Introducción a la Matemática Discreta

Manuel Murillo Tsijli

Editorial Tecnológica de Costa Rica

4a edición

Introducción a la Matemática Discreta

Introducción a la Matemática Discreta

Manuel Murillo Tsijli

Editorial Tecnológica de Costa Rica

Primera edición.
Editorial Tecnológica de Costa Rica, 2004.

Segunda edición.
Editorial Tecnológica de Costa Rica, 2007.

Tercera edición.
Editorial Tecnológica de Costa Rica, 2009.

Cuarta edición.
Editorial Tecnológica de Costa Rica, 2010.

511.3
M977-i4
Murillo Tsijli, Manuel
Introducción a la matemática discreta / Manuel Murillo Tsijli. -- 4a. ed. -- Cartago, Costa Rica : Editorial Tecnológica de Costa Rica, 2010.
454 páginas.
ISBN 978-9977-66-224-4.
1. Matemática discreta 2. Lógica 3. Conjuntos 4. Relaciones binarias 5. Funciones

Correo electrónico: *editorial@itcr.ac.cr*
Instituto Tecnológico de Costa Rica
Apdo. 159-7050, Cartago
Tel: (506) 2550-2297 / 2550-2336 / 2550-2392
Fax: (506) 2552-5354

A Héctor y Felipe,
por quienes, en ocasiones sin saberlo,
he cruzado ríos, atravesado valles,
escalado montañas y domado volcanes.

Agradezco profundamente a los colegas y amigos
Evelyn Agüero, Manuel Alfaro,
José Luis Espinoza, Alicia León,
Félix Núñez y Geovanny Sanabria
por sus oportunos comentarios y valiosas sugerencias.
Su interés y apoyo contribuyeron a la
publicación de esta nueva edición.

Contenido

Presentación

Esta obra está dirigida principalmente a estudiantes de Matemática y de Computación. Sin embargo, también es de interés para todas aquellas personas que encuentran en las matemáticas el lenguaje universal con el que se pueden explicar los fenómenos que se presentan en nuestro entorno y, por supuesto, a todos los que ven en ella una puerta que los llevará hacia la búsqueda del conocimiento orientado al desarrollo científico y tecnológico.

Contiene los temas que habitualmente se imparten en un curso de matemática discreta de nivel universitario, como base para una formación académica sólida. Uno de sus objetivos principales es presentar los contenidos de forma rigurosa y atractiva; para ello, se han escogido diversos ejemplos donde se observan los métodos de demostración usuales en la matemática.

Se ha tratado de que los temas sean asimilados en forma paulatina. Con ese propósito se han incluido, al final de cada sección, ejercicios ilustrativos de los temas expuestos, y de la mayoría de ellos se puede encontrar la solución, parcial o completa, en el Apéndice A. Además, los conceptos o definiciones más importantes se presentan en recuadros sombreados para recalcar su importancia.

En esta nueva edición se han incluido algunos teoremas importantes con sus respectivas demostraciones; para mayor claridad, el final de ellas se indica con el símbolo $\square$.

Asimismo, se presenta una cantidad considerable de ejemplos que ayudarán al lector a comprender los conceptos que aquí se desarrollan. Dichos ejemplos son una guía para resolver los ejercicios propuestos; en la medida de lo posible debe observarse, en cada ejemplo desarrollado, el método expuesto; se ha intentado que éstos sean lo más explicativos posible. El final de cada uno se indica con el símbolo $\blacksquare$.

El procedimiento expuesto para resolver cada ejemplo o ejercicio no siempre es único. Debe intentarse y quizá encuentre uno que sea igualmente efectivo y eficiente.

Puede suceder que algunos de los contenidos de esta obra ya sean dominados por el lector; sin embargo, se quiere fortalecer aquellos que, por su importancia, se convierten en herramientas esenciales para la comprensión de los temas en cursos posteriores y para su formación académica integral y su desarrollo profesional.

En el capítulo 1 se presenta una introducción a la lógica. Se inicia con las proposiciones lógicas, se enuncian las leyes esenciales de la lógica, las reglas de inferencia, cuantificadores y sus diversas aplicaciones. Se presenta un resumen de los principales métodos de demostración que se utilizan a lo largo del texto y se presenta un interesante aporte sobre la enseñanza de la demostración de implicaciones, del profesor M.Sc. Geovanny Sanabria.

En el capítulo 2 se introduce la teoría de conjuntos. Se inicia con las operaciones básicas de conjuntos, simplificación de expresiones y su representación mediante diagramas de Venn, además de incluir una nueva sección dedicada al tema de las familias de conjuntos. En la última sección de este capítulo se profundiza sobre la demostración de proposiciones que involucran conjuntos.

En el capítulo 3 se presenta el tema de las relaciones binarias, sus operaciones básicas y algunas propiedades que permiten clasificarlas. Se profundiza en las relaciones de equivalencia y en las de orden, particiones inducidas, grafos, matriz asociada a una relación y algunas aplicaciones.

En el capítulo 4 se introduce el tema de las funciones desde un punto de vista teórico y práctico, como extensión de una relación binaria. Se profundiza en los conceptos de inyectividad y sobreyectividad, en las operaciones con funciones y las funciones inversas.

En el capítulo 5 se presenta el método de demostración conocido como el *principio de inducción matemática*. Se aplica este método para probar, principalmente, proposiciones cuantificadas que involucran igualdades, desigualdades y divisibilidad. Por último, se aborda el tema de la recursividad, sobre todo en el campo de las relaciones recurrentes y la búsqueda de su fórmula explícita, mediante el análisis hacia atrás y la ecuación característica; en esta sección se incluyen algunos ejemplos interesantes relacionados con el análisis numérico aplicado a la solución de ecuaciones.

En el capítulo 6 se hace una introducción al tema de las estructuras algebraicas, con especial interés en grupos y subgrupos.

En el capítulo 7 se hace una breve introducción al tema de los sistemas de numeración con distintos tipos de bases, además de las congruencias numéricas y su utilidad, siempre como herramientas fundamentales en la programación de computadoras. Además, se muestran algunos teoremas importantes en la teoría de números, en el contexto de las congruencias, como son los teoremas de Wilson, Fermat, Euler y otros.

En el apéndice A se aporta la solución, parcial o completa, de la mayoría de los ejercicios de cada una de las secciones.

Como aportes importantes de esta nueva edición están la inclusión de las secciones 1.7, 2.2, 2.3, 2.6, 3.2, 3.4, 3.5, 4.2, 4.3, 4.5, 4.6, 5.1, 6.3, 6.4, y de una cantidad considerable de ejemplos, ejercicios y soluciones que sin duda hará más clara la exposición de los temas aquí tratados.

Manuel Murillo

Prólogo

Matemática discreta, también conocida como matemática finita, es el estudio de las estructuras matemáticas que son fundamentalmente discretas, en el sentido de que no requieren la noción de continuidad.

Algunos de los conceptos de la matemática discreta no son nuevos, pero como disciplina matemática independiente, es relativamente nueva y ha tenido un crecimiento vertiginoso en las últimas décadas, principalmente debido a su conexión con las ciencias de la computación y su rápido desarrollo.

Los que introdujeron las nociones básicas de la matemática discreta fueron los hindúes. En el siglo VI, ellos ya conocían las fórmulas para, primero, el número de permutaciones de un conjunto con n elementos y, segundo, para el número de subconjuntos, de cardinalidad k, de un conjunto de n elementos. La matemática combinatoria tuvo sus orígenes en los trabajos de Pascal y de De Moivre durante el siglo XVII, y siguió su desarrollo con Jacob Bernoulli y Leonard Euler, principalmente con las ideas de éste último sobre la teoría de grafos. Por otro lado, los métodos probabilísticos iniciados por Paul Erdös se han convertido en una potente herramienta para la combinatoria y la teoría de probabilidad. En realidad, la matemática discreta es una disciplina que unifica diversas áreas de las matemáticas (combinatoria, probabilidad, aritmética y grafos, entre otras) y sus conceptos aparecen, con frecuencia, en muchas ramas de las matemáticas y de otras disciplinas.

La matemática discreta es el ámbito de las matemáticas que se relaciona más de cerca con las computadoras, pues en éstas la información se almacena y se manipula en forma discreta (palabras formadas por ceros y unos), se necesita contar objetos (unidades de memoria, unidades de tiempo), estudiar relaciones entre conjuntos finitos (búsquedas en bases de datos) y analizar procesos que incluyan un número finito de pasos (algoritmos). Entonces los conceptos y notaciones de la matemática discreta son útiles para estudiar y expresar objetos o problemas en algoritmos y lenguaje de programación.

Es posible encontrar aplicaciones en la teoría de la información, tratamiento digital de datos, física estadística, biología molecular, geometría discreta y computacional, criptografía, modelos discretos aplicados a la industria y ciencias de la computación. Debido a sus importantes aplicaciones, el estudio de las estructuras discretas es una de las áreas que está generando más desarrollo e interés en las matemáticas en las últimas décadas.

Para mí es un honor poder elaborar el prólogo de esta obra sobre matemática discreta, escrita por mi colega Manuel Murillo, profesor del Instituto Tecnológico de Costa Rica, y publicada por la Editorial Tecnológica de Costa Rica. En la obra, el desarrollo de los temas se presenta de forma clara, precisa, elegante y con el rigor matemático necesario.

En cada uno de los capítulos se hace una breve introducción y, además, los distintos conceptos y resultados importantes se ilustran con numerosos ejemplos resueltos que figuran intercalados entre el desarrollo teórico de cada sección en cada capítulo, finalizando la sección con una serie de ejercicios propuestos que de seguro ayudará a afianzar los conocimientos adquiridos con el estudio de la sección en cuestión.

El apéndice A contiene las demostraciones y soluciones, parciales o completas, de la mayoría de los ejercicios propuestos en cada una de las secciones, lo cual, sin duda, será de gran ayuda para los lectores en el proceso de enseñanza-aprendizaje.

Esta nueva edición conserva las fortalezas de la anterior e incorpora nuevas características y mejorías, proporcionando un equilibrio entre teoría y práctica. Incluye nuevas secciones, más ejercicios propuestos y sus soluciones, decenas de ejemplos adicionales y datos actualizados; por ejemplo, la mención del hallazgo de los primos de Mersenne número 45 y 46, en el 2008 y el número 47, en el 2009.

Las secciones incluidas son pertinentes y necesarias: inferencias que involucran proposiciones cuantificadas (sección 1.7); conjuntos numéricos (sección 2.2); diagramas de Venn (sección 2.3) como una representación figural de relaciones entre conjuntos; familias de conjuntos (sección 2.6); matriz y grafo asociado a una relación (sección 3.2); las relaciones de equivalencia (sección 3.4) para asociar elementos afines de un conjunto; las relaciones de orden (sección 3.5) para ordenar los elementos de un conjunto; conjuntos equipotentes, numerables y contables (sección 4.5); principios de conteo (sección 4.6) para introducir los conceptos fundamentales del arte de contar, como lo son las permutaciones y las combinaciones de objetos; los símbolos para sumas y productos (sección 5.1); subgrupos (sección 6.4) y la ampliación de los métodos de demostración, en la sección 1.8, con la inclusión de una propuesta del uso de demostraciones desde la lógica matemática, por ser un método que se adapta a la demostración desde la lógica intuitiva.

En el capítulo 5 (sección 5.3) se agregaron algunos ejemplos sobre el uso de la recursividad para determinar los puntos fijos de una función, lo cual representa una buena aplicación de la matemática discreta al análisis numérico.

Los ejercicios de lógica contextualizados con los habitantes de una galaxia ficticia denominada *Vacilonia* atrapan el interés de los lectores. Las referencias a los problemas abiertos, como la conjetura de Goldbach (todo número par mayor que dos es la suma de dos números primos), a conjeturas recién verificadas como la de Poincaré, a aplicaciones prácticas como la criptografía, arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas, las falacias y las paradojas son algunas de las estrategias metodológicas utilizadas por el autor.

Los contenidos principales de un curso introductorio a la matemática discreta son: fundamentos de lógica, teoría de conjuntos, relaciones binarias, funciones, principio de inducción, recursividad y estructuras algebraicas, entre otros temas que se abordan tangencialmente, como las congruencias numéricas y los métodos de demostración, que son expuestos con claridad, rigor, elegancia y de forma agradable.

Estoy seguro de que este libro, especialmente esta reciente edición, será de interés y utilidad para estudiantes de computación, matemática e ingenierías, así como para la comunidad académica en general.

Edison De Faria Campos

Presidente, periodo 2006 – 2008

Asociación de Matemática Educativa

Centro de Investigaciones Matemáticas y Meta-Matemáticas

Escuela de Matemática

Universidad de Costa Rica

Simbología

$P,\ Q,\ R, \ldots$	denotan proposiciones
$\neg P$	negación de P
$P \wedge Q$	conjunción de P y Q
$P \vee Q$	disyunción de P y Q
$P \to Q$	P implica Q
$P \leftrightarrow Q$	P si y solo si Q
$P \Rightarrow Q$	si $P \to Q$ es tautología
$P \Leftrightarrow Q$	si $P \leftrightarrow Q$ es tautología
$P \equiv Q$	P equivalente a Q
V_0	denota una tautología
F_0	denota una contradicción
$\therefore$	por lo tanto
$(\Rightarrow\Leftarrow)$	contradicción
$\exists$	cuantificador existencial (existe)
$\nexists$	no existe
$\forall$	cuantificador universal (para todo)
$A,\ B,\ C, \ldots$	denotan conjuntos
$a,\ b,\ c, \ldots$	denotan elementos
$a \in A$	a pertenece a A
$A \subseteq B$	A es subconjunto de B
$A \subset B$	A es subconjunto propio de B

$[a, b]$	intervalo cerrado
$]a, b[$	intervalo abierto
$\mathbb{N}$	$\{0, 1, 2, \ldots\}$
$\mathbb{N}^*$	$\{1, 2, \ldots\}$
$\mathbb{Z}$	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}^*$	$\mathbb{Z} - \{0\}$
$\mathbb{Q}$	conjunto de los números racionales
$\mathbb{I}$	conjunto de los números irracionales
$\mathbb{R}$	conjunto de los números reales
$\mathbb{R}^*$	$\mathbb{R} - \{0\}$
$\mathbb{R}^+$	conjunto de los números reales positivos
$A - B$	diferencia de conjuntos
$A \cup B$	unión de conjuntos
$A \cap B$	intersección de conjuntos
$A \triangle B$	diferencia simétrica de conjuntos
$\lvert A \rvert$	cardinalidad de A
$\varnothing$ o $\{\ \}$	conjunto vacío
$\mathcal{U}$	conjunto universo
$A \approx B$	conjuntos equipotentes
$a \approx b$	aproximación de números
$A \preceq B$	A de menor potencia que B
$A \times B$	conjunto producto de A y B
(a, b), (a, b, c)	par ordenado y triplete ordenado
$P(A)$ o 2^A	conjunto potencia de A
$\overline{A}$ o $\complement_A^{\mathcal{U}}$	complemento de A
$\mathcal{R}$, $\mathcal{S}$, $\mathcal{T}, \ldots$	denotan relaciones
$a\mathcal{R}b$	a se relaciona con b
$\dot{a}$ o $\overline{a}$ o $[a]$	clase de equivalencia de a
$A/\mathcal{R}$	conjunto cociente
$D_{\mathcal{R}}$	dominio de $\mathcal{R}$

$\mathcal{R}[A]$	rango de $\mathcal{R}$
$G_{\mathcal{R}}$	gráfico de $\mathcal{R}$
$\mathcal{S} \circ \mathcal{R}$	composición de $\mathcal{R}$ y $\mathcal{S}$
$f,\ g,\ h, \ldots$	denotan funciones
$f \circ g$	composición de f y g
$\lvert x \rvert$	valor absoluto de x
$\lceil x \rceil$	función techo
$\lfloor x \rfloor$	función piso o parte entera
$\chi_A(x)$	función característica de A
$f(E)$	imagen del conjunto E
$f^{-1}(F)$	imagen inversa del conjunto F
$f^{-1}(x)$	función inversa de f
$\mathcal{O}(s)$	órbita de s
$n!$	factorial de n
$(\mathcal{G}, *)$	grupo
$*,\ \perp,\ \otimes,\ \oplus, \ldots$	denotan operaciones binarias
$\mathcal{H} < \mathcal{G}$	$\mathcal{H}$ subgrupo de $\mathcal{G}$
S_n	grupo simétrico
$o(\mathcal{G})$	orden del grupo $\mathcal{G}$
$\varphi(n)$	función de Euler
$\equiv$	equivalencia o congruencia
$E_p(m)$	exponente de p en factorización prima de m
N_f	núcleo del homomorfismo f
$\mathbb{Z}_n$	partición de $\mathbb{Z}$ módulo n
$\mathbb{N}_n$	$\{1, 2, 3, \ldots, n\}$
$P(n, r)$	permutaciones
$C(n, r)$	combinaciones
B^A	funciones de A en B
$\mathcal{I}(A, B)$	funciones inyectivas de A en B
$\mathcal{B}(A, B)$	funciones biyectivas de A en B

∞	infinito
$\aleph_0$	aleph cero
$\sum$	suma
$\prod$	producto
$a\|b$	a divide a b
m.c.d.(a, b)	máximo común divisor de a y b
sii	si y solo si
hqd	hay que demostrar que

Capítulo 1

Fundamentos de lógica

"TWEEDLEDEE (A ALICIA): *Sé lo que estás pensando, pero no es así de todas formas.*
TWEEDLEDUM: *Al contrario, si fue así, podría ser; y si fuera así, sería; pero como no es, no es. La lógica es así*".

Lewis Carroll

En este capítulo se hace una formalización de la lógica, aquella que se utiliza todos los días para razonar, debatir, deducir, comprender e inferir. Cuando se dice, por ejemplo: "solo las personas mayores de 18 *años pueden votar" y "Héctor tiene* 17 *años", se concluye lógicamente que "Héctor no puede votar"; o cuando se dice que la expresión "el hielo es caliente" es falsa, sin duda se emite un juicio de valor o conclusión a partir del conocimiento adquirido con anterioridad o a partir de las diferentes premisas.*

Se inicia con la terminología propia de toda teoría matemática, luego con la particular de la lógica formal y simbólica: conectivas, cuantificadores, proposiciones, entre otros términos, y se clasifican estas proposiciones con base en las tablas de verdad. Luego se ven las leyes de la lógica y las reglas de inferencia, con su respectiva aplicación. Al final se definen los cuantificadores y se trabaja con proposiciones cuantificadas.

Para profundizar el tema tratado en este capítulo, es recomendable consultar las referencias bibliográficas [2], [5], [7], [12], [15], [31] *y para el tema de las paradojas, el interesante artículo* [30].

1.1 Introducción

Para algunos, la *lógica* es la teoría del pensar, la ciencia de los límites del pensar justo y razonado; para otros, se puede definir brevemente como el estudio del razonamiento. En este caso, la lógica es la teoría de la inferencia, véase [5]. Su estudio es importante porque ayuda a razonar de forma correcta y, con ello, a no incurrir en las llamadas falacias argumentativas. Las leyes de la deducción son innatas en los seres humanos, pero su uso no es obligado y pueden ser ignoradas, incluso, como es el caso de algunas normas morales, sin darse cuenta de ello. Conocer estas leyes con mayor profundidad permite su aplicación.

Algunos de los argumentos lógicos más originales corresponden al matemático y Reverendo Charles Lutwidge Dodgson (1832-1898), conocido por su seudónimo Lewis Carroll, quien además fue lógico, dibujante, fotógrafo y poeta. Catedrático de la Universidad de Cambridge, en Inglaterra, y autor prolífico, dentro de sus obras destacan *Lógica Simbólica*, *Alicia en el País de las Maravillas* y *Silvia y Bruno*. Él mismo explica en su bella obra *Lógica Simbólica* las razones del por qué es importante el estudio de este tema:

> *"La lógica simbólica dará a usted claridad de pensamiento, la habilidad para ver su camino a través de un acertijo, el hábito de arreglar sus ideas en una forma adecuada y clara, y, lo más valioso, el poder para detectar falacias y separar las piezas de los argumentos endebles e ilógicos que encontramos continuamente en libros, periódicos, discursos, y aún sermones, y que fácilmente engañan a aquellos que nunca se han tomado la molestia de dominar este fascinante arte".* (Véase [24]).

El concepto de lógica tiene sus orígenes en los estoicos, probablemente en Zenón de Elea (490-430 a.C.), discípulo de Parménides, aunque la primera lógica sistemática se debe a Aristóteles de Estagira (384-322 a.C.), quien, en uno de los escritos referentes a este tema, se ocupa de las teorías del concepto del *juicio*, de la *conclusión* y de la *prueba*, y es a partir de él que queda constituida como una disciplina propia.

La llamada *lógica inductiva* se caracteriza por el razonamiento de que, a partir de observaciones específicas, se conduce a conclusiones generales y por supuesto que con ella es posible obtener una idea correcta de lo que podría ser una buena conclusión, pero no se puede pensar que algo es verdadero solamente porque ha sido verdadero en cierto número de casos. Otro tipo de razonamiento es el método deductivo, que consiste en relacionar conocimientos que se suponen verdaderos de manera que se obtienen nuevos resultados. En este caso, se hará una separación de la lógica clásica y se utilizarán símbolos matemáticos, por lo que se hablará de la *lógica simbólica*.

En toda *teoría matemática* se requiere de una terminología propia o lenguaje asociado con la notación respectiva; a continuación se analizan los distintos elementos de esta terminología.

Para iniciar, las **definiciones** describen y caracterizan los **objetos matemáticos** por tratar, a los cuales se refieren las proposiciones: número, número primo o divisibilidad en la Teoría de los Números; punto, recta, plano o ángulo en Geometría; intervalos o conjunto compacto en el Análisis; vector o matriz en Álgebra, entre muchos otros. En diferentes teorías existen objetos matemáticos que no se pueden definir, estos reciben el nombre de términos primitivos.

El **axioma** es una proposición cuya validez se acepta sin demostración. Los axiomas son los fundamentos de todo desarrollo teórico, son la base sobre la cual se construye una teoría; por ejemplo, son conocidos los axiomas de Peano, el axioma de especificación, el axioma de elección, el axioma del extremo superior y los cinco postulados de Euclides, entre otros. En matemática se procura tener la menor cantidad posible de axiomas; usualmente se encuentran en las teorías fundamentales, como es el caso de la teoría de conjuntos. Sin embargo, muchas veces se hacen desarrollos axiomáticos de teorías que pueden prescindir de axiomas y construirse sobre otras teorías, para simplificar su presentación.

Como ejemplo considere el de la Geometría Euclideana, expuesta y desarrollada por Euclides en su monumental y trascendental obra *Los Elementos* (para más detalles, véase [31], [35] y [36]). Esta obra se fundamenta en 23 definiciones, y solo para ilustrar algunas a modo de ejemplo, el *punto* lo define como "*es lo que no tiene partes*", y una *recta* como "*es una longitud sin anchura*"; él mismo enuncia y propone cinco postulados:

P-1. Se puede trazar una recta desde un punto a otro cualquiera.

P-2. Se puede extender un segmento continuamente a una recta.

P-3. Se puede describir un círculo con cualquier centro y radio.

P-4. Que todos los ángulos rectos son iguales.

P-5. Que si una línea recta corta a otras dos rectas formando con ellas ángulos interiores del mismo lado menores que dos ángulos rectos, las dos líneas rectas, prolongadas indefinidamente, se cortan del lado por el cual los ángulos son menores que dos ángulos rectos.

En algunos textos se ha reemplazado el enunciado del quinto postulado por el equivalente *Axioma de Playfair*, cuyo enunciado es: *por un punto que no pertenece a una recta, existe una única recta paralela a la primera que contiene al punto.* Por otro lado, Euclides utiliza lo que denomina *nociones comunes* y enuncia cinco, estas últimas llamadas por Proclus, axiomas. Él sigue a Aristóteles: mientras que las nociones comunes se aplican a todas las ciencias, los **postulados** se aplican solo a la geometría. Como ejemplo, se mencionan solo dos nociones comunes:

1. El todo es mayor que cualquiera de sus partes.

2. Dos cantidades iguales a una tercera, son iguales entre sí.

Al negar el quinto postulado (P-5), se obtienen dos nuevas geometrías, llamadas *geometrías no euclideanas.* La negación de la afirmación de que existe una recta paralela se puede dar por medio de la tricotomía clásica, hay menos de una (ninguna) o hay más de una (varias). Así, manteniendo los cuatro primeros postulados, pero reemplazando el quinto en el caso de que no existan las rectas paralelas, se obtiene la *geometría esférica* (de Riemann); en el otro caso, se obtiene la *geometría hiperbólica* (de Bolyai y Lobachevski), en donde por un punto que no esté en una recta pasan varias paralelas (consulte [31] y [35]). En estas geometrías, curiosamente, el teorema que afirma que la suma de los ángulos internos de un triángulo es 180 grados resulta no ser cierto. Los resultados que se obtienen serán distintos, pues las premisas lo son.

El **teorema** es una proposición cuya validez se verifica como consecuencia lógica de los axiomas; se debe probar a partir de los axiomas y definiciones o de otros teoremas ya probados.

A los teoremas que no son relevantes en el desarrollo de una teoría, se acostumbra denominarlos simplemente **proposiciones**.

El **corolario** es un teorema que se deduce fácilmente de un teorema anterior o es un caso particular de un teorema general.

El **lema** es un teorema necesario para la demostración de un resultado posterior, pero que se sale del contexto de la teoría que se está desarrollando. Es decir, los lemas no son resultados centrales en el desarrollo de una teoría matemática; sin embargo, un lema en una teoría puede ser un teorema central en otra teoría.

El **escolio** es un resultado que se obtiene en el desarrollo de una demostración y que no tiene relación con la teoría que se está estudiando.

Una **conjetura** es una proposición de la que no se puede asegurar su validez; ejemplo interesante es la conocida conjetura de Goldbach, propuesta por Christian Goldbach a Leonhard Euler en 1742, en donde se afirma que todo número entero, par, mayor o igual que 4 se puede escribir como la suma de dos números primos. Hasta el día de hoy no se ha podido demostrar su validez, pero tampoco se ha encontrado un número par que no sea la suma de dos primos; solamente se ha podido comprobar para una gran cantidad de números, por ejemplo, observe que $4 = 2 + 2, \quad 10 = 7 + 3, \quad 50 = 43 + 7, \quad 100 = 89 + 11.$

Otra conjetura (véase [22]), pues todavía no se ha refutado ni demostrado su validez, es que hay un número infinito de números primos de Mersenne. La definición de estos números es sencilla: los *números de Mersenne* son de la forma $M_p = 2^p - 1$ para p primo, en caso de que M_p sea primo, se le llama primo de Mersenne. Curiosamente, sólo se han encontrado 47 de estos primos; el mayor de ellos es $M_{43112609} = 2^{43112609} - 1$, que además corresponde al mayor primo conocido y es el número 45 de esa lista, consta de 12 978 189 dígitos y fue descubierto en agosto del 2008 por Edson Smith, de la UCLA, en Estados Unidos.

En septiembre del 2008, Hans-Michael Elvenich, en Langenfeld, Alemania, encontró el primo de Mersenne número 46 dado por $M_{37156667} = 2^{37156667} - 1$, de 11 185 272 dígitos, que curiosamente, es menor que el anterior. Odd Magnar Strindmo, en Noruega, descubrió a $2^{42643801} - 1$ en abril del 2009, el primo número 47, que cuenta con 12 837 064 dígitos. Para mayores detalles, consulte [22] o [26].

Al igual que las dos anteriores, de Goldbach y de Mersenne, existen muchas otras conjeturas planteadas (véase [26]), unas de ellas seguirán esperando, a otras se les prueba su falsedad mientras que a otras su validez, como es el caso de von Lindemann quien probó, en 1882, que el número π es trascendente, o el caso más reciente de la conjetura de Poincaré, propuesta en 1904 y considerada uno de los problemas abiertos más importantes y difíciles en matemáticas, que ha sido demostrada afirmativamente por el matemático ruso Grigori Perelman.

Una **paradoja** es una proposición contradictoria en sí misma: no puede ser falsa ni verdadera. La palabra paradoja proviene del griego $\pi\alpha\rho\alpha$ (para), que significa *contra*, y $\delta o\xi\alpha$ (doxa), que significa *opinión*. Para profundizar sobre este tema, consulte [30].

Ejemplo 1. *La frase* "estoy mintiendo" *es una paradoja en sí misma, pues, si es verdadera, estoy mintiendo y por lo tanto es falsa; por otro lado, si es falsa, no estoy mintiendo y por lo tanto es verdadera. Es decir, la proposición no puede ser verdadera ni falsa, pues en cualquier caso se obtiene una contradicción.* ■

La paradoja anterior radica en la estructura misma del lenguaje, por lo que se dice que es una **paradoja semántica**; por otro lado, si la paradoja es debida a la escogencia de los axiomas, se dice que es una **paradoja lógica**.

Es importante señalar que los griegos fueron los primeros en plantear distintos tipos de paradojas, muchas de ellas relacionadas con la teoría de números. Fue precisamente Zenón de Elea quien formuló en el siglo V a.C. cuatro paradojas: la de la *Dicotomía*, la de *Aquiles*, la de la *Flecha* y la del *Estadio*, que en la actualidad son referente obligatorio en el estudio de este tema.

Ejemplo 2. *La idea de la paradoja de la Dicotomía (véase [31]) es la siguiente: un corredor debe recorrer una distancia d. Para lograrlo debe recorrer la mitad de esa distancia $\frac{d}{2}$ y también la mitad de esa mitad, que es $\frac{d}{4}$; luego la siguiente distancia $\frac{d}{8}$, $\frac{d}{16}$ y así se sigue. La conclusión es que el corredor debe recorrer un número infinito de distancias y el problema es que lo tiene que hacer en un tiempo finito. Por lo tanto, nunca podrá recorrer esa distancia; entonces, no hay movimiento. El problema es el concepto de infinito, en particular, realizar una división de manera infinita. En estos tiempos, todo se reduce a calcular la suma de la serie infinita:*

$$\frac{d}{2}+\frac{d}{4}+\frac{d}{8}+\frac{d}{16}+\cdots = d\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots\right) = d\cdot 1 = d$$

o, con un argumento geométrico, se puede pensar que $\frac{1}{2}$ representa la mitad de un cuadrado de lado 1, $\frac{1}{4}$ la cuarta parte, $\frac{1}{8}$ la octava parte y así sucesivamente, de forma que $\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots$ es igual al área de todo el cuadrado que se sabe es 1. ■

A modo de ejemplo, se presenta además, la *Paradoja de Protágoras* (480 − 410 a.C.), una de las más antiguas conocidas y que surge de la argumentación entre el sofista y maestro de leyes llamado Protágoras y su estudiante Eualzo (véase [30]).

Ejemplo 3. *Protágoras aceptó como estudiante a Eualzo, quien, aunque pobre, era talentoso. Protágoras convino con él en impartirle enseñanza sin cobrarle, a condición de que una vez que el estudiante hubiese completado sus estudios y ganara el primer litigio en ejercicio de su profesión, le pagaría a Protágoras el costo de los estudios. El estudiante aceptó esta condición. Tras completar sus estudios, Eualzo no emprendió ningún caso legal. Transcurrido cierto tiempo, Protágoras buscó al estudiante y reclamó el pago o lo llevaría a los tribunales. He aquí los argumentos que alegaron uno y otro:*

– EUALZO*: Estimado maestro Protágoras, ¡no pagaré!, ya que en los tribunales solo pueden suceder dos cosas: gano o pierdo. Si gano, la ley no me obliga a pagarte. Si pierdo, entonces no se habrá cumplido que yo haya ganado mi primer litigio. Por lo tanto, y de acuerdo con nuestro convenio, no deberé pagarte.*

– PROTÁGORAS*: Estimado ex-discípulo Eualzo,... ¡pagarás!, ya que si vamos a los tribunales, podrán suceder solamente dos cosas: gano yo o ganas tú. Si gano yo, entonces la ley te obliga a pagarme. Si ganas tú, habrás ganado tu primer litigio. Por lo tanto, y de acuerdo con nuestro convenio, tendrás que pagarme.*

Parece que Protágoras y Eualzo tienen razón, o más bien, parece que ninguno tiene la razón. ■

Como dato curioso, Kurt Gödel planteó en 1931 que hay proposiciones que son *indecidibles*, ya que es imposible demostrar su validez o refutarla a partir de los axiomas. Aún más, en 1963, Paul Cohen demostró que la existencia de un número mayor que $\aleph_0$ (la cardinalidad del conjunto $\mathbb{N}$) y menor que $\boldsymbol{c}$ (la cantidad de elementos de $\mathbb{R}$) era indecidible con base en los axiomas de la teoría de conjuntos. Incluso se pensó, en algún momento, que la conjetura de Fermat era indecidible; sin embargo, ya fue demostrada por el británico Andrew Wiles en 1995 en definitiva (porque había sido anunciada por él mismo el 23 de junio de 1993 y todavía contenía algunos errores).

Una **demostración** de una proposición es un ensayo estructurado en donde se verifica y constata de forma irrefutable y convincente que dicha proposición es verdadera. Las palabras **demostración** y **prueba** son sinónimos, el término **verificar** se utiliza a veces en lugar de **probar**, sobre todo cuando la demostración es esencialmente un cálculo.

Para finalizar esta sección, es interesante la comparación que hace Mariano Perero en [28]:

> *"La matemática, como un sistema puramente formal, se puede comparar con el ajedrez, los elementos primitivos en ajedrez son las* 32 *piezas y el tablero; los axiomas son las descripciones de los movimientos de las piezas, no son evidentes, no son ni verdaderos ni falsos, son así y se aceptan sin discutir, las reglas del juego constituyen la lógica del sistema. Nadie se pregunta si el ajedrez es verdadero o falso, lo único importante es saber si se siguen las reglas".*

Ejercicios (sección 1.1)

Los siguientes ejercicios pueden ser resueltos utilizando su destreza mental, ordene bien sus ideas y, en algunos, analice o deseche casos.

1. Había un hombre viendo un retrato y alguien le preguntó: ¿Quién aparece en el retrato? Él contesto: *"yo no tengo hermanos ni hermanas, pero el padre de este hombre es el hijo de mi padre."* ¿Qué retrato está viendo? Si el hombre hubiera respondido *"yo no tengo hermanos ni hermanas, pero el hijo de este hombre es el hijo de mi padre."* ¿Qué retrato está viendo?

2. La oración "*En hesta orasión hay tres errores*" tiene tres errores, ¿cuáles son?

3. Al visitar una tienda, es posible hallar preciosos muebles, el más antiguo de 1825. Deduzca cuándo y dónde fue tallado cada uno y el tipo de madera, si se cuenta con los siguientes datos: la silla es un cuarto de siglo más antigua que la cama (que no es francesa); el mueble de cedro, el más antiguo, tiene un cuarto de siglo más que el de fresno; la mesa es austriaca y el mueble de roble, suizo (pero no de 1850).

4. A tres prisioneros que se hallaban en cierta cárcel, los tres por lo menos de inteligencia media, el carcelero les dijo que de un conjunto de tres sombreros blancos y dos rojos, elegiría tres de ellos y los colocaría sobre sus cabezas. Se prohibía a cada uno de ellos que viera el color del sombrero que tenía sobre su propia cabeza. Además, estaban colocados en fila, uno detrás del otro, de manera que el primero no veía ningún sombrero, el segundo veía solo el sombrero del primero y el tercero veía los sombreros de los otros dos. El carcelero ofreció la libertad al tercero, si podía decir de qué color era el sombrero que tenía sobre su propia cabeza. Éste dijo que no podría. Luego, el carcelero ofreció la libertad al segundo, a condición de que dijera cuál era el color del sombrero que tenía sobre su propia cabeza. Éste confesó que no podría decirlo. El carcelero no se molestó en hacer el ofrecimiento al primero, pero a pedido de éste, le concedió la misma oportunidad. El primer prisionero esbozó una amplia sonrisa y dijo: *No necesito ver el sombrero de ninguno de mis compañeros, pues, por lo que ellos han dicho, deduzco claramente que mi sombrero es. . . .*

5. En una fiesta hay 10 niños, se les pide que formen 5 filas de manera que se tengan 4 niños por fila y que todos ellos estén en alguna fila. ¿De qué forma deben distribuirse?

6. ¿Cómo se pueden formar 4 triángulos iguales (equiláteros) con 6 palitos del mismo tamaño (sin cortarlos)?

7. Considere nueve puntos distribuidos de la siguiente manera

Con un trazo que contenga solamente cuatro segmentos de recta y sin levantar el lápiz, una todos los puntos.

8. Un niño y una niña están sentados en los escalones afuera de su escuela. “Yo soy un niño”, dijo quien tiene el pelo negro. “Yo soy una niña”, dijo quien tiene el pelo rojo. Si al menos uno de ellos está mintiendo, ¿quién tiene el pelo rojo?

9. Manuel fue a consultar a su biblioteca tres tomos de una colección de cuentos, colocados de la manera usual, el primer tomo a la izquierda; el segundo, al centro; el tercero, a la derecha. Cada tomo tenía 100 hojas y cuando los abrió se dio cuenta de que una polilla había atravesado desde la primera hoja del primer tomo hasta la última hoja del tercero. ¿Cuántas hojas atravesó la polilla?

10. Determine el número que hace falta en cada una de las siguientes series o arreglos de números.

    (a) $7 - 8 - X - 13 - 17$

    (b) $3 - X - 31 - 95 - 283 - 851$

    (c) $17 - 19 - 22 - 16 - X - 13 - 32$

    (d) $2 - 5 - 15 - 18 - 54 - 57 - 171 - X$

    (e) $60 - 30 - 28 - X - 12 - 6 - 4$

    (f)

1	2	3	4	5	6	7	8
2	3	6	9	36	41	246	X

11. Determine el sexto término de la siguiente serie

12. Si se asume que el 70% de los hombres son inteligentes, el 70% guapos y el 70% buenos. Como mínimo, en un grupo de 100 hombres, ¿cuántos de ellos serán a la vez inteligentes, guapos y buenos?

13. Juan necesita recoger 5 litros de agua de una laguna, pero solo dispone de dos jarras, una de 7 litros y otra de 4 litros. Describa el proceder de Juan para lograr su cometido.

14. Existe un pequeño planeta de una lejana galaxia llamado *Vacilonia*, sus habitantes, los vacilonios, están clasificados en dos categorías: los *sinceros* y los *mentirosos*[1]. Los sinceros siempre dicen la verdad y los mentirosos siempre mienten. Un terrícola llega a este planeta y se encuentra con dos vacilonios, A y B. El vacilonio A dice: "B es sincero o yo soy mentiroso". ¿Qué son A y B?

15. Suponga que el vacilonio A dice: "yo soy un mentiroso o, en caso contrario, uno más uno es igual a tres" ¿Qué se puede concluir?

16. Alguien le pregunta al vacilonio A "¿es usted sincero?" y él responde: "si yo soy sincero, entonces me comeré mi sombrero". Concluya que A debe comerse el sombrero.

17. Es conocido que a los vacilonios les gusta la pimienta. Hubo un robo de esta especia y los tres sospechosos fueron A, B y C. En el juicio A dijo que B era inocente y B dijo que C era culpable. Se sabe que solo hay un culpable y que ningún inocente mintió y ningún culpable dijo la verdad, pues como es sabido, los que roban pimienta nunca dicen la verdad. ¿Quién se robó la pimienta?

18. Tres vacilonios han llegado a la Tierra. Se le pregunta al primero si es un mentiroso. Éste responde a la pregunta. El segundo dice entonces que el primero negó ser un mentiroso. Finalmente, el

[1]Algunos de estos acertijos se deben al gran matemático, lógico, filósofo, ajedrecista y mago profesional Raymond Smullyan (consulte [33]).

tercero afirma que el primero es realmente un mentiroso. ¿Cuántos de los vacilonios eran mentirosos? ¿Qué era el segundo vacilonio?

19. Nos encontramos a tres vacilonios A, B y C que han llegado a la Tierra. Un terrícola le pregunta a A "¿eres sincero o mentiroso?"; responde A, pero el terrícola no pudo escucharlo y por eso le pregunta a B "¿qué ha dicho A?" y B le responde "A ha dicho que es un mentiroso". Pero al mismo tiempo C dice "no le crea a B, está mintiendo". ¿Qué son B y C?

20. De nuevo nos encontramos a tres vacilonios A, B y C. Pero esta vez el terrícola le pregunta a A "¿cuántos sinceros hay entre ustedes?"; de nuevo responde A, pero el terrícola no pudo escucharlo y por eso le pregunta a B "¿qué ha dicho A?" y B le responde "A ha dicho que hay un sincero entre nosotros". Pero al mismo tiempo C dice "no le crea a B, está mintiendo". ¿Qué son B y C?

21. En esta oportunidad, usted se encuentra en Vacilonia. Se sabe que en Vacilonia hay hombres y mujeres y que cada uno puede ser sincero o mentiroso. Usted va a un baile de máscaras y se encuentra con un par de vacilonios, A y B. Usted no puede determinar el sexo ni la categoría de cada uno de ellos; sin embargo, A afirma: "ambos somos mentirosos(as)" y B afirma: "ambos somos mujeres". ¿Qué son A y B?

22. A y B, aburridos de ser sinceros, decidieron cambiar por una semana. Ahora, A sería sincero solamente los lunes, martes y miércoles, y mentiroso el resto de la semana; B sería sincero solamente los jueves, viernes y sábado, mentiroso los otros días. Se encuentran un día de esa semana y A dice: "ayer no dije la verdad". B le responde: "ayer yo también mentí". ¿Qué día se encontraron los vacilonios A y B?

23. Manuel afirma que "*Solo hay tres clases de personas, los que saben contar y los que no*", ¿qué se puede concluir?

24. Se tienen cuatro mujeres: Alicia, Bárbara, Carolina y Diana. Sus ocupaciones son: abogada, bióloga, costurera y dentista. Cada una de ellas tiene un automóvil cuyas marcas son: Toyota, Fiat, Mercedes y Subarú. No se sabe quién es quién ni cuál automóvil tiene, pero se cuenta con la siguiente información: la abogada derrotó a Bárbara jugando al tenis. Carolina y la costurera van a nadar con las mujeres que tienen automóviles Mercedes y Subarú. Alicia y la dentista visitaron a la mujer del Subarú, quien no es la bióloga, pues esta última tiene un Toyota. Deduzca la ocupación y la marca del vehículo de cada mujer.

25. Encuentre el dígito asociado con cada letra utilizada en la suma

$$\begin{array}{ccccc} & \mathrm{T} & \mathrm{R} & \mathrm{E} & \mathrm{S} \\ & \mathrm{T} & \mathrm{R} & \mathrm{E} & \mathrm{S} \\ + & \mathrm{T} & \mathrm{R} & \mathrm{E} & \mathrm{S} \\ \hline \mathrm{N} & \mathrm{U} & \mathrm{E} & \mathrm{V} & \mathrm{E} \end{array}$$

de manera que esta suma sea aritméticamente correcta y a letras distintas les correspondan dígitos distintos. Como es natural en el sistema decimal, los posibles dígitos son 0, 1, 2,. . . , 8, 9.

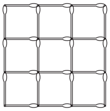
26. Análogo al ejercicio anterior, con $\begin{array}{ccccc} & \mathrm{S} & \mathrm{E} & \mathrm{N} & \mathrm{D} \\ + & \mathrm{M} & \mathrm{O} & \mathrm{R} & \mathrm{E} \\ \hline \mathrm{M} & \mathrm{O} & \mathrm{N} & \mathrm{E} & \mathrm{Y} \end{array}$

27. Un crimen es cometido por una persona y hay 4 sospechosos: Juan, Andrés, Pedro y Rafael. Al ser interrogados, cada uno declara:
    Andrés: "*Pedro es culpable*".
    Rafael: "*yo no soy culpable*".
    Pedro: "*Juan es culpable*".
    Juan: "*Pedro miente cuando dice que yo soy culpable*".
    Si se sabe que solo uno dice la verdad, ¿quién es el culpable?

28. Suponga que se tienen cuatro interruptores y solo uno de ellos enciende un bombillo que se encuentra en una habitación cerrada. Usted puede entrar a la habitación una única vez, pero puede

conectar o desconectar los interruptores las veces que quiera antes de ingresar al cuarto. ¿Podría usted encontrar la manera de deducir cuál de los cuatro interruptores enciende el bombillo?

29. La figura siguiente está formada con 24 fósforos, elimine 4 de ellos para que queden solamente 5 cuadrados.



30. Un rey ordenó a su orfebre confeccionar 800 monedas de oro de 10 gramos cada una, todas del mismo tamaño. Éste se las entregó distribuidas en 8 sacos de 100 monedas cada una. Uno de sus fieles le confirmó que todas las monedas de uno de los sacos pesaban solamente 9 gramos, pues el orfebre mezcló parte del oro con otro metal. Al enterarse de ello, el rey colocó una báscula y ofreció como recompensa uno de los sacos al que lograra descubrir cuál era el saco con las monedas adulteradas utilizando la menor cantidad de veces la báscula. Determine cuál es la menor cantidad posible de veces que se puede utilizar la báscula para descubrir el saco de las monedas falsas.

31. Este ejercicio de lógica fue tomado del libro *Harry Potter y la piedra filosofal* de la autora inglesa J. K. Rowling. Inicia cuando Hermione y Harry, en busca de la piedra filosofal, se encuentran frente a una mesa que contiene siete botellas de diferente tamaño puestas en fila, en donde la botella más pequeña está al centro.

   –¡Mira!– Hermione cogió un rollo de papel que estaba cerca de las botellas. Harry miró por encima de sus hombros para leerlo:

   El peligro yace ante ti, mientras la seguridad está detrás, dos queremos ayudarte, cualquiera que encuentres, una entre nosotras siete te dejará adelantarte, otra llevará al que lo beba para atrás, dos *contienen sólo vino de ortiga, tres son mortales, esperando escondidas en la fila. Elige, a menos que quieras quedarte para siempre; para ayudarte en tu elección, te damos cuatro claves:*

1. *Por más astucia que tenga el veneno para ocultarse siempre encontrarás alguno al lado izquierdo del vino de ortiga y no hay dos venenos consecutivos.*
2. *Son diferentes las que están en los extremos, pero si quieres moverte hacia adelante, ninguna es tu amiga.*
3. *Como claramente ves, todas tenemos tamaños diferentes: ni el enano ni el gigante guardan la muerte en su interior.*
4. *La segunda a la izquierda y la segunda a la derecha son gemelas una vez que las pruebes, aunque a primera vista sean diferentes.*

Hermione dejó escapar un gran suspiro y Harry, sorprendido, vio que sonreía, lo último que había esperado que hiciera.
−Muy bueno−dijo Hermione−. Esto no es magia... es lógica... es un acertijo. Muchos de los más grandes magos no han tenido una gota de lógica y se quedarían aquí para siempre...

Puede usted descifrar este acertijo y concluir cuál botella los hará volver y cuál les permitirá seguir adelante.

32. Dos amigos matemáticos hablan de sus familias. Uno le pregunta al otro que si tiene hijos y qué edades tienen, la respuesta simple se disfraza de acertijo y el diálogo entre la conversación fue:

    – El producto de las edades de mis tres hijos es, actualmente, 36 y la suma es justamente el número de la casa en que tú vives. ¿Aciertas las edades de ellos?
    – A decir verdad, todavía no puedo, pues me falta un dato− le responde luego de algunos minutos.
    – Tienes razón, le contestó. ¡El mayor toca piano!

    Con esta información, puede usted deducir las edades de los hijos.

33. Tengo el doble de la edad que tú tenías cuando yo tenía la edad que tú tienes, y cuando tengas la edad que tengo, nuestras edades sumarán 63. ¿Qué edad tengo?

34. Discuta y analice las siguientes paradojas:

    (a) *Paradoja de Epiménides*, el cretense, quien afirmó que todos los cretenses son mentirosos.

    (b) *Paradoja de Protágoras.* Véase ejemplo 3, página 34.

    (c) *Paradoja del barbero*, propuesta por B. Russell, que dice: El único barbero de la ciudad dice que afeitará a todos aquellos que no se afeiten a sí mismos. ¿quién afeitará al barbero?

    (d) *Paradoja de Aquiles.* Según este argumento, el más rápido de los hombres, Aquiles, no podrá alcanzar nunca al más lento de los animales, la tortuga, si se da a ésta una ventaja inicial en una carrera. Pues, mientras Aquiles recorre el camino que la tortuga llevaba por la ventaja inicial, ésta habrá recorrido otra porción, aunque más pequeña. Cuando Aquiles haya llegado a recorrer esta última porción de camino, la tortuga habrá avanzado otra porción más pequeña y así la tortuga siempre llevará la ventaja hasta en espacios infinitamente pequeños, con lo cual Aquiles nunca podrá alcanzarla.

    (e) Cervantes, en el capítulo LI de El Quijote, escribió: "*Si alguno pasare por este puente de una parte a otra, ha de jurar primero a dónde va y a qué va; y si jurare la verdad, déjenle pasar, y si dijere mentira, muera por ello ahorcado en la horca que allí se muestra, sin remisión alguna". Sabida esta ley y la rigurosa condición de ella, pasaban muchos, que luego en lo que juraban se echaba de ver que decían la verdad y los jueces los dejaban pasar libremente. Sucedió, pues, que tomando juramento a un hombre, juró y dijo que para el juramento que hacía, iba a morir en aquella horca que allí estaba y no a otra cosa.* ¿Este hombre dice verdad o mentira?

1.2 Conectivas lógicas

El lenguaje de la lógica formal está estructurado de manera que no admite paradojas semánticas. Las teorías matemáticas formulan sus axiomas de tal forma que no conducen a ninguna paradoja. En este sentido, para esta formalización son necesarias algunas definiciones y principios que permitan levantar esta teoría matemática, sin caer en paradojas análogas a las que se mencionaron anteriormente.

Se dice que una **proposición** (enunciado o cláusula) es una combinación de símbolos del lenguaje, cuya característica fundamental es que se le puede asignar un **valor de verdad**: verdadero o falso, **V** o **F** respectivamente.

Toda proposición debe cumplir con los principios:

1. **De identidad**: si una proposición es verdadera, entonces es siempre verdadera.
2. **De no-contradicción**: ninguna proposición puede ser falsa y verdadera a la vez.
3. **Del tercero excluido**: una proposición es falsa o es verdadera.

Estos tres principios establecen que toda proposición debe tener un y solo un valor de verdad. A partir de las proposiciones *simples* o llamadas *atómicas*, se obtienen las proposiciones *compuestas* o *moleculares*, mediante la aplicación de las *conectivas lógicas*: negación, conjunción, disyunción, disyunción exclusiva, implicación y equivalencia.

Seguidamente, para describir el comportamiento de estas conectivas, se utilizará la **tabla de verdad**, en donde se indica el valor de verdad de la proposición compuesta, para todos los posibles valores de verdad de las proposiciones atómicas que la componen. Ponga especial atención en el lenguaje que se utiliza y las diferentes maneras de referirse a ellas.

Si P es una proposición, la **negación** de P es la nueva proposición $\boldsymbol{\neg P}$, que se lee "no es cierto que P" o "no P"

P	$\neg P$
V	F
F	V

Ejemplo 4. *Si se considera la proposición verdadera $P : 3 > 2$, la negación es $\neg P : 3 \leq 2$, cuyo valor de verdad es F.* ■

Ejemplo 5. *Si P es la proposición "$2 + 1 = 5$", la proposición $\neg P$ es "no es cierto que $2 + 1 = 5$" o simplemente "$2 + 1 \neq 5$". Claramente, el valor de verdad de P es falso y el de $\neg P$ es verdadero.* ■

Si P y Q son dos proposiciones, la conectiva binaria **conjunción** de P y Q es la nueva proposición $\boldsymbol{P \wedge Q}$, que se lee "P y Q". Su valor de verdad está dado por la tabla

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo 6. *Si se consideran las dos proposiciones $P : 3 > 2$ y $Q : 2 + 2 = 3$, donde claramente P es verdadera y Q es falsa, se tiene que la proposición compuesta $P \wedge Q$ es falsa.* ■

La conectiva **disyunción** de P y Q es la nueva proposición $\boldsymbol{P \vee Q}$, que se lee "P o Q". Su valor de verdad está dado por la tabla

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo 7. *Considere* $P : 2^3 = 6$ *y* $Q : 2+2 = 4$ *dos proposiciones donde claramente* P *es falsa y* Q *es verdadera. Se tiene que la proposición compuesta* $P \vee Q$ *es verdadera.* ■

La conectiva binaria **disyunción exclusiva** de P y Q es la nueva proposición $\boldsymbol{P \veebar Q}$, que se lee "P o Q, pero no ambas". Su valor de verdad está dado por la tabla

P	Q	$P \veebar Q$
V	V	F
V	F	V
F	V	V
F	F	F

En la lengua castellana se utiliza la misma letra "o" para las proposiciones que admiten como verdaderas ambas y para las que solo se admite una verdadera. Se debe hacer la diferencia, por ejemplo, en casos como la proposición "Mario es hombre o mujer, pero no ambos". En latín se utilizaba la palabra *aut* para la o exclusiva y la palabra *vel* para la inclusiva, es decir, para el caso en que se admiten ambos. La inicial de *vel* se tomó como el símbolo $\vee$ (véase [21]).

Si P y Q son dos proposiciones, la **implicación** de Q por P es la nueva proposición $\boldsymbol{P \rightarrow Q}$, que se lee "si P entonces Q" o "P implica Q". Su valor de verdad está dado por la tabla

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

Otras formas de leer esta proposición son "Q si P" o "P solo si Q" o "P es suficiente para Q" o "Q es necesario para P". A la proposición P se le llama **antecedente** y a Q, **consecuente**.

Ejemplo 8. *Considere* $P : 1 + 1 = 3$ *y* $Q : 5$ *es impar, dos proposiciones donde evidentemente* P *es falsa y* Q *es verdadera. Se tiene que la proposición compuesta* $P \to Q$ *es verdadera.* ■

La **doble implicación** o **bicondicional** de P y Q es la nueva proposición $\boldsymbol{P \leftrightarrow Q}$, que se lee "$P$ si y solo si Q". La proposición $P \leftrightarrow Q$ es equivalente con $(P \to Q) \wedge (Q \to P)$ y su valor de verdad está dado por la tabla

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

Otra forma de leer esta proposición es "P es necesario y suficiente para Q".

Ejemplo 9. *Si se consideran las proposiciones* $P :$ 4 *es un número impar;* $Q : 1 + 1 = 3$, *es claro que tanto* P *como* Q *son proposiciones falsas; por lo tanto, se tiene que la proposición compuesta* $P \leftrightarrow Q$ *es verdadera.* ■

En la aplicación de las conectivas se puede establecer una prioridad para evitar el uso excesivo de los paréntesis, y se debe entender en el orden: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$. Por ejemplo, con esta convención, sería posible escribir $P \to Q \vee R$ en vez de $P \to (Q \vee R)$, o escribir

$$P \vee Q \to R \wedge S \leftrightarrow \neg T \vee V$$

en vez de

$$\big[(P \vee Q) \to (R \wedge S)\big] \leftrightarrow (\neg T \vee V)$$

Sin embargo, se tratará de ser lo más específico posible y en algunos casos se utilizarán los paréntesis, aunque no sean necesarios.

Ejemplo 10. *Sean P y Q las proposiciones*

P : 31 *es un número primo*

Q : *el hielo es caliente*

Determine el valor de verdad de las proposiciones $P \wedge Q$, $P \vee Q$.

Solución. El valor de verdad de P es verdadero; el de Q es falso. La proposición $P \wedge Q$ es "31 es un número primo y el hielo es caliente" es F, mientras que $P \vee Q$ es V. ■

Ejemplo 11. *Si P y Q corresponden a las proposiciones*

P : *hay vida en la Luna*

Q : $2 + 1 = 3$

Determine el valor de verdad de P, Q, $P \vee Q$, $P \wedge Q$, $P \rightarrow Q$, $P \leftrightarrow Q$.

Solución. Claramente, el valor de verdad de P es F y el de Q es V; así, la proposición $P \vee Q$, que se lee "hay vida en la Luna o $2+1 = 3$", tiene como valor de verdad V. Análogamente, el valor de verdad de $P \wedge Q$ es F, de $P \rightarrow Q$ es V, de $P \leftrightarrow Q$ es F. ■

Ejemplo 12. *Considere las proposiciones P, Q y R dadas por*

P : *el problema tiene solución*

$Q : a + b = 1$

R: *n es un número primo.*

- *La proposición "Una condición necesaria para que el problema tenga solución es que $a + b = 1$ y n sea un número primo" se simboliza como $P \rightarrow (Q \wedge R)$.*

- *La proposición "Si $a + b = 1$ y n es un número primo, entonces el problema tiene solución" se simboliza como $(Q \wedge R) \rightarrow P$.*

- *La proposición "$a + b = 1$ y si n es un número primo entonces el problema tiene solución" se simboliza como $Q \wedge (R \rightarrow P)$.*

– *La proposición "Una condición suficiente para que el problema tenga solución es que $a + b = 1$" se simboliza como $Q \to P$.*

– *La proposición "El problema tiene solución si n es un número primo o si $a + b \neq 1$" se simboliza como $(R \vee \neg Q) \to P$.* ■

Ejemplo 13. *Simbolice y valide las proposiciones:*
S : *Si hay elefantes en Marte y el fuego es frío, entonces* $2 + 1 = 4$
T : *Hay elefantes en Marte, y si el fuego es frío, entonces* $2 + 1 = 4$.

Solución. Se toman las proposiciones atómicas
P : hay elefantes en Marte
Q : el fuego es frío
$R : 2 + 1 = 4$.
Claramente, estas tres proposiciones son falsas; así, la proposición S se simboliza como $(P \wedge Q) \to R$ y su valor de verdad es:

$$[(F \wedge F) \to F] \equiv [F \to F] \equiv V$$

Se utiliza el símbolo $\equiv$ para representar proposiciones equivalentes, es decir, que tienen el mismo valor de verdad. La proposición T se simboliza como $P \wedge (Q \to R)$ y su valor de verdad es

$$[F \wedge (F \to F)] \equiv [F \wedge V] \equiv F$$

es decir, T es falsa. ■

Ejemplo 14. *Construya la tabla de verdad de la proposición*

$$(\neg P \wedge Q) \to (\neg Q \vee P)$$

Solución. Para construir la tabla, se parte de las proposiciones atómicas y en cada columna se van formando las proposiciones compuestas, hasta llegar, en la última columna, a la proposición dada.

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

■

Se dice que una proposición compuesta es una **tautología** si es verdadera para todos los posibles valores de verdad de las proposiciones atómicas que la componen. Para representar una tautología se utiliza el símbolo $\boldsymbol{V_0}$.

Ejemplo 15. *La proposición* $P \vee \neg P$ *es una tautología, pues su valor de verdad siempre es verdadero para toda proposición* P*. En este caso, se puede escribir* $P \vee \neg P \equiv V_0$*.* ■

Se dice que una proposición compuesta que es falsa para todos los posibles valores de verdad de las proposiciones atómicas que la componen es una **contradicción**. Para representarla se utiliza el símbolo $\boldsymbol{F_0}$.

Ejemplo 16. *La proposición* $P \wedge \neg P$ *es una contradicción, pues su valor de verdad siempre es falso para toda proposición* P*, independiente de si* P *es falsa o verdadera. En este caso, se puede escribir* $P \wedge \neg P \equiv F_0$*.* ■

Se dice que una proposición compuesta será una **contingencia** o **eventualidad** si no es una tautología ni una contradicción.

Ejemplo 17. *La proposición*

$$(\neg P \wedge Q) \rightarrow (\neg Q \vee P)$$

es una contingencia, pues, como se verificó en el ejemplo 14*, no es tautología ni contradicción.* ■

Sean P y Q dos proposiciones, se dice que:

- **P implica (tauto)lógicamente a Q** si y solo si $P \to Q$ es una tautología. En este caso se escribe $\boldsymbol{P \Rightarrow Q}$.
- **P es (tauto)lógicamente equivalente a Q** si y solo si $P \leftrightarrow Q$ es una tautología. En este caso se escribe $\boldsymbol{P \Leftrightarrow Q}$ o $\boldsymbol{P \equiv Q}$.

En matemáticas, las tautologías son conocidas como **teoremas**. Muchas de las proposiciones, resultados o teoremas son implicaciones lógicas o equivalencias lógicas. Por ejemplo, en el álgebra usual de los números reales se tiene la proposición "Si $a \neq 0$, entonces $a^0 = 1$", y en geometría, "Si un triángulo es equilátero y l es la longitud de su lado, entonces su área es $\frac{l^2\sqrt{3}}{4}$", ambas son implicaciones que siempre se cumplen, es decir, son implicaciones lógicas y, por lo tanto, son teoremas. El conocido teorema de Pitágoras afirma que "En un triángulo rectángulo se cumple que la suma del cuadrado de los catetos es igual al cuadrado de la hipotenusa", pero además afirma que "Si a, b y c son las medidas de los lados de un triángulo y se cumple que $a^2 + b^2 = c^2$, entonces el triángulo es rectángulo". Este teorema es, básicamente, una equivalencia lógica.

Ejemplo 18. *Por medio de una tabla de verdad, determine si la proposición $P \to Q$ es lógicamente equivalente a la proposición $\neg P \vee Q$.*

Solución. Es necesario determinar si $(P \to Q) \longleftrightarrow (\neg P \vee Q)$ es o no una tautología. Se construye la tabla de verdad asociada:

P	Q	$P \to Q$	$\neg P$	$\neg P \vee Q$	$(P \to Q) \longleftrightarrow (\neg P \vee Q)$
V	V	V	F	V	V
V	F	F	F	F	V
F	V	V	V	V	V
F	F	V	V	V	V

Como la última columna es verdadera en todos los casos, la proposición dada es una tautología y se cumple que $(P \to Q) \Longleftrightarrow (\neg P \vee Q)$. ■

Sean P y Q dos proposiciones:

- La **recíproca** de $P \to Q$ es la nueva proposición $Q \to P$.
- La **contrapositiva** de la proposición $P \to Q$ es $\neg Q \to \neg P$.

Ejemplo 19. *Sea T la proposición*

$$T: \text{ si } 1+1=3, \text{ entonces } 5 \geq 4$$

La contrapositiva de T es la proposición "si $5 < 4$, entonces $1+1 \neq 3$", mientras que la recíproca de T es la proposición "si $5 \geq 4$, entonces $1+1=3$". Es claro que T y su contrapositiva son verdaderas, en cambio, su recíproca es falsa. ■

Recuerde ahora la fórmula para a y b números reales, conocida como la *primera fórmula notable*:

$$(a+b)^2 = a^2 + 2ab + b^2 \tag{1.1}$$

Lo que esta fórmula dice es que para cualquier valor de a y de b se puede reemplazar la expresión $(a+b)^2$ por $a^2+2ab+b^2$ o viceversa, y el resultado no se altera.

El ejemplo 18 no dice que las dos proposiciones sean iguales, sino más bien equivalentes, es decir, es una especie de fórmula notable en donde se puede reemplazar la expresión $P \to Q$ por $\neg P \vee Q$ o viceversa, y el valor de verdad no cambia. Para indicar esta equivalencia tautológica, en ocasiones, como ya se mencionó, se utiliza el símbolo $\equiv$.

Como las fórmulas son válidas vía reemplazos, se tiene que

$$(x^2+3)^2 = x^4 + 6x^2 + 9$$

es verdadera al sustituir a por x^2 y sustituir b por 3 en la fórmula (1.1). De la misma forma,

$$[(P \wedge Q) \to \neg R] \equiv [\neg(P \wedge Q) \vee \neg R]$$

es verdadera, pues se obtiene de la equivalencia $(P \to Q) \Leftrightarrow (\neg P \vee Q)$, probada en el ejemplo 18 al sustituir la proposición P por la proposición $(P \wedge Q)$ y, al mismo tiempo, sustituir Q por $\neg R$.

Ejemplo 20. *Construya la tabla de verdad para la siguiente proposición y clasifíquela.*

$$[P \to (Q \vee R)] \longleftrightarrow (\neg P \wedge R)$$

Solución. Se procede como en el ejemplo anterior, pero como hay 3 proposiciones atómicas involucradas, se tienen $2^3 = 8$ posibles asignaciones de valores de verdad diferentes, que corresponden a las 8 filas. Por otro lado, para simplificar la escritura, la última columna corresponde a la proposición dada, etiquetada con $*$, que se obtiene de la doble equivalencia entre la quinta y séptima columnas.

P	Q	R	$Q \vee R$	$P \to (Q \vee R)$	$\neg P$	$\neg P \wedge R$	$*$
V	V	V	V	V	F	F	F
V	V	F	V	V	F	F	F
V	F	V	V	V	F	F	F
V	F	F	F	F	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	V	V	F	F
F	F	V	V	V	V	V	V
F	F	F	F	V	V	F	F

Con lo cual, la proposición dada es una contingencia. ∎

Ejercicios (sección 1.2)

1. Si P, Q, R son verdaderas y S, T son falsas, determine el valor de verdad de las proposiciones:

   (a) $\big[P \to (R \to T)\big] \leftrightarrow \big[(\neg P \wedge S) \to (Q \to \neg T)\big]$

   (b) $\big[(\neg T \vee \neg P) \leftrightarrow [T \to (R \vee S)]\big] \leftrightarrow \big[(P \wedge Q \wedge \neg T) \to (\neg Q \to \neg S)\big]$

2. Determine, utilizando tablas de verdad, si cada proposición compuesta es tautología, contradicción o contingencia.

   (a) $\neg(P \to Q) \leftrightarrow (P \wedge \neg Q)$

   (b) $R \to \big[(\neg P \vee Q) \wedge (P \wedge \neg Q)\big]$

   (c) $(P \vee Q) \to \big[Q \to (P \wedge Q)\big]$

   (d) $\big[(P \to Q) \to R\big] \longleftrightarrow \big[(P \wedge \neg R) \to \neg Q\big]$

   (e) $\big[\neg(\neg P \wedge R) \vee Q\big] \longleftrightarrow \big[(\neg P \vee R) \wedge Q\big]$

3. Determine una asignación de valores de verdad para A, B, C, D y E que verifique que $\big[\big(A \to (B \vee C)\big) \wedge \big(C \to (D \wedge E)\big) \wedge \neg D\big]$ no implica tautológicamente a $A \to E$.

4. Determine valores de verdad para A, B, C y D, de manera que se verifique que $\big[(A \to B) \wedge (C \to D) \wedge (B \vee C)\big]$ no implica tautológicamente a $A \vee D$.

5. Utilice tablas de verdad para determinar si la proposición $(P \to Q) \vee \big[(\neg Q \to \neg P) \wedge \neg R\big]$ es tautológicamente equivalente a la proposición $\neg(P \wedge \neg Q)$.

6. Si $P \to Q$ es falsa, determine el valor de verdad de la proposición $\big[(P \vee R) \wedge \neg Q\big] \to \big[(\neg P \wedge S) \to (T \vee P)\big]$.

7. Si $(P \to Q) \wedge R$ es verdadera, determine el valor de verdad de la proposición $\big[(\neg P \vee T) \vee Q\big] \wedge \big(\neg R \to S\big)$.

8. Utilice tablas de verdad para comprobar que

   (a) $\big[(Q \to R) \wedge (\neg Q \to S)\big] \Longrightarrow (R \vee S)$

   (b) $\big[\neg P \vee (Q \to R)\big] \Longleftrightarrow \big[\neg(P \wedge Q) \vee R\big]$

9. Utilice una tabla de verdad para demostrar que $P \veebar Q$ es equivalente a $(P \wedge \neg Q) \vee (Q \wedge \neg P)$.

10. Considere las proposiciones P : Héctor estudia; Q : Felipe estudia; R : Héctor juega fútbol; S : Felipe juega fútbol; T : Héctor invita a Felipe a jugar fútbol.
    Simbolice las proposiciones:
    (a) Héctor o Felipe estudian, pero Héctor invita a Felipe a jugar fútbol.
    (b) Si Héctor invita a Felipe a jugar fútbol, entonces Felipe no estudia.
    (c) Si Héctor y Felipe juegan fútbol, entonces ni Héctor ni Felipe estudian.
    (d) Felipe estudia si y solo si no juega fútbol.
    (e) Una condición necesaria para que Felipe y Héctor estudien es que no jueguen fútbol.
    (f) No es cierto que Héctor invita a Felipe a jugar fútbol y Héctor estudie.
11. Considere las proposiciones P : se nombre presidente; Q : la mayoría vote por él; R : tenga buena salud; S : habrá una crisis de gobierno.
    Simbolice las siguientes proposiciones:
    (a) Una condición necesaria para que se nombre presidente es que la mayoría vote por él y tenga buena salud.
    (b) La mayoría votó por él y tiene buena salud. Por lo tanto, se nombró presidente.
    (c) No habrá crisis si y solo si una condición suficiente para que se nombre presidente es que la mayoría vote por él.
    (d) Si la mayoría no vota por él o no tiene buena salud, entonces no se nombra presidente y habrá una crisis de gobierno.
    (e) O la mayoría vota por él o habrá una crisis de gobierno si y solo si no se nombra presidente.

12. Escriba la contrapositiva y la recíproca de las proposiciones:

    (a) Si $1 < 4$, entonces $5 \geq 8$

    (b) Si la inundación destruye mi casa o el fuego destruye mi casa, entonces la compañía de seguros me pagará.

    (c) Si no es cierto que $2+2 = 4$ y 9 es un número primo, entonces $2 + 2 = 5$ u 11 es un número par.

    (d) Si n no es un cuadrado perfecto, entonces n es un número primo o n es un número par, pero no ambos.

13. Defina la conectiva *trazo de Sheffer*, que se denota por $\mid$, como la *anticonjunción*, es decir, la negación de la conjunción, por la tabla:

P	Q	$P \mid Q$
V	V	F
V	F	V
F	V	V
F	F	V

Determine cuál de las conectivas estudiadas corresponde a $P \mid P$, cuál a $(P \mid Q) \mid (P \mid Q)$ y cuál a $(P \mid P) \mid (Q \mid Q)$.

14. Defina la conectiva *flecha de Pierce*, que se denota por $\downarrow$, como la *antidisyunción*, es decir, la negación de la disyunción, por la tabla:

P	Q	$P \downarrow Q$
V	V	F
V	F	F
F	V	F
F	F	V

Determine cuál de las conectivas estudiadas corresponde a $P \downarrow P$, cuál a $(P \downarrow Q) \downarrow (P \downarrow Q)$ y cuál a $(P \downarrow P) \downarrow (Q \downarrow Q)$.

15. Si P, Q, T son verdaderas y R, S son falsas, determine el valor de verdad de $\big[(P \vee S) \downarrow (R \mid T)\big] \veebar \big[(\neg P \mid S) \downarrow (Q \rightarrow \neg T)\big]$.

1.3 Leyes de la lógica

En el mismo sentido de equivalencia explicado al final de la sección anterior, las leyes que se dan en la tabla 1.1 hablan de proposiciones que serán equivalentes. Estas leyes o equivalencias (tauto)lógicas permiten simplificar expresiones lógicas en el sentido tautológico y sirven para conjeturar nuevos resultados.

Además, permiten demostrar algunos resultados sin construir tablas de verdad, lo cual es muy tedioso en algunos casos donde la proposición compuesta involucra a cuatro o más proposiciones atómicas.

La validez de estas leyes se puede verificar mediante tablas de verdad (ver ejemplo 18) o por medio de un desarrollo lógico y la aplicación de las leyes dadas en la tabla 1.1 (ver ejemplo 25).

Para simplificar la notación y el desarrollo de los siguientes ejemplos, en algunas ocasiones se usarán las claves dadas en esta tabla, así por ejemplo, en vez de Implicación y Disyunción, se escribe ID; en vez de Doble Negación, se escribe DN y así sucesivamente.

Ejemplo 21. *Pruebe que la proposición* $P \to Q$ *es lógicamente equivalente a la proposición* $\neg Q \to \neg P$*, es decir, que* $(P \to Q) \Leftrightarrow (\neg Q \to \neg P)$.

