 0$, entonces $-(ab) = (-a)b > 0$, es decir, $-x \in Q^+$

5.3.4. El orden de los números racionales. La Inmersión de Z en Q

- **Definición (<).**

Sean $x,y \in Q$, arbitrarios. Decimos que x es menor que y, y lo denotamos por $x < y$, si y sólo si, $y - x \in Q^+$.

Teorema 5.3.4.1 (propiedades de (<))

Sean $x,y,z \in Q$ arbitrarios. Entonces:

1. Si $x < y \wedge y < z$, entonces $x < z$. (propiedad transitiva de (<))

2. Exactamente una y sólo una de las siguientes proposiciones es verdadera: $x < y$, $x = y$, $y < x$.

Demostración:

1. Inmediato aplicando que la adición es cerrada en Q^+, pues de ahí se sigue que $(y - x) + (z - y) \in Q^+$, de donde usando las propiedades de la adición de números racionales $z - x \in Q^+$, es decir, $x < z$.

2. Sean $x = \frac{a}{b}$, $y = \frac{c}{d}$. Entonces, como $x < y$, $x = y$, $y < x$ equivale por definición a $y - x \in Q^+$, $x = y$, $x - y \in Q^+$, se obtiene que equivale a que

$$(ad - bc)bd > 0,\ ad = bc,\ (bc - ad)bd > 0.$$

Pero como $bd \neq 0$, esto equivale a

$$(ad - bc) > 0,\ ad = bc,\ (bc - ad) > 0,$$

y aplicando ahora la propiedad de tricotomía para enteros se concluye la demostración de 2.

- **Definición (≤)**

Sean $x,y \in Q$, diremos que x es menor o igual que y lo denotamos por $x \leq y$ si, y sólo si, $x < y$, *o*, $x = y$.

Usando las propiedades correspondientes entre enteros se obtiene el siguiente resultado inmediatamente.

Teorema 5.3.4.2. (propiedades de (≤))

$(\mathcal{Q},\leq)$ es un conjunto totalmente ordenado, es decir:

1. $(\forall x,y \in \mathcal{Q})\ (x \leq y \vee y \leq x)$.
2. Es reflexiva, es decir, $(\forall x, \in \mathcal{Q})\ (x \leq x)$
3. Es transitiva, es decir, $(\forall x,y,z \in \mathcal{Q})\ (x \leq y \wedge y \leq z \Rightarrow x \leq z)$
4. Es antisimétrica, es decir, $(\forall x,y \in \mathcal{Q})\ (x \leq y \wedge y \leq x) \Rightarrow x = y$

Teorema 5.3.4.3 (de inmersión de Z en $\mathcal{Q}$)

***Z* está inmerso en $\mathcal{Q}$.**

La aplicación $Z \xrightarrow{f} \mathcal{Q}$ definida por $f(x) = \frac{x}{1}$ es una inmersión de Z en $\mathcal{Q}$, la cual es un isomorfismo respecto a la adición, a la multiplicación y al orden (≤), sobre su imagen, es decir, sobre el subconjunto de $\mathcal{Q}$ definido por $\left\{ \frac{x}{1} / x \in Z \right\}$ y, por ello se puede identificar $x \in Z$ con $f(x) = \frac{x}{1} \in \mathcal{Q}$, y considerar $Z \subset \mathcal{Q}$.

Esto significa que $f: Z \to \left\{ \frac{x}{1} / x \in Z \right\}$ definida por $f(x) = \frac{x}{1}$ es una aplicación biyectiva que satisface:

1. $(\forall x,y \in Z)\ \big(f(x + y) = f(x) + f(y)\big)$
2. $(\forall x,y \in Z)\ \big(f(x \cdot y) = f(x) \cdot f(y)\big)$
3. $(\forall x,y \in Z)\ \big(x \leq y \Rightarrow f(x) \leq f(y)\big)$

Demostración

f **es uno a uno,** pues *para cualesquiera* $x,y \in Z$ $f(x) = f(y) \Rightarrow \frac{x}{1} = \frac{y}{1}$ $\Rightarrow x = y$.

f **es sobre,** trivial.

Por tanto, es una aplicación biyectiva.

1. $f(x+y) = \frac{x+y}{1} = \frac{x \cdot 1 + y \cdot 1}{1 \cdot 1} = \frac{x}{1} + \frac{y}{1} = f(x) + f(y)$.

2. $f(x \cdot y) = \frac{x \cdot y}{1} = \frac{x \cdot y}{1 \cdot 1} = \frac{x}{1} \cdot \frac{y}{1} = f(x) \cdot f(y)$.

3. $x \leq y \Rightarrow y - x \geq 0 \Rightarrow \frac{y-x}{1} \geq 0 \Rightarrow \frac{y \cdot 1 - x \cdot 1}{1 \cdot 1} \geq 0 \Rightarrow \frac{y}{1} - \frac{x}{1} \geq 0$
   $\Rightarrow f(y) - f(x) \geq 0 \Rightarrow f(x) \leq f(y)$.

Mediante las inmersiones de N en Z y de Z en Q, podemos considerar que $N \subset Z \subset Q$.

5.3.5. Ejercicios propuestos

1. Demuestre que la relación $\equiv$, definida sobre $Z \times Z^*$ por: $(x,y) \equiv (u,v)$ si y sólo si $xv = yu$, es una relación de equivalencia.

2. Complete la demostración del teorema 5.3.3.1 sobre propiedades de la adición y de la multiplicación de números racionales.

3. Demuestre el teorema 5.3.4.2 sobre propiedades de $\leq$.

4. Diremos que x es un número racional negativo si, y sólo si $-x \in Q^+$ El conjunto de números racionales negativos lo denotamos por Q^-. Pruebe que:

   - $\frac{0}{1} \notin Q^-$.
   - La suma de dos números racionales negativos es un número racional negativo, es decir, Q^- es cerrado por la adición.
   - El producto de dos números racionales negativos es un número racional positivo.
   - Para todo número racional x, si $x \notin Q^-$ y $x \neq 0$, entonces $-x \in Q^-$

5. Sean $\frac{a}{b}, \frac{c}{\mathrm{d}}, \in Q^+$, Pruebe que $\frac{a}{b} < \frac{c}{\mathrm{d}}$, si y sólo si, $ad < bc$.

6. Teniendo en cuenta las identificaciones mediante las cuales podemos considerar que $N \subset Z \subset Q$. Pruebe que: $\forall x,y \in Q^+$ existe $n \in N$ tal que $y < nx$. (esta propiedad es conocida como la propiedad de Arquímides)

5.4 CUARTA PARTE: NÚMERO REAL

5.4.0. Introducción a la cuarte parte

En la primera y segunda parte se hizo el estudio, en forma esquemática, del concepto de número natural teniendo como base los axiomas de Peano y el de número entero por abstracción y se probó que el de los naturales está inmerso en el de los enteros.

En la tercera parte se definieron los números racionales y se probó que el conjunto de los números enteros está inmerso en el de los racionales.

En esta cuarta parte se definen los números reales por abstracción y se prueba que el conjunto de los números racionales está inmerso en el de los reales.

Sabemos que el conjunto de números racionales no es suficiente para medir longitudes. Desde hace mas de 25 siglos se conoce que el cuadrado de la medida de una hipotenusa en un triangulo rectángulo es igual a la suma de los cuadrados de las medidas de sus catetos.