Solución. Tome la proposición $P \to Q$ y al aplicar las leyes que se enuncian en la columna de justificación, se obtiene la proposición $\neg Q \to \neg P$, así:

$P \to Q$	**Justificación**
$\equiv \neg P \vee Q$	ID
$\equiv Q \vee \neg P$	Conmutatividad
$\equiv \neg(\neg Q) \vee \neg P$	Doble Negación
$\equiv \neg Q \to \neg P$	ID

Con lo cual, se ha probado la equivalencia lógica. ∎

Implicación y disyunción (ID)	$P \to Q \equiv \neg P \vee Q$
Contrapositiva	$P \to Q \equiv \neg Q \to \neg P$
Doble negación (DN)	$\neg\neg P \equiv P$
De Morgan (DM)	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
Conmutativa (Con.)	$P \vee Q \equiv Q \vee P$ $P \wedge Q \equiv Q \wedge P$
Asociativa (Aso.)	$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
Distributiva (Dis.)	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
Idempotencia (Ide.)	$P \wedge P \equiv P$ $P \vee P \equiv P$
Neutro (Ne.)	$P \vee F_0 \equiv P$ $P \wedge V_0 \equiv P$
Inversos (Inv.)	$P \vee \neg P \equiv V_0$ $P \wedge \neg P \equiv F_0$
Dominación (Dom.)	$P \wedge F_0 \equiv F_0$ $P \vee V_0 \equiv V_0$
Absorción (Abs.)	$P \vee (P \wedge Q) \equiv P$ $P \wedge (P \vee Q) \equiv P$
Exportación (Exp.)	$P \to (Q \to R) \equiv (P \wedge Q) \to R$

Tabla 1.1: Equivalencias lógicas.

Como se mencionó anteriormente, la proposición $\neg Q \to \neg P$ se conoce como la **contrapositiva** de $P \to Q$. Recuerde que la contrapositiva no debe confundirse, pues no es equivalente con $Q \to P$, que se conoce como la **recíproca** de $P \to Q$.

Ejemplo 22. *Simplifique la expresión* $[P \vee (Q \wedge R)] \vee (\neg Q \wedge R)$

Solución. Se toma la expresión y, al aplicar las leyes que se enuncian en la columna de justificación, se va simplificando como sigue:

$$\begin{array}{ll} [P \vee (Q \wedge R)] \vee (\neg Q \wedge R) & \textbf{Justificación} \\ \equiv P \vee [(Q \wedge R) \vee (\neg Q \wedge R)] & \text{Asociatividad} \\ \equiv P \vee [(Q \vee \neg Q) \wedge R)] & \text{Distributividad} \\ \equiv P \vee [V_0 \wedge R] & \text{Inversos} \\ \equiv P \vee R & \text{Neutro} \end{array}$$

Es decir, $[P \vee (Q \wedge R)] \vee (\neg Q \wedge R)$ se simplifica como $P \vee R$. ■

Ejemplo 23. *Simplifique la expresión*

$$\neg\Big[(\neg Q \vee P) \wedge \neg[(\neg P \wedge (Q \wedge R)) \wedge (P \vee R)]\Big]$$

Solución. Como en el ejemplo anterior:

$$\begin{array}{ll} \neg\Big[(\neg Q \vee P) \wedge \neg[(\neg P \wedge (Q \wedge R)) \wedge (P \vee R)]\Big] & \textbf{Justificación} \\ \equiv \neg(\neg Q \vee P) \vee \neg\Big[\neg[(\neg P \wedge (Q \wedge R)) \wedge (P \vee R)]\Big] & \text{DM} \\ \equiv (Q \wedge \neg P) \vee [(\neg P \wedge (Q \wedge R)) \wedge (P \vee R)] & \text{DM, DN} \\ \equiv (Q \wedge \neg P) \vee [((\neg P \wedge Q) \wedge R) \wedge (P \vee R)] & \text{Aso.} \\ \equiv (Q \wedge \neg P) \vee [(\neg P \wedge Q) \wedge (R \wedge (P \vee R))] & \text{Aso.} \\ \equiv (\neg P \wedge Q) \vee [(\neg P \wedge Q) \wedge R] & \text{Con. y Abs.} \\ \equiv \neg P \wedge Q & \text{Abs.} \end{array}$$

Es decir, $\neg\Big[(\neg Q \vee P) \wedge \neg[(\neg P \wedge (Q \wedge R)) \wedge (P \vee R)]\Big] \equiv \neg P \wedge Q$. ■

Ejemplo 24. *Simplifique la expresión*

$$\Big[(P \vee Q) \wedge \neg(\neg P \wedge Q)\Big] \vee \Big[\neg\big[Q \wedge (R \vee Q)\big] \wedge (P \vee \neg Q)\Big]$$

Solución. Siguiendo el mismo procedimiento de los ejemplos anteriores, la expresión se simplifica como sigue:

$\Big[(P \vee Q) \wedge \neg(\neg P \wedge Q)\Big] \vee \Big[\neg\big[Q \wedge (R \vee Q)\big] \wedge (P \vee \neg Q)\Big]$	**Justificación**
$\equiv \big[(P \vee Q) \wedge (P \vee \neg Q)\big] \vee \Big[\neg\big[Q \wedge (R \vee Q)\big] \wedge (P \vee \neg Q)\Big]$	DM, DN
$\equiv \big[(P \vee Q) \wedge (P \vee \neg Q)\big] \vee \big[\neg Q \wedge (P \vee \neg Q)\big]$	Abs.
$\equiv \big[P \vee (Q \wedge \neg Q)\big] \vee \neg Q$	Dis., Abs.
$\equiv (P \vee F_0) \vee \neg Q$	Inv.
$\equiv P \vee \neg Q$	Ne.

Es decir, la expresión inicial es lógicamente equivalente a $P \vee \neg Q$. ■

Como se mencionó anteriormente, la validez de las leyes presentadas en la tabla 1.1 se puede verificar mediante tablas de verdad. En el siguiente ejemplo se presenta una prueba con base en un desarrollo lógico y la aplicación de otras leyes.

Ejemplo 25. *Pruebe la Ley de Exportación, es decir demuestre que* $[P \to (Q \to R)] \Leftrightarrow [(P \wedge Q) \to R]$.

Solución. Se debe probar que la proposición $P \to (Q \to R)$ es equivalente a $(P \wedge Q) \to R$

$P \to (Q \to R)$	**Justificación**
$\equiv \neg P \vee (Q \to R)$	ID
$\equiv \neg P \vee (\neg Q \vee R)$	ID
$\equiv (\neg P \vee \neg Q) \vee R$	Aso.
$\equiv \neg(P \wedge Q) \vee R$	DM
$\equiv (P \wedge Q) \to R$	ID

Con esto se verifica la ley. ■

Ejercicios (sección 1.3)

Simplifique las siguientes expresiones:

1. $P \vee \neg(\neg R \vee P) \vee R$

2. $(P \leftrightarrow R) \wedge \neg(\neg P \vee R)$

3. $\big[P \vee \neg(\neg Q \vee \neg S)\big] \vee \neg(\neg Q \rightarrow \neg S)$

4. $[(\neg P \vee Q) \wedge P] \rightarrow Q$

5. $[(\neg P \wedge Q) \vee \neg(Q \vee P)] \wedge [(P \vee R) \wedge (P \vee \neg R)]$

6. $\neg[P \wedge \neg(T \wedge R)] \wedge (T \rightarrow \neg P)$

7. $[(\neg P \vee Q) \wedge \neg R] \rightarrow [(\neg Q \wedge R) \vee P]$

8. $(\neg P \wedge Q) \vee [\neg P \wedge \neg(Q \wedge R)] \vee \neg(R \rightarrow P)$

9. $[P \rightarrow (Q \wedge P)] \vee [\neg Q \wedge (P \vee Q)]$

10. $\neg Q \vee \neg\Big[\big[\neg[(P \wedge Q) \vee (P \wedge \neg Q)] \vee Q\big] \wedge P\Big]$

11. $[(P \vee Q) \wedge \neg(R \vee P)] \vee [(R \wedge Q) \vee P]$

12. $\neg\,[(\neg P \vee \neg Q) \wedge (\neg Q \vee P)] \wedge (\neg Q \vee R)$

13. $(\neg P \wedge Q) \vee [\neg(Q \wedge R) \wedge \neg P] \vee (P \wedge \neg R)$

14. $\neg\Big[(Q \vee P) \wedge \neg\big[(\neg P \wedge (\neg Q \wedge R)) \wedge (P \vee R)\big]\Big]$

15. $\neg\Big[\neg\big[[\neg P \vee (\neg Q \vee R)] \vee (S \wedge R)\big] \vee (Q \wedge P)\Big]$

16. $(P \rightarrow \neg Q) \wedge \Big[\big[\neg(R \vee \neg P) \wedge (Q \vee P)\big] \vee (R \wedge P)\Big]$

1.4 Inferencias lógicas

"Cuando uno ha eliminado el imposible,
lo que permanece, sin embargo improbable,
debe ser la verdad".

Sherlock Holmes

La **inferencia** es la relación entre las *premisas* y la *conclusión* de un argumento o razonamiento. Los **silogismos** son un tipo especial de razonamiento: a partir de dos premisas se obtiene una conclusión, en donde el término medio incluido en las premisas no aparece en la conclusión; por ejemplo, "*Todos los hombres son mortales; Sócrates es hombre, luego Sócrates es mortal*".

Dentro del lenguaje lógico, en ocasiones es necesario determinar si un grupo dado de proposiciones puede garantizar la validez de otra proposición. Es decir, dadas las proposiciones P_1, P_2, $\ldots$, P_n, que se llamarán **premisas**, y una **conclusión** Q, se debe decidir si la proposición

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to Q$$

es una tautología, es decir, si se cumple que $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \Rightarrow Q$. Si es así, se dice que el argumento (o el razonamiento) es **válido**. De acuerdo con lo estudiado en las secciones anteriores, se sabe que el razonamiento no será válido si la condicional anterior es falsa, y esto ocurre cuando $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ es verdadero y Q es falsa.

Ejemplo 26. *Simbolice el siguiente razonamiento y analice si es válido o no: Si Juan participa como jurado, entonces saldrá de viaje y deberá comprar un traje nuevo. Pero salió de viaje o compró un traje nuevo. Por lo tanto, Juan participa como jurado.*

Solución. En primer lugar, a cada proposición se le asigna una letra:

$P:$ Juan participa como jurado
$Q:$ Juan saldrá de viaje
$R:$ Juan deberá comprar un traje nuevo

Con ellas, la proposición "Juan saldrá de viaje y deberá comprar un traje nuevo" se simboliza $Q \wedge R$, así "Si Juan participa como jurado, entonces saldrá de viaje y deberá comprar un traje nuevo" se simboliza $P \to (Q \wedge R)$; por otro lado, la proposición "Pero salió de viaje o compró un traje nuevo" es $Q \vee R$. De manera que se cuenta con dos premisas:

$$P_1 : \quad P \to (Q \wedge R) \qquad\qquad P_2 : \quad Q \vee R$$

y la conclusión es P. Luego, el argumento se simboliza como

$$\big[\big(P \to (Q \wedge R)\big) \wedge (Q \vee R)\big] \to P \tag{1.2}$$

y se construye la tabla de verdad:

P	Q	R	$Q \wedge R$	$P \to (Q \wedge R)$	$Q \vee R$	$[P \to (Q \wedge R)] \wedge (Q \vee R)$	$*$
V	V	V	V	V	V	V	V
V	V	F	F	F	V	F	V
V	F	V	F	F	V	F	V
V	F	F	F	F	F	F	V
F	V	V	V	V	V	V	F
F	V	F	F	V	V	V	F
F	F	V	F	V	V	V	F
F	F	F	F	V	F	F	V

Al observar la columna $*$, que corresponde al valor de verdad de la proposición (1.2), se concluye que la proposición no es tautología; por lo tanto, el argumento propuesto no es válido. ■

El método utilizado de determinar la validez de un argumento por medio de las tablas de verdad, por lo general, no es eficiente para más de tres proposiciones atómicas. Sin embargo, la tabla 1.2 enumera algunas reglas de inferencia, implicaciones tautológicas, que se pueden utilizar para inferir conclusiones a partir de premisas dadas.

El nombre de la regla *Modus ponens* en su forma completa en latín es *Modus ponendo ponens*, que quiere decir "el método de obtención mediante la aserción". Igualmente, *Modus tollens*, *Modus tollendo tollens*, que quiere decir "el método de negar mediante la negación" [24].

Regla de inferencia	**Premisas**	**Conclusión**
Simplificación (Simp.)	$P \wedge Q$	P Q
Adjunción (Adj.)	P Q	$P \wedge Q$
Adición (Adi.) para cualquier proposición Q	P	$P \vee Q$
Separación (Sep.) o **Modus ponens** (MP)	P $P \to Q$	Q
Contraposición o **Modus tollens** (MT)	$P \to Q$ $\neg Q$	$\neg P$
Silogismo disyuntivo (SD)	$P \vee Q$ $\neg P$	Q
Silogismo hipotético (SH)	$P \to Q$ $Q \to R$	$P \to R$
Dilema constructivo (DC)	$P \vee Q$ $P \to R$ $Q \to S$	$R \vee S$
Dilema destructivo (DD)	$\neg R \vee \neg S$ $P \to R$ $Q \to S$	$\neg P \vee \neg Q$
Ley de casos (LC)	$P \to Q$ $\neg P \to R$	$Q \vee R$

Tabla 1.2: Inferencias lógicas.

Ejemplo 27. *Demuestre la proposición* T *a partir de las proposiciones* $(P \vee Q) \to R$, $(R \vee S) \to T$, $S \vee P$, $\neg S$.

Solución. Se trabaja en forma vertical y se indica la regla utilizada

1.	$(P \vee Q) \to R$	Premisa
2.	$(R \vee S) \to T$	Premisa
3.	$S \vee P$	Premisa
4.	$\neg S$	Premisa
5.	P	Silogismo disyuntivo a 3 y 4.
6.	$P \vee Q$	Adición a 5.
7.	R	Separación a 1 y 6.
8.	$R \vee S$	Adición a 7.
9.	T	Separación a 2 y 8.

Así, la conclusión T es válida a partir de las premisas dadas. ■

Ejemplo 28. *Demuestre la proposición* $(A \wedge R) \vee (A \wedge S)$ *a partir de las proposiciones* $C \to (R \vee S)$, $A \to (B \vee C)$, $B \to \neg A$, $\neg D$, $A \vee D$.

Solución. De la misma manera que el ejemplo anterior:

1.	$C \to (R \vee S)$	Premisa
2.	$A \to (B \vee C)$	Premisa
3.	$B \to \neg A$	Premisa
4.	$\neg D$	Premisa
5.	$A \vee D$	Premisa
6.	A	SD a 4. y 5.
7.	$B \vee C$	Sep. a 2 y 6.
8.	$\neg B$	MT a 3 y 6.
9.	C	SD a 7 y 8.
10.	$R \vee S$	Sep. a 1 y 9.
11.	$A \wedge (R \vee S)$	Adj. a 6 y 10.
12.	$(A \wedge R) \vee (A \wedge S)$	Dis. a 11.

Con esto, la conclusión es válida a partir de las premisas dadas. ■

Ejemplo 29. *Considere el siguiente razonamiento y establezca su validez: Si no compro el boleto del tren o no me gusta el arte moderno, entonces me quedaré en la ciudad y le obsequiaré flores a mi esposa. Si me hubiera quedado en la ciudad, habría asistido a la recepción. Pero no asistí a la recepción. Por lo tanto, compré el boleto del tren.*

Solución. En primer lugar, es necesario convertir este razonamiento en forma simbólica, asignando a cada proposición una letra, así:

P : compro el boleto del tren
Q : me gusta el arte moderno
R : me quedaré en la ciudad
S : le obsequiaré flores a mi esposa
T : asisto a la recepción

Con lo cual el argumento se puede escribir simbólicamente como:

$$\begin{array}{l} (\neg P \vee \neg Q) \to (R \wedge S) \\ R \to T \\ \neg T \\ \hline \hfill \therefore P \end{array}$$

Se utiliza el símbolo $\therefore$ para escribir la conclusión; este se lee “por lo tanto”. Para verificar la validez del argumento anterior, observe que

1.	$(\neg P \vee \neg Q) \to (R \wedge S)$	Premisa
2.	$R \to T$	Premisa
3.	$\neg T$	Premisa
4.	$\neg R$	MT a 2 y 3.
5.	$\neg R \vee \neg S$	Adi. a 4.
6.	$\neg(R \wedge S)$	DM a 5.
7.	$\neg(\neg P \vee \neg Q)$	MT a 1 y 6.
8.	$P \wedge Q$	DM y DN a 7.
9.	P	Simp. a 8.

de donde se comprueba la validez del argumento. ■

Ejemplo 30. *Considere el siguiente razonamiento y establezca su validez: No ocurre que $a+b=7$ y b sea positivo. Si b no es positivo, entonces $2a-3<0$. Si el problema tiene solución única, entonces $2a-3\geq 0$. Si el problema no tiene solución única, entonces no ocurre que $a+b=7$ o b no es positivo. Por lo tanto, se concluye que $a+b\neq 7$.*

Solución. En primer lugar, se debe convertir este razonamiento en forma simbólica, asignando a cada proposición una letra, así:

$$\begin{aligned} P:&\quad a+b=7\\ Q:&\quad b \text{ es positivo}\\ R:&\quad 2a-3<0\\ S:&\quad \text{el problema tiene solución única} \end{aligned}$$

Con esto, el argumento se puede escribir simbólicamente como:

$$\begin{array}{ll} 1. & \neg(P\wedge Q)\\ 2. & \neg Q\to R\\ 3. & S\to\neg R\\ 4. & \neg S\to\neg(P\vee\neg Q)\\ \hline & \therefore\ \neg P \end{array}$$

Para verificar la validez, observe que:

$$\begin{array}{lll} 5. & \neg P\vee\neg Q & \text{De Morgan a 1.}\\ 6. & \neg S\vee\neg R & \text{ID a 3.}\\ 7. & \neg R\to Q & \text{Contrapositiva a 2.}\\ 8. & \neg(P\vee\neg Q)\vee Q & \text{DC a 4, 6 y 7.}\\ 9. & (\neg P\wedge Q)\vee Q & \text{DM y DN a 8.}\\ 10. & Q & \text{Absorción a 9.}\\ 11. & \neg P & \text{SD a 5 y 10.} \end{array}$$

de donde se comprueba la validez del argumento. ■

Ejemplo 31. *Este ejemplo se relaciona con el razonamiento que hace Sherlock Holmes para esclarecer un asesinato en su libro* Un estudio en escarlata [14]. *Allí se escribe:*
"Y ahora llegamos a la gran pregunta del porqué. El robo no ha sido el objeto del asesinato, puesto que nada desapareció. ¿Fue por motivos políticos o por una mujer? Ésta es la pregunta con que me enfrento. Desde el principio me he inclinado hacia esta última suposición. Los asesinos políticos se complacen demasiado en hacer solo su trabajo y huir. Este asesinato, por el contrario, había sido realizado muy deliberadamente y quien lo perpetró ha dejado huellas por toda la habitación, mostrando que estuvo ahí todo el tiempo".
Simbolice el argumento empleado y deduzca que el asesinato fue perpetrado por causa de una mujer.

Solución. Utilizando las proposiciones:

P_1 : fue un robo

P_2 : algo desapareció

P_3 : fue por motivos políticos

P_4 : fue por causa de una mujer

P_5 : el asesino huyó inmediatamente

P_6 : el asesino dejó huellas por toda la habitación

Se convierte el argumento a forma simbólica:

1.	$P_1 \to P_2$	Si fue un robo, hubiera desaparecido algo.
2.	$\neg P_2$	No desapareció nada.
3.	$\neg P_1 \to (P_3 \vee P_4)$	Si no fue un robo, fue algo político o una mujer.
4.	$P_3 \to P_5$	Si hubiera sido algo político, el asesino hubiera huido inmediatamente.
5.	$P_6 \to \neg P_5$	Si el asesino dejó huellas por toda la habitación, no pudo haber huido inmediatamente.
6.	P_6	El asesino dejó huellas por toda la habitación.

A partir de estas premisas, se obtienen las siguientes conclusiones:

7.	$\neg P_1$	MT a 1 y 2.
8.	$P_3 \vee P_4$	MP a 3 y 7.
9.	$\neg P_5$	MP a 5 y 6.
10.	$\neg P_3$	MT a 4 y 9.
11.	P_4	SD a 8 y 10.

de donde se comprueba la validez del argumento. ■

Ejemplo 32. *Demuestre la Ley de Casos, es decir, pruebe que se cumple la tautología*

$$\big[(P \to Q) \wedge (\neg P \to R)\big] \Longrightarrow (Q \vee R)$$

Solución. Es claro que se podría efectuar la demostración comprobando, por medio de una tabla de verdad, que la proposición dada es, en efecto, una implicación lógica, es decir, una tautología. Sin embargo, se hará de una forma más simple, utilizando las reglas de inferencia dadas en esta sección y demostrando la validez del argumento:

$$\begin{array}{r} P \to Q \\ \neg P \to R \\ \hline \therefore Q \vee R \end{array}$$

para ello:

1.	$P \to Q$	Premisa
2.	$\neg P \to Q$	Premisa
3.	$P \vee \neg P$	Ley de inversos
4.	$Q \vee R$	DC a 1, 2 y 3.

de donde se comprueba la validez del argumento. Además note que esta ley de casos es un caso particular del dilema constructivo en donde las premisas de las implicaciones son P y $\neg P$. ■

El siguiente ejemplo determina un *sistema formal* en donde se definen términos primitivos, reglas de inferencia propias de este sistema, axiomas (se asumen válidos) y teoremas (que deben probarse). Ponga especial atención en las "demostraciones" que se realizan en este ejemplo. Sobre este interesante juego, puede consultar [11], [12] y [17].

Ejemplo 33. *A partir de los símbolos primitivos* M, I, U, *se define una palabra como una combinación de ellos. Además, se definen las siguientes reglas de deducción:*

Regla 1.	*Toda palabra se puede triplicar.*
Regla 2.	*Una* U *se puede reemplazar por* II
Regla 3.	*Si aparece* IIII, *se puede eliminar.*
Regla 4.	*Después de una* M *se puede insertar una* U.
Regla 5.	*Si en una palabra aparece* IMU, *puede quitarse la* M.

Se dice que una palabra es admisible si se obtiene al aplicar una o varias de estas reglas a otra palabra admisible. Si, para empezar, se asume como admisible (axioma) la palabra MI, *pruebe que la palabra* MMI *es admisible en este sistema.*

Solución. Se debe partir de la única palabra que se sabe es admisible. Sobre la flecha se indica la regla que se utiliza:

$$\mathrm{MI} \xrightarrow{1} \mathrm{MIMIMI} \xrightarrow{4} \mathrm{MIMUIMI} \xrightarrow{5} \mathrm{MIUIMI} \xrightarrow{2} \mathrm{MIIIIMI} \xrightarrow{3} \mathrm{MMI}$$

Con lo cual, se ha demostrado que MMI es otra palabra admisible. Por supuesto, a partir de MMI es posible obtener, por ejemplo, MUMI al aplicar la regla 4. Las palabras que se probaron admisibles se pueden usar como nuevas premisas (ver ejercicio 8). ■

Ejercicios (sección 1.4)

1. En cada caso, utilice las reglas de inferencia y las leyes de la lógica para demostrar la proposición indicada a partir de las premisas dadas. Justifique cada paso.

   (a) Demuestre P a partir de $(\neg P \vee \neg Q) \rightarrow (R \wedge S)$, $R \rightarrow T$, $\neg T$.

   (b) Demuestre $P \wedge Q$ a partir de $Q \rightarrow \neg R$, $P \vee R$, Q.

   (c) Demuestre D a partir de $A \rightarrow (B \vee C)$, $B \rightarrow C$, $A \vee D$, $\neg C$.

   (d) Demuestre U a partir de $P \rightarrow Q$, $Q \rightarrow (R \wedge S)$, $\neg R \vee \neg T \vee U$, $P \wedge T$.

   (e) Demuestre $R \wedge (P \vee Q)$ a partir de $P \vee Q$, $Q \rightarrow R$, $P \rightarrow T$, $\neg T$.

   (f) Demuestre $\neg(L \wedge D)$ a partir de $V \rightarrow (R \vee P)$, $R \rightarrow \neg V$, $L \rightarrow \neg P$, V.

   (g) Demuestre $Q \vee T$ a partir de $P \rightarrow Q$, $\neg R \rightarrow (S \rightarrow T)$, $R \vee P \vee S$, $\neg R$

   (h) Demuestre T a partir de $(P \vee Q) \rightarrow (R \wedge S)$, $\neg(\neg P \vee \neg R)$, $\neg T \rightarrow \neg(P \wedge S)$.

   (i) Demuestre $\neg U$ a partir de $(Q \wedge R) \rightarrow \neg P$, $\neg Q \rightarrow S$, $R \vee T$, P, $U \rightarrow (\neg S \wedge \neg T)$.

   (j) Demuestre P a partir de $(\neg P \vee Q) \rightarrow R$, $R \rightarrow (S \vee T)$, $\neg S \wedge \neg U$, $\neg U \rightarrow \neg T$.

   (k) Demuestre $\neg(T \wedge \neg U)$ a partir de $(R \vee Q) \rightarrow \neg T$, $\neg Q \vee R$, $P \vee Q$, $P \rightarrow (R \wedge S)$.

   (l) Demuestre una F_0 a partir de $(S \vee T) \vee (T \wedge K)$, $\neg(T \wedge K)$, $\neg T$, $(R \vee S) \rightarrow (T \wedge K)$.

   (m) Demuestre $\neg R \rightarrow \neg T$ a partir de $P \rightarrow (Q \rightarrow R)$, $P \vee S$, $T \rightarrow Q$, $\neg S$.

(n) Demuestre $\neg(T \to A)$, a partir de E, $\neg P \vee Q$, $E \to (B \wedge \neg Q)$, $A \to (P \wedge C)$, T.

(o) Demuestre $S \vee \neg T$, a partir de $P \wedge \neg R$, $(R \to S) \to (P \to Q)$, $(Q \vee T) \to (S \vee R)$.

(p) Demuestre $x = 5$ a partir de $z > x \to x < 7$, $\big(x < 6 \vee x = 3\big) \to z > x$, $x < 6 \wedge z = 8$, $x \geq 7 \vee x = 5$

(q) Demuestre $T \to A$ a partir de $Q \to S$, $\neg P \to Q$, $P \to (R \wedge S)$, $A \vee \neg S$.

2. En cada caso, utilice las reglas de inferencia y las leyes de la lógica para demostrar las siguientes proposiciones. Justifique cada paso.

   (a) $\Big[\big(P \to Q\big) \wedge \big(P \vee (T \wedge S)\big) \wedge \big(Q \to R\big) \wedge \big(\neg R\big)\Big] \Longrightarrow S$

   (b) $\Big[\big(P \vee Q\big) \wedge \big(\neg R \vee \neg P\big) \wedge \big(S \to R\big) \wedge \big(T \vee S\big) \wedge \big(R \to \neg Q\big)\Big] \Longrightarrow T$

3. En cada uno de los siguientes casos, simbolice las proposiciones involucradas y demuestre la validez de la conclusión.

   (a) Si S campeoniza, entonces C gana o H gana. Si C gana, entonces S no campeoniza. Si H gana, entonces A no gana. De hecho, S campeoniza. Por lo tanto, A no gana o L gana.

   (b) Si estudio matemática discreta o asisto al dentista, entonces no podré matricular el curso de danza. Si no matriculo el curso de danza, entonces no participaré en el festival. Participaré en el festival y me opondré a la explotación petrolera. Por lo tanto, no ocurre que asista al dentista o no me pueda matricular en el curso de danza.

   (c) Si José gana la carrera, entonces Pedro fue el segundo o Ramón fue el segundo. Si Pedro fue el segundo, entonces José no ganó la carrera. Si Carlos fue el segundo, entonces Ramón no fue el segundo. José ganó la carrera. Por lo tanto, Carlos no fue el segundo.

(d) Si estudio computación, entonces debo matricular un curso de matemática. No estudio mucho o no tengo tiempo para leer o necesito vacaciones. Estudio computación y tengo tiempo para leer. Si matriculo un curso de matemática, entonces debo estudiar mucho y no puedo ir al estadio. Por lo tanto, necesito vacaciones.

(e) Si Luis va al partido de fútbol, entonces Laura se irá a nadar. Si Manuel ve televisión toda la noche, entonces Carolina se irá a nadar. Si Laura va a nadar o Carolina va a nadar, Jorge las acompañará. De hecho, Jorge no las acompañará. En consecuencia, no ocurre que Luis fue al partido de fútbol o Manuel ve televisión toda la noche.

(f) O los precios son altos o los salarios son bajos. Si los precios son altos, entonces hay control de precios. Si los salarios son bajos, entonces hay control de precios. Si no hay inflación o la cosecha de café es buena, entonces no hay control de precios. Por lo tanto, hay inflación.

(g) Si no matriculo el curso Matemática discreta, entonces gano los otros cuatro cursos matriculados. Gano los otros cuatro cursos matriculados o cambio de carrera. Si matriculo Matemática discreta y cambio de carrera, entonces no me he decidido. No es cierto que gano los otros cuatro cursos matriculados y no quiero estudiar computación. No quiero estudiar computación. Por lo tanto, no me he decidido.

(h) Si hay secuestros, entonces no hay paz en mi país. Hay secuestros o la prensa informa de manera insensible, o tengo lástima por los delincuentes. Si la prensa informa de manera insensible, entonces no hay paz en mi país. No tengo lástima por los delincuentes. Por lo tanto, no hay paz en mi país.

(i) Si Bill es declarado culpable, entonces su perro no se deprime o Mónica se alegra. Si su perro no se deprime, entonces Bill no es declarado culpable. El precio del petróleo no baja o Mónica no se alegra. De hecho, Bill es declarado culpable. Por lo tanto, su perro se deprime y el precio del petróleo no baja.

(j) Si Leo es un muchacho, entonces Leo es más joven que Juan. Si Leo tiene 13 años, entonces Leo es una muchacha. Si Leo no tiene 13 años, entonces Leo tiene, al menos, la edad de Juan. ¿Leo es un muchacho o una muchacha?

(k) Si le pago al sastre, no me quedará dinero. Puedo llevar a mi novia al baile solo si tengo dinero. Si no la llevo al baile, ella se enojará conmigo. Pero si no le pago al sastre, no me entregará el traje. Sin el traje no puedo llevar a mi novia al baile. Luego, mi novia se enojará conmigo.

4. Verifique que el siguiente argumento no es válido.

$$\begin{array}{l} P \\ P \vee Q \\ Q \rightarrow (R \rightarrow S) \\ T \rightarrow R \\ \hline \quad \therefore \neg S \rightarrow \neg T \end{array}$$

5. A partir de las tres premisas:
   - Los niños son ilógicos.
   - Nadie es despreciado cuando puede domar un cocodrilo.
   - Las personas ilógicas son despreciadas.

   Obtenga como conclusión válida la proposición: *Los niños no pueden domar cocodrilos.*

6. Considere el siguiente razonamiento y demuestre que no es válido: *Una condición necesaria para que se nombre presidente es que la mayoría vote por él y no tenga mala salud. La mayoría votó por él. Tiene buena salud. Por lo tanto, se nombró presidente.*

7. En *Vacilonia* (véase página 38), un día un vacilonio mentiroso afirmó lo siguiente: "*Si en Vacilonia no llueve y las vacas vuelan, entonces los vacilonios no son altos o tienen tres ojos*". Además, un vacilonio sincero afirmó que "*todos los vacilonios tienen tres ojos o tienen cinco ojos*". Con la información anterior, determine si en Vacilonia llueve, si las vacas vuelan, si sus habitantes son altos y cuántos ojos tienen.

8. De acuerdo con el sistema definido en el ejemplo 33, demuestre que son admisibles las palabras MIM, MUIM, MIIIMII, MIU, MUMI, MMIII, MIIIM, MIMUU, MUUIUIMIII. Además, demuestre que no es posible deducir MU.

9. Sean a y b dos números reales. Demuestre que si $a \geq b$ y $a \leq b$, entonces se concluye que $a = b$.

10. Este ejercicio de lógica fue propuesto por Lewis Carroll (véase [8]). En él se sugiere una conclusión a partir de cinco premisas, trate de justificar la conclusión propuesta. Más adelante, cuando tenga un mayor conocimiento de la lógica proposicional, usted encontrará una forma de obtener la conclusión de una manera precisa (ejemplo 46 de la sección 1.6).

    Ningún gato que gusta del pescado es indomesticable.
    Ningún gato sin cola jugará con un gorila.
    Gatos con bigotes siempre gustan del pescado.
    Ningún gato tiene cola a menos que tenga bigotes.
    Ningún gato domesticable tiene ojos grises.

    Conclusión: Los gatos de ojos grises no jugarán con un gorila.

11. Compruebe que si Juan no cumple la promesa: "*el domingo, o no te regalo un libro o te invito a comer*", entonces cumple la promesa "*el domingo te regalo un libro y no te invito a comer*".

12. Lea, disfrute y analice el siguiente texto, tomado de [8]:
    ¿Podrías decirme, por favor, cuál camino debo seguir para salir de

aquí? –preguntó Alicia al Minino de Cheshire–.
–Esto depende en gran parte del sitio al que quieras llegar –dijo el Gato.
–No me importa mucho el sitio... –dijo Alicia.
–Entonces tampoco importa mucho el camino que tomes –dijo el Gato.
– ...siempre que llegue a alguna parte –añadió Alicia.
–¡Oh, siempre llegarás a alguna parte –aseguró el Gato–, si caminas lo suficiente!

A Alicia le pareció que esto no tenía vuelta de hoja y decidió hacer otra pregunta: ¿Qué clase de gente vive por aquí?
–En esta dirección –dijo el Gato, haciendo un gesto con la pata derecha– vive un Sombrerero. Y en esta dirección –e hizo un gesto con la otra pata– vive una Liebre de Marzo. Visita al que quieras: los dos están locos.
–Pero es que a mí no me gusta tratar a gente loca –protestó Alicia.
–Oh, eso no lo puedes evitar –repuso el Gato–. Aquí todos estamos locos. Yo estoy loco. Tú estás loca.
–¿Cómo sabes que yo estoy loca? –preguntó Alicia.
–Tienes que estarlo –afirmó el Gato– o no habrías venido aquí.
Alicia pensó que esto no demostraba nada. Sin embargo, continuó con sus preguntas: –¿Y cómo sabes que tú estás loco?
–Para empezar –repuso el Gato–, los perros no están locos. ¿De acuerdo?
–Supongo que sí –concedió Alicia.
–Muy bien. Pues en tal caso –siguió su razonamiento el Gato–, ya sabes que los perros gruñen cuando están enfadados y mueven la cola cuando están contentos. Pues bien, yo gruño cuando estoy contento y muevo la cola cuando estoy enfadado. Por lo tanto, estoy loco.
–A eso yo le llamo ronronear, no gruñir –dijo Alicia.

1.5 Formas normales

En esta sección se definen las formas normales y se exponen, con base en ejemplos, la manera de determinar la forma normal de una proposición, primero por medio de las leyes, luego mediante las tablas de verdad.

Se dice que una proposición está en su **forma normal disyuntiva** (FND) si está escrita como disyunciones de conjunciones; por ejemplo:

$$\underbrace{\underbrace{(P \wedge Q)}_{\text{conjunción}} \vee \underbrace{(\neg P \wedge R)}_{\text{conjunción}}}_{\text{disyunción}} \tag{1.3}$$

Además, se dice que una proposición está en su **forma normal conjuntiva** (FNC) si está escrita como conjunciones de disyunciones; por ejemplo, note cómo al aplicar la distributividad en (1.3) se obtiene:

$$\underbrace{\underbrace{(P \vee \neg P)}_{\text{disyunción}} \wedge \underbrace{(P \vee R)}_{\text{disyunción}} \wedge \underbrace{(Q \vee \neg P)}_{\text{disyunción}} \wedge \underbrace{(Q \vee R)}_{\text{disyunción}}}_{\text{conjunción}} \tag{1.4}$$

Al estar formada por conjunciones de disyunciones, hace que la expresión (1.4) sea la FNC de (1.3).

Ejemplo 34. *Utilice las leyes de la lógica y determine la forma normal conjuntiva (FNC) de* $\neg\big[(\neg P \wedge \neg Q) \wedge (\neg Q \to R)\big] \wedge (\neg R \to P)$

Solución. Se debe escribir la expresión dada como una conjunción de disyunciones:

$$\begin{array}{cll}
 & \neg\big[(\neg P \wedge \neg Q) \wedge (\neg Q \to R)\big] \wedge (\neg R \to P) & \textbf{Justificación} \\
\equiv & \neg\big[(\neg P \wedge \neg Q) \wedge (Q \vee R)\big] \wedge (R \vee P) & \text{ID} \\
\equiv & \big[\neg(\neg P \wedge \neg Q) \vee \neg(Q \vee R)\big] \wedge (R \vee P) & \text{Morgan} \\
\equiv & \big[(P \vee Q) \vee (\neg Q \wedge \neg R)\big] \wedge (R \vee P) & \text{Morgan} \\
\equiv & \big[(P \vee Q \vee \neg Q) \wedge (P \vee Q \vee \neg R)\big] \wedge (R \vee P) & \text{Distributividad}
\end{array}$$

Es decir, la proposición dada se logró reescribir como la conjunción de $P \vee Q \vee \neg Q$, $P \vee Q \vee \neg R$, y de $R \vee P$, donde cada una de estas tres es una disyunción. De esta forma, la proposición

$$(P \vee Q \vee \neg Q) \wedge (P \vee Q \vee \neg R) \wedge (R \vee P)$$

es la FNC de la proposición dada. ■

La manera de obtener la forma normal completa de una proposición por medio de una tabla de verdad es sencilla; para ello debe tener en cuenta que para la FND, es necesario considerar los casos donde el valor de verdad resultante sea verdadero y hacer verdaderas las proposiciones atómicas que la provocan.

Ejemplo 35. *Determine la FND de la proposición* $(\neg P \wedge Q) \rightarrow (Q \rightarrow P)$.

Solución. La tabla de verdad es:

P	Q	$\neg P$	$\neg P \wedge Q$	$\neg Q$	$\neg Q \vee P$	$(\neg P \wedge Q) \rightarrow (Q \rightarrow P)$
V	***V***	F	F	F	V	***V***
V	***F***	F	F	V	V	***V***
F	V	V	V	F	F	F
F	***F***	V	F	V	V	***V***

Se tienen tres casos donde el valor de verdad es V, así:

$$FND : (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$$

es la forma normal disyuntiva asociada a la expresión dada. ■

Por otro lado, la manera de obtener la FNC por medio de una tabla de verdad también es sencilla; se deben considerar los casos donde el valor de verdad resultante es falso y se hacen falsas las proposiciones atómicas que la provocan.

Ejemplo 36. *Determine la FNC de la proposición* $(\neg P \vee Q) \rightarrow (\neg Q \wedge P)$.

Solución. Al construir la tabla, se obtiene:

P	Q	$\neg P$	$\neg P \vee Q$	$\neg Q$	$\neg Q \wedge P$	$(\neg P \vee Q) \to (\neg Q \wedge P)$
V	***V***	F	V	F	F	***F***
V	F	F	F	V	V	V
F	***V***	V	V	F	F	***F***
F	***F***	V	V	V	F	***F***

Se tienen tres casos donde el valor de verdad es F; estos se utilizan para escribir que $FNC : (\neg P \vee \neg Q) \wedge (P \vee \neg Q) \wedge (P \vee Q)$. ■

Ejemplo 37. *Determine las formas normales, conjuntiva y disyuntiva, de la proposición* $[P \to (Q \vee R)] \leftrightarrow (\neg P \wedge R)$.

Solución. Al construir la tabla, se obtiene:

P	Q	R	$Q \vee R$	$P \to (Q \vee R)$	$\neg P$	$\neg P \wedge R$	$*$
V	V	V	V	V	F	F	F
V	V	F	V	V	F	F	F
V	F	V	V	V	F	F	F
V	F	F	F	F	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	V	V	F	F
F	F	V	V	V	V	V	V
F	F	F	F	V	V	F	F

Se tienen tres casos donde el valor de verdad es verdadero, estos se utilizan para escribir que la FND es:

$$(P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$$

Además, se tienen cinco casos donde el valor de verdad es falso, los cuales se utilizan para escribir la FNC, que es:

$$(\neg P \vee \neg Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$$

■

Ejercicios (sección 1.5)

1. Use las leyes de la lógica y determine la forma normal que se indica:

    (a) FNC de $[(P \wedge Q) \vee (\neg P \vee R)] \vee (Q \wedge R)$

    (b) FND de $(P \rightarrow Q) \wedge R$

    (c) FND de $\neg\big[\neg(\neg P \wedge \neg Q) \vee \neg(Q \rightarrow R)\big] \wedge \neg(R \rightarrow P)$

    (d) FND de $\neg(P \vee \neg Q) \wedge (S \rightarrow T)$

    (e) FNC de $(P \wedge Q) \vee [R \wedge (S \vee T)]$

2. Use tablas de verdad y determine la forma normal que se indica:

    (a) FND y FNC de $(P \rightarrow Q) \wedge R$

    (b) FND de $\big[P \vee \neg(\neg Q \vee \neg S)\big] \vee \neg(\neg Q \rightarrow \neg S)$

    (c) FND y FNC de $\big[\neg(Q \wedge R) \vee P\big] \leftrightarrow \big[(P \rightarrow Q) \rightarrow R\big]$

    (d) FND y FNC de $(P \wedge \neg Q \wedge R) \vee [(P \rightarrow \neg Q) \leftrightarrow (Q \leftrightarrow R)]$

1.6 Cuantificadores

Una **proposición abierta** o **predicado** será una proposición que depende de una o más variables; por ejemplo, se utiliza la expresión $P(n)$ para indicar que la proposición P depende de la variable n, donde n es un elemento arbitrario o **individuo**. A $P(n)$ se le asigna un valor de verdad para cada escogencia de los valores posibles de la variable n.

El conjunto de individuos (personas, ideas, símbolos y otros) que afectan al argumento que se está considerando se llama **universo de discurso** o **dominio**.

Ejemplo 38. *Considere la proposición abierta definida para n, con n un número natural:*

$$P(n): \ 2n+1 \quad \textit{es un número impar}$$

Para $n = 2$ se tiene que $P(2)$ es verdadera, ya que "5 es un número impar" es verdadera; como 7 es un número impar, se tiene que $P(3)$ es verdadero; como 21 es impar, $P(10)$ también es verdadera. Un análisis más cuidadoso indica que para cualquier n que se tome en el conjunto de los números naturales, el residuo al dividir $2n+1$ por 2 siempre será 1, con lo cual siempre será impar, es decir, la proposición será verdadera siempre. ■

Ejemplo 39. *Considere la proposición abierta*

$$P(n): \ n^2-1 \quad \textit{es un número par}$$

definida para un número natural n. Para $n = 2$ se tiene que $P(2)$ es falsa, ya que "$2^2 - 1$ es un número par" es falsa, pues se sabe que 3 es un número impar; como $3^2 - 1 = 8$ es un número par, se tiene que $P(3)$ es verdadero; como $6^2 - 1 = 35$ no es par, $P(6)$ es falso; $P(7)$ es verdadero. Con base en estos valores de verdad, sería posible conjeturar que la proposición será verdadera si n es un número impar y será falsa si n es par. ■

Ejemplo 40. *Considere la proposición abierta*

$$P(a,b,c):\ a^2+b^2=c^2$$

donde a, b, c *son números naturales. Se tiene, por ejemplo, que* $P(3,4,5)$ *es verdadera, ya que* "$3^2+4^2=5^2$" *es una identidad, mientras que* $P(5,6,12)$ *es falsa, ya que* $5^2+6^2=25+36=61\neq 144=12^2$. ■

Las frases "para algún x", "no todos cumplen", "algún n cumple $P(n)$", "ningún x cumple $Q(x)$", de alguna manera cuantifican la cantidad de elementos que satisfacen o no una proposición abierta. Para ello, se definen dos tipos de **cuantificadores**:

- **Cuantificador existencial**, que se lee "para algún x" o "existe al menos un x" o "existe un x tal que". El símbolo del cuantificador existencial es $\exists$; así, la frase "existe un x tal que $P(x)$" se simboliza $\boldsymbol{\exists x P(x)}$.
- **Cuantificador universal**, que se lee "para todo x" o "para cada x". El símbolo del cuantificador universal es $\forall$; así, la frase "todo x cumple $P(x)$" se simboliza $\boldsymbol{\forall x P(x)}$.

La proposición cuantificada $\exists x P(x)$ será verdadera si, para algún a en el universo, $P(a)$ es verdadera. La proposición cuantificada $\forall x P(x)$ será verdadera si $P(a)$ es verdadera para todos los posibles valores de a en el universo. Por otro lado, es usual utilizar el símbolo $\nexists$ para denotar a $\neg\exists$, que en ambos caso se lee "no existe".

En el caso particular de que $\mathcal{U}=\{a_1,a_2,\ldots,a_n\}$, es decir, de un *universo discreto finito*, es posible escribir:

$$\begin{aligned}\exists x P(x) &\equiv P(a_1)\vee P(a_2)\vee\cdots\vee P(a_n)\\ \forall x P(x) &\equiv P(a_1)\wedge P(a_2)\wedge\cdots\wedge P(a_n)\end{aligned}$$

Teorema 1. *Se satisfacen las siguientes equivalencias:*

$$\nexists x\, P(x) \equiv \forall x\, [\neg P(x)] \tag{1.5}$$
$$\neg\big[\forall x\, P(x)\big] \equiv \exists x\, [\neg P(x)] \tag{1.6}$$
$$\forall x\, \big[P(x) \wedge Q(x)\big] \equiv \forall x\, P(x) \wedge \forall x\, Q(x) \tag{1.7}$$
$$\exists x\, \big[P(x) \vee Q(x)\big] \equiv \exists x\, P(x) \vee \exists x\, Q(x) \tag{1.8}$$

Demostración. Se probará la identidad (1.5), las otras cinco se dejan como ejercicio. Para obtener la negación de $\exists x P(x)$, observe que:

$$\begin{aligned} \nexists x P(x) &\equiv \neg\big[\exists x P(x)\big] \\ &\equiv \neg[P(a_1) \vee P(a_2) \vee \cdots \vee P(a_n)] \\ &\equiv \neg P(a_1) \wedge \neg P(a_2) \wedge \cdots \wedge \neg P(a_n) \\ &\equiv \forall x[\neg P(x)] \end{aligned}$$

Es decir, se ha probado la identidad (1.5). □

Corolario 1. *Se satisfacen las siguientes equivalencias:*

$$\exists x\, P(x) \equiv \neg\forall x\, [\neg P(x)] \tag{1.9}$$
$$\forall x\, P(x) \equiv \nexists x\, [\neg P(x)] \tag{1.10}$$

Demostración. Basta negar las equivalencias (1.5) y (1.6). □

Ejemplo 41. *Aplicando la equivalencia* (1.10)*, afirmar que "Todos los hombres son mortales" es quivalente a decir que "No existen hombres no mortales". Por otro lado, al aplicar la equivalencia* (1.5)*, afirmar que "No existe una persona que mida* 20 *metros" es quivalente a decir que "Todas las personas no miden* 20 *metros". Por último, es claro que decir que "Todos los perros ladran y tienen cola" es equivalente a afirmar que "Todos los perros ladran y todos los perros tienen cola", como asevera la equivalencia* (1.7)*.* ■

Ejemplo 42. *Si n es un número natural y "$P(n) : n^2 - 1$ es un número par" es una proposición abierta, se tiene que $\exists x P(x)$ es verdadera, pues $P(3)$ es verdadera; $\forall x P(x)$ es falsa, pues $P(2)$ es falsa.* ■

En el caso de que el universo $\mathcal{U}$ sea un conjunto finito, es decir, $\mathcal{U} = \{a_1, a_2, \ldots, a_n\}$ y se tenga P_1, P_2,. . . , P_m proposiciones abiertas, es posible elaborar la **tabla de asignación de predicados**, en la cual la entrada i-j denota el valor de verdad de $P_j(a_i)$:

	P_1	P_2	$\ldots$	P_j	$\ldots$	P_m
a_1						
a_2						
$\vdots$						
a_i				$P_j(a_i)$		
$\vdots$						
a_n						

Ejemplo 43. *Suponga que se tiene un universo de discurso formado por tres personas: Ana, Bárbara y Carmen, representadas por A, B y C respectivamente. La asignación de los predicados $P(x)$, $Q(x)$, $R(x)$ y $S(x)$ está dada en la siguiente tabla.*

	$P(x)$	$Q(x)$	$R(x)$	$S(x)$
A	V	V	F	F
B	V	F	V	F
C	V	V	F	V

Determine el valor de verdad de las cuatro proposiciones: $\forall x\ [P(x)]$, $\forall x\ \big[R(x) \vee S(x)\big]$, $\exists x\ \big[\neg S(x) \to R(x)\big]$, $\exists x\ \big[(Q(x) \wedge S(x)) \leftrightarrow P(x)\big]$.

Solución. A partir de la tabla dada, se tiene:

- $\forall x\ [P(x)] \equiv P(A)\ \wedge\ P(B)\ \wedge\ P(C) \equiv V \wedge V \wedge V \equiv V$.

- $\forall x\ \big[R(x) \lor S(x)\big] \equiv \big[R(A) \lor S(A)\big] \land \big[R(B) \lor S(B)\big] \land \big[R(C) \lor S(C)\big] \equiv [F \land V \land V] \equiv F$.

- $\exists x\ \big[\neg S(x) \to R(x)\big]$ es una proposición verdadera, pues basta ver que $\big[\neg S(C) \to R(C)\big] \equiv [F \to F] \equiv V$, es decir, Carmen satisface la proposición.

- $\exists x\ \big[(Q(x)\ \land\ S(x))\ \leftrightarrow\ P(x)\big]$ es verdadera, pues basta ver que $\big[(Q(C)\ \land\ S(C)) \leftrightarrow P(C)\big] \equiv [(V \land V) \leftrightarrow V] \equiv V$. Es decir, Carmen cumple la proposición. ■

Ejemplo 44. *Suponga que se tiene un universo de discurso formado por cinco gatos: Mini, Black, Soko, Balín y Terrón. Solo los tres primeros son de pura raza; Mini y Soko comen solo atún, mientras que Black y Balín solo comen pollo. Terrón come pollo y atún, pero no toma leche y los otros sí. Excepto Black, ninguno tiene collar.*

1. *Por medio de una tabla, presente la asignación de los predicados $R(x)$: x es de raza, $CA(x)$: x come atún, $CP(x)$: x come pollo, $TL(x)$: x toma leche, $TC(x)$: x tiene collar.*

2. *Valide las proposiciones $\exists g\ \big[CA(g) \land TC(g)\big]$, $\forall x\ \big[CP(x) \lor TL(x)\big]$, $\forall x\ \big[CP(x)\big] \lor \forall x\ \big[TL(x)\big]$, $\forall x\ \big[CA(x) \to R(x)\big]$.*

3. *Simbolice y valide la proposición: "No todos los gatos comen pollo o, si son de raza, tienen collar".*

Solución. En primer lugar, la tabla:

	$R(x)$	$CA(x)$	$CP(x)$	$TL(x)$	$TC(x)$
Mini	V	V	F	V	F
Black	V	F	V	V	V
Soko	V	V	F	V	F
Balín	F	F	V	V	F
Terrón	F	V	V	F	F

muestra la asignación de predicados y a partir de ella se tiene que:

- $\exists g\ \big[CA(g) \wedge TC(g)\big]$ es falsa, pues no existe ningún gato que coma atún y tenga collar simultáneamente.
- $\forall x\ \big[CP(x) \vee TL(x)\big]$ es verdadera, pues cada uno de los gatos come pollo o toma leche.
- $\forall x\ \big[CP(x)\big] \vee \forall x\ \big[TL(x)\big]$ es falsa, pues la expresión $\forall x\ CP(x)$ es falsa, ya que Mini no come pollo; la expresión $\forall x\ TL(x)$ es falsa, ya que Terrón no toma leche. Así, $\forall x\ CP(x) \vee \forall x\ TL(x) \equiv F \vee F \equiv F$.
- $\forall x\ \big[CA(x) \rightarrow R(x)\big]$ es falsa, pues, como involucra el $\forall$, para que sea verdadera se debe cumplir para todo; sin embargo, para Terrón se tiene que $\big[CA(\text{Terrón}) \rightarrow R(\text{Terrón})\big] \equiv [V \rightarrow F] \equiv F$.

Por último, "No todos los gatos comen pollo o, si son de raza, tienen collar" se simboliza y reescribe como:

$$\begin{aligned} & \neg\forall x\ \big[CP(x) \vee (R(x) \rightarrow TC(x))\big] \\ \equiv\ & \exists x\ \neg\big[CP(x) \vee \neg R(x) \vee TC(x))\big] \\ \equiv\ & \exists x\ \big[\neg CP(x) \wedge R(x) \wedge \neg TC(x))\big] \end{aligned}$$

que claramente satisfacen Mini o Soko, con lo cual es verdadera. ■

Ejemplo 45. *Considere la proposición "Ningún ser humano que sea inteligente luchará contra un elefante" y para x un ser humano, considere las proposiciones abiertas:*

$P(x)$: x *es inteligente*
$Q(x)$: x *luchará contra un elefante*

Así, esta proposición se simboliza como $\neg\exists x\ \big[P(x) \wedge Q(x)\big]$, y utilizando la identidad (1.5) *se tiene que:*

$$\begin{aligned} \neg\exists x\ \big[P(x) \wedge Q(x)\big] &\equiv \forall x\ \neg\big[P(x) \wedge Q(x)\big] \\ &\equiv \forall x\ \big[\neg P(x) \vee \neg Q(x)\big] \\ &\equiv \forall x \big[P(x) \rightarrow \neg Q(x)\big] \end{aligned}$$

De esta manera, la proposición dada inicialmente se puede enunciar también como "Todo ser humano que sea inteligente no luchará contra un elefante" o en un lenguaje más cotidiano, "Si un ser humano es inteligente, no luchará contra un elefante". Equivalentemente, utilizando la contrapositiva

$$\forall x\big[Q(x) \rightarrow \neg P(x)\big]$$

que se puede leer como "Si un ser humano lucha contra un elefante, no es inteligente". ∎

Ejemplo 46. *Simbolice el argumento planteado en el ejercicio* 10 *de la sección* 1.4*.*

Solución. Se debe trabajar con cada una de las proposiciones que se dan. En primer lugar, se hará con la proposición "*Ningún gato que gusta del pescado es indomesticable*", para ello considere las proposiciones abiertas:

$P(x):\quad x$ gusta del pescado
$Q(x):\quad x$ es domesticable

Así, esta primera premisa se simboliza como:

$$\neg\exists x\ \big[P(x) \wedge \neg Q(x)\big]$$

y utilizando la identidad (1.5) se tiene que:

$$\begin{aligned}\forall x\ \big[\neg P(x) \vee Q(x)\big] &\equiv \forall x\big[P(x) \rightarrow Q(x)\big]\\ &\equiv \forall x\ \big[\neg Q(x) \rightarrow \neg P(x)\big]\end{aligned}$$

Es decir, la primera premisa "*Ningún gato que gusta del pescado es indomesticable*" se puede reescribir como "*Los gatos que no pueden ser domesticados no gustan del pescado*". De la misma manera, la segunda proposición "*Ningún gato sin cola jugará con un gorila*" se puede reescribir como "*Los gatos que no tienen cola no jugarán con un gorila*". Repitiendo este análisis para las otras tres premisas y reordenando las cinco en forma análoga a los silogismos, donde la conclusión de una sea la premisa de la siguiente, se tiene:

Los gatos con ojos grises no pueden ser domesticados.

Los gatos que no pueden ser domesticados no gustan del pescado.

Los gatos que no gustan del pescado no tienen bigotes.

Los gatos que no tienen bigotes no tienen cola.

Los gatos que no tienen cola no jugarán con un gorila.

De donde se obtiene, aplicando el Silogismo hipotético, la conclusión: los gatos de ojos grises no jugarán con un gorila. ■

En el caso de una proposición abierta de dos variables $P(x, y)$, se tienen cuatro tipos de proposiciones cuantificadas:

1. $\boldsymbol{\forall x \, \forall y \, P(x, y)}$ significa que cualquier par de elementos del universo satisface la proposición.

2. $\boldsymbol{\exists x \, \forall y \, P(x, y)}$ significa que existe un elemento x tal que para todos los elementos del universo se satisface la proposición. El x que existe debe servir para todos los y.

3. $\boldsymbol{\forall x \, \exists y \, P(x, y)}$ significa que para cada elemento x existe un elemento y tal que se satisface la proposición. Conforme se cambia el x, se puede cambiar y.

4. $\boldsymbol{\exists x \, \exists y \, P(x, y)}$ significa que existe al menos una pareja de elementos que satisface la proposición. Esto no excluye que $x = y$.

Es importante resaltar el hecho de que

$$\forall x \, \exists y \; P(x, y) \not\equiv \exists y \forall x \; P(x, y)$$

es decir, ambas proposiciones no son lógicamente equivalentes. Para comprobar esto, observe los siguientes ejemplos.

Ejemplo 47. *Para x, y números reales. La proposición*

$$\forall x\ \exists y\ [x < y]$$

es verdadera, pues para cada x siempre es posible encontrar un valor de y de manera que $x < y$, es decir, para todo número siempre hay otro mayor que él. Por otro lado, la proposición

$$\exists y\ \forall x\ [x < y]$$

es falsa, pues sugiere que existe un número y que es mayor que todos los números reales, y se sabe que esta afirmación es falsa. ■

Ejemplo 48. *Recuerde que, para el caso de los números reales, el elemento neutro en la multiplicación es el elemento 1, con lo cual*

$$\exists y\ \forall x\ [x \cdot y = x]$$

es una proposición verdadera. Por otro lado, el inverso multiplicativo de cualquier número real diferente de 0 también existe, de esta forma

$$\forall x\ \exists y\ [x \cdot y = 1]$$

es una proposiciónes verdadera si $x \neq 0$. ■

Es decir, el elemento neutro para la multiplicación en los números reales existe, se conoce como *uno*, se denota por 1 y funciona para todos, de manera que al multiplicarlo por cualquier número real no lo altera; mientras que el elemento inverso cambia para cada elemento; por ejemplo, el inverso multiplicativo de $\frac{3}{4}$ es $\frac{4}{3}$ y se simboliza como $\left(\frac{3}{4}\right)^{-1} = \frac{4}{3}$.

Ejemplo 49. *De nuevo, para el caso de los números reales, el número 0 es el elemento absorbente de la multiplicación, ya que $0 \cdot x = 0$ para todo x en $\mathbb{R}$. Con lo cual, la proposición*

$$\exists y\ \forall x\ [y \cdot x = y]$$

es verdadera. Además, la adición no tiene elemento absorbente, ya que no existe un elemento único y *que cumpla* $y + x = y$ *para todo* x *en* $\mathbb{R}$*, con lo cual, la proposición*

$$\exists y \, \forall x \, [y + x = y]$$

es falsa. ■

Ejemplo 50. *Si se considera el conjunto de los números reales como universo, la proposición*

$$\forall x \, \exists y \, [2x + 3y = 1]$$

es verdadera, pues al fijar un valor de x*, basta tomar* $y = \frac{1-2x}{3}$ *para calcular*

$$2x + 3y = 2x + 3\left(\frac{1-2x}{3}\right) = 2x + 1 - 2x = 1$$

con lo cual es claro que se satisface la condición. ■

Debe observarse que el universo escogido es vital para la validez o invalidez de una proposición; para esto, observe que en el ejemplo anterior, con solo tomar como universo el conjunto $\mathbb{Z}$, la proposición $\forall x \; \exists y \; [2x + 3y = 1]$ sería falsa, pues $y = \frac{1-2x}{3}$ no necesariamente pertenece a $\mathbb{Z}$.

Ejemplo 51. *Demuestre, por contradicción, la validez de la proposición*

$$\forall x \in \mathbb{N}\big[7x + 4 < 40 \; \vee \; \forall \, y \in \mathbb{N}(x + y \neq 5)\big]$$

Solución. Asuma, razonando por contradicción, que la negación de esta proposición es verdadera, es decir, se asume la validez de:

$$\neg\forall x \in \mathbb{N}\big[7x + 4 < 40 \; \vee \; \forall \, y \in \mathbb{N}(x + y \neq 5)\big]$$

Al aplicar el teorema 1, se obtiene:

$$\begin{aligned} & \exists x \in \mathbb{N} \neg \big[7x + 4 < 40 \ \vee \ \forall\, y \in \mathbb{N}(x + y \neq 5) \big] \\ \equiv \quad & \exists x \in \mathbb{N} \big[7x + 4 \geq 40 \ \wedge \ \exists\, y \in \mathbb{N}(x + y = 5) \big] \end{aligned}$$

Es decir, se ha asumido que existe un número natural x que cumple con las proposiciones $7x + 4 \geq 40$ y $\exists\, y \in \mathbb{N}(x + y = 5)$. De la primera se obtiene que $x \geq \frac{36}{7}$, y como x es natural, se debe tener que $x \geq 6$. Como y también es natural, se concluye que $x + y \geq 6$, es decir, se ha demostrado que $5 = x + y \geq 6$, con lo cual $5 \geq 6$, que claramente es una contradicción. Por lo tanto, lo que se asumió es falso; entonces, se ha probado que la proposición dada es verdadera. ■

Ejercicios (sección 1.6)

1. Simbolice completamente las siguientes proposiciones, utilizando predicados, términos, conectivas y cuantificadores:

   (a) Para todo a y b números reales positivos existe un número entero n tal que na es mayor o igual que b.

   (b) Existe un número natural mayor que 5, de manera que su triple o su cuadrado sea menor que 30 y mayor que 20.

   (c) Existen tres números reales de manera que la suma de los dos primeros es igual a la suma del tercero más 4.

   (d) Para todo número real positivo x existe al menos un número natural n diferente de cero, tal que el inverso multiplicativo de n es menor que x.

   (e) Para todo número natural a y para todo número natural b, a y b son primos relativos si y sólo si el máximo común divisor de a y b es igual a uno.

   (f) Todo número natural n es divisible por 3 si existe un número natural k, de manera que el producto de 3 y k sea n.

(g) No existe un número real que sea mayor que todos los reales.

(h) Si el entero n es divisible por 2 y el entero m es divisible por 3, entonces el producto de m y n es divisible por 6.

(i) Existe un número real que al elevarlo al cuadrado dé -1.

(j) No existe un número racional tal que su cuadrado sea 2.

(k) Entre dos números racionales existe un número irracional.

2. Suponga que se tiene un universo de discurso formado por cinco personas: Juan, Raquel, Pedro, Rosa y Francis. Solamente las tres primeras son casadas. Pedro y Raquel tienen casa propia, mientras que Juan, Rosa y Francis alquilan casa. Solo Pedro y Rosa tienen automóvil propio. Todos, excepto Pedro, estudian en la universidad.

   (a) Presente la tabla de asignación de los predicados $C(x)$: x es casado, $CP(x)$: x tiene casa propia, $AC(x)$: x alquila casa, $AP(x)$: x tiene automóvil propio, $E(x)$: x estudia en la universidad.

   (b) Valide las proposiciones

      i. $\exists x\big[C(x) \wedge CP(x) \wedge AP(x)\big]$

      ii. $\forall x\big[CP(x) \vee E(x)\big]$

      iii. $\forall x\big[CP(x)\big] \vee \forall x\big[E(x)\big]$

      iv. $\forall x\big[C(x) \rightarrow \big(CP(x) \vee AC(x)\big)\big]$

3. Escriba y simplifique la negación de las siguientes proposiciones:

   (a) $(\forall n \in \mathbb{N})\big[n^2 - 2n + 5 \geq 4\big]$

   (b) $(\exists x \in \mathbb{R})\big[x > 2 \rightarrow x^2 \leq 5\big]$

   (c) $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})\big[n > x \ \vee \ nx \leq 0\big]$

4. Simbolice, escriba y simplifique la negación de las proposiciones siguientes:

(a) Todos los estudiantes de la universidad estudian medicina y no practican deporte.

(b) Todos los miembros del club tienen más de 30 años.

(c) Algunos de los personajes de la novela saben inglés o francés.

5. Para x entero, considere las siguientes proposiciones abiertas:
   $P(x): \ 2 < x \leq 10$
   $Q(x): \ x$ es número impar
   $R(x): \ x$ es número primo
   $S(x): \ 4x - 1$ es divisible por 3
   $T(x): \ x$ se puede escribir como la suma de dos primos
   Determine el valor de verdad de las siguientes proposiciones:

   (a) $(\exists x \in \mathbb{N}) \left[P(x) \wedge Q(x) \wedge \neg R(x)\right]$
   (b) $(\exists x \in \mathbb{N}) \left[P(x) \wedge R(x) \wedge S(x)\right]$
   (c) $(\forall x \in \mathbb{N}) \left[P(x) \rightarrow \big(Q(x) \vee \neg R(x)\big)\right]$
   (d) $(\forall x \in \mathbb{N}) \left[(P(x) \wedge Q(x) \wedge R(x)) \rightarrow \neg S(x)\right]$
   (e) $(\forall x \in \mathbb{N}) \left[(P(x) \wedge \neg Q(x)) \rightarrow T(x+2)\right]$

6. Determine el valor de verdad de las siguientes proposiciones:

   (a) $(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z}) \left[x = y + 1\right]$
   (b) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z}) \left[x = y + 1\right]$
   (c) $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R}) \left[2x + 3y = 1\right]$
   (d) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R}) \left[2x + 3y = 1\right]$
   (e) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z}) \left[2x + 3y = 1\right]$
   (f) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R}) \left[xy = 0\right]$
   (g) $\big(\forall x \in \,]0, +\infty[\big)(\exists y \in \mathbb{R}) \left[0 < y < x\right]$

7. Considere $A = \{2, 3, 4, 5, 6, 7\}$ y las proposiciones abiertas

$$\begin{aligned} P(x) &: \ x + 1 \text{ es un número primo} \\ Q(x) &: \ x^2 + x \text{ es un número impar} \end{aligned}$$

Determine el valor de verdad de las proposiciones:

(a) $\forall x \in \mathbb{N}\left[x \in A \to x < 9\right] \wedge \exists x \in \mathbb{N}\left[x \notin A \wedge P(2x)\right]$

(b) $\exists x \in A\left[P(2x-1) \leftrightarrow Q(x+1)\right]$

(c) $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})\left[x \in A \to (Q(x) \vee P(x+y))\right]$

8. Simbolice la proposición "Ningún conejo que gusta de la poesía es indomesticable"; además, encuentre una equivalencia donde se utilice el cuantificador $\forall$.

9. Demuestre la validez de las siguientes proposiciones:

   (a) $\forall x \in \mathbb{N}\ \left[x < 7 \ \vee\ x^2 \geq 40\right]$

   (b) $\forall x \in \mathbb{N}\ \left[4x < 27 \to x^2 + 1 \leq 38\right]$

10. Para n un número entero, considere las siguientes definiciones:
    $D1$: n es par si y solo si $\exists k \in \mathbb{Z}$ tal que $n = 2k$.
    $D2$: n es impar si y solo si $\exists k \in \mathbb{Z}$ tal que $n = 2k+1$.
    Demuestre las siguientes proposiciones:

    (a) n^2 es par si y solo si n es par.

    (b) n^2 es impar si y solo si n es impar.

    (c) Si n es impar, entonces $3n^2 + 7n + 5$ es impar.

    (d) $n^2 + 3n + 2$ es par.

    (e) Si $n + m$ es par, entonces $n^2 + m^2$ también es par.

11. Es claro que la afirmación "Todo ejemplo es un contraejemplo" es falsa. ¿Cuál sería un contraejemplo de esta afirmación?

12. Hay una "regla" que dice: *toda regla tiene su excepción*. Si esta regla fuera verdadera, ella misma tendría una excepción, ¿cuál sería esta excepción?, ¿qué se puede concluir?

13. Obtenga la negación y simplifique la siguiente proposición:

$$(\forall \epsilon > 0)(\exists \delta > 0)\big[x < \delta \rightarrow f(x) < \epsilon\big]$$

14. Demuestre, por contradicción, el siguiente teorema:

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})\Big[6x + 9y = 101 \rightarrow x \notin \mathbb{Z} \vee y \notin \mathbb{Z}\Big]$$

15. Si p es un número primo, con $p > 2$, pruebe que $2^p + p^2$ es impar.

16. Suponga que se tiene una cantidad de puntos y de rectas que satisfacen los axiomas:
    $A1$: cada par de rectas tiene un punto en común.
    $A2$: todo punto está exactamente sobre dos rectas.
    $A3$: hay exactamente cuatro rectas en el sistema.
    Obtenga una representación geométrica de este sistema de puntos y rectas.

17. Demuestre la validez de la proposición:

$$\big[(\forall\ a, b \in \mathbb{R})\ ax + by = 0\big] \rightarrow (x = 0\ \wedge\ y = 0)$$

18. Determine el valor de verdad de la proposición:

$$(\forall\ a, b \in \mathbb{R})\ \big[ax + by = 0 \rightarrow (x = 0\ \wedge\ y = 0)\big]$$

    y compare con el ejercicio anterior.

19. Si $f(x) = 3x - 2$, demuestre la validez de la proposición:

$$(\forall \epsilon > 0)(\exists \delta > 0)\big[|x - 2| < \delta \rightarrow |f(x) - 4| < \epsilon\big]$$

1.7 Inferencias cuantificadas

Para verificar la validez de argumentos con proposiciones cuantificadas, a continuación se presentan tres argumentos básicos cuya demostración se omite. Sin embargo, se puede realizar como ejercicio. El primero es:

$$\forall x \left[P(x) \to Q(x)\right] \land \forall x \left[Q(x) \to R(x)\right] \Longrightarrow \forall x \left[P(x) \to R(x)\right] \tag{1.11}$$

Por claridad, en ocasiones se recomienda utilizar la notación vertical, que en el caso del argumento (1.11) se reescribe como:

$$\begin{array}{ll} 1. & \forall x \left[P(x) \to Q(x)\right] \\ 2. & \forall x \left[Q(x) \to R(x)\right] \\ \hline & \therefore \forall x \left[P(x) \to R(x)\right] \end{array}$$

Como segundo argumento válido se tiene:

$$\exists x \left[P(x) \to Q(x)\right] \land \forall x \left[Q(x) \to R(x)\right] \Longrightarrow \exists x \left[P(x) \to R(x)\right] \tag{1.12}$$

es decir,

$$\begin{array}{ll} 1. & \exists x \left[P(x) \to Q(x)\right] \\ 2. & \forall x \left[Q(x) \to R(x)\right] \\ \hline & \therefore \exists x \left[P(x) \to R(x)\right] \end{array}$$

Como tercer argumento válido se tiene:

$$\forall x \left[P(x) \to Q(x)\right] \land \exists x \left[Q(x) \to R(x)\right] \Longrightarrow \exists x \left[P(x) \to R(x)\right] \tag{1.13}$$

que, de la misma forma, se reescribe como:

$$\begin{array}{ll} 1. & \forall x \left[P(x) \to Q(x)\right] \\ 2. & \exists x \left[Q(x) \to R(x)\right] \\ \hline & \therefore \exists x \left[P(x) \to R(x)\right] \end{array}$$

En este momento, es importante aclarar que la proposición

$$\exists x\ \big[P(x) \rightarrow Q(x)\big] \land \exists x\ \big[Q(x) \rightarrow R(x)\big] \longrightarrow \exists x\ \big[P(x) \rightarrow R(x)\big]$$

no es una tautología, pues el individuo del universo que satisface la primer proposición no necesariamente satisface la segunda, por lo que no se puede garantizar la existencia de un individuo que satisfaga ambas y así aplicar *modus ponens* para obtener la conclusión. Por lo anterior, al no ser verdadera, no se puede utilizar como un teorema.