Si el conjunto de números racionales fuera suficiente para medir longitudes, debería entonces existir un número racional x cuyo cuadrado fuera 2, pero de suponer que esto fuera posible es fácil llegar a una contradicción. (Suponga que $x = \frac{p}{q}$ donde p y q son primos entre sí, y $x^2 = 2$; entonces se obtiene que tanto p como q son pares, lo que es una contradicción pues niega que son primos entre sí)

De este hecho se puede concluir, que si consideramos una recta de puntos y le asociamos a cada número racional un punto de la recta, no hay forma de hacer la correspondencia de manera que se cubra la recta. Por tanto, si queremos tener un campo numérico que permita medir cualquier longitud de un segmento de recta, será necesario definir un nuevo campo en el cual se pueda considerar como subconjunto de este nuevo campo al conjunto de números racionales.

Esto se puede hacer de varias formas: Dedekind, en el año 1872, definió el número real mediante cortaduras; en el mismo año, Méray y Cantor desarrollaron un método mediante sucesiones de Cauchy, el cual evolucionó a través de los trabajos de Lipschitz (1877), Arzela (1883), y Bachmann (1892) hasta llegar a ser el de dos sucesiones monótonas contiguas; las clases contiguas fueron introducidas por Capelli en 1897.

Si bien las sucesiones de números racionales es el método de cálculo de la Aritmética para determinar raíces, logaritmos, el número e, etc; las clases contiguas son los instrumentos de la Aritmética y la Geometría para definir longitudes, áreas, volúmenes, etc. Por ejemplo el número π puede definirse como el número frontera entre dos sucesiones de números racionales, perímetros de polígonos inscriptos y circunscriptos.

5.4.1. El número real

Consideremos el conjunto Ω que tiene como elementos los pares de sucesiones racionales $(a,a') = ((a_n), (a'_n))$ que satisfacen las siguientes condiciones:

1. (a_n) es una sucesión creciente y (a'_n) es una sucesión decreciente de números racionales, es decir, $(\forall n \in N)\ (a_n \leq a_{n+1} \wedge a'_{n+1} \leq a'_n)$
2. $(\forall i,j \in N)\ (a_i \leq a'_j)$
3. $(\forall \varepsilon \in Q^+)\ (\exists m \in N) / (\forall n \in N)\ (n \geq m \Rightarrow a'_n - a_n < \varepsilon)$

Definimos, sobre ese conjunto Ω de pares de sucesiones de números racionales que satisfacen 1,2 y 3, la relación $(a,a') \equiv (b,b')$, por: $(a,a') \equiv (b,b')$ si y sólo si *para todo* $i \in N$, $[a_i \leq b_i \leq a'_i \vee b_i \leq a_i \leq b'_i] \wedge [b_i \leq a'_i \leq b'_i \vee a_i \leq b'_i \leq a'_i]$. Esta relación es una relación de equivalencia sobre Ω. Sobre Ω es evidentemente reflexiva y simétrica; probemos ahora que también es transitiva sobre dicho conjunto. Supongamos que $(a,a') \equiv (b,b')$ y $(b,b') \equiv (c,c')$, donde (a,a'), (b,b') y $(c,c') \in \Omega$.

Entonces: para todo $i \in N$, $\{[a_i \leq b_i \leq a'_i \vee b_i \leq a_i \leq b'_i] \wedge$
$[b_i \leq a'_i \leq b'_i \vee a_i \leq b'_i \leq a'_i] \wedge$
$[b_i \leq c_i \leq b'_i \vee c_i \leq b_i \leq c'_i] \wedge [c_i \leq b'_i \leq c'_i \vee b_i \leq c'_i \leq b'_i]\}$

Como: $(a_i \leq b_i \leq a'_i \vee b_i \leq a_i \leq b'_i) \wedge (b_i \leq c_i \leq b'_i \vee c_i \leq b_i \leq c'_i)$ equivale a $(a_i \leq b_i \leq a'_i \wedge b_i \leq c_i \leq b'_i) \vee (a_i \leq b_i \leq a'_i \wedge c_i \leq b_i \leq c'_i) \vee (b_i \leq a_i \leq b'_i \wedge b_i \leq c_i \leq b'_i) \vee (b_i \leq a_i \leq b'_i \wedge c_i \leq b_i \leq c'_i)$.

Obtenemos:

- de $a_i \leq b_i \leq a'_i \wedge b_i \leq c_i \leq b'_i$, que: $a_i \leq c_i$ y,
- de $b_i \leq a_i \leq b'_i \wedge c_i \leq b_i \leq c'_i$, que: $c_i \leq a_i$

Luego: $a_i \leq c_i \vee c_i \leq a_i$ (*)

Y, también obtenemos:

- de $a_i \leq b_i \leq a'_i \wedge c_i \leq b_i \leq c'_i$, que y $a_i \leq c'_i$ y
- como $a_i \leq a'_i$, de $c_i \leq a_i$, se sigue que $c_i \leq a'_i$.

Luego: $a_i \leq c'_i \vee c_i \leq a'_i$ (**)

Como: $\{[b_i \leq a'_i \leq b'_i \vee a_i \leq b'_i \leq a'_i] \wedge [c_i \leq b'_i \leq c'_i \vee b_i \leq c'_i \leq b'_i]\}$ equivale a $\{[b_i \leq a'_i \leq b'_i \wedge c_i \leq b'_i \leq c'_i] \vee [b_i \leq a'_i \leq b'_i \wedge b_i \leq c'_i \leq b'_i]\} \vee \{[a_i \leq b'_i \leq a'_i \wedge c_i \leq b'_i \leq c'_i] \vee [a_i \leq b'_i \leq a'_i \wedge b_i \leq c'_i \leq b'_i]\}$.

Obtenemos:

- de $[a_i \leq b'_i \leq a'_i \wedge c_i \leq b'_i \leq c'_i]$, que $c_i \leq a_i$ y,
- de $[a_i \leq b'_i \leq a'_i \wedge c_i \leq b'_i \leq c'_i]$, que $a_i \leq c'_i$,

Luego: $c_i \leq a'_i \vee a_i \leq c'_i$ (***)

Y, también obtenemos:

- de $[b_i \leq a'_i \leq b'_i \wedge c_i \leq b'_i \leq c'_i]$, que $a'_i \leq c'_i$ y,
- de $[a_i \leq b'_i \leq a'_i \wedge b_i \leq c'_i \leq b'_i]$, que $c'_i \leq a'_i$

Luego: $a'_i \leq c'_i \vee c'_i \leq a'_i$ (****)

Así, de (*) y (***), obtenemos que $a_i \leq c_i \leq a'_i \vee c_i \leq a_i \leq c'_i$

Y, de (***) y (****) que: $c_i \leq a'_i \leq c'_i \vee a_i \leq c'_i \leq a'_i$

Se sigue que $[a_i \leq c_i \leq a'_i \vee c_i \leq a_i \leq c'_i] \wedge [c_i \leq a'_i \leq c'_i \vee a_i \leq c'_i \leq a'_i]$, es decir, $(a,a') \equiv (c,c')$

Luego (≡) es transitiva y, por tanto, de equivalencia.

Si denotamos por $\overline{(a,a')}$ la clase de equivalencia correspondiente, entonces decimos que cada clase es un número real, y al conjunto cociente $\Omega/\equiv$ lo denotamos por $\mathbb{R}$ y lo llamamos conjunto de números reales.