Ejemplo 52. *Demuestre la validez del siguiente argumento:*

$$\begin{array}{ll} 1. & \exists x\ \big[P(x) \rightarrow Q(x)\big] \\ 2. & \nexists x\ \big[R(x) \land S(x)\big] \\ 3. & \forall x\ \big[Q(x) \rightarrow S(x)\big] \\ \hline & \therefore \exists x\ \big[P(x) \rightarrow \neg R(x)\big] \end{array}$$

Solución. Utilizando los teoremas y las reglas de inferencia ya estudiadas, se tiene:

1.	$\exists x\ \big[P(x) \rightarrow Q(x)\big]$	Premisa
2.	$\nexists x\ \big[R(x) \land S(x)\big]$	Premisa
3.	$\forall x\ \big[Q(x) \rightarrow S(x)\big]$	Premisa
4.	$\forall x\ \big[\neg(R(x) \land S(x))\big]$	Teorema 1(pág. 83) a 2.
5.	$\forall x\ \big[\neg R(x) \lor \neg S(x)\big]$	De Morgan a 4.
6.	$\forall x\ \big[S(x) \rightarrow \neg R(x)\big]$	ID a 5.
7.	$\exists x\ \big[P(x) \rightarrow S(x)\big]$	(1.12) a 1. y 3.
8.	$\exists x\ \big[P(x) \rightarrow \neg R(x)\big]$	(1.13) a 6. y 7.

como se quería probar. ■

Ejercicios (sección 1.7)

1. Demuestre la validez de los siguientes argumentos:

(a)
$$\begin{array}{rl} 1. & \nexists x\ \big[R(x) \wedge \neg S(x)\big] \\ 2. & \forall x\ \big[P(x) \to Q(x)\big] \\ 3. & \forall x\ \big[Q(x) \to \neg S(x)\big] \\ \hline & \therefore\ \forall x\ \big[P(x) \to \neg R(x)\big] \end{array}$$

(b)
$$\begin{array}{rl} 1. & \forall x\ \big[\neg Q(x) \to \neg P(x)\big] \\ 2. & \forall x\ \big[Q(x) \to (R(x) \wedge S(x))\big] \\ 3. & \nexists x\ \big[\neg P(x) \vee \neg T(x)\big] \\ \hline & \therefore\ \forall x\ S(x) \end{array}$$

(c)
$$\begin{array}{rl} 1. & \nexists x\ \big[P(x) \wedge R(x)\big] \\ 2. & \nexists x\ \big[Q(x) \wedge \neg R(x)\big] \\ 3. & \forall x\ \big[S(x) \to P(x)\big] \\ \hline & \therefore\ \forall x\ \big[S(x) \to \neg Q(x)\big] \end{array}$$

(d)
$$\begin{array}{rl} 1. & \exists x\ \big[P(x) \wedge Q(x)\big] \\ 2. & \nexists x\ \big[R(x) \wedge Q(x)\big] \\ 3. & \forall x\ \big[\big(P(x) \wedge \neg R(x)\big) \to T(x)\big] \\ \hline & \therefore\ \exists x\ T(x) \end{array}$$

2. Para x, y, z variables reales, F, G proposiciones abiertas en una variable y H, I proposiciones abiertas en dos variables, compruebe la validez de las siguientes equivalencias:

   (a) $\neg\exists x\ \forall y\ \big[x \geq y\ \vee\ x - y = 2\big] \equiv \forall x\ \exists y\ \big[x < y\ \wedge\ x - y \neq 2\big]$

   (b) $\exists x\ H(x,2) \to \big(G(8) \to F(3)\big) \equiv \neg G(8) \vee F(3) \vee \forall x\big[\neg H(x,2)\big]$

   (c) $\forall x\big[\exists y\ H(x,y) \to \forall z\ I(x,z)\big] \equiv \forall x\big[\exists z \neg I(x,z) \to \forall y \neg H(x,y)\big]$

1.8 Métodos de demostración

"Si no cambias de dirección,
llegarás exactamente donde querías llegar".

Proverbio chino

A lo largo del texto se utilizan varios tipos de demostraciones formales y en esta sección se describen los principales métodos de demostración que, en general, servirán para verificar si una proposición lógica es verdadera y, con ello, determinar la validez de un argumento. Estos métodos no se inscriben solamente dentro de los temas aquí tratados; por el contrario, son de gran utilidad en campos como la geometría, el análisis y la probabilidad, entre otros. Además de esta breve descripción, se profundiza sobre algunos aspectos didácticos acerca de la enseñanza de la demostración y sobre la demostración de implicaciones, con especial interés en tres de los métodos. Para el desarrollo de esta sección, se contó con la valiosa colaboración del M.Sc. Geovanny Sanabria Brenes[2].

Las demostraciones, consideradas problemas de conclusión conocida, engendran en el estudiante una nueva concepción de matemática muy distinta a la presente en secundaria. En ésta se introducen conceptos desconocidos en su mayoría: axiomas, teoremas, definiciones. . . ; además, se introduce la práctica de habilidades: conjeturar, realizar un contraejemplo, inducir, deducir, justificar y generalizar.

Durante el primer año de estudio en carreras afines a la de matemática, usualmente se estudia la enseñanza de la demostración, en donde se quiere ver a la matemática, en su esencia y estructura, como una disciplina que se encarga de formular, estructurar y sintetizar modelos generales con los cuales se pueden simular, representar y luego resolver diversos problemas. El éxito que tenga el estudiante es, sin duda, proporcional al aprendizaje y desarrollo de estas habilidades. Por lo

[2]Profesor de la Escuela de Matemática del Instituto Tecnológico de Costa Rica. Correo electrónico: gsanabria@itcr.ac.cr

tanto, es importante educar a los estudiantes en la forma de articular sus pensamientos para resolver un problema de conclusión conocida, y una forma de lograrlo es mediante una comprensión adecuada de los métodos de demostración.

1. **Demostración por tablas de verdad**
   Se obtiene una tabla de verdad para todos los casos posibles de asignación de valores de verdad para las proposiciones atómicas involucradas. La proposición compuesta dada será verdadera si en la tabla se observa que es una tautología, es decir, a la proposición se le asigna un valor verdadero en todos los casos.

2. **Demostración de proposiciones $\neg \boldsymbol{P}$**
   Se debe probar que P es falsa.

3. **Demostración de proposiciones $\boldsymbol{P} \vee \boldsymbol{Q}$**
   Se puede hacer demostrando que una de las dos proposiciones P o Q es verdadera.

4. **Demostración de proposiciones $\boldsymbol{P} \wedge \boldsymbol{Q}$**
   Se debe probar, en forma independiente, que tanto P como Q son verdaderas. Es básicamente la regla de inferencia conocida como *adjunción* (véase página 64).

5. **Demostración de proposiciones $\boldsymbol{H} \Rightarrow \boldsymbol{C}$**
   Esto equivale a probar, como ya se ha mencionado, que $H \to C$ es una tautología. La mayoría de los teoremas en las distintas teorías matemáticas es de este tipo; por ejemplo, en el álgebra usual de los números reales se tiene que "si $a \neq 0$, entonces $a^0 = 1$", y en geometría, "si un triángulo es equilátero y l es la longitud de su lado, entonces su área es $\frac{l^2\sqrt{3}}{4}$" son resultados que siempre se cumplen y, por lo tanto, son teoremas. Usualmente, los métodos de demostración de implicaciones se estudian por medio de la enseñanza de teoría de conjuntos con proposiciones como "Si $A \subseteq B$, entonces

$A \cap B = A$", o de la teoría de números con teoremas como "Si p es primo, entonces $2^{p-1}(2^p - 1)$ es un número perfecto". Aunque los dos resultados anteriores son del tipo condicional, es importante aclarar que algunas, como la igualdad $(a+b)^2 = a^2 + 2ab + b^2$, es verdadera si a y b son números reales, pero será falsa si, por ejemplo, a y b son matrices. Así, la proposición anterior será verdadera para algunos objetos matemáticos, y sobre ellos se tienen axiomas, definiciones y otros resultados que pasarán a formar parte de las hipótesis aunque no se escriban explícitamente. Se denomina a H como la **hipótesis** (proposición cuyo valor de verdad se asume) y a C la **conclusión** (proposición cuyo valor de verdad se desea averiguar). En un proceso de demostración de $H \Rightarrow C$ se utilizan, además de H, otras "hipótesis" que no son mencionadas, éstas pueden ser axiomas o teoremas, incluso fórmulas válidas o nociones comunes (véase página 30). Se tienen los siguientes métodos de demostración de implicaciones:

(a) **Prueba directa**
En este método se parte de que H es verdadera, y por medio de las reglas de inferencias, leyes de la lógica, axiomas, definiciones, y probablemente otros resultados o teoremas ya probados, se deduce que C es verdadero. Un modelo para éste es:

Hipótesis: H
Hay que mostrar (hqm): C
Se supone H verdadero

1)	H es verdadero	(hipótesis)
2)	$\Rightarrow C_1$ es verdadero	(Justificación)
$\vdots$	$\vdots$	$\vdots$
n)	$\Rightarrow C_n$ es verdadero	(Justificación)
$n+1$)	$\Rightarrow C$ es verdadero	(Justificación)

Es conveniente justificar cada deducción, indicando entre paréntesis, las reglas, axiomas o teoremas en que se basó.

(b) **Prueba indirecta**
Se prueba la contrapositiva (véase página 58), es decir, se prueba la proposición $\neg C \Rightarrow \neg H$ que, como se sabe, es lógicamente equivalente a $H \Rightarrow C$.

(c) **Prueba por contradicción**
Si se quiere probar la proposición C, se asume que es falsa (o equivalentemente $\neg C$ es verdadera) y si se logra probar que se contradice con alguna de las premisas, leyes u otros teoremas ya probados, se concluye que C no puede ser falsa y, por el principio del Tercero Excluido (véase página 44), C debe ser verdadera. Este método sigue el modelo:

Hipótesis: H (se asume verdadera pero no se usa)
Hay que mostrar (hqm) : C
Suponga por contradicción $\neg C$ es verdadero
Utilizando axiomas, definiciones o teoremas, se obtienen las siguientes deducciones:

$$\begin{aligned} &\neg C \text{ es verdadero} \\ \Rightarrow\ &I_1 \text{ es verdadero} \\ &\vdots \\ \Rightarrow\ &I_n \text{ es verdadero} \\ \Rightarrow\ &\neg H \text{ es verdadero} \end{aligned}$$

Pero H se asume verdadero, por lo que se llega a una contradicción ($\Rightarrow\Leftarrow$). Por lo tanto, lo supuesto $(\neg C)$ es falso, es decir, C es verdadero.

(d) **Prueba por reducción al absurdo**
En éste se usa la hipótesis y la negación de la conclusión para obtener un absurdo, es decir, una proposición que es falsa. Cuando se realiza una prueba utilizando reducción al absurdo, se suele seguir el siguiente modelo:

Hipótesis: H (se asume verdadera y se usa)
Hay que mostrar (hqm): C
Suponga por contradicción $\neg C$ es verdadero
Entonces $\neg C \wedge H$ es verdadero (adjunción de la hipótesis)
Utilizando axiomas, definiciones o teoremas, se obtienen las siguientes deducciones:

$$\begin{array}{l} \quad \neg C \wedge H \text{ es verdadero} \\ \Rightarrow I_1 \text{ es verdadero} \\ \Rightarrow I_2 \text{ es verdadero} \\ \quad \vdots \\ \Rightarrow I_n \text{ es verdadero} \\ \Rightarrow F_0 \text{ es verdadero} \quad (\text{pero } F_0 \text{ es falsa}) \\ \quad (\Rightarrow\Leftarrow)\,. \end{array}$$

Note que el supuesto $\neg C$ lleva a un absurdo
Por lo tanto, lo supuesto $\neg C$ es falso, así: C es verdadero.

Este método se suele confundir con el de contradicción. La diferencia es que en éste último se utilizan la hipótesis y la negación de la conclusión para llegar a un absurdo.

(e) **Prueba vacía**
Se prueba estableciendo que el valor de verdad de H siempre es falso.

(f) **Prueba trivial**
Se prueba estableciendo que el valor de verdad de C siempre es verdadero.

6. **Demostración de proposiciones $P \Rightarrow (Q \Rightarrow R)$**
Se puede utilizar la Ley de Exportación (véase página 58), y se puede probar que la proposición $(P \wedge Q) \Rightarrow R$ es verdadera, es decir, a partir de las premisas P y Q se prueba la validez de R.

7. **Demostración de proposiciones $P \Leftrightarrow Q$**
Esto equivale a probar, como ya se ha mencionado, que $P \leftrightarrow Q$ es una tautología. En este caso se debe probar $P \Rightarrow Q$, y además

se debe probar $Q \Rightarrow P$. Muchos de los resultados en matemáticas son de este tipo; por ejemplo, el conocido Teorema de Pitágoras afirma que "En un triángulo rectángulo se cumple que la suma del cuadrado de los catetos es igual al cuadrado de la hipotenusa", pero además afirma que "si a, b y c son las medidas de los lados de un triángulo y se cumple que $a^2 + b^2 = c^2$, entonces el triángulo es rectángulo".

8. **Demostración de proposiciones $\exists x\ [P(x)]$**
   Basta determinar un valor o elemento x del universo relativo para el cual $P(x)$ es cierta.

9. **Demostración de proposiciones $\forall x\ [P(x)]$**
   Se debe tomar un x arbitrario en el universo, sin asignarle un valor específico, y probar que este satisface la proposición $P(x)$.

10. **Demostración de proposiciones $\forall n \in \mathbb{N}\ [P(n)]$**
    En este caso, se puede recurrir al método de Inducción matemática dado en la sección 5.2.

11. **Contraejemplos**. Un ejemplo donde se muestra que la proposición no es verdadera, es decir, que es falsa, se conoce como un contraejemplo de la proposición.

Ahora se presentan algunos ejemplos en donde se utilizan tres de los métodos expuestos para la demostración de implicaciones lógicas.

Ejemplo 53. *Sea A un conjunto de números reales que cumple las siguientes proposiciones (axiomas):*

$$\begin{aligned}
&\textit{Axioma } 1. \quad 3 \in A \\
&\textit{Axioma } 2. \quad x \in A \Rightarrow 3x + 1 \in A \\
&\textit{Axioma } 3. \quad x \in A \ \wedge \ y \in A \Rightarrow (x + y) \in A
\end{aligned}$$

Demuestre los siguientes teoremas utilizando el método directo.

Teorema 1. *Si* $7 \in A$*, entonces* $25 \in A$.

Demostración. **Hipótesis:** $7 \in A$

hqm: $25 \in A$

1. $7 \in A$ (Premisa)
2. $\Rightarrow 3 \cdot 7 + 1 = 22 \in A$ (Axioma 2)
3. $\Rightarrow 22 \in A \ \wedge \ 3 \in A$ (Adjunción de axioma 1)
4. $\Rightarrow 25 \in A$ (Axioma 3) □

Teorema 2. *Si* $2 \in A$*, entonces* $27 \in A$.

Demostración. **Hipótesis:** $2 \in A$

hqm: $27 \in A$

1. $2 \in A$ (Premisa)
2. $\Rightarrow 3 \cdot 2 + 1 = 7 \in A$ (Axioma 2)
3. $\Rightarrow 25 \in A$ (Teorema 1)
4. $\Rightarrow 25 \in A \ \wedge \ 2 \in A$ (Adjunción de 1.)
5. $\Rightarrow 27 \in A$ (Axioma 3) □

Con ello se han probado los dos teoremas propuestos. Note cómo para la demostración del teorema 2 *se utilizó el teorema* 1. ■

Ejemplo 54. *Sea* A *un conjunto de números reales que cumple las siguientes proposiciones (axiomas):*

$$\textit{Axioma } 1. \quad 5 \in A$$

$$\textit{Axioma } 2. \quad x \in A \ \wedge \ y \in A \Rightarrow (x + y) \in A$$

Utilice el método de contradicción para demostrar las proposiciones:

Teorema 1. *Si* $13 \notin A$*, entonces* $4 \notin A$.

Demostración. **Hipótesis:** $13 \notin A$

hqm: $4 \notin A$

1. $4 \in A$
2. $\Rightarrow 4 \in A \ \wedge \ 4 \in A$ (Idempotencia)

3. $\quad 4+4=8 \in A$ (Axioma 2)
4. $\Rightarrow 8 \in A \ \wedge \ 5 \in A$ (Adjunción del axioma 1)
5. $\Rightarrow 13 \in A$ (Axioma 2)

$(\Rightarrow\Leftarrow)$ Contradice la hipótesis

Por lo tanto, lo supuesto es falso, es decir:

$\therefore \ 4 \notin A$ $\square$

Teorema 2. *Si* $(3x-6) \notin A$, *entonces* $(x \notin A \ \vee \ -11 \notin A)$.
Demostración. **Hipótesis:** $(3x-6) \notin A$

hqm: $(x \notin A \ \vee \ -11 \notin A)$

Suponga por contradicción que: $x \in A \ \wedge \ -11 \in A$

1. $\quad x \in A \ \wedge \ -11 \in A$
2. $\Rightarrow 2x \in A \ \wedge \ -11 \in A$ (Axioma 2)
3. $\Rightarrow 3x \in A \ \wedge \ -11 \in A$ (Axioma 2 : a 1 *y* 2)
4. $\Rightarrow (3x-11) \in A$ (Axioma 2)
5. $\Rightarrow (3x-11) \in A \ \wedge \ 5 \in A$ (Adjunción del axioma 1)
6. $\Rightarrow (3x-6) \in A$ (Axioma 2)

$(\Rightarrow\Leftarrow)$ Contradice la hipótesis

Por lo tanto, lo supuesto es falso, es decir:

$\therefore \ x \notin A \ \vee \ -11 \notin A$ $\square$

Así, se probaron los dos teoremas, que son independientes entre sí, pues para la prueba de cada uno no se utiliza el resultado del otro. $\blacksquare$

En el siguiente ejemplo se darán algunos axiomas y con el método de reducción al absurdo se demostrarán dos teoremas que, de nuevo, serán independientes entre sí.

Ejemplo 55. *Sea* B *un conjunto de números reales que cumple las siguientes proposiciones (axiomas):*

Axioma 1. $\quad 3 \in B$

Axioma 2. $\quad x \in B \ \wedge \ y \in B \Rightarrow xy \in B$

Axioma 3. $\quad 6 \notin B$

Pruebe los siguientes dos teoremas utilizando la reducción al absurdo.

Teorema 1. *Si* $\frac{5}{2} \in B$, *entonces* $\frac{4}{5} \notin B$.

Demostración. **Hipótesis:** $\frac{5}{2} \in B$
hqm: $\frac{4}{5} \notin B$
Suponga por contradicción que: $\frac{4}{5} \in B$
1. $\frac{4}{5} \in B$
2. $\Rightarrow \frac{4}{5} \in B \ \wedge \ \frac{5}{2} \in B$ (Adjunción de la hipótesis)
3. $\Rightarrow \frac{4}{5} \cdot \frac{5}{2} \in B$ (Axioma 2)
4. $\Rightarrow 2 \in B$ (Simplificación en 3)
5. $\Rightarrow 2 \in B \ \wedge \ 3 \in B$ (Adjunción del axioma 1)
6. $\Rightarrow 6 \in B$ (Axioma 2)

$(\Rightarrow\Leftarrow)$ (Absurdo: contradice el axioma 3)

Por lo tanto, lo supuesto es falso, es decir, $\frac{4}{5} \notin B$. □

Teorema 2. *Si* $\frac{1}{x} \in B$, *entonces* $\sqrt{2}\,x \notin B$.

Demostración. **Hipótesis:** $\frac{1}{x} \in B$
hqm: $\sqrt{2}\,x \notin B$
Suponga por contradicción que: $\sqrt{2}\,x \in B$
1. $\sqrt{2}\,x \in B$
2. $\Rightarrow \sqrt{2}\,x \in B \ \wedge \ \frac{1}{x} \in B$ (Adjunción de la hipótesis)
3. $\Rightarrow \sqrt{2}\,x \cdot \frac{1}{x} \in B$ (Axioma 2)
4. $\Rightarrow \sqrt{2} \in B$ (Simplificación en 3)
5. $\Rightarrow \sqrt{2} \cdot \sqrt{2} \in B$ (Axioma 2)
6. $\Rightarrow 2 \in B$ (propiedad de radicales a 5)
7. $\Rightarrow 2 \in B \ \wedge \ 3 \in B$ (Adjunción del axioma 1)
8. $\Rightarrow 6 \in B$ (Axioma 2)

$(\Rightarrow\Leftarrow)$ (Absurdo: contradice el axioma 3)

Por lo tanto, lo supuesto es falso, es decir, $\sqrt{2}\,x \notin B$. □

Con ello se han probado los dos teoremas con el método de reducción al absurdo. Note cómo ellos son independientes entre sí. ■

Ejercicios (sección 1.8)

Sea A un conjunto de números reales que cumple las proposiciones:

$$\begin{aligned} \text{Axioma I}: &\quad 5 \in A \\ \text{Axioma II}: &\quad x \in A \Rightarrow 3x + 2 \in A \\ \text{Axioma III}: &\quad x \in A \ \wedge \ y \in A \Rightarrow (x + y) \in A \\ \text{Axioma IV}: &\quad 7 \notin A \end{aligned}$$

Demuestre los siguientes teoremas utilizando el método indicado.

1. $3 \in A \Rightarrow 16 \in A.$ (Directo)
2. $4 \in A \Rightarrow 23 \in A.$ (Directo)
3. $11 \in A \Rightarrow (28 \in A \ \vee \ 31 \notin A).$ (Directo)
4. $3 \in A \ \wedge \ 11 \in A \Rightarrow 51 \in A.$ (Directo)
5. $x \in A \ \wedge \ y \in A \Rightarrow (3x + 2y + 17) \in A.$ (Directo)
6. $x \in A \ \wedge \ y \in A \Rightarrow (7x + 3y + 16) \in A.$ (Directo)
7. $11 \notin A \Rightarrow 3 \notin A.$ (Contradicción)
8. $24 \notin A \Rightarrow (4 \notin A \ \vee \ 12 \in A).$ (Contradicción)
9. $(3y + z + 7) \notin A \Rightarrow \left(y \notin A \ \vee \ \dfrac{z}{2} \notin A\right).$ (Contradicción)
10. $(3y \notin A \ \wedge \ (z + 10) \notin A) \Rightarrow (y \notin A \ \wedge \ z \notin A).$ (Contradicción)
11. $3 \in A \Rightarrow 1 \notin A.$ (Reducción al absurdo)
12. $21 \in A \Rightarrow -31 \notin A.$ (Reducción al absurdo)
13. $x \in A \ \wedge \ y \in A \Rightarrow (-3 - 3x - y) \notin A.$ (Reducción al absurdo)
14. $2 \notin A$
15. $(\exists x \in A)\left(x^2 - 17x + 70 = 0\right)$

Capítulo 2

Teoría de conjuntos

"Gris, querido amigo,
es toda teoría y verde
el árbol dorado de la vida".

Goethe

Definiciones y operaciones
Conjuntos numéricos
Diagramas de Venn
Leyes de conjuntos
Cardinalidad
Familias de conjuntos
Resultados y demostraciones

Como disciplina matemática, la teoría de conjuntos se origina con los trabajos de Georg Cantor (1845-1918) y George Boole (1815-1864). Los estudios de Cantor se centran sobre todo en conjuntos infinitos y números transfinitos. Boole, por su parte, se centra en el estudio algebraico y lógico, enfoque que se sigue en este libro. Además, en este capítulo se hace un desarrollo axiomático de la teoría de conjuntos de Zermelo-Fraenkel. Como es usual en cada teoría matemática, como se mencionó en el capítulo anterior, este desarrollo se hará a partir de algunas definiciones y axiomas mediante los cuales se pueden probar algunos resultados más generales.

Para profundizar en el tema tratado en este capítulo, es recomendable consultar las referencias bibliográficas [2], [7], [15], [19] y [20].

2.1 Definiciones y operaciones

Para iniciar esta sección, se considera la palabra **conjunto** como un término primitivo; intuitivamente, un conjunto será una colección de objetos, los cuales se llamarán **elementos**. Por ejemplo, si se toma en consideración el conjunto formado por las letras del abecedario, estas últimas serán los elementos del conjunto. Se representa con los símbolos $\varnothing$ o $\{\ \}$ al **conjunto vacío**, que no posee elementos.

Además, se utiliza el símbolo $\in$ para determinar la relación de pertenencia de un elemento en un conjunto. Así, la proposición $\boldsymbol{a} \in \boldsymbol{A}$

se lee "a pertenece al conjunto A". La negación de la proposición $a \in A$, es decir, $\neg(a \in A)$, se representa por $a \notin A$ y se lee "a no pertenece al conjunto A".

Consecuente con lo estudiado en la sección 1.6, se puede decir que la proposición $\nexists x\ [x \in \varnothing]$, o su equivalencia $\forall x\ [x \notin \varnothing]$, son proposiciones verdaderas; asimismo, las proposiciones $5 \in \{3, 5, 6\}$ y $5 \notin \{3, 7\}$ son verdaderas.

Usualmente, se representa a los conjuntos con letras mayúsculas; por ejemplo, A, B, C, D, ..., y a los elementos de los conjuntos, con letras minúsculas: a, b, c, d, ...

Por otro lado, dado un conjunto universo $\mathcal{U}$, la forma usual de representar el conjunto A de los elementos del universo que satisfacen la proposición abierta $P(x)$ es:

$$\begin{aligned} A &= \big\{x \ / \ x \in \mathcal{U} \ \wedge \ P(x)\big\} \\ &= \big\{x \in \mathcal{U} \ / \ P(x)\big\} \end{aligned}$$

En el caso de que el conjunto universo esté claramente definido, se puede escribir de la manera $A = \big\{x \ / \ P(x)\big\}$. Esta forma se llama representación por **comprensión** o por **abstracción**; sin mostrar los elementos, se especifica la naturaleza de ellos y la condición que deben cumplir para estar en el conjunto. Por el contrario, en la representación por **extensión** se escriben todos los elementos del conjunto. Es importante referirse aquí a Bertrand Russell (1872-1970), filósofo y matemático inglés, Premio Nobel de Literatura de 1950, quien en 1901 apuntó el peligro que se corre al no especificar el conjunto universo claramente, planteando así la conocida paradoja de Russell (véase página 120 o consulte [12], [17], [21], [31]).

Por último, y antes de presentar algunos ejemplos, se asumirá el conocimiento de algunos conjuntos numéricos básicos, como son $\mathbb{N}$ y $\mathbb{Z}$, entre otros. Si desea efectuar un breve repaso y así lograr una mayor comprensión de este tema, es recomendable leer primero la sección 2.2.

Ejemplo 1. *Determine el conjunto* $B = \{x \in \mathbb{Z} \ / \ \ 4x^2 - 1 = 0\}$.

Solución. Dado que la ecuación $4x^2 - 1 = 0$ tiene como soluciones solamente los valores $x = -\frac{1}{2}$ y $x = \frac{1}{2}$, que no pertenecen a $\mathbb{Z}$, se tiene que la ecuación no posee solución en el conjunto de los números enteros, con lo cual se concluye que $B = \varnothing$. ■

Ejemplo 2. *El conjunto* $\{x \ / \ \ x \in \mathbb{N} \ \wedge \ 2x + 1 = 7\}$ *representa, por comprensión, el conjunto de todos los números naturales que satisfacen la ecuación lineal* $2x + 1 = 7$ *y se puede reescribir también como*

$$\{x \in \mathbb{N} \ / \ \ 2x + 1 = 7\}$$

Al resolver la ecuación, se tiene que este conjunto, expresado por extensión, es el conjunto unitario $\{3\}$. ■

Ejemplo 3. *Calcule el conjunto* $C = \{x \in \mathbb{Z} \ / \ \ x^2 - 4 = 0 \ \wedge \ x < 1\}$.

Solución. Los elementos de C son las soluciones enteras de la ecuación $x^2 - 4 = 0$, es decir, $x = 2$ y $x = -2$, pero que satisfagan simultáneamente la condición $x < 1$, con lo cual se obtiene que $C = \{-2\}$. ■

Ejemplo 4. *Determine el conjunto* $B = \{x \in \mathbb{R} \ / \ \ x^2 + 1 = 0\}$.

Solución. $B = \varnothing$, pues la ecuación $x^2 + 1 = 0$ no tiene solución en el conjunto de los números reales. ■

Se dice que A es **subconjunto** de B, A está **contenido** en B ó A está **incluido** en B, y se denota por $\boldsymbol{A \subseteq B}$ si y solo si todo elemento de A también es elemento de B, es decir:

$$A \subseteq B \Longleftrightarrow (\forall x)[x \in A \to x \in B]$$

Ejemplo 5. *Las proposiciones*

$$\{4,2,3\} \subseteq \{2,3,4\}, \qquad \{a\} \subseteq \{a,b\}, \qquad \mathbb{N} \subseteq \mathbb{Z}, \qquad \varnothing \subseteq \{3,5\}$$

son verdaderas, mientras que las proposiciones

$$\{2,4,6\} \subseteq \{4,2\}, \qquad \mathbb{R} \subseteq \mathbb{Q}, \qquad \{\varnothing\} \subseteq \{\ \}$$

son falsas. ■

Se dice que A es igual a B si todos los elementos de A están en B y todos los elementos de B están en A, es decir:

$$A = B \Longleftrightarrow [A \subseteq B \ \wedge \ B \subseteq A]$$

Ejemplo 6. *Las siguientes igualdades*

$$\{1,3,1\} = \{3,1,3\}, \qquad \mathbb{Q} = \mathbb{R} - \mathbb{I}, \qquad \{1,\varnothing\} = \big\{\{\ \},1\big\}$$

son proposiciones verdaderas, mientras que las proposiciones

$$\{1,3,4\} = \{3,4\}, \qquad \mathbb{Q} = \mathbb{Z}, \qquad \{2,3\} = \{2,4\}$$

son falsas. ■

Se dice que A es **subconjunto propio** de B y se denota por $\boldsymbol{A \subset B}$ si y solo si $A \subseteq B$ y $A \neq B$.

Ejemplo 7. *Las siguientes inclusiones*

$$\{2,4\} \subset \{2,3,4\}, \qquad \mathbb{N} \subset \mathbb{Z}, \qquad \varnothing \subset \{\varnothing\}$$

son proposiciones verdaderas, mientras que las proposiciones

$$\{1,3,4\} \subset \{3,4\}, \qquad \mathbb{Q} \subset \mathbb{Q}, \qquad \{1,3\} \subset \{3,1\}$$

son falsas. ■

En teoría de conjuntos, como en cualquier rama de las matemáticas, la notación es importante, y poder determinar el grado de verdad de algunas proposiciones depende de que se entienda lo que se escribe. Los siguientes ejemplos muestran, con base en conjuntos sencillos, el valor de verdad de algunas proposiciones asociadas con ellos que involucran los conceptos de inclusión de conjuntos y de pertenencia de elementos.

Ejemplo 8. *Si* $A = \big\{1, 3, \{2\}\big\}$ *y* $B = \big\{1, \{3\}, 5\big\}$*, es posible afirmar que las proposiciones*

$$3 \in A, \quad \{3\} \subseteq A, \quad \{3\} \in B, \quad \big\{\{3\}\big\} \subseteq B, \quad \{1, 5\} \subseteq B, \quad \varnothing \subseteq B$$

son verdaderas, mientras que las proposiciones

$$5 \in A, \quad 1 \subseteq B, \quad \{1, 3, 5\} \subseteq B, \quad \{2\} \subseteq A, \quad \{1, 2\} \subseteq A, \quad \{2\} \subset \{2\}$$

son falsas. ■

Ejemplo 9. *Considere el conjunto* $A = \big\{1, 2, \{1, 2\}, 3\big\}$*, donde claramente se observa que posee cuatro elementos. Algunas proposiciones, con su respectivo valor de verdad, son:*

$$\begin{aligned}
2 \in A &\equiv \text{V}\\
\{3\} \in A &\equiv \text{F}\\
\{3\} \subseteq A &\equiv \text{V}\\
\{1, 2\} \in A &\equiv \text{V}\\
\{3, 2\} \subseteq A &\equiv \text{V}\\
\big\{\{1, 2\}\big\} \subseteq A &\equiv \text{V}\\
\big\{3, 2, \{1, 2\}\big\} \subseteq A &\equiv \text{V}\\
\varnothing \in A &\equiv \text{F}\\
\varnothing \subseteq A \wedge 3 \in A &\equiv \text{V}
\end{aligned}$$

■

Ejemplo 10. *Para cualquier conjunto A, la proposición $\varnothing \subseteq A$ siempre es verdadera.*

Solución. Para comprobar esto, es posible razonar por contradicción, es decir, si fuera falsa se tendría que $\varnothing \nsubseteq A$ sería verdadera y no se cumple la definición de la inclusión. Por lo tanto, existiría un elemento x que cumpliría $x \in \varnothing$ y que al mismo tiempo $x \notin A$, lo cual es una clara contradicción, pues $\varnothing$ no tiene elementos; de esta manera, se ha concluido que la proposición $\varnothing \subseteq A$ no puede ser falsa, por lo que debe ser verdadera. ■

A partir de dos conjuntos, A y B, se definen los conjuntos:

- **unión**, como $A \cup B = \{x \ / \ \ x \in A \vee x \in B\}$
- **intersección**, como $A \cap B = \{x \ / \ \ x \in A \wedge x \in B\}$
- **diferencia**, como $A - B = \{x \ / \ \ x \in A \wedge x \notin B\}$
- **diferencia simétrica**, como $A \triangle B = (A - B) \cup (B - A)$

Ejemplo 11. *Si $A = \{a, b, c, e\}$, $B = \{b, c, d\}$ y $C = \{a, c, e, f\}$ es posible calcular los conjuntos:*

$$
\begin{aligned}
A \cup B &= \{a, b, c, d, e\} \\
A \cap B &= \{b, c\} \\
A - B &= \{a, e\} \\
B - A &= \{d\} \\
C - B &= \{a, e, f\} \\
A \triangle B &= \{a, e\} \cup \{d\} = \{a, d, e\} \\
(A \cap B) \cup (A - B) &= \{b, c\} \cup \{a, e\} = \{a, b, c, e\} \\
(A \cup C) - (B \cap C) &= \{a, b, c, e, f\} - \{c\} = \{a, b, e, f\}
\end{aligned}
$$

■

Si se tiene un conjunto A y otro conjunto $\mathcal{U}$ tal que $A \subseteq \mathcal{U}$, se define el **complemento de $\boldsymbol{A}$ con respecto a $\boldsymbol{\mathcal{U}}$** como:

$$\overline{A} = \mathcal{U} - A$$

Al conjunto $\mathcal{U}$ se le llama **universo relativo** y en ocasiones $\overline{A}$ se denota como $\complement_A^{\mathcal{U}}$.

Ejemplo 12. *Si* $\mathcal{U} = \{1,2,3,4,5\}$, $A = \{2,5\}$ *y* $B = \{1,5\}$, *entonces:*

$$\begin{aligned} \overline{A} &= \{1,3,4\} \\ \overline{A \cup B} &= \overline{\{1,2,5\}} = \{3,4\} \\ \overline{B - A} &= \overline{\{1\}} = \{2,3,4,5\} \end{aligned}$$

■

Ejemplo 13. *Si* $\mathcal{U} = \{0,2,4,6,8,9\}$, $A = \{0,2,8\}$, $B = \{2,8,9\}$ *y* $C = \{0,4,8,9\}$, *calcule* $\overline{A \cap B} - (A \triangle C)$.

Solución.

$$\begin{aligned} & \overline{A \cap B} - (A \triangle C) \\ = \; & \overline{\{0,2,8\} \cap \{2,8,9\}} - \big(\{0,2,8\} \triangle \{0,4,8,9\}\big) \\ = \; & \overline{\{2,8\}} - \big(\{2\} \cup \{4,9\}\big) \\ = \; & \{0,4,6,9\} - \{2,4,9\} \; = \; \{0,6\} \end{aligned}$$

■

Se dice que dos conjuntos A y B son **disjuntos** si no tienen elementos en común, es decir, si $A \cap B = \varnothing$.

Ejemplo 14. *Los conjuntos* $\mathbb{I}$ *y* $\mathbb{Q}$ *son conjuntos disjuntos, pues no existe un número real que sea racional e irracional simultáneamente.* ■

Ejemplo 15. *Es claro que el conjunto de los números pares y el conjunto de los números impares son disjuntos. Si, por otro lado, se considera el conjunto de los pares y el conjunto de los múltiplos de* 5*, es claro que no serán disjuntos, pues, por ejemplo, el número* 10 *pertenece a ambos conjuntos.* ■

Ejemplo 16. *Los dos conjuntos* $A - B$ *y* $B - A$ *son conjuntos disjuntos, pues claramente los elementos de* $A - B$ *están en* A *y no están en* B*, y los elementos de* $B - A$ *están en* B *pero no en* A*, con lo cual se cumple que* $A \cap B = \varnothing$*.* ■

Para el conjunto A, se define el **conjunto potencia** o **conjunto de partes de $\boldsymbol{A}$**, que se denota $\boldsymbol{P(A)}$, como el conjunto formado por todos los subconjuntos de A, es decir:

$$P(A) = \{S \ / \ S \subseteq A\}$$

En ocasiones, el conjunto $P(A)$ se denota $\mathbf{2}^{\boldsymbol{A}}$ (véase página 145).

Ejemplo 17. *Para el conjunto* $A = \{1, 2\}$*, calcule* $P(A)$*.*

Solución. Se debe calcular el conjunto formado por todos los subconjuntos de A, en este caso se tiene:

$$P(A) = \big\{\varnothing, \{1\}, \{2\}, A\big\}$$

Note que son 4 elementos que corresponden a 2^2. ■

Ejemplo 18. *Para el conjunto* $B = \{1, 2, 3\}$*, calcule* $P(B)$*.*

Solución. Análogamente, el conjunto de los subconjuntos de B es

$$P(B) = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, B\big\}$$

Note que son 8 elementos que corresponden a 2^3. ■

Ejemplo 19. *Considere los conjuntos* $A = \{1, 2\}$ *y* $B = \{1, 2, 3\}$*. Calcule* $P(B - A)$ *y* $P(B) - P(A)$*.*

Solución. Para $P(B - A)$ se realiza primero la diferencia de conjuntos; así, es claro que:

$$P(B - A) = P(\{3\}) = \big\{\varnothing, \{3\}\big\}$$

Además, considerando los cálculos efectuados en los dos ejemplos precedentes, se tiene que

$$P(B) - P(A) = \big\{\{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, B\big\}$$

■

Para los conjuntos A y B, se define el **producto cartesiano de $\boldsymbol{A}$ y $\boldsymbol{B}$** como el conjunto

$$A \times B = \{(a, b) \;\; / \;\; a \in A \;\wedge\; b \in B\}$$

A los elementos de este conjunto producto, cuya forma es (a, b), se les llama **pares ordenados**, donde a es la primera entrada y b la segunda. Claro que este concepto se puede extender a tripletas ordenadas (a, b, c) y en general a n-tuplas $(x_1, x_2, \ldots, x_n)$, útiles para representar vectores en el espacio o clasificar individuos en análisis de datos, entre muchas otras aplicaciones.

Ejemplo 20. *Si* $A = \{1, 2\}$, $B = \{a, b\}$ *y* $C = \{5\}$*, entonces* $C \times A = \{(5, 1), (5, 2)\}$*; además,* $A \times B = \{(1, a), (1, b), (2, a), (2, b)\}$*.* ■

Ejemplo 21. *Si* $\mathcal{U} = \{1, 2, 3\}$, $A = \{1, 3\}$ *y* $B = \{2\}$*, calcule* $\overline{A \times B} - \big(\overline{A} \times \overline{B}\big)$*.*

Solución. Para el universo de conjunto producto se considera $\mathcal{U} \times \mathcal{U}$:

$$\begin{aligned}
\overline{A \times B} - \left(\overline{A} \times \overline{B}\right) &= \overline{\{(1,2),(3,2)\}} - \left(\{2\} \times \{1,3\}\right) \\
&= \big\{(1,1),(1,3),(2,1),(2,2),(2,3),(3,1),(3,3)\big\} \\
&\quad - \big\{(2,1),(2,3)\big\} \\
&= \big\{(1,1),(1,3),(2,2),(3,1),(3,3)\big\}
\end{aligned}$$

■

Ejemplo 22. *Si* $B = \{2\}$*, calcule* $P(B) \times P(B)$ *y* $P(B \times B)$*.*

Solución. Es claro que $P(B) = \{\varnothing, \{2\}\}$, por lo que

$$P(B) \times P(B) = \big\{(\varnothing,\varnothing),(\varnothing,\{2\}),(\{2\},\varnothing),(\{2\},\{2\})\big\}$$

Además, como $B \times B = \{(2,2)\}$, se obtiene:

$$P(B \times B) = \big\{\varnothing, \{(2,2)\}\big\}$$

■

Paradoja de Bertrand Russell. Para comprender esta paradoja, se considerarán algunos conjuntos y se analizará si ellos son o no subconjuntos de ellos mismos. Sea A el conjunto formado por los archivos, A se puede considerar como un nuevo archivo, y en este caso se cumple que $A \in A$; por supuesto, también se cumple $A \subseteq A$. De la misma forma, se debe considerar el conjunto C formado por todos los conjuntos, C sería un nuevo conjunto y, por lo tanto, se pertenecería a sí mismo, es decir, $C \in C$, pues C es un conjunto. Sin embargo, el conjunto S que contiene una silla no es una silla, de donde lo verdadero sería $S \notin S$.

De lo anterior se observa que es posible distinguir solo dos tipos de conjuntos, los que se pertenecen a sí mismos y los que no se pertenecen a sí mismos. Considere el conjunto M formado por todos los conjuntos X que no se pertenecen a sí mismos, es decir:

$$M = \{X \ / \ X \notin X\}$$

Como M es un nuevo conjunto, necesariamente se debe cumplir que $M \in M$ o $M \notin M$.

Se analizan ambas proposiciones:

- Si $M \in M$, satisface la condición de estar en M, es decir, $M \notin M$.
- Si $M \notin M$, se cumple que M no satisface la condición de estar en M, es decir, $M \in M$.

Este análisis dice que en ambos casos se satisfacen las proposiciones $M \in M$ y $M \notin M$ simultáneamente, y esto es, utilizando la ley de los inversos, claramente una contradicción. Es decir, se ha encontrado un conjunto M que no satisface alguna de las proposiciones $M \in M$ o $M \notin M$. Ésta se conoce como la *paradoja de Russell*.

Por supuesto, como se mencionó anteriormente, esta paradoja se evita definiendo el conjunto universo apropiadamente.

Ejercicios (sección 2.1)

1. Si $A = \{a, b, c\}$, $B = \{c, d, e\}$ y $C = \{c, e, f, g\}$, calcule:
   (a) $A \times (B - C)$
   (b) $P(A - B)$
   (c) $(A \triangle C) \cap B$
2. Si $\mathcal{U} = \{a, b, c, d, e, f\}$, $A = \{a, b, e\}$, $B = \{c, e, f\}$ y $C = \{b, e, f\}$, calcule $[(A - B) \cup C] \cap \overline{(B \triangle C) \cup \{d\}}$.
3. Si $A = \{\varnothing, 2, \{2\}\}$ y $B = \{1, \{2\}\}$, determine los conjuntos $B \times A$, $A \cap B$, $P(A)$ y $B - A$.

4. Si $A = \{\{\varnothing\}, 1, \{2\}, \{3\}\}$ y $B = \{3, \{2\}\}$, calcule:

   (a) $(A \cap B) - (A \triangle B)$

   (b) $(A - B) \times (B - A)$

   (c) $P(A - B)$

5. Si $A = \{a, b\}$, $B = \{b, c, d\}$ y $C = \{a, d\}$, donde el conjunto universo es $\mathcal{U} = \{a, b, c, d, e, f\}$, calcule:

   (a) $(A \cup C) \triangle B$

   (b) $P(\overline{A} \cap \overline{B})$

   (c) $(C \times B) - (A \times C)$

6. Sea $\mathcal{U} = \{1, 2, \ldots, 8, 9\}$ el universo, $A = \{3, 4, 5\}$ y $B = \{3, 5, 8, 9\}$. Calcule los conjuntos:

   (a) $P(A \cap B)$

   (b) $\overline{B - A}$

   (c) $(A \triangle B) \times \left(\overline{A \cup B}\right)$

7. Si $A = \{a, b, g\}$, $B = \{b, d, e, g\}$ y $C = \{a, b, d, f, g\}$, con $\mathcal{U} = \{a, b, c, d, e, f, g\}$ como el conjunto universo, calcule:

   (a) $(A \triangle C) \cap \overline{B - A}$

   (b) $P(C - B) \times (A \cap B)$

8. Si $A = \{a\}$, calcule $P(P(A))$ y $P(A) \times P(A)$.

9. Dé un ejemplo de cuatro conjuntos A, B, C y D, tales que $A \in B$, $B \in C$, $C \in D$ y $A \in D$.

10. Sean $A = \{2, 3, 4\}$, $B = \{1, 3, 4\}$ y $C = \{1, 2, 4\}$, con el conjunto $\mathcal{U} = \{0, 1, 2, 3, 4, 5\}$ como universo. Calcule:

    (a) $C - (A \triangle B)$

(b) $P(A) - P(B)$

(c) $(A \cap C) \times \overline{(B \cup C)}$

11. Si $A = \{1, 2\}$, $B = \{3, 5, 7\}$, $C = \{2, 4, 5, 6\}$ y $D = \{2, 5, 6\}$, con $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7\}$ como el conjunto universo, calcule:

    (a) $\overline{(A \triangle B) - B} \cap D$

    (b) $P(B - D) \times P(B - C)$

12. Sean P y Q dos proposiciones abiertas definidas por:
    $P(x) : x$ es múltiplo de 2
    $Q(x) : x$ es múltiplo de 3
    Si $\mathcal{U} = \{1, 2, 3, \ldots, 10\}$, calcule:

$$\begin{array}{rcl} A & = & \{x \in \mathcal{U} \ / \ P(x) \vee Q(x)\} \\ B & = & \{x \in \mathcal{U} \ / \ P(x) \wedge Q(x)\} \\ C & = & \{x \in \mathcal{U} \ / \ P(x) \veebar Q(x)\} \end{array}$$

13. Si $A = \{1, 2, 3\}$, $B = \{\varnothing\}$ y $C = \big\{\{1\}, \{2, 3\}, \{2\}\big\}$, determine el valor de verdad de las siguientes proposiciones:

    (a) $\exists x \, [x \in C \to x \subseteq A]$.

    (b) $\forall x \, [x \in A \to \{x\} \in C]$.

    (c) $\neg \forall x \, [x \in B \to x = \varnothing]$.

14. Si $A = \{3n - 2 \ / \ n \in \mathbb{Z}\}$ y $B = \{3m + 4 \ / \ m \in \mathbb{Z}\}$, determine si la expresión $A = B$ es verdadera o no.

15. Si es posible, determine un conjunto S, no vacío, que satisfaga la proposición $\forall \, x \; (x \in S \to x \subseteq S)$.

16. Si $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 5, 6\}$ y $C = \{1, 2, 7, 8\}$, con el conjunto $\mathcal{U} = \{1, 2, \ldots, 7, 8\}$ como universo:

    (a) Calcule $P\left(\overline{A} \cap C\right)$.

(b) Calcule $(A - B) \times \{e, f\}$.

(c) Determine el valor de verdad de las siguientes proposiciones:

i. $(\exists x \in B)\ [x^2 - 1 \in C]$.

ii. $(\forall x)\ [x \in A \to (x + 1) \in B]$.

17. Para cada una de las siguientes parejas de conjuntos A y B, calcule los conjuntos $A \cup B$, $A \cap B$, $A - B$, $B - A$ y $A \bigtriangleup B$:

    (a) $A = [-1, 4[$, $B = [0, 2]$

    (b) $A = [1, 5]$, $B = [0, 3[$

    (c) $A =]-\infty, 2]$, $B = [1, 3]$

    (d) $A = [3, +\infty[$, $B =]1, 5]$

18. Para cada uno, represente en un sistema cartesiano el conjunto $A \times B$:

    (a) $A = \{-1, 0, 1\}$, $B = \{2, 3\}$

    (b) $A = [-1, 3]$, $B = [1, 2[$

    (c) $A = \{-1, 3\}$, $B = [1, 2[$

    (d) $A = [-1, 3[$, $B = \{1, 2\}$

    (e) $A = \mathbb{R}$, $B = \{2\}$

    (f) $A = [1, +\infty[$, $B =]-\infty, 3[$

19. Considere los conjuntos $A = [-1, 1]$, $B = [-2, 2]$, $C = \{-1, 0, 1\}$ y $D = \{-2, -1, 0, 1, 2\}$. Represente en un sistema cartesiano los conjuntos siguientes:

    (a) $\{(x, y) \in A \times B \ / \ y = x\}$

    (b) $\{(x, y) \in C \times D \ / \ y = x\}$

    (c) $\{(x, y) \in C \times D \ / \ y = 2x - 1\}$

    (d) $\{(x, y) \in A \times B \ / \ y = 2x - 1\}$

(e) $\{(x, y) \in C \times D \;\; / \;\; |x + y| = 1\}$
(f) $\{(x, y) \in C \times D \;\; / \;\; |x + y| \leq 1\}$
(g) $\{(x, y) \in C \times D \;\; / \;\; |x| + |y| \leq 1\}$

20. Si $A = [0, 1]$, el intervalo cerrado que contiene todos los números reales x que satisfacen la condición $0 \leq x \leq 1$, determine el valor de verdad de las proposiciones:

    (a) $\exists x \in A \wedge \exists y \in A$ tal que $x + y < 1$
    (b) $(\forall x \in A)(\exists y \in A)\ [0 < y < x]$
    (c) $(\forall x \in A)(\forall y \in A)\ [\exists z \in A \;\; / \;\; x + y < z]$

21. Considere los tres conjuntos $A = \{x \in \mathbb{N} \;\; / \;\; -3x + 2 = -13\}$, $B = \{2, 3, 4, 5\}$ y $C = \{1, 2, 3, 6\}$, con $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ como el conjunto universo. Determine el valor de verdad de las siguientes proposiciones:

    (a) $(\forall x \in C)(\exists y \in B)\,[x + 1 = y]$
    (b) $(\exists x \in C)\left[x \in C \;\rightarrow\; (x^2 + 1) \in A \cap B\right]$

22. Si $A = \{2, 3, 4\}$ y $B = \{3, \varnothing\}$, determine:

    (a) dos elementos del conjunto $P(B) \times P(A)$
    (b) dos elementos del conjunto $P(B \times P(A))$
    (c) dos elementos del conjunto $B \times P(A \times P(B))$

23. Considere el universo formado por las palabras, específicamente los adjetivos. Es claro que éstos se pueden clasificar en dos tipos:

    (a) Las palabras *autológicas* son las que cumplen lo que ellas significan. Por ejemplo, la palabra *esdrújula* es una palabra esdrújula, por lo tanto es autológica; la palabra *pentasílaba* es autológica, ya que la palabra pentasílaba es ella misma una palabra pentasílaba (tiene cinco sílabas); como la palabra *grave* es una palabra grave, grave es también autológica.

(b) Las palabras *heterológicas* son las que no son autológicas, es decir, no cumplen lo que ellas significan. Por ejemplo, *invisible* no es invisible, por lo tanto es heterológica; *larga*, *olorosa* y *caliente* son heterológicas.

¿Cómo clasificaría la palabra *heterológica*?, es decir, la palabra *heterológica* ¿será autológica o heterológica?

2.2 Conjuntos numéricos

Es necesario recordar que el conjunto de los **números naturales**, que se denota por $\mathbb{N}$, es:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

Además, el conjunto de los **números enteros**, que se denota por $\mathbb{Z}$, es:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Un **número racional** es un número que se puede expresar de la forma $\frac{a}{b}$ con a y b enteros, con $b \neq 0$. El conjunto formado por los números racionales se representa por $\mathbb{Q}$, simbólicamente:

$$\mathbb{Q} = \left\{ \frac{a}{b} \ / \ a, b \in \mathbb{Z} \quad \text{tal que} \quad b \neq 0 \right\}$$

Se observa que todo número natural es, a su vez, un número entero, pero algunos números enteros no son números naturales. Como $\frac{a}{1} = a$, todos los números enteros son a su vez números racionales. Los números racionales se pueden expresar en notación fraccionaria y en notación decimal.

Ejemplo 23. *Considere el número racional $\frac{3}{5}$; al efectuar la división de 3 por 5, se obtiene la expresión decimal finita del racional $\frac{3}{5}$, es decir, $\frac{3}{5} = 0{,}6$.* ■

Ejemplo 24. *Determine la fracción racional equivalente $0,123$.*

Solución. Como $0,123$ tiene tres dígitos decimales, la representación racional de éste se obtiene del cociente del número 123 entre 1000 (por tener tres decimales); así, el número $0,123 = \frac{123}{1000}$. ■

Existen racionales donde la parte decimal de su expresión decimal tiene infinito número de cifras decimales, ya que un grupo de ellas se repite indefinidamente. En este caso, el grupo de cifras que se repite se denomina **período** y se dice que la expresión decimal del número respectivo es periódica. Se acostumbra escribir el período una vez con una raya sobre él. El **anteperíodo** es la sucesión de números que anteceden al período y que forman parte de los decimales. En general se tiene:

$$a_k \ldots a_0,\ \underbrace{b_1 \ldots b_j}_{\text{anteperíodo}}\ \underbrace{\overline{c_1 \ldots c_i}}_{\text{período}}$$

Ejemplo 25. *Es claro que los números* $\frac{4}{5}$ *y* $2,2\overline{34}$ *son racionales.* ■

Ejemplo 26. *Al efectuar la división de* 17 *por* 18*, se obtiene la representación decimal* $0,944\ldots$*, donde los puntos suspensivos sugieren que el "4" se repite indefinidamente, y se escribe* $\frac{17}{18} = 0,9\overline{4}$*. Otras expresiones válidas son, por ejemplo,* $\frac{26}{15} = 1,7\overline{3} = 1,733\ldots$*, y la igualdad* $\frac{673}{4995} = 0,1347347\ldots = 0,1\overline{347}$*.* ■

En general, todos los números racionales son periódicos, pues en los casos en que la representación decimal es finita, se puede considerar que el período es 9; por ejemplo, $0,6 = 0,5\overline{9}$. Para algunos cálculos conviene expresar un número decimal como fracción; para ello, observe los siguientes ejemplos donde se ilustra la forma de efectuar la conversión.

Ejemplo 27. *Determine la fracción racional equivalente* $0,\overline{2}$*.*

Solución. Sea $x = 0,\overline{2}$, al multiplicar por 10 se obtiene la igualdad $10x = 2,\overline{2}$. Al restar ambas igualdades, se tiene $9x = 2$, por lo que $x = \frac{2}{9}$, es decir $0,\overline{2} = \frac{2}{9}$. ■

Ejemplo 28. *Exprese* $2,34\overline{123}$ *en su forma racional canónica.*

Solución. Sea $x = 2,34\overline{123}$, al multiplicar por 100 se obtiene la igualdad

$$100x = 234,\overline{123}$$

Al multiplicar por 1 000, se obtiene la igualdad

$$100\,000x = 234\,123,\overline{123}$$

Al restar las últimas dos igualdades, se tiene $99\,900x = 233\,889$, por lo que $x = \frac{233889}{99900}$; finalmente, al simplificar, $2,34\overline{123} = \frac{77963}{33300}$. ■

Ejemplo 29. *Determine la fracción racional equivalente con* $0,1\overline{23}$*.*

Solución. Sea $x = 0,1\overline{23}$, al multiplicar x por 100 se obtiene: $100x = 12,3\overline{23}$. Al restar estas dos ecuaciones, se tiene $100x - x = 12,3\overline{23} - 0,1\overline{23}$. Como $100x - x = 99x$ y además $12{,}3\overline{23} - 0,1\overline{23} = 12,2$, pues al tener el mismo período, éste desaparece, se tiene la igualdad $99x = 12{,}2$. Al multiplicar la ecuación por 10, se obtiene $990x = 122$. Así, al despejar el valor de x, se obtiene $x = \frac{122}{990} = \frac{61}{495}$, es decir, $0,1\overline{23} = \frac{61}{495}$. ■

Teorema 1. *La representación racional de* $a_k \ldots a_0, b_1 \ldots b_j\overline{c_1 \ldots c_i}$ *es*

$$\frac{(a_k \ldots a_0 b_1 \ldots b_j c_1 \ldots c_i) - (a_k \ldots a_0 b_1 \ldots b_j)}{(10^i - 1) \cdot 10^j}$$

Demostración. Ejercicio. □

Ejemplo 30. *Al utilizar el teorema anterior, se obtiene directamente que la fracción racional equivalente a* $32,73\overline{386}$ *es*

$$32,73\overline{386} = \frac{3273386 - 3273}{99900} = \frac{3270113}{99900}$$

en donde la cantidad de nueves en el denominador es el tamaño del período y la cantidad de ceros es el tamaño del anteperíodo. ■

Los números cuya expresión decimal es infinita no periódica se denominan **irracionales**, y el conjunto formado por ellos se representa por $\mathbb{I}$. El conjunto que se obtiene al unir los números racionales con los números irracionales recibe el nombre de conjunto de los **números**

reales y se representa por $\mathbb{R}$. Además, es importante notar que $\mathbb{Q}$ e $\mathbb{I}$ no tienen elementos en común, por lo cual se dice que son conjuntos disjuntos; simbólicamente, estas dos afirmaciones se representan por:

$$\begin{aligned} \mathbb{Q} \cup \mathbb{I} &= \mathbb{R} \\ \mathbb{Q} \cap \mathbb{I} &= \varnothing \end{aligned}$$

Ejemplo 31. *Demuestre que* $\sqrt{2} \in \mathbb{I}$.

Solución. Se procede por contradicción. Suponga que $\sqrt{2} \in \mathbb{I}$ es falso; de esta forma, $\sqrt{2} \notin \mathbb{I}$ y, por lo tanto, $\sqrt{2} \in \mathbb{Q}$, es decir, existen a y b enteros de manera que $\sqrt{2} = \frac{a}{b}$, en donde es posible asumir que ya es una fracción irreducible con a y b sin factores en común, es decir, m.c.d.$(a, b) = 1$. Al elevar al cuadrado y despejar, se tiene que $2b^2 = a^2$ y con ello a^2 es un número par, y utilizando el resultado del ejercicio 10a en página 94, se cumple que a también es par y por tanto existe $k \in \mathbb{Z}$ tal que $a = 2k$. Al sustituir se obtiene que $2b^2 = (2k)^2$, y al despejar se tiene que $b^2 = 2k^2$; así, b^2 es un número par y, de forma análoga, se cumple que b también es par. Se ha llegado a una clara contradicción, pues se ha probado que tanto a y b tienen a 2 como factor común; sin embargo, se escogieron coprimos entre sí. Esta contradicción indica que lo supuesto, $\sqrt{2} \notin \mathbb{I}$, no puede ser verdadero y, por lo tanto, la negación debe serlo, es decir, se ha probado que $\sqrt{2} \in \mathbb{I}$. ■

Ejemplo 32. *Además de* $\sqrt{2}$, *del que se probó su irracionalidad en el ejemplo anterior, otros números irracionales conocidos son todas las raíces no exactas como* $\sqrt{3}$, $\sqrt[3]{5}$ *o* $\sqrt[5]{13}$, *también* π, $\ln(2)$ *o* $\cos(2)$, *que son irracionales trascendentes.* ■

Ejemplo 33. *El número* $0,10110111011110\ldots$ *en donde en la parte decimal aparece un cero luego de un uno, luego de dos unos, luego de tres unos, y así sucesivamente, no es periódico; por lo tanto, es posible concluir que es un número irracional.* ■

Ejemplo 34. *Algunas proposiciones y su valor de verdad son:*

$$\begin{aligned}
\mathbb{Q} \subseteq \mathbb{I} &\equiv \text{F}\\
\{-2,3,10\} \subseteq \mathbb{Q} &\equiv \text{V}\\
\mathbb{R}-\mathbb{Q}=\mathbb{I} &\equiv \text{V}\\
\mathbb{N}\cap\mathbb{Z}=\mathbb{N} &\equiv \text{V}\\
\left\{\frac{3}{5},2,-1\right\} \subseteq \mathbb{Z} &\equiv \text{F}\\
-2\in\mathbb{Z} \ \wedge \ \pi\in\mathbb{I} &\equiv \text{V}\\
\mathbb{Z}\cap\mathbb{I}=\varnothing &\equiv \text{V}
\end{aligned}$$

■

Ejercicios (sección 2.2)

1. Determine el valor de verdad de las proposiciones:

   (a) $\mathbb{I} \subseteq \mathbb{R}$

   (b) $\varnothing \subseteq \mathbb{Q}$

   (c) $\mathbb{Q}-\mathbb{I}=\mathbb{I}$

   (d) $\mathbb{N}\cup\mathbb{Q}=\mathbb{R}-\mathbb{I}$

   (e) $\left\{\frac{5}{4},-2,4,\sqrt{9}\right\} \subseteq \mathbb{Z}$

   (f) $3\notin\mathbb{Z} \ \vee \ \pi\notin\mathbb{I}$

   (g) $-4\in\mathbb{N} \ \rightarrow \ \pi\in\mathbb{Q}$

   (h) $\mathbb{N}\cap\mathbb{I}\neq\varnothing$

   (i) $\left\{\frac{3^{100}-1}{2},\frac{\sqrt{225}}{\sqrt{25}},-3\right\} \subseteq \mathbb{Z}$

2. Sin utilizar el teorema 1, determine la forma fraccionaria de los siguientes números:

   (a) $1,\overline{52}$

(b) $1,5\overline{2}$

(c) $5,4\overline{561}$

(d) $0,3\overline{46}$

(e) $5,22\overline{681}$

(f) $37,344\overline{57}$

(g) $267,345\overline{768923}$

3. Demuestre el teorema 1.

4. Utilice la fórmula dada en el teorema 1 para determinar la representación racional de:

(a) $56,23\overline{374}$

(b) $2\,573,343\overline{48}$

2.3 Diagramas de Venn

Los conjuntos y el resultado de operaciones entre ellos se pueden representar de una forma gráfica e intuitiva por medio de los **diagramas de Venn**. Es importante aclarar que estas representaciones gráficas fueron propuestas por el lógico inglés John Venn (1834-1882) −de allí su nombre− en su obra *Symbolic Logic* en 1881, aunque con anterioridad ya habían sido empleadas por Euler y por Leibniz [31]. Esta representación permite aclarar conceptos y resultados, además de la posibilidad de hacer conjeturas.

Por lo general, el universo relativo se representa en forma de rectángulo y los conjuntos en forma circular, de manera que se satisfagan las condiciones deseadas.

En ellos se puede sombrear una región que represente un conjunto; por ejemplo, la figura 2.1 representa la expresión $A \cap B$, mientras que la figura 2.2 representa la expresión $A - B$.

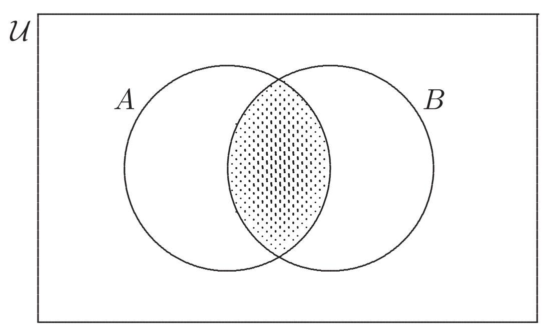


Figura 2.1: $A \cap B$

Para expresiones más complicadas, se debe tener mucho cuidado en el orden de las operaciones que se aplican o etiquetar las regiones disjuntas y proceder como en el siguiente ejemplo.

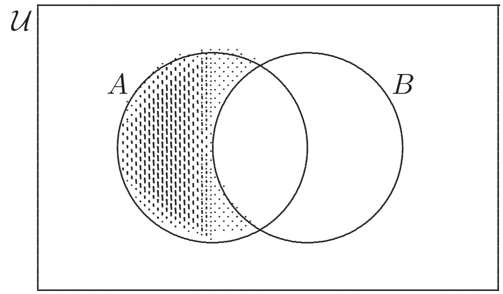


Figura 2.2: $A - B$

Ejemplo 35. *Sean A, B y C conjuntos arbitrarios, con $A \cap B \cap C \neq \varnothing$. Represente el conjunto $[(A \triangle C) - B] \cup (B \cap \overline{C})$ en un Diagrama de Venn.*

Solución. Considere las ocho regiones disjuntas del diagrama de Venn de la figura 2.3. Para estas regiones, se calcula

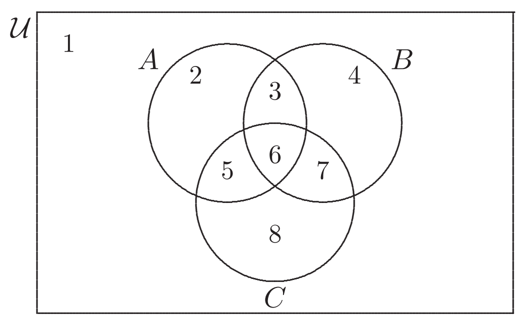


Figura 2.3: Diagrama general con tres conjuntos.

$$
\begin{aligned}
& \big[(A \triangle C) - B\big] \cup \big(B \cap \overline{C}\big) \\
= \; & \big[(\{2,3,5,6\} \triangle \{5,6,7,8\}) - \{3,4,6,7\}\big] \cup \big(\{3,4,6,7\} \cap \overline{\{5,6,7,8\}}\big) \\
= \; & \big[\{2,3,7,8\} - \{3,4,6,7\}\big] \cup \big(\{3,4,6,7\} \cap \{1,2,3,4\}\big) \\
= \; & \{2,8\} \cup \{3,4\} = \{2,3,4,8\}
\end{aligned}
$$

Con lo cual, la figura 2.4 muestra la zona sombreada que representa a la expresión $[(A \triangle C) - B] \cup (B \cap \overline{C})$. ■

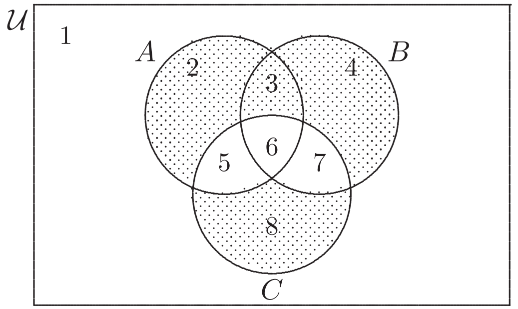


Figura 2.4: $[(A \triangle C) - B] \cup (B \cap \overline{C})$

Ejercicios (sección 2.3)

1. Represente en un Diagrama de Venn el conjunto $(A-B)\cup(B\cap C)$.

2. Suponga que todas las X son Y, pero solo algunas Y son Z. Determine cuál de los siguientes enunciados es verdadero.

   (a) Ninguna X puede ser Z.

   (b) Si algo no es una Y, entonces no es una X.

   (c) Si algo es una Z, entonces no es una X.

3. Represente, en un Diagrama de Venn, los conjuntos A, B, C y D, de manera que satisfagan la siguiente situación: $A \cap B = \varnothing$, $A \cap C \neq \varnothing$, $B \subseteq C$, $D \subseteq A$, $D \subseteq \overline{C}$.

4. Represente, en un Diagrama de Venn, los conjuntos A, B, C y D, de manera que satisfagan la siguiente situación: $A \cap B \neq \varnothing$, $A \cap C = \varnothing$, $B \cap C \neq \varnothing$, $D \subseteq B \cap C$.

5. Si $A \cap B \cap C \neq \varnothing$, represente el conjunto $[(A - C) - B] \cup (B - \overline{C})$ en un Diagrama de Venn.

6. Si $A \cap B \cap C \neq \varnothing$, utilice un Diagrama de Venn para verificar que la igualdad

$$[(B \cup C) \cap (A \cup B)] - \overline{B} = [(A \triangle B) \cap (C \cup B)] \cup (A \cap B)$$

es falsa. ¿Bajo cuáles condiciones se podría tener la igualdad?

7. Mediante una representación en Diagramas de Venn, verifique que la igualdad $[A \cup (B \cap C)] \cup (\overline{B} \cap C) = A \cup C$ es verdadera.

8. Compruebe que si A, B y C son conjuntos que satisfacen las condiciones $C \subseteq \overline{A}$ y $C \cap \overline{B} = \varnothing$, entonces se cumple que $C \subseteq B - A$.

2.4 Leyes de conjuntos

La tabla 2.1, dada en la página 138, muestra las leyes básicas de los conjuntos. Estos resultados, que se asumen como válidos y se llaman leyes, permiten simplificar expresiones que contengan operaciones con conjuntos; también se utilizarán para probar proposiciones que involucran la igualdad de dos conjuntos y, además, sirven para conjeturar nuevos resultados.

Existe una clara relación entre las equivalencias lógicas, dadas en la tabla 1.1, página 58, y las leyes de conjuntos, tabla 2.1. Básicamente, todas las leyes de conjuntos reciben el mismo nombre que las dadas anteriormente, salvo el caso del doble complemento.

Luego de observar detenidamente el siguiente ejemplo, repase el ejemplo 22 dado en la página 59 del capítulo 1 y observe cómo se ha modificado la solución de éste al contexto y lenguaje de los conjuntos.

Ejemplo 36. *Simplifique al máximo la expresión*

$$[A \cup (B \cap C)] \cup (\overline{B} \cap C)$$

Solución. Se toma la expresión y, al aplicar las leyes que se enuncian en la columna de justificación, se va simplificando del siguiente modo:

$[A \cup (B \cap C)] \cup (\overline{B} \cap C)$	**Justificación**
$= A \cup [(B \cap C) \cup (\overline{B} \cap C)]$	Asociatividad
$= A \cup [(B \cup \overline{B}) \cap C)]$	Distributividad
$= A \cup [\mathcal{U} \cap C]$	Inversos
$= A \cup C$	Neutro

con lo cual $[A \cup (B \cap C)] \cup (\overline{B} \cap C) = A \cup C$. ■

Luego de analizar la solución del siguiente ejemplo, compárela con la solución del ejemplo 23 dado en la página 59.

Doble Complemento (DC)	$\overline{\overline{A}} = A$
De Morgan (DM)	$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$
Conmutativa (Con.)	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Asociativa (Aso.)	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
Distributiva (Dis.)	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Idempotencia (Ide.)	$A \cap A = A$ $A \cup A = A$
Neutro (Ne.)	$A \cup \varnothing = A$ $A \cap \mathcal{U} = A$
Inversos (Inv.)	$A \cup \overline{A} = \mathcal{U}$ $A \cap \overline{A} = \varnothing$
Dominación (Dom.)	$A \cap \varnothing = \varnothing$ $A \cup \mathcal{U} = \mathcal{U}$
Absorción (Abs.)	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$

Tabla 2.1: Leyes de conjuntos.

Ejemplo 37. *Simplifique la expresión*

$$\overline{(\overline{B}\cup A)\cap\overline{[(\overline{A}\cap(B\cap C))\cap(A\cup C)]}}$$

Solución. Siguiendo el mismo procedimiento del ejemplo anterior:

$$\begin{array}{ll}
\overline{(\overline{B}\cup A)\cap\overline{[(\overline{A}\cap(B\cap C))\cap(A\cup C)]}} & \textbf{Justificación}\\
=\overline{(\overline{B}\cup A)}\cup\overline{\overline{[(\overline{A}\cap(B\cap C))\cap(A\cup C)]}} & \text{DM}\\
=(\overline{\overline{B}}\cap\overline{A})\cup[(\overline{A}\cap(B\cap C))\cap(A\cup C)] & \text{DM y DC}\\
=(B\cap\overline{A})\cup[((\overline{A}\cap B)\cap C)\cap(A\cup C)] & \text{DC y Asociatividad}\\
=(B\cap\overline{A})\cup[(\overline{A}\cap B)\cap(C\cap(A\cup C))] & \text{Asociatividad}\\
=(\overline{A}\cap B)\cup[(\overline{A}\cap B)\cap C] & \text{Conmutatividad y Absorción}\\
=\overline{A}\cap B & \text{Absorción}
\end{array}$$

la expresión dada es igual a $\overline{A}\cap B$. ■

Observe cómo en los dos ejemplos anteriores se ha pedido solamente la simplificación. En el siguiente ejemplo se probará una identidad.

Ejemplo 38. *Pruebe que la igualdad*

$$\left(A\cup\overline{B}\right)\cap\left[\overline{\left(A\cup\overline{B}\right)}\cup\overline{B}\right]=\overline{B}$$

es verdadera.

Solución. Tome la expresión del lado izquierdo y pruebe que es igual al lado derecho:

$$\begin{array}{ll}
\left(A\cup\overline{B}\right)\cap\left[\overline{\left(A\cup\overline{B}\right)}\cup\overline{B}\right] & \textbf{Justificación}\\
=\left[\left(A\cup\overline{B}\right)\cap\overline{\left(A\cup\overline{B}\right)}\right]\cup\left[\left(A\cup\overline{B}\right)\cap\overline{B}\right] & \text{Distributividad}\\
=\varnothing\cup\overline{B} & \text{Inversos y Absorción}\\
=\overline{B} & \text{Neutro}
\end{array}$$

con lo cual se prueba la igualdad. ■

Ejercicios (sección 2.4)

Simplifique las siguientes expresiones utilizando las leyes de conjuntos. Indique la ley que utiliza en cada paso.

1. $\overline{[(\overline{A}\cup B)\cap A]}\cup B$
2. $\left[A\cup\overline{(\overline{B}\cup\overline{C})}\right]\cup(\overline{B}\cap C)$
3. $[\overline{(\overline{A}\cup B)}\cup C]\cup(\overline{B}\cap C)\cup A$
4. $(\overline{A}\cap B)\cup[\overline{A}\cap\overline{(B\cap C)}]\cup(\overline{A}\cap C)$
5. $[\overline{A}\cup(B\cap A)]\cup[\overline{B}\cap(A\cup B)]$
6. $B\cup\overline{\left[\overline{[(A\cap B)\cup(A\cap\overline{B})]\cup B}\right]\cap A}$
7. $[(A\cup B)\cap\overline{(C\cup A)}]\cup[(C\cap B)\cup A]$
8. $\overline{\left(\overline{A}\cup\overline{B}\right)\cap\left(\overline{B}\cup A\right)}\cap\left(\overline{B}\cup C\right)$
9. $(\overline{A}\cap B)\cup\left[\overline{B\cap C}\cap\overline{A}\right]\cup(A\cap\overline{C})$
10. $\overline{\overline{[(\overline{A}\cup(\overline{B}\cup C))\cup(D\cap C)]}\cup(B\cap A)}$
11. $\left[\left[\overline{(C\cup\overline{A})}\cap(B\cup A)\right]\cup(C\cap A)\right]\cap\overline{A\cap B}$

2.5 Cardinalidad

Cuando se habla de conjuntos, es importante conocer acerca de la cantidad de elementos que lo forman. Algunos de los resultados de esta sección son necesarios en campos como la probabilidad.

Se define la **cardinalidad** de un conjunto A, que se denota $|\boldsymbol{A}|$, como el número de elementos de éste.

Ejemplo 39. *El conjunto vacío no tiene elementos, así,* $|\varnothing| = 0$*; el conjunto* $\{3\}$ *tiene solo un elemento, por lo tanto,* $|\{3\}| = 1$*; el conjunto* $\{*, \dagger, \$\}$ *tiene tres elementos, así,* $|\{*, \dagger, \$\}| = 3$*. El conjunto* $\{5, 5, 5\}$ *contiene solo el elemento* 5*, por lo tanto,* $|\{5, 5, 5\}| = 1$*.* ■

Ejemplo 40. *Determine la cardinalidad de* $A = \big\{\varnothing, \{\ \}, \{3\}, \{\sqrt{9}, 3\}\big\}$*.*

Solución. Como $\varnothing = \{\ \}$ y además $\{3\} = \{\sqrt{9}, 3\}$, los únicos dos elementos diferentes de A son $\varnothing$ y $\{3\}$, por lo tanto, $|A| = 2$. ■

Ejemplo 41. *Considere la proposición abierta* $P(x) : x$ *es un número primo, y el conjunto*

$$A = \{x \in \mathbb{N} \ / \ \ P(x) \ \wedge \ (5 < x \leq 32)\}$$

Determine la cardinalidad de A*.*

Solución. El conjunto A está formado por todos los números naturales que sean primos y que se cumpla $5 < x \leq 32$; por lo tanto, $A = \{7, 11, 13, 17, 19, 23, 29, 31\}$ es la representación por extensión, es decir, A tiene 8 elementos diferentes, $|A| = 8$. ■

Las siguientes fórmulas serán útiles para cuando haya que analizar cardinalidades en problemas que involucran varios conjuntos. Para la cardinalidad de la unión de dos conjuntos, se cumple:

$$|A \cup B| \ = \ |A| + |B| - |A \cap B| \tag{2.1}$$

Ejemplo 42. *Suponga que de un grupo de* 30 *personas,* 15 *saben inglés,* 10 *francés y* 5 *hablan los dos idiomas. ¿Cuántas personas no saben inglés ni francés?*

Solución. Sean A y B los conjuntos formados por las personas que saben inglés y francés respectivamente, se tiene:

$$|A \cup B| = |A| + |B| - |A \cap B| = 15 + 10 - 5 = 20$$

de donde se concluye que son $30 - 20 = 10$ las personas que no saben inglés ni francés. ■

Para el caso particular en que los conjuntos sean disjuntos, el resultado anterior se conoce como el *principio de la regla de la suma*:

Principio de la regla de la suma
Si A y B son conjuntos finitos y disjuntos, $A \cap B = \varnothing$, se cumple que:

$$|A \cup B| = |A| + |B|$$

Esto equivale a pensar que si se tienen dos eventos independientes E y F, es decir, que no pueden ocurrir simultáneamente, y si el primer evento E puede ocurrir de n formas diferentes y el segundo evento F puede ocurrir de m formas diferentes, entonces el evento E o F puede ocurrir de $n + m$ formas diferentes.

Ejemplo 43. *Suponga que Manuel desea pedir en préstamo un libro de poesía; en el estante se tienen* 5 *títulos de un autor y* 6 *de otro; es claro que Manuel puede escoger el libro de* $5 + 6 = 11$ *formas diferentes.* ■

Ejemplo 44. *Para* $A = \{a, b, c\}$ *y* $B = \{2, 3, 5, 7\}$*, es claro que* A *y* B *son conjuntos disjuntos; como* $|A| = 3$ *y* $|B| = 4$*, se tiene que* $|A \cup B| = 3 + 4 = 7$. ■

Para el caso de la unión de tres conjuntos, se puede demostrar (véase ejercicio 18) que se satisface:

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| \\ &\quad - |B \cap C| + |A \cap B \cap C| \end{aligned} \tag{2.2}$$

Ejemplo 45. *Se realizó una encuesta a* 4800 *niños, en la cual se obtuvo la siguiente información: a* 2300 *les gustan los juegos de acción; a* 2000 *los juegos de aventuras; a* 1250 *los juegos de deportes. También se obtuvo que a* 550 *no les gustó ninguno de estos juegos, pues les gustan los de estrategias, y* 50 *niños no tienen preferencia por ninguno de los juegos mencionados. Además, hay* 100 *niños a quienes les gustan los tres juegos;* 300 *los de aventuras y deportes, y a* 800 *solamente les gustan de aventuras. Realice el Diagrama de Venn para esta situación y encuentre el número de personas de cada región disjunta. ¿A cuántos niños les gustan solo los juegos de acción?, ¿a cuántos niños les gustan solo los juegos de acción y deportes?, ¿a cuántos niños les gustan los juegos de acción y deportes?, ¿a cuántos niños les gusta solo un juego?*

Solución. De acuerdo con los datos dados, es posible representar tres conjuntos A, B y C formados por los niños a quienes les gustan los juegos de acción, aventuras y deportes, respectivamente. Además, aparte de ellos hay dos conjuntos disjuntos formados por los 550 niños a quienes les gustan juegos de estrategia, y los 50 niños a quienes no les gusta ninguno. Para representar esta situación, analice primero la frase "a 300 les gustan de aventuras y deportes", que sería muy diferente a la frase "a 300 les gustan solamente de aventuras y deportes"; con la primera están incluidos los 100 que gustan de los deportes (si les gustan los tres, lógicamente les gustan dos), con la segunda, estos 100 no están incluidos. En la figura 2.5 se representa con la variable x la cantidad de niños a quienes les gustan juegos de acción y deportes, pero no de aventuras. Note que la cardinalidad de $A \cup B \cup C$ es $4800 - 550 - 50 = 4200$. Con

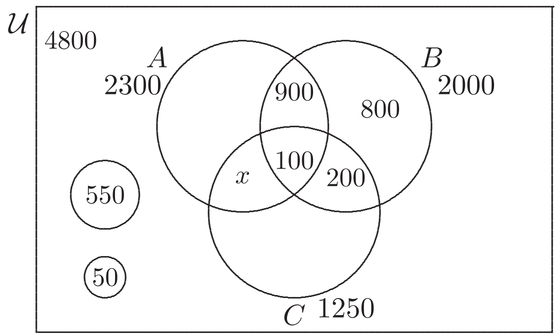


Figura 2.5: Representación de regiones disjuntas.

estos datos y aplicando la fórmula (2.2), se puede plantear la ecuación:

$$4200 = 2300 + 2000 + 1250 - 300 - 1000 - (x + 100) + 100$$

cuya solución es $x = 50$. Con ello, note que a $2300-900-100-50 = 1250$ niños a quienes les gustan solo los juegos de acción. Análogamente, solo a 900 niños les gustan de deportes. Les gustan solo los juegos de acción y deportes a 50 niños. Les gustan los juegos de acción y deportes a $100 + 50 = 150$ niños. Por último, les gusta solo un juego a $1250 + 800 + 900 + 550 = 3500$ niños. ■

El siguiente resultado se conoce como el *principio de la regla del producto*, que es equivalente a pensar que si se tienen dos eventos independientes E y F, y el evento E puede ocurrir de n formas diferentes y el evento F puede ocurrir de m formas diferentes, entonces las combinaciones de E y de F pueden ocurrir de nm formas diferentes.

Principio de la regla del producto
Si A y B son conjuntos finitos, se cumple que:

$$|A \times B| = |A| \cdot |B|$$

Ejemplo 46. *Como en el ejemplo* 43*, suponga ahora que Manuel desea pedir dos libros, uno de cada autor; de esta forma, la escogencia la podría hacer de* $5 \cdot 6 = 30$ *formas diferentes.* ■

Ejemplo 47. *En un restaurante se ofrece el plato ejecutivo, donde se puede escoger entre* 2 *tipos de refresco,* 4 *tipos de plato principal,* 3 *tipos de ensalada y* 4 *tipos de postres. La cantidad de posibles combinaciones, es decir, la cantidad de posibles platos completos diferentes que se ofrecen, es de* $2 \cdot 4 \cdot 3 \cdot 4 = 96$*.* ■

Ejemplo 48. *Para* $A = \{a, b, c\}$ *y* $B = \{2, 3, 5, 7\}$*, es claro que* A *y* B *son conjuntos disjuntos; como* $|A| = 3$ *y* $|B| = 4$*, se tiene que* $|A \cup B| = 3 + 4 = 7$*, mientras que* $|A \times B| = 3 \cdot 4 = 12$*.* ■

Cardinalidad del conjunto diferencia
Para A y B conjuntos finitos, se satisface la identidad:

$$|A - B| = |A| - |A \cap B|$$

Ejemplo 49. *Para los conjuntos* $A = \{a, b, c, d, e, f\}$ *y* $B = \{b, e, h\}$*, es claro que* A *contiene* 6 *elementos y* B *tiene* 3 *elementos, por lo que* $|A| = 6$ *y* $|B| = 3$*; además,* $|A \cap B| = 2$*, utilizando el resultado anterior,* $|A - B| = |A| - |A \cap B| = 6 - 2 = 4$*. Por otro lado, se puede aplicar la misma fórmula para calcular también que* $|B - A| = |B| - |B \cap A| = 3 - 2 = 1$*.* ■

El siguiente resultado se puede demostrar utilizando el Principio de Inducción, pero se hará posteriormente en el ejercicio 19 de la sección 5.2 (véase página 292).

Cardinalidad del conjunto potencia
Si A es un conjunto finito, se satisface la identidad:

$$|P(A)| = 2^{|A|}$$

Ejemplo 50. *Para los conjuntos* $A = \{1, 2\}$ *y* $B = \{a, b, c\}$*, es claro que* A *contiene* 2 *elementos y* B *tiene* 3 *elementos, por lo que* $|A| = 2$ *y* $|B| = 3$*; utilizando el resultado anterior,* $|P(A)| = 2^2 = 4$*, mientras que* $|P(B)| = 2^3 = 8$*.* ■

Ejemplo 51. *Si* $A = \{a, \{a\}, b\}$ *y* $B = \{2, 3, 5, 7\}$*, determine* $|A|$*,* $|B|$*,* $|P(A)|$*,* $|A \times B|$*.*

Solución. Como A tiene tres elementos y B tiene cuatro elementos, $|A| = 3$, $|B| = 4$, $|P(A)| = 2^3 = 8$, $|A \times B| = 3 \cdot 4 = 12$. ■

Ejemplo 52. *Si* $|A| = 4$ *y* $|B| = 3$*, determine* $|P(A) \times B|$*,* $|P(A \times B)|$*,* $|P(P(A))|$*.*

Solución. Como A tiene 4 elementos, $P(A)$ tiene 2^4 elementos, así:

$$|P(A) \times B| = 2^4 \cdot 3 = 48$$

Por otro lado, $|A \times B| = 4 \cdot 3$, con lo cual:

$$|P(A \times B)| = 2^{4 \cdot 3} = 2^{12} = 4096$$

Por último, como se sabe que $P(A)$ tiene $2^4 = 16$ elementos, se tiene que $|P(P(A))| = 2^{2^4} = 2^{16} = 65536$. ■

Ejercicios (sección 2.5)

1. Una biblioteca cuenta con 8 títulos diferentes de poesía, 6 de novela y 7 de cuento. De cuántas formas se puede hacer la escogencia si una persona:

   (a) Solo desea un libro.

   (b) Desea 3 libros.

   (c) Desea 3 libros, uno de cada tipo.

2. En una ciudad se distribuyen 10 periódicos diariamente. Si una persona desea comprar solo 2 periódicos diferentes, ¿de cuántas maneras puede efectuar dicha compra?

3. En una encuesta aplicada a 135 personas acerca de los medios de información que utilizan para enterarse de las noticias, se obtuvo la siguiente información: 70 utilizan la prensa escrita; 83, la radio; 74, la televisión; 50, la prensa escrita y la radio; 38, la prensa escrita y la televisión; 41, la radio y la televisión; por último, 27 personas utilizan la prensa escrita, la radio y la televisión.

   (a) ¿Cuántas personas utilizan al menos uno de los tres medios de información?

   (b) ¿Cuántas personas utilizan exactamente dos de esos tres medios de información?

4. Se realizó una encuesta de preferencia a 4065 músicos, en la cual se obtuvo la siguiente información: a 2500 les gusta tocar guitarra; a 2200, tocar la batería; 1400 prefieren el saxofón. También se obtuvo que a 50 no les gustó ninguno de estos instrumentos, pues prefieren el piano, y 15 músicos no tienen preferencia por ninguno de los instrumentos mencionados. Además, hay 300 músicos a quienes les gusta la guitarra, la batería y el saxofón; 1000 prefieren solamente la batería, y 400 prefieren solamente la batería y el saxofón.

   (a) Realice el Diagrama de Venn para esta situación y encuentre el número de personas de cada región disjunta.

   (b) ¿Cuántos músicos prefieren solamente la guitarra?

   (c) ¿Cuántos músicos prefieren solamente el saxofón?

   (d) ¿Cuántos músicos prefieren la guitarra y el saxofón?

   (e) ¿A cuántos músicos les gusta solo un instrumento?

5. En un estudio realizado sobre 1200 personas, se obtuvo lo siguiente: solo 1000 observan deportes, de los cuales, a 420 les gusta el fútbol; a 500 el atletismo y a 550 el ciclismo. A 50 de las personas les gustan los tres deportes; a 170 les gusta el fútbol y el atletismo, y a 200 les gusta el ciclismo y el atletismo.

   (a) Realice el Diagrama de Venn para esta situación y encuentre el número de personas de cada región disjunta.

   (b) ¿A cuántas personas les gusta solamente un deporte?

6. De un conjunto de 120 estudiantes de una facultad, 100 eligieron por lo menos un idioma entre francés, alemán y ruso. De éstos, 65 estudian francés, 45 estudian alemán y 42 estudian ruso. También se sabe que 8 escogieron los tres idiomas, que 20 estudian francés y alemán, y que 15 estudian alemán y ruso.

   (a) Determine el número de estudiantes que estudian francés y ruso.

   (b) Determine el número correcto de estudiantes en cada una de las ocho regiones, mediante un Diagrama de Venn.

   (c) ¿Cuántos estudian exactamente uno de los tres idiomas?

7. En un barco viajaban 3000 personas, de las cuales 200 hablaban inglés, danés e italiano; 2500 hablaban inglés; 600 hablaban danés y 1000, italiano; 100 personas hablaban solamente italiano y danés, y 700 hablaban inglés e italiano.

   (a) Realice el Diagrama de Venn para esta situación y encuentre el número de personas de cada región disjunta.

   (b) ¿Cuántos hablan solamente inglés?

   (c) ¿Cuántos hablan inglés y danés?

   (d) ¿Cuántos hablan solamente italiano?

8. Si $|A| = 2$ y $|B| = 3$, calcule:

   (a) $|P(A) \times P(B)|$

   (b) $|P(A \times B)|$

9. Si $|A| = 3$ y $|B| = 5$, calcule:

   (a) $|P(A) \times B|$

   (b) $|P(A \times B)|$

   (c) $|A \times P(B)|$

   (d) $|P(P(P(A)))|$

10. Sean A y B conjuntos arbitrarios que cumplen $|A| = 2$, $|B| = 4$ y $|A \cap B| = 1$, determine las siguientes cardinalidades:

    (a) $|P(B - A) \times A|$

    (b) $\big|P\big((A \cup B) \times (A - B)\big)\big|$

    (c) $|P(P(A))|$

11. Sean A, B y C conjuntos arbitrarios tal que $|A| = 5$, $|A \cap C| = 2$ y $|A \times P(B)| = 80$. Determine la cardinalidad de los conjuntos:

    (a) $P(A) \times B$

    (b) $(A - C) \times P(A) \times P(B)$

12. Para los conjuntos $A = \{0\}$, $B = \{2, 4\}$ y $C = \{0, 3, 4, 5\}$, calcule la cardinalidad del conjunto $(C - A) \times P(B \cup C)$.

13. Sean A, B y C conjuntos arbitrarios que cumplen con: $|A| = 5$, $|B| = 4$, $|A \cap B| = 2$, $|P(C)| = 64$, $|C - A| = 2$. Determine:

    (a) La cardinalidad del conjunto $(A - B) \times P(C - A)$

    (b) La cardinalidad del conjunto $P[(A \cap C) \times C]$

14. Sean A, B y C conjuntos arbitrarios tales que $B \cap C = \varnothing$, $|A| = 8$, $|B| = 5$, $|A \cap B| = 2$, $|P(C)| = 128$, $|C - A| = 4$. Calcule:

    (a) La cardinalidad de $(A - (B \cup C)) \times P(A - C)$.

    (b) La cardinalidad de $P[(A \cap C) \times C]$.

15. Si $A = \{w, 2\}$ y $B = \{2, 3\}$, donde el conjunto universo es $\mathcal{U} = \{2, 3, w\}$, ¿cuántos elementos tiene el conjunto $\overline{P(A \times B)}$?

16. Sean A, B y D conjuntos arbitrarios tales que $|A| = 3$, $|B| = 3$, $|A \cap B| = 1$, $|B - D| = 2$, $|D| = 4$. Calcule la cardinalidad de $P(A \cap D) \times (B \cup D) \times P(A \cup D)$.

17. Muestre, si es posible, un conjunto A que cumpla:

    (a) $A \subseteq P(A)$

    (b) $|P(A)| = 64$

    (c) $|P(P(P(A)))| = 16$

    (d) $|P(A \cup P(A))| = 64$

    (e) $|P(A \cup P(A))| = 32$

    (f) $|P(A) - A| = 15$

18. Utilice la fórmula (2.1) para demostrar la fórmula (2.2).

19. Con base en las fórmulas (2.1) y (2.2), conjeture una posible fórmula para $|A \cup B \cup C \cup D|$.

2.6 Familias de conjuntos

De forma análoga a como se define la unión e intersección de dos conjuntos, se generaliza de forma natural y se define la unión e intersección de una colección de conjuntos que puede contener, incluso, una cantidad infinita de ellos, que se llamará *familia de conjuntos*. En general, una familia de conjuntos será un conjunto S de conjuntos A_i, con i en una colección de índices I.

Ejemplo 53. *Observe que* $S = \big\{\{0\}, \{0,5\}, \{2,x,6\}, \{x,y\}\big\}$ *es una familia finita de conjuntos, donde se puede tomar como conjunto de índices a* $I = \{1,2,3,4\}$ *y como elementos de esta familia a* $A_1 = \{0\}$, $A_2 = \{0,5\}$, $A_3 = \{2,x,6\}$, $A_4 = \{x,y\}$. *Con esta notación, es posible escribir* $S = \{A_i\}_{i\in I}$. ■

Un elemento x estará en la unión de una familia si está en al menos uno de los conjuntos de ésta, y estará en la intersección de la familia si está incluido en cada uno de los conjuntos de ésta, es decir:

Dada una familia de conjuntos $\{A_i\}$, definida para una colección de índices I, con I finito o infinito, se definen los conjuntos:

$$\begin{aligned}\bigcup_{i\in I} A_i &= \{x \ / \ \exists k \in I \ \text{ tal que } \ x \in A_k\}\\ \bigcap_{i\in I} A_i &= \Big\{x \ / \ \forall k \in I\,[x \in A_k]\Big\}\end{aligned}$$

Ejemplo 54. *Para la familia de conjuntos del ejemplo 53, se tiene que los elementos que se encuentran en al menos un conjunto de S, forman la unión de dicha familia, es decir,* $\displaystyle\bigcup_{i\in I} A_i = \bigcup_{i=1}^{4} A_i = \{0,5,2,x,6,y\}$; *además, el conjunto* $\displaystyle\bigcap_{i\in I} A_i = \bigcap_{i=1}^{4} A_i = \varnothing$, *pues no existe un elemento que se encuentre en todos los conjuntos que conforman la familia S.* ■

Ejemplo 55. *Observe que si se definen los conjuntos A_i como los intervalos $A_i = [-i, i]$ para todo $i \in \mathbb{N}$, se obtiene la familia de conjuntos $S = \{A_i\}$; con el conjunto de índices $I = \mathbb{N}$, se tiene que la unión de la familia S es*

$$\bigcup_{i\in\mathbb{N}} A_i = \bigcup_{n=0}^{+\infty} A_n = \mathbb{R}$$

y el conjunto

$$\bigcap_{i\in\mathbb{N}} A_i = \bigcap_{n=0}^{+\infty} A_n = \{0\}$$

■

Ejemplo 56. *Si se define el conjunto $A_n = \{0, 1, 2, \ldots, n+1\}$ para cada número natural n, es posible obtener los conjuntos*

$$\bigcup_{i\in\mathbb{N}} A_i = \bigcup_{n=0}^{+\infty} A_n = \mathbb{N}$$

y el conjunto

$$\bigcap_{i\in\mathbb{N}} A_i = \bigcap_{n=0}^{+\infty} A_n = \{0, 1\}$$

■

Ejemplo 57. *Si se define el conjunto $A_n = \{0, n\}$ para cada número natural n, se obtiene el nuevo conjunto*

$$\bigcap_{i\in\mathbb{N}} P(A_i) = \{\varnothing, \{0\}\}$$

pues los únicos elementos que pertenecen a todos los conjuntos $P(A_i)$ son $\varnothing$, $\{0\}$. ■

Ejemplo 58. *Si se define el conjunto* A_n *como el intervalo cerrado* $\left[0, \frac{1}{n}\right]$ *para cada número natural positivo* n*, es decir,* $A_n = \left[0, \frac{1}{n}\right]$*, se pueden calcular los conjuntos*

$$\bigcup_{i \in \mathbb{N}^*} A_i = \bigcup_{n=0}^{+\infty} A_n = [0, 1]$$

y el conjunto

$$\bigcap_{i \in \mathbb{N}^*} A_i = \bigcap_{n=0}^{+\infty} A_n = \{0\}$$

■

Ejercicios (sección 2.6)

1. Sea $A_n = \{k \in \mathbb{Z} \ / \quad -n \leq k \leq n\}$ para todo entero $n \geq 0$. Calcule:

   (a) $A_2 \times A_0$

   (b) $(A_7 - A_5) \cup (A_6 \cap A_3)$

   (c) $\displaystyle\bigcap_{n=0}^{+\infty} (\mathbb{Z} - A_n)$

2. Calcule $\displaystyle\bigcup_{i \in \mathbb{N}^*} A_i$ y $\displaystyle\bigcap_{i \in \mathbb{N}^*} A_i$ para cada uno de las siguientes familias de conjuntos A_n:

   (a) $A_n = \left[\dfrac{1}{n}, 3\right]$

   (b) $A_n = \left]-\dfrac{1}{n}, \dfrac{1}{n}\right[$

   (c) $A_n = \left[2^{-n}, 2^n\right]$

   (d) $A_n = [1 + (-1)^n, 4]$

   (e) $A_n = \left[\dfrac{1 + (-1)^n}{n}, 4\right]$

3. Defina el conjunto $I_n = \left[3 - \dfrac{1}{n}, 4 + \dfrac{1}{n}\right[$ para cada natural n, con $n \neq 0$. Calcule el conjunto $A = \displaystyle\bigcup_{n=1}^{+\infty} I_n$ y el conjunto $B = \displaystyle\bigcap_{n=1}^{+\infty} I_n$.

4. Para la familia de conjuntos $\{A_n\}_{n\in\mathbb{N}}$, se definen:

$$\begin{aligned} \overline{\lim} A_n &= \bigcap_{n=0}^{+\infty} \left(\bigcup_{k=0}^{+\infty} A_{n+k} \right) \\ \underline{\lim} A_n &= \bigcup_{n=0}^{+\infty} \left(\bigcap_{k=0}^{+\infty} A_{n+k} \right) \end{aligned}$$

   Si $A_n = [0, n+1]$ para $n \in \mathbb{N}$, calcule $\overline{\lim} A_n$ y $\underline{\lim} A_n$.

2.7 Resultados y demostraciones

En esta sección se pretende introducir al lector en las demostraciones de proposiciones lógicas que involucran conjuntos. Para ello es fundamental tener claras las definiciones dadas anteriormente y, por supuesto, las leyes de la lógica y las reglas de inferencia.

Algunos de los ejercicios propuestos al final de la sección son, en realidad, teoremas dentro de la teoría de conjuntos; sin embargo, para ganar claridad en la exposición, se ha omitido la formalidad, no así la rigurosidad.

Si aún no lo ha hecho, se recomienda repasar la sección 1.8, en la página 99, donde se exponen algunos de los métodos que se pueden utilizar para demostrar proposiciones que involucran, principalmente, las implicaciones lógicas. Note que, en los siguientes ejemplos, las demostraciones corresponden a tautologías y por lo tanto se utiliza el simbolo $\Rightarrow$ en vez de $\rightarrow$.

Ejemplo 59. *Demuestre la validez de la proposición*

$$(A - B) - C \subseteq A - (B \cup C)$$

Solución. Se debe probar una inclusión, es decir, probar que

$$\forall a \,[a \in (A - B) - C \Rightarrow a \in A - (B \cup C)\,]$$

cuya prueba es:

$$\begin{aligned}
a \in (A - B) - C &\Rightarrow a \in A - B \,\wedge\, a \notin C \\
&\Rightarrow (a \in A \,\wedge\, a \notin B) \,\wedge\, a \notin C \\
&\Rightarrow a \in A \,\wedge\, \neg(a \in B \,\vee\, a \in C) \\
&\Rightarrow a \in A \,\wedge\, \neg(a \in B \cup C) \\
&\Rightarrow a \in A \,\wedge\, a \notin B \cup C \\
&\Rightarrow a \in A - (B \cup C)
\end{aligned}$$

■

Ejemplo 60. *Demuestre la validez de la proposición*

$$A - (B \cup C) = (A - B) \cap (A - C)$$

Solución. Se debe probar la igualdad de dos conjuntos, es decir, que $A - (B \cup C) \subseteq (A - B) \cap (A - C)$ y además, se debe probar que $(A - B) \cap (A - C) \subseteq A - (B \cup C)$; en este caso, se probarán ambas inclusiones con una sola equivalencia:

$$\begin{aligned}
a \in A - (B \cup C) \quad &\Leftrightarrow \quad a \in A \ \wedge \ a \notin (B \cup C) \\
&\Leftrightarrow \quad a \in A \ \wedge \ a \notin B \ \wedge \ a \notin C \\
&\Leftrightarrow \quad (a \in A \ \wedge \ a \notin B) \ \wedge \ (a \in A \ \wedge \ a \notin C) \\
&\Leftrightarrow \quad a \in (A - B) \ \wedge \ a \in (A - C) \\
&\Leftrightarrow \quad a \in (A - B) \cap (A - C)
\end{aligned}$$

■

Ejemplo 61. *Demuestre la validez de la proposición*

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Solución. Al igual que en el ejemplo anterior, se debe probar una igualdad de dos conjuntos; en este caso, se debe probar que $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ y además, se debe probar que $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

$$\begin{aligned}
a \in \overline{A \cap B} \quad &\Leftrightarrow \quad \neg(a \in A \cap B) \\
&\Leftrightarrow \quad \neg(a \in A \ \wedge \ a \in B) \\
&\Leftrightarrow \quad a \notin A \ \vee \ a \notin B \\
&\Leftrightarrow \quad a \in \overline{A} \ \vee \ a \in \overline{B} \\
&\Leftrightarrow \quad a \in \overline{A} \cup \overline{B}
\end{aligned}$$

■

Antes del siguiente ejemplo, recuerde que la proposición $A \subseteq B$ es equivalente a que para todo x se satisface $x \in A \Rightarrow x \in B$, lo cual es equivalente, aplicando la contrapositiva de la implicación, a la proposición $x \notin B \Rightarrow x \notin A$. Simbólicamente, se escribe como:

$$A \subseteq B \Longleftrightarrow (\forall x)\ [x \in A \Rightarrow x \in B] \Longleftrightarrow (\forall x)\ [x \notin B \Rightarrow x \notin A]$$

que, iniciando en el siguiente ejemplo, se utilizará con frecuencia.

Ejemplo 62. *Pruebe la validez de la proposición*

$$(A \subseteq B\ \wedge\ A \subseteq D) \Rightarrow \overline{B \cap D} \subseteq \overline{A}$$

Solución. Para probar esta implicación, con $A \subseteq B\ \wedge\ A \subseteq D$ como hipótesis, se debe probar que $\overline{B \cap D} \subseteq \overline{A}$, es decir, se debe probar que:

$$\forall a \left[a \in \overline{B \cap D} \Rightarrow a \in \overline{A}\,\right]$$

Para ello considere un elemento arbitrario a y la prueba es:

$$\begin{array}{lll} & a \in \overline{B \cap D} & \\ \Rightarrow & a \notin (B \cap D) & \\ \Rightarrow & a \notin B\ \vee\ a \notin D & \text{(por ley de De Morgan)} \\ \Rightarrow & a \notin A\ \vee\ a \notin A & \text{(contrapositiva de la hipótesis } A \subseteq B) \\ \Rightarrow & a \in \overline{A} & \text{(por ley de idempotencia)} \end{array}$$

al ser a arbitrario, se ha probado para todo a. ■

Ejemplo 63. *Demuestre la validez de la proposición*

$$C \subseteq A \cap B \Rightarrow C \cap (B - A) = \varnothing$$

Solución. Se debe probar que, bajo la hipótesis $C \subseteq A \cap B$, se cumple $C \cap (B - A) = \varnothing$. Se efectúa la prueba por contradicción, es decir, suponga que $C \cap (B - A) \neq \varnothing$; a partir de esta proposición, se sigue:

$$\begin{aligned}
& \exists a \in C \cap (B - A) \\
\Rightarrow\ & (a \in C) \ \wedge\ (a \in B - A) \\
\Rightarrow\ & (a \in A \cap B) \ \wedge\ (a \in B \ \wedge\ a \notin A) \qquad \text{(por hipótesis)} \\
\Rightarrow\ & (a \in A \ \wedge\ a \in B) \ \wedge\ (a \in B \ \wedge\ a \notin A) \\
\Rightarrow\ & a \in A \ \wedge\ a \notin A \quad (\Rightarrow\Leftarrow)
\end{aligned}$$

La última proposición es una contradicción, que se obtuvo al suponer que $C \cap (B - A) \neq \varnothing$, con lo cual esta suposición es falsa y se concluye que $C \cap (B - A) = \varnothing$ es verdadera. ■

Ejemplo 64. *Sin hacer uso de la demostración por contradicción, como ya se realizó en el ejemplo anterior, y utilizando la Prueba Directa, demuestre la validez de la proposición*

$$C \subseteq A \cap B \Rightarrow C \cap (B - A) = \varnothing$$

Solución. De nuevo, bajo la hipótesis $C \subseteq A \cap B$, se debe probar la validez de la proposición $C \cap (B - A) = \varnothing$, su conclusión. Observe que lo que se debe probar es una igualdad de conjuntos, así, en virtud de la definición, es necesario comprobar ambas inclusiones:

"$\subseteq$" Se debe probar que $C \cap (B - A) \subseteq \varnothing$, para ello:

$$\begin{aligned}
& x \in C \cap (B - A) \\
\Rightarrow\ & x \in C \ \wedge\ x \in B - A \\
\Rightarrow\ & x \in A \cap B \ \wedge\ x \in B - A \qquad \text{(Hipótesis)} \\
\Rightarrow\ & x \in A \ \wedge\ x \in B \ \wedge\ x \in B \ \wedge\ x \notin A \\
\Rightarrow\ & x \in A \ \wedge\ x \in \overline{A} \qquad \text{(Simplificación)} \\
\Rightarrow\ & x \in (A \cap \overline{A}) \\
\Rightarrow\ & x \in \varnothing \qquad \text{(Ley de inversos)}
\end{aligned}$$

"$\supseteq$" Es claro que $C \cap (B - A) \supseteq \varnothing$ (véase ejemplo 10).

con lo cual, se completa la prueba. ■

Ejemplo 65. *Demuestre la validez de la proposición*

$$A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$$

Solución. Se debe probar una equivalencia; para ello, se probarán ambas implicaciones:

"$\Rightarrow$" Bajo la hipótesis $A \subseteq B$, se debe probar que $P(A) \subseteq P(B)$, es decir, que $\forall S\, [S \in P(A) \Rightarrow S \in P(B)]$.
Prueba:

$$\begin{aligned} S \in P(A) &\Rightarrow S \subseteq A \\ &\Rightarrow S \subseteq B \qquad \text{(por hipótesis)} \\ &\Rightarrow S \in P(B) \end{aligned}$$

"$\Leftarrow$" Bajo la hipótesis $P(A) \subseteq P(B)$, se debe probar que $A \subseteq B$, es decir, que $\forall x\, [x \in A \Rightarrow x \in B]$.
Prueba:

$$\begin{aligned} x \in A &\Rightarrow \{x\} \subseteq A \\ &\Rightarrow \{x\} \in P(A) \\ &\Rightarrow \{x\} \in P(B) \qquad \text{(por hipótesis)} \\ &\Rightarrow \{x\} \subseteq B \\ &\Rightarrow x \in B \end{aligned}$$

con lo cual se ha probado la equivalencia deseada. ■

Ejemplo 66. *Demuestre que la proposición*

$$(A - B) \times C = (A \times C) - (B \times C)$$

es verdadera.

Solución. Para probar esta igualdad entre conjuntos, se deben probar dos inclusiones: $(A - B) \times C \subseteq (A \times C) - (B \times C)$ y $(A - B) \times C \supseteq (A \times C) - (B \times C)$, que se probarán por separado:

"$\subseteq$" Es necesario probar que

$$\forall (a, c) \left[(a, c) \in (A - B) \times C \Rightarrow (a, c) \in (A \times C) - (B \times C) \right]$$

Prueba:

$$\begin{aligned}
(a, c) \in (A - B) \times C \quad &\Rightarrow \quad a \in (A - B) \ \wedge \ c \in C \\
&\Rightarrow \quad (a \in A \ \wedge \ a \notin B) \ \wedge \ c \in C \\
&\Rightarrow \quad (a \in A \ \wedge \ c \in C) \ \wedge \ (a \notin B \ \wedge \ c \in C) \\
&\Rightarrow \quad (a, c) \in A \times C \ \wedge \ (a, c) \notin B \times C \\
&\Rightarrow \quad (a, c) \in (A \times C) - (B \times C)
\end{aligned}$$

"$\supseteq$" Es necesario probar que

$$\forall (a, c) \left[(a, c) \in (A \times C) - (B \times C) \Rightarrow (a, c) \in (A - B) \times C \right]$$

Prueba:

$$\begin{aligned}
& \quad (a, c) \in (A \times C) - (B \times C) \\
\Rightarrow & \quad (a, c) \in A \times C \ \wedge \ (a, c) \notin B \times C \\
\Rightarrow & \quad (a \in A \ \wedge \ c \in C) \ \wedge \ (a \notin B \ \vee \ c \notin C) \qquad \text{(De Morgan)} \\
\Rightarrow & \quad (a \in A \ \wedge \ c \in C \ \wedge \ a \notin B) \ \vee \ \underbrace{(a \in A \ \wedge \ c \in C \ \wedge \ c \notin C)}_{\text{es una contradicción}} \\
\Rightarrow & \quad (a \in A \ \wedge \ c \in C \ \wedge \ a \notin B) \qquad \text{(ley del neutro)} \\
\Rightarrow & \quad (a \in A \ \wedge \ a \notin B) \ \wedge \ c \in C \\
\Rightarrow & \quad a \in (A - B) \ \wedge \ c \in C \\
\Rightarrow & \quad (a, c) \in (A - B) \times C
\end{aligned}$$

lo cual completa la prueba. $\blacksquare$

Para comprender mejor el paso de la prueba del ejemplo anterior, en donde se indica la aplicación de la ley de De Morgan, es importante recordar que, por esta ley, se tiene que:

$$\begin{aligned}(a,c) \notin B \times C &\equiv \neg[(a,c) \in B \times C]\\ &\equiv \neg[a \in B \ \wedge \ c \in C]\\ &\equiv a \notin B \ \vee \ c \notin C\end{aligned}$$

Ejemplo 67. *Muestre que la proposición* $(A - B) \cup C \subseteq A - (B - C)$ *no es verdadera.*

Solución. Para probar que esta inclusión no es verdadera, basta con mostrar conjuntos que no la satisfagan, es decir, encontrar un contraejemplo (véase página 104); para ello considere $A = \{1\}$, $B = \{2\}$ y $C = \{2\}$; para estos conjuntos se tiene que $(A - B) \cup C = \{1, 2\}$ y $A - (B - C) = \{1\}$, y es claro que $\{1, 2\} \nsubseteq \{1\}$. ∎

Para finalizar esta sección, observe con atención el siguiente ejemplo; en él se propone la demostración de una proposición condicional y se da su prueba. Luego se presentan dos pruebas alternativas, la directa y la indirecta (véase página 101), válidas y muy instructivas. Es importante que en cada una de la pruebas identifique el momento en que se utiliza la hipótesis.

Ejemplo 68. *Pruebe que* $A \cap B = \varnothing \Rightarrow A \subseteq \overline{B}$.

Solución. Con hipótesis $A \cap B = \varnothing$, se tiene que

$$\begin{aligned} x \in A &\Rightarrow x \notin B\\ &\Rightarrow x \in \overline{B}\end{aligned}$$

es decir, se ha probado que $A \subseteq \overline{B}$. ∎

Observe la *Prueba Indirecta* de $A \cap B = \varnothing \Rightarrow A \subseteq \overline{B}$:

$$\begin{aligned} A \not\subseteq \overline{B} &\Rightarrow \exists x\,[x \in A \;\wedge\; x \notin \overline{B}] \\ &\Rightarrow \exists x\,[x \in A \;\wedge\; x \in B] \\ &\Rightarrow \exists x\,[x \in A \cap B] \\ &\Rightarrow A \cap B \neq \varnothing \end{aligned}$$

Es decir, se probó $A \not\subseteq \overline{B} \Rightarrow A \cap B \neq \varnothing$, con lo cual la contrapositiva de esta proposición, $A \cap B = \varnothing \Rightarrow A \subseteq \overline{B}$, es verdadera.

Ahora, observe la *Prueba Directa* de $A \cap B = \varnothing \Rightarrow A \subseteq \overline{B}$:

$$\begin{aligned} A \cap B = \varnothing &\Rightarrow \nexists x[x \in A \cap B] \\ &\Rightarrow \forall x[x \notin A \cap B] \\ &\Rightarrow \forall x[x \in \overline{A \cap B}] \\ &\Rightarrow \forall x[x \in \overline{A} \cup \overline{B}] \\ &\Rightarrow \forall x[x \in \overline{A} \vee x \in \overline{B}] \\ &\Rightarrow \forall x[x \notin \overline{A} \Rightarrow x \in \overline{B}] \\ &\Rightarrow \forall x[x \in A \Rightarrow x \in \overline{B}] \\ &\Rightarrow A \subseteq \overline{B} \end{aligned}$$

Ejercicios (sección 2.7)

1. Sean A, B, C y D conjuntos arbitrarios. Demuestre la validez de las siguientes inclusiones:

   (a) $A - (B \cup C) \subseteq (A - B) \cup C$

   (b) $P(A) \cup P(B) \subseteq P(A \cup B)$

   (c) $\overline{A} \times \overline{B} \subseteq \overline{A \times B}$

   (d) $B - A \subseteq \overline{A - B}$

   (e) $A \cap B \subseteq A$

   (f) $A \subseteq A \cup B$

(g) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

(h) $A \cap B \subseteq \overline{A \triangle B}$

(i) $P(A - B) \subseteq [P(A) - P(B)] \cup \{\varnothing\}$

2. Sean A, B, C y D conjuntos arbitrarios. Demuestre la validez de las siguientes igualdades:

(a) $A \cap (B - A) = \varnothing$

(b) $A - (B \cap C) = (A - B) \cup (A - C)$

(c) $A \cap (B - C) = (A \cap B) - (A \cap C)$

(d) $(A - B) - C = A - (B \cup C)$

(e) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

(f) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(g) $A \cap (A \cup B) = A$

(h) $A \cap \overline{A} = \varnothing$

(i) $A \cap \varnothing = \varnothing$

(j) $A \times (B - C) = (A \times B) - (A \times C)$

(k) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(l) $(A \cap B) \cup \left(A \cap \overline{B}\right) = A$

(m) $(A - C) - (B - C) = (A - B) - C$

(n) $(A \cap C) - B = (A - B) \cap (C - B)$

(o) $A \times \left(\overline{B \cap C}\right) = \left(A \times \overline{B}\right) \cup \left(A \times \overline{C}\right)$

(p) $A \times \left(\overline{B - C}\right) = \left(A \times \overline{B}\right) \cup (A \times C)$

(q) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

(r) $A \triangle B = (A \cup B) - (A \cap B)$

(s) $A - (B \cup C) = (A - B) \cap \overline{C}$

(t) $P(A) \cap P(B) = P(A \cap B)$

3. Sean A, B, C y D conjuntos arbitrarios. Demuestre la validez de las siguientes proposiciones:

   (a) $A \subseteq B \Rightarrow A - B = \varnothing$

   (b) $A - B = \varnothing \Rightarrow A \subseteq B$

   (c) $A \subseteq B \Rightarrow A \cap \overline{B} = \varnothing$

   (d) $A \cap B \neq \varnothing \Rightarrow (A \neq \varnothing \wedge B \neq \varnothing)$

   (e) $A - B = B - A \Rightarrow A = B$

   (f) $(A \subseteq C \ \wedge \ B \subseteq D) \Rightarrow (A \times B) \subseteq (C \times D)$

   (g) $(D \subseteq A - B \ \ \wedge \ \ E \subseteq A \cap B) \Rightarrow D \cap E = \varnothing$

   (h) $A \subseteq \overline{B} \Rightarrow A \cap B = \varnothing$

   (i) $(A \subseteq B \ \wedge \ A \cup B \neq B \cap C) \Rightarrow B \nsubseteq C$

   (j) $B \subseteq C \Rightarrow A \times B \subseteq A \times C$

   (k) $A \cap B = A \cap C \Rightarrow (B \bigtriangleup C) \cap A = \varnothing$

   (l) $A \neq \varnothing \Rightarrow \big(A \times B \subseteq A \times C \Rightarrow B \subseteq C\big)$

   (m) $\big(A \cap B \subseteq \overline{D} \ \wedge \ \overline{B} \cap D = \varnothing\big) \Rightarrow A \subseteq \overline{D}$

   (n) $A \cup B \subseteq C \cap D \Rightarrow \overline{C} \subseteq \overline{A} \cap \overline{B}$

   (o) $\big(C \subseteq \overline{A} \ \wedge \ C \cap \overline{B} = \emptyset\big) \Rightarrow C \subseteq B - A$

   (p) $A \cup B = A \cup C \Rightarrow (B \bigtriangleup C) \subseteq A$

   (q) $P(A) \subseteq B \Rightarrow \{A\} \in P(B)$

   (r) $\big[B \in P(A) \ \wedge \ B \in P(P(A))\big] \Rightarrow B = \varnothing$

   (s) $A \cup B = A \bigtriangleup C \Rightarrow A \cap C = \varnothing$

4. Sean A, B, C y D conjuntos arbitrarios. Demuestre la validez de las siguientes proposiciones:

   (a) $A \subseteq B \Leftrightarrow A \cup B = B$

   (b) $A \subseteq B \Leftrightarrow \overline{A} \cap \overline{B} = \overline{B}$

   (c) $A \subseteq B \Leftrightarrow A \cap B = A$

(d) $(A \subseteq D \ \wedge \ B \subseteq D) \Leftrightarrow A \cup B \subseteq D$

(e) $A \subseteq \overline{B} \Leftrightarrow B \subseteq \overline{A}$

(f) $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$

(g) $A \cup B \neq \varnothing \Leftrightarrow (A \neq \varnothing \ \vee \ B \neq \varnothing)$

(h) $A \cap B = \varnothing \Leftrightarrow A \subseteq \overline{B}$

(i) $A \subseteq \{A\} \Leftrightarrow A = \varnothing$

(j) $P(A) = \{\varnothing\} \Leftrightarrow A = \varnothing$

(k) $A \times B = \varnothing \Leftrightarrow (A = \varnothing \ \vee \ B = \varnothing)$

(l) $A \triangle B = A \triangle C \Leftrightarrow B = C$

5. Muestre, con un contraejemplo, que las siguientes proposiciones son falsas:

(a) $(A \neq \varnothing \ \wedge \ B \neq \varnothing) \Rightarrow A \cap B \neq \varnothing$

(b) $(A - B) \cup C \subseteq A - (B \cup C)$

(c) $A - (B \cap C) \subseteq (A - B) \cap (A - C)$

(d) $B = A \cup C \Rightarrow A = B - C$

(e) $\overline{A \cap B} \subseteq \overline{A} \cap \overline{B}$

(f) $P(A \cup B) \subseteq P(A) \cup P(B)$

(g) $(A \cup C) \cap (B \cup C) \subseteq A \cup B$

(h) $(A - B \neq \varnothing \ \wedge \ B - C \neq \varnothing) \Rightarrow A - C \neq \varnothing$

(i) $\overline{A \times B} \subseteq \overline{A} \times \overline{B}$

(j) $A \cup B = A \cup C \Rightarrow B = C$

(k) $A \cap B = A \cap C \Rightarrow B = C$

(l) $\overline{A - B} \subseteq B - A$

(m) $(A \cap B \subseteq D \ \wedge \ B \cap D \neq \varnothing) \Rightarrow A \subseteq D$

(n) $A \cup B = A \triangle C \Rightarrow (A \cap C = \varnothing \ \wedge \ C = B)$

(o) $P(A - B) \subseteq P(A) - P(B)$

6. Se dice que una colección de conjuntos A_1, A_2,..., A_n es *mutuamente excluyente* si para todo $i \neq j$ se cumple que $A_i \cap A_j = \varnothing$, es decir, si la intersección de cualesquiera dos conjuntos distintos de esta colección es vacía.
   Demuestre que los tres conjuntos $A \cap B$, $A - B$, $B - A$ son mutuamente excluyentes.

7. Demuestre que si colocan 100 bolas en 9 cajas, alguna de estas cajas contiene al menos 12 bolas.
   (Sugerencia: proceda por contradicción).

8. Se dice que una colección de conjuntos A_1, A_2,..., A_n es una *partición* de A si esta familia satisface:

   (a) $A_i \neq \varnothing$, para todo i.
   (b) A_1, A_2,..., A_n son mutuamente excluyentes.
   (c) $A_1 \cup A_2 \cup \cdots \cup A_n = A$

   Busque tres particiones distintas del conjunto $A = \{1, 2, 3, 4, 5, 6\}$. Además, determine la partición de A con la mayor cantidad de elementos posible y la partición de A con la menor cantidad.

9. Sea B un conjunto arbitrario y $\{A_i\}_{i \in I}$ una familia arbitraria de conjuntos. Pruebe que:

   (a) $$B \cap \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} (B \cap A_i)$$

   (b) $$B \cup \left(\bigcap_{i \in I} A_i \right) = \bigcap_{i \in I} (B \cup A_i)$$

   (c) $$B - \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} (B - A_i)$$

   (d) $$\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}$$

Capítulo 3
Relaciones binarias

"Las matemáticas comparan los más diversos fenómenos y descubren las analogías secretas que los unen".

Joseph Fourier (1768-1830)

En este capítulo se introduce el tema de las relaciones binarias: definiciones básicas, operaciones entre ellas, relaciones de orden y de equivalencia, particiones asociadas a una relación, matriz asociada a una relación, grafos dirigidos y algunas aplicaciones.

Para profundizar el tema tratado en este capítulo, es recomendable consultar las referencias bibliográficas [2], [7], [15] y [20].

3.1 Definiciones y operaciones

Dados dos conjuntos A y B, una **relación $\boldsymbol{\mathcal{R}}$** de A en B es el triplete (G, A, B) con $G \subseteq A \times B$, donde $\boldsymbol{A}$ se llama el **conjunto emisor** o **conjunto de partida**, $\boldsymbol{B}$ se llama el **conjunto receptor** o **conjunto de llegada** y el conjunto $\boldsymbol{G}$ se llama el **gráfico** de la relación. Para $a \in A$ y $b \in B$, se dice que **$\boldsymbol{a}$ se relaciona con $\boldsymbol{b}$** si y solo si $(a, b) \in G$, en cuyo caso se escribe $\boldsymbol{a\mathcal{R}b}$.

Ejemplo 1. *Considere los conjuntos $A = \{3, 5, 6\}$ y $B = \{4, 7\}$, y la relación $\mathcal{R}$ de A en B, definida por $a\mathcal{R}b$ si y solo si $a = b-1$. Determine el gráfico de $\mathcal{R}$.*

Solución. En el gráfico se deben incluir todos los pares ordenados (a, b) que pertenezcan a $A \times B$, para los cuales la proposición $a = b - 1$ sea verdadera. Por ejemplo, el par ordenado $(3, 7)$ no satisface dicha condición, pues $3 \neq 7 - 1$, mientras que los que sí la cumplen son los pares $(3,4)$ y $(6,7)$; de esta forma, al evaluar los 6 pares ordenados posibles de $A \times B$, se obtiene que

$$G_{\mathcal{R}} = \big\{(3,4), (6,7)\big\}$$

es el gráfico de la relación. ■

> Se dice que una relación $\mathcal{R}$ está definida sobre A si el emisor y el receptor son el mismo conjunto A, es decir, si $\mathcal{R} = (G, A, A)$.

Ejemplo 2. *Sobre el conjunto $A = \{1,2,3,4\}$, considere la relación $\mathcal{R}$ dada por $a\mathcal{R}b$ si y solo si $[a = b+1 \ \vee \ 2a = b]$. Calcule el gráfico de $\mathcal{R}$.*

Solución. En el gráfico se deben incluir todos los pares ordenados (a,b) para los que la proposición $a = b+1 \ \vee \ 2a = b$ sea verdadera. Por ejemplo, los pares ordenados $(3,2)$ y $(4,3)$ satisfacen $a = b+1$ y el par ordenado $(1,2)$ satisface la condición $2a = b$; así, al evaluar los 16 pares ordenados de $A \times A$, se obtiene que

$$G_{\mathcal{R}} = \big\{(1,2), (2,1), (2,4), (3,2), (4,3)\big\}$$

es el gráfico de la relación. ■

> Para la relación $\mathcal{R}$ de A en B, el conjunto definido por
>
> $$D_{\mathcal{R}} = \{a \in A \ / \ \exists b \in B \ \text{ tal que } \ a\mathcal{R}b\}$$
>
> se llama **dominio** de $\mathcal{R}$, y el conjunto definido por
>
> $$\mathcal{R}[A] = \{b \in B \ / \ \exists a \in A \ \text{ tal que } \ a\mathcal{R}b\}$$
>
> se llama **ámbito** o **rango** de $\mathcal{R}$.

Ejemplo 3. *El dominio de la relación definida en el ejemplo anterior es $D_{\mathcal{R}} = \{1,2,3,4\}$ y el rango es $\mathcal{R}[A] = \{1,2,3,4\}$.* ■

Ejemplo 4. *Sean* $A = \{a, b, f, h\}$ *y* $B = \{c, h, k\}$*; considere la relación* $\mathcal{R}$ *de* A *en* B *cuyo gráfico es* $G_{\mathcal{R}} = \big\{(b, c), (b, k), (h, c), (h, k)\big\}$*. Determine el dominio y el rango de* $\mathcal{R}$*.*

Solución. En el dominio se deben incluir todos los elementos de A que se relacionan con algún elemento de B; así, en el dominio solamente deben incluirse b y h, por lo que $D_{\mathcal{R}} = \{b, h\}$. Análogamente, se obtiene que el rango es $\mathcal{R}[A] = \{c, k\}$. ■

Ejemplo 5. *Sobre el conjunto* $A = \{2, 3, 5, 6\}$*, considere la relación* $\mathcal{R}$ *definida por* $a\mathcal{R}b$ *si y solo si* $a < b$*. Determine el gráfico, dominio y rango de* $\mathcal{R}$*.*

Solución. De la misma manera que en el ejemplo anterior, en el gráfico se deben incluir todos los pares ordenados (a, b) que pertenecen al conjunto $A \times A$, para los cuales la proposición $a < b$ sea verdadera; así, se obtiene $G_{\mathcal{R}} = \big\{(2, 3), (2, 5), (2, 6), (3, 5), (3, 6), (5, 6)\big\}$. Con ello, el dominio es $D_{\mathcal{R}} = \{2, 3, 5\}$ y el rango es $\mathcal{R}[A] = \{3, 5, 6\}$. ■

Si $\mathcal{R} = (G, A, B)$ y $\mathcal{S} = (H, A, B)$ son dos relaciones de A en B, se definen las relaciones:

- **unión de $\mathcal{R}$ y $\mathcal{S}$** como $\mathcal{R} \cup \mathcal{S} = (G \cup H, A, B)$.
- **intersección de $\mathcal{R}$ y $\mathcal{S}$** como $\mathcal{R} \cap \mathcal{S} = (G \cap H, A, B)$.
- **diferencia de $\mathcal{R}$ y $\mathcal{S}$** como $\mathcal{R} - \mathcal{S} = (G - H, A, B)$.
- **inversa de $\mathcal{R}$** como $\mathcal{R}^{-1} = (G^{-1}, B, A)$, donde

$$G^{-1} = \{(b, a) \;\; / \;\; (a, b) \in G\}$$

- **complemento de $\mathcal{R}$** como $\overline{\mathcal{R}} = (\overline{G}, A, B)$, donde

$$\overline{G} = \{(a, b) \;\; / \;\; (a, b) \notin G\}$$

Ejemplo 6. *Sobre* $A = \{1, 2, 3\}$*, considere las relaciones* $\mathcal{R}$ *y* $\mathcal{S}$*. El gráfico de* $\mathcal{R}$ *es* $G_{\mathcal{R}} = \{(1, 2), (1, 3), (2, 3), (3, 2), (3, 3)\}$*; el gráfico de* S *es* $G_{\mathcal{S}} = \{(1, 2), (2, 2), (3, 3)\}$*. Determine el gráfico de las relaciones* $\mathcal{R} \cup \mathcal{S}$*,* $\mathcal{R} \cap \mathcal{S}$*,* $\mathcal{R}^{-1}$ *y* $\overline{\mathcal{R}}$*.*

Solución. En el gráfico de $\mathcal{R} \cup \mathcal{S}$ estarán los pares ordenados que pertenecen a cualquiera de los gráficos de $\mathcal{R}$ o de $\mathcal{S}$:

$$G_{\mathcal{R}\cup\mathcal{S}} = \big\{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\big\}$$

En el gráfico de la intersección están los que pertenecen simultáneamente a los gráficos de $\mathcal{R}$ y $\mathcal{S}$:

$$G_{\mathcal{R}\cap\mathcal{S}} = \big\{(1, 2), (3, 3)\big\}$$

En el gráfico de $\mathcal{R}^{-1}$ solamente se intercambian los componentes de los pares ordenados de los elementos de $\mathcal{R}$:

$$G_{\mathcal{R}^{-1}} = \big\{(2, 1), (3, 1), (3, 2), (2, 3), (3, 3)\big\}$$

Por último, para calcular $G_{\overline{\mathcal{R}}}$ es necesario recordar que el complemento se toma sobre el universo; en este ejemplo es $A \times A$, con lo cual

$$G_{\overline{\mathcal{R}}} = \big\{(1, 1), (2, 1), (2, 2), (3, 1)\big\}$$

que coincide con $(A \times A) - G_{\mathcal{R}}$. ∎

Si $\mathcal{R} = (G, A, B)$ y $\mathcal{S} = (H, B, C)$, se define la relación **compuesta de** $\boldsymbol{\mathcal{R}}$ **y** $\boldsymbol{\mathcal{S}}$ como $\mathcal{S} \circ \mathcal{R} = (H \circ G, A, C)$, donde

$$H \circ G = \big\{(a, c) \ / \ \ \exists b \in B \ \text{ tal que } \ a\mathcal{R}b \ \wedge \ b\mathcal{S}c\big\}$$

Ejemplo 7. *Sobre* $A = \{1, 2, 3, 4\}$ *se definen las relaciones* $\mathcal{R}$ *y* $\mathcal{S}$*, donde el gráfico de* $\mathcal{R}$ *es* $G_{\mathcal{R}} = \big\{(1, 2), (2, 3), (2, 4), (3, 2), (4, 1), (4, 4)\big\}$ *y el de* $\mathcal{S}$ *es* $G_{\mathcal{S}} = \big\{(2, 4), (3, 2), (4, 3)\big\}$*. Determine el gráfico de* $\mathcal{S} \circ \mathcal{R}$*.*

Solución. Para calcular el gráfico de $\mathcal{S} \circ \mathcal{R}$, se buscan todos los caminos posibles de la siguiente forma: se toma $(1,2)$, el primer elemento de $G_{\mathcal{R}}$, y como su segunda componente es 2, se busca en $G_{\mathcal{S}}$ los que tienen como primera componente el mismo 2, así:

$$1\mathcal{R}2 \ \wedge \ 2\mathcal{S}4 \quad \Rightarrow \quad (1,4) \in G_{\mathcal{S}\circ\mathcal{R}}$$

Para el segundo elemento $(2,3)$ de $G_{\mathcal{R}}$, como su segunda componente es 3, se busca en $G_{\mathcal{S}}$ los que tienen como primera componente el 3:

$$2\mathcal{R}3 \ \wedge \ 3\mathcal{S}2 \quad \Rightarrow \quad (2,2) \in G_{\mathcal{S}\circ\mathcal{R}}$$

Se procede de la misma manera para los otros cuatro elementos de $G_{\mathcal{R}}$ y se obtiene que como $2\mathcal{R}4 \ \wedge \ 4\mathcal{S}3$, entonces $(2,3) \in G_{\mathcal{S}\circ\mathcal{R}}$. Como $3\mathcal{R}2 \ \wedge \ 2\mathcal{S}4$, entonces $(3,4) \in G_{\mathcal{S}\circ\mathcal{R}}$ y, por último, como $4\mathcal{R}4 \ \wedge \ 4\mathcal{S}3$, entonces $(4,3) \in G_{\mathcal{S}\circ\mathcal{R}}$; por lo tanto, $G_{\mathcal{S}\circ\mathcal{R}} = \big\{(1,4),(2,2),(2,3),(3,4),(4,3)\big\}$.■

Antes de continuar, es importante aclarar que como las relaciones han sido definidas como tripletes ordenados, dos relaciones son iguales si y solo si tienen el mismo conjunto emisor, el mismo conjunto receptor y el mismo gráfico. En ocasiones, dos relaciones tienen el mismo gráfico, pero los conjuntos emisores o receptores son diferentes; por lo tanto, las dos relaciones son diferentes.

Ejemplo 8. *A partir de los conjuntos* $A = \{1,2,3,4\}$, $B = \{x,y,z\}$ *y* $C = \{5,6,7\}$, *considere la relación* $\mathcal{R}$ *de* A *en* B *cuyo gráfico es* $G_R = \big\{(1,x),(1,y),(2,z),(3,y),(4,z)\big\}$, *y la relación* $\mathcal{S}$ *de* B *en* C *con gráfico* $G_S = \big\{(x,6),(y,5),(z,5)\big\}$. *Determine el gráfico de* $G_{\mathcal{S}\circ\mathcal{R}}$.

Solución. Note que $\mathcal{S} \circ \mathcal{R}$ es una relación de A en C, es decir, su gráfico es subconjunto de $A \times C$; para encontrar este gráfico, se deben hallar todos los pares ordenados (a,c) de manera que para algún elemento b de B se tenga como verdadera la proposición $a\mathcal{R}b \ \wedge \ b\mathcal{S}c$; por ejemplo, el par ordenado $(1,6)$ cumple con que $1\mathcal{R}x \ \wedge \ x\mathcal{S}6$, por lo cual se debe incluir en el gráfico; siguiendo con las evaluaciones, se obtiene que $G_{\mathcal{S}\circ\mathcal{R}} = \big\{(1,6),(1,5),(2,5),(3,5),(4,5)\big\}$. ■

Ejercicios (sección 3.1)

1. Sobre el conjunto $A = \{2, 3, 5, 6\}$ se define una relación $\mathcal{R}$, de manera que el par ordenado (a, b) pertenece al gráfico de $\mathcal{R}$ si y solo si ab es un número par. Calcule el gráfico de $\mathcal{R}$ y de $\overline{\mathcal{R}}$.

2. Sobre $A = \{1, 2, 3, 4, 5, 6\}$ se define una relación $\mathcal{R}$ con gráfico $G_{\mathcal{R}} = \{(a, b) \;/\; (a - b)^2 < 4\}$. Calcule el gráfico de $\mathcal{R}$ y de $\mathcal{R}^{-1}$.

3. Sobre $A = \{1, 2, 4, 8\}$, defina la relación $\mathcal{S}$ por $a\mathcal{S}b$ si y solo si $[ab = 8 \;\vee\; a + b = 5]$. Determine el gráfico de $\mathcal{S}$ y el de $\mathcal{S}^{-1}$.

4. Considere las relaciones $\mathcal{R}$ y $\mathcal{S}$ definidas sobre el conjunto $A = \{1, 2, 3, 4, 5\}$, donde $\mathcal{R}$ está definida por $a\mathcal{R}b \Leftrightarrow (a - b)^2 \in A$, y el gráfico de S es $G_S = \{(i, j) \;/\; i - j \geq 1\}$, es decir, el par ordenado (i, j) pertenece al gráfico de $\mathcal{S}$ si y solo si $i - j \geq 1$.

   (a) Calcule los gráficos de $\mathcal{R}$, de $\mathcal{S}$, de $\mathcal{R} \cup \mathcal{S}$ y de $\mathcal{R} \cap \mathcal{S}$.

   (b) Calcule el gráfico de $(\mathcal{R} - \mathcal{S})^{-1}$.

   (c) Calcule el gráfico de $(\mathcal{S} \circ \mathcal{R}) - (\mathcal{R} \circ \mathcal{S})$.

5. Sea $A = \{1, 2, 3, 4\}$, sean $\mathcal{R}$ y $\mathcal{S}$ relaciones sobre A, definidas por $a\mathcal{R}b \Leftrightarrow a + b \in A$ y por $a\mathcal{S}b \Leftrightarrow b = a + 1$.

   (a) Determine el dominio y el rango de $\mathcal{R}$, $\mathcal{S}$ y de $\mathcal{S}^{-1}$.

   (b) Determine los gráficos de $\mathcal{R}$, de $\mathcal{S}$, de $\mathcal{R} \cup \mathcal{S}$, de $\mathcal{S} \cap \mathcal{R}$, de $\overline{\mathcal{S} - \mathcal{R}}$, y de $\mathcal{S}^{-1} - \overline{\mathcal{R}}$.

6. Considere las relaciones $\mathcal{R}$ y $\mathcal{S}$ definidas sobre el conjunto $A = \{a, b, c\}$, donde $G_{\mathcal{R}} = \big\{(a, a), (a, c), (b, a), (b, b), (c, c)\big\}$ es el gráfico de $\mathcal{R}$ y el gráfico de S es $G_{\mathcal{S}} = \big\{(a, a), (a, b), (b, b), (c, a)\big\}$.

   (a) Determine las gráficos de $\mathcal{R}$, de $\mathcal{R} \cup \mathcal{S}$, de $\mathcal{R} \cap \mathcal{S}$, y de $\mathcal{R} - \mathcal{S}$.

   (b) Determine los gráficos $G_{\overline{\mathcal{R}} - \mathcal{S}^{-1}}$, y $G_{\overline{\mathcal{R} \cup \mathcal{S}}}$.

   (c) Si $\mathcal{R}^3 = \mathcal{R} \circ \mathcal{R} \circ \mathcal{R}$, calcule $G_{\mathcal{R}^3}$.

3.2 Matrices y grafos asociados

En esta sección se definen las matrices booleanas que resultan útiles para guardar la información de los elementos del gráfico de una relación binaria; además, se hace una breve introducción al tema de los grafos, que se utilizan aquí para representar los gráficos de las relaciones.

Una **matriz** M de tamaño m por n es un arreglo rectangular de mn números ordenados en m **filas** (horizontales) y n **columnas** (verticales). Esta matriz se denota por $\boldsymbol{M = (m_{ij})}$, donde m_{ij} es la entrada i-j de la matriz; en ocasiones se escribirá $\boldsymbol{M[i, j]}$ para denotar la entrada i-j de la matriz M.

Ejemplo 9. *La matriz* $M = \begin{pmatrix} 1 & 3 & -2 \\ 0 & 5 & 2 \end{pmatrix}$ *es una matriz de tamaño* 2×3*, donde, por ejemplo,* $m_{11} = 1$*,* $m_{23} = 2$*,* $m_{13} = -2$*.* ■

Una matriz de $1 \times n$ se llamará **matriz fila** y una de $m \times 1$ se llamará **matriz columna**.

Ejemplo 10. *La matriz* $\begin{pmatrix} 1 & 2 & -3 & -6 \end{pmatrix}$ *es una matriz fila de* 1×4 *y la matriz* $\begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$ *es una matriz columna de* 3×1*.* ■

Se define como la **matriz identidad** de tamaño $n \times n$ a la matriz $I_n = (\delta_{ij})$, con $\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$

Ejemplo 11. *Las matrices* $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$*,* $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *son las matrices identidad de* 2×2 *y* 3×3*, respectivamente.* ■

No es el interés de esta obra profundizar en el tema general de las matrices, solamente interesa desarrollarlo en el caso particular de las matrices **booleanas**, donde sus entradas pueden ser solamente 0 o 1, ya que, como se verá más adelante, serán útiles para representar los gráficos de las relaciones definidas sobre conjuntos finitos.

Se define la **matriz nula** o matriz cero, de tamaño n por m, como la matriz cuyas entradas son 0 y se denota $\mathbf{0}_{n\times m}$. Además, se define la **matriz unidad** o matriz uno, de tamaño n por m, como la matriz cuyas entradas son 1 y se denota $\mathbf{1}_{n\times m}$.

Ejemplo 12. *La matriz nula de* 2 *por* 3 *es* $\mathbf{0}_{2\times 3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. ■

Ejemplo 13. *La matriz unidad de* 3 *por* 2 *es* $\mathbf{1}_{3\times 2} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}$. ■

Si $A = (a_{ij})$ y $B = (b_{ij})$ son dos matrices booleanas de $m \times n$, se define la **disyunción** de A y B como la nueva matriz $A \vee B = D$, donde las entradas son:

$$D[i,j] = \begin{cases} 1 & \text{si } a_{ij} = 1 \ \vee \ b_{ij} = 1 \\ 0 & \text{si } a_{ij} = 0 \ \wedge \ b_{ij} = 0 \end{cases}$$

Además, se define la **conjunción** de A y B como la nueva matriz $A \wedge B = C$, donde las entradas son:

$$C[i,j] = \begin{cases} 1 & \text{si } a_{ij} = 1 \ \wedge \ b_{ij} = 1 \\ 0 & \text{si } a_{ij} = 0 \ \vee \ b_{ij} = 0 \end{cases}$$

Ejemplo 14. *Si* $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ *y* $B = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, *matrices* *de* 3×4*, se obtienen las nuevas matrices*

$$A \vee B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad A \wedge B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ambas de tamaño 3×4*.* ■

Además de estas dos operaciones con matrices booleanas, se define la **matriz traspuesta** de M como la matriz cuyas columnas son las filas de M y las filas son las columnas de M; esta nueva matriz se denota por $\boldsymbol{M^T}$. Simbólicamente, si $M = (m_{ij})$ se tiene que $M^T = (m_{ji})$.