Por supuesto, para que podamos llamarlos números, es necesario que se puedan definir las operaciones de adición y multiplicación entre ellos y se mantengan las propiedades conocidas a las correspondientes operaciones entre los números racionales.

5.4.2. La adición, la multiplicación y el orden entre números reales. La Inmersión de *Q* en *R*.

En este epígrafe se define la adición y multiplicación de números reales, se define su orden natural, se prueba que es un conjunto totalmente ordenado por ese orden y que Q está inmerso en R.

5.4.2.1 La adición de números reales

- **Definición de la adición de números reales.-** La adición de números reales se define asignando a cada par $\overline{(a,a')}$ y $\overline{(b,b')}$ un elemento de $\mathbb{R}$, llamado suma de $\overline{(a,a')}$ y $\overline{(b,b')}$, el cual queda definido por: $\overline{(a,a')} + \overline{(b,b')} = \overline{(a + b,a' + b')}$ donde la suma de sucesiones está definida como usualmente, es decir: $(a_n) + (b_n) = (c_n)$ donde $c_n = a_n + b_n$ y, aquí la suma, es la suma de números racionales.

Esta operación está bien definida, pues:

- Si (a,a'), $(b,b') \in \Omega$, entonces es trivial que $(a + b, a' + b') \in \Omega$. También.
- Si $\overline{(a,a')} = \overline{(c,c')}$ y $\overline{(b,b')} = \overline{(d,d')}$, entonces $\overline{(a + b,a' + b')} = \overline{(c + d,c' + d')}$

Demostremos esta última afirmación:

Si $\overline{(a,a')} = \overline{(c,c')}$ y $\overline{(b,b')} = \overline{(d,d')}$, entonces:

$\forall\, i \in N,\ [a_i \le c_i \le a'_i \vee c_i \le a_i \le c'_i] \wedge [c_i \le a'_i \le c'_i \vee a_i \le c'_i \le a'_i]$ y

$\forall\, i \in N,\ [b_i \le d_i \le b'_i \vee d_i \le b_i \le d'_i] \wedge [d_i \le b'_i \le d'_i \vee b_i \le d'_i \le b'_i]$

de donde se obtiene en forma inmediata que:

$\forall\, i \in N,\ [a_i + b_i \le c_i + d_i \le a'_i + b'_i \vee c_i + d_i \le a_i + b_i \le c'_i + d'_i] \wedge$
$[c_i + d_i \le a'_i + b'_i \le c'_i + d'_i \vee a_i + b_i \le c'_i + d'_i \le a'_i + b'_i]$

Es decir:

$$\overline{(a + b,a' + b')} = \overline{(c + d,c' + d)}$$

Notas.

A) Si tomamos las sucesiones de números racionales (a_n) y (a'_n) como las idénticamente nulas, entonces es trivial que $((a_n), (a'_n)) \in \Omega$, y que el elemento $\overline{(0,0)} = \overline{((a_n), (a'_n))}$ actúa como elemento neutro para la adición de números reales.

B) También es fácil ver que si $\overline{((a_n), (a'_n))} \in \Omega$, entonces $\overline{((-a'_n), (-a_n))} \in \Omega$

C) Además, si sumamos $\overline{((a_n), (a'_n))}$ y $\overline{((-a'_n), (-a_n))}$, la suma $\overline{((a_n) + (-a'_n), (a'_n) + (-a_n))}$ coincide con (0,0), pues es trivial que se cumple que $(\forall i \in N)\ [a_i - a'_i \le 0 \le a'_i - a_i]$

D) Por C), tiene sentido que: si denotamos por $x = \overline{((a_n), (a'_n))}$ a un número real, entonces para su inverso aditivo usar la notación: $-x = \overline{((-a'_n), (-a_n))}$

E) Análogamente a como se hizo en el caso racional, se define la resta o diferencia de números reales mediante la suma con el inverso aditivo, es decir, mediante la resta de sucesiones de números racionales, quedando así bien definida. Así $-\overline{(a,a')} = \overline{(-a',-a)}$ y $\overline{(a,a')} - \overline{(b,b')} = \overline{(a - b',a' - b)}$

F) Es fácil probar que $(\mathbb{R},+)$ es un grupo conmutativo.

- **Definición de número real positivo.** Decimos que el número real $\overline{(a_n), (a'_n)}$ es positivo si y sólo si, para algún $n \in N$ se tiene que $a_n > 0$.

Notas.

1) Veamos que está bien definido, es decir, que no depende del elemento que representa la clase. Sea $\overline{((a_n), (a'_n))} = \overline{((c_n), (c'_n))}$ y $a_n > 0$ para algún $n \in N$. Se tiene entonces que cualquiera sea $i \in N$, $[a_i \leq c_i \leq a'_i \vee c_i \leq a_i \leq c'_i] \wedge [c_i \leq a'_i \leq c'_i \vee a_i \leq c'_i \leq a'_i]$, luego, si $a_n \leq c_n$, se obtiene inmediatamente que $c_n > 0$ además, como $(c,c') \in \Omega$, y $\frac{1}{2} a_n$ es un número racional positivo, existe $k \in N$ tal que, si $m \geq k$ entonces $c'_m - c_m < \frac{1}{2} a_n$.

Además, es claro que $(\forall i,j \in N)\ (a_i \leq c'_j)$ es verdadero y, por tanto $a_n \leq c'_m$, de donde:

$a_n - c_m \leq c'_m - c_m < \frac{1}{2} \cdot a_n$ si $m \geq k$ y, de aquí inmediatamente se sigue que: $c_m > 0$ si $m \geq k$, es decir, $\overline{(c,c')} = \overline{((c_n),(c'_n)}$ es un número real positivo.

2) Si el número real $\overline{(a,a')} = \overline{((a_n),(a'_n))}$ es positivo, existe $(c,c') \in \Omega$, tal que $\overline{(a,a')} = \overline{((c_n),(c'_n)}$ y las sucesiones $c = (c_n)$ y $c' = (c'_n)$ son sucesiones de términos positivos. Para demostrar esto basta definir $c_n = a_{n+m}$ y $c'_n = a'_{n+m}$, donde $a_m > 0$. Es decir, cada vez que hablemos de un número $x = \overline{((a_n),(a'_n))}$ real positivo, podemos suponer que $a_n > 0$, *para todo* $n \in N$.

- **Definición de número real negativo.-** Decimos que el número real $x = \overline{((a_n),(a'_n))}$ es negativo si existe $n \in N$ tal que $-a'_n > 0$, en dicho caso, el número real $-x = \overline{((-a'_n), (-a_n))}$ es un número real positivo. Por tanto, de la nota anterior 2, cada vez que hablemos del número real negativo $x = \overline{((a_n),(a'_n))}$, podemos suponer que, $a'_n > 0$, *para todo* $n \in N$.

- **Definición del cero real.** Si un número real $x = \overline{((a_n),(a'_n))}$ no es positivo ni negativo, entonces $x = \overline{(0,0)}$

Esto es trivial, pues si no existe $n \in N$, tal que $a_n > 0$, y no existe tampoco $n \in N$, tal que $-a'_n > 0$, entonces $(\forall n \in N)\ (a_n \leq 0 \wedge 0 \leq a'_n)$.