Ejemplo 15. *Para la matriz* $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *de* 2×3*, su traspuesta es la matriz* $M^T = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$ *de* 3×2*.* ■

Si $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$ son conjuntos finitos, toda relación $\mathcal{R}$ de A en B se puede representar por medio de una **matriz asociada** que se denota por $\boldsymbol{M_{\mathcal{R}}}$. La entrada i-j es 0 si el par ordenado (a_i, b_j) no pertenece al gráfico de $\mathcal{R}$, es decir, si $a_i \not\mathcal{R} b_j$, y es 1 si el par ordenado (a_i, b_j) sí pertenece al gráfico de $\mathcal{R}$, es decir, es 1 si $a_i \mathcal{R} b_j$. Se representará por $\boldsymbol{M_{\mathcal{R}}[i, j]}$ a la entrada i-j de la matriz $M_{\mathcal{R}}$, así:

$$M_{\mathcal{R}}[i, j] = \begin{cases} 0 & \text{si } a_i \not\mathcal{R} b_j \\ 1 & \text{si } a_i \mathcal{R} b_j \end{cases}$$

Ejemplo 16. *Si se define la relación* $\mathcal{R}$ *de* A *en* B*, con* $A = \{3, 4\}$ *y* $B = \{x, y, z\}$*, con gráfico* $G_{\mathcal{R}} = \big\{(3, x), (3, z), (4, y), (4, z)\big\}$*, entonces la* *matriz asociada a esta relación es la matriz de* 2×3*:*

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Mientras que la matriz

$$M_{\mathcal{S}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

está asociada a la relación $\mathcal{S}$*, de* B *en* A*, con* $G_{\mathcal{S}} = \big\{(x,3),(z,4)\big\}$*.* ■

Ejemplo 17. *Sean* $A = \{-1,3,2\}$ *y* $B = \{x,z,w,t\}$*, y la relación* $\mathcal{R}$ *de* A *en* B*, de manera que la matriz de esta relación está definida por*

$$M_{\mathcal{R}}[i,j] = 1 \Leftrightarrow \big(\, i = j \ \vee \ j - i = 2 \,\big)$$

Calcule $M_{\mathcal{R}}$ *y* $G_{\mathcal{R}}$*.*

Solución. Por la forma de definir la matriz, se observa que ella tendrá un 1 solamente en las entradas $M_{\mathcal{R}}[1,1]$, $M_{\mathcal{R}}[2,2]$, $M_{\mathcal{R}}[3,3]$, pues allí se cumple que $i = j$, y en las entradas $M_{\mathcal{R}}[1,3]$, $M_{\mathcal{R}}[2,4]$, pues se cumple que $j - i = 2$. Por lo tanto,

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

y así, al analizar los conjuntos A y B, se obtiene que el gráfico de esta relación es el conjunto $G_{\mathcal{R}} = \big\{(-1,x),(-1,w),(3,z),(3,t),(2,w)\big\}$. ■

Es sencillo verificar que para relaciones definidas sobre conjuntos finitos, las matrices de unión e intersección de dos relaciones, así como la matriz de la relación inversa, se obtienen mediante

$$M_{\mathcal{R}\cup\mathcal{S}} = M_{\mathcal{R}} \vee M_{\mathcal{S}} \tag{3.1}$$

$$M_{\mathcal{R}\cap\mathcal{S}} = M_{\mathcal{R}} \wedge M_{\mathcal{S}} \tag{3.2}$$

$$M_{\mathcal{R}^{-1}} = M_{\mathcal{R}}^{T} \tag{3.3}$$

Ejemplo 18. *Si $A = \{a, b\}$ y $B = \{c, d, e\}$, y se definen dos relaciones $\mathcal{R}$ y $\mathcal{S}$ de A en B, donde $G_{\mathcal{R}} = \big\{(a, c), (a, e), (b, d), (b, e)\big\}$ es el gráfico de $\mathcal{R}$ y el de $\mathcal{S}$ es $G_{\mathcal{S}} = \big\{(a, c), (a, d), (b, e)\big\}$, calcule $M_{\mathcal{R}}$, $M_{\mathcal{S}}$, $M_{\mathcal{R}\cup\mathcal{S}}$, $M_{\mathcal{R}\cap\mathcal{S}}$ y $M_{\mathcal{R}^{-1}}$.*

Solución. De los gráficos dados, se tiene que:

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad\qquad M_{\mathcal{S}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

y al calcular la disyunción y la conjunción de estas matrices, se obtiene:

$$M_{\mathcal{R}\cup\mathcal{S}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad\qquad M_{\mathcal{R}\cap\mathcal{S}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Por último, $M_{\mathcal{R}^{-1}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$. ■

Ejemplo 19. *Para la relación definida en el ejemplo 2, determine la matriz de la relación $\mathcal{R}$; además, calcule el gráfico de $\mathcal{R} \circ \mathcal{R}$, la matriz $M_{\mathcal{R}\circ\mathcal{R}}$, su dominio y su rango.*

Solución. Del ejemplo 2, $G_{\mathcal{R}} = \big\{(1, 2), (2, 1), (2, 4), (3, 2), (4, 3)\big\}$, así, la matriz de $\mathcal{R}$ es:

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Para calcular el gráfico de $\mathcal{R}\circ\mathcal{R}$, se buscan todos los caminos posibles de la siguiente forma: se toma el primer elemento $(1, 2)$, y como su segunda componente es 2, se buscan los que tienen como primera componente el mismo 2, así:

$$\begin{aligned} 1\mathcal{R}2 \ \wedge\ 2\mathcal{R}1 \quad &\Rightarrow \quad (1, 1) \in G_{\mathcal{R}\circ\mathcal{R}} \\ 1\mathcal{R}2 \ \wedge\ 2\mathcal{R}4 \quad &\Rightarrow \quad (1, 4) \in G_{\mathcal{R}\circ\mathcal{R}} \end{aligned}$$

Para el segundo elemento $(2,1)$, como su segundo componente es 1, se buscan los que tienen como primera componente el mismo 1, así:

$$2\mathcal{R}1 \ \wedge \ 1\mathcal{R}2 \quad \Rightarrow \quad (2,2) \in G_{\mathcal{R}\circ\mathcal{R}}$$

Para el tercer elemento $(2,4)$, como su segunda componente es 4, se buscan los que tienen como primera componente 4, así:

$$2\mathcal{R}4 \ \wedge \ 4\mathcal{R}3 \quad \Rightarrow \quad (2,3) \in G_{\mathcal{R}\circ\mathcal{R}}$$

Análogamente, como $3\mathcal{R}2 \ \wedge \ 2\mathcal{R}1$, entonces $(3,1) \in G_{\mathcal{R}\circ\mathcal{R}}$. Como $3\mathcal{R}2 \ \wedge \ 2\mathcal{R}4$, entonces $(3,4) \in G_{\mathcal{R}\circ\mathcal{R}}$ y, por último, como $4\mathcal{R}3 \ \wedge \ 3\mathcal{R}2$, entonces $(4,2) \in G_{\mathcal{R}\circ\mathcal{R}}$; por lo tanto:

$$G_{\mathcal{R}\circ\mathcal{R}} = \big\{(1,1),(1,4),(2,2),(2,3),(3,1),(3,4),(4,2)\big\}$$

La matriz de $\mathcal{R}\circ\mathcal{R}$ es:

$$M_{\mathcal{R}\circ\mathcal{R}} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Para finalizar, el dominio es $D_{\mathcal{R}\circ\mathcal{R}} = A$ y el rango es $\mathcal{R}[A] = A$. ■

Otra operación importante entre matrices booleanas es la multiplicación; para definirla, considere las matrices $A = (a_{ij})$ de $m \times n$ y $B = (b_{ij})$ de $n \times p$. La multiplicación booleana de A y B es la nueva matriz de $m \times p$ que se denota por $A \odot B$, de manera que $A \odot B[i,j] = 1$, si existe un 1 en la misma posición en la fila i de A y en la columna j de B, y $A \odot B[i,j] = 0$ si no hay coincidencia. Para comprender esta operación, observe el siguiente ejemplo:

Ejemplo 20. *Si A es la matriz de 3×3 dada por* $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ *y B es la matriz de 3×2 dada por* $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$, *calcule la nueva* *matriz que se obtiene de la multiplicación de* A *y* B*. Para iniciar, se debe comparar, para buscar coincidencias de unos, la primera fila de* A *con cada una de las columnas de* B*, es decir, comparar* $\begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$ *con* $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ *y se observa que coinciden en la primera entrada; luego, se compara* $\begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$ *con* $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ *y se observa que no hay coincidencias. Por lo tanto, la primera fila de* $A \odot B$ *es* $\begin{pmatrix} 1 & 0 \end{pmatrix}$*. Ahora se compara la segunda fila de* A *con cada una de las columnas de* B *y se observa que no hay coincidencias de unos; por lo tanto, la segunda fila de* $A \odot B$ *es* $\begin{pmatrix} 0 & 0 \end{pmatrix}$*. Análogamente, se compara la tercera fila de* A *con cada una de las columnas de* B *y se observa la coincidencia en ambos casos; por lo tanto:*

$$A \odot B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$$

que corresponde a una matriz de 3×2*.* ■

Conociendo las matrices de dos relaciones, se puede determinar la matriz de la composición por medio de la multiplicación booleana de sus matrices:

$$M_{\mathcal{S} \circ \mathcal{R}} = M_{\mathcal{R}} \odot M_{\mathcal{S}} \tag{3.4}$$

Ejemplo 21. *En el ejemplo* 19 *se calcula, por medio de la definición, la matriz de* $\mathcal{R} \circ \mathcal{R}$*; ahora se puede utilizar el resultado* (3.4) *para obtener:*

$$M_{\mathcal{R} \circ \mathcal{R}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \odot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Observe que se obtuvo el mismo resultado que en el ejemplo 19*.* ■

Anteriormente, se vio que las diferentes relaciones de A en B se pueden representar por medio de su criterio, su gráfico o su matriz asociada. En el caso particular de relaciones definidas de A en A, es decir, sobre A, se pueden representar por medio de un **grafo dirigido** o **dígrafo**. Este grafo estará formado por los elementos de A, que se llamarán **vértices** o **nodos**, y un conjunto de **flechas** o **aristas**, de manera que hay una flecha del vértice a al vértice b si $(a, b) \in G_{\mathcal{R}}$. En el caso especial de las flechas de a en a, se llamarán **lazos**.

Ejemplo 22. *Para la relación $\mathcal{R}$ definida sobre $A = \{1, 2, 3, 4\}$ de manera que su gráfico es*

$$G_{\mathcal{R}} = \big\{(1,1), (1,2), (2,3), (3,2), (3,3), (4,3)\big\}$$

el grafo asociado a $\mathcal{R}$ está dado en la figura 3.1. En él se observa que en los nodos 1 y 3 hay lazos y además, se tienen cuatro flechas. ■

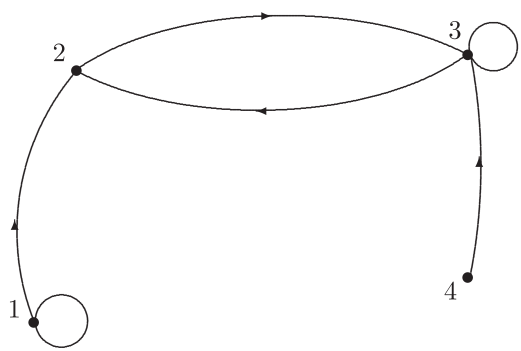


Figura 3.1: Grafo con 4 nodos, 4 flechas y 2 lazos.

Ejemplo 23. *Para la relación $\mathcal{R}$ definida sobre $A = \{a, b, c, d, e, f\}$, con gráfico $G_{\mathcal{R}} = \big\{(b,c), (b,d), (c,a), (c,c), (d,c), (d,d), (d,e), (f,f)\big\}$, se tiene que el grafo asociado a $\mathcal{R}$ está dado en la figura 3.2. En él se observa que se tienen cinco flechas, y lazos en los nodos c, d y f.* ■

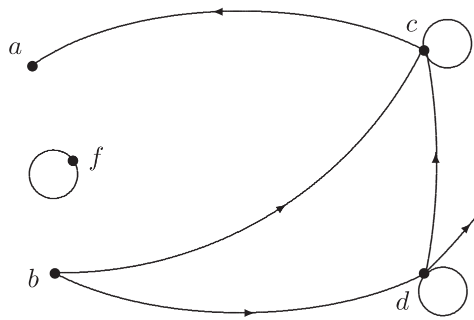


Figura 3.2: Grafo con 6 nodos, 5 flechas y 3 lazos.

Ejercicios (sección 3.2)

1. Considere las relaciones $\mathcal{R}$ y $\mathcal{S}$ definidas sobre el conjunto $A = \{a, b, c\}$, donde $G_{\mathcal{R}} = \big\{(a, a), (a, c), (b, a), (b, b), (c, c)\big\}$ es el gráfico de $\mathcal{R}$ y el gráfico de S es $G_{\mathcal{S}} = \big\{(a, a), (a, b), (b, b), (c, a)\big\}$.

   (a) Calcule las matrices $M_{\mathcal{R}}$, $M_{\mathcal{R}\cup\mathcal{S}}$, $M_{\mathcal{R}\cap\mathcal{S}}$, $M_{\mathcal{R}-\mathcal{S}}$

   (b) Determine los grafos de $\overline{\mathcal{R}} - \mathcal{S}^{-1}$ y de $\overline{\mathcal{R} \cup \mathcal{S}}$.

2. Considere las relaciones $\mathcal{R}$ y $\mathcal{S}$ definidas sobre el conjunto $A = \{1, 2, 3, 4, 5\}$, donde $\mathcal{R}$ está definida por

$$a\mathcal{R}b \Leftrightarrow (a - b)^2 \in A$$

   y el gráfico de S es $G_S = \{(i, j) \ / \ \ i - j \geq 1\}$

   (a) Determine la matriz de $\mathcal{R}$, de $\mathcal{S}$, de $\overline{\mathcal{R} \cup \mathcal{S}}$ y de $\mathcal{S} \circ \mathcal{R}$.

   (b) Calcule el grafo de $\mathcal{R}$, de $\mathcal{S}$ y de $\mathcal{R} \cup \mathcal{S}$.

3. Para $A = \{1, 4, 7\}$, sea $\mathcal{R}$ una relación sobre A, definida por

$$a\mathcal{R}b \Leftrightarrow ab < 16$$

y sea $\mathcal{S}$ otra relación sobre A, cuya matriz es $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

(a) Determine la matriz, el gráfico y el grafo asociados a $\mathcal{R}$.

(b) Determine la matriz, el gráfico y el grafo asociados a $\mathcal{S}$.

(c) Determine la matriz de $\mathcal{S}^{-1} \circ \mathcal{R}$.

(d) Determine el gráfico asociado a $(\mathcal{S}^{-1} \circ \mathcal{R}) - \overline{\mathcal{R}}$.

4. Considere la relación $\mathcal{R}$ definida sobre $A = \{a, b, c, d, e\}$, de manera que la matriz asociada a $\mathcal{R}$ es

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

y la relación $\mathcal{S}$ definida de A en el conjunto $B = \{1, 3, 5, 7\}$, cuyo gráfico es $G_{\mathcal{S}} = \big\{(a, 3), (a, 7), (b, 1), (c, 5), (c, 7), (e, 1), (e, 7)\big\}$.

(a) Determine las matrices $M_{\mathcal{S}}$, $M_{\mathcal{R}\circ\mathcal{R}}$, $M_{\mathcal{S}\circ\mathcal{R}}$.

(b) Determine los gráficos $G_{(\mathcal{S}\circ\mathcal{R})^{-1}}$, $G_{\mathcal{S}\circ\mathcal{S}^{-1}}$.

(c) Determine el grafo asociado a la relación $\mathcal{S}^{-1} \circ \mathcal{S}$.

5. Sea $A = \{\sharp, a, 2, 0\}$ y sea $\mathcal{R}$ una relación sobre A, cuya matriz asociada satisface

$$M_{\mathcal{R}}[i, j] = 1 \Leftrightarrow \big(\, 2i = j \;\vee\; j = 1 \;\vee\; i = 4 \,\big)$$

Determine la matriz $M_{\mathcal{R}}$, el gráfico $G_{\mathcal{R}}$ y el gráfico de $\overline{\mathcal{R}} - \mathcal{R}^{-1}$

6. Sea $A = \{0, 1, 3, 4\}$ y sea $\mathcal{R}$ una relación sobre A, cuya matriz asociada está definida por

$$M_{\mathcal{R}}[i, j] = \begin{cases} 1 & \text{si } \; |3 - i| = 1 \;\vee\; i = j \\ 0 & \text{en cualquier otro caso} \end{cases}$$

y sea $\mathcal{S}$ otra relación sobre A, definida por

$$a\mathcal{S}b \Leftrightarrow a - b \in A$$

(a) Determine las matrices de $\mathcal{R}$ y de $\mathcal{S}$, y el gráfico de $\mathcal{R} \circ \mathcal{S}^{-1}$.

(b) Determine la matriz asociada a $(\overline{\mathcal{R}} \cap \mathcal{S})^{-1}$.

7. Sea $A = \{0, 2, 4, 6\}$, sea $\mathcal{R}$ una relación sobre A, cuya matriz asociada está definida por

$$M_{\mathcal{R}}[i,j] = \begin{cases} 1 & \text{si } \ i = 4 \ \vee \ j = 3 \ \vee \ i = j \\ 0 & \text{en cualquier otro caso} \end{cases}$$

y sea $\mathcal{S}$ otra relación sobre A, definida por

$$a\mathcal{S}b \Leftrightarrow a + b \in A$$

(a) Determine el gráfico y la matriz asociada a $\mathcal{R}$, a $\mathcal{S}$ y a $\overline{\mathcal{S}} \circ \mathcal{R}^{-1}$

(b) Determine la matriz asociada y el grafo de $(\mathcal{R} \cup \mathcal{S}) - (\mathcal{R} \cap \mathcal{S})$

8. Sea $A = \{1, 3, 5, 6\}$ y sea $\mathcal{R}$ una relación sobre A, cuya matriz asociada está definida por

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

(a) Determine el menor número natural n tal que $M_{\mathcal{R}^n} = I_4$.

(b) Calcule $M_{\mathcal{R}^{2006}}$.

9. Sea $A = \{1, 3, 5, 6, 9\}$ y sea $\mathcal{R}$ una relación sobre A, cuyo gráfico asociado es $G_{\mathcal{R}} = \big\{(1, 3), (3, 5), (5, 6), (6, 9), (9, 1)\big\}$

(a) Determine el menor natural n, con $n > 1$, tal que $M_{\mathcal{R}^n} = M_{\mathcal{R}}$.

(b) Calcule $M_{\mathcal{R}^{10001}}$.

10. Sea $A = \{a, b, c, d\}$ y sean $\mathcal{R}$, $\mathcal{S}$, $\mathcal{T}$ relaciones sobre A, tales que

$$M_{\mathcal{R}}[i,j] = \begin{cases} 1 & \text{si } |i-1| = 1 \ \vee \ i = j^2 \\ 0 & \text{en cualquier otro caso} \end{cases}$$

$$M_{\mathcal{S}}[i,j] = \begin{cases} 0 & \text{si } M_{\mathcal{R}}[i, j-1] = 1 \text{ para } j \neq 1 \\ 1 & \text{en cualquier otro caso} \end{cases}$$

$$M_{\mathcal{T}}[i,j] = \begin{cases} 0 & \text{si } M_{\mathcal{R}}[i+1, j] = 0 \text{ para } i \neq 4 \\ 1 & \text{en cualquier otro caso} \end{cases}$$

(a) Determine las matrices de $\mathcal{R}$, de $\mathcal{S}$, de $\mathcal{T}$ y de $\mathcal{S} \cup \mathcal{T}$.

(b) Construya el grafo asociado a $\mathcal{R}$, a $\mathcal{S}$, a $\mathcal{T}$ y a $\mathcal{S} \cup \mathcal{T}$.

(c) Determine el gráfico de $\mathcal{R}^{-1}$, de $\mathcal{S} \cup \mathcal{T}$ y de $\mathcal{R}^{-1} \circ \overline{\mathcal{S} \cup \mathcal{T}}$.

3.3 Propiedades de las relaciones

En esta sección se definen algunas propiedades de las relaciones con la finalidad, como se verá en las siguientes secciones, de clasificarlas en relaciones de equivalencia o en relaciones de orden. Las relaciones del primer tipo permitirán asociar los elementos afines de los conjuntos y así particionarlos en subconjuntos, de manera que éstos sean disjuntos. Las relaciones del segundo tipo permitirán ordenar, en algún sentido, los elementos del conjunto donde se define la relación.

Si $\mathcal{R}$ es una relación definida sobre A, se dice que la relación $\mathcal{R}$ es:

- **Reflexiva** si y solo si $\forall a \in A \; [a\mathcal{R}a]$, es decir, $\mathcal{R}$ es reflexiva si $a\mathcal{R}a$ para todo $a \in A$.
- **Simétrica** si y solo si $\forall a, b \in A \; [a\mathcal{R}b \Rightarrow b\mathcal{R}a]$, es decir, $\mathcal{R}$ es simétrica si cuando $a\mathcal{R}b$ también $b\mathcal{R}a$.
- **Transitiva** si y solo si $\forall a, b, c \in A \; [a\mathcal{R}b \; \wedge \; b\mathcal{R}c \Rightarrow a\mathcal{R}c]$, es decir, $\mathcal{R}$ es transitiva si cuando $a\mathcal{R}b$ y $b\mathcal{R}c$ se concluye que $a\mathcal{R}c$.
- **Antisimétrica** si y solo si $\forall a, b \in A \; [a\mathcal{R}b \; \wedge \; b\mathcal{R}a \Rightarrow a = b]$, es decir, $\mathcal{R}$ es antisimétrica si para $a\mathcal{R}b$, con $a \neq b$, no se cumple que $b\mathcal{R}a$.
- **Total** si y solo si $\forall a, b \in A \; [a\mathcal{R}b \; \vee \; b\mathcal{R}a]$, es decir, $\mathcal{R}$ es total si para cualquier par de elementos a y b de A, se cumple que $a\mathcal{R}b$ o $b\mathcal{R}a$.

Ejemplo 24. *Sea $A = \{1, 2, 3, 4\}$ y sea $\mathcal{R}$ una relación definida sobre A, cuyo gráfico G es*

$$G = \big\{(1,1), (1,2), (1,3), (2,1), (2,2), (3,1), (3,3), (4,4), (4,1)\big\}$$

Determine si $\mathcal{R}$ es reflexiva, simétrica, transitiva, antisimétrica o total.

Solución. En primer lugar, se observa que sí es reflexiva, pues $1\mathcal{R}1$, $2\mathcal{R}2$, $3\mathcal{R}3$ y $4\mathcal{R}4$. No es simétrica, pues se tiene que $4\mathcal{R}1$ pero $1\not\mathcal{R}4$, es decir, $4\mathcal{R}1 \Rightarrow 1\not\mathcal{R}4$ es falsa. No es transitiva, ya que $4\mathcal{R}1$ y $1\mathcal{R}3$, pero $4\mathcal{R}3$, es decir, $4\mathcal{R}1 \wedge 1\mathcal{R}3 \Rightarrow 4\mathcal{R}3$ es falsa. No es antisimétrica, ya que $1\mathcal{R}2$ y $2\mathcal{R}1$, pero $1 \neq 2$. Por último, no es total, ya que $2\not\mathcal{R}4$ y $4\not\mathcal{R}2$, esto último es equivalente a decir que $2\mathcal{R}4 \vee 4\mathcal{R}2$ es falsa. ■

Es importante aclarar que los conceptos de simetría y antisimetría no son opuestos, es decir, se pueden obtener relaciones que sean simétricas y antisimétricas al mismo tiempo (vea ejercicio 5 de la sección 3.3).

Ejemplo 25. *Sea E un conjunto no vacío y sea $\mathcal{R}$ una relación definida sobre $P(E)$ que satisface*

$$A\mathcal{R}B \iff (A \cup B = A)$$

Analice cuáles propiedades cumple $\mathcal{R}$.

Solución. Es claro que sí es reflexiva, pues $A \cup A = A$, y así se cumple que $A\mathcal{R}A$ para todo $A \in P(E)$. Además, recuerde que en el capítulo 2 se demostró que $A \cup B = A$ es equivalente a la proposición $B \subseteq A$, con la cual se verifica que la relación sí es transitiva y no es simétrica. Por otro lado, como se sabe que $A \subseteq B \wedge B \subseteq A$ implica que $A = B$, se concluye que la relación sí es antisimétrica. Por último, la relación no es total, pues es fácil verificar que para el conjunto de tres elementos $E = \{1, 2, 3\}$ se verifica que $\{1, 2\} \cup \{2, 3\} \neq \{1, 2\}$, y además $\{2, 3\} \cup \{1, 2\} \neq \{2, 3\}$, con lo cual no se cumple la definición de total. ■

Ejemplo 26. *Sobre $\mathbb{Z}$ se define la relación $\mathcal{R}$, por:*

$$a\mathcal{R}b \iff (\exists k \in \mathbb{Z} \quad \textit{tal que} \quad b - a = 3k)$$

Analice cuáles propiedades satisface la relación $\mathcal{R}$.

Solución. Se analizará si $\mathcal{R}$ es reflexiva, simétrica, transitiva, antisimétrica o total.

- Sí es reflexiva, pues para $k = 0$ se tiene que $a - a = 0 = 3 \cdot 0$, y esto verifica que $a\mathcal{R}a$ para todo a en $\mathbb{Z}$.

- Sí es simétrica, pues si $a\mathcal{R}b$, $\exists k \in \mathbb{Z}$ tal que $b - a = 3k$, y al multiplicar ésta por -1 se obtiene $a - b = 3 \cdot (-k)$. Como $-k \in \mathbb{Z}$, esto ha probado que $b\mathcal{R}a$.

- Se prueba que sí es transitiva:

$$\begin{aligned} & a\mathcal{R}b \ \wedge \ b\mathcal{R}c \\ \Rightarrow \ & (\exists k_1 \in \mathbb{Z} \ / \ \ b - a = 3k_1) \ \wedge \ (\exists k_2 \in \mathbb{Z} \ / \ \ c - b = 3k_2) \\ \Rightarrow \ & b - a + c - b = 3k_1 + 3k_2 \\ \Rightarrow \ & c - a = 3(k_1 + k_2) = 3k_3 \\ \Rightarrow \ & a\mathcal{R}c \end{aligned}$$

  Puesto que $k_3 \in \mathbb{Z}$, se ha probado que $a\mathcal{R}b \ \wedge \ b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

- No es antisimétrica, pues se cumple que, por ejemplo, $2\mathcal{R}5$ y también se cumple que $5\mathcal{R}2$, y con ello no satisface la definición.

- No es total, pues se cumple que, por ejemplo, $2\not{\mathcal{R}}3$ y también se cumple que $3\not{\mathcal{R}}2$, y con ello no satisface la definición.

■

Si $\mathcal{R} = (G, A, A)$ es una relación definida sobre A, se define la **diagonal** de A como el conjunto

$$D = \{(x, x) \ / \ \ x \in A\}$$

Ejemplo 27. *Si $\mathcal{R} = (G, A, A)$ es una relación definida sobre A, demuestre que $\mathcal{R}$ es antisimétrica si y solo si $G \cap G^{-1} \subseteq D$.*

Solución. Es necesario probar ambas direcciones:

"$\Rightarrow$" Sea $(a,b) \in G \cap G^{-1} \Rightarrow (a,b) \in G \ \wedge \ (a,b) \in G^{-1} \Rightarrow a\mathcal{R}b \ \wedge \ a\mathcal{R}^{-1}b \Rightarrow a\mathcal{R}b \wedge b\mathcal{R}a$ y esto implica que $a = b$, pues por hipótesis, $\mathcal{R}$ es antisimétrica. Con esto se ha probado que $(a,b) \in G \cap G^{-1} \Rightarrow a = b$, es decir, $(a,b) \in D$.

"$\Leftarrow$" Sean a y b tales que $a\mathcal{R}b \wedge b\mathcal{R}a$, así $a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a\mathcal{R}b \wedge a\mathcal{R}^{-1}b \Rightarrow (a,b) \in G \wedge (a,b) \in G^{-1} \Rightarrow (a,b) \in G \cap G^{-1}$ y como por hipótesis se tiene que $G \cap G^{-1} \subseteq D$, se conluye que $(a,b) \in D$, esto implica que $a = b$. Se ha probado que $a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a = b$; por lo tanto, se ha probado que $\mathcal{R}$ es antisimétrica. ■

Ejemplo 28. *Pruebe que si $\mathcal{R}$ y $\mathcal{R}^{-1}$ son reflexivas, entonces $\mathcal{R} \cup \mathcal{R}^{-1}$ es reflexiva.*

Solución. A partir de la hipótesis se sabe que $a\mathcal{R}a$ y $a\mathcal{R}^{-1}a$, para todo $a \in A$, pues $\mathcal{R}$ y $\mathcal{R}^{-1}$ son reflexivas. Por la regla de inferencia de la adición, se tiene que $a\mathcal{R}a \ \vee \ a\mathcal{R}^{-1}a$, y de ahí se implica que $a\mathcal{R} \cup \mathcal{R}^{-1}a$, con lo cual $\mathcal{R} \cup \mathcal{R}^{-1}$es reflexiva. ■

Ejemplo 29. *Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones definidas sobre un conjunto A, con A no vacío. Si $\mathcal{R}$ es transitiva y se cumple que $a(\mathcal{R} \cup \mathcal{S})b$ y $b\mathcal{R}c$, entonces demuestre que $a\,[\mathcal{R} \cup (\mathcal{R} \circ \mathcal{S})]\,c$.*

Solución. Aplicando las definiciones y la hipótesis de que $\mathcal{R}$ es transitiva, se obtiene:

$$\begin{aligned}
a(\mathcal{R} \cup \mathcal{S})b \ \wedge \ b\mathcal{R}c \ &\Rightarrow \ (a\mathcal{R}b \ \vee \ a\mathcal{S}b) \ \wedge \ b\mathcal{R}c \\
&\Rightarrow \ (a\mathcal{R}b \ \wedge \ b\mathcal{R}c) \ \vee \ (a\mathcal{S}b \ \wedge \ b\mathcal{R}c) \\
&\Rightarrow \ a\mathcal{R}c \ \vee \ a(\mathcal{R} \circ \mathcal{S})c \\
&\Rightarrow \ a\,[\mathcal{R} \cup (\mathcal{R} \circ \mathcal{S})]\,c
\end{aligned}$$

■

Para finalizar esta sección, se define la propiedad $\leq$ para matrices booleanas, que será útil para verificar las propiedades que satisfacen las relaciones definidas sobre un conjunto finito A (véase teorema 2).

Si A y B son matrices booleanas de tamaño $m \times n$, se dice que **A es menor o igual que B** si y solo si $a_{ij} \leq b_{ij}$, para todo $1 \leq i \leq m$, $1 \leq j \leq n$, y se simboliza como $\boldsymbol{A \leq B}$.

Ejemplo 30. *Si* $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ *y* $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$, *es claro que se cumple* $A \leq B$*, es decir,* $A \leq B$ *es verdadera, pues al comparar entrada por entrada se satisface que* $a_{ij} \leq b_{ij}$. ■

Ejemplo 31. *Si* $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ *y* $B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, *es claro que* $A \leq B$ *no se cumple, es decir, la proposición* $A \leq B$ *es falsa; así, se tiene que* $A \nleq B$*, pues al comparar entrada por entrada se observa que* $A[2,3] = 1 \nleq 0 = B[2,3]$. ■

Teorema 1. *Si* $\mathcal{R}$ *y* $\mathcal{S}$ *son relaciones definidas de* A *en* B*, entonces*

$$M_{\mathcal{R}} \leq M_{\mathcal{S}} \Longleftrightarrow G_{\mathcal{R}} \subseteq G_{\mathcal{S}}$$

Demostración. Ejercicio. □

Teorema 2. *Si* $\mathcal{R}$ *es una relación definida sobre un conjunto finito* A*, donde* A *contiene* n *elementos, entonces se cumple:*

1. $\mathcal{R}$ *es reflexiva si y solo si* $I_n \leq M_{\mathcal{R}}$
2. $\mathcal{R}$ *es simétrica si y solo si* $M_{\mathcal{R}} = M_{\mathcal{R}}^T$
3. $\mathcal{R}$ *es transitiva si y solo si* $M_{\mathcal{R} \circ \mathcal{R}} \leq M_{\mathcal{R}}$

4. *$\mathcal{R}$ es antisimétrica si y solo si $M_{\mathcal{R}} \wedge M_{\mathcal{R}}^T \leq I_n$*

5. *$\mathcal{R}$ es total si y solo si $M_{\mathcal{R}} \vee M_{\mathcal{R}}^T = \mathbf{1}_{n\times n}$*

Demostración. Se prueba solamente la parte 3., el resto está enunciado en el ejercicio 19. Así, como por hipótesis A es finito y tiene n elementos, es posible suponer que $A = \{a_1, a_2, \ldots, a_n\}$.

"$\Rightarrow$" Suponiendo que $\mathcal{R}$ es transitiva, se debe probar que $M_{\mathcal{R}\circ\mathcal{R}} \leq M_{\mathcal{R}}$, es decir, que la entrada ij de la matriz $M_{\mathcal{R}\circ\mathcal{R}}$ es menor o igual que la entrada ij de la matriz $M_{\mathcal{R}}$.
Prueba: Si $M_{\mathcal{R}\circ\mathcal{R}}[i,j] = 0$ no hay nada que probar, pues la desigualdad se satisface.
Si $M_{\mathcal{R}\circ\mathcal{R}}[i,j] = 1$, entonces existe k de manera que $M_{\mathcal{R}}[i,k] = 1$ y $M_{\mathcal{R}}[k,j] = 1$; por lo tanto, $a_i\mathcal{R}a_k$ y $a_k\mathcal{R}a_j$, por lo que $a_i\mathcal{R}a_j$ por hipótesis, pues se asume que $\mathcal{R}$ es transitiva. De donde se concluye que $M_{\mathcal{R}}[i,j] = 1$.

"$\Leftarrow$" Asumiendo que $M_{\mathcal{R}\circ\mathcal{R}} \leq M_{\mathcal{R}}$ como hipótesis, se debe probar que $\mathcal{R}$ es transitiva.
Prueba: suponga que $a_i\mathcal{R}a_k$ y $a_k\mathcal{R}a_j$, esto implica que $M_{\mathcal{R}}[i,k] = 1$ y $M_{\mathcal{R}}[k,j] = 1$, es decir, se tiene que $M_{\mathcal{R}\circ\mathcal{R}}[i,j] = 1$, pero como $M_{\mathcal{R}\circ\mathcal{R}} \leq M_{\mathcal{R}}$ y se sabe que el lado izquierdo es 1, se concluye que $M_{\mathcal{R}}[i,j] = 1$, por lo que se concluye que $a_i\mathcal{R}a_j$.

□

Ejemplo 32. *Sobre un conjunto $A = \{a, b, c\}$ se define una relación $\mathcal{R}$, de manera que* $M_{\mathcal{R}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. *Utilice el teorema anterior y analice las propiedades que satisface la relación $\mathcal{R}$.*

Solución. En primer lugar, se observa que $I_3 \not\leq M_{\mathcal{R}}$; por lo tanto, $\mathcal{R}$ no es reflexiva. Como $M_{\mathcal{R}}^T = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, es claro que $M_{\mathcal{R}} \neq M_{\mathcal{R}}^T$, por lo que $\mathcal{R}$ no es simétrica. Al calcular, se obtiene que $M_{\mathcal{R}\circ\mathcal{R}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, por lo que $M_{\mathcal{R}\circ\mathcal{R}} \not\leq M_{\mathcal{R}}$ y consecuentemente $\mathcal{R}$ no es transitiva. Se tiene que $M_{\mathcal{R}} \wedge M_{\mathcal{R}}^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \not\leq I_3$, por lo que $\mathcal{R}$ no es antisimétrica y, finalmente, $M_{\mathcal{R}} \vee M_{\mathcal{R}}^T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \neq \mathbf{1}_{3\times 3}$, por lo que $\mathcal{R}$ no es total. ■

Ejercicios (sección 3.3)

1. Sea $A = \{1, 2, 3, 4\}$ y las relaciones $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, $\mathcal{R}_4$ y $\mathcal{R}_5$, definidas sobre A, cuyos gráficos respectivos son:

   (a) $G_1 = \big\{(1, 1), (4, 4)\big\}$
   (b) $G_2 = \big\{(1, 1), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\big\}$
   (c) $G_3 = \big\{(1, 1), (2, 1), (1, 2), (2, 2), (2, 3), (3, 2)\big\}$
   (d) $G_4 = \big\{(1, 1), (1, 2), (2, 3), (1, 3), (4, 4)\big\}$
   (e) $G_5 = \big\{(1, 1), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\big\}$

   Para cada una de estas relaciones, establezca si son reflexivas, simétricas, transitivas, antisimétricas o totales.

2. Si $A = \{1, 2, 3, 4, 5\}$ y $\mathcal{R}$ una relación definida en A, cuyo gráfico es $\big\{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 1), (2, 3), (3, 3), (4, 4), (3, 2), (1, 4)\big\}$,

determine si $\mathcal{R}$ es una relación reflexiva, simétrica, transitiva, antisimétrica o total.

3. Dé un ejemplo de una relación que sea simétrica y reflexiva pero no transitiva, y un ejemplo de una relación que sea transitiva y reflexiva pero no simétrica.

4. Para cada una de las siguientes relaciones, definidas sobre $\mathbb{Z}$, determine si $\mathcal{R}$ es reflexiva, simétrica, transitiva, antisimétrica o total.

   (a) $a\mathcal{R}b \Longleftrightarrow a - b \leq 10$.

   (b) $a\mathcal{R}b \Longleftrightarrow (a > 0 \ \wedge \ b > 0) \ \vee \ (a < 0 \ \wedge \ b < 0)$.

5. Determine una relación sobre $A = \{1, 2, 3\}$ que sea reflexiva, simétrica y antisimétrica.

6. Utilice el teorema 2 para analizar las propiedades que cumple la relación $\mathcal{R}$ si su matriz asociada es:

   (a) $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

   (b) $\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

7. Analice cuáles propiedades cumple la relación $\mathcal{R}$, definida en $\mathbb{N}$ por:

$$a\mathcal{R}b \Longleftrightarrow a - b \in \mathbb{N}$$

8. Analice cuáles propiedades cumple la relación $\mathcal{R}$, definida en $\mathbb{R}$ por:

$$a\mathcal{R}b \Longleftrightarrow a - b \in \mathbb{Z}$$

9. Si $A = \{1, 2, 3\}$. Se define una relación $\mathcal{R}$ sobre $P(A)$ como

$$M \,\mathcal{R}\, N \iff \big[(M \cap N = \varnothing) \vee (M = N)\big]$$

Analice cuáles propiedades cumple la relación $\mathcal{R}$, calcule su gráfico.

10. Sea E un conjunto no vacío. Para cada una de las siguientes relaciones, definidas sobre $P(E)$, analice cuáles propiedades cumple:

    (a) $A\mathcal{R}B \iff (A \cap B = \varnothing)$
    (b) $A\mathcal{R}B \iff (A \cap B = A)$
    (c) $A\mathcal{R}B \iff (A - B \neq \varnothing)$

11. Sea $\mathcal{R}$ una relación definida sobre A, $A \neq \varnothing$, demuestre:

    (a) Si $\mathcal{R}$ es simétrica, entonces $\mathcal{R}^{-1}$ es simétrica.
    (b) Si $\mathcal{R}$ es antisimétrica, entonces $\mathcal{R}^{-1}$ es antisimétrica.
    (c) Si $\mathcal{R}$ es reflexiva, entonces $\mathcal{R} \cap \mathcal{R}^{-1}$ es reflexiva.
    (d) Si $\mathcal{R}$ es transitiva, entonces $\mathcal{R} \cap \mathcal{R}^{-1}$ es transitiva.
    (e) Si $\mathcal{R}$ es antisimétrica, entonces $\mathcal{R} \cap \mathcal{R}^{-1}$ es antisimétrica.

12. Sea $\mathcal{R}$ una relación definida sobre A, $A \neq \varnothing$. Muestre, con un contraejemplo, que las siguientes proposiciones son falsas.

    (a) $\mathcal{R}$ y $\mathcal{R}^{-1}$ son transitivas, entonces $\mathcal{R} \cup \mathcal{R}^{-1}$ es transitiva.
    (b) $\mathcal{R} \cup \mathcal{R}^{-1}$ es transitiva, entonces $\mathcal{R}$ y $\mathcal{R}^{-1}$ son transitivas.
    (c) $\mathcal{R}$ es antisimétrica, entonces $\mathcal{R} \cup \mathcal{R}^{-1}$ es antisimétrica.

13. Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones definidas sobre un conjunto A, con A no vacío. Demuestre que si $\mathcal{R}$ es antisimétrica, entonces $\mathcal{R}^{-1} \cap \mathcal{S}$ es antisimétrica.

14. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones transitivas definidas sobre un conjunto A, con A no vacío. Demuestre que si $a(\mathcal{R} \cap \mathcal{S})b \;\wedge\; b(\mathcal{R} \circ \mathcal{S})a$, entonces $a(\mathcal{R} \circ \mathcal{S})b$.

15. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones definidas sobre un conjunto A, con A no vacío. Si se sabe que $\mathcal{R}$ es transitiva y $\mathcal{S}$ es simétrica, demuestre que si $a(\mathcal{R} \cap \mathcal{S})b \,\wedge\, b\mathcal{R}c$, entonces $b(\mathcal{R} \circ \mathcal{S})c$.

16. Sea $\mathcal{R}$ una relación definida sobre A y se dice que $\mathcal{R}$ es **irreflexiva** si para toda $a \in A$, se cumple $a \not\mathcal{R} a$.

    (a) Dé un ejemplo de una relación, sobre $A = \{a, b, c\}$, que no sea reflexiva y no sea irreflexiva.

    (b) Dé un ejemplo de una relación, sobre determinado conjunto A, que sea reflexiva e irreflexiva.

17. Sea $\mathcal{R}$ una relación definida sobre A y se dice que $\mathcal{R}$ es **asimétrica** si $\forall a, b \in A$, se cumple $a\mathcal{R}b \Rightarrow b \not\mathcal{R} a$.

    (a) Dé un ejemplo de una relación, sobre $A = \{a, b, c\}$, que no sea simétrica, no sea antisimétrica y no sea asimétrica.

    (b) Si es posible, dé un ejemplo de una relación que sea simétrica, antisimétrica y asimétrica.

18. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones definidas sobre un conjunto A, con A no vacío. Demuestre que si $\mathcal{R}$ y $\mathcal{S}$ son simétricas, entonces $\mathcal{R} \circ \mathcal{S} = (\mathcal{S} \circ \mathcal{R})^{-1}$.

19. Suponga que $\mathcal{R}$ es una relación definida sobre un conjunto finito A de n elementos. Demuestre que:

    (a) $\mathcal{R}$ es reflexiva si y solo si $I_n \leq M_{\mathcal{R}}$

    (b) $\mathcal{R}$ es simétrica si y solo si $M_{\mathcal{R}} = M_{\mathcal{R}}^T$

    (c) $\mathcal{R}$ es antisimétrica si y solo si $M_{\mathcal{R}} \wedge M_{\mathcal{R}}^T \leq I_n$

    (d) $\mathcal{R}$ es total si y solo si $M_{\mathcal{R}} \vee M_{\mathcal{R}}^T = \mathbf{1}_{n \times n}$

20. Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones definidas de A en B, demuestre que:

    (a) $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$

(b) $(\mathcal{R} \cup \mathcal{S})^{-1} = \mathcal{R}^{-1} \cup \mathcal{S}^{-1}$

(c) $(\mathcal{R} \cap \mathcal{S})^{-1} = \mathcal{R}^{-1} \cap \mathcal{S}^{-1}$

(d) $(\mathcal{R} - \mathcal{S})^{-1} = \mathcal{R}^{-1} - \mathcal{S}^{-1}$

21. Para las relaciones $\mathcal{R} = (G, A, B)$, $\mathcal{S} = (H, B, C)$ y $\mathcal{T} = (F, B, C)$, demuestre que:

    (a) $(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$

    (b) $(\mathcal{S} \cup \mathcal{T}) \circ \mathcal{R} = (\mathcal{S} \circ \mathcal{R}) \cup (\mathcal{T} \circ \mathcal{R})$

    (c) $(\mathcal{S} \cap \mathcal{T}) \circ \mathcal{R} \subseteq (\mathcal{S} \circ \mathcal{R}) \cap (\mathcal{T} \circ \mathcal{R})$

22. Sean $\mathcal{R} = (G, A, B)$ y $\mathcal{S} = (H, A, B)$, demuestre que:

    (a) $D_{\mathcal{R} \cup \mathcal{S}} = D_{\mathcal{R}} \cup D_{\mathcal{S}}$

    (b) $D_{\mathcal{R} \cap \mathcal{S}} \subseteq D_{\mathcal{R}} \cap D_{\mathcal{S}}$

    (c) $D_{\mathcal{R}} - D_{\mathcal{S}} \subseteq D_{\mathcal{R} - \mathcal{S}}$

    (d) $(\mathcal{R} \cup \mathcal{S})[A] = \mathcal{R}[A] \cup \mathcal{S}[A]$

    (e) $(\mathcal{R} \cap \mathcal{S})[A] \subseteq \mathcal{R}[A] \cap \mathcal{S}[A]$

    (f) $\mathcal{R}[A] - \mathcal{S}[A] \subseteq (\mathcal{R} - \mathcal{S})[A]$

3.4 Relaciones de equivalencia

De acuerdo con las propiedades que satisface o no determinada relación, se puede clasificar de diferentes formas. En esta sección se definen los conceptos básicos sobre las relaciones de equivalencia que, como se verá, permitirán asociar o agrupar los elementos afines de los conjuntos y así particionarlos en subconjuntos de tal manera que éstos sean disjuntos.

Si $\mathcal{R}$ es una relación sobre el conjunto A, se dice que la relación $\mathcal{R}$ es de **equivalencia** si y solo si es reflexiva, simétrica y transitiva.

Ejemplo 33. *Si se considera la definición de* ***hermanos*** *como las personas que tienen el mismo padre y la misma madre, y se define la relación $\mathcal{R}$ sobre un conjunto de personas A, como $a\mathcal{R}b$ si y solo si a es hermano de b. Con base en la definición dada, $a\mathcal{R}a$ es verdadera, ya que a y a tienen el mismo padre y la misma madre; así, esta relación es reflexiva, además, es fácil corroborar que es simétrica y transitiva; por lo tanto, es de equivalencia sobre este conjunto de personas.* ■

Si $\mathcal{R} = (G, A, A)$ es una relación de equivalencia sobre el conjunto A, entonces la **clase de equivalencia de $\boldsymbol{a}$**, que se denota por $\overset{\bullet}{\boldsymbol{a}}$, es el conjunto

$$\overset{\bullet}{a} = \{b \in A \;\; / \;\; a\mathcal{R}b\}$$

En otras palabras, la clase de equivalencia de un elemento está formada por todos los elementos que se relacionan con él. Además, el conjunto formado por todas las clases de equivalencia se llama el **conjunto cociente** y se denota por $\boldsymbol{A/\mathcal{R}}$, es decir:

$$A/\mathcal{R} = \left\{\overset{\bullet}{a} \;\; / \;\; a \in A\right\}$$

En ocasiones, la clase de equivalencia de a se representa por medio de los símbolos $\overline{\boldsymbol{a}}$ o $[\boldsymbol{a}]$.

Ejemplo 34. *En el ejemplo* 33 *se analizó la relación "hermano de" y se comprobó que es una relación de equivalencia; por lo tanto, se puede hablar de clases de equivalencia. En este caso, la clase de equivalencia de cualquier persona estaría formada por ella y sus hermanos, si los tuviera.* ■

Ejemplo 35. *Sea* $A = \{a, c, d, f\}$ *y sea* $\mathcal{R}$ *una relación definida sobre* A*, donde su gráfico es* $\big\{(a,a),(a,d),(c,c),(d,a),(d,d),(f,f)\big\}$*. Si se sabe que* $\mathcal{R}$ *es una relación de equivalencia sobre* A*, determine todas las clases de equivalencia y el conjunto cociente de la relación* $\mathcal{R}$ *sobre* A*.*

Solución. Los elementos que se relacionan con a son a y d, con lo cual $\overset{\bullet}{a}= \{a, d\}$; el único elemento que se relaciona con c es c, con lo cual $\overset{\bullet}{c}= \{c\}$; de la misma manera, el único elemento que se relaciona con f es f, así $\overset{\bullet}{f}= \{f\}$. Además, dado que los conjuntos $\overset{\bullet}{d}$ y $\overset{\bullet}{a}$ contienen los mismos elementos, es claro que $\overset{\bullet}{d}=\overset{\bullet}{a}$. Por último, el conjunto cociente es $A/\mathcal{R} = \left\{\overset{\bullet}{a}, \overset{\bullet}{c}, \overset{\bullet}{f}\right\}$. ■

Ejemplo 36. *Sobre* $\mathbb{Z}$ *se define la relación* $\mathcal{R}$ *por:*

$$a\mathcal{R}b \Longleftrightarrow (\exists k \in \mathbb{Z} \quad tal\ que \quad b - a = 3k)$$

En el ejemplo 26*, página* 188*, se demostró que esta relación es reflexiva, simétrica y transitiva; por lo tanto,* $\mathcal{R}$ *es una relación de equivalencia. Por otro lado, la clase de equivalencia de* 2 *es* $\overset{\bullet}{2}= \{b \in \mathbb{Z} \ / \ 2\mathcal{R}b\}$*, es decir, es el conjunto de los enteros* b *para los cuales* $b-2$ *es un múltiplo de* 3*, así:*

$$\overset{\bullet}{2}= \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

De la misma manera se obtiene que

$$\begin{aligned} \overset{\bullet}{0} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ \overset{\bullet}{1} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \end{aligned}$$

Por último, para determinar el conjunto cociente, se deben calcular todas las clases de equivalencia posibles, pero es necesario observar que cualquier otra clase de equivalencia es una de las tres anteriores, pues, por ejemplo, $\dot{3}=\dot{-6}=\dot{0}$*, de donde se obtiene que* $\mathbb{Z}/\mathcal{R} = \left\{\dot{0}, \dot{1}, \dot{2}\right\}$. ■

Como se mencionó anteriormente, las relaciones de equivalencia particionan los conjuntos en conjuntos disjuntos, donde estos son las clases de equivalencia que forman el conjunto cociente. Antes de continuar, es necesario repasar el concepto de partición dado en el ejercicio 8 de la sección 2.7.

> Si A es un conjunto y K es una familia de subconjuntos no vacíos de A, se dice que K es una **partición** de A si se cumple que todo elemento de A pertenece a uno y solo uno de los conjuntos de la familia K.

Esta definición establece que una colección de subconjuntos no vacíos de A es una partición de A si y solo si la unión de todos estos es A y la intersección de cualesquiera dos de estos conjuntos es vacía.

Ejemplo 37. *Para el conjunto* $A = \{1, 2, 3, 4\}$ *se verifica que la familia* $K_1 = \big\{\{1, 3, 4\}, \{2\}\big\}$ *es una partición de* A*, pues satisface todas las condiciones de la definición dada, mientras que la familia* $K_2 = \big\{\{1, 2, 3\}, \{3, 4\}\big\}$ *no es una partición de* A*, pues el elemento* 3 *pertenece a dos elementos distintos de* K. ■

Ejemplo 38. *Si* $A = \{1, 2, 3\}$*, determine las posibles particiones de* A.

Solución. Existen cinco: $K_1 = \big\{\{1\}, \{2\}, \{3\}\big\}$; $K_2 = \big\{\{1, 2\}, \{3\}\big\}$; $K_3 = \big\{\{1, 3\}, \{2\}\big\}$; $K_4 = \big\{\{2, 3\}, \{1\}\big\}$; $K_5 = \big\{\{1, 2, 3\}\big\}$. ■

Ejemplo 39. *En el ejemplo* 36 *se demostró que el conjunto cociente en la relación módulo* 3 *es* $\mathbb{Z}/\mathcal{R} = \left\{\dot{0}, \dot{1}, \dot{2}\right\}$*; como* $\dot{0}$, $\dot{1}$, $\dot{2}$ *son no vacíos, mutuamente excluyentes y su unión da como resultado el conjunto* $\mathbb{Z}$*, la familia* $\left\{\dot{0}, \dot{1}, \dot{2}\right\}$ *es una partición de* $\mathbb{Z}$. ■

Ejemplo 40. *Si* $A = \{a, b, c, d, e\}$, *determine el gráfico de la relación de equivalencia asociada a la partición* $P = \big\{\{a, c\}, \{e\}, \{b, d\}\big\}$ *de* A.

Solución. Los conjuntos $\{a, c\}$, $\{e\}$, $\{b, d\}$ deben ser las clases de equivalencia de la relación inducida; por lo tanto, los elementos de cada uno de estos conjuntos se deben relacionar solamente con los de ese conjunto, así, $G = \big\{(a, a), (c, c), (a, c), (c, a), (e, e), (b, b), (d, d), (b, d), (d, b)\big\}$ es el gráfico asociado a la relación. ■

Ejemplo 41. *Suponga que una universidad tiene* 5 *años de fundada y los estudiantes pueden optar por* 6 *diferentes carreras. Sobre el conjunto* U *formado por los estudiantes de esta universidad se definen dos relaciones* $\mathcal{R}$ *y* $\mathcal{S}$ *de la siguiente manera: en primer lugar,* $a\mathcal{R}b$ *si y solo si* a *y* b *ingresaron el mismo año a la universidad; en segundo lugar,* $a\mathcal{S}b$ *si y solo si* a *estudia la misma carrera que* b. *Se verifica fácilmente que ambas relaciones son de equivalencia; por lo tanto, cada una de ellas determina una partición. De esta forma, es claro que* $\mathcal{R}$ *particiona a* U *en* 5 *clases de equivalencia, donde cada una está formada por todos los estudiantes que entraron el mismo año. Mientras,* $\mathcal{S}$ *particiona a* U *en* 6 *clases de equivalencia, donde cada una está formada por todos los estudiantes que entraron en una determinada carrera. Por otro lado,* $\mathcal{R} \cap \mathcal{S}$ *particionará a* U *en* 30 *clases de equivalencia, donde cada una está formada por todos los estudiantes que entraron en el mismo año y estudian la misma carrera.* ■

Ejercicios (sección 3.4)

1. Sea $A = \{a, b, c, d, e, f\}$ y sea $\mathcal{R}$ una relación definida sobre A, con $G_{\mathcal{R}} = \big\{(a, a),(a, b),(b, a),(b, b),(c, e),(d, d),(c, c),(e, c),(e, e),(f, f)\big\}$ su gráfico. Si se sabe que $\mathcal{R}$ es una relación de equivalencia sobre A, determine la clase de equivalencia $\dot{a}$ y determine el conjunto cociente de la relación $\mathcal{R}$ sobre A.

2. Determine todas las posibles matrices asociadas a una relación de equivalencia sobre un conjunto de cuatro elementos, de manera que la mitad de sus entradas sean unos y la otra mitad sean ceros.

3. Defina la relación $\mathcal{R}$ sobre $\mathbb{N}^* = \{1, 2, 3, \dots\}$, por:

$$a\mathcal{R}b \iff (\exists k \in \mathbb{Z} \quad \text{tal que} \quad b = a \cdot k)$$

   Determine si $\mathcal{R}$ es de equivalencia.

4. Sea A un conjunto, sobre $P(A)$ se define la relación $\mathcal{R}$ de manera que $M\mathcal{R}N$ si y solo si $|M| = |N|$, es decir, M se relaciona con N si y solo si tienen la misma cardinalidad. Pruebe que $\mathcal{R}$ es de equivalencia.

5. Si $A = \{a, b, c, d\}$ y la relación $\mathcal{R}$ está definida como en el ejercicio 4, calcule $\overset{\bullet}{\varnothing}$ y $\overset{\bullet}{\{b, c\}}$.

6. Sobre $\mathbb{Z}$ se define la relación $\mathcal{R}$, por:

$$a\mathcal{R}b \iff (\exists k \in \mathbb{Z} \quad \text{tal que} \quad b - a = 5k)$$

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Calcule la clase de equivalencia $\overset{\bullet}{2}$ y el conjunto cociente $\mathbb{Z}/\mathcal{R}$.

7. Sobre $\mathbb{R}^*$ se define la relación $\mathcal{R}$, por $a\mathcal{R}b \Leftrightarrow ab > 0$:

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Determine el conjunto cociente $\mathbb{R}^*/\mathcal{R}$.

8. Sobre $\mathbb{N} \times \mathbb{N}$ se define la relación $\mathcal{R}$ de la siguiente manera:

$$(a, b)\mathcal{R}(c, d) \iff [a + d = b + c]$$

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Determine las clases de equivalencia de $(1, 1)$ y de $(3, 4)$.

9. Sobre $\mathbb{Z}$ se define la relación $\mathcal{R}$ de la siguiente manera:

$$a\mathcal{R}b \iff [a = b \ \vee \ a + b = 10]$$

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Represente su gráfico en un sistema de coordenadas.

   (c) Determine la $\overset{\bullet}{-3}$ y el conjunto cociente $\mathbb{Z}/\mathcal{R}$.

10. En $\mathbb{N}^* \times \mathbb{N}^*$ se define la relación $\mathcal{R}$ de la siguiente manera:

$$(a, b)\mathcal{R}(c, d) \iff [ad = bc]$$

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Determine las clases de equivalencia de $(2, 2)$ y de $(7, 4)$.

11. Sobre $\mathbb{Z} \times \mathbb{Z}$ se define la relación $\mathcal{R}$ de la siguiente manera:

$$(a, b)\mathcal{R}(c, d) \iff [3(a - c) = 2(b - d)]$$

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Determine las clases de equivalencia de $(0, -1)$ y de $(4, 9)$.

12. Sobre $\mathbb{Z}^* \times \mathbb{Z}^*$ se define una relación $\mathcal{R}$ de la siguiente manera:

$$\forall (a, b), (c, d) \in \mathbb{Z}^* \times \mathbb{Z}^* \big[\, (a, b)\mathcal{R}(c, d) \iff ac > 0 \ \ \wedge \ \ bd > 0 \,\big]$$

   (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

   (b) Determine la clase de equivalencia de $(-3, 5)$.

   (c) Determine $\mathbb{Z}^* \times \mathbb{Z}^*/\mathcal{R}$.

13. Verifique que $P = \big\{\{1, 4\}, \{3, 5\}, \{2\}, \{6\}\big\}$ es una partición del conjunto $A = \{1, 2, 3, 4, 5, 6\}$ y determine el gráfico de la relación inducida sobre A.

14. Verifique que $P = \big\{\{1,3,5,6\},\{2,4\}\big\}$ es una partición del conjunto $A = \{1,2,3,4,5,6\}$ y determine la matriz y el grafo asociados a la relación inducida sobre A.

15. Determine si $K = \big\{[n, n+1[\ \ / \ \ n \in \mathbb{Z}\big\}$ es una partición de $\mathbb{R}$.

16. Determine si $K = \big\{[n, n+2[\ \ / \ \ n \in \mathbb{Z}\big\}$ es una partición de $\mathbb{R}$.

17. Sea A el conjunto $\{1,2,3,4,5,6\}$. Sobre A se definen las relaciones de equivalencia $\mathcal{R}$, $\mathcal{S}$, donde sus gráficos son:

    (a) $G_{\mathcal{R}} = \big\{(1,1),(5,1),(1,5),(5,5),(2,2),(2,3),(2,4),(3,2),$
    $(3,3),(3,4),(4,2),(4,3),(4,4),(6,6)\big\}$

    (b) $G_{\mathcal{S}} = \big\{(1,1),(2,2),(3,3),(4,4),(4,5),(5,4),(5,5),(6,6)\big\}$

    Determine la partición de A inducida por cada una de ellas.

18. En una academia de lenguas, Juan, Ana, Mario, Pedro, Inés y María estudian francés y Marco, Cindy, Emily, Tomás, Carlos, Manuel, Felipe y Héctor estudian inglés. Sobre el conjunto U formado por los estudiantes de esta academia se definen dos relaciones $\mathcal{R}$ y $\mathcal{S}$, de manera que $a\mathcal{R}b$ si y solo si a y b estudian el mismo idioma y $a\mathcal{S}b$ si y solo si a y b son del mismo sexo. Verifique que ambas relaciones son de equivalencia. Además, determine el conjunto cociente determinado por la relación $\mathcal{R} \cap \mathcal{S}$.

19. Sea E un conjunto y $H \subseteq E$. Sobre $P(E)$ se define $\mathcal{R}$ por:

$$A\,\mathcal{R}\,B \Longleftrightarrow A \cap H = B \cap H$$

    (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

    (b) Si $E = \{a,b,c\}$ y $H = \{b\}$, determine todas las clases de equivalencia y escriba el conjunto cociente en este caso.

    (c) En general, ¿cuáles son las clases de equivalencia?

20. Sobre $\mathbb{Q}$ se define la relación $\mathcal{R}$ de la siguiente manera:

$$x\mathcal{R}y \iff \left[\exists h \in \mathbb{Z} \quad \text{tal que} \quad x = y + \frac{h}{3}\right]$$

    (a) Demuestre que $\mathcal{R}$ es una relación de equivalencia.

    (b) Calcule las clases de equivalencia $\overset{\bullet}{\frac{5}{3}}$ y $\overset{\bullet}{\frac{1}{2}}$ y determine dos elementos de cada una de ellas.

21. Un número n se llama **organizado** si existe una partición A_i del conjunto $A = \{1, 2, 3, \ldots, n\}$ de manera que el menor elemento de cada A_i corresponde a la cardinalidad de A_i. Verifique que 11 y 21 son números organizados.

22. Una relación $\mathcal{R}$ sobre A se llama **circular** si cumple la condición:

$$a\mathcal{R}b \ \wedge \ b\mathcal{R}c \Rightarrow c\mathcal{R}a$$

Demuestre que $\mathcal{R}$ es una relación de equivalencia si y solo si es reflexiva y circular.

23. Si $\mathcal{R}$ es una relación definida sobre A que satisface

$$a\mathcal{R}b \ \wedge \ c\mathcal{R}b \Rightarrow a\mathcal{R}c$$

y además cumple la condición

$$(\forall a \in A)(\exists b \in A) \ [a\mathcal{R}b]$$

demuestre que $\mathcal{R}$ es una relación de equivalencia.

3.5 Relaciones de orden

En esta sección se definen los conceptos básicos sobre las relaciones de orden y, lo que es muy importante, se plantea cómo este tipo de relaciones permite ordenar, en algún sentido, los elementos del conjunto donde ésta se define.

Si $\mathcal{R} = (G, E, E)$ es una relación sobre el conjunto E, se dice que la relación $\mathcal{R}$ es

- Un **pre-orden** si y solo si es reflexiva y transitiva.
- De **orden (parcial)** si y solo si es reflexiva, antisimétrica y transitiva.
- De **orden total** si y solo si es de orden y es total.

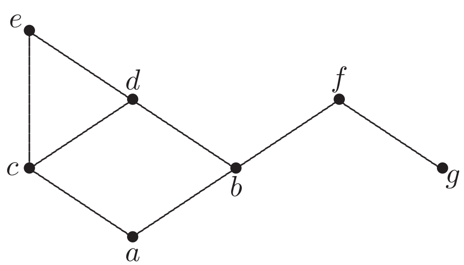
Ejemplo 42. *En el ejemplo* 33 *se definió la relación* $\mathcal{R}$ *sobre un determinado conjunto de personas, de manera que* $a\mathcal{R}b$ *si y solo si* a *es hermano de* b *y se demostró que ésta es de equivalencia sobre dicho conjunto de personas. Sin embargo, esta relación no es antisimétrica, ya que si* a *es hermano de* b *y lógicamente* b *es hermano de* a*, no se puede concluir que* $a = b$*; como no es antisimétrica, no es de orden parcial, por lo que tampoco será de orden total. Por último, note que no es total, pues no se puede garantizar, necesariamente, que dos personas arbitrarias del conjunto sean hermanos.* ■

Si lo que se quiere es ordenar un grupo de personas, se puede pensar en la edad, la estatura o el salario mensual, entre otros valores numéricos, y el concepto del primero y el último, en este orden que se considere, depende de cómo se defina la relación: una persona puede ser la primera en el grupo si se ordena por salario, pero podría ser la última si se ordena por estatura, e incluso ni el primero ni el último si se ordena por la edad, solo por imaginar una situación. Pero si lo que se quiere es ordenar conjuntos en vez de personas, una manera de hacerlo es pensar en la inclusión de conjuntos, como se verá en el ejemplo 45.

Ejemplo 43. *Sea* $E = \{a, b, c, d, e, f, g\}$ *y* $\mathcal{R}$ *una relación definida sobre* E*, cuyo gráfico es:*

$$\begin{aligned} G_{\mathcal{R}} \;=\; & \big\{(a,a),(a,b),(a,c),(a,d),(a,e),(a,f),(b,b),(b,d),(b,e),\\ & (b,f),(c,c),(c,d),(c,e),(d,d),(d,e),(e,e),(f,f),(g,g),(g,f)\big\} \end{aligned}$$

Se puede verificar fácilmente que $\mathcal{R}$ *es una relación de orden. Este gráfico se puede representar mediante el organigrama*



en donde, por claridad, se omiten los lazos en cada vértice. Además, x *está en un nivel inferior que* y *para cuando* $x\mathcal{R}y$*; por ejemplo, en este organigrama se tiene que* $a\mathcal{R}d$ *y se verifica para cada uno de los elementos de su gráfico. Es claro que la relación de orden no es total pues, por ejemplo,* $b \not\mathcal{R} g$ *y también* $g \not\mathcal{R} b$*.* ■

Si $\mathcal{R}$ es una relación de orden sobre E, se dice que E está $\mathcal{R}-$ordenado y se denota por $(E, \mathcal{R})$.

Ejemplo 44. *Sobre* $\mathbb{R}$ *la relación* $\leq$ *es una relación de orden total (véase ejercicio* 1*), por lo que es posible decir que* $\mathbb{R}$ *está ordenado por la relación* $\leq$*.* ■

Ejemplo 45. *Sobre $P(E)$ la relación $\subseteq$ es de orden (véase ejercicio 6), por lo que es posible decir que $P(E)$ está ordenado por la relación $\subseteq$.* ■

Sea $(E, \mathcal{R})$ un conjunto ordenado. Sea $A \subseteq E$, con $A \neq \varnothing$ y sea $x \in A$. Se dice que x es:

- un **elemento minimal** de A sii $\forall y \in A\ [y\mathcal{R}x \Rightarrow y = x]$.
- un **primer elemento** de A sii $x\mathcal{R}y$, $\forall y \in A$.
- un **elemento maximal** de A sii $\forall y \in A\ [x\mathcal{R}y \Rightarrow x = y]$.
- un **último elemento** de A sii $y\mathcal{R}x$, $\forall y \in A$.

Es decir, un elemento minimal es tal que no tiene predecesores, mientras que un primer elemento precede a todos. Por otro lado, un elemento maximal es tal que no tiene sucesores y el último elemento les sucede a todos los demás. Es claro que todo primer elemento será minimal, pero no a la inversa; además, todo último elemento será maximal, pero no necesariamente a la inversa.

Ejemplo 46. *En la misma situación del ejemplo 43, donde se tiene $E = \{a, b, c, d, e, f, g\}$, observe que:*

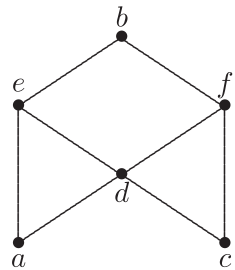
- *a y g son minimales de E, pero E no tiene primer elemento.*
- *e y f son elementos maximales de E, pero no hay último elemento.*

Si ahora se considera $A = \{a, b, c, d\}$ subconjunto de E, se tiene que:

- *el elemento a es primer elemento de A.*
- *el elemento d sería un último elemento de A.*

■

Ejemplo 47. *Sea* $E = \{a, b, c, d, e, f\}$ *y* $\mathcal{R}$ *una relación definida sobre* E*, cuyo organigrama, con las mismas convenciones que se explicaron en la página* 207*, es:*



A partir de él es posible determinar que su gráfico es:

$$\begin{aligned} G_{\mathcal{R}} &= \big\{(a,a),(a,e),(a,d),(a,f),(a,b),(d,f),(d,e),(d,b),(e,b),\\ &\quad (c,d),(c,e),(c,f),(c,b),(f,b),(b,b),(c,c),(d,d),(e,e),(f,f)\big\} \end{aligned}$$

Se puede verificar fácilmente que $\mathcal{R}$ *es una relación de orden. Es claro que la relación de orden no es total, pues* $a \not\mathcal{R} c$ *y también* $c \not\mathcal{R} a$*. Además,* a *y* c *son los elementos minimales, no hay primer elemento,* b *es el único maximal y, además, es el último elemento.* ■

Ejemplo 48. *Para* $E = \{a, b, c, d, e, f\}$ *y la misma situación del ejemplo* 47*, si se considera* $A = \{b, c, d, e, f\}$*, el elemento* c *es primer elemento de* A*, mientras que* b *sería un último elemento de* A*.* ■

Ejemplo 49. *Defina la relación* $\mathcal{R}$ *sobre* $\mathbb{Z}^*$*, por*

$$a\mathcal{R}b \Longleftrightarrow \left(\exists k \in \mathbb{Z} \quad \textit{tal que} \quad a = b^k\right)$$

Analice cuáles propiedades cumple la relación $\mathcal{R}$ *y determine si* $\mathcal{R}$ *es una relación de equivalencia, de orden o de orden total.*

Solución. A partir de las definiciones dadas, se procede a analizar:

- Es reflexiva, pues para $k = 1$ se tiene que $a = a^1$, y esto verifica que $a\mathcal{R}a$ para todo a en $\mathbb{Z}$

- No es simétrica pues, por ejemplo, con $k = 2$ se tiene que $9 = 3^2$ y así $9\mathcal{R}3$, pero $3 \not\mathcal{R} 9$, pues no existe un entero k que satisfaga $3 = 9^k$; note que el posible valor es $k = \frac{1}{2}$, pero $\frac{1}{2} \notin \mathbb{Z}$.

- Se prueba que sí es transitiva:

$$\begin{aligned}
& a\mathcal{R}b \ \wedge \ b\mathcal{R}c \\
\Rightarrow \quad & \exists k_1 \in \mathbb{Z} \ \text{ tal que } \ a = b^{k_1} \ \wedge \ \exists k_2 \in \mathbb{Z} \ \text{ tal que } \ b = c^{k_2} \\
\Rightarrow \quad & a = (c^{k_2})^{k_1} \\
\Rightarrow \quad & a = c^{k_2 \cdot k_1}
\end{aligned}$$

  y como $k_2 \cdot k_1 \in \mathbb{Z}$, se ha probado que $a\mathcal{R}c$.

- Se prueba que sí es antisimétrica:

$$\begin{aligned}
a\mathcal{R}b \ \wedge \ b\mathcal{R}a \quad & \Rightarrow \quad (\exists k_1 \in \mathbb{Z} \ / \ \ a = b^{k_1}) \ \wedge \ (\exists k_2 \in \mathbb{Z} \ / \ \ b = a^{k_2}) \\
& \Rightarrow \quad a = (a^{k_2})^{k_1} \\
& \Rightarrow \quad a = a^{k_2 \cdot k_1} \\
& \Rightarrow \quad k_2 \cdot k_1 = 1 \\
& \Rightarrow \quad (k_2 = k_1 = 1) \ \vee \ (k_2 = k_1 = -1) \\
& \Rightarrow \quad (a = b) \ \vee \ (a = b = 1) \ \vee \ (a = b = -1) \\
& \Rightarrow \quad a = b
\end{aligned}$$

  con lo cual $\mathcal{R}$ es antisimétrica.

- Es claro que no es total, pues, por ejemplo, $5 \not\mathcal{R} 4$ y $4 \not\mathcal{R} 5$.

De lo anterior se concluye que $\mathcal{R}$ no es de equivalencia, sí es de orden parcial y no es de orden total. En el ejercicio 5 deberá analizar los elementos minimales y maximales de este conjunto ordenado. ■

Ejercicios (sección 3.5)

1. Sobre $\mathbb{R}$ se define una relación $\leq$ de la siguiente manera:

$$\forall a, b \in \mathbb{R}\, [a \leq b \Longleftrightarrow b - a \geq 0]$$

   (a) Demuestre que $\leq$ es una relación de orden total.

   (b) Analice los elementos maximales, minimales, primer y último elementos para el conjunto $A = \,]-1, 5]$.

2. Dé un ejemplo de una relación sobre $E = \{1, 2, 3\}$ que sea total y de equivalencia.

3. Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ y $\mathcal{R}$ una relación definida sobre E, cuyo gráfico es

$$\begin{aligned} G_{\mathcal{R}} \;\; = \;\; & \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3),(4,3),(4,4),(4,5), \\ & (4,6),(5,3),(5,5),(5,6),(6,6),(7,7),(8,8),(9,9), \\ & (7,3),(7,5),(7,6),(7,8),(8,3),(8,5),(8,6),(9,6)\} \end{aligned}$$

   (a) Verifique que $\mathcal{R}$ es una relación de orden.

   (b) Represente mediante un organigrama.

   (c) Si existen, determine los elementos maximales, minimales, primero y último elemento.

4. Defina la relación $\mathcal{R}$ sobre $\mathbb{N}^* = \{1, 2, 3, \dots\}$, por

$$a\mathcal{R}b \Longleftrightarrow (\exists k \in \mathbb{Z} \;\; \text{tal que} \;\; b = a \cdot k)$$

   Determine si $\mathcal{R}$ es de orden o de orden total.

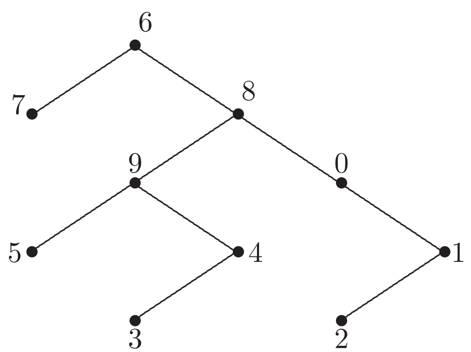
5. Analice los elementos maximales, minimales, primer y último elementos para el conjunto ordenado del ejemplo 49.