Al número $x = \overline{(0,0)}$ el cual vimos en la nota anterior A) que es la identidad aditiva, se le llama el cero real.

Nota: *Es evidente que todo número real es positivo, negativo o coincide con el cero real, y que estas condiciones son excluyentes.*

5.4.2.2 El orden en $\mathbb{R}$

- **Definición de desigualdades.-** $(<,\leq,>,\geq)$ Dados dos números reales arbitrarios x y y, decimos que x es mayor que y, o que y es menor que x, y lo denotamos respectivamente por $x > y$ y $y < x$, si y sólo si, $x - y$ es positivo. Es inmediato, de la nota anterior, que dados dos números reales x,y, una y sólo una de las proposiciones siguientes es verdadera: $x < y$, $y < x$, $x = y$.

Como antes, definimos que, $x \geq y$ si, y sólo si, $x > y$ *o* $x = y$

Se siguen inmediatamente las propiedades siguientes:

Teorema 5.4.2.2.1.- (propiedades de $(\leq)$)

$(\mathbb{R},\leq)$ es un conjunto totalmente ordenado, es decir:

1. *Para cualesquiera* $x,y \in \mathbb{R}$, $x \leq y \vee y \leq x$
2. Es reflexiva, es decir, *para todo* $x \in \mathbb{R}$, $x \leq x$
3. Es transitiva, es decir, *para cualesquiera* $x,y \in \mathbb{R}$
   $x \leq y \wedge y \leq z \Rightarrow x \leq z$
4. Es antisimétrica, es decir, *para cualesquiera* $x,y \in \mathbb{R}$
   $x \leq y \wedge y \leq x \Rightarrow x = y$

5.4.2.3 La multiplicación de números reales

Definición de la multiplicación de números reales positivos

Dados dos números reales positivos x y y, podemos tomar, por la nota 2 de números positivos, $x = \overline{((a_n),(a'_n))}$ y $y = \overline{((b_n),(b'_n))}$ donde $a_n > 0$ y $b_n > 0$ para todo $n \in N$ y definir el producto de estos números reales positivos como: $xy = \overline{((a_n b_n),(a'_n b'_n))}$ pues:

Teorema 5.4.2.3.1. (la multiplicación de números reales positivos está bien definida)

- $\overline{((a_n b_n),(a'_n b'_n))} \in \Omega$
- el producto de la multiplicación no depende de los elementos que representan las clases correspondientes.
- xy es un número real positivo.

Al conjunto de números reales positivos lo denotamos por $\mathbb{R}^+$

Demostración

- Demostremos primero que, si $\overline{((a_n),(a'_n))} \in \Omega$ y $\overline{((b_n),(b'_n))} \in \Omega$, entonces: $\overline{((a_n b_n),(a'_n b'_n))} \in \Omega$ Por supuesto que $(a_n b_n)$ y $(a'_n b'_n)$ son sucesiones de números racionales, pues el producto de racionales es racional.
  Como $(\forall n \in N)\ (a_n \leq a_{n+1} \wedge a'_{n+1} \leq a'_n)$ y $(\forall n \in N)\ (b_n \leq b_{n+1} \wedge b'_{n+1} \leq b'_n)$ son proposiciones verdaderas entonces se sigue que también es verdadero que: $(\forall n \in N)\ (a_n b_n \leq a_{n+1} b_{n+1} \wedge a'_{n+1} b'_{n+1} \leq a'_n b'_n)$ de donde $(a_n b_n)$ es creciente y $(a'_n b'_n)$ es decreciente. Además, como para cualesquiera $i,j \in N$, $a_i \leq a'_j$ y $b_i \leq b'_j$, obtenemos que, para cualesquiera $i,j \in N$, $a_i b_i \leq a'_j b'_j$

Sabemos que: $\forall \varepsilon \in Q^+ \ \exists m_1 \in N / \forall n \in N,\ n \geq m_1 \Rightarrow a'_n - a_n < \varepsilon$
$\forall \varepsilon \in Q^+ \ \exists m_2 \in N / \forall n \in N,\ n \geq m_2 \Rightarrow b'_n - b_n < \varepsilon$
$\forall n \in N \quad a_n > 0 \wedge b'_n > 0 \quad$ (Pues $b'_n \geq b_n$)

Sea $\varepsilon \in Q^+$ arbitrario, y $m_1, m_2 \in N$, tales que:

$$\forall n \in N,\ n \geq m_1 \Rightarrow a'_n - a_n < \frac{1}{2b'_n} \cdot \varepsilon \quad \text{y}$$

$$\forall n \in N,\ n \geq m_2 \Rightarrow b'_n - b_n < \frac{1}{2a_n} \cdot \varepsilon$$

Entonces, para $m = max\{m_1, m_2\}$, se tiene que:

$$\forall n \in N,\ (n \geq m \Rightarrow b'_n - b_n < \frac{1}{2a'_n} \cdot \varepsilon) \wedge (n \geq m \Rightarrow a'_n - a_n < \frac{1}{2b'_n} \cdot \varepsilon)$$

De donde, $\forall n \in N$ si $n \geq m$, se tiene que $(b'_n - b_n)\, a_n < \frac{1}{2} \cdot \varepsilon$ y $b'_n (a'_n - a_n) < \frac{1}{2} \cdot \varepsilon$.

Y, de aquí se sigue, usando que la adición es cerrada en $\mathbb{R}^+$, que:

$$\forall n \in N,\ \exists m \in N,\ n \geq m \Rightarrow a'_n b'_n - a_n b_n < \varepsilon.$$

Por tanto, podemos concluir que:

$$((a_n b_n),(a'_n b'_n)) \in \Omega$$

- Sean $x = \overline{(a,a')} = \overline{(c,c')}$ y $y = \overline{(b,b')} = \overline{(d,d')}$ números reales positivos, y supongamos, sin pérdida de generalidad que $a_n > 0$, $c_n > 0$, $b_n > 0$ y $d_n > 0$, *para todo* $n \in N$, entonces debemos probar que: $\overline{(a,a')} \cdot \overline{(b,b')} = \overline{(b,b')} \cdot \overline{(d,d')}$, es decir,

$$(\overline{(a_n b_n),(a'_n b'_n)}) = (\overline{(c_n d_n),(c'_n d'_n)})$$

Para ello debemos probar que:

$$\forall i \in N, \quad [a_i b_i \leq c_i d_i \leq a'_i b'_i \vee c_i d_i \leq a_i b_i \leq c'_i d'_i] \wedge$$
$$[c_i d_i \leq a'_i b'_i \leq c'_i d'_i \vee a_i b_i \leq c'_i d'_i \leq a'_i b'_i] \quad (*)$$

Como $\forall i \in N,\ [a_i \leq c_i \leq a'_i \vee c_i \leq a_i \leq c'_i] \wedge [c_i \leq a'_i \leq c'_i \vee a_i \leq c'_i \leq a'_i]$

$\forall i \in N,\ [b_i \leq d_i \leq b'_i \vee d_i \leq b_i \leq d'_i] \wedge [d_i \leq b'_i \leq d'_i \vee b_i \leq d'_i \leq b'_i]$ se obtiene (*) inmediatamente.

- Es trivial que el producto de números reales positivos es positivo, pues el producto de números racionales positivos es positivo.

Definición de la multiplicación en general de números reales

Se define ahora el producto de la multiplicación de números reales arbitrarios de la siguiente forma:

1. Si x y y son positivos, ya lo definimos.

2. Si x y y son negativos, lo definimos como el producto de la multiplicación de los números positivos $(-x)$ y $(-y)$, es decir, $x \cdot y = (-x)(-y)$.

3. Si x es negativo y y es positivo, entonces se define por: $x \cdot y = -((-x) \cdot y)$ Y, en forma análoga, si x es positivo y y es negativo, por: $x \cdot y = -(x \cdot (-y))$

4. Si x o y no es positivo ni negativo, es decir, si $x = \overline{(0,0)}$ o $y = \overline{(0,0)}$ entonces $xy = \overline{(0,0)}$

Las propiedades siguientes se siguen inmediatamente.

Teorema 5.4.2.3.1 (Propiedades de la adición y la multiplicación de números reales)

1. La adición y la multiplicación de números reales es asociativa.

2. La adición y la multiplicación de números reales es conmutativa.

3. La multiplicación es distributiva respecto a la adición en los números reales.

4. La adición y la multiplicación de números reales tiene elemento identidad o neutro, los cuales son respectivamente $\overline{(0,0)}$ y $\overline{((1),(1))}$

5. Todo número real x tiene inverso aditivo o recíproco $-x$.

6. Todo número real $x \neq \overline{(0,0)}$ (por lo que podemos tomar $x = \overline{(a_n),(a'_n)}$ con $a_n > 0 \vee a'_n < 0$, $\forall n \in N$, tiene inverso multiplicativo $\frac{1}{x}$, donde $\frac{1}{x} = \overline{\left(\left(\frac{1}{a'_n}\right),\left(\frac{1}{a_n}\right)\right)}$

7. $\overline{(0,0)} \neq \overline{((1),(1))}$

Además, es fácil probar que, cualesquiera sean x,y números reales tales que, para todo ε número real positivo $x \leq y + \varepsilon$, entonces se tiene que $x \leq y$.

Teorema 5.4.2.3.2 está inmerso en $\mathbb{R}$

La aplicación f: $Q \to \mathbb{R}$ definida por $f(x) = (\overline{(x),(x)})$ es una inmersión de Q en $\mathbb{R}$ la cual es un isomorfismo respecto a la adición, a la multiplicación y respecto al orden **(≤),** sobre su imagen, es decir, sobre el subconjunto de $\mathbb{R}$ definido por $\{(\overline{(x),(x)}): x \in Q\}$, y por ello se puede identificar x con $(\overline{(x),(x)})$ y considerar a $Q \subset \mathbb{R}$ Esto significa que la función definida anteriormente es una aplicación biyectiva sobre su imagen que satisface: $\forall x,y \in Q$

1. $f(x + y) = f(x) + f(y)$
2. $f(x \cdot y) = f(x) \cdot f(y)$
3. $x \leq y \Rightarrow f(x) \Rightarrow f(y)$

Lo cual es evidente. Así podemos considerar $N \subset Z \subset Q \subset \mathbb{R}$

Nota.- Notemos ahora que para cada número real $x = (\overline{(a_n),(a'_n)})$ existen dos únicas posibilidades: existe un único $y \in Q$ tal que $a_n \leq y \leq a'_n$, *para todo* $n \in N$, en cuyo caso $x = (\overline{(y),(y)}) = y$, o no existe tal y, en cuyo caso decimos que x es irracional y lo denotamos por $x \in$ I, así tenemos que $\mathbb{R} = Q \cup I$.

Además, ahora podemos hacer una correspondencia biunívoca entre los puntos de una recta y los números reales, pues los huecos que dejan los racionales los llenan los irracionales, al quedar encerrados entre dos sucesiones contiguas de puntos correspondientes a números racionales.

Por tanto, hemos construido un campo numérico, el campo numérico de los números reales, con el cual podemos medir segmentos de recta con longitudes de cualquier valor.

5.4.3. Sobre cotas y conjuntos acotados

- **Definición de conjunto acotado superiormente**

Sea $A \subset R$. Si existe $b \in R$, tal que cada $x \in A$, $x \leq b$, diremos que b es una cota superior de A, y que A es un conjunto acotado superiormente por b.

Decimos una cota superior, pues cualquier número real mayor que una cota superior de un conjunto dado, también es, evidentemente, una cota superior de dicho conjunto.

Un conjunto no vacío de números reales sin cota superior, se dice que no es acotado superiormente. Es claro que cualquier número real es cota superior del conjunto vacío en el universo R.

- **Definición de máximo de un conjunto de números reales.**

Si una cota superior b de un conjunto A, es elemento de A, decimos que b es el último elemento o máximo de A. A lo sumo un conjunto A puede tener un elemento máximo b, en el caso que lo tenga, escribiremos $b = \max A$.

- **Definición de supremo de un conjunto de números reales.-**

Sea $A \subset R$, y $b \in R$. Diremos que b es el supremo de A, o extremo superior de A, y escribiremos $b = \sup A$, si se cumple que:

1. b es cota superior de A.
2. Para cada $y \in R$ si $y < b$ entonces y no es cota superior de A.

Es fácil probar que un conjunto de números reales no puede tener dos extremos superiores diferentes, es decir, si tiene supremo es único, por lo que podemos hablar del extremo superior o supremo de A.

Es también inmediato que si A tiene máximo, entonces $\max A = \sup A$.

Las definiciones de cota inferior, conjunto acotado inferiormente, conjunto no acotado inferiormente, mínimo e ínfimo se pueden dar en forma análoga y se deja como ejercicio.

El conjunto de números reales puede también definirse en forma axiomática, como se hace generalmente en análisis matemático, por ejemplo vea la referencia 3. Una proposición que muchas veces se toma como axioma, y es el axioma que distingue en esa definición a los reales de los racionales, es el conocido como "axioma del supremo" o "axioma de completitud", que nosotros damos a continuación como teorema.

Teorema 5.4.3.1 (del supremo o de completitud de *R*)

Sea $A \subset R$, $A \neq \emptyset$, y A acotado superiormente. Entonces existe $\sup A$.

Demostración

Por hipótesis existen $a \in A$ y $b \in R$ cota superior de A, así $a \leq b$. Si $a = b$ o si $b \in A$, entonces $b = \sup A = \max A$ y no hay nada que demostrar. Supongamos que $a < b$ y $b \notin A$. Sean $a = \overline{((a_n),(a'_n))}$ y $b = \overline{((b_n),(b'_n))}$ donde sin perdida de generalidad podemos suponer que $\forall n,m \in N$, $a'_n < b_m$, pues $a < b$. Consideremos ahora el punto medio entre a y b, que es el número real $\frac{a+b}{2} = \overline{\left(\left(\frac{a_n + b_n}{2}\right), \left(\frac{a'_n + b'_n}{2}\right)\right)}$. Hay dos posibilidades: 1) que $\frac{a+b}{2}$ sea cota superior de A, y 2) que no lo sea.

En el primer caso puede ocurrir que $\frac{a+b}{2} \in A$, o que $\frac{a+b}{2} \notin A$. Si $\frac{a+b}{2} \in A$, entonces $\frac{a+b}{2} = \sup A = \max A$ y terminamos. Si $\frac{a+b}{2} \notin A$, entonces consideramos $a^{(1)} = a = \left((a_n^{(1)}), (a'_n{}^{(1)})\right)$ y $b^{(1)} = \frac{a+b}{2} = \left(\overline{(b_n^{(1)}), (b'_n{}^{(1)})}\right)$ donde, sin perdida de generalidad, podemos suponer que $\forall n,m \in N$, $a'_n{}^{(1)} < b_m^{(1)}$ pues $a^{(1)} < b^{(1)}$ y $b^{(1)} \notin A$.