6. Sea E un conjunto no vacío. En $P(E)$ se define una relación $\mathcal{R}$ de la siguiente manera:

$$\forall A, B \in P(E)\,[A\,\mathcal{R}\,B \iff A \subseteq B]$$

Demuestre que $\mathcal{R}$ es una relación de orden. Además, determine si $\mathcal{R}$ es una relación de orden total.

7. Sea $E = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ y $\mathcal{R}$ una relación definida sobre E, cuyo organigrama es:



(a) Determine su gráfico y verifique que $\mathcal{R}$ es una relación de orden.

(b) Si existen, determine los elementos maximales, minimales, primero y último elemento.

8. Para la relación $\mathcal{R}$ del ejercicio anterior, tomando $E = \{a, b, c\}$, realice el organigrama y analice la existencia o no de los elementos maximales, minimales, primer y último elementos de $P(E)$.

9. Si $\mathcal{R}$ es una relación de orden sobre E, demuestre que $\mathcal{R}^{-1}$ es también una relación de orden sobre E.

Capítulo 4

Funciones

"Detrás de las paredes,
juegan los dioses;
juegan con números,
de los que está hecho el universo".

Le Corbusier

Conceptos y definiciones
Funciones lineal y cuadrática
Operaciones con funciones
Funciones inversas
Equipotencia
Principios de conteo

En este capítulo se analiza el tema de las funciones vistas como relaciones binarias. Además de sus definiciones, operaciones, gráficos, inversas, composición, funciones especiales y propiedades.

La principal intención no es hacer una exposición detallada sobre el tema de funciones reales de variable real, por supuesto que algunos conceptos básicos sobre funciones lineales y cuadráticas son abordados de manera superficial, así como algunos ejemplos de dominios máximos (sección 4.3*). De esta forma, el interés se centrará fundamentalmente en funciones definidas sobre conjuntos discretos, conjuntos producto o potencia, entre otros, principalmente finitos.*

Para repasar o profundizar en el tema tratado en este capítulo, se recomienda consultar las referencias bibliográficas [2], [15], [20] y [25].

4.1 Conceptos y definiciones

En el capítulo anterior se definieron las relaciones, las funciones serán un caso particular de ellas, es decir, las funciones son relaciones entre dos conjuntos, en donde el conjunto emisor debe ser el dominio y, además, los elementos del conjunto de salida deben tener una sola imagen. Esto es natural, ya que en el entorno es importante relacionar, por ejemplo, a cada persona con un único peso, edad, número de seguro social, carné universitario, entre otros, donde las variables relacionadas son personas con datos discretos y no continuos.

Otros ejemplos de funciones pueden ser la que asocia a cada provincia o estado de un país, su población en número de personas, su extensión en kilómetros cuadrados, su tasa de mortalidad, el gasto anual en salud, entre otras.

Sean A y B conjuntos no vacíos. Una **función** f de A en B es una relación de A en B tal que:

- $D_f = A$, es decir, el dominio es el conjunto emisor.
- Si (a, b) y (a, c) pertenecen al gráfico de f, entonces $b = c$, es decir, cada elemento de A se relaciona con un único elemento de B.

Una función f de A en B, consecuente con la notación de relaciones, se puede representar como $f = (G_f, A, B)$. Sin embargo, es usual representarla como $\boldsymbol{f\colon A \longmapsto B}$ o como $\boldsymbol{A \xmapsto{f} B}$. Al conjunto de llegada $\boldsymbol{B}$ se le llama **codominio**.

Si (a, b) pertenece al gráfico de f, se dice que b es la **imagen** de a por f y se escribe $\boldsymbol{b = f(a)}$. Análogamente, se dice que a es una **preimagen** de b por f.

En general, se dice que una función $f\colon A \to B$ es de variable en A con valores en B. Si la función es $f\colon \mathbb{R} \to \mathbb{R}$, se dice que es una *función real de variable real*; como ejemplo de estas funciones, es necesario recordar la función lineal y la cuadrática, entre otras. Como ya se mencionó anteriormente, el principal interés no es profundizar en ellas.

Ejemplo 1. *Si $f\colon \mathbb{R} \to \mathbb{R}$ con $f(x) = x^2 + 1$, se tiene que $f(1) = 2$, es decir, 2 es la imagen de 1 por la función f. Además, $f(3) = 10$, con lo cual, 3 es una preimagen de 10 por la función f.* ■

Ejemplo 2. *Si $f\colon \{0, 2, 3, 5\} \to \{1, 2, 3, 4, 5, 6\}$ con $f(x) = x + 1$, se tiene que $f(0) = 1$, es decir, 1 es la imagen de 0 por la función f.*

Además, $f(2) = 3$, $f(3) = 4$, $f(5) = 6$, *con lo cual el gráfico de* f *es*

$$G_f = \big\{(0,1),(2,3),(3,4),(5,6)\big\}$$

Algunos elementos, como el 5 *del conjunto receptor, no tienen preimagen; sin embargo, todos los elementos del conjunto de salida tienen una y solo una imagen, con lo cual* f *sí es una función.* ■

Sea f una función de A en B, si existe un elemento $k \in B$, tal que $\forall x \in A$, se tiene que $f(x) = k$, entonces se dice que f es la **función constante** de valor k.

Ejemplo 3. *Si* $f\colon \{0,2,3,5\} \to \{1,2,3,4,5,6\}$, *la función constante de valor* 3 *tiene como gráfico a* $G_f = \big\{(0,3),(2,3),(3,3),(5,3)\big\}$. ■

Ejemplo 4. *Sea* $E = \{a,b\}$, *si* $f\colon P(E) \to P(E)$, *la función constante de valor* $\varnothing$ *tiene a*

$$G_f = \Big\{\big(\varnothing,\varnothing\big),\big(\{a\},\varnothing\big),\big(\{b\},\varnothing\big),\big(E,\varnothing\big)\Big\}$$

como su gráfico. ■

La función de A en A denotada por ***id***, tal que $id(x) = x$, $\forall x \in A$, se llama **función identidad** de A.

Ejemplo 5. *Si* $f\colon \{0,2,3,5\} \to \{0,2,3,5\}$, *la función identidad sobre este conjunto tiene como gráfico a* $G_f = \big\{(0,0),(2,2),(3,3),(5,5)\big\}$. ■

Sea f una función de A en B. Sea $E \subseteq A$ y $F \subseteq B$, entonces, el conjunto definido por:

$$f[A] = \big\{ b \in B \ / \ \ \exists a \in A \ \ \text{tal que} \ \ b = f(a) \big\}$$

se llama **ámbito** o **imagen** de f. El conjunto definido por:

$$f(E) = \big\{ b \in B \ / \ \ \exists a \in E \ \ \text{tal que} \ \ b = f(a) \big\}$$

se llama la **imagen directa** de E por f. Por último, el conjunto definido por:

$$f^{-1}(F) = \big\{ a \in A \ / \ \ \exists b \in F \ \ \text{tal que} \ \ b = f(a) \big\}$$

se llama la **imagen inversa** de F por f.

Ejemplo 6. *Sea* $A = \{1, 2, 3, 7\}$*; defina la función* $f\colon A \to \mathbb{N}$ *cuyo criterio es* $f(n) = 3n - 2$*. Calcule el ámbito de* f*, el gráfico de* f *y la imagen inversa de* $\{1, 2, 6, 7\}$*.*

Solución. Para calcular el ámbito de f, se evalúa la función en los cuatro elementos del dominio: $f(1) = 1$, $f(2) = 4$, $f(3) = 7$, $f(7) = 19$, con lo cual el ámbito es $f(A) = \{1, 4, 7, 19\}$ y el gráfico de f es $G_f = \big\{(1, 1), (2, 4), (3, 7), (7, 19)\big\}$. Por último, $f^{-1}(\{1, 2, 6, 7\}) = \{1, 3\}$. ■

Ejemplo 7. *Sea* $A = \{1, 2, 3, 5, 12\}$*, defina la función*

$$f\colon P(A) \to \mathbb{N}$$

de manera que $f(\varnothing) = 0$ *y* $f(X)$ *es el mínimo elemento de* X *cuando* $X \neq \varnothing$*. Calcule la imagen directa de* $B = \big\{\{2, 5\}, \{2, 3, 12\}, \{3, 5\}\big\}$ *y la imagen inversa de* $C = \{3, 10\}$*.*

Solución. Como $f(\{2, 5\}) = 2$, $f(\{2, 3, 12\}) = 2$ y además $f(\{3, 5\}) = 3$, se tiene que la imagen directa de B es $f(B) = \{2, 3\}$. Por último, para calcular $f^{-1}(C)$ se deben encontrar todos los subconjuntos de $P(A)$ que tengan como elemento mínimo al 3 o al 10; de esta manera, la imagen inversa de C es $f^{-1}(C) = \big\{\{3\}, \{3,5\}, \{3,12\}, \{3,5,12\}\big\}$. ■

Así como las funciones lineales, cuadráticas y constantes, en el campo de las matemáticas existe gran cantidad de funciones específicas. Para el desarrollo del tema, a continuación se definirán algunas de ellas.

La **función factorial** de n, $f\colon \mathbb{N} \to \mathbb{N}$ denotada por $f(n) = n!$, está definida por

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1$$

y además se define $0! = 1$.

Es importante mencionar que la definición anterior está dada en forma explícita; además, un aspecto muy útil para algunas simplificaciones es que se puede definir de forma recursiva por medio de la igualdad:

$$n! = n \cdot (n-1)! \tag{4.1}$$

Ejemplo 8. *Algunos valores de la función factorial son* $3! = 3 \cdot 2 \cdot 1 = 6$, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$. ■

Ejemplo 9. *La fracción* $\frac{300!}{298!}$ *se simplifica de la siguiente manera:*

$$\frac{300!}{298!} = \frac{300 \cdot 299 \cdot 298!}{298!} = 300 \cdot 299 = 89700$$

■

La función $f\colon \mathbb{R} \to \mathbb{Z}$ definida por $f(x) = n$ donde n es el entero que satisface $n \leq x < n+1$ se llama **función parte entera** o la **función piso**, es decir, la función piso de x corresponde al entero más grande que sea menor o igual a x. Se denota por $\lfloor \boldsymbol{x} \rfloor$.

Ejemplo 10. *Algunos valores de la función piso son* $\lfloor 5 \rfloor = 5$, $\lfloor 7,2 \rfloor = 7$ *y* $\lfloor \pi \rfloor = 3$. ■

De forma análoga se define la **función techo**, que se denota por $\lceil \boldsymbol{x} \rceil$, como el entero más pequeño que sea mayor o igual a x.

Ejemplo 11. *Algunos valores de la función techo son* $\lceil 5 \rceil = 5$, $\lceil \sqrt{5} \rceil = 3$ *y* $\lceil 7,2 \rceil = 8$. ■

El siguiente resultado es muy interesante y relativo al campo de la teoría de los números; relaciona dos de las funciones que se han definido y para su demostración puede consultar [26].

Si $\boldsymbol{E_p(m)}$ denota el **exponente del primo** $\boldsymbol{p}$ en la factorización prima de m, entonces

$$E_p(n!) \quad = \quad \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor + \cdots$$

donde la suma es finita, pues es claro que, a partir de algún s, la potencia p^s será mayor que n y los términos sucesivos serán cero.

Ejemplo 12. *Como la factorización prima de* 486 *es* $2 \cdot 3^5$, *se tiene que* $E_2(486) = 1$; *además,* $E_3(486) = 5$. ■

Ejemplo 13. *Determine el exponente del factor* 3 *en la factorización prima del número* 85!

Solución. Se sabe que el exponente corresponde a $E_3(85!) = \left\lfloor \frac{85}{3} \right\rfloor + \left\lfloor \frac{85}{9} \right\rfloor + \left\lfloor \frac{85}{27} \right\rfloor + \left\lfloor \frac{85}{81} \right\rfloor = 28 + 9 + 3 + 1 = 41$ ■

Ejemplo 14. *Pruebe que los últimos* 20 *dígitos de* 85! *son iguales a* 0.

Solución. Para ver el número de ceros al final de 85!, basta ver cuántas veces es divisible por 10, pero como $10 = 2 \cdot 5$, se calcula:

$$
\begin{aligned}
E_2(85!) &= \left\lfloor \frac{85}{2} \right\rfloor + \left\lfloor \frac{85}{4} \right\rfloor + \left\lfloor \frac{85}{8} \right\rfloor + \left\lfloor \frac{85}{16} \right\rfloor + \left\lfloor \frac{85}{32} \right\rfloor + \left\lfloor \frac{85}{64} \right\rfloor \\
&= 42 + 21 + 10 + 5 + 2 + 1 = 81 \\
E_5(85!) &= \left\lfloor \frac{85}{5} \right\rfloor + \left\lfloor \frac{85}{25} \right\rfloor = 17 + 3 = 20
\end{aligned}
$$

con lo cual los últimos 20 dígitos son ceros. ■

Sea E un conjunto y $A \subseteq E$. La función $\chi_A \colon E \to \{0,1\}$ definida por:

$$
\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}
$$

se llama **función característica** de A.

Ejemplo 15. *Si $E = \{1,2,3,4,5\}$, algunos valores de la función $\chi_{\{2,5\}}$ son $\chi_{\{2,5\}}(1) = 0$ y $\chi_{\{2,5\}}(2) = 1$. El gráfico de esta función es el conjunto $G_{\chi_{\{2,5\}}} = \big\{(1,0),(2,1),(3,0),(4,0),(5,1)\big\}$* ■

Se ha visto que si f es una función de A en B, entonces a cada elemento a A le corresponde uno y solo un elemento $b \in B$; sin embargo, si $b \in B$, puede haber varios elementos $a \in A$ (o quizás ninguno), tal que $b = f(a)$. Con base en estas consideraciones, se hace la siguiente clasificación de las funciones:

Si f es una función de A en B, se dice que f es **inyectiva** o **uno a uno** (abreviado, se escribe 1-1) si y solo si para todo a y b en A se cumple $a \neq b \Rightarrow f(a) \neq f(b)$. Es decir, elementos diferentes de A poseen imágenes diferentes en B.

La definición anterior establece que una función es inyectiva si cada elemento de B tiene, a lo sumo, una preimagen.

Una forma alternativa para probar que f es una función inyectiva es aplicar la contrapositiva a la expresión $a \neq b \Rightarrow f(a) \neq f(b)$ y, con ello, es equivalente probar que f es inyectiva si y solo si para todo a y b en A se cumple

$$f(a) = f(b) \Rightarrow a = b \tag{4.2}$$

Si f es una función de A en B, se dice que f es **sobreyectiva** si y solo si $f(A) = B$. Es decir, f es sobreyectiva si el ámbito y el codominio de f son iguales.

La definición anterior establece que una función es sobreyectiva si cada elemento de B tiene al menos una preimagen.

Además, una forma alternativa para probar que f es una función sobreyectiva es probar que se cumple la proposición:

$$\forall b \in B \; \exists a \in A \; [b = f(a)] \tag{4.3}$$

Si f es una función de A en B, se dice que f es **biyectiva** si y solo si es inyectiva y sobreyectiva.

La definición anterior establece que una función es biyectiva si cada elemento de B tiene exactamente una preimagen.

Ejemplo 16. *Sea* $A = \{-1, 0, 1, 2\}$ *y considere la función* $f\colon A \times A \to \mathbb{Z}$ *definida por* $f((a, b)) = |a - b|$. *Calcule el rango de* f *y determine si* f *es sobreyectiva. Calcule la imagen del conjunto* $\{(1, 2), (2, -1), (2, 1)\}$. *Calcule la imagen inversa del conjunto* $\{2\}$ *y determine si* f *es inyectiva.*

Solución. El dominio está formado por los 16 elementos de $A \times A$; además, después de hacer algunas evaluaciones, se obtiene que el rango de f es $\{0,1,2,3\}$, y como el codominio es $\mathbb{Z}$, la función no es sobreyectiva. Como $f((1,2)) = |1-2| = 1$, $f((2,-1)) = |2-(-1)| = 3$ y $f((2,1)) = |2-1| = 1$, se tiene que:

$$f\big(\{(1,2),(2,-1),(2,1)\}\big) = \{1,3\}$$

Por último, el conjunto $f^{-1}(\{2\})$ representa el conjunto de todas las preimágenes de 2; con ello se tiene que:

$$f^{-1}(\{2\}) = \big\{(0,2),(2,0),(-1,1),(1,-1)\big\}$$

Como el 2 tiene varias preimágenes, f no es inyectiva. ■

Ejemplo 17. *Sean $A = \{1,2,3\}$ y $B = \{a,b,c\}$, y f una función de A en B, cuyo gráfico es $G_f = \big\{(1,a),(2,a),(3,b)\big\}$. El gráfico de la relación inversa f^{-1} es*

$$G_{f^{-1}} = \big\{(a,1),(a,2),(b,3)\big\}$$

y es claro que f^{-1} no es función de B en A, pues el elemento a del conjunto de salida se relaciona con dos elementos diferentes del conjunto de llegada. ■

Ejemplo 18. *Considere la función $f\colon \mathbb{R} \to \mathbb{R}$ cuyo criterio es $f(x) = 5x-4$. Pruebe que f es biyectiva.*

Solución. Primero, utilice (4.2) para probar que f es inyectiva

$$\begin{aligned} f(a) = f(b) \quad &\Rightarrow \quad 5a-4 = 5b-4 \\ &\Rightarrow \quad 5a = 5b \\ &\Rightarrow \quad a = b \end{aligned}$$

En segundo lugar, utilice el resultado (4.3) para demostrar que f es sobreyectiva: sea $b \in B$, es necesario demostrar que existe un elemento

a en $\mathbb{R}$ tal que $b = f(a)$. Se tiene que:

$$\begin{aligned} b = f(a) &\Leftrightarrow b = 5a - 4 \\ &\Leftrightarrow b + 4 = 5a \\ &\Leftrightarrow a = \frac{b+4}{5} \end{aligned}$$

Como este valor de a está definido para cualquier valor real de b, se concluye que $\frac{b+4}{5}$ es la preimagen de b; por lo tanto, f es sobreyectiva.■

Ejemplo 19. *Considere la función* $f\colon \mathbb{R}-\{4\} \to \mathbb{R}-\{5\}$, *cuyo criterio es* $f(x) = \dfrac{5x-2}{x-4}$. *Pruebe que es biyectiva.*

Solución. Primero, utilice el resultado (4.2) para demostrar que f es inyectiva

$$\begin{aligned} f(a) = f(b) &\Rightarrow \frac{5a-2}{a-4} = \frac{5b-2}{b-4} \\ &\Rightarrow (5a-2)(b-4) = (5b-2)(a-4) \\ &\Rightarrow 5ab - 20a - 2b + 8 = 5ab - 20b - 2a + 8 \\ &\Rightarrow -18a = -18b \\ &\Rightarrow a = b \end{aligned}$$

En segundo lugar, utilice el resultado (4.3) para probar que f es sobreyectiva: sea $b \in \mathbb{R} - \{5\}$, es necesario demostrar que existe un elemento a en $\mathbb{R} - \{4\}$ tal que $b = f(a)$. Se tiene que:

$$\begin{aligned} b = f(a) &\Leftrightarrow b = \frac{5a-2}{a-4} \\ &\Leftrightarrow ab - 4b = 5a - 2 \\ &\Leftrightarrow a(b-5) = 4b - 2 \\ &\Leftrightarrow a = \frac{4b-2}{b-5} \end{aligned}$$

con lo cual se obtiene la preimagen de b para todo $b \neq 5$. ■

Ejemplo 20. *Si $f\colon E \to F$ es una función que satisface que $\forall A,\ B \in P(E)$, se cumple que:*

$$f(A \cap B) = f(A) \cap f(B)$$

Pruebe que f es inyectiva.

Solución. Sean $a,\ b \in D_f$ tal que $f(a) = f(b)$, entonces $f(\{a\}) = f(\{b\}) = \{c\}$ por ser f función, por lo que

$$f(\{a\} \cap \{b\}) = f(\{a\}) \cap f(\{b\}) = \{c\} \neq \varnothing$$

es decir, $f(\{a\} \cap \{b\}) \neq \varnothing$, por lo tanto $\{a\} \cap \{b\} \neq \varnothing$, y se concluye que $a = b$. ■

Sea f una función real de variable real, se dice que f es:

1. una función **par** si satisface que $f(-x) = f(x)$ para todo x en su dominio.

2. una función **impar** si cumple que $f(-x) = -f(x)$ para todo x en su dominio.

Ejemplo 21. *Verifique que la función $f(x) = \frac{x^3-2x}{x+4x^5}$ es par.*

Solución. Se calcula

$$f(-x) = \frac{(-x)^3 - 2(-x)}{(-x) + 4(-x)^5} = \frac{-x^3 + 2x}{-x - 4x^5} = \frac{x^3 - 2x}{x + 4x^5} = f(x)$$

Es decir, se ha probado que $f(-x) = f(x)$, y según la definición, corresponde a una función par. ■

Ejercicios (sección 4.1)

1. Sea $A = \{1, 2, 3\}$ y las relaciones $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, y $\mathcal{R}_4$, definidas sobre A, cuyos gráficos respectivos son:

   (a) $G_1 = \big\{(1,1),(2,3)\big\}$
   (b) $G_2 = \big\{(1,2),(2,3),(2,2),(3,3)\big\}$
   (c) $G_3 = \big\{(2,1),(3,1),(1,3)\big\}$
   (d) $G_4 = \big\{(3,1),(2,2),(1,3),(3,3)\big\}$

   Para cada una de estas relaciones, determine si son funciones.

2. Sea $A = \{1, 2, 3, 4, 5\}$ y sea $\mathcal{R}$ una relación definida en A, cuya gráfica H viene dada por $H = \{(1,1),(2,3),(4,2),(5,4),(3,5)\}$. Justifique si $\mathcal{R}$ es una función biyectiva.

3. Determine todas las funciones biyectivas sobre $A = \{1, 2, 3\}$.

4. Determine todas las funciones sobreyectivas de $A = \{1, 2, 3\}$ en $B = \{1, 2\}$.

5. Si $|A| = 4$ y $|B| = 6$, ¿cuántas funciones existen de A en B?, ¿cuántas funciones inyectivas existen de A en B?

6. Sea $A = \{a, b, c\}$ y considere la función $f\colon P(A) \to \{0,1,2,3,4\}$ definida por $f(B) = |B|$.

   (a) Determine $f(\{a, c\})$ y $f\big(\big\{\{a\},\{a,b\},\{b\}\big\}\big)$
   (b) Determine $f^{-1}\big(\{2,4\}\big)$
   (c) Determine si f es inyectiva o sobreyectiva.

7. Para $A = \{0, 1, 2, 3, 4, 5, 6\}$ y la función $f\colon A \to A$ definida por:

$$f(a) = \begin{cases} a-3 & \text{si } a \geq 4 \\ a+3 & \text{si } a < 4 \end{cases}$$

(a) Determine si f es inyectiva y si f es sobreyectiva.

(b) Calcule $f\big(\{0,3,6\}\big)$

(c) Calcule $f^{-1}\big(\{0\}\big) \cup f^{-1}\big(f\big(\{6\}\big)\big)$

8. Sea $A = \{1,2,3\}$, $B = \{1,2,3,4\}$ y $f\colon A \times A \to B$ definida por

$$f((a,b)) = \begin{cases} 1 & \text{si } a < b \\ 3 & \text{si } a > b \\ 4 & \text{si } a = b \end{cases}$$

(a) Determine si f es inyectiva y si f es sobreyectiva.

(b) Determine $f^{-1}\big(\{2\}\big)$, $f^{-1}\big(\{3\}\big)$

9. Sea $A = \{2,3,5\}$ y $B = \{1,2,3,4\}$, considere la función

$$f\colon A \times B \to \{1,2,3,4,5,6\}$$

definida por

$$f((a,b)) = \begin{cases} 2a & \text{si } a < b \\ b & \text{si } a > b \\ a+b & \text{si } a = b \end{cases}$$

(a) Determine si f es inyectiva y si f es sobreyectiva.

(b) Calcule $f^{-1}\big(\{1,3,5\}\big)$, $f\big(f^{-1}\big(\{5\}\big)\big)$, $f\big(f^{-1}\big(\{4,5\}\big)\big)$

(c) Si $C = \big\{(a,b) \in A \times B \ \ / \ \ a+b = 6\big\}$, calcule $f^{-1}(f(C))$

(d) Calcule $f\Big(\big(f(3,2), f\big(\big(f(3,2), f(3,2)\big)\big)\big)\Big)$

10. Sea $A = \{3,4,5,6\}$ y $B = \{1,2,3\}$, considere la función

$$f\colon A \times B \to [1,6]$$

definida por $f((a,b)) = \dfrac{a}{b}$

(a) Determine si f es inyectiva.

(b) Determine la cardinalidad del ámbito de f.

(c) Determine si f es sobreyectiva.

(d) Calcule $f\big(C\big)$, donde $C = \{(a, b) \in A \times B \quad \text{tal que} \quad a+b = 6\}$

(e) Calcule $f^{-1}\big(\{2, 3\}\big)$

11. Pruebe que los últimos diez dígitos del número 45! son iguales a 0.

12. Calcule el valor de las siguientes expresiones:

(a) $7! + 6!$

(b) $\dfrac{100! - 99!}{98!}$

(c) $\dfrac{100! \cdot 101!}{(5 \cdot 6 \cdot 7 \cdot \cdots \cdot 98 \cdot 99 \cdot 100)^2}$

13. Calcule el exponente del 2 en la factorización prima de 75!.

14. Se dice que p es un **punto fijo** de la función f si satisface que $f(p) = p$. Determine los puntos fijos de las siguientes funciones:

(a) $f(x) = x^2 - 2x - 4$

(b) $f(x) = \dfrac{x^3 - 3x + 4}{x + 1}$

15. Verifique que $g(x) = x^2 - \dfrac{x}{x+1} + \dfrac{x}{1-x}$ es una función par.

16. Verifique que $g(x) = 2x + \dfrac{1}{x+1} - \dfrac{1}{1-x}$ es una función impar.

17. Si los dominios de las funciones están definidos adecuadamente, pruebe que:

(a) Si f es impar, entonces $f(0) = 0$.

(b) El producto de dos funciones impares es una función par.

(c) El producto de una función par y una impar es impar.

(d) Si f es impar y g par, entonces $g \circ f$ es par y $f \circ g$ es impar.

(e) Si f y g son impares, entonces $g \circ f$ es impar y $f + g$ es impar.

18. Encuentre una función que sea, a la vez, par e impar.

19. Encuentre una función que no sea par y que no sea impar.

20. Considere la función $f\colon \mathbb{R} \to \mathbb{R}$ definida por

$$f(x) = \begin{cases} x+1 & \text{si } x < 2 \\ 3 & \text{si } x \geq 2 \end{cases}$$

    (a) Represente el gráfico de f en el sistema cartesiano y calcule las imágenes de 1, 2, 3 y las preimágenes de 1, 2, 3.
    (b) Determine el dominio, el codominio y el ámbito de f.
    (c) Determine si f es inyectiva y si es sobreyectiva.
    (d) Calcule $f([0,4])$, es decir, la imagen directa de $[0,4]$.
    (e) Calcule $f^{-1}([0,4])$, es decir, la imagen inversa de $[0,4]$.

21. Considere la función $f = (G, \mathbb{R} - \{-1\}, \mathbb{R})$ definida por:

$$f(x) = \begin{cases} 2x+1 & \text{si } x < -1 \\ 3 & \text{si } -1 < x < 1 \\ -x+2 & \text{si } x \geq 1 \end{cases}$$

    (a) Represente el gráfico de f en el sistema cartesiano y calcule las imágenes de -2, 0, 3 y las preimágenes de -2 y de 1.
    (b) Encuentre el dominio, el codominio y el ámbito de f.
    (c) Determine si es inyectiva y si es sobreyectiva.

22. Considere la función $f(x)$ definida por:

$$f(x) = \begin{cases} -x^2 - 2x + 3 & \text{si } x < 0 \\ 3 & \text{si } 0 \leq x < 2 \\ x+1 & \text{si } x \geq 2 \end{cases}$$

    (a) Calcule $f\left(\left[\frac{1}{2}, 1\right[\right)$, es decir, la imagen directa de $\left[\frac{1}{2}, 1\right[$.

(b) Calcule $f^{-1}\left([0,3[\right)$, es decir, la imagen inversa de $[0,3[$.

(c) Calcule las imágenes de -2, 1, 3 y las preimágenes de -5 y 3.

23. Sean A y B subconjuntos de E

(a) Determine $\chi_{\varnothing}$ y χ_E.

(b) Pruebe que $\chi_{\overline{A}}(x) = 1 - \chi_A(x)$ para todo $x \in E$.

(c) Pruebe que $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$ para todo $x \in E$.

(d) Pruebe que $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$ para todo $x \in E$.

(e) Pruebe que $\chi_{A-B}(x) = \chi_A(x) - \chi_{A\cap B}(x)$ para todo $x \in E$.

(f) Encuentre una fórmula para $\chi_{A\triangle B}(x)$.

24. Sean A y B conjuntos no vacíos; suponga que f es una función de A en B y sean $D \subseteq A$, $E \subseteq A$. Demuestre que:

(a) $f(D \cup E) \subseteq f(D) \cup f(E)$.

(b) $f(D \cap E) \subseteq f(D) \cap f(E)$.

(c) Si f es inyectiva, entonces $f(D \cap E) = f(D) \cap f(E)$.

(d) $f(D) - f(E) \subseteq f(D - E)$.

(e) Si f es inyectiva, pruebe que $f(D) - f(E) = f(D - E)$.

4.2 Funciones lineal y cuadrática

La función lineal permite, a partir de la imagen de dos elementos del dominio, encontrar el criterio que define la función.

Sea $D \subseteq \mathbb{R}$, se dice que la función $f\colon D \longmapsto \mathbb{R}$ es una **función lineal** si existen $m, b \in \mathbb{R}$ tal que:

$$f(x) = mx + b$$

El valor de $\boldsymbol{m}$ se llama **pendiente**. Si los pares ordenados (x_1, y_1) y (x_2, y_2) pertenecen al gáfico de la función lineal, su pendiente es:

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Ejemplo 22. *Si una función lineal satisface que $f(7) = 9$ y $f(13) = 33$, determine el criterio general $f(x)$ para cualquier $x \in \mathbb{R}$.*

Solución. Se tiene que $m = \frac{f(13)-f(7)}{13-7} = 4$. Al reemplazar el par ordenado $(7, 9)$ en la fórmula $b = f(x) - mx$, se obtiene:

$$b = 9 - 4 \cdot 7 = -19$$

Por lo tanto, $f(x) = 4x - 19$. ■

Ejemplo 23. *La siguiente tabla indica dos valores, el de congelación y de ebullición normal del agua en las escalas de temperatura Fahrenheit (F) y Celsius (C).*

Agua	C	F
congelación	0	32
ebullición	100	212

Con estos datos, exprese F como una función lineal de C.

Solución. Suponiendo que F y C están relacionadas linealmente, se toman dos valores para F y C respectivamente en la tabla; por ejemplo, $F_1 = 32$ y $F_2 = 212$, $C_1 = 0$ y $C_2 = 100$, los cuales corresponden a los valores de C para los F escogidos. De esta manera:

$$\begin{aligned} m &= \frac{F_2 - F_1}{C_2 - C_1} \\ &= \frac{212 - 32}{100 - 0} = \frac{180}{100} = 1,8 \end{aligned}$$

Con ello se puede afirmar que $F(C) = 1,8C + b$. Note que el valor de b se puede determinar sustituyendo los valores correspondientes:

$$b = F_2 - mC_2 = 212 - 1,8 \cdot 100 = 32$$

Por lo tanto,

$$F(C) = 1,8C + 32$$

es la función que expresa a F en función de C. ■

Sea $f\colon \mathbb{R} \longmapsto \mathbb{R}$ una función, se dice que f es una **función cuadrática** si existen constantes a, b y $c \in \mathbb{R}$ con $a \neq 0$ y

$$f(x) = ax^2 + bx + c$$

La gráfica de una función cuadrática es una curva llamada **parábola**, cuya forma es como la gráfica dada en la figura 4.1.

El **eje de simetría** de la gráfica de una función cuadrática lo representa la recta $x = \frac{-b}{2a}$; ésta es importante cuando se grafican funciones cuadráticas, pues cualquier punto de la gráfica a la derecha de esta recta tiene un punto simétrico a la izquierda. Por eso solo basta con tomar valores de $x > \frac{-b}{2a}$ o $x < \frac{-b}{2a}$.

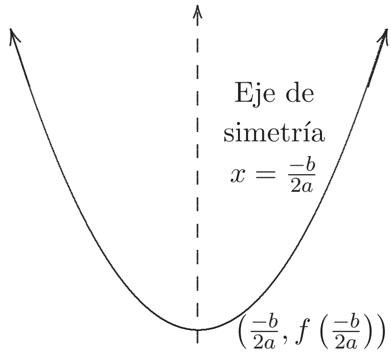


Figura 4.1: Parábola.

El **vértice** (V) de la parábola estará en el punto de coordenadas

$$\begin{aligned} V &= \left(\frac{-b}{2a}, f\left(\frac{-b}{2a}\right)\right) \\ &= \left(\frac{-b}{2a}, \frac{-\Delta}{4a}\right) \end{aligned}$$

donde $\Delta = b^2 - 4ac$ se conoce como **discriminante**.

Ejemplo 24. *Determine el vértice y las intersecciones con los ejes de coordenadas de la gráfica de la función $f(x) = x^2 - x - 2$.*

Solución. Se tiene $a = 1$, $b = -1$ y $c = -2$. En este caso, $\frac{-b}{2a} = \frac{1}{2}$ y

$$\begin{aligned} \frac{-\Delta}{4a} &= -\frac{b^2 - 4ac}{4a} \\ &= -\frac{(-1)^2 - 4(1)(-2)}{4 \cdot 3} \\ &= -\frac{3}{4} \end{aligned}$$

Entonces, el vértice está en el punto $(\frac{1}{2}, -\frac{3}{4})$. Además, se sabe que interseca al eje y en el punto $(0, -2)$ y los puntos de intersección con el eje x se encuentran al resolver la ecuación cuadrática $x^2 - x - 2 = 0$. Así, los puntos de intersección con el eje x son $(-1, 0)$ y $(2, 0)$. ■

Ejemplo 25. *Grafique* $f(x) = x^2 - 5x - 6$.

Solución. En este ejemplo, $a = 1$, $b = -5$ y $c = -6$. Se nota que $a > 0$, por lo que es cóncava hacia arriba. El eje de simetría está dado por la ecuación $x = \frac{5}{2}$. Es creciente en $\left[\frac{5}{2}, +\infty\right[$ y decreciente en $\left]-\infty, \frac{5}{2}\right]$. Las intersecciones con el eje x se encuentran al resolver la ecuación $f(x) = 0$, es decir:

$$x^2 - 5x - 6 = 0$$

cuyas soluciones son:

$$x = 6 \text{ o } x = -1.$$

Interseca al eje y en $y = f(0) = -6$. El vértice, que en este ejemplo es un punto mínimo, tiene coordenadas $\left(\frac{-b}{2a}, \frac{-\Delta}{4a}\right) = \left(\frac{5}{2}, \frac{-49}{4}\right)$. De esta forma, los puntos encontrados son:

x	-1	0	$2,5$	6
y	0	-6	$-12,25$	0

Se colocan estos puntos en un sistema de coordenadas y se traza la parábola (véase figura 4.2). ■

Ejemplo 26. *En forma análoga, considere la función* $g\colon \mathbb{R} \to \mathbb{R}$ *definida por:*

$$g(x) = \begin{cases} x^2 - 1 & si \quad x < -1 \\ 2x - 1 & si \quad -1 \leq x < 3 \\ 2 & si \quad x \geq 3 \end{cases}$$

Se tiene que $g(2) = 3$, *es decir,* 3 *es la imagen de* 2 *por* g*; a su vez,* 2 *es una preimagen de* 3 *por* g. *Además,* $g(4) = 2$, *es decir,* 2 *es la imagen de* 4 *y, a su vez,* 4 *es una preimagen de* 2. *Análogamente, se tiene* $g(-2) = 3$. ■

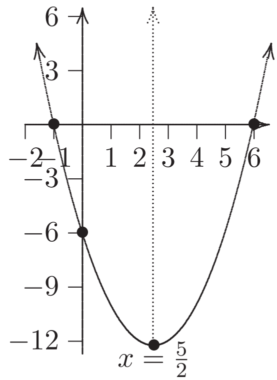


Figura 4.2: Gráfica de $f(x) = x^2 - 5x - 6$.

Ejemplo 27. *Determine la función cuadrática con vértice en* $(-1, 4)$ *y que pasa por* $(2, -5)$.

Solución. Se busca $f(x) = ax^2 + bx + c$ con $a \neq 0$. Dado que $(-1, 4)$ es el vértice y las coordenadas de este siempre son $\left(\frac{-b}{2a}; \frac{-\Delta}{4a}\right)$, se debe tener:

$$\begin{aligned} \frac{-b}{2a} &= -1 \\ \frac{-\Delta}{4a} = \frac{-(b^2 - 4ac)}{4a} &= 4 \end{aligned}$$

De la primera ecuación se encuentra que $b = 2a$, y al sustituir esto en la segunda ecuación se tiene que:

$$\frac{-\left((2a)^2 - 4ac\right)}{4a} = 4$$

Note que el discriminante $(2a)^2 - 4ac = 4a^2 - 4ac = 4a(a - c)$. Con esto, la fracción anterior es: $\frac{-4a(a-c)}{4a} = 4$ y se simplifica en: $-a + c = 4$, obteniendo de esta que $c = 4 + a$. Así, hasta este momento, $f(x) = ax^2 + 2ax + 4 + a$. Por último, como $f(2) = -5$, se tiene:

$$f(2) = a \cdot 2^2 + 2a \cdot 2 + 4 + a = 4a + 4a + 4 + a = -5$$

que es equivalente a $9a = -9$, o bien, $a = -1$. Por lo tanto, $f(x) = -x^2 - 2x + 3$. ■

Ejercicios (sección 4.2)

1. Determine la función lineal f, de manera que $f(2) = -5$ y que $f(-1) = 6$.

2. Sea la función $f\colon \mathbb{R} \to \mathbb{R}$, cuyo criterio es $f(x) = -\frac{x}{2} + \frac{5}{2}$. Calcule $f\big([2,5[\big)$ y calcule $f^{-1}\big([2,5[\big)$.

3. En la entrada a la ciudad de Cartago hay un parque con una escultura en forma de arco parabólico cóncavo hacia abajo. Sobre el suelo, la distancia entre los extremos es de 12 m; la altura del monumento a 1 m de uno de los extremos es de $1,5$ m. ¿Cuál es la altura máxima de este monumento?

4. Determine la función cuadrática tal que $f(3) = 0$, $f(-5) = 0$ y $f(-1) = 12$.

5. Determine la función cuadrática cuyo gráfico tiene vértice en el punto $(3,-9)$ y pasa por el punto $(-2,0)$.

6. Determine la ecuación de la recta que es perpendicular a la recta con ecuación $3x + 2y = 5$, y pasa por el vértice de la parábola $y = 3x^2 - 5x + 1$.

7. Determine el criterio de la función cuadrática cuya gráfica tiene como vértice a $(3,15)$ y pasa por el punto $(-1,-17)$.

8. Calcule la distancia del punto $(2,3)$ a la mediatriz del segmento que une a los puntos de intersección de las gráficas de las funciones f y g, con $f(x) = x^2 + x + 1$ y $g(x) = -2x + 5$.

4.3 Operaciones con funciones

En esta sección se definen las operaciones básicas con funciones. La composición será la que permitirá definir las funciones inversas; además, se desarrollarán algunos ejemplos soble el concepto del dominio máximo y su respectivo cálculo. De la misma manera en que se definió la composición de relaciones como un caso particular de ellas, se definirá la composición de las funciones.

Dadas dos funciones $f\colon A \to B$ y $g\colon B \to C$, se define la **composición de las funciones** f y g como la nueva función $\boldsymbol{g \circ f\colon A \to C}$, que cumple:

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

Ejemplo 28. *Sea* $f\colon \mathbb{R} \to \mathbb{R}$ *cuyo criterio es* $f(x) = 5x - 4$*. Determine el criterio* $(f \circ f)(x)$*.*

Solución. Basta calcular:

$$(f \circ f)(x) = f(f(x)) = f(5x - 4) = 5(5x - 4) - 4 = 25x - 24$$

Así, el criterio es $(f \circ f)(x) = 25x - 24$. ■

Ejemplo 29. *Para las funciones* f*,* g*, con criterio* $f(x) = 3x - 4$*,* $g(x) = 2x + 5$*, calcule el criterio de las funciones* $f \circ g$*,* $g \circ f$*, es decir, calcule* $(f \circ g)(x)$ *y* $(g \circ f)(x)$*.*

Solución. Se debe tener en cuenta cuál es la función que se evalúa primero, así:

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) = f(2x + 5) = 3(2x + 5) - 4 = 6x + 11\\ (g \circ f)(x) &= g(f(x)) = g(3x - 4) = 2(3x - 4) + 5 = 6x - 3\end{aligned}$$

■

Ejemplo 30. *Sea* $f(x) = 5 - \frac{1}{x-4}$. *Pruebe que* $(f \circ f \circ f)(x) = x$. *Además, determine el dominio de* f *y el dominio de* $f \circ f \circ f$.

Solución. Es claro que el dominio de f es $\mathbb{R} - \{4\}$; se calcula ahora:

$$\begin{aligned}
f(f(f(x))) &= f\left(f\left(5 - \frac{1}{x-4}\right)\right) \\
&= f\left(5 - \frac{1}{\left(5 - \frac{1}{x-4}\right) - 4}\right) \\
&= f\left(5 - \frac{x-4}{x-5}\right) \\
&= f\left(\frac{4x-21}{x-5}\right) \\
&= 5 - \frac{1}{\left(\frac{4x-21}{x-5}\right) - 4} \\
&= 5 - \frac{x-5}{4x-21-4x+20} \\
&= 5 + x - 5 \\
&= x
\end{aligned}$$

Por último, para el dominio de $f \circ f \circ f$ se deben excluir los valores que indefinen los pasos del cálculo anterior. Así, el dominio de $f \circ f \circ f$ es $\mathbb{R} - \{4, 5\}$. ■

Ejemplo 31. *Considere las funciones* g *definida por* $g(x) = -x + 5$ *y* f *definida por:*

$$f(x) = \begin{cases} 2x+1 & \text{si } x \geq 2 \\ -3x-1 & \text{si } x < 2 \end{cases}$$

Determine el criterio de $(f \circ g)(x)$.

Solución. Para evaluar $f(g(x))$ se deben determinar los valores de x para los que $g(x) \geq 2$ y cuáles cumplen con $g(x) < 2$, pues dependiendo

de este dato se puede aplicar f. Así, $-x+5 \geq 2$ para $x \leq 3$ y, en este caso, $f(g(x)) = f(-x+5) = 2(-x+5)+1 = -2x+11$. Por otro lado, $-x+5 < 2$ para $x > 3$, en cuyo caso, $f(g(x)) = f(-x+5) = -3(-x+5)-1 = 3x-16$ y finalmente, el criterio de la composición es:
$(f \circ g)(x) = \begin{cases} -2x+11 & \text{si } x \leq 3 \\ 3x-16 & \text{si } x > 3 \end{cases}$ ■

En el caso particular de las funciones reales de variable real, se puede multiplicar por un escalar sumar, restar, multiplicar o dividir. Para ello se utilizan las propiedades de las expresiones algebraicas que las constituyen, es decir, la definición de las cinco operaciones básicas de funciones es:

Dadas dos funciones, $f\colon A \to D$ y $g\colon B \to C$, con A, B, C, D subconjuntos de $\mathbb{R}$, se define:

$$\begin{aligned} (cf)(x) &= cf(x) \\ (f+g)(x) &= f(x)+g(x) \\ (f-g)(x) &= f(x)-g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x) \\ \left(\frac{f}{g}\right)(x) &= \frac{f(x)}{g(x)} \quad \text{siempre que } g(x) \neq 0 \end{aligned}$$

En la definición anterior de las últimas cuatro operaciones básicas con funciones, el dominio de la función resultante es la intersección de los dominios de cada función involucrada, es decir, $A \cap B$. En la división de funciones, de esta intersección de los dominios se deben eliminar los valores que anulan a la función g, para así evitar la indefinición de la fracción.

Ejemplo 32. *Considere las funciones $f(x) = 2x+1$, $g(x) = x-1$. Determine el criterio de las funciones $f+g$, $f-g$, $f \cdot g$, $\frac{f}{g}$, $f \circ g$, $g \circ f$.*

Solución. El criterio de la función suma de f y g es:

$$(f+g)(x) = (2x+1) + (x-1) = 3x$$

El criterio de la resta es $(f-g)(x) = (2x+1) - (x-1) = x-2$; el del producto es:

$$(f \cdot g)(x) = (2x+1)(x-1) = 2x^2 - x - 1$$

El criterio del cociente es $\left(\frac{f}{g}\right)(x) = \frac{2x+1}{x-1}$; el criterio de la composición de f y g es:

$$(f \circ g)(x) = 2(x-1) + 1 = 2x - 1$$

Por último, $(g \circ f)(x) = (2x+1) - 1 = 2x$. ■

Ejemplo 33. *Determine el dominio máximo de* $f(x) = \frac{x+2}{x-5}$.

Solución. Al ser una fracción racional, se deben eliminar del conjunto de los números reales solamente los valores donde el denominador se anula, es decir, solamente $x = 5$. Así, el dominio máximo de f es $\mathbb{R} - \{5\}$. ■

Ejemplo 34. *Determine el dominio máximo de* $f(x) = \sqrt{x-5}$.

Solución. Al ser un radical de índice par, se deben eliminar del conjunto de los números reales todos los valores donde el radicando es negativo, es decir, el dominio debe incluir solamente los valores de x que satisfacen que $x \geq 5$. Así, el dominio máximo de f es el intervalo $[5, +\infty[$. ■

Ejemplo 35. *Determine el dominio máximo de* $f(x) = \sqrt{\frac{4x+13}{(x+5)(2-x)}}$

Solución. Se debe resolver la inecuación:

$$\frac{4x+13}{(x+5)(2-x)} \geq 0$$

Los valores que anulan los tres factores son $x = -\frac{13}{4}$, $x = -5$ y $x = 2$, ordenados de menor a mayor. Se observa que $-5 < -\frac{13}{4} < 2$.

	$]-\infty,-5[$	$]-5,-\frac{13}{4}[$	$]-\frac{13}{4},2[$	$]2,+\infty[$
signo de $4x+13$	$-$	$-$	$+$	$+$
signo de $x+5$	$-$	$+$	$+$	$+$
signo de $2-x$	$+$	$+$	$+$	$-$
signo resultante	$+$	$-$	$+$	$-$

En este caso, se deben escoger los intervalos donde el signo resultante es positivo; como la inecuación permite que sea cero, se incluye el $-\frac{13}{4}$, mientras que los extremos -5 y 2 no se deben incluir, pues originan una división por cero (esto se indica en la tabla con doble línea vertical). Así, se obtiene que la solución de la inecuación, es decir, el dominio máximo de la función f, es $D =]-\infty,-5[\cup \left[-\frac{13}{4},2\right[$. ■

Ejercicios (sección 4.3)

1. Considere las funciones $f(x) = 3x+2$ y $g(x) = 1-2x$. Calcule los criterios $(f \circ g)(x)$, $(g \circ f)(x)$ y $(g \circ g)(x)$.

2. Encuentre las funciones lineales f tales que $(f \circ f)(x) = 4x+1$.

3. Encuentre las funciones lineales f tales que $(f \circ f \circ f)(x) = -8x+5$.

4. Sea $f(x) = 7 + \frac{1}{6-x}$. Pruebe que $(f \circ f \circ f)(x) = x$. Además, determine el dominio de f y el dominio de $f \circ f \circ f$.

5. Considere la función $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ con criterio $f(x) = 8x^3 - 5$. Además, sea $g\colon \mathbb{R} \longrightarrow \mathbb{R}$ otra función que cumple $(f \circ g)(x) = 35 - 8x$. Determine el criterio $g(x)$.

6. Sea f una función de $\mathbb{R}$ en $\mathbb{R}$, que satisface $f(x+1) = x^2 - 3x + 2$. Determine el criterio de $f(x)$.

7. Sea $f\colon \mathbb{R} \to \mathbb{R}$ una función biyectiva. Además, sea $g\colon \mathbb{R} \to \mathbb{R}$ una función tal que $g(x) = 2f(x) + 3$. Pruebe que g es biyectiva.

8. Considere las funciones reales de variable real f, g, h, i, con criterios $f(x) = \sqrt{x}$, $g(x) = x + 3$, $h(x) = 4 - x$, $i(x) = \sqrt[4]{x}$. Calcule los siguientes criterios de las respectivas funciones y su dominio:

   (a) $[f \circ (h - g)]\,(x)$

   (b) $\left(\dfrac{f}{g \cdot h}\right)(x)$

   (c) $(f \circ g - i \circ h)\,(x)$

9. Para cada caso, determine dos funciones f y g, diferentes de la función identidad, de manera que se cumpla que $h(x) = (f \circ g)(x)$:

   (a) $h(x) = (2x + 3)^4$, y que g no sea una función lineal.

   (b) $h(x) = 4x^4 + 4x^2 + 1$

   (c) $h(x) = \sqrt{x^2 + 4x + 5} + x + 5$

   (d) $h(x) = \dfrac{x + 3}{x^2 + 2x} - 2x + 4$

10. Calcule el dominio máximo de las funciones reales de variable real:

    (a) $f(x) = \dfrac{2x}{x^2 + 3x - 4} + \sqrt{2 - x}$

    (b) $f(x) = \sqrt{4 - x} + \sqrt{x - 1}$

    (c) $f(x) = \sqrt{\dfrac{x + 1}{(x + 2)(3 - x)}}$

    (d) $f(x) = \sqrt{x(x - 2)} + \sqrt{9 - x^2}$

11. Considere la función f definida por:

$$f(x) = \begin{cases} 2x - 3 & \text{si } x \geq 2 \\ -x + 2 & \text{si } x < 2 \end{cases}$$

    y la función g definida por $g(x) = x^2 + x + 2$. Determine el criterio de $(f + g)(x)$ y el criterio de $(f \circ g)(x)$.

12. Considere la función f definida por:

$$f(x) = \begin{cases} 2x+1 & \text{si } x \leq 1 \\ 1-2x & \text{si } x > 1 \end{cases}$$

y la función g definida por:

$$g(x) = \begin{cases} -x+2 & \text{si } x \leq 3 \\ x-5 & \text{si } x > 3 \end{cases}$$

Determine el criterio de $(f+g)(x)$ y el criterio de $(f \circ g)(x)$.

13. Sea $f\colon \mathbb{R} - \{\frac{1}{2}\} \to \mathbb{R}$ una función con criterio $f(x) = \frac{5}{2x-1}$ y $g\colon \mathbb{R} \to \mathbb{R} - \{\frac{1}{2}\}$ otra función. Si g es inyectiva, pruebe que $f \circ g$ es inyectiva.

14. Sean A, B y C conjuntos no vacíos; suponga que f y g son funciones tales que $f\colon A \to B$ y $g\colon B \to C$. Pruebe que si f y g son biyectivas, entonces $g \circ f$ es biyectiva.

15. Sean A, B y C conjuntos no vacíos, y las funciones $f\colon A \to B$, $f'\colon A \to B$, $g\colon B \to C$, y $g'\colon B \to C$. Pruebe que:

    (a) Si $g \circ f$ es inyectiva, entonces f inyectiva.

    (b) Si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.

    (c) Si $g \circ f$ es inyectiva y f sobreyectiva, entonces g es inyectiva.

    (d) Si $g \circ f$ es sobreyectiva y g es $1-1$, entonces f es sobreyectiva.

    (e) Si g es inyectiva y $g \circ f = g \circ f'$, entonces $f = f'$.

    (f) Si f es sobreyectiva y $g \circ f = g' \circ f$, entonces $g = g'$.

4.4 Funciones inversas

En el capítulo 3 se observó que a toda relación $\mathcal{R}$ se le puede definir su relación inversa $\mathcal{R}^{-1}$, ambas serán relaciones; sin embargo, para el caso de una función f vista como relación, su inversa como relación no necesariamente será una función. La condición para que esto sea verdadero se indica en la siguiente definición.

> Si f es una función de A en B, se dice que f es **invertible** o que f tiene **función inversa** si y solo si su relación inversa f^{-1} también es función. Además, esto sucederá si y solo si f es biyectiva.

Ejemplo 36. *Como la función identidad de un conjunto sobre sí mismo es una biyección, se tiene que esta función es invertible.* ■

Ejemplo 37. *Sea $f\colon \mathbb{R} \to \mathbb{R}$ cuyo criterio es $f(x) = 5x - 4$. Pruebe que f es invertible. Además, determine el criterio de $f^{-1}(x)$ y calcule $(f^{-1} \circ f)(x)$.*

Solución. En el ejemplo 18 se probó que f es biyectiva; por lo tanto, es invertible. Por otro lado, para encontrar el criterio de $f^{-1}(x)$, se despeja x del criterio de f:

$$\begin{aligned} y = f(x) \quad &\Leftrightarrow \quad y = 5x - 4 \\ &\Leftrightarrow \quad y + 4 = 5x \\ &\Leftrightarrow \quad \frac{y+4}{5} = x \end{aligned}$$

de donde $f^{-1}(x) = \frac{x+4}{5}$. Por último,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(5x-4) = \frac{(5x-4)+4}{5} = \frac{5x}{5} = x$$

de donde $(f^{-1} \circ f)(x) = x$. ■

Ejemplo 38. *Si* $f(x) = 2x - 2$ *y* $g(x) = 2x + 1$, *calcule* $(g \circ f \circ f)^{-1}(x)$.

Solución. En primer lugar, se calcula $(g \circ f \circ f)(x)$:

$$\begin{aligned}(g \circ f \circ f)(x) = g\Big(f\big(f(x)\big)\Big) =& g\big(f(2x-2)\big)\\ =& g\big(2(2x-2)-2\big)\\ =& g(4x-6) = 2(4x-6)+1\\ =& 8x-11\end{aligned}$$

por lo que $(g \circ f \circ f)^{-1}(x) = \dfrac{x+11}{8}$. ■

Ejemplo 39. *Considere* $f\colon \mathbb{R} - \{2\} \to B$ *con* $B \subseteq \mathbb{R}$, *cuyo criterio es* $f(x) = \frac{3x+1}{x-2}$. *Determine el conjunto* B *de manera que* f *sea biyectiva; pruebe que es biyectiva. Además, determine el criterio de* $f^{-1}(x)$ *y calcule* $(f^{-1} \circ f)(x)$.

Solución. Primero se utiliza el resultado (4.2) para probar que f es inyectiva:

$$\begin{aligned}f(a) = f(b) \quad &\Rightarrow \quad \frac{3a+1}{a-2} = \frac{3b+1}{b-2}\\ &\Rightarrow \quad (3a+1)(b-2) = (3b+1)(a-2)\\ &\Rightarrow \quad 3ab - 6a + b - 2 = 3ab - 6b + a - 2\\ &\Rightarrow \quad -7a = -7b\\ &\Rightarrow \quad a = b\end{aligned}$$

En segundo lugar, se aplica el resultado (4.3) para probar que f es sobreyectiva. Sea $b \in B$, es necesario demostrar que existe un elemento a en $\mathbb{R} - \{2\}$ tal que $b = f(a)$. Así:

$$\begin{aligned}b = f(a) \quad &\Leftrightarrow \quad b = \frac{3a+1}{a-2}\\ &\Leftrightarrow \quad ab - 2b = 3a + 1\\ &\Leftrightarrow \quad a(b-3) = 2b + 1\\ &\Leftrightarrow \quad a = \frac{2b+1}{b-3}\end{aligned}$$

Con lo anterior se obtiene la preimagen de b, siempre que se escoja $B = \mathbb{R} - \{3\}$, para evitar la división por cero. Por otro lado, para encontrar el criterio de $f^{-1}(x)$, se despeja x del criterio de f:

$$\begin{aligned} y = f(x) \quad &\Leftrightarrow \quad y = \frac{3x+1}{x-2} \\ &\Leftrightarrow \quad xy - 2y = 3x + 1 \\ &\Leftrightarrow \quad x(y-3) = 2y + 1 \\ &\Leftrightarrow \quad x = \frac{2y+1}{y-3} \end{aligned}$$

De donde $f^{-1}(x) = \dfrac{2x+1}{x-3}$. Por último, hay que calcular $(f^{-1} \circ f)(x)$:

$$\begin{aligned} f^{-1}(f(x)) &= f^{-1}\left(\frac{3x+1}{x-2}\right) \\ &= \frac{2\left(\frac{3x+1}{x-2}\right) + 1}{\frac{3x+1}{x-2} - 3} \\ &= \frac{\frac{6x+2+x-2}{x-2}}{\frac{3x+1-3x+6}{x-2}} \\ &= \frac{7x}{7} = x \end{aligned}$$

El resultado era de esperar, pues la composición de una función con su inversa es la función identidad. ■

Ejemplo 40. *Sea $f\colon D \longmapsto A_f$ tal que $f(x) = 3x^2 - x - 2$. Determine el dominio máximo D para que f sea una función estrictamente creciente y determine f^{-1}.*

Solución. Para determinar la función inversa de f se necesita que la función sea biyectiva. Este ejemplo enfatiza la necesidad de buscar un dominio y codominio adecuados. Se sabe que el ámbito de una función cuadrática con $a > 0$ es $A_f = \left[\frac{-\Delta}{4a}; +\infty\right[$. En el caso del ejemplo,

$A_f = \left[-\frac{25}{12}; +\infty\right[$. Además, f es estrictamente creciente si $x \in \left[\frac{1}{6}; +\infty\right[$, de manera que, al tomar este intervalo como el dominio, se tiene la biyectividad. Recuerde que para calcular la inversa se escribe $f(x) = y$ y se expresa x en función de y. Se hará uso de la fórmula general para ecuaciones cuadráticas a fin de despejar el valor de x en la ecuación $3x^2 - x - 2 = y$; si se pasa a restar el valor de y se tiene:

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

Y usando la fórmula general con $a = 3$, $b = -1$ y $c = -2 - y$, se obtiene:

$$x = \frac{1 \pm \sqrt{(-1)^2 - 4(3)(-2 - y)}}{2 \cdot 3}$$

Es decir, $x = \frac{1+\sqrt{25+12y}}{6}$ o $x = \frac{1-\sqrt{25+12y}}{6}$. Como se sabe que $x \geq \frac{1}{6}$ pues $x \in D$, entonces la única expresión que determina valores mayores que $\frac{1}{6}$ es $x = \frac{1+\sqrt{25+12y}}{6}$. Por lo tanto:

$$f^{-1}(x) = \frac{1 + \sqrt{25 + 12x}}{6}$$

Recuerde siempre que $f^{-1} \colon A_f \longmapsto D$. ■

Note que, si en el ejemplo anterior se pide un dominio en donde la función sea decreciente, el proceso de cálculo es similar, pero en este caso la función tendría dominio $]-\infty, \frac{1}{6}]$ y la función inversa cambia de criterio por:

$$f^{-1}(x) = \frac{1 - \sqrt{25 + 12x}}{6}$$

por lo que la fórmula de f^{-1} no se puede calcular sin saber el dominio en que se desea definir.

Si $f \colon A \to A$ es una función biyectiva, se dice que f es una **permutación** del conjunto A.

El conjunto formado por todas las funciones biyectivas sobre un conjunto finito (véase página 262), es muy importante, como se indicará en el capítulo 6, para la clasificación de diversas estructuras algebraicas.

Ejemplo 41. *En el ejemplo* 18 *se demostró que la función* f *de* $\mathbb{R}$ *en* $\mathbb{R}$*, cuyo criterio es* $f(x) = 5x - 4$*, es una función biyectiva; por lo tanto,* f *es una permutación de* $\mathbb{R}$*.* ■

Si p es una permutación sobre el conjunto finito $\{a_1, a_2, \ldots, a_n\}$, es posible representarla por medio del arreglo:

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{pmatrix}$$

En la primera fila se ubican los elementos de A y en la segunda las imágenes de ellos.

Ejemplo 42. *Sobre* $A = \{1, 2, 3, 4\}$*, considere las permutaciones:*

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Calcule $p_1 \circ p_2$*.*

Solución. En primer lugar, es claro que $p_1 \circ p_2 \colon A \to A$. Así, se evalúa $p_1 \circ p_2$ en cada elemento de A; por ejemplo:

$$p_1 \circ p_2(1) = p_1(p_2(1)) = p_1(3) = 4$$
$$p_1 \circ p_2(2) = p_1(p_2(2)) = p_1(2) = 1$$

De la misma forma, $p_1 \circ p_2(3) = 2$ y $p_1 \circ p_2(4) = 3$, y se puede escribir que $p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$. ■

Ejemplo 43. *Sobre $A = \{1, 2, 3, 4, 5, 6\}$, considere las permutaciones:*

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 2 & 4 & 6 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}$$

Calcule $p_1 \circ p_2$ y p_2^{-1}.

Solución. En primer lugar, recuerde que para evaluar una composición de funciones, primero se aplica la función escrita a la derecha y luego la de la izquierda. Así, para calcular $p_1 \circ p_2$, primero se aplica p_2 y luego p_1 a cada elemento de A:

$$1 \xmapsto{p_2} 4 \xmapsto{p_1} 2 \qquad 2 \xmapsto{p_2} 3 \xmapsto{p_1} 1 \qquad 3 \xmapsto{p_2} 5 \xmapsto{p_1} 4$$
$$4 \xmapsto{p_2} 1 \xmapsto{p_1} 5 \qquad 5 \xmapsto{p_2} 2 \xmapsto{p_1} 3 \qquad 6 \xmapsto{p_2} 6 \xmapsto{p_1} 6$$

Por lo tanto, se tiene que $p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 3 & 6 \end{pmatrix}$. Por último, $p_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$ ■

Ejercicios (sección 4.4)

1. Para la función $f\colon \mathbb{R} \to \mathbb{R}$, cuyo criterio es $f(x) = 3x - 5$:

   (a) Pruebe que f es biyectiva.

   (b) Determine $f^{-1}(x)$. Además, compruebe que $(f^{-1} \circ f)(x) = x$.

2. Si $f(x) = -3x + 1$, calcule $(f \circ f \circ f)^{-1}(x)$.

3. Si $f(x) = 3x - 1$ y $g(x) = -2x + 4$, calcule $(f \circ g \circ f)^{-1}(x)$.

4. Considere las funciones G y H, definidas sobre sus respectivos dominios reales, con criterios $G(x) = \dfrac{x}{x+4}$, $H(x) = 3x - 4$. Calcule $(H^{-1} \circ G \circ H)(x)$ y $(H \circ G^{-1})(x)$.

5. Considere las dos funciones f y g, definidas sobre sus respectivos dominios de números reales, con $g(x) = \frac{x}{x+2}$, $f(x) = x - 1$. Verifique que $(g^{-1} \circ f \circ g)(x) = \frac{-4}{x+4}$.

6. Sea $f\colon \mathbb{R} \to \mathbb{R}$ biyectiva, si $(2,3) \in G_f$ y además $f^{-1}\left(\frac{k+3}{k-2}\right) = 2$, calcule el valor de k.

7. Dé un ejemplo de una función que sea inyectiva y no invertible.

8. Dé un ejemplo de una función que sea sobreyectiva y no invertible.

9. Sea $f\colon \mathbb{R}-\left\{\frac{2}{3}\right\} \to \mathbb{R}-\left\{\frac{5}{3}\right\}$ definida por $f(x) = \frac{5x+3}{3x-2}$.

   (a) Pruebe que f es una función biyectiva.

   (b) Calcule $f^{-1}(x)$ y compruebe que $(f \circ f^{-1})(x) = x$.

10. Sea $f\colon \mathbb{R}-\left\{\frac{-2}{3}\right\} \to \mathbb{R}-\left\{\frac{1}{3}\right\}$ definida por $f(x) = \frac{3x-7}{9x+6}$.

    (a) Si se sabe que f es biyectiva, calcule el criterio de f^{-1}.

    (b) Compruebe que $f^{-1}(x) = (f \circ f)(x)$.

11. Sea $f\colon \mathbb{R}-\{3\} \to \mathbb{R}$ definida por $f(x) = \frac{2x+3}{x-3}$. Pruebe que f es inyectiva pero no es sobreyectiva.

12. Si $f(x) = x^2 + 4x + 1$, especifique el dominio y codominio de f de manera que sea invertible; además, determine el criterio de $f^{-1}(x)$.

13. Considere la función $f\colon \mathbb{R} \to]-\infty, 0[\cup [3, +\infty[$ definida por:

$$f(x) = \begin{cases} 2x+1 & \text{si } x \geq 1 \\ x-1 & \text{si } x < 1 \end{cases}$$

    Encuentre el criterio de $f^{-1}(x)$.

14. Considere la función $f\colon \mathbb{R} \to \mathbb{R}$ definida por:

$$f(x) = \begin{cases} 1-x^2 & \text{si } x \leq 0 \\ x+1 & \text{si } x > 0 \end{cases}$$

Encuentre el criterio de $f^{-1}(x)$, grafique $f(x)$ y $f^{-1}(x)$ en un mismo sistema cartesiano. Además, encuentre dónde se intersecan f y f^{-1}.

15. Sea $f\colon [1,+\infty[\to [2,+\infty[$ definida por $f(x)=\frac{x^2+1}{x}$.

    (a) Pruebe que f es una función biyectiva.

    (b) Determine el criterio de su inversa $f^{-1}(x)$.

16. Considere la función $f\colon [1,+\infty[\longrightarrow]1,3]$ definida por $f(x)=\frac{x^2+2}{x^2}$.

    (a) Pruebe que f es una función biyectiva.

    (b) Determine $f^{-1}(x)$.

17. Considere la función $f\colon]-\infty,-1] \longrightarrow]1,3]$ definida por $f(x)=\frac{x^2+2}{x^2}$. Si se sabe que f es biyectiva, calcule el criterio $f^{-1}(x)$; además, compruebe que $\left(f\circ f^{-1}\right)(x)=x$.

18. Sobre $A=\{1,2,3,4,5\}$, considere las permutaciones:

$$p_1=\begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 2 & 3 & 5 & 1 & 4\end{pmatrix} \qquad p_2=\begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 4 & 1 & 2 & 5 & 3\end{pmatrix}$$

    Calcule $p_2\circ p_2$, $p_1\circ p_2$ y p_2^{-1}.

19. Sea f una función definida sofre E. Para $s\in E$ se define la **órbita** de s relativa a f, que se denota por $\boldsymbol{\mathcal{O}(s)}$ como el conjunto:

$$\mathcal{O}(s)=\{f^j(s)\ \ /\ \ j\in\mathbb{N}\}$$

    Es decir, es el conjunto formado por las aplicaciones sucesivas de la función f al elemento fijo s. Calcule las órbitas de todos los elementos de $A=\{1,2,\ldots,8,9\}$. Para la biyección dada por:

$$f=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 2 & 1 & 4 & 6 & 7 & 3 & 9 & 8 & 5\end{pmatrix}$$

20. Sea $f\colon \mathbb{R} \to \mathbb{R}$ una función biyectiva. Si se define $f_a(x) = f(ax)$ para todo $a \neq 0$, pruebe que $f_a\colon \mathbb{R} \to \mathbb{R}$ es una función biyectiva. Además, pruebe que $f_a^{-1}(x) = \frac{1}{a} f^{-1}(x)$.

21. Sean A y B conjuntos no vacíos, suponga que f es una función de A en B y sean $D \subseteq A$, $E \subseteq B$. Demuestre que:

    (a) $D \subseteq f^{-1}(f(D))$.

    (b) Si f es inyectiva, entonces $D = f^{-1}(f(D))$.

    (c) $f(f^{-1}(E)) \subseteq E$.

    (d) Si f es sobreyectiva, entonces $E = f(f^{-1}(E))$.

4.5 Equipotencia

Para finalizar el capítulo, en esta sección se introduce la noción de los conjuntos finitos e infinitos, contables y numerables, así como el concepto de equipotencia y algunos resultados y teoremas importantes relacionados con este tema.

Se dice que un conjunto A es **finito** si y solo si para algún $n \in \mathbb{N}$ existe una biyección con el conjunto $\mathbb{N}_n = \{1, 2, 3, \ldots, n\}$. De acuerdo con lo estudiado en la sección 2.5, se tiene que $\mid A \mid = n$ y por supuesto $\mid \varnothing \mid = 0$, con lo cual el vacío es finito. Si un conjunto no es finito, se dice que es **infinito**.

Ejemplo 44. *Es claro que el conjunto* $A = \{-3, 0, 5\}$ *es finito, pues se puede definir una función biyectiva* f *de* A *en* $\mathbb{N}_3$ *por medio de la correspondencia* $f(-3) = 1$, $f(0) = 2$, $f(5) = 3$. ■

Se dice que el conjunto A es **numerable** si y solo si existe una biyección con $\mathbb{N}$. Además, se dice que el conjunto A es **contable** si y solo si es finito o numerable.

Es decir, A es contable si existe una función biyectiva de él con algún subconjunto de $\mathbb{N}$. Para conjuntos contables, pueden suceder dos situaciones: que sea finito o que sea infinito; así, numerable es equivalente a contable infinito. Además, no todos los conjuntos infinitos son contables, como se explicará en próximos ejemplos.

Teorema 1. $\mathbb{Z}$ *es numerable, es decir, contable infinito.*

Demostración. Para verificar esta proposición, basta encontrar una función biyectiva entre $\mathbb{Z}$ y $\mathbb{N}$. Para ello, considere la función f que aplica linealmente los números mayores o iguales que cero a los números pares y aplica los números negativos a los impares. Es decir, el criterio de la función $f\colon \mathbb{Z} \to \mathbb{N}$ descrita es:

$$f(n) = \begin{cases} 2n & \text{si } n \geq 0 \\ -2n-1 & \text{si } n < 0 \end{cases}$$

Faltaría probar que f es biyectiva, lo cual es sencillo y se deja como ejercicio (véase ejercicio 9). Por lo tanto, $\mathbb{Z}$ es numerable. $\square$

Teorema 2. *Si B es finito y $A \subseteq B$, entonces A es finito.*

Teorema 3. *Si A y B son finitos, entonces $A \cup B$ es finito. Además, si $\mid A \mid = m$ y $\mid B \mid = n$, entonces $\mid A \cup B \mid \leq m + n$.*

Teorema 4. *Si A y B son contables, entonces $A \cup B$ es contable.*

La demostración de los teoremas 2, 3 y 4 es sencilla y se deja como ejercicio al lector.

Se dice que dos conjuntos A y B son **equipotentes** y se escribe $\boldsymbol{A \approx B}$ si y solo si existe una función biyectiva de A en B.

Ejemplo 45. *Es claro que el conjunto $A = \{2, -3, 4\}$ es equipotente con $B = \{1, 2, 3\}$, pues se puede definir una función biyectiva f de A en B por medio de $f(2) = 1$, $f(-3) = 2$, $f(4) = 3$. De esta forma se ha verificado que $\{2, -3, 4\} \approx \{1, 2, 3\}$.* $\blacksquare$

Ejemplo 46. *Pruebe que el intervalo $[1, 2]$ es equipotente con $[1, 6]$.*

Solución. Para probarlo, se debe encontrar una biyección entre estos conjuntos; para ello, considere la función lineal $f(x)$ tal que $f(1) = 1$ y $f(2) = 6$. Así, $f\colon [1, 2] \to [1, 6]$ tal que $f(x) = 5x - 4$ es biyectiva (ver ejemplo 18) y, por lo tanto, son equipotentes. $\blacksquare$

La definición de conjunto finito, dada al inicio de esta sección, fue propuesta por Bolzano. Equivalente a ella, se puede establecer que un conjunto A es *finito* si el único subconjunto de A equipotente con él es A mismo. Es decir, A es finito si satisface la proposición:

$$(S \subseteq A \wedge S \approx A) \Rightarrow S = A$$

Un conjunto A es *infinito* si y solo si A no es finito, es decir, un conjunto A es infinito si existe un subconjunto propio de A que sea equipotente con A.