En el segundo caso existe $a^{(1)} = \left((a_n^{(1)}), (a'_n{}^{(1)})\right) \in A$ con $a^{(1)} \geq \frac{a+b}{2}$. Consideramos $b^{(1)} = b = \left(\overline{(b_n^{(1)}), (b'_n{}^{(1)})}\right)$, así que $a^{(1)} < b^{(1)}$ y podemos suponer, sin pérdida de generalidad que $\forall n,m \in N$, $a'_n{}^{(1)} < b_m^{(1)}$.

Notemos que en cualquiera de los dos casos o encontramos un elemento de A que es cota superior de A y por tanto su máximo que es su supremo, o dos números reales, $a^{(1)} = \left((a_n^{(1)}), (a'_n{}^{(1)})\right) \in A$ y $b^{(1)} = \left(\overline{(b_n^{(1)}), (b'_n{}^{(1)})}\right)$ la cual es una cota superior de A que no pertenece a A, tales que $\forall n,m \in N$, $a'_n{}^{(1)} < b_m^{(1)}$.

Reiterando el procedimiento, o para algún $k \in N$, $b^{(k)}$ es el supremo de A con lo que se terminaría la demostración, o construimos una secuencia de pares de números reales $(a^{(k)},b^{(k)})$, con $a^{(k)} = \left((a_n^{(k)}), (a'_n{}^{(k)})\right)$ y $b^{(k)} = \left((b_n^{(k)}), (b'_n{}^{(k)})\right)$, tales que:

1) $a^{(k)} \in A$ y $b^{(k)}$ es una cota superior de A, *para todo* $k \in N$

2) $\forall n,m \in N$, $a'_n{}^{(k)} < b_m^{(k)}$

3) $b^{(k)} - a^{(k)} \leq \frac{b - a}{2^{k+1}}$

Ahora es fácil demostrar que el número real definido por $c = \left((a_n^{(n)}), (b'_n{}^{(n)})\right)$ es el supremo de A. El lector deberá concluir la demostración.

El lector deberá enunciar y demostrar una propiedad, análoga a la anterior, para el ínfimo.

A continuación enunciamos y demostramos otras tres propiedades del supremo que tienen cada una, respectivamente, su análogo con el ínfimo.

1) Propiedad de la aproximación.- Sea A un conjunto no vacío de números reales con $b = \sup A$. Entonces para cada y con $y < b$, existe $x \in A$ con $y < x \leq b$.

Demostración. Si existe y, con $y < b$, tal que para cada $x \in A$ $x \leq y$, entonces b no puede ser supremo de A, ya que y sería una cota superior de A y $y < b$.

2) Propiedad aditiva. Sean A y B conjuntos no vacíos de números reales acotados superiormente. Consideremos el conjunto C definido por $C = \{x + y, / x \in A, y \in B\}$. Entonces C es acotado superiormente y $\sup C = \sup A + \sup B$.

Demostración. Sabemos que existen números reales a y b tales que $a = \sup A$, y $b = \sup B$. Si $z \in C$, entonces existen $x \in A$, $y \in B$, tales que $z = x + y$, luego $z \leq a + b$. Así $a + b$ es una cota superior de C, y C es acotado superiormente, luego existe un número real c tal que $c = \sup C$. Probemos que $c = a + b$:

1) $c \leq a + b$, por definición de supremo.

2) Sea $\varepsilon > 0$ arbitrario, por definición de supremo y ser $\frac{\varepsilon}{2} > 0$, existen $x \in A$, $y \in B$, tales que $a - \frac{\varepsilon}{2} < x$, y $b - \frac{\varepsilon}{2} < y$; por ser $c = \sup C$, y $x + y \in C$, se sigue que $a + b - \varepsilon < x + y \leq c$; luego para cada $\varepsilon > 0$ se tiene que $a + b \leq c + \varepsilon$, lo que implica que $a + b \leq c$.

Por tanto, de 1) y 2), $c = a + b$

3) Propiedad de la comparación

Sean A y B conjuntos no vacíos de números reales que cumplen la relación $(\leq)$ $\forall a \in A, b \in B, a \leq b$. Entonces si B está acotado superiormente, A también lo está y $\sup A \leq \sup B$.

Demostración.- Evidente, se deja como ejercicio.

***Nota.* Corolarios:**

1. **El conjunto de los enteros positivos no es acotado superiormente.-** Supongamos que lo fuera, entonces existe $a \in \mathbb{R}$, $a = sup Z^+$. Luego $a - 1$ no es cota superior de Z^+ y existe $z \in Z^+$, tal que $a - 1 < z$. Se sigue que $a < z + 1$, y como $z + 1 \in Z^+$, pues $z \in Z^+$, entonces a no puede ser cota superior de Z^+. Esto es una contradicción con $a = \sup Z^+$, y por tanto Z^+ no está acotado superiormente.

2. **Para cada número real x, existe un entero positivo n, tal que $n > x$.-** Inmediato, en caso contrario Z^+ estaría acotado superiormente.

3. **(Propiedad Arquimediana de los números reales) Si x es un número real positivo, y si y es un número real arbitrario, existe un entero positivo n, tal que $nx > y$.**

Basta aplicar 2 al número real $\frac{y}{x} = y \cdot \left(\frac{1}{x}\right)$, y después multiplicar a ambos miembros de la desigualdad $n > \frac{y}{x}$, por el real positivo x.

5.4.4. Representación decimal

Un número real de la forma $r = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n}$, para cada $n \in N$, donde a_0 es un entero no negativo y $a_1, \ldots, a_n$ son enteros con $0 \leq a_i \leq 9$, *para cada i*, se escribe usualmente de la forma $r = a_0 a_1 a_2 \ldots a_n$.. Esta expresión recibe el nombre de representación decimal finita de r. Por ejemplo:

$$\frac{29}{4} = 7 + \frac{2}{10} + \frac{5}{10^2} = 7.25$$

Los números reales que pueden simbolizarse de esta forma son números racionales, de hecho $r = \frac{a}{10^n}$, donde a es un entero. Pero no todo número racional es de este tipo, por ejemplo, $\frac{1}{3}$ no lo es, pues si lo fuera, $10^n = 3a$ para algún entero a y por tanto 10^n, para algún n natural, sería múltiplo de 3, lo cual sabemos que es falso.

Como una consecuencia del teorema del supremo, podemos probar que todo número real se puede aproximar, tanto como se quiera, por racionales de representación decimal finita.

Teorema 5.4.4.1 (de aproximación por racionales de representación decimal finita)

Sea x un número real no negativo, es decir $x \geq 0$. Entonces para todo $n \in N$, existe un racional r_n de representación decimal finita, tal que:

$$r_n \leq x < r_n + \frac{1}{10^n}$$

Demostración

Sea A el conjunto de todos los enteros no negativos menores o igual a x. El conjunto A está acotado superiormente por x, luego existe $a_0 = \sup A$, y es fácil probar que $a_0 \in A$. Llamaremos a_0 el mayor entero menor o igual a x, y lo denotaremos por $a_0 = [x]$. Es trivial que $0 \leq a_0 \leq x < a_0 + 1$.

Sea ahora $a_1 = [10x - 10a_0]$, el mayor entero menor o igual a $10x - 10a_0$. Se sigue de $0 \leq 10x - 10a_0 = 10(x - a_0) < 10$, que $0 \leq a_1 \leq 9$, y $a_1 \leq 10x - 10a_0 < a_1 + 1$, es decir, a_1 es el mayor entero, con $0 \leq a_1 \leq 9$, tal que:

$$a_0 + \frac{a_1}{10} \leq x < a_0 + \frac{a_1 + 1}{10}$$

Reiterando el procedimiento obtenemos que: habiendo elegido para $n \in N$, una secuencia de enteros no negativos $a_1, a_2, \ldots, a_{n-1}$, con $0 \leq a_i \leq 9$, *para todo i*, escogemos a_n el mayor entero que satisface las desigualdades:

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n + 1}{10^n} . \qquad (*)$$

De donde $0 \leq a_n \leq 9$, y podemos concluir que:

$$r_n \leq x < r_n + \frac{1}{10^n} \qquad \text{con} \qquad r_n = a_0 \cdot a_1 a_2 \ldots a_n ,$$

lo cual completa la demostración.

Es fácil verificar que x es el supremo del conjunto de los números racionales: $\{r_n : n \in N\}$

Los enteros a_0, a_1, a_2 ... obtenidos en la demostración anterior, pueden utilizarse para definir una representación decimal infinita del número real x. Escribiremos así:

$$x = a_0 \, . \, a_1 a_2 \ldots$$

donde $\forall n \in N$, a_n es el mayor entero que satisface (*)

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n + 1}{10^n}$$

Por ejemplo: si $x = \frac{1}{4}$ obtendremos $a_0 = 0$, $a_1 = 2$, $a_2 = 5$, $a_n = 0$, *para* $n \geq 3$ por lo que podemos escribir

$$\frac{1}{4} = 0.25000 \ldots$$

Si intercambiamos los signos en las desigualdades de (*) y ponemos

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} < x \leq a_0 + \frac{a_1}{10} + \ldots + \frac{a_n + 1}{10^n},$$

obtenemos una definición ligeramente diferente de representación decimal infinita. En este caso, para $x = \frac{1}{4}$, obtendremos:

$a_0 = 0$, $a_1 = 2$, $a_2 = 4$, $a_n = 9$, *para cada* $n \geq 3$, por lo que podemos escribir

$$\frac{1}{4} = 0.24999 \ldots$$

El hecho de que un número real pueda tener más de una representación decimal no debe extrañar, pues dos conjuntos diferentes pueden tener el mismo supremo.

En todo lo que sigue, una representación decimal del número real no negativo x es cualquiera de las que se obtiene de acuerdo a los dos modelos de construcción anteriores; es de destacar que las representaciones que se obtienen por ambos modelos de construcción son las mismas, excepto casos similares al anterior, donde cada una de las representaciones terminan en infinitos ceros consecutivos e infinitos nueves consecutivos respectivamente, pues la solución de los a_i es única.

- **Definición de representación decimal infinita periódica.-** Sea x un número real no negativo, y $x = a_0 \cdot a_1 a_2 \ldots$ una representación decimal de x. Diremos que la representación decimal de x es infinita periódica, si y sólo si, existen j,k, enteros no negativos, tales que:

$$\textit{Para cada } n \in N,\ a_j = a_{j+nk},\ a_{j+1} = a_{j+1+nk},\ldots,\ a_{j(k-1)} = a_{j+(k-1)+nk}$$

Teorema 5.4.4.2 (acerca de la representación decimal de racionales e irracionales)

Sea x un número real no negativo, y $x = a_0 \cdot a_1 a_2 \ldots$ una representación decimal de x. Entonces x es un número racional, si y sólo si, la representación decimal de x es infinito periódica.

Demostración:

Sea x un número real no negativo, y $x = a_0 \cdot a_1 a_2 \ldots$ una representación decimal infinita periódica de x. Probemos que x es un número racio-

nal. Sabemos que x es el supremo del conjunto de números racionales $\{r_n : n \in N\}$, donde

$x = a_0 \cdot a_1a_2 \ldots a_n$, es decir $r_n = a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}$.

Sean j,k los enteros no negativos de la definición de representación decimal infinita periódica de x, y sea el número entero

$$a + 10^{k-1} a_j + 10^{k-2} a_{j+1} + \ldots + a_{j+(k-1)}$$

Sea $R_n = a_0 + \frac{a_1}{10} + \ldots + \frac{a_{j-1}}{10^{j-1}} + \frac{a}{10^{j+1(k-1)}} \left(1 + \frac{1}{10^k} + \ldots + \frac{1}{10^{kn}}\right)$

Entonces, como es evidente que $\{r_n\} = \sup\{R_n\}$. Por tanto, se puede concluir:

$$x = \sup\{R_n\} = a_0 + \frac{a_1}{10} + \ldots + \frac{a_{j-1}}{10^{j-1}} + \frac{a}{10^{j+1(k-1)}} \cdot \frac{10^k}{10^k - 1} \in Q$$

Supongamos ahora que x es un número real no negativo y que $x = a_0 \cdot a_1a_2 \ldots$ es la representación decimal de x lograda según las desigualdades en (*). Debemos probar que si $x \in Q$ entonces la representación decimal es infinita periódica. Es claro que podemos considerar, sin perdida de generalidad, que la representación decimal es la lograda según el modelo con las desigualdades según (*).

Sea $x = \frac{p}{q}$, $p,q \in Z^+$, primos entre sí (Si $p = 0$, es trivial, pues $x = 0.000\ldots$ sería la representación decimal infinita periódica de x). Por tanto, $a_0 + \left(\frac{p}{q}\right)$ y habiendo elegido para $n \in N$, una secuencia de enteros no negativos $x = a_0 \cdot a_1a_2 \ldots a_{n-1}$, con $0 \leq a_i \leq 9$, $\forall i$, escogemos a_n el mayor entero que satisface las desigualdades:

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \leq \frac{p}{q} < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n + 1}{10^n}.$$

De donde $0 \leq a_n \leq 9$.

Notemos que para cada $n \in N$, a_n es la solución al problema de encontrar el máximo entero, que cumple $0 \leq a_n \leq 9$ y para el cual, dado cierto número entero no negativo b_n, con $b_n < q$, resulta: $b_n 10^n = q a_n 10^n + b_{n+1}$ con b_{n+1} un entero no negativo y $b_{n+1} < q$. Como el conjunto de enteros no negativos que son menores que q es un conjunto finito, deben existir j,k, enteros no negativos, tales que: $b_j = b_{j+k}$, por lo que se tiene que:

Para cada $n \in N$, $a_j = a_{j+nk}$, $a_{j+1} = a_{j+1+nk}$, ..., $a_{j+(k-1)} = a_{j+(k-1)+nk}$

Lo cual implica que la representación decimal de $x = \frac{p}{q}$ es infinita periódica.

Con esto queda completa la demostración del teorema.

Como un corolario de este teorema se tiene que x es irracional, es decir, real no racional, si y sólo si, su representación decimal es infinita no periódica.