Ejemplo 47. *Observe cómo a partir del ejemplo* 46 *se prueba que el intervalo cerrado* $[1, 6]$ *es un conjunto infinito, pues allí se probó que es equipotente con* $[1, 2]$*, o sea, es equipotente con un subconjunto propio de él.* ■

Teorema 5. *La relación de equipotencia* $\approx$ *definida sobre* $P(E)$ *para* E *un conjunto dado es una relación de equivalencia.*

Demostración. En primer lugar, $\approx$ es reflexiva, ya que la función identidad es biyectiva de A en A y se cumple que $A \approx A$. Para la simetría, se supone que $A \approx B$, es decir, $\exists f : A \to B$ con f biyectiva. Se sabe que f^{-1} será biyectiva y se cumple que $\exists f^{-1} : B \to A$, con lo cual $B \approx A$. Por último, si $A \approx B$ y $B \approx C$, entonces $\exists f : A \to B$ y $\exists g : B \to C$ biyectivas y se sabe que $g \circ f : A \to C$ también será biyectiva, con lo cual $A \approx C$ y la relación $\approx$ es transitiva. □

En la demostración del teorema 1 se ha construído una función biyectiva entre los conjuntos $\mathbb{Z}$ y $\mathbb{N}$, es decir, se ha definido una biyección entre ellos y se probó que $\mathbb{Z} \approx \mathbb{N}$. Con esto se muestra que ambos conjuntos tienen la misma cantidad de elementos.

Para demostrar el resultado −poco intuitivo− de que $\mathbb{Q}$ es numerable, es decir, $\mathbb{Q} \approx \mathbb{N}$, y con ello que $\mathbb{Q}$ y $\mathbb{N}$ son equipotentes, para evidenciar así que tienen la misma cantidad de elementos, véase el interesante artículo [9].

Se dice que A es de **menor o igual potencia** que B y se escribe $\boldsymbol{A \preceq B}$ si y solo si existe una función inyectiva de A en B. Además, A es de **menor potencia** que B y se escribe $\boldsymbol{A \prec B}$ si y solo si $A \preceq B \wedge A \not\approx B$.

En el siguiente teorema se afirma y demuestra que el conjunto $\mathbb{R}$ (de los números reales) no es equipotente con $\mathbb{N}$ (el conjunto de los naturales), es decir, $\mathbb{R}$ también es un conjunto infinito, pero de cardinalidad mayor que la de $\mathbb{N}$. A este tipo de conjuntos, infinitos y no equipotentes con $\mathbb{N}$, se les denomina **no numerables**.

El interesante argumento dado en la siguiente demostración es original del gran matemático alemán, Georg Cantor.

Teorema 6. $\mathbb{N} \prec \mathbb{R}$.

Demostración. Es claro que $\mathbb{N} \preceq \mathbb{R}$, pues la función identidad sería inyectiva. Para probar que cualquier función $f \colon \mathbb{N} \to \mathbb{R}$ no puede ser sobreyectiva, se construye un número real x de manera que no tenga preimagen por f. Considere $x = 0, a_1 a_2 a_3 \ldots a_n \ldots$, donde a_n denota el n-ésimo decimal y está dado por el criterio:

$$a_n = \begin{cases} 0 & \text{si el } n\text{-ésimo decimal de } f(n) \text{ es diferente de cero} \\ 1 & \text{si el } n\text{-ésimo decimal de } f(n) \text{ es igual a cero} \end{cases}$$

Es fácil justificar ahora que x no tiene preimagen por f, ya que si $\exists k \in \mathbb{N}$ tal que $f(k) = x$, se tiene que $a_k = 0 \Rightarrow a_k = 1$ y $a_k \neq 0 \Rightarrow a_k = 0$, que en cualquier caso es una contradicción. $\square$

Teorema 7. (De Cantor) *Dado A un conjunto, entonces $A \prec P(A)$.*

Demostración. Sea A un conjunto, es claro que la función $I \colon A \to P(A)$ con $I(a) = \{a\}$ es inyectiva. Para demostrar que $A \not\approx P(A)$, se probará que toda función $f\colon A \to P(A)$ no es sobreyectiva. Para ello, considere el conjunto:

$$C = \{x \in A \ / \ \ x \notin f(x)\} \tag{4.4}$$

Claramente, $C \in P(A)$, pues $C \subseteq A$. Para probar que el conjunto C no tiene preimagen por f, suponga, por contradicción, que a es una preimagen de C, con lo cual se cumple que $f(a) = C$. Como $a \in A$ y $C \subseteq A$, analice los únicos dos casos posibles:

– $a \in C \Rightarrow a \notin f(a) \Rightarrow a \notin C$ $(\Rightarrow\Leftarrow)$

– $a \notin C \Rightarrow a \in f(a) \Rightarrow a \in C$ $(\Rightarrow\Leftarrow)$

En ambos casos se obtiene una contradicción, con lo cual f no es sobreyectiva. $\square$

Ejemplo 48. *Para el conjunto $A = \{1, 2, 3, 4\}$ defina la función f de A en $P(A)$, es decir, $f\colon A \to P(A)$, por medio de la siguiente asignación: $f(1) = \{1, 3\}$, $f(2) = \{1, 4\}$, $f(3) = \{2\}$, $f(4) = \{2, 4\}$. Encuentre el conjunto C construido en la demostración del teorema de Cantor y confirme que éste no tiene preimagen por f.*

Solución. Se tiene que $C = \{x \in A \ / \ \ x \notin f(x)\}$, según se definió en (4.4). Verifique si los elementos de A cumplen o no la condición para pertenecer a C. Primero $1 \notin C$, pues $1 \in \{1, 3\} = f(1)$; $2 \in C$, pues $2 \notin \{1, 4\} = f(2)$; $3 \in C$, pues $3 \notin \{2\} = f(3)$, y $4 \notin C$, pues $4 \in \{2, 4\} = f(4)$, para finalmente escribir $C = \{2, 3\}$, que evidentemente no tiene preimagen por f. $\blacksquare$

La cardinalidad de $\mathbb{R}$ es conocida como *el continuo* y se denota mediante $\boldsymbol{c}$. El continuo c coincide con la cardinalidad del conjunto de partes o conjunto potencia de $\mathbb{N}$, es decir:

$$c = |\mathbb{R}| = |P(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$$

Teorema 8. (De Schröder-Bernstein) *Si se cumple que $A \preceq B$ y $B \preceq A$, entonces $A \approx B$.*

Demostración. Véase [21]. $\square$

La definición de conjunto infinito no garantiza la existencia de un conjunto infinito; sin embargo, dicha existencia se axiomatiza por medio del conocido **axioma de infinitud**, por medio del cual se asume la existencia de un conjunto infinito, denotado mediante $\mathcal{I}$.

Sobre el conjunto $\mathcal{F}$ formado por todos los conjuntos finitos subconjuntos de $\mathcal{I}$, es decir:

$$\mathcal{F} = \{S \subseteq \mathcal{I} \ / \ \ S \text{ es finito}\}$$

se define la relación de equivalencia (ver ejercicio 4 de sección 3.3), de manera que $M\mathcal{R}N$ si y solo si $M \approx N$, es decir, dos elementos de $\mathcal{F}$ se relacionan si tienen la misma cardinalidad. El conjunto cociente $\mathcal{F}/\approx$ se conoce como el conjunto de los **números naturales**, es decir:

$$\mathcal{F}/\!\approx \,= \,\mathbb{N}$$

Así, se llama *cero* al conjunto $\overset{\bullet}{\varnothing}$, denotado como el número natural 0. Se denomina *uno* al conjunto $\overset{\bullet}{\{\varnothing\}}$, denotado como el número natural 1, es decir, el número natural 1 representa a la clase de equivalencia de todos los conjuntos que tienen un elemento. Se denomina *dos* al conjunto $\overset{\bullet}{\{\varnothing, \{\varnothing\}\}}$, denotado como el número natural 2, es decir, el número natural 2 representa a la clase de equivalencia de todos los conjuntos que tienen dos elementos. De la misma manera, se definen los números naturales 3, 4, ...

El principal interés no es profundizar en la construcción de los números naturales; sin embargo, para ello puede consultar en [2], [9], [21].

Ejercicios (sección 4.5)

1. Pruebe que el conjunto de los números enteros positivos múltiplos de 5 es equipotente con el conjunto de los números pares positivos.

2. Demuestre que el intervalo semiabierto $]2, 5]$ es equipotente con el intervalo semiabierto $[3, 4[$.

3. Demuestre que el intervalo abierto $]0, 1[$ es equipotente con $\mathbb{R}$.

4. Demuestre que el intervalo abierto $]0, 4[$ es infinito.

5. Demuestre que el conjunto de los enteros múltiplos de 3 es un conjunto infinito.

6. Demuestre el teorema 2.

7. Demuestre el teorema 3.

8. Demuestre el teorema 4.

9. Pruebe que la función definida en el teorema 1 (página 253), es biyectiva.

10. Para el conjunto $A = \{1, 2, 3, 4, 5\}$ y la función $f\colon A \to P(A)$ dada por $f(1) = \{2, 3, 5\}$, $f(2) = \{1, 2, 4\}$, $f(3) = \{1, 2\}$, $f(4) = \{1, 4\}$, $f(5) = \{1\}$, encuentre el conjunto C construido en la demostración del teorema de Cantor y confirme que este conjunto no tiene preimagen por f.

11. Sea $E = \{a, b, c, d\}$ un conjunto dado y considere la relación de equipotencia $\approx$ definida sobre $P(E)$. Calcule $P(E)/\approx$.

4.6 Principios de conteo

"Dios no juega a los dados".

Albert Einstein

Como ya se ha mencionado, una permutación de un conjunto es una función biyectiva sobre este conjunto, es decir, dado un orden en una colocación de n objetos, una *permutación* sería una nueva ordenación de ellos. A continuación, se extenderá el concepto y se deberá pensar en que en la nueva colocación de objetos no se considera la totalidad de los n objetos, sino más bien a r de ellos, con $r \leq n$. Así, se habla de una permutación de n objetos tomados de r en r sin repetición, y se denotará con $\boldsymbol{P(n, r)}$. Para comprender esto, analice el siguiente ejemplo.

Ejemplo 49. *Considere las cuatro letras a, b, c, d. De esta manera, las permutaciones abdc, adcb son algunas permutaciones de estas cuatro letras tomadas todas a la vez. Las permutaciones bda, abc o cda son algunas de las permutaciones tomadas de tres en tres, y da, bc o cd son algunas de las permutaciones tomadas de dos en dos.* ■

En el ejemplo anterior se mostraron algunas de las permutaciones posibles; sin embargo, es importante conocer el número exacto de permutaciones de r en r que se pueden formar. Para ello, considere las mismas cuatro letras y piense que forma permutaciones de tres en tres. Así, es claro que la primera letra se puede escoger de 4 formas distintas, la segunda letra se puede escoger de 3 formas distintas, pues al haber escogido la primera letra, ya no se puede escoger de nuevo. Por último, la tercera letra se puede escoger de 2 formas distintas. Por lo tanto, se tienen en total $4 \cdot 3 \cdot 2 = 24$ permutaciones posibles.

El comentario anterior se puede generalizar para el número de permutaciones de n objetos tomados de r en r sin repetición, de manera que se cumple:

$$P(n, r) = n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)$$

Al amplificar la expresión multiplicándola por $(n-r)!$, se obtiene:

$$\begin{aligned} P(n,r) &= \frac{n\cdot(n-1)\cdot(n-2)\cdots(n-r+1)\cdot(n-r)!}{(n-r)!} \\ &= \frac{n!}{(n-r)!} \end{aligned}$$

Finalmente, resulta válida y útil la fórmula para el número de permutaciones de n objetos tomados de r en r sin repetición:

$$P(n,r) = \frac{n!}{(n-r)!} \tag{4.5}$$

Además, es claro que para $r=n$ se tiene $P(n,n)=n!$, pues se sabe que $0! = 1$.

Ejemplo 50. *Considere las cuatro letras a, b, c, d. De esta manera, ¿cuántas permutaciones de estas* 4 *letras tomadas de tres en tres existen?*

Solución. Basta calcular:

$$P(4,3) = \frac{4!}{(4-3)!} = 24$$

Así, existen 24 posibles maneras de ordenar estas 4 letras. ■

Ejemplo 51. *¿Cuántas palabras de tres letras se pueden formar utilizando, sin repetición, las letras de la palabra UNIVERSO?*

Solución. Basta observar que esta palabra tiene 8 letras distintas, con lo cual se calcula $P(8,3) = \frac{8!}{(8-3)!} = 8\cdot 7\cdot 6 = 336$, y se concluye que son 336 las posibles palabras. ■

Ejemplo 52. *Si se tiene un conjunto A con cuatro elementos, ¿cuántas funciones biyectivas sobre A existen?*

Solución. En este caso, se debe considerar $n=r=4$, con lo cual se tienen $P(4,4)=4!=24$ funciones biyectivas. ■

Como se mencionó al inicio de esta sección, en una permutación de un conjunto de n objetos es importante el orden en la colocación de ellos. Por el contrario, si el orden no se considera importante y se piensa en conjuntos y no en arreglos ordenados, una *combinación* de n objetos tomados de r en r es cualquier selección de r objetos, sin repetición, y se denotará con $\boldsymbol{C(n,r)}$. Note que, en este caso, las 6 permutaciones de las letras a, b, c son: *abc*, *acb*, *bac*, *bca*, *cab*, *cba* y como conjunto se representan como la única combinación $\{a,b,c\}$.

Extendiendo el comentario anterior, y dado que cualquier combinación de n objetos tomados de r en r determina la existencia de $r!$ permutaciones de los objetos de la combinación, se concluye que:

$$P(n,r) = r!\, C(n,r)$$

Al despejar, se obtiene la útil fórmula:

$$C(n,r) = \frac{n!}{(n-r)!\, r!} \tag{4.6}$$

Ejemplo 53. *De un grupo de* 7 *personas se debe formar un comité de* 3 *personas. ¿De cuántas maneras distintas se puede formar este comité?*

Solución. Es claro que el orden en el comité que se forme no es importante; por lo tanto, se calcula $C(7,3) = \frac{7!}{(7-3)!\,3!} = 35$. Por lo que se pueden formar 35 comités diferentes. ∎

Sean A y B conjuntos arbitrarios, se define $\boldsymbol{B^A}$ como el conjunto de todas las funciones de A en B; se define $\boldsymbol{\mathcal{I}(A,B)}$ como el conjunto de todas las funciones inyectivas de A en B. Por último, el conjunto $\boldsymbol{\mathcal{B}(A,B)}$ formado por todas las funciones biyectivas de A en B, es decir:

$$\begin{aligned} B^A &= \{f\colon A \to B \ / \ f \text{ es función}\} \\ \mathcal{I}(A,B) &= \{f\colon A \to B \ / \ f \text{ es función inyectiva}\} \\ \mathcal{B}(A,B) &= \{f\colon A \to B \ / \ f \text{ es función biyectiva}\} \end{aligned}$$

Teorema 9. *Para A y B conjuntos finitos tales que $|A| = p$ y $|B| = n$, se cumple:*

$$\begin{aligned}
\left|B^A\right| &= |B|^{|A|} = n^p \\
|\mathcal{I}(A,B)| &= \begin{cases} 0 & si \;\; n < p \\ \frac{n!}{(n-p)!} & si \;\; n \geq p \end{cases} \\
|\mathcal{B}(A,B)| &= \begin{cases} 0 & si \;\; n \neq p \\ n! & si \;\; n = p \end{cases}
\end{aligned}$$

Demostración. Véase [15] o [21]. □

Ejemplo 54. *Determine cuántas son las funciones inyectivas distintas que se tienen de un conjunto A de 4 elementos, en un conjunto B de 6 elementos.*

Solución. Como $|B| \geq |A|$, al aplicar el teorema anterior se calcula $|\mathcal{I}(A,B)| = \frac{6!}{(6-4)!} = 360$, con lo cual se tienen 360 posibles funciones inyectivas de A en B. ■

Ejercicios (sección 4.6)

1. En un pueblo se desea poner una placa metálica a las avenidas, de manera que conste de dos vocales, seguidas de tres dígitos. Cada dígito puede ser del 0 al 9.
   (a) ¿Cuántas placas diferentes se pueden confeccionar?
   (b) Si no es posible repetir vocales ni números, ¿cuántas serían?
2. De un grupo de 15 personas, con 8 mujeres y 7 hombres, se debe formar un comité de 6 personas, con 3 hombres y 3 mujeres. ¿De cuántas maneras distintas se puede formar este comité?
3. Determine el número de maneras en que 11 juguetes se pueden repartir entre 4 niños A, B, C, D, de manera que reciban 4, 3, 2, 2 regalos respectivamente.

4. ¿Cuántas palabras se pueden formar utilizando todas las letras de la palabra CARRETERA?

5. Un grupo de 10 personas está conformado por 6 mujeres y 4 hombres. Determine el número de posibles comités si:

   (a) Se deben elegir 4 personas.

   (b) Se deben elegir 4 personas, dos hombres y dos mujeres.

   (c) Se deben elegir 4 personas, cada una con un cargo específico (presidente, secretario, tesorero, vocal).

6. Un anuncio de un restaurante de comidas rápidas indica que un cliente puede ordenar su hamburguesa con alguno (o ninguno, o todos) de los siguientes ingredientes: mostaza, mayonesa, lechuga, tomate, cebolla, pepinillo, queso, jamón. ¿Cuántas hamburguesas diferentes se pueden hacer?

7. Se deben formar 4 comités de nueve personas, de un grupo de 36 personas. Determine el número de posibles comités que se pueden formar.

8. Las placas de identificación de un producto empiezan con dos vocales, seguidas por dos números tomados del 0 al 9. Determine el número de posibles placas si:

   (a) El primer dígito que les sigue a las vocales no puede ser par.

   (b) La primera letra no puede ser una E y los números no se pueden repetir.

   (c) Tanto las vocales como los números son iguales.

9. Dado un grupo de 9 estudiantes, determine:

   (a) El número de posibilidades que tienen para realizar tres exámenes si cada uno debe ser realizado por tres estudiantes.

(b) De cuántas maneras distintas se puede dividir para formar tres equipos de 3 estudiantes.

10. Verifique que para r y n naturales con $r < n$ se cumple:

    (a) $C(n,r) = C(n,n-r)$

    (b) $C(n-1,r-1) + C(n-1,r) = C(n,r)$

11. Para A, B, C y D conjuntos finitos tales que $|A| = 3$, $|B| = 4$, $|C| = 5$ y $|D| = 3$, calcule:

    (a) $\left|A^B\right|$

    (b) $|\mathcal{I}(D,C)|$

    (c) $|\mathcal{I}(A,\mathcal{B}(D,A))|$

    (d) $\left|C^{\mathcal{I}(A,B))}\right|$

12. Para A, B, C conjuntos finitos tales que $|A| = 5$, $|B| = 3$, $|C| = 4$ y $|D| = 2$ calcule:

    (a) $\left|B^A \times A^C\right|$

    (b) $|\mathcal{I}(B,A)|$

    (c) $|\mathcal{B}(A,A))|$

    (d) $\left|C^{\mathcal{I}(B,C))}\right|$

    (e) $\left|P\left(B^D\right) \times P\left(D^B\right)\right|$

Capítulo 5

Inducción y recursividad

"Tuvo esposas Fibonacci, que comer
nada comían (pastas aparte).
Tanto así pesaba cada una
como juntas sus dos antecesoras
¡Era la quinta una gran signora!".

J. A. Lindon

Notación Σ y Π

Inducción matemática

Recursividad

En este capítulo se introduce la notación Σ *para la suma y* Π *para el producto; además, se introduce el método de demostración conocido como inducción matemática, el cual tiene múltiples aplicaciones, tanto en el campo de la computación como en geometría, probabilidad, teoría de números, entre otros.*

Por último, se introducen los conceptos básicos de recursividad y las relaciones definidas por recurrencia; a partir de una sucesión definida por recurrencia, se determinará, en algunos casos, la fórmula explícita para esta relación utilizando la ecuación característica asociada.

Para profundizar en el tema tratado en este capítulo, es recomendable consultar las referencias bibliográficas [1], [2], [6], [7], [15] y [21].

5.1 Notación Σ y Π

En esta sección se introduce la notación *sigma* para representar la adición de términos en donde se sigue un comportamiento definido. Así, esta útil notación para la suma, donde se utilizará la letra griega Σ, se define como:

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_n \tag{5.1}$$

Donde m y n son números enteros tales que $m \leq n$. El símbolo i es el **índice** de la suma; m es el **límite inferior** del índice y n es el **límite superior** del índice.

Ejemplo 1. *Calcule el valor exacto de la suma* $\sum_{i=3}^{8}(2i+3)$.

Solución. Es claro que el primer sumando se calcula al evaluar en $i = 3$ y corresponde al valor $2 \cdot 3 + 3 = 9$. Al evaluar en $i = 4$, se obtiene el valor 11, y siguiendo el proceso para los seis sumandos, se tiene que:

$$\sum_{i=3}^{8}(2i+3) = 9 + 11 + 13 + 15 + 17 + 19 = 84$$

■

En el caso particular en que $m = 1$ en la identidad (5.1), la ***n*-ésima suma parcial**, corresponde a la suma de los primeros n términos de la sucesión a_n y se escribe:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$$

Ejemplo 2. *El valor exacto de la suma* $\sum_{i=1}^{5} i^2$*, que representa la suma de los primeros cinco cuadrados, corresponde a* $1 + 4 + 9 + 16 + 25$*, es decir,* $\sum_{i=1}^{5} i^2 = 55$. ■

Ejemplo 3. *Calcule el valor exacto de la suma* $\sum_{i=4}^{10} 5$.

Solución. El primer sumando que se debe calcular al evaluar en $i = 4$ corresponde al valor 5. Al evaluar en $i = 5$, se obtiene el valor 5, y siguiendo el proceso para los siete sumandos, se obtiene:

$$\sum_{i=4}^{10} 5 = 5 + 5 + 5 + 5 + 5 + 5 + 5 = 35$$

■

Ejemplo 4. *Calcule el valor exacto de la suma* $\displaystyle\sum_{i=1}^{100} i$.

Solución. Por supuesto, es posible efectuar los cálculos que se indican; sin embargo, si se toma en cuenta que la adición es conmutativa y se denota con S la suma que se pide, es claro que:

$$S = 1 + 2 + 3 + 4 + \cdots + 99 + 100 \tag{5.2}$$

Además, al reescribir en orden descendente:

$$S = 100 + 99 + 98 + \cdots + 3 + 2 + 1 \tag{5.3}$$

Al sumar término a término las igualdades (5.2) y (5.3), se obtiene la nueva igualdad:

$$2S = \underbrace{101 + 101 + 101 + \cdots + 101 + 101 + 101}_{\text{100 veces 101}} \tag{5.4}$$

Al despejar S de la igualdad $2S = 10100$, se obtiene que $S = 5050$, es decir, $1 + 2 + 3 + 4 + \cdots + 99 + 100 = 5050$. ■

Propiedades de la suma:

1. $\displaystyle\sum_{i=1}^{n} 1 = n$

2. $\displaystyle\sum_{i=1}^{n} c = nc$

3. $\displaystyle\sum_{i=1}^{n} ca_i = c\sum_{i=1}^{n} a_i$

4. $\displaystyle\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$

En ocasiones, la cantidad de sumandos que se tienen dificulta la parte aritmética, pero utilizando las propiedades anteriores y algunas sumas conocidas, se puede simplificar significativamente el cálculo.

Ejemplo 5. *Calcule el valor exacto de la suma* $\displaystyle\sum_{i=1}^{100}(3i-5)$.

Solución. De nuevo, es posible efectuar los cálculos que se indican; sin embargo, se utilizará el resultado que obtenido en el ejemplo 4 y las propiedades de la suma:

$$\sum_{i=1}^{100}(3i-5) = 3\sum_{i=1}^{100} i - \sum_{i=1}^{100} 5 = 3\cdot 5050 - 5\cdot 100 = 14\,650$$

■

Análogo a la notación de suma, donde se utiliza Σ, se introduce una notación para el producto, donde se utiliza la letra griega Π:

$$\prod_{i=1}^{n} a_i = a_1\cdot a_2\cdot a_3\cdots a_n$$

Esta notación es útil para representar un producto de términos que sigue un comportamiento definido.

Ejemplo 6. *El valor exacto que corresponde a la expresión* $\displaystyle\prod_{i=1}^{5}(3i-2)$ *es el producto* $1\cdot 4\cdot 7\cdot 10\cdot 13 = 3640$ ■

Ejemplo 7. *Calcule el valor exacto de* $\displaystyle\sum_{j=1}^{3}\prod_{i=1}^{j}(3i^2-i)$.

Solución. Se debe calcular cada uno de los tres sumandos:

$$\begin{aligned}\sum_{j=1}^{3}\prod_{i=1}^{j}(3i^2-i) &= \prod_{i=1}^{1}(3i^2-i)+\prod_{i=1}^{2}(3i^2-i)+\prod_{i=1}^{3}(3i^2-i)\\ &= 2+2\cdot 10+2\cdot 10\cdot 24=502\end{aligned}$$

■

La notación sigma se puede generalizar considerando una proposición abierta $P(n)$ y definiendo $\displaystyle\sum_{P(n)} a_n$ como la suma de todos los a_n para los n que satisfacen $P(n)$. De la misma manera, $\displaystyle\prod_{P(n)} a_n$ como el producto de todos los a_n para los n que satisfacen $P(n)$. Si no existen valores que satisfacen la proposición, se define $\displaystyle\sum_{P(n)} a_n = 0$ y $\displaystyle\prod_{P(n)} a_n = 1$.

Ejemplo 8. *Calcule el valor de* $\displaystyle\sum_{2<n\leq 5}(n^2-1)$.

Solución. Se procede a realizar la suma de los términos $3^2-1=8$, $4^2-1=15$, $5^2-1=24$, pues los valores enteros de n que satisfacen la proposición $2<n\leq 5$ son solamente 3, 4 y 5, con lo cual:

$$\sum_{2<n\leq 5}(n^2-1)=8+15+24=47$$

■

Ejemplo 9. *Para calcular el valor exacto de* $\displaystyle\sum_{\substack{n|12\\ n\geq 3}} n$, *observe que los únicos valores enteros de* n, *tales que* $n\geq 3$, *que satisfacen la proposición* $n|12$, *es decir, que sean divisores de* 12, *son solamente* 3, 4, 6 *y* 12, *con lo cual* $\displaystyle\sum_{\substack{n|12\\ n\geq 3}} n=3+4+6+12=25$. ■

Ejemplo 10. *Es claro que los divisores positivos de* 20 *son* 1, 2, 4, 5, 10, 20, *por lo que para cada uno de ellos en la suma siguiente se debe sumar la expresión* d^2, *de esta manera, se obtiene* $\sum_{\substack{d|45 \\ d>0}} d^2 = 1^2 + 2^2 + 4^2 + 5^2 + 10^2 + 20^2 = 546$. ■

Ejemplo 11. *Para calcular el valor exacto de* $\prod_{\substack{n|15 \\ n>3}} n$, *observe que los únicos valores enteros de* n, *tales que* $n > 3$, *que satisfacen la proposición* $n|15$, *es decir, que sean divisores de* 15, *son solamente* 5 *y* 15, *con lo cual* $\prod_{\substack{n|15 \\ n>3}} n = 5 \cdot 15 = 75$. ■

Ejemplo 12. *Como no existe un entero que satisface la proposición* $n^2 < 0$, *se tiene que* $\sum_{n^2<0} n^3 = 0$. *Además, se tiene que* $\prod_{n^2<0} n^3 = 1$. ■

Ejercicios (sección 5.1)

1. Utilice la notación Σ o Π para representar:

   (a) $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{56} + \frac{1}{57}$

   (b) $5 + 7 + 9 + \cdots + 41 + 43$

   (c) $\frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \cdots + \frac{33}{34} + \frac{34}{35}$

   (d) $\frac{1}{2} - \frac{2}{3} + \frac{3}{4} + \cdots + \frac{33}{34} - \frac{34}{35}$

   (e) $\left(3 - \frac{1}{2}\right)\left(4 - \frac{1}{3}\right)\left(5 - \frac{1}{4}\right)\cdots\left(101 - \frac{1}{100}\right)$

   (f) $(2 - 8) + (3 - 27) + (4 - 64) + \cdots + (10 - 1000)$

   (g) $(1+4)(1+4+9)(1+4+9+16)\cdots(1+4+9+16+\cdots+121)$

2. Determine el valor exacto de:

   (a) $\sum_{i=1}^{6}(2i^2 - 3i + 2)$

(b) $\displaystyle\sum_{i=3}^{5}(3^i - 2^i)$

(c) $\displaystyle\prod_{i=1}^{5}(3i^2 - 4i)$

(d) $\displaystyle\sum_{k=1}^{4}(1 + k^3)$

(e) $\displaystyle\sum_{j=3}^{5}\prod_{k=2}^{j}\left(\frac{2^k}{k+1}\right)$

(f) $\displaystyle\sum_{k=3}^{5}\sum_{i=1}^{k}\sum_{j=1}^{i}\left(j^2 + 3j\right)$

3. Si se define $\overline{x} = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} x_i$, pruebe que:

$$\sum_{i=1}^{n}(x_i - \overline{x})^2 = \sum_{i=1}^{n} x_i^2 - n\overline{x}^2$$

4. Para n un número natural, considere las proposiciones P y Q dadas por $P(n) : n$ divide a 54, $Q(n) : n$ divide a 24. Calcule los valores exactos de:

(a) $\displaystyle\prod_{\substack{P(n)\\ n>10}} (2n - 3)$

(b) $\displaystyle\sum_{\substack{P(n)\\ Q(n)}} (n + 2)$

5.2 Inducción matemática

Se asumirá sin demostración el siguiente principio, que establece la existencia del menor elemento. Este será de gran utilidad en para justificar la representación de un número en diferentes bases.

> **Principio de buen ordenamiento**.
> Todo subconjunto del conjunto de los números naturales tiene un **primer elemento**, también llamado elemento mínimo.

En algunas ocasiones, es necesario demostrar que una proposición abierta $P(n)$ es válida para todos los números naturales (o para algún subconjunto infinito de $\mathbb{N}$); para ello, se debe probar que la proposición dada es verdadera para cada uno de los elementos de $\mathbb{N}$. Claro que, como el conjunto de los números naturales es infinito, tal afirmación no siempre es fácil de probar.

Con esa finalidad, se utilizará un método de demostración que se enuncia a continuación. Observe cómo se fundamenta en la regla de inferencia *modus ponens* $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$, dada en el capítulo 1.

> El **método de inducción matemática** se utiliza para demostrar que una proposición de la forma $(\forall n \in \mathbb{N})\ [P(n)]$ es verdadera. Para esto, basta demostrar que
>
> 1. $P(0)$ es verdadera.
>
> 2. Si $P(n)$ es verdadera, entonces $P(n+1)$ es verdadera.

Es decir, se prueba la validez de la proposición abierta en $n = 0$, se asume la validez de la proposición para n. A esta hipótesis se le conoce como **hipótesis de inducción** (H.I.) y se demuestra que la proposición es válida para $n + 1$, este último se conoce como el *paso inductivo*. Por otro lado, se debe aclarar que, en algunas ocasiones, el primer valor donde la proposición es válida no es $n = 0$, sino más bien otro valor n_0, en cuyo caso se prueba que $P(n_0)$ es verdadera.

Básicamente, el método de inducción matemática se utilizará para demostrar tres tipos de proposiciones cuantificadas, relacionadas con igualdades, desigualdades y divisibilidad; sin embargo, como se mencionó anteriormente, éste se utiliza en muchos campos de la matemática.

Ejemplo 13. *Pruebe que, para $n \in \mathbb{N}$, la suma de todos los números impares menores que $2n$ es igual a n^2.*

Solución. El enunciado afirma la validez para $n \geq 1$ de la igualdad:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \tag{5.5}$$

Para su demostración se aplica el método de inducción matemática:

- Para $n = 1$ es válido, pues el único número impar menor que $2 \cdot 1$ es 1, y claramente es igual a 1^2.

- Se asume que la proposición es válida para n, es decir, se asume como Hipótesis de Inducción (H.I.) la expresión (5.5).

- Es necesario probar que la proposición es válida para $n + 1$, es decir, se debe probar que:

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

  Lo anterior se prueba de esta manera:

  $$\begin{aligned} 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) &\overset{H.I.}{=} n^2 + (2n + 1) \\ &= (n + 1)^2 \end{aligned}$$

  Así, la proposición es válida para $n + 1$.

Con lo cual es válida para todo $n \geq 1$. ■

Por supuesto, con la notación *sigma* estudiada en la sección anterior, el resultado que se probó en el ejemplo 13, es decir, la igualdad (5.5), se puede reescribir como la fórmula:

$$\sum_{i=1}^{n}(2i-1) = n^2 \tag{5.6}$$

Ejemplo 14. *Utilizando la identidad* (5.6) *para* $n = 100$, *se puede verificar y asegurar que* $\sum_{i=1}^{100}(2i-1) = 10000$, *es decir, la suma* $1+3+5+\cdots+197+199$ *de los primeros* 100 *números impares es* 10000. ■

Ejemplo 15. *Para calcular el valor exacto de la suma de los números impares*

$$41 + 43 + 45 + \cdots + 105 + 107$$

se obtiene el valor total de la suma para $n = 54$, *pues* $2 \cdot 54 - 1 = 107$, *y se le resta la suma para* $n = 20$, *pues* $2 \cdot 20 - 1 = 39$. *De esta forma, la suma es:*

$$41 + 43 + 45 + \cdots + 105 + 107 = 54^2 - 20^2 = 2516$$

■

Ejemplo 16. *La fórmula del ejercicio propuesto* 1g *establece una equivalencia para la suma de los n primeros cubos* $1^3+2^3+3^3+\cdots+n^3$, *la cual es válida para todo* $n \geq 1$. *Utilizando esta identidad, se puede calcular el valor exacto de la suma de los primeros n cubos de una manera rápida y eficiente. En el caso de* $n = 50$:

$$\sum_{i=1}^{50} i^3 = \frac{50^2(50+1)^2}{4} = 1\ 625\ 625$$

■

Ejemplo 17. *Pruebe que para* $n \geq 1$ *es válida la fórmula:*

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n \cdot (n+2) = \frac{n(n+1)(2n+7)}{6}$$

Solución. Se aplica el método de inducción:

- Para $n = 1$ es válido, pues el lado izquierdo da $1 \cdot 3 = 3$ y el lado derecho $\frac{1(2)(9)}{6} = 3$; se da la igualdad en este caso.

- Se asume que la proposición es válida para n, es decir, se asume como Hipótesis de Inducción (H.I.) la igualdad:

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n \cdot (n+2) = \frac{n(n+1)(2n+7)}{6} \tag{5.7}$$

- Se debe probar que la proposición es válida para $n+1$, es decir, que:

$$1 \cdot 3 + 2 \cdot 4 + \cdots + n \cdot (n+2) + (n+1) \cdot (n+3) = \frac{(n+1)(n+2)(2n+9)}{6}$$

Esto se prueba como sigue:

$$\begin{aligned}
& 1 \cdot 3 + 2 \cdot 4 + \cdots + n \cdot (n+2) + (n+1) \cdot (n+3) \\
\overset{H.I.}{=} \quad & \frac{n(n+1)(2n+7)}{6} + (n+1) \cdot (n+3) \\
= \quad & \frac{n(n+1)(2n+7) + 6(n+1) \cdot (n+3)}{6} \\
= \quad & \frac{(n+1)[n(2n+7) + 6(n+3)]}{6} \\
= \quad & \frac{(n+1)(2n^2 + 7n + 6n + 18)}{6} \\
= \quad & \frac{(n+1)(n+2)(2n+9)}{6}
\end{aligned}$$

Así, la proposición es válida para $n+1$

Con lo cual es válida para todo $n \in \mathbb{N}$. ■

Ejemplo 18. *Utilizando la identidad que se probó en el ejemplo anterior, se puede afirmar que* $\displaystyle\sum_{i=1}^{50} i\cdot(i+2) = \frac{50(50+1)(2\cdot 50+7)}{6} = 45\,475$, *es decir,* $1\cdot 3 + 2\cdot 4 + 3\cdot 5 + \cdots + 50\cdot 52 = 45\,475$. ■

Ejemplo 19. *Calcule el valor exacto de la suma*

$$151\cdot 153 + 152\cdot 154 + 153\cdot 155 + \cdots + 201\cdot 203$$

Solución. Para este cálculo se utiliza nuevamente la fórmula que se probó en el ejemplo 17. Se debe observar que la suma no está completa, por lo que es necesario restar los primeros términos $1\cdot 3+2\cdot 4+\cdots+150\cdot 152$ al resultado. Así:

$$\begin{aligned} & 151\cdot 153 + 152\cdot 154 + 153\cdot 155 + \cdots + 201\cdot 203 \\ = \; & \frac{201\cdot 202\cdot 409}{6} - \frac{150\cdot 151\cdot 307}{6} \\ = \; & 1\,608\,778 \end{aligned}$$

■

Para a y b enteros, se dice que ***a* divide a *b*** si existe $k \in \mathbb{Z}$ tal que $b = ak$; en este caso, se escribe $\boldsymbol{a|b}$. Además, esto dice que ***b* es divisible por *a*** o que ***a* es un factor de *b***. Si a no divide a b, se escribe $\boldsymbol{a \nmid b}$.

Ejemplo 20. *Es claro que* $7|42$, *pues con* $k = 6$ *se tiene* $42 = 7\cdot 6$. *Además,* $5 \nmid 18$, *pues no existe* k *entero de manera que* $18 = 5\cdot k$. ■

Ejemplo 21. *Pruebe que* $3^{2n+1} + 4\cdot 23^n$ *es divisible por* 7, $\forall n \in \mathbb{N}$.

Solución. Se procede por inducción:

- Para $n = 0$ es válido, pues $3 + 4 = 7$, y 7 es divisible por 7.

- Se asume que la proposición es válida para n, es decir, que existe $k \in \mathbb{Z}$ tal que $3^{2n+1} + 4 \cdot 23^n = 7k$.

- Se prueba que la proposición es válida para $n + 1$:

$$\begin{aligned}
3^{2(n+1)+1} + 4 \cdot 23^{(n+1)} &= 3^{2n+3} + 4 \cdot 23 \cdot 23^n \\
&= 3^2 \cdot 3^{2n+1} + 92 \cdot 23^n \\
&\overset{H.I.}{=} 9\left(7k - 4 \cdot 23^n\right) + 92 \cdot 23^n \\
&= 9 \cdot 7k - 36 \cdot 23^n + 92 \cdot 23^n \\
&= 9 \cdot 7k + 56 \cdot 23^n = 7\left(9k + 8 \cdot 23^n\right)
\end{aligned}$$

  Como $9k+8\cdot 23^n$ es un número entero, se prueba que es un múltiplo de 7 y así la proposición es válida para $n + 1$. ■

Ejemplo 22. *Pruebe que* $n^3 - 4n + 6$ *es divisible por* 3, $\forall n \geq 1$.

Solución. Al aplicar el método de inducción, la proposición es válida para $n = 1$, pues $1 - 4 + 6 = 3$, y 3 es divisible por 3.

- Se asume que la proposición es válida para n, es decir, que existe $k \in \mathbb{Z}$ tal que $n^3 - 4n + 6 = 3k$.

- Se prueba que la proposición es válida para $n + 1$:

$$\begin{aligned}
(n+1)^3 - 4(n+1) + 6 &= n^3 + 3n^2 + 3n + 1 - 4n - 4 + 6 \\
&= n^3 - 4n + 6 + 3n^2 + 3n - 3 \\
&\overset{H.I.}{=} 3k + 3(n^2 + n - 1) \\
&= 3(k + n^2 + n - 1) = 3k'
\end{aligned}$$

  Con $k' = (k + n^2 + n - 1) \in \mathbb{Z}$ se prueba que es un múltiplo de 3, y así la proposición es válida para $n + 1$. ■

Ejemplo 23. *Pruebe que* $4^{n-1} + 15n - 16$ *es divisible por* 9 *para todo* $n \in \mathbb{N}$ *con* $n \geq 1$.

Solución. Se procede por inducción:

- Para $n = 1$ es válido, pues $1 + 15 - 16 = 0$, y 0 es divisible por 9.
- Se asume que la proposición es válida para n, es decir, que existe $k \in \mathbb{Z}$ tal que $4^{n-1} + 15n - 16 = 9k$, es decir, $4^{n-1} = 9k - 15n + 16$.
- Se prueba que la proposición es válida para $n + 1$:

$$\begin{aligned} 4^{n+1-1} + 15(n+1) - 16 &= 4 \cdot 4^{n-1} + 15n + 15 - 16 \\ &\overset{H.I.}{=} 4(9k - 15n + 16) + 15n - 1 \\ &= 36k - 60n + 64 + 15n - 1 \\ &= 9\,(4k - 5n + 7) \end{aligned}$$

  Como $4k - 5n + 7$ es un número entero, se prueba que es un múltiplo de 9 y así la proposición es válida para $n + 1$.

Con lo cual se ha demostrado la proposición. ■

En los dos ejemplos siguientes, ponga mucha atención en la prueba y el hecho de que la relación "menor que" es transitiva, es decir, si $a < b$ y $b < c$, entonces $a < c$. Este resultado se utilizará en ambos ejemplos para probar el paso inductivo a $n + 1$.

Ejemplo 24. *Pruebe que la validez, para todo $n \geq 1$, de la desigualdad:*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \frac{n}{2} + 1$$

Solución. Se utiliza el método de inducción:

- Para $n = 1$ es válido, pues $1 \leq \frac{1}{2} + 1$ es verdadera.
- Se asume que la proposición es válida para n, es decir, se toma como Hipótesis de Inducción (H.I.) la validez de:

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \frac{n}{2} + 1 \tag{5.8}$$

- Se debe probar que la proposición es válida para $n+1$, es decir:

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}+\frac{1}{n+1}\leq\frac{n+1}{2}+1 \tag{5.9}$$

Para lograrlo, se prueban primero las proposiciones:

$$\begin{aligned} 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}+\frac{1}{n+1} &\leq \frac{n}{2}+1+\frac{1}{n+1} \quad (5.10)\\ \frac{n}{2}+1+\frac{1}{n+1} &\leq \frac{n+1}{2}+1 \quad (5.11)\end{aligned}$$

La proposición (5.10) se obtiene inmediatamente de la hipótesis de inducción (5.8). Por otro lado, se prueba (5.11):

$$\begin{aligned} & \frac{n}{2}+1+\frac{1}{n+1}\leq\frac{n+1}{2}+1\\ \Longleftrightarrow\quad & \frac{n(n+1)+2}{2(n+1)}\leq\frac{n+1}{2}\\ \Longleftrightarrow\quad & n^2+n+2\leq(n+1)^2\\ \Longleftrightarrow\quad & n^2+n+2\leq n^2+2n+1\\ \Longleftrightarrow\quad & 1\leq n\end{aligned}$$

Al ser una doble equivalencia, y como $1\leq n$ es verdadera, se tiene por verdadera (5.11). Utilizando la transitividad, en las desigualdades (5.10) y (5.11) se obtiene (5.9). Con lo cual se completa la prueba. ■

Ejemplo 25. *Pruebe que para $n\geq 1$ se cumple la desigualdad:*

$$\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{n+(n+1)}\leq\frac{5}{6} \tag{5.12}$$

Solución. Demostrar la desigualdad (5.12) es equivalente a demostrar la desigualdad:

$$\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n+1}\leq\frac{5}{6} \tag{5.13}$$

que sería equivalente, pasando a restar, a la desigualdad:

$$\frac{1}{n+2}+\cdots+\frac{1}{2n+1}\leq\frac{5}{6}-\frac{1}{n+1} \tag{5.14}$$

Se procede por inducción:

- Para $n=1$ es válido, pues $\frac{1}{1+1}+\frac{1}{1+2}=\frac{5}{6}\leq\frac{5}{6}$ es verdadera.
- Se asume que la proposición es válida para n, es decir, se toma como Hipótesis de Inducción (H.I.) la validez de la expresión (5.14).
- Se debe probar que la proposición es válida para $n+1$, es decir:

$$\frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\cdots+\frac{1}{(n+1)+((n+1)+1)}\leq\frac{5}{6}$$

Que sería equivalente a demostrar:

$$\frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{2n+3}\leq\frac{5}{6} \tag{5.15}$$

Primero, note que:

$$\begin{aligned}
& \frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{2n+3} \\
= \quad & \underbrace{\frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{2n+1}}_{\text{se utiliza H.I., desigualdad (5.14)}}+\frac{1}{2n+2}+\frac{1}{2n+3} \\
\overset{(5.14)}{\leq} \quad & \frac{5}{6}-\frac{1}{n+1}+\frac{1}{2n+2}+\frac{1}{2n+3}
\end{aligned}$$

Con lo cual se tiene que:

$$\frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{2n+3}\leq\frac{5}{6}-\frac{1}{n+1}+\frac{1}{2n+2}+\frac{1}{2n+3} \tag{5.16}$$

Por otro lado:

$$\begin{aligned}
& \frac{5}{6} - \frac{1}{n+1} + \frac{1}{2n+2} + \frac{1}{2n+3} \leq \frac{5}{6} \\
\iff \quad & \frac{-1}{n+1} + \frac{1}{2(n+1)} + \frac{1}{2n+3} \leq 0 \\
\iff \quad & \frac{-4n-6+2n+3+2n+2}{2(n+1)(2n+3)} \leq 0 \\
\iff \quad & -1 < 0
\end{aligned}$$

Lo cual es cierto; así, se ha probado que:

$$\frac{5}{6} - \frac{1}{n+1} + \frac{1}{2n+2} + \frac{1}{2n+3} \leq \frac{5}{6} \tag{5.17}$$

Utilizando la transitividad en la desigualdades (5.16) y (5.17), se obtiene (5.14). Con lo cual se completa la prueba. ■

Ejemplo 26. *Determine una fórmula para la siguiente suma:*

$$3 + 10 + 17 + \cdots + (7n-4)$$

Solución. Es claro que la suma es:

$$\sum_{i=1}^{n} 7i - 4 = 7\sum_{i=1}^{n} i - \sum_{i=1}^{n} 4 = 7 \cdot \frac{n(n+1)}{2} - 4n = \frac{n(7n-1)}{2}$$

Así, la fórmula buscada es $3 + 10 + 17 + \cdots + (7n-4) = \frac{n(7n-1)}{2}$. ■

Se denota $\boldsymbol{S_p}$ a la suma de los n primeros números elevados a la potencia p, es decir:

$$S_p = \sum_{i=1}^{n} i^p = 1^p + 2^p + 3^p + \cdots + n^p$$

En el ejercicio 1a), usted debe probar la validez de la fórmula para S_1; en el ejercicio 1f), la de la fórmula para S_2, y en el ejercicio 1g), la de S_3. Por su importancia, se resumen en el siguiente cuadro:

$$S_0 = \sum_{i=1}^{n} 1 = 1 + 1 + 1 + \cdots + 1 = n$$
$$S_1 = \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$
$$S_2 = \sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$
$$S_3 = \sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

En general, se puede obtener la suma S_p si se conocen las anteriores S_1, S_2, S_3, $\ldots$, S_{p-1}. El procedimiento se da en el siguiente ejemplo, y con base en él, usted deberá determinar la fórmula para S_4.

Ejemplo 27. *Como se mencionó anteriormente, en este ejemplo se dará un procedimiento para deducir la fórmula S_2 (ver ejercicio $1f$), conociendo la suma S_1. Para tal propósito, en la conocida fórmula*

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1$$

Al sustituir n por $n-1$; n por $n-2$, $\ldots$, hasta $n=1$ se obtiene:

$$\begin{aligned}
(n+1)^3 &= n^3 + 3n^2 + 3n + 1 \\
n^3 &= (n-1)^3 + 3(n-1)^2 + 3(n-1) + 1 \\
(n-1)^3 &= (n-2)^3 + 3(n-2)^2 + 3(n-2) + 1 \\
\vdots &= \vdots \\
2^3 &= 1^3 + 3 \cdot 1^2 + 3 \cdot 1 + 1
\end{aligned}$$

Al sumar todas estas igualdades, se obtiene la ecuación:

$$(n+1)^3 + n^3 + \cdots + 2^3 = n^3 + \cdots + 2^3 + 1^3 + 3\sum_{i=1}^{n} i^2 + 3\sum_{i=1}^{n} i + n$$

Al cancelar los términos homogéneos, se tiene:

$$(n+1)^3 = 1 + 3S_2 + 3S_1 + n$$

Al despejar S_2 y sustituir la fórmula $S_1 = \frac{n(n+1)}{2}$, el resultado es:

$$\begin{aligned} 3S_2 &= (n+1)^3 - \frac{3}{2}n(n+1) - (n+1) \\ &= \frac{n(n+1)(2n+1)}{2} \end{aligned}$$

Finalmente, se obtiene $S_2 = \frac{n(n+1)(2n+1)}{6}$. ■

Ejemplo 28. *De forma análoga, para determinar S_3, se puede verificar:*

$$(n+1)^4 = 1 + 4S_3 + 6S_2 + 4S_1 + n$$

Al despejar S_3 y sustituir las fórmulas conocidas de S_1 y de S_2, se obtiene la fórmula $S_3 = \frac{n^2(n+1)^2}{4}$. ■

Ejercicios (sección 5.2)

1. Utilice el método de inducción para probar la validez de siguientes igualdades para todo $n \geq 0$ o $n \geq 1$, según corresponda:

   (a) $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$

   (b) $2 + 5 + 8 + \cdots + (3n-1) = \dfrac{n(3n+1)}{2}$

   (c) $3 + 11 + \cdots + (8n-5) = 4n^2 - n$

   (d) $1 \cdot 2 + 2 \cdot 4 + 3 \cdot 8 + \cdots + n \cdot 2^n = 2 + (n-1)2^{n+1}$

   (e) $1 + 9 + 25 + \cdots + (2n-1)^2 = \dfrac{n(2n-1)(2n+1)}{3}$

   (f) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

(g) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$

(h) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$

(i) $\dfrac{1}{2} + \dfrac{3}{4} + \dfrac{5}{8} + \cdots + \dfrac{2n-1}{2^n} = 3 - \dfrac{2n+3}{2^n}$

(j) $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

(k) $1 + a + \cdots + a^{n-1} + a^n = \dfrac{a^{n+1}-1}{a-1}$, si $a \neq 1$

(l) $\dfrac{2}{3} + \dfrac{2}{9} + \cdots + \dfrac{2}{3^n} = 1 - \dfrac{1}{3^n}$

(m) $\dfrac{1}{1\cdot 3} + \dfrac{1}{3\cdot 5} + \cdots + \dfrac{1}{(2n-1)(2n+1)} = \dfrac{n}{2n+1}$

(n) $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$

(o) $\dfrac{1^2}{1\cdot 3} + \dfrac{2^2}{3\cdot 5} + \cdots + \dfrac{n^2}{(2n-1)(2n+1)} = \dfrac{n(n+1)}{2(2n+1)}$

(p) $\dfrac{3}{1\cdot 2\cdot 2} + \dfrac{4}{2\cdot 3\cdot 2^2} + \cdots + \dfrac{n+2}{n(n+1)2^n} = 1 - \dfrac{1}{(n+1)2^n}$

(q) $\displaystyle\sum_{i=2}^{n}(i^2 - i) = \frac{n(n^2-1)}{3}$

(r) $\displaystyle\sum_{i=2}^{n}\frac{1}{\sqrt{i-1}+\sqrt{i}} = \sqrt{n} - 1$

(s) $\displaystyle\sum_{i=1}^{n} i(i!) = (n+1)! - 1$

(t) $\displaystyle\sum_{i=1}^{n}\frac{1}{(4i-3)(4i+1)} = \frac{n}{4n+1}$

(u) $\displaystyle\prod_{i=2}^{n}\left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$

2. Utilice el método de inducción matemática para demostrar que las siguientes proposiciones son verdaderas para todo $n \geq 1$:

(a) $n^4 + 2n^3 + n^2$ es divisible por 4

(b) $n(n+1)(n+2)$ es divisible por 6

(c) $n^3 + 11n$ es divisible por 6

(d) $n^7 - n$ es divisible por 7

(e) $3^{2n+1} + 2^{n+2}$ es divisible por 7

(f) $3^{2n} - 1$ es divisible por 8

(g) $3^n + 7^n - 2$ es divisible por 8

(h) $4^n + 15n - 1$ es divisible por 9

(i) $10^n + 3 \cdot 4^{n+2} + 5$ es divisible por 9

(j) $3^{2n} + 2^{6n-5}$ es divisible por 11

(k) $10^{2n+1} + 1$ es divisible por 11

(l) $4^{2n+1} + 3^{n+2}$ es divisible por 13

(m) $7^{2n} + 16n - 1$ es divisible por 64

3. Utilice el método de inducción matemática para demostrar la validez de las siguientes desigualdades:

(a) $2^n < n!$, para $n \geq 4$

(b) $1 + 2 + 3 + \cdots + n \leq \dfrac{(2n+1)^2}{8}$, para $n \geq 1$

(c) $\dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \cdots + \dfrac{1}{2^n} < n \cdot \ln(2)$, para $n \geq 1$

(d) $1^2 + 2^2 + \cdots + (n-1)^2 < \dfrac{n^3}{3} < 1^2 + 2^2 + \cdots + n^2$, para $n \geq 2$

(e) $1^3 + 2^3 + \cdots + (n-1)^3 < \dfrac{n^4}{4} < 1^3 + 2^3 + \cdots + n^3$, para $n \geq 2$

(f) $\dfrac{1}{n+1} + \dfrac{1}{n+2} + \cdots + \dfrac{1}{2n} > \dfrac{13}{24}$, para $n \geq 2$

(g) $\displaystyle\sum_{i=1}^{n} \frac{2i-1}{2^i} \leq \frac{7}{2} - \frac{2n+3}{2^n}$, para $n \geq 1$

(h) $\sqrt{n} \leq \dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{3}} + \cdots + \dfrac{1}{\sqrt{n}} \leq n\sqrt{n}$, para $n \geq 1$

(i) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1)n < \dfrac{n^2(n+1)}{3}$, para $n \geq 2$

(j) $\dfrac{4^n}{n+1} \leq \dfrac{(2n)!}{(n!)^2}$, para $n \geq 1$

4. Observe y compruebe las siguientes igualdades:

$$\begin{aligned} 1 &= 1 \\ 1-4 &= -(1+2) \\ 1-4+9 &= 1+2+3 \\ 1-4+9-16 &= -(1+2+3+4) \end{aligned}$$

A partir de ellas, determine la fórmula respectiva y pruébela con el método de inducción matemática.

5. Observe y compruebe las siguientes igualdades:

$$\begin{aligned} 1-\frac{1}{2} &= \frac{1}{2} \\ \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) &= \frac{1}{3} \\ \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right) &= \frac{1}{4} \end{aligned}$$

A partir de ellas, determine la fórmula respectiva y pruébela con el método de inducción matemática.

6. Encuentre una fórmula para la suma de los primeros n números positivos que sean múltiplos de 2. Pruébela por inducción. (Sugerencia: observe que $2 = 1 \cdot 2$, $2+4 = 2 \cdot 3$ y $2+4+6 = 3 \cdot 4$).

7. Encuentre una fórmula para la suma de los primeros n múltiplos positivos de 3 y pruébela con el método de inducción matemática. (Sugerencia: observe que $3 = \frac{3}{2} \cdot 1 \cdot 2$, $3+6 = \frac{3}{2} \cdot 2 \cdot 3$).

8. Encuentre una fórmula para la suma $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)}$ y pruébela utilizando el método de inducción matemática.

9. Determine una fórmula para las sumas (repase el ejemplo 26):

   (a) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1)n$

   (b) $2 + 7 + 12 + \cdots + (5n - 3)$

   (c) $1 \cdot 6 + 2 \cdot 7 + 3 \cdot 8 + \cdots + n(n+5)$

10. Calcule el valor exacto de las siguientes sumas:

    (a) $1^2 + 2^2 + 3^2 + \cdots + 10000$

    (b) $\dfrac{1}{1 \cdot 3} + \dfrac{1}{3 \cdot 5} + \cdots + \dfrac{1}{1023}$

    (c) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + 930$

    (d) $1^3 + 2^3 + 3^3 + \cdots + 12167$

    (e) $\dfrac{1}{7} + \dfrac{2}{7^2} + \dfrac{1}{7^3} + \dfrac{2}{7^4} + \cdots + \dfrac{2}{7^{20}}$

    (f) $\dfrac{1}{17 \cdot 21} + \dfrac{1}{21 \cdot 25} + \cdots + \dfrac{1}{397 \cdot 401}$

    (g) $10 \cdot 13 + 11 \cdot 14 + 12 \cdot 15 + \cdots + 1258$

11. Un *cuadrado mágico* de orden n es una distribución de los números 1, 2, 3,. . . , n^2 en forma de cuadrado, donde al sumar los elementos de cada fila, de cada columna y de cada diagonal, se obtiene el mismo resultado, conocida como la suma mágica.

    (a) Compruebe que los cuadrados siguientes son mágicos.

4	9	2
3	5	7
8	1	6

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

    (b) Pruebe que la suma mágica S, en el caso general de un cuadrado mágico de orden n, es $S = \frac{n(n^2+1)}{2}$.

12. En cada caso, determine el criterio de a_i si se sabe que:

    (a) $\displaystyle\sum_{i=1}^{n} a_i = \frac{n^2+3n}{2}$

    (b) $\displaystyle\sum_{i=1}^{n} a_i = \frac{n^3+2n}{3}$

13. Determine una fórmula para S_4 (repase los ejemplos 27 y 28, en la página 286).

14. Si a y b son números enteros, pruebe que $a^n - b^n$ es divisible por $a-b$ para todo $n \in \mathbb{N}$.

15. Considere los cuadrados C_n definidos como $C_1 = 1$, $C_2 = \begin{matrix} 2 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 2 \end{matrix}$,

    $C_3 = \begin{matrix} 3 & 3 & 3 & 3 & 3 \\ 3 & 2 & 2 & 2 & 3 \\ 3 & 2 & 1 & 2 & 3 \\ 3 & 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 3 & 3 \end{matrix}$ y así sucesivamente, donde a C_n se le agrega un borde con el siguiente número para obtener C_{n+1}. Si se denota como S_n la suma de todos los números presentes en C_n, determine la fórmula exacta de S_n.

16. Pruebe que si $n \in \mathbb{N}$, con $n \geq 8$, entonces existen $k \in \mathbb{N}$ y $c \in \mathbb{N}$ tales que $n = 5k + 3c$.

17. Utilice el método de inducción para probar que la desigualdad:

    $$(1+x)^n > 1 + nx$$

    es válida para $n \geq 2$, $x > -1$ y $x \neq 0$.

18. Determine el residuo $R(x)$ que se obtiene al dividir el polinomio $P(x) = 1 + x + x^2 + \cdots + x^{100}$ por el polinomio $x^2 - x - 2$.

19. Pruebe que si el conjunto A tiene n elementos, su conjunto potencia $P(A)$ tiene 2^n elementos.

5.3 Recursividad

En general, una **sucesión** es simplemente una lista de objetos dispuestos en orden: el primer elemento, el segundo elemento, y así sucesivamente; por ejemplo, la sucesión: a, ab, abb, $aabb$, $aabbb$, $\ldots$, donde los puntos suspensivos se leen *y así sucesivamente*, define una colección de tiras o arreglos de las letras a y b, en la cual se puede conjeturar que su sexto término sería $aaabbb$ y el séptimo $aaabbbb$, continuando de la misma forma. En esta sección, lo principal es el caso de las sucesiones numéricas, definidas como funciones con dominio $\mathbb{N}$, es decir:

$$\begin{array}{rcl} f\colon \mathbb{N} & \longrightarrow & \mathbb{R} \\ n & \mapsto & f(n) \end{array}$$

En donde los únicos posibles valores para n son números naturales, por comodidad se denota a la imagen de n por f como a_n, es decir, $\boldsymbol{f(n) = a_n}$. Considere, por ejemplo, la sucesión $1, 4, 9, 16, \ldots$ induce a pensar en una serie numérica en donde el n-ésimo elemento es n^2 y los puntos significan que la sucesión continúa infinitamente; así, el sexto término de esta sucesión es 36, el décimo término es 100, entre otros. La definición de esta sucesión es:

$$\begin{array}{rcl} f\colon \mathbb{N} & \longrightarrow & \mathbb{R} \\ n & \mapsto & f(n) = n^2 \end{array}$$

Simplemente se puede escribir como $a_n = n^2$, con lo cual se obtiene una **fórmula explícita** para su comportamiento.

En otras ocasiones, las sucesiones están definidas de **forma recursiva**, esto es, a_n depende de algunos de los términos anteriores. Es decir, si dependiera de los dos anteriores, para calcular por ejemplo el término a_{10}, es necesario calcular los términos a_9 y a_8 y, para ello, se deben calcular los términos a_7 y a_6 y así sucesivamente hasta llegar a los dos datos iniciales conocidos.

Ejemplo 29. *La sucesión* $F_n = F_{n-1} + F_{n-2}$ *con condiciones iniciales* $F_1 = 1$ *y* $F_2 = 1$ *es claramente recursiva, pues el n-ésimo término depende de los dos anteriores, de manera que se define el término n-ésimo como la suma de los dos términos anteriores y se cumple que* $F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13, \ldots.$ *Esta sucesión se conoce como la sucesión de Fibonacci.* ■

Lo anterior podría llevar algún trabajo si, por ejemplo, se quisiera calcular el valor de F_{200}. Lo ideal sería encontrar una fórmula explícita que permita, de una manera más rápida, determinar cualquier término de la sucesión sin necesidad de conocer los términos anteriores. Para esto, se dan algunas definiciones básicas sobre la clasificación de las sucesiones recursivas; luego, y bajo ciertas condiciones, se verán algunos ejemplos de cómo obtener la fórmula explícita a partir de la recursiva, y viceversa.

Se dice que una relación por recurrencia es:

1. **De orden k** si permite expresar a_n en función de los k términos anteriores, es decir, $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$.

2. **Lineal homogénea de orden k** con coeficientes constantes si permite expresarse por medio de la ecuación

$$A_0a_n + A_1a_{n-1} + A_2a_{n-2} + \cdots + A_ka_{n-k} = 0$$

donde los A_i son constantes.

3. **Lineal no homogénea de orden k** con coeficientes constantes si permite expresarse por medio de la ecuación

$$A_0a_n + A_1a_{n-1} + A_2a_{n-2} + \cdots + A_ka_{n-k} = f(n)$$

donde los A_i son constantes.

Ejemplo 30. *La sucesión definida por recurrencia por* $a_n = 2a_{n-1} + 1$ *es lineal no homogénea, y su orden es* 1. ■

Ejemplo 31. *La sucesión definida por* $b_n = 3b_{n-1} - b_{n-2} + n^2$ *es lineal no homogénea de orden* 2. ■

Ejemplo 32. *La sucesión definida por* $c_n = c_{n-1} + 4c_{n-3}$ *es lineal homogénea de orden* 3. ■

Ejemplo 33. *La sucesión definida por* $U_n = 3n^2U_{n-2} - U_{n-4} + 3$ *es de orden* 4, *no lineal y no homogénea.* ■

Para la relación

$$A_0a_n + A_1a_{n-1} + A_2a_{n-2} + \cdots + A_ka_{n-k} = 0$$

dada por recurrencia, lineal, homogénea de orden k, con coeficientes constantes la ecuación de grado k:

$$A_0x^k + A_1x^{k-1} + A_2x^{k-2} + \cdots + A_{k-1}x + A_k = 0$$

se llamará **ecuación característica** asociada a a_n.

Ejemplo 34. *La ecuación característica asociada a la sucesión definida por recurrencia* $U_n = 3U_{n-1} - U_{n-3}$, *de orden* 3, *es* $x^3 = 3x^2 - 1$. ■

Ejemplo 35. *La sucesión dada por recurrencia* $a_n = a_{n-3} - 4a_{n-5}$, *de orden* 5, *tiene como ecuación característica a* $x^5 = x^2 - 4$. ■

Ejemplo 36. *La sucesión dada por recurrencia* $U_{n+2} = 4U_{n-1} - 3U_{n-2}$, *de orden* 4, *tiene como ecuación característica a* $x^4 = 4x - 3$. ■

En el caso de que el orden sea 2, la ecuación característica se puede escribir como $x^2 - r_1x - r_2 = 0$; en este caso, el siguiente resultado da la forma general de la fórmula explícita en el caso de que las soluciones sean números reales. Esta fórmula dependerá de la naturaleza de sus soluciones, es decir, soluciones diferentes o una única solución. Se omite el caso en que las soluciones sean complejas.

Si $a_n = r_1 a_{n-1} + r_2 a_{n-2}$, lineal homogénea de orden 2 con coeficientes constantes, entonces:

1. Si su ecuación característica es $x^2 - r_1 x - r_2 = 0$, tiene dos soluciones distintas s_1 y s_2; la fórmula explícita es de la forma:
$$a_n = A \cdot s_1^n + B \cdot s_2^n$$
2. Si su ecuación característica es $x^2 - r_1 x - r_2 = 0$, tiene solo una solución s; entonces, la fórmula explícita es de la forma:
$$a_n = A \cdot s^n + B \cdot ns^n$$

donde A y B se determinan por las dos condiciones iniciales.

Ejemplo 37. *Determine una fórmula explícita para la sucesión definida por recurrencia por* $a_n = 2a_{n-1} + 3a_{n-2}$ *con* $a_1 = 3$ *y* $a_2 = 21$.

Solución. La ecuación característica $x^2 - 2x - 3 = 0$ tiene dos soluciones distintas $s_1 = -1$ y $s_2 = 3$; así, la fórmula explícita es de la forma:

$$a_n = A \cdot (-1)^n + B \cdot 3^n \tag{5.18}$$

Para determinar las constantes A y B, se utilizan las dos condiciones iniciales: con $a_1 = 3$ se evalúa (5.18) en $n = 1$ y se obtiene la ecuación $a_1 = A \cdot (-1)^1 + B \cdot 3^1 = 3$; análogamente, con $a_2 = 21$ y evaluando en

$n = 2$, se plantea la ecuación $a_2 = A \cdot (-1)^2 + B \cdot 3^2 = 21$, es decir, se debe resolver el sistema

$$\left\{ \begin{array}{rcr} -A + 3B & = & 3 \\ A + 9B & = & 21 \end{array} \right.$$

cuyas soluciones son $A = 3$ y $B = 2$, con lo cual, la fórmula explícita es $a_n = 3 \cdot (-1)^n + 2 \cdot 3^n$. ■

Ejemplo 38. *Determine una fórmula explícita para la sucesión definida por recurrencia por* $a_n = 6a_{n-1} - 9a_{n-2}$ *con* $a_1 = 0$ *y* $a_2 = -9$.

Solución. La ecuación característica es $x^2 - 6x + 9 = 0$, tiene solamente la solución $s = 3$; así, la fórmula explícita es de la forma:

$$a_n = A \cdot 3^n + B \cdot n \cdot 3^n$$

Para determinar las constantes A y B, se utilizan las dos condiciones iniciales: con $a_1 = 0$ se plantea la ecuación $a_1 = A \cdot 3^1 + B \cdot 1 \cdot 3^1 = 0$ y con $a_2 = -9$ se plantea la ecuación $a_2 = A \cdot 3^2 + B \cdot 2 \cdot 3^2 = -9$, es decir, se debe resolver el sistema

$$\left\{ \begin{array}{rcr} 3A + 3B & = & 0 \\ 9A + 18B & = & -9 \end{array} \right.$$

cuyas soluciones son $A = 1$ y $B = -1$, con lo cual, $a_n = 3^n - n3^n$. ■

El método utilizado en los ejemplos anteriores se puede extender, de forma natural, a los ordenes superiores, como se ilustra en los siguientes ejemplos. Recuerde que todo polinomio de grado mayor o igual a tres se puede factorizar como un producto de factores lineales y factores cuadráticos; como se mencionó anteriormente, se trabajá solamente el caso en que las soluciones de la ecuación característica sean reales.

Ejemplo 39. *Determine una fórmula explícita para la sucesión definida por recurrencia por* $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$ *con* $a_0 = -1$, $a_1 = 10$ *y* $a_2 = -2$.

Solución. La ecuación característica es $x^3-2x^2-5x+6=0$; tiene tres soluciones distintas: $s_1=1$, $s_2=-2$ y $s_3=3$. Así, la fórmula explícita es de la forma:

$$a_n = A\cdot 1^n + B\cdot(-2)^n + C\cdot 3^n$$

Para determinar A, B y C, se utilizan las tres condiciones iniciales dadas: Con $a_0=-1$ se plantea la ecuación $a_0 = A\cdot 1^0 + B\cdot(-2)^0 + C\cdot 3^0 = -1$. Con $a_1=10$ se plantea la ecuación $a_1 = A\cdot 1^1 + B\cdot(-2)^1 + C\cdot 3^1 = 10$. Con $a_2=-2$ se plantea la ecuación $a_2 = A\cdot 1^2 + B\cdot(-2)^2 + C\cdot 3^2 = -2$. Es decir, se resuelve el sistema

$$\left\{\begin{array}{rcr} A+B+C & = & -1 \\ A-2B+3C & = & 10 \\ A+4B+9C & = & -2 \end{array}\right.$$

Su solución es $A=1$, $B=-3$ y $C=1$; por lo tanto, la fórmula explícita es $a_n = 1-3\cdot(-2)^n+3^n$. ■

Ejemplo 40. *Determine una fórmula explícita para la sucesión definida por recurrencia por* $a_n = a_{n-1}+a_{n-2}-a_{n-3}$ *con* $a_0=6$, $a_1=1$ *y* $a_2=12$. *Además, utilice ambas fórmulas para calcular el valor de* a_5.

Solución. La ecuación característica es $x^3 = x^2+x-1$. Al igualar a cero y factorizar, se obtiene la ecuación $(x-1)^2(x+1)=0$, la cual tiene tres soluciones: $s_1=1$, $s_2=1$ y $s_3=-1$. Así, la fórmula explícita es de la forma:

$$a_n = A\cdot 1^n + B\cdot n\cdot 1^n + C\cdot(-1)^n$$

Para determinar A, B y C, se utilizan las tres condiciones iniciales dadas: Para $n=0$, con $a_0=6$, se plantea la ecuación $A+C=6$; para $n=1$, con $a_1=1$, se plantea la ecuación $A+B-C=1$; por último, para $n=2$, con $a_2=12$, se obtiene la ecuación $A+2B+C=12$, es decir, se resuelve el sistema

$$\left\{\begin{array}{rcl} A+C & = & 6 \\ A+B-C & = & 1 \\ A+2B+C & = & 12 \end{array}\right.$$

Su solución es $A = 2$, $B = 3$ y $C = 4$. Así, se concluye que la fórmula explícita es $a_n = 2+3n+4\cdot(-1)^n$. Para calcular el valor de a_5 utilizando la fórmula recursiva, se tiene que $a_0 = 6$, $a_1 = 1$, $a_2 = 12$, $a_3 = 12+1-6 = 7$, $a_4 = 7+12-1 = 18$ y $a_5 = 18+7-12 = 13$. Utilizando la fórmula explícita, se obtiene $a_5 = 2+15-4 = 13$. ■

Ejemplo 41. *Determine la fórmula por recurrencia para la relación b_n definida explícitamente por $b_n = 2\cdot 3^n + 2 + n$, para $n \geq 0$.*

Solución. Se observa que $b_n = 2\cdot 3^n + 2 + n = 2\cdot 3^n + 2\cdot(1)^n + n(1)^n$. Así, las soluciones de la ecuación característica asociada a la ecuación por recurrencia son $s_1 = 3$, $s_2 = 1$ y $s_3 = 1$, y la ecuación característica es $(x-3)(x-1)^2 = 0$. Al desarrollar el lado izquierdo de esta ecuación, se obtiene $x^3 - 5x^2 + 7x - 3 = 0$, al despejar el término de mayor exponente, se tiene $x^3 = 5x^2 - 7x + 3$, con lo cual se determina la relación por recurrencia $b_n = 5b_{n-1} - 7b_{n-2} + 3b_{n-3}$. Para completar, basta encontrar los valores de las condiciones iniciales, para lo cual se evalúa $n = 0$, $n = 1$ y $n = 2$ en $b_n = 2\cdot 3^n + 2 + n$, y se obtiene que $b_0 = 4$, $b_1 = 9$, $b_2 = 22$. Por lo que, finalmente, la relación por recurrencia es $b_n = 5b_{n-1} - 7b_{n-2} + 3b_{n-3}$, para $n \geq 3$, con $b_0 = 4$, $b_1 = 9$, $b_2 = 22$. ■

Los próximos dos ejemplos se consideran sucesiones que no son homogéneas; por lo tanto, para ellas no es posible utilizar el procedimiento estudiado en los ejemplos anteriores, por lo que se debe proceder de forma diferente.