5.4.5. Ejercicios propuestos

1. Demuestre que la relación $\equiv$ sobre Ω es una relación de equivalencia.

2. Sean $(a,a'), (b,b') \in \Omega$. Pruebe que: a) $(-a',-a) \in \Omega$, y b) $(a+b,a'+b') \in \Omega$.

3. Pruebe que $(R,+)$ es un grupo conmutativo.

4. Demuestre el teorema sobre propiedades de $(\leq)$, es decir, que $(R,\leq)$ es totalmente ordenado.

5. Pruebe que todo número real es positivo, negativo o coincide con el cero real, y que estas condiciones son excluyentes.

6. Demuestre el teorema sobre propiedades de la adición y multiplicación de números reales y concluya que $(R,+,\cdot)$ es un cuerpo conmutativo.

7. Sean $x,y \in R$. Pruebe que si $x \leq y + \varepsilon$, *para todo* $\varepsilon > 0$, entonces $x \leq y$.

8. Complete la demostración del teorema: Q está inmerso en R.

9. Para conjutos no vacíos de números reales, dé las definiciones de: cota inferior, conjunto acotado inferiormente, ínfimo, y mínimo. Demuestre que todo conjunto no vacío de números reales acotado inferiormente tiene ínfimo.

10. Enuncie y demuestre una propiedad de aproximación para el ínfimo.

11. Enuncie y demuestre una propiedad aditiva para el ínfimo.

12. Demuestre la propiedad de comparación para el supremo y, enuncie y demuestre una para el ínfimo.

13. Complete la demostración de la propiedad Arquimediana para los números reales.

14. Pruebe que *para todo* $n \in N$, $\sqrt{n-1} + \sqrt{n+1}$ es irracional.

15. Sea $x \in Q^+$, expresado en la forma: $x = \sum_{k=1}^{n} \frac{a_k}{k!}$ donde cada a_k es un entero no negativo con $a_k \leq k - 1$ para $k \geq 2$, y $a_n > 0$. Sea $[x]$ el mayor entero contenido en x. Pruebe que: $a_1 = [x]$, que $a_k = [k!x] - k[(k-1)!x]$ para $k = 2,..., n$, y que n es el menor entero tal que $n!x$ es entero. Recíprocamente, pruebe que cada número racional positivo x puede ser expresado en esta forma de una manera y sólo una.

Bibliografía

Avelsgaard, C. (1990). *Foundations for Advanced Mathematics.* USA: Scott, Foresman and Company.

Aponte, G. (1998). *Fundamentos de matemáticas básicas*, México: Addison Wesley Longman.

Apóstol, T. (2001). *Análisis matemático.* (2da ed.), España: Editorial Reverté.

Bartle, R. G. (1992). *Introducción al análisis matemático*, México: Editorial Limusa.

Chartrand, G.. Polimeni, A. & Shang, P. (2003). *Mathematical Proofs. A Transition to Advanced Mathematics.* USA: Pearson Education, Inc.

Dieudonné, J. (1966). *Fundamentos de análisis moderno,* España: Editorial Reverté, S. A.

Friedman, A. (1982). *Foundations of Modern Analysis,* N.Y. USA: Dover Publicationss, Inc.

Fraguela Collar, A. (2004). *Análisis matemático avanzado,* México: Benemérita Universidad Autónoma de Puebla, Dirección General de Fomento Editorial.

Fraleigh, J. B (1987). *Álgebra abstracta,* USA: Editorial Addison Wesley Iberoamericana, S. A.

Jiménez Pozo, M. (2004). "Viaje al infinito" [en línea] *Revista Elementos* No. 63, disponible en www.elementos.buap.mx/num63/pdf/15.pdf [Accesado el 23 de mayo de 2012].

Rey Pastor, J., Calleja, P. & Trejo, C. (1960). *Análisis matemático*, Vol. 1. (5ta ed.), Argentina: Editorial Kapelusz.

Ross, K. A. (1980). *Elementary Analysis: The Theory of Calculus*, USA: Springer Verlag.

Silva, J. M. & Lazo, A. (2003). *Fundamentos de matemáticas.* (6ta ed.), México: Editorial Limusa.

Solow, D. (1992). *Cómo entender y hacer demostraciones en matemáticas*, México: Editorial Limusa.

Suppes, P. & Hill, S. (1996). *Introducción a la lógica matemática.* México: Editorial Reverté.

Zuazua, E. (2007). *El momento de las matemáticas*, España: Sigma 31.

Esta edición de *Fundamentos de matemática avanzada*, de René Piedra, se terminó de imprimir en el mes de octubre de 2012, la edición consta de 500 ejemplares, impreso en los talleres gráficos de Editora Búho, Santo Domingo, República Dominicana.

Es miembro de número de la Academia de Ciencias de República Dominicana y miembro de la sociedad de Matemáticos de República Dominicana. Participó además en el Segundo Congreso Internacional para la mejora de la Enseñanza de la Matemática, de los dos conferencistas invitados. Ha participado como jefe de la delegación de Repíblica Dominicana en las Olimpiadas Iberoamericanas durante el 2003, 2004, 2005 y 2008. Participó activamente en el Simposio Internacional Certificación Docente y Calidad Educativa, certificado por INTEC y el College Board de Puerto Rico y América Latina.

Participó en el Seminario sobre Espacios de funciones realizado en el Centro Internacional Stephan Banach de la Academia de Ciencias de Varsovia; en el Seminario Internacional sobre Aproximación en el Instituto Steklov de la Academia de Ciencias de Moscú.

Tiene diversas publicaciones en el área de matemática: artículos en revistas científicas internacionales de reconocido prestigio, tales como a Springer-Verlag, la revista Ciencias Matemáticas de Cuba, la publicación que hace el Centro Internacional Stephan Banach de la Academía de Ciencias de Varsovia, Polonia, y la que realiza el Seminario Internacional Interuniversitario de la Universidad de Puerto Rico.

Sus escritos forman parte de algunas de las memorias anuales de la Academia de Ciencias de R.D. y de la revistas Sociedad de Matemática de Primero a Cuartp Grado. Tuvo la encomienda de realizar la adaptación de la sexta edición del libro de Precálculo de Max Sobel y la revisión técnica de la décimo primera edición del Libro de Cálculo de George Thomas, ambas para la Editorial Pearson.

El Instituto Tecnológico de Santo Domingo se enorgullece de publicar esta singular obra que aporta al conocimiento de los fundamentos, las competencias y el análisis de la matemática en nuestro país.

Este libro constituye un excelente aliado para la información del profesor de Matemático del Nivel Medio y de los primeros años de la universidad, o sea, previo al Cálculo. Está abordado con un lenguaje científico, dando mayor importancia a la notación matemática, a las generalizaciones, las propiedades y las demostraciónes. Creemos que la obra es valiosa porque aporta al desarrollo de competencias matemáticas en República Dominicana.

En una rápida revisión del texto, pudimos constatar que sigue un orden lógico y secuencial, con explicaciones claras y ejemplos ilustrativos y de fácil compresión. Indudablemente, la obra proporciona al docente un instrumento para retomar la visualización general del tema.

Este texto confirma el hecho de que suprimir las estructuras algebraicas del programa de Matemática de Media ha significado un retroceso en el aprendizaje de la misma en nuestro país.

Teresa Peña y Ada Pérez

Profesoras de matemáticas,

Colegio Lux Mundi

ISBN 978-9945-472-14-1