Ejemplo 42. *Determine una fórmula explícita para la sucesión definida por recurrencia por $a_n = a_{n-1} + 5$ con $a_1 = 3$.*

Solución. Proceda con un análisis *hacia atrás* y observe que:

$$\begin{aligned}
a_n &= a_{n-1} + 5 = a_{n-1} + 1\cdot 5 \\
&= (a_{n-2} + 5) + 5 = a_{n-2} + 2\cdot 5 \\
&= ((a_{n-3} + 5) + 5) + 5 = a_{n-3} + 3\cdot 5 \\
&\;\vdots
\end{aligned}$$

Con lo cual se puede conjeturar que $a_n = 3 + (n-1) \cdot 5$. Ahora, se procede a probar esta conjetura, para lo cual se utiliza el método de inducción:

- Para $n = 1$ es válido, pues $a_1 = 3 + (1-1) \cdot 5 = 3 + 0 = 3$.
- Se asume que la proposición es válida para n, es decir, se toma como Hipótesis de Inducción (H.I.) que $a_n = 3 + (n-1) \cdot 5$.
- Se debe probar que la proposición es válida para $n+1$, es decir:

  $$a_{n+1} = 3 + n \cdot 5$$

  Esto se prueba como sigue:

  $$\begin{aligned} a_{n+1} &= a_n + 5 \\ &\overset{H.I.}{=} (3 + (n-1) \cdot 5) + 5 \\ &= 3 + n \cdot 5 - 5 + 5 \\ &= 3 + n \cdot 5 \end{aligned}$$

  Así, la proposición es válida para $n+1$.

con lo cual, la fórmula explícita $a_n = 3 + (n-1) \cdot 5$ para $n \geq 1$ y la recursiva $a_n = a_{n-1} + 5$ con $a_1 = 3$ definen la misma sucesión. ■

Ejemplo 43. *Determine una fórmula explícita para la sucesión definida por recurrencia por $a_n = 2a_{n-1} + 1$ con $a_1 = 3$.*

Solución. Proceda con un análisis *hacia adelante* y observe el siguiente comportamiento:

$$\begin{aligned} a_1 &= 3 \\ a_2 &= 2a_1 + 1 = 2 \cdot 3 + 1 \\ a_3 &= 2a_2 + 1 = 2(2 \cdot 3 + 1) + 1 = 2^2 \cdot 3 + 2 + 1 \\ a_4 &= 2a_3 + 1 = 2(2^2 \cdot 3 + 2 + 1) + 1 = 2^3 \cdot 3 + 2^2 + 2 + 1 \\ &\vdots \end{aligned}$$

Con lo cual se puede conjeturar que:

$$a_n \quad = \quad 2^{n-1} \cdot 3 + 2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2 + 1$$

Utilizando el resultado dado en el ejercicio 1j de la sección 5.2, la fórmula se puede reescribir como:

$$\begin{aligned} a_n &= 3 \cdot 2^{n-1} + 2^{n-1} - 1 \\ &= 4 \cdot 2^{n-1} - 1 \\ &= 2^{n+1} - 1 \end{aligned}$$

Ahora, se debe probar esta conjetura.

- Para $n = 1$ es válido, pues $a_1 = 2^2 - 1 = 3$.
- Se asume que la proposición es válida para n, es decir, la Hipótesis de Inducción (H.I.) es $a_n = 2^{n+1} - 1$.
- Se debe probar que la proposición es válida para $n + 1$, es decir:

  $$a_{n+1} = 2^{n+2} - 1$$

  esto se prueba como sigue:

  $$\begin{aligned} a_{n+1} &= 2a_n + 1 \\ &\overset{H.I.}{=} 2 \cdot (2^{n+1} - 1) + 1 \\ &= 2 \cdot 2^{n+1} - 2 + 1 \\ &= 2^{n+2} - 1 \end{aligned}$$

  Así, la proposición es válida para $n + 1$.

Con lo cual, la fórmula explícita $a_n = 2^{n+1} - 1$ para $n \geq 1$ y por recurrencia $a_n = 2a_{n-1} + 1$ con $a_1 = 3$ definen la misma sucesión. ■

Para finalizar esta sección, se presentan algunas aplicaciones de la recursividad al análisis numérico, principalmente para aproximar las soluciones de una ecuación.

Una manera de determinar el *punto fijo* p de una función f, es decir, el punto p que satisface la igualdad $f(p) = p$ (véase página 228), es utilizando la fórmula recursiva dada por:

$$p_{n+1} = f(p_n)$$

donde el valor inicial p_0 se escoge adecuadamente. La sucesión p_0, p_1, p_2,... se irá aproximando al valor de p.

Ejemplo 44. *Aproxime, utilizando el algoritmo del punto fijo, la solución de la ecuación $x^3 + x - 5 = 0$, de manera que tenga al menos* 5 *decimales exactos.*

Solución. Al despejar y reescribir la ecuación $x^3+x-5 = 0$ en la forma $x = f(x)$, se obtiene que $x^3 = 5 - x$, es decir, $x = \sqrt[3]{5-x}$; por lo tanto, la solución buscada es el punto fijo de la función $f(x) = \sqrt[3]{5-x}$. Al tomar, por ejemplo, $p_0 = 1$ como aproximación inicial, se obtiene:

$$\begin{aligned}
p_1 &= f(1) \approx 1{,}58740105197\\
p_2 &= f(p_1) \approx 1{,}50554965674\\
p_3 &= f(p_2) \approx 1{,}51749158397\\
p_4 &= f(p_3) \approx 1{,}51576098691\\
p_5 &= f(p_4) \approx 1{,}51601202599\\
p_6 &= f(p_5) \approx 1{,}51597561561\\
p_7 &= f(p_6) \approx 1{,}51598089663\\
p_8 &= f(p_7) \approx 1{,}51598013067
\end{aligned}$$

Note que las aproximaciones iteradas se van estabilizando, de manera que el valor p_7 tiene 4 decimales exactos y p_8 ya tiene 6 decimales exactos. ■

Por supuesto que la forma de despejar la ecuación para reescribirla de la forma $x = f(x)$ no es única. En la ecuación $x^3 + x - 5 = 0$ del ejemplo anterior, se pudo haber iniciado con $x(x^2 + 1) = 5$ para finalmente obtener $x = \frac{5}{x^2+1}$ y, por lo tanto, se hubiera tenido que aproximar el punto fijo de la función $f(x) = \frac{5}{x^2+1}$.

Una fórmula recursiva, conocida en el análisis númerico que se utiliza para obtener una *aproximación* racional de la raíz k-ésima de un número A, es decir, de $\sqrt[k]{A}$, viene dada por:

$$a_{n+1} = \frac{1}{k}\left((k-1)a_n + \frac{A}{a_n^{k-1}}\right) \tag{5.19}$$

donde el valor inicial a_0 se escoge convenientemente.

Ejemplo 45. *Utilice la fórmula anterior, utilizando* 3 *iteraciones, para aproximar el valor de* $\sqrt{7}$.

Solución. La fórmula (5.19) para $k = 2$ y $A = 7$ es:

$$a_{n+1} = \frac{1}{2}\left(a_n + \frac{7}{a_n}\right) \tag{5.20}$$

en donde es posible escoger $a_0 = 2$, y así se obtiene:

$$\begin{aligned}
a_1 &= \frac{1}{2}\left(2 + \frac{7}{2}\right) = \frac{11}{4} \\
a_2 &= \frac{1}{2}\left(\frac{11}{4} + \frac{7}{\frac{11}{4}}\right) = \frac{233}{88} \\
a_3 &= \frac{1}{2}\left(\frac{233}{88} + \frac{7}{\frac{233}{88}}\right) = \frac{108497}{41008} \approx 2{,}64575204
\end{aligned}$$

Note que el valor encontrado al utilizar la fórmula coincide con el valor exacto en los primeros 5 decimales. Por supuesto, se puede iniciar con un valor diferente de $a_0 = 2$. ■

Ejercicios (sección 5.3)

1. Determine el valor de a_4 para cada una de las sucesiones siguientes:

   (a) $a_n = 2a_{n-1} + a_{n-2}$ si $n \geq 3$, $a_1 = 3$, $a_2 = -2$.

   (b) $a_n = n^2 a_{n-1}$ si $n \geq 2$, $a_1 = 1$.

   (c) $a_n = a_{n-1}^2 + 3n$ si $n \geq 2$, $a_1 = 2$.

   (d) $a_n = a_{n-1} - a_{n-2} + a_{n-3}$ si $n \geq 3$, $a_0 = 4$, $a_1 = 7$, $a_2 = 6$.

2. Determine la fórmula explícita de las relaciones de orden 2:

   (a) $a_n = 5a_{n-1} + 6a_{n-2}$ si $n \geq 2$, $a_0 = 2$, $a_1 = -1$.

   (b) $a_n = a_{n-1} + 6a_{n-2}$ si $n \geq 2$, $a_0 = 1$, $a_1 = -2$.

   (c) $a_n = 3a_{n-1} - 2a_{n-2}$ si $n \geq 3$, $a_1 = 5$, $a_2 = 3$.

   (d) $a_n = 6a_{n-1} - 9a_{n-2}$ si $n \geq 2$, $a_0 = 1$, $a_1 = 3$.

   (e) $a_n = \frac{1}{2}a_{n-1} + \frac{1}{2}a_{n-2}$ si $n \geq 3$, $a_1 = 3$, $a_2 = 5$.

3. Determine la fórmula explícita de las relaciones de orden 3:

   (a) $b_n = -b_{n-1} + b_{n-2} + b_{n-3}$ si $n \geq 3$, $b_0 = 5$, $b_1 = -2$, $b_2 = 7$.

   (b) $b_n = -b_{n-1} + 8b_{n-2} + 12b_{n-3}$ si $n \geq 3$, $b_0 = 3$, $b_1 = -2$, $b_2 = 46$.

   (c) $U_n = 3U_{n-2} + 2U_{n-3}$ si $n \geq 3$, $U_0 = 5$, $U_1 = 3$, $U_2 = 16$.

   (d) $c_n = -3c_{n-1} - 3c_{n-2} - c_{n-3}$ si $n \geq 3$, $c_0 = 2$, $c_1 = -4$, $c_2 = 8$.

   (e) $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ si $n \geq 3$, $a_0 = 2$, $a_1 = 9$, $a_2 = 11$.

   (f) $a_n = a_{n-1} + a_{n-2} - a_{n-3}$ si $n \geq 3$, $a_0 = 6$, $a_1 = 1$, $a_2 = 12$.

   (g) $b_n = 6b_{n-1} - 12b_{n-2} + 8b_{n-3}$ si $n \geq 4$, $b_1 = 0$, $b_2 = -44$, $b_3 = -240$.

4. Determine la fórmula explícita de las relaciones de orden 4:

   (a) $a_n = 5a_{n-1} - 6a_{n-2} - 4a_{n-3} + 8a_{n-4}$ si $n \geq 4$, $a_0 = 2$, $a_1 = 1$, $a_2 = 13$, $a_3 = 55$.

(b) $a_n = -8a_{n-1} - 22a_{n-2} - 24a_{n-3} - 9a_{n-4}$ si $n \geq 4$, $a_0 = 4$, $a_1 = -6$, $a_2 = 4$, $a_3 = 22$.

5. Determine la fórmula por recurrencia para las siguientes relaciones dadas en su forma explícita:

   (a) $U_n = 2(-3)^n - 5n(-3)^n$ para $n \geq 1$.

   (b) $a_n = 5 + (-2)^n$ para $n \geq 0$.

   (c) $U_n = (-2)^n - 3(2)^n + 3^n$ para $n \geq 1$.

   (d) $a_n = -2^n + 3n2^n + n^2 2^n + 5 + n$ para $n \geq 0$.

6. Considere $a_n = 5a_{n-1} - 6a_{n-2}$, si $n \geq 2$, con $a_0 = -1$, $a_1 = 0$.

   (a) Utilice esta fórmula para encontrar el valor de a_4 y a_7.

   (b) Determine la fórmula explícita para esta relación y utilícela para encontrar el valor de a_4 y a_7.

7. Para la siguiente sucesión: $0, 1, \frac{1}{2}, \frac{3}{4}, \frac{5}{8}, \frac{11}{16}, \ldots$, cada uno de los números que aparecen, salvo los dos primeros, es el promedio de los dos términos anteriores. Encuentre su criterio en forma recursiva y su fórmula explícita.

8. Considere la sucesión de Fibonacci $F_n = F_{n-1} + F_{n-2}$ para todo $n \geq 3$, con $F_1 = 1$ y $F_2 = 1$ como condiciones iniciales.

   (a) Utilice esta fórmula para encontrar el valor de F_4 y de F_{15}.

   (b) Calcule su fórmula explícita y verifique que es:

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

   (c) Utilice la fórmula explícita para comprobar que $F_3 = 2$ y que $F_4 = 3$.

9. Clasifique en números pares o impares los números de Fibonacci F_5, F_{12} y F_{4311}.

10. Sea F_n la sucesión de Fibonacci, pruebe, que $F_n < \left(\frac{7}{4}\right)^n$, $\forall n \geq 1$.

11. Sea F_n la sucesión de Fibonacci, pruebe utilizando el método de inducción, que $\displaystyle\sum_{k=1}^{n} F_k^2 = F_n \cdot F_{n+1}$.

12. Determine la fórmula explícita y pruébela por inducción para la sucesión definida por recurrencia por $a_n = 3a_{n-1} + 1$ con $a_1 = 5$.

13. Utilice la fórmula (5.19) con 4 iteraciones para obtener una aproximación de $\sqrt[3]{5}$, para ello utilice $a_0 = 1$. Luego, compare con el valor que se obtiene utilizando la calculadora.

14. Utilice el método del punto fijo (repase el ejemplo 44, página 302) para obtener una aproximación de la solución de la ecuación

$$x^5 + 2x^3 - 8 = 0$$

que cuente con 5 decimales exactos.

15. Una fórmula recursiva, conocida en el análisis numérico como el **método de la secante**, que se utiliza para obtener una aproximación racional de la solución de la ecuación $f(x) = 0$, es:

$$x_{n+1} = x_n - \frac{f(x_n)}{f(x_n) - f(x_{n-1})}\,(x_n - x_{n-1}) \tag{5.21}$$

donde los valores iniciales x_0, x_1 se escogen convenientemente. Utilice la fórmula (5.21) con 4 iteraciones para obtener una aproximación de las soluciones de las ecuaciones:

(a) $x^3 + x - 5 = 0$.

(b) $x^5 + 2x^3 = 8$.

Capítulo 6

Estructuras algebraicas

"He descubierto cosas tan maravillosas
que me dejaron atónito...
de la nada he creado un extraño universo".

Janos Bolyai

En este capítulo se introducen los conceptos de operación interna, estructura algebraica, subgrupos, grupos, homomorfismo de grupos, entre otros. Como se trata de un tópico muy amplio, se realizará solamente una breve introducción.

Para profundizar en el tema tratado en este capítulo, es recomendable consultar las referencia bibliográficas [13], [15], [16], [20] y [32].

6.1 Estructuras algebraicas

Sea $\mathcal{E}$ un conjunto no vacío, una función f

$$f : \mathcal{E} \times \mathcal{E} \longmapsto \mathcal{E}$$

Se llama **ley de composición interna** (operación) sobre $\mathcal{E}$ sobre $\mathcal{E}$. Además, la imagen $f(a, b)$ se llama el operado de a y b.

Es usual representar las operaciones internas con algunos símbolos especiales, en vez de letras, como $*$, $\triangle$, $\perp$, entre otros.

Note que, por definición, si $*$ es una ley de composición interna sobre $\mathcal{E}$, entonces es **cerrada** sobre $\mathcal{E}$, es decir, se cumple que:

$$\forall a, b \in \mathcal{E}\ [a * b \in \mathcal{E}]$$

Si $*$ es una ley de composición interna sobre $\mathcal{E}$, se dice que $(\mathcal{E}, *)$ posee una **estructura algebraica**.

Ejemplo 1. *La operación usual de adición sobre* $\mathbb{R}$ *que se representa con* $+$ *es la función:*

$$+: \ \mathbb{R} \times \mathbb{R} \longmapsto \mathbb{R}$$

De manera que $+(a,b) = a+b$, *donde* $a+b$ *es la suma de* a *y* b. *De la misma forma, multiplicación se representa con* $\times$. *Ambas son leyes de composición interna definidas sobre* $\mathbb{R}$. ■

Ejemplo 2. *La función* $*: \ \mathbb{N} \times \mathbb{N} \longmapsto \mathbb{N}$, *definida como*

$$a * b = a^2 + b^2$$

es una ley de composición interna sobre $\mathbb{N}$. *Algunos ejemplos de aplicación son* $2 * 5 = 29$ *y* $(2 * 2) * 3 = 8 * 3 = 73$. ■

Ejemplo 3. *La sustracción de dos números* a *y* b, *definida como* $a - b$, *no es una ley de composición interna sobre* $\mathbb{N}$, *ya que, por ejemplo,* 2 *y* 4 *pertenecen a* $\mathbb{N}$, *sin embargo,* $2 - 4 = -2$ *y* $-2 \notin \mathbb{N}$. *Note que sí puede ser una ley de composición interna si se define sobre* $\mathbb{Z}$. ■

Si $*$ es una ley de composición interna sobre $\mathcal{E}$, se dice que $*$:

- Es **asociativa** si $\forall a, b, c \in \mathcal{E}$ se cumple:

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

- Posee **elemento neutro** si $\exists e \in \mathcal{E} \ \forall a \in \mathcal{E}$ tal que:

$$a * e = e * a = a$$

- Tiene **elementos inversos** si $\forall a \in \mathcal{E} \ \exists b \in \mathcal{E}$ tal que:

$$a * b = b * a = e$$

  en cuyo caso se escribe $a^{-1} = b$.

- Es **conmutativa** si $\forall a, b \in \mathcal{E} \ [a * b = b * a]$.

Es importante observar que si el elemento neutro existe, éste será único; por el contrario, los elementos inversos cambian para cada elemento.

Ejemplo 4. *Considere en* $G = \mathbb{R} - \{0\}$ *la operación* $*$ *definida por*

$$a * b = a^2 \cdot b$$

Analice cuáles propiedades se satisfacen en $(G, *)$.

Solución. En primer lugar, claramente es cerrada, pues si a y b son números reales diferentes de cero, $a * b = a^2 \cdot b \in \mathbb{R} - \{0\}$. No es asociativa pues, por ejemplo, $(2 * 2) * 3 = 8 * 3 = 192$, mientras que $2 * (2 * 3) = 2 * 12 = 48$. No tiene neutro pues, si e fuera el neutro, $a * e = a \Leftrightarrow a^2 \cdot e = a \Leftrightarrow a \cdot e = 1$, con lo que $e = \frac{1}{a}$ y dependería de cada valor de a, lo cual no puede ser, ya que el neutro debe servir para todos los elementos. Al no tener neutro, no hay inversos. Tampoco es conmutativa pues, por ejemplo, $2 * 3 = 12$, mientras que $3 * 2 = 18$. ■

En el caso de que $\mathcal{E}$ sea un conjunto finito, es decir, $\mathcal{E} = \{a_1, a_2, \ldots, a_n\}$, la operación $*$ se puede representar en una **tabla**, donde la entrada i-j denota al elemento $a_i * a_j$:

$*$	a_1	a_2	$\ldots$	a_j	$\ldots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

Ejemplo 5. *En el conjunto* $\mathcal{E} = \{1, 2, 5\}$ *se define la operación* $*$ *para todo* a *y* b *en* $\mathcal{E}$ *por* $a * b = k$, *donde* k *es el resto de la división de* a^b *por* 3. *Construya la tabla para esta ley y analice si tiene elemento neutro, si es conmutativa y si es asociativa.*

Solución. La tabla es:

$*$	1	2	5
1	1	1	1
2	2	1	2
5	2	1	2

Se observa que no tiene neutro por la derecha ni por la izquierda; así, no tiene neutro. La estructura no es asociativa pues, por ejemplo, $(2*1)*2 = 1 \neq 2 = 2*(1*2)$. No es conmutativa, ya que $2*1 = 2 \neq 1 = 1*2$. ■

Si $*$ es una ley de composición interna sobre $\mathcal{E}$, se dice que un elemento h es absorbente por la izquierda si $h*a = h$, y lo es por la derecha si $a*h = h$ para todo $a \in \mathcal{E}$. Se dice que es el elemento **absorbente** si lo es por la derecha y por la izquierda.

Ejemplo 6. *La estructura* $(\mathbb{R}, +)$ *no tiene elemento absorbente, mientras que* 0 *es el absorbente en* $(\mathbb{R}, \cdot)$. *(Véase ejemplo* 49 *de página* 89*).*

Ejemplo 7. *En la estructura algebraica del ejemplo* 5*, se observa que* 1 *es elemento absorbente por la izquierda, no posee elemento absorbente por la derecha.* ■

Dada una estructura algebraica $(\mathcal{E}, *)$, se dice que $\boldsymbol{a}$ es un **elemento idempotente** si $a*a = a$.

Ejemplo 8. *La estructura algebraica* $(\mathbb{R}, *)$*, con* $a*b = a+3b-1$*, tiene como elemento idempotente al* $\frac{1}{3}$*, pues resolver* $a*a = a$ *equivale a la ecuación* $a+3a-1 = a$*, cuya solución es precisamente* $a = \frac{1}{3}$. ■

Dada una estructura algebraica $(\mathcal{E}, *)$ que posee elemento neutro e, se dice que $\boldsymbol{a}$ es un **elemento involutivo** si $a*a = e$.

Ejemplo 9. *Para la estructura algebraica* $(\mathbb{R}, \cdot)$ *con* $a \cdot b$ *el producto habitual de los números reales. Si existen, determine los elementos involutivos e idempotentes.*

Solución. Es claro que el elemento neutro es $e = 1$; de esta forma, para encontrar los elementos involutivos se debe resolver $a \cdot a = 1$, que equivale a la ecuación $a^2 = 1$, cuyas soluciones $a = -1$ y $a = 1$. Para encontrar los elementos idempotentes se debe resolver $a \cdot a = a$, que equivale a la ecuación $a^2 - a = 0$, cuyas soluciones son $a = 0$ y $a = 1$.■

Dada una estructura algebraica $(\mathcal{E}, *)$ tal que $a \in \mathcal{E}$, se dice que $\boldsymbol{a}$ es un **elemento central** si conmuta con todos los elementos de $\boldsymbol{\mathcal{E}}$, es decir, a es central si $\forall b \in \mathcal{E}, a * b = b * a$. El conjunto formado por todos los elementos centrales se llama el **centro** de $\mathcal{E}$ y se denota por $\boldsymbol{C(\mathcal{E})}$.

Ejemplo 10. *En el conjunto* $\mathcal{E} = \{0, 2, 4, 6, 8\}$ *se define una ley de composición interna* $*$ *por medio de la tabla:*

$*$	0	2	4	6	8
0	8	4	0	6	2
2	4	0	2	6	4
4	0	2	4	6	8
6	6	6	6	6	6
8	2	0	8	6	4

Determine el neutro, los elementos absorbentes, involutivos, idempotentes y los centrales de $(\mathcal{E}, *)$ *y el centro de* $\mathcal{E}$*.*

Solución. En primer lugar, note que en 6 es el absorbente, ya que $\forall a \in \mathcal{E}$ se cumple que $a * 6 = 6 * a = 6$. El elemento neutro es el 4; de esta forma, se concluye que los involutivos son 4 y 8, pues $4 * 4 = 4$ y $8 * 8 = 4$. Los idempotentes son 4 y 6, pues $4 * 4 = 4$ y $6 * 6 = 6$, los elementos centrales son 0, 4 y 6; así, $C(\mathcal{E}) = \{0, 4, 6\}$. ■

Ejemplo 11. *Considere la operación* $\perp$ *definida sobre* $\mathbb{R}^*$ *dada por:*

$$a \perp b = 5ab$$

Pruebe que esta ley de composición interna es asociativa, conmutativa, posee elemento neutro y todos los elementos tienen inverso.

Solución. Es asociativa, pues:

$$(a \perp b) \perp c = (5ab) \perp c = 5(5ab)c = 25abc$$

Y claramente es igual a:

$$a \perp (b \perp c) = a \perp (5bc) = 5a(5bc) = 25abc$$

Para determinar el elemento neutro e, se debe cumplir $a \perp e = a$, es decir, se debe resolver la ecuación $5ae = a$, dado que el universo es $\mathbb{R}^*$; es claro que $a \neq 0$ y se puede cancelar de la ecuación, con lo cual $e = \frac{1}{5}$ es el neutro. Para determinar el inverso de a, se debe analizar $a \perp b = \frac{1}{5}$, es decir, $5ab = \frac{1}{5}$, de donde se obtiene que $b = \frac{1}{25a}$; de este modo, $a^{-1} = \frac{1}{25a}$. Por último, es conmutativa, pues $a \perp b = 5ab = 5ba = b \perp a$. ■

Ejemplo 12. *Sea* $S = \{a, b\}$*. Sobre* $P(S)$*, el conjunto potencia de* S*,*

$$P(S) = \big\{\varnothing, \{a\}, \{b\}, S\big\}$$

Se define la diferencia simétrica $\triangle$ *como su ley de composición interna que, como se indicó en la sección* 2.1*, es:*

$$A \triangle B = (A - B) \cup (B - A)$$

Para obtener la tabla de operación, es necesario operar cada elemento de $P(S)$ *con cada elemento de* $P(S)$*; por ejemplo, se opera* $\varnothing \triangle \{a\} = \{a\}$*,* $\{a\} \triangle \{b\} = S$ *y* $S \triangle \{a\} = \{b\}$*. Así se obtiene la siguiente tabla:*

$\triangle$	$\varnothing$	$\{a\}$	$\{b\}$	S
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	S
$\{a\}$	$\{a\}$	$\varnothing$	S	$\{b\}$
$\{b\}$	$\{b\}$	S	$\varnothing$	$\{a\}$
S	S	$\{b\}$	$\{a\}$	$\varnothing$

Es claro que es conmutativa y que $\varnothing$ es el elemento neutro; además, cada elemento es su propio inverso; por ejemplo, $\{b\}^{-1} = \{b\}$, pues $\{b\} \triangle \{b\} = \varnothing$. ■

Ejemplo 13. *Analice las propiedades que satisface la operación $*$ definida sobre $\mathbb{N}$ por:*

$$a * b = a + b^2$$

Solución. Esta operación no es asociativa pues, por ejemplo, $(2*2)*3 = 6*3 = 15$, mientras que $2*(2*3) = 2*11 = 123$. Tampoco es conmutativa pues, por ejemplo, $2*3 = 11$ mientras que $3*2 = 7$. Como no es conmutativa, se debe analizar por la derecha y por la izquierda para determinar el neutro e: por la derecha se debe resolver $a * e = a$, es decir, $a + e^2 = a$, de donde $e = 0$ es neutro derecho; por otro lado, para encontrar el neutro por la izquierda $e * a = a$, es decir, es necesario resolver $e + a^2 = a$. Dado que la solución sería $e = a - a^2$ y no pertenece a $\mathbb{N}$, no tiene neutro a la izquierda. Al no tener elemento neutro, no tiene inversos. ■

Ejemplo 14. *Considere la siguiente operación interna $*$ con criterio*

$$x * y = \frac{x+y}{1-xy}$$

definida siempre que $xy \neq 1$, para evitar la división por cero. Demuestre que la ley $*$ es asociativa, conmutativa, posee elemento neutro e inversos.

Solución. Calculando, se obtiene que:

$$(x*y)*z = \frac{x+y}{1-xy} * z = \frac{\frac{x+y}{1-xy} + z}{1 - \left(\frac{x+y}{1-xy}\right) z} = \frac{x+y+z-xyz}{1-xy-xz-yz} \tag{6.1}$$

De la misma forma:

$$x * (y * z) = x * \frac{y+z}{1-yz} = \frac{x + \frac{y+z}{1-yz}}{1 - x\left(\frac{y+z}{1-yz}\right)} = \frac{x+y+z-xyz}{1-xy-xz-yz} \qquad (6.2)$$

Con lo cual, de (6.1) y (6.2) se cumple que $x * (y * z) = x * (y * z)$, es decir, la operación $*$ es asociativa. Además:

$$\begin{aligned} x * y &= \frac{x+y}{1-xy} \\ &= \frac{y+x}{1-yx} = y * x \end{aligned}$$

y se verifica que $*$ es conmutativa. Por último, al despejar la ecuación $x*y = x$, se obtiene que 0 es el elemento neutro, y al despejar la ecuación $x * y = 0$, se obtiene que el inverso de x es $-x$. ■

Ejemplo 15. *Sobre $\mathbb{Z}$ se define (ver ejemplo 36 de la sección 3.3) la relación $\mathcal{R}$ por:*

$$a\mathcal{R}b \Leftrightarrow [\exists k \in \mathbb{Z} \quad tal\ que \quad a - b = 3k]$$

Construya una tabla de operación para el conjunto cociente $\mathbb{Z}/\mathcal{R}$ para la operación $\oplus$, suma de clases, dada por:

$$\overset{\bullet}{a} \oplus \overset{\bullet}{b} = \overset{\bullet}{(a+b)}$$

Es decir, la suma de dos clases es la clase de la suma. Estudie las propiedades de la estructura algebraica.

Solución. El conjunto cociente $\mathbb{Z}/\mathcal{R}$ está formado por tres elementos: $\overset{\bullet}{0}$ es el conjunto de números múltiplos de 3; $\overset{\bullet}{1}$ es el conjunto de números de la forma $3k+1$, y $\overset{\bullet}{2}$ es el conjunto de números de la forma $3k+2$, con $k \in \mathbb{Z}$. A partir de la definición de $\oplus$, se tiene, por ejemplo, que $\overset{\bullet}{0} \oplus \overset{\bullet}{1} = \overset{\bullet}{(0+1)} = \overset{\bullet}{1}$ y también $\overset{\bullet}{1} \oplus \overset{\bullet}{2} = \overset{\bullet}{(1+2)} = \overset{\bullet}{3} = \overset{\bullet}{0}$. De la misma forma se calculan los demás resultados, y con ellos se obtiene la tabla:

$\oplus$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{0}$	$\dot{1}$

Así, el neutro en $\mathbb{Z}/\mathcal{R}$ es $\dot{0}$; el inverso de $\dot{0}$ es $\dot{0}$, es decir, $\left(\dot{0}\right)^{-1}=\dot{0}$; el inverso de $\dot{1}$ es $\dot{2}$, es decir, $\left(\dot{1}\right)^{-1}=\dot{2}$ y, análogamente, $\left(\dot{2}\right)^{-1}=\dot{1}$. Por último, esta operación es asociativa y conmutativa. ■

Ejercicios (sección 6.1)

1. Determine si el conjunto $\mathbb{R}^*$ con la operación $a * b = a + b + 2$ es una estructura algebraica.

2. En el conjunto $\mathcal{E} = \{0, 1, 5\}$ se define la operación $*$ por la tabla:

$*$	0	1	5
0	0	1	5
1	1	5	0
5	5	0	1

   Determine si tiene elemento neutro, absorbente, si es conmutativa o asociativa.

3. En el conjunto $\mathcal{E} = \{0, 1, 5, 7\}$ se define $*$ por la tabla:

$*$	0	1	5	7
0	0	0	0	0
1	0	1	5	7
5	1	5	0	5
7	5	7	1	1

   Determine si tiene elemento neutro, absorbente, si es conmutativa o asociativa.

4. Determine los elementos idempotentes y los elementos involutivos de cada una de las siguientes estructuras algebraicas:

   (a) $(\mathbb{R}, +)$

   (b) $(\mathbb{R}^*, *)$, con $a * b = 5ab$

   (c) $(\mathbb{R}, *)$ con $a * b = ab + 3b^2$

5. En el conjunto $\mathcal{E} = \{a, b, c, d, e, f\}$ se define $*$ por la tabla:

$*$	c	e	f	a	b	d
c	e	c	e	a	c	a
e	c	e	c	a	e	a
f	e	c	b	a	f	d
a	a	a	a	a	a	a
b	c	e	f	a	b	d
d	a	a	d	a	d	d

   Si tiene, determine los elementos: neutro, absorbente, involutivos e idempotentes.

6. En el conjunto $\mathcal{E} = \{a, b, c, d\}$ se define una ley de composición interna $*$ por medio de la tabla:

$*$	a	b	c	d
a	c	b	a	b
b	b	d	a	c
c	d	a	b	a
d	b	c	a	d

   Determine los elementos centrales de $(\mathcal{E}, *)$ y el centro de $\mathcal{E}$.

7. Sobre el conjunto de los números reales no negativos, es decir, el intervalo $[0, +\infty[$, se define la operación $a * b = \sqrt{a^2 + b^2}$. Pruebe que $([0, +\infty[, *)$ es una estructura algebraica asociativa, conmutativa y con elemento neutro.

8. En $\mathbb{N} = \{1, 2, 3, \dots\}$ se define $a * b = \min\{a, b\}$, es decir, el mínimo de a y b. Pruebe que $(\mathbb{N}, *)$ es una estructura algebraica asociativa. Determine si existe elemento neutro y elemento absorbente.

9. En el conjunto $\mathcal{E} = \{1, 2, 3, 4, 5, 6\}$ se define la operación $\otimes$, donde $a \otimes b$ es el residuo de la división de $a \cdot b$ por 7. Construya la tabla de la operación, determine si tiene elemento neutro, absorbente, idempotente, involutivo y si la estructura es conmutativa. Además, determine el elemento inverso de cada elemento de $\mathcal{E}$.

10. Sobre $\mathbb{R}$ se define la operación $\perp$ como $a \perp b = ab + ka + kb + 42$, donde k es una constante. Determine k de manera que $\perp$ sea asociativa.

11. En el conjunto $\mathcal{E} = \{1, 2, 4, 5\}$ se define la operación $*$, de manera que $a * b = k$, donde k es el residuo de la división entera de a^b por 6. Construya la tabla de la operación, determine si tiene elemento neutro, absorbente, idempotente, involutivo y si la estructura es conmutativa o asociativa.

12. Considere el conjunto de números enteros no negativos menores que 10, es decir, $D_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, y sobre él defina la operación $*$ de manera que $x * y = d$ si y solo si d es el dígito final de la representación decimal del número $x + y + xy$ (por ejemplo: $4 * 3 = 19$, pues $4 + 3 + 4 \cdot 3 = 19$). Construya la tabla de la operación y determine si la operación tiene elemento neutro, absorbente, idempotente, involutivo y si la estructura es conmutativa o asociativa.

13. Sea $S = \{a, b, c\}$. Sobre el conjunto potencia de S defina la ley de composición interna $\triangle$. Obtenga la tabla de operación, el elemento neutro y el inverso de cada elemento.

6.2 Grupos

Si $\mathcal{G}$ es un conjunto no vacío y $*$ es una operación interna definida sobre $\mathcal{G}$, se dice que $(\boldsymbol{\mathcal{G}}, \boldsymbol{*})$ es:

- Un **semigrupo** si $*$ es asociativa.
- Un **monoide** si es un semigrupo con elemento neutro.
- Un **grupo** si es un monoide que cumple la propiedad de los inversos, es decir, $(\mathcal{G}, *)$ es un grupo si $*$ es cerrada, asociativa, posee elemento neutro y cada elemento tiene inverso.
- Un **grupo abeliano** o grupo conmutativo si es un grupo y se cumple la conmutatividad. En el caso de que no sea grupo, se dirá que la estructura algebraica es conmutativa.

Ejemplo 16. $(\mathbb{R}, \cdot)$ *es un monoide donde el neutro es* 1*. Observe que el* 0 *no tiene inverso multiplicativo; por lo tanto, la operación no cumple con la propiedad de los inversos.* ■

Ejemplo 17. $(\mathbb{R}^*, \cdot)$ *es un grupo abeliano con* $e = 1$ *y* $a^{-1} = \frac{1}{a}$. ■

Ejemplo 18. *A partir del ejemplo* 12*, se tiene que la estructura algebraica* $(P(S), \triangle)$ *es un grupo abeliano con* $\varnothing$ *como elemento neutro y* $A^{-1} = A$ *para todo* $A \in P(S)$. ■

Ejemplo 19. *Considere la operación* $\oplus$ *definida sobre* $\mathbb{R}$ *dada por:*

$$a \oplus b = a + b + 2$$

Pruebe que $(\mathbb{R}, \oplus)$ *es un grupo abeliano.*

Solución. Es cerrada, pues si a y b son reales, entonces $a+b+2$ también lo es. Es asociativa, pues:

$$(a \oplus b) \oplus c = (a + b + 2) \oplus c = (a + b + 2) + c + 2 = a + b + c + 4$$

y claramente es igual a:

$$a \oplus (b \oplus c) = a \oplus (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4$$

Para determinar el elemento neutro e, se debe cumplir $a \oplus e = a$, es decir, $a + e + 2 = a$, con lo cual $e = -2$ es el neutro. Para determinar el inverso de a, se debe analizar $a \oplus b = -2$, es decir, $a + b + 2 = -2$, de donde se obtiene que $b = -a - 4$; de este modo, $a^{-1} = -a - 4$. Por último, es conmutativa, pues $a \oplus b = a + b + 2 = b + a + 2 = b \oplus a$. ■

Ejemplo 20. *Considere la operación* $\perp$ *definida sobre* $\mathbb{R}^* \times \mathbb{R}$ *por:*

$$(a, b) \perp (c, d) = (4ac, b + d + 3)$$

Pruebe que $(\mathbb{R}^* \times \mathbb{R}, \perp)$ *es un grupo abeliano.*

Solución. Es claro que $\perp$ es una operación cerrada, ya que si $a \neq 0$ y $c \neq 0$, se tiene que $4ac \neq 0$, y si $b \in \mathbb{R}$ y $d \in \mathbb{R}$, se tiene que $b+d+3 \in \mathbb{R}$. Par ver que es asociativa, basta ver que:

$$\begin{aligned}
& [(a, b) \perp (c, d)] \perp (e, f) = (a, b) \perp [(c, d) \perp (e, f)] \\
\Leftrightarrow \quad & [(4ac, b + d + 3)] \perp (e, f) = (a, b) \perp [(4ce, d + f + 3)] \\
\Leftrightarrow \quad & (4 \cdot 4ace, b + d + 3 + f + 3) = (4a4ce, b + d + f + 3 + 3) \\
\Leftrightarrow \quad & (16ace, b + d + f + 6) = (16ace, b + d + f + 6)
\end{aligned}$$

Posee elemento neutro si $\forall (a, b) \in \mathbb{R}^* \times \mathbb{R}$ se cumple que existe $e \in \mathbb{R}^* \times \mathbb{R}$ tal que $(a, b) \perp e = (a, b)$, se encuentra e de la siguiente manera:

$$\begin{aligned}
& (a, b) \perp (c, d) = (a, b) \\
\Leftrightarrow \quad & (4ac, b + d + 3) = (a, b) \\
\Leftrightarrow \quad & 4ac = a \quad \wedge \quad b + d + 3 = b \\
\Leftrightarrow \quad & c = \frac{1}{4} \quad \wedge \quad d = -3
\end{aligned}$$

Por lo tanto, el neutro existe y es $e = \left(\frac{1}{4}, -3\right)$. Para probar que satisface la propiedad de los inversos, es necesario encontrar el inverso de (a, b):

$$\begin{aligned} & (a,b)\perp(c,d) = \left(\frac{1}{4}, -3\right) \\ \Leftrightarrow \quad & (4ac, b+d+3) = \left(\frac{1}{4}, -3\right) \\ \Leftrightarrow \quad & 4ac = \frac{1}{4} \quad \wedge \quad b+d+3=-3 \\ \Leftrightarrow \quad & c = \frac{1}{16a} \quad \wedge \quad d = -6-b \end{aligned}$$

Por lo tanto, existe el inverso y $(a, b)^{-1} = \left(\frac{1}{16a}, -6-b\right)$. Falta verificar que se satisface la conmutatividad, para ello:

$$(a,b)\perp(c,d) = (4ac, b+d+3) = (4ca, d+b+3) = (c,d)\perp(a,b)$$

De esta manera, se sabe que $(\mathbb{R}^* \times \mathbb{R}, \perp)$ es un grupo abeliano. ■

En este contexto, se utiliza la misma idea de la notación de exponentes enteros para números reales, con la finalidad de simbolizar la aplicación de la operación $*$ varias veces.

Si $(\mathcal{G}, *)$ es un monoide, se tiene que $\boldsymbol{a^0 = e}$, y si n es un número natural con $n \geq 1$:

$$\begin{aligned} a^n &= a * a^{n-1} \\ &= \underbrace{a * a * a * \cdots * a}_{n \text{ veces } a} \end{aligned}$$

Si además cumple con la propiedad de los inversos, los exponentes negativos se definen como:

$$a^{-n} = \left(a^{-1}\right)^n$$

Ejemplo 21. *Para el conjunto $\mathbb{Z}$, se tiene que $(\mathbb{Z}, +)$ es un grupo abeliano donde el neutro es 0 y el inverso de a es $-a$. Como ejemplo de algunas potencias en este grupo, se tiene que* $3^2 = 3+3 = 6$, $4^{-1} = -4$

$$5^{-2} = \left(5^{-1}\right)^2 = (-5)^2 = (-5) + (-5) = -10$$

Además, $1^5 = 1+1+1+1+1 = 5$. ■

Teorema 1. *Si $(\mathcal{G}, *)$ es un grupo, en general se tiene que:*

$$(a * b)^{-1} = b^{-1} * a^{-1} \tag{6.3}$$

$$(a^{-1})^{-1} = a \tag{6.4}$$

Demostración. Se debe probar dos condiciones, en primer lugar, es claro que:

$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} \\ &= a * e * a^{-1} \\ &= a * a^{-1} \\ &= e \end{aligned}$$

análogamente se prueba $(b^{-1} * a^{-1}) * (a * b) = e$, con lo cual se prueba (6.3). De la misma manera, como

$$\begin{aligned} \left(a^{-1}\right)^{-1} &= \left(a^{-1}\right)^{-1} * e \\ &= \left(a^{-1}\right)^{-1} * \left(a^{-1} * a\right) \\ &= \left(\left(a^{-1}\right)^{-1} * a^{-1}\right) * a \\ &= e * a \\ &= a \end{aligned}$$

se completa la demostración de (6.4). □

Note que si el grupo es abeliano, sí se puede escribir $(a*b)^{-1} = a^{-1}*b^{-1}$; en caso contrario, se debe respetar el orden inverso dado en (6.3).

Ejemplo 22. *Sea* $(\mathcal{G}, *)$ *un grupo. Pruebe que si* $\forall a \in \mathcal{G}$ *se cumple* $a = a^{-1}$*, entonces* $(\mathcal{G}, *)$ *es un grupo abeliano.*

Solución. Dados a, b en $\mathcal{G}$, se debe probar que $a * b = b * a$. Por hipótesis, $a = a^{-1}$ y $b = b^{-1}$; además, como $\mathcal{G}$ es cerrado, $a * b \in \mathcal{G}$ y se cumple $a * b = (a * b)^{-1}$. Finalmente, utilizando (6.3) se tiene que:

$$\begin{aligned} a * b &= (a * b)^{-1} \\ &= b^{-1} * a^{-1} \\ &= b * a \end{aligned}$$

Es decir, la operación es conmutativa. ■

Teorema 2. (Ley de cancelación) *Si* $(\mathcal{G}, *)$ *es un grupo, entonces* $\forall\, a, b, c \in \mathcal{G}$ *se cumple que*

$$a * b = a * c \quad \Rightarrow \quad b = c \tag{6.5}$$

$$b * a = c * a \quad \Rightarrow \quad b = c \tag{6.6}$$

Demostración. Como $a \in \mathcal{G}$, existe a^{-1}, por lo que para la cancelación por la izquierda (6.5) basta ver que

$$\begin{aligned} a * b = a * c \quad &\Rightarrow \quad a^{-1} * (a * b) = a^{-1} * (a * c) \\ &\Rightarrow \quad (a^{-1} * a) * b = (a^{-1} * a) * c \\ &\Rightarrow \quad e * b = e * c \\ &\Rightarrow \quad b = c \end{aligned}$$

Para la cancelación por la derecha se procede de forma análoga. □

Ejemplo 23. *Para* $\mathcal{G} = \{a, b, c, d\}$ *y la ley de composición* $*$ *definida por la siguiente tabla, se sabe que* $(\mathcal{G}, *)$ *es un grupo. Complete la tabla:*

$*$	a	b	c	d
a	a			d
b				c
c		d		
d	d	c	b	

Solución. Se comprobará que $a * b = b$ descartando las tres opciones posibles $a * b = a$; $a * b = c$; $a * b = d$. Suponga que $a * b = a$, de la tabla se sabe que $a * a = a$, de donde $a * b = a * a$, por lo que al aplicar la ley de cancelación se tiene que $b = a$, lo cual es una contradicción. Análogamente, si $a * b = c$, como $d * b = c$, se concluye que $a = d$, por lo que no es posible. Finalmente si $a * b = d$, como $a * d = d$, se concluye que $b = d$, por lo que no es posible. Con un razonamiento análogo, finalmente se completa la tabla como:

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

■

Si el grupo es finito, su **orden** se denota por $\boldsymbol{o(\mathcal{G})}$ y corresponde a la cardinalidad como conjunto.

Ejemplo 24. *A partir del ejemplo* 12*, se tiene que* $(P(S), \triangle)$ *es un grupo abeliano de orden* 4*, es decir,* $o(P(S)) = 4$*. Además, en este grupo se cumple, por ejemplo, que* $S^2 = \varnothing$*,* $\{a\}^{-3} = \{a\}$*.* ■

Ejemplo 25. *A partir del ejemplo* 15*, se tiene que* $(\mathbb{Z}/\mathcal{R}, \oplus)$ *es un grupo abeliano con* $e = \dot{0}$*; el inverso de* $\dot{0}$ *es* $\dot{0}$*; el inverso de* $\dot{1}$ *es* $\dot{2}$*, y el inverso de* $\dot{2}$ *es* $\dot{1}$*. El orden de este grupo es* 3 *y se escribe* $o(\mathbb{Z}/\mathcal{R}) = 3$*.* ■

Para $n \in \mathbb{N}$ con $n \geq 2$, y la relación $\mathcal{R}$ definida sobre $\mathbb{Z}$ por

$$a\mathcal{R}b \Leftrightarrow \left(\exists k \in \mathbb{Z} \quad \text{tal que} \quad a - b = nk\right)$$

se define al conjunto $\boldsymbol{\mathbb{Z}_n = \mathbb{Z}/\mathcal{R}}$, es decir, $\mathbb{Z}_n$ es el conjunto de clases residuales módulo n.

Sobre estos conjuntos $\mathbb{Z}_n$ se definen las operaciones usuales de suma $\oplus$ y multiplicación $\odot$ de clases. En el ejemplo 15 se trabajó con $n = 3$, y en los ejemplos 26 y 27 se trabajará con $n = 5$.

Los resultados enunciados a continuación son centrales y muy importantes en la teoría de grupos, en la búsqueda de subgrupos de un grupo finito y en la clasificación de los grupos. Sus demostraciones se omiten; sin embargo, se pueden encontrar en [13].

- Para todo $n \geq 2$, $(\mathbb{Z}_n, \oplus)$ es grupo abeliano y $o(\mathbb{Z}_n) = n$.
- $(\mathbb{Z}_n^*, \odot)$ es grupo abeliano si y solo si n es un número primo. Además, $o(\mathbb{Z}_n^*) = n - 1$.

Ejemplo 26. *En el conjunto $\mathbb{Z}_5$ se define la operación $\oplus$ para todo $\dot{a}$ y $\dot{b}$ en $\mathbb{Z}_5$ por $\dot{a} \oplus \dot{b} = \overset{\bullet}{(a+b)}$. Construya la tabla para esta ley, determine el elemento neutro y el inverso de cada uno de los cinco elementos de este grupo.*

Solución. Para construir la tabla de operación, se deben calcular los 25 posibles resultados, es decir, los residuos de la división por 5 de cada suma; por ejemplo, $\dot{4} \oplus \dot{3} = \overset{\bullet}{(4+3)} = \dot{7} = \dot{2}$. Así, la tabla completa es:

$\oplus$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

A partir de ahí es posible notar que $\dot{0}$ es elemento neutro; el inverso de $\dot{0}$ es $\dot{0}$; el inverso de $\dot{1}$ es $\dot{4}$, además, $(\dot{2})^{-1} = \dot{3}$, $(\dot{3})^{-1} = \dot{2}$ y $(\dot{4})^{-1} = \dot{1}$. Se puede verificar fácilmente que es cerrada, asociativa y conmutativa. ■

Ejemplo 27. *En el conjunto $\mathbb{Z}_5^*$ se define la operación $\odot$ para todo $\dot{a}$ y $\dot{b}$ en $\mathbb{Z}_5^*$ por $\dot{a} \odot \dot{b} = (\dot{a \cdot b})$. Construya la tabla para esta ley, determine el elemento neutro y el inverso de cada uno de los cuatro elementos de este grupo.*

Solución. Para construir la tabla de operación, se deben calcular los 16 posibles resultados, al igual que los residuos de la división por 5 de cada producto; por ejemplo, $\dot{3} \odot \dot{3} = (\dot{3 \cdot 3}) = \dot{9} = \dot{4}$. Así, la tabla completa es:

$\odot$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Así, se nota que $\dot{1}$ es elemento neutro; el inverso de $\dot{1}$ es $\dot{1}$, el inverso de $\dot{2}$ es $\dot{3}$, análogamente $\left(\dot{3}\right)^{-1} = \dot{2}$ y $\left(\dot{4}\right)^{-1} = \dot{4}$. Se puede verificar fácilmente que es cerrada, asociativa y conmutativa. ■

Ejemplo 28. *Sea $\mathcal{G}$ un grupo. Pruebe que si $\forall a, b \in \mathcal{G}$ se cumple $(ab)^2 = a^2b^2$, entonces $\mathcal{G}$ es un grupo abeliano.*

Solución. Es necesario probar que $ab = ba$ para todo a, b en $\mathcal{G}$. Por hipótesis, $(ab)^2 = a^2b^2$, es decir, $abab = aabb$, y por ser grupo existen a^{-1} y b^{-1}; multiplicando la anterior igualdad por a^{-1} a la izquierda y por b^{-1} a la derecha, se obtiene que:

$$a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1}$$

Luego, al aplicar la asociatividad, se tiene que:

$$(a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1})$$

Finalmente, al usar la propiedad de los inversos y el neutro, se obtiene que $ab = ba$, es decir, la operación es conmutativa. ■

Ejercicios (sección 6.2)

1. Sea $\mathcal{G} = \{-1, 1\}$, compruebe que $(\mathcal{G}, \cdot)$ es grupo abeliano, pero $(\mathcal{G}, +)$ ni siquiera es una estructura algebraica.

2. Pruebe que $(\mathbb{R}, *)$ con $a * b = a + b - 4$ es un grupo abeliano. Además, calcule el valor exacto de:
$$3^3 * \left[7 * \left(2 * \frac{1}{4}\right)^{-2}\right]^4$$

3. Pruebe que $(\mathbb{R}^*, *)$ con $a * b = 4ab$ es un grupo abeliano. Además, calcule el valor exacto de:
$$3^3 * \left[7 * \left(2 * \frac{1}{4}\right)^{-2}\right]^4$$

4. En el conjunto $\mathbb{R} \times \mathbb{R}^*$ se define la operación $\otimes$ como:
$$(a, b) \otimes (c, d) = (a + c - 4, 2bd)$$
   (a) Pruebe que $(\mathbb{R} \times \mathbb{R}^*, \otimes)$ es grupo abeliano.
   (b) Calcule el valor exacto de:
$$(2, -1)^3 \otimes \left[\left(0, \frac{1}{3}\right) \otimes (1, -1)^{-1}\right]^2$$

5. En el conjunto $\mathbb{R} \times \mathbb{R}^*$ se define la operación $\otimes$ como:
$$(a, b) \otimes (c, d) = (a + c + 3, 2bd)$$
   Si se sabe que $(\mathbb{R} \times \mathbb{R}^*, \otimes)$ es un grupo, calcule:
$$\left(5, \frac{1}{8}\right)^2 \otimes \left[\left(3, \frac{5}{2}\right)^{-1} \otimes (-2, 3)\right]^{-1}$$

6. Construya la tabla de operación para el grupo $(\mathbb{Z}_7, \oplus)$, determine el elemento neutro y los inversos de cada elemento del grupo.

7. Considere el grupo $(\mathbb{Z}_7^*, \odot)$.

   (a) Construya su tabla de operación.

   (b) Determine el neutro y los inversos de cada elemento.

   (c) Calcule los valores exactos de $\left(\overset{\bullet}{3}\right)^4$, $\left(\overset{\bullet}{3}\right)^{-4}$ y $\left(\overset{\bullet}{2}\right)^{-409}$

   (d) Calcule el valor exacto de:

$$\left[\left(\overset{\bullet}{3}\right)^7 \odot \left(\overset{\bullet}{5}\right)\right]^{-3} \odot \left[\left(\overset{\bullet}{4}\right) \odot \left(\overset{\bullet}{2}\right)^{-4}\right]^2$$

8. Considere el grupo $(\mathbb{Z}_{11}^*, \odot)$.

   (a) Construya su tabla de operación.

   (b) Determine el neutro y los inversos de cada elemento.

   (c) Calcule el valor exacto de:

$$\left[\left(\overset{\bullet}{8}\right)^6 \odot \left(\overset{\bullet}{3}\right)\right]^{-4} \odot \left[\left(\overset{\bullet}{9}\right) \odot \left(\overset{\bullet}{2}\right)^{-5}\right]^3$$

9. Sobre el conjunto de los números reales $\mathbb{R}$, se define la operación interna $a * b = \sqrt{a^3 + b^3}$. Pruebe que $(\mathbb{R}, *)$ es un grupo abeliano.

10. Para cada uno de los siguientes conjuntos, donde se define una operación interna, analice las propiedades que cumple e indique qué tipo de estructura es.

    (a) $(\mathbb{Z}, *)$ con $a * b = a + b - 5$

    (b) $(\mathbb{Z}, *)$ con $a * b = 5ab$

    (c) $(\mathbb{Z}, *)$ con $a * b = a + b + ab$

    (d) $(\mathbb{R} - \{-1\}, *)$ con $a * b = a + b + ab$

(e) $(\mathbb{Z}, *)$ con $a * b = a^2 - b^2$

(f) $(\mathbb{R}, *)$ con $a * b = a + 2ab + 4$

(g) $(\mathbb{Z} \times \mathbb{Z}, *)$ con $(a, b) * (c, d) = (a + c, b + d)$

(h) $(\mathbb{Z} \times \mathbb{Z}, *)$ con $(a, b) * (c, d) = (ad + bc, bd)$

(i) $(\mathbb{R} \times \mathbb{R}^*, \otimes)$ con $(a, b) \otimes (c, d) = (a + c + 3, 4bd)$

(j) $(\mathbb{R} - \{-1\} \times \mathbb{R}, \otimes)$ con $(a, b) \otimes (c, d) = (a + c + ac, b + d + 2)$

11. Si $(\mathcal{G}, *)$ es un grupo tal que para todo $x \in G$ se cumple que $x^2 = e$, demuestre que G es abeliano.

12. Si $(\mathcal{G}, *)$ es un grupo, pruebe que $\mathcal{G}$ es abeliano si y solo si $\forall a, b \in \mathcal{G}$, se cumple $(a * b)^{-1} = a^{-1} * b^{-1}$.

13. Si $P(E)$ denota el conjunto de partes de E, con $E \neq \varnothing$. Sobre este conjunto se definen diferentes operaciones internas, analice las propiedades que cumple e indique qué tipo de estructura es.

(a) $(P(E), *)$ con $A * B = A \cup B$

(b) $(P(E), *)$ con $A * B = A \cap B$

(c) $(P(E), *)$ con $A * B = A - B$

14. Complete la siguiente tabla de manera que $(\mathcal{G}, *)$ sea un grupo.

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a		e	f	c	d
b	b	e	a			
c	c				a	
d	d	f				
f	f	c		a		

15. Considere el conjunto A formado por los polinomios de la forma $ax + b$ con a, $b \in \mathbb{Z}$, con la suma de polinomios usual como la operación interna, es decir, $(ax + b) + (cx + d) = (a + c)x + (b + d)$. Pruebe que $(A, +)$ es un grupo abeliano.

16. Sea $\mathcal{G}$ el conjunto formado por todos los números reales de la forma $a+b\sqrt{2}$, con a y b números racionales, dotado de la multiplicación usual como operación; además, a y b no son cero simultáneamente. Pruebe que $(\mathcal{G},\cdot)$ es un grupo abeliano.

17. Sea A un conjunto cualquiera, y sea $\mathcal{G}$ el conjunto formado por todas las funciones biyectivas de A en A. Demuestre que $(\mathcal{G},\circ)$ es un grupo no conmutativo.

18. Sobre el conjunto de funciones $\mathcal{G} = \{f_1, f_2, f_3, f_4\}$, donde el dominio de todas ellas es $\mathbb{R}^*$ y sus respectivos criterios vienen dados por $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = \frac{-1}{x}$; por último, considere la composición de funciones como operación interna. Compruebe que $(\mathcal{G},\circ)$ es un grupo.

19. Sobre el conjunto de funciones $\mathcal{G} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, donde el dominio de todas ellas es $\mathbb{R}-\{0,1\}$ y sus criterios vienen dados por $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1-x$, $f_4(x) = \frac{1}{1-x}$, $f_5(x) = \frac{x-1}{x}$, $f_6(x) = \frac{x}{x-1}$, con la composición de funciones como operación interna. Construya la tabla de operación, determine el neutro y el inverso de cada elemento.

20. Si $(\mathcal{G},*)$ es un grupo finito de orden par mayor o igual a 2, demuestre que existe a, con $a \neq e$ tal que $a = a^{-1}$.

21. Pruebe que cualquier grupo finito de orden menor o igual a 4 es abeliano.

6.3 Otros grupos

En la sección anterior se desarrolló, de manera general, el concepto de la estructura algebraica que se conoce como grupo; sin embargo, existen muchos grupos que, por su importancia o alguna propiedad particular, reciben un nombre especial y la mayoría tiene gran aplicación. Sobre ellos tratará esta breve sección.

Sea $\mathcal{G}$ un grupo y un elemento $x \in \mathcal{G}$. Se dice que $\mathcal{G}$ es un **grupo cíclico** generado por x si para cada elemento $y \in \mathcal{G}$ existe un $n \in \mathbb{Z}$ tal que $y = x^n$.

Teorema 3. *Si $\mathcal{G}$ es cíclico, entonces es grupo abeliano; además, si $\mathcal{G}$ es generado por x, entonces también es generado por su inverso x^{-1}.*

Demostración. Se probará, en primer lugar, que si $\mathcal{G}$ es cíclico entonces es abeliano: sean y y $z \in \mathcal{G}$, como $\mathcal{G}$ cíclico generado por x, entonces existen n y $m \in \mathbb{Z}$ tal que $y = x^n$ y $z = x^m$, de donde:

$$yz = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = zy$$

Con lo cual, es abeliano. Por otro lado, si $\mathcal{G}$ es generado por x, dado $y \in \mathcal{G}$, existe $n \in \mathbb{Z}$ tal que $y = x^n$, es decir, $y = (x^{-1})^{-n}$, y como $-n \in \mathbb{Z}$, $\mathcal{G}$ es generado por x^{-1}. $\square$

Ejemplo 29. *El grupo $(\mathbb{Z}_5^*, \odot)$ es un grupo cíclico generado por $\dot{2}$, ya que $\left(\dot{2}\right)^1 = \dot{2}$, $\left(\dot{2}\right)^2 = \dot{4}$, $\left(\dot{2}\right)^3 = \dot{3}$, $\left(\dot{2}\right)^4 = \dot{1}$, es decir, cada elemento de $\mathbb{Z}_5^*$ es alguna potencia de $\dot{2}$. Note que, de acuerdo con el ejemplo anterior, también $\dot{3}$ (el inverso de $\dot{2}$) es un generador, pues fácilmente se comprueba que $\left(\dot{3}\right)^1 = \dot{3}$, $\left(\dot{3}\right)^2 = \dot{4}$, $\left(\dot{3}\right)^3 = \dot{2}$, $\left(\dot{3}\right)^4 = \dot{1}$, es decir, cada elemento de $\mathbb{Z}_5^*$ es también una potencia de $\dot{3}$.* $\blacksquare$

Para el conjunto $X = \{1, \ldots, n\}$ se define el **grupo simétrico** $\boldsymbol{S_n}$ como el conjunto de todas las funciones biyectivas de X en X, dotado con la composición de funciones como operación interna.

Ejemplo 30. *Calcule el orden del grupo S_n. (Compare con el teorema 9, página 263)*

Solución. Observe que para asignar la imagen al primer elemento se tienen n posibilidades; fijando una de éstas, para asignar la imagen del segundo elemento se tienen $n-1$ posibilidades; así, al ir fijando las imágenes para hacer la función biyectiva, el número de funciones que se obtiene es $n!$, y con ello $o(S_n) = n!$. ■

Si p es un número primo y $\mathcal{G}$ un grupo, se dice que $\mathcal{G}$ es un $\boldsymbol{p}$**-grupo** si su orden es una potencia de p.

Ejemplo 31. *Pruebe que el grupo simétrico S_n no es un p-grupo para todo $n \geq 3$.*

Solución. Para el grupo simétrico S_n (véase página 333), se sabe que $o(S_n) = n!$ y es claro que nunca será igual a p^k para todo $k \in \mathbb{N}$, $n \geq 3$ y p primo; por lo tanto, S_n no es un p-grupo. ■

Ejemplo 32. *Como el orden del grupo $(\mathbb{Z}_5^*, \odot)$ es 4, y $4 = 2^2$, se tiene que $(\mathbb{Z}_5^*, \odot)$ es un 2-grupo.* ■

Ejemplo 33. *Como el orden del grupo $(\mathbb{Z}_{10}^*, \oplus)$ es 10, y 10 no se puede escribir como una potencia de un número primo, se tiene que $(\mathbb{Z}_{10}^*, \odot)$ no es un p-grupo.* ■

Ejemplo 34. *Como el orden del grupo $(\mathbb{Z}_{17}^*, \odot)$ es 16, y $16 = 2^4$, se tiene que $(\mathbb{Z}_{17}^*, \odot)$ es un 2-grupo.* ■

Como se mencionó en la sección anterior, una condición necesaria para que $(\mathbb{Z}_n^*, \odot)$ sea grupo es que p sea primo, como se ha trabajado en el ejemplo 37 con $p = 5$. Así, en el caso de que p no sea primo, no se obtiene la deseada estructura de grupo. Por ejemplo, en el conjunto $\mathbb{Z}_6^*$ se tiene que $\overset{\bullet}{2} \odot \overset{\bullet}{3} = \overset{\bullet}{6} = \overset{\bullet}{0}$ y no es una operación cerrada, por lo que no es grupo; sin embargo, al considerar el subconjunto de $\mathbb{Z}_n^*$ formado por las clases residuales que son relativamente primos con n, se obtiene un grupo abeliano.

> La estructura algebraica $(U_n, \odot)$, donde el conjunto U_n está definido por
>
> $$U_n = \left\{ \overset{\bullet}{a} \in \ \mathbb{Z}_n^* \ \ / \quad \text{m.c.d.}(a, n) = 1 \right\}$$
>
> es un grupo abeliano.

Ejemplo 35. *El conjunto* $U_8 = \left\{ \overset{\bullet}{1}, \overset{\bullet}{3}, \overset{\bullet}{5}, \overset{\bullet}{7} \right\}$ *es un grupo de orden* 4. ■

En general, el orden de este grupo viene dado por la función de Euler y se cumple que

$$o(U_n) = \varphi(n)$$

Una forma sencilla de calcular el valor de esta función para n es con base en la factorización en factores primos de n, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$; de esta forma, se tiene que:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right)$$

Ejemplo 36. *Para determinar el* $o(U_{56})$ *se observa que la factorización en factores primos de* 56 *es* $2^3 \cdot 7$. *Así,* $\varphi(56) = 56\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 24$ *y con ello* $o(U_{56}) = 24$. ■

Ejercicios (sección 6.3)

1. Verifique que $(\mathbb{Z}_7^*, \odot)$ es un grupo cíclico.
2. Para el grupo $(\mathbb{Z}_7^*, \odot)$, encuentre un valor $\beta \in \mathbb{N}$ tal que para todo $a \in \mathbb{Z}_7^*$ se tiene que $a^\beta = e$.
3. Calcule el conjunto U_9 y compruebe que es un grupo cíclico. Además, determine todos sus generadores.
4. Calcule el conjunto U_{15} y compruebe que para todos sus elementos se cumple que $a^4 = e$.
5. Determine el grupo U_{15} y construya su tabla de operación.
6. Determine el orden de los grupos U_{25}, U_{70}, U_{500}.
7. Suponga que se tiene un rectángulo R no cuadrado en el plano XY con centro O, con vértices A, B, C y D, y los siguientes movimientos de R, llamadas las simetrías de R:

   $\boldsymbol{r}$, la rotación de 180° alrededor de O, es decir, $r(R) = CDAB$.
   $\boldsymbol{h}$, la reflexión en el eje horizontal, es decir, $h(R) = DCBA$.
   $\boldsymbol{v}$, la reflexión en el eje vertical, es decir, $v(R) = BADC$.
   $\boldsymbol{e}$, ningún movimiento del todo, es decir, $e(R) = R$.

   Complete la tabla de operación para el conjunto $\mathcal{K} = \{r, h, v, e\}$ y la composición de funciones.

$\circ$	r	h	v	e
r	e	v	h	
h			r	
v	h			
e		h		

   Determine el elemento neutro y los inversos de cada elemento del grupo $(\mathcal{K}, \circ)$; este grupo se llama **Grupo de Klein**.

6.4 Subgrupos

Algunos conjuntos con estructura de grupo poseen subconjuntos que también tienen esta misma estructura. A continuación, se definirán y luego se enunciarán los teoremas que permiten simplificar su búsqueda.

Si $(\mathcal{G}, *)$ es un grupo y $\mathcal{H} \subseteq \mathcal{G}$ con $\mathcal{H} \neq \varnothing$, $\mathcal{H}$ se llamará **subgrupo** de $\mathcal{G}$, y se denota por $\boldsymbol{\mathcal{H} < \mathcal{G}}$ si y solo si $(\mathcal{H}, *)$ es un grupo. Es decir, un subgrupo de un grupo es un subconjunto no vacío del grupo que sea grupo con la operación restringida a sus elementos.

Teorema 4. (De Lagrange) *El orden del subgrupo es un divisor del orden del grupo.*

Demostración. Se omite, puede consultar [13]. $\square$

Teorema 5. *Sea $(\mathcal{G}, *)$ un grupo con $\mathcal{H} \subseteq \mathcal{G}$, $\mathcal{H} \neq \varnothing$, entonces:*

$$\mathcal{H} < \mathcal{G} \iff \forall a, b \in \mathcal{H} \ \left[a * b^{-1} \in \mathcal{H}\right]$$

Demostración. Es necesario demostrar la equivalencia.

"$\Rightarrow$" Sean a, $b \in \mathcal{H}$. Como $\mathcal{H}$ es subgrupo, se tiene que $\exists b^{-1} \in \mathcal{H}$; además, por la cerradura, se tiene que $a * b^{-1} \in \mathcal{H}$.

"$\Leftarrow$" Se debe probar que $\mathcal{H} < \mathcal{G}$. Para iniciar, en el caso de que $b = a$, por hipótesis se tiene que $a * a^{-1} = e \in \mathcal{H}$, con lo que $\mathcal{H}$ posee elemento neutro. Además, para $e \in \mathcal{H}$, $a \in \mathcal{H}$, por hipótesis se tiene que $e * a^{-1} = a^{-1} \in \mathcal{H}$, con lo que todo elemento de $\mathcal{H}$ posee inverso en $\mathcal{H}$. Es claro que la asociatividad se cumple. Por último, se cumple la cerradura, ya que para a, $b \in \mathcal{H}$ se ha probado que $b^{-1} \in \mathcal{H}$, y por hipótesis $a * \left(b^{-1}\right)^{-1} = a * b \in \mathcal{H}$.

Con lo cual, se ha demostrado este resultado. $\square$

Teorema 6. *Sea $(\mathcal{G}, *)$ un grupo finito, con $\mathcal{H} \subseteq \mathcal{G}$, $\mathcal{H} \neq \varnothing$, entonces:*

$$\mathcal{H} < \mathcal{G} \iff \forall a, b \in \mathcal{H} \ [a * b \in \mathcal{H}]$$

Demostración. Se omite, puede consultar [13]. $\square$

El teorema 4 ayuda a determinar la cantidad de elementos que debe tener un subgrupo, en caso de que el grupo tenga orden finito. Sin embargo, son los teoremas 5 y 6 los que dan la condición necesaria y suficiente si se quiere demostrar o verificar que un subconjunto de un grupo es o no un subgrupo de él, pues es suficiente comprobar que se cumple la condición de cerradura planteada en ellos. Sin duda, esta condición es más sencilla en el caso de los grupos finitos, ya que solamente bastaría verificar la cerradura bajo la operación, según el teorema 6. Además, al ser una equivalencia en ambos teoremas, en el caso de que no se cumpla la condición de cerradura planteada, se concluye que el subconjunto no es subgrupo.

Ejemplo 37. *Determine todos los subgrupos de $(\mathbb{Z}_5^*, \odot)$.*

Solución. En el ejemplo 27 se encontraron los inversos de cada elemento de $\mathbb{Z}_5^*$; además, se sabe que el orden de $\mathbb{Z}_5^*$ es 4. Utilizando el teorema de Lagrange, se tiene que el orden del subgrupo puede ser 1, 2 o 4, los divisores de 4, pero no de orden 3. Así, se obtiene que de orden 1 se tiene el subgrupo $\left\{\overset{\bullet}{1}\right\}$; de orden 2 está el subgrupo $\left\{\overset{\bullet}{1}, \overset{\bullet}{4}\right\}$; de orden 4 el subgrupo $\mathbb{Z}_5^*$. $\blacksquare$

Ejemplo 38. *Determine todos los subgrupos del grupo $(\mathbb{Z}_8, \oplus)$.*

Solución. Dado que el orden de $\mathbb{Z}_8$ es 8, y aplicando el teorema de Lagrange, se concluye que los únicos posibles órdenes de los subgrupos son 1, 2, 4 o 8. Así, luego de determinar los inversos de cada uno de los ocho elementos del grupo, se tiene que el subgrupo de orden 1 es $\left\{\overset{\bullet}{0}\right\}$; de orden 2 es $\left\{\overset{\bullet}{0}, \overset{\bullet}{4}\right\}$; de orden 4 es $\left\{\overset{\bullet}{0}, \overset{\bullet}{2}, \overset{\bullet}{4}, \overset{\bullet}{6}\right\}$; de orden 8 es $\mathbb{Z}_8$. $\blacksquare$

Ejemplo 39. *En el ejemplo* 20 *(página* 321*), se probó que* $(\mathbb{R}^* \times \mathbb{R}, \perp)$ *es un grupo abeliano, donde la operación interna* $\perp$ *es definida por:*

$$(a, b) \perp (c, d) = (4ac, b + d + 3)$$

Pruebe que $\mathcal{H} = \{(x, -3) \;/\; x \in \mathbb{R}^*\}$ *es subgrupo de* $\mathbb{R}^* \times \mathbb{R}$*, es decir,* $\mathcal{H} < \mathbb{R}^* \times \mathbb{R}$*.*

Solución. Es claro que $\mathcal{H}$ es no vacío y además, $\mathcal{H} \subseteq \mathbb{R}^* \times \mathbb{R}$. Para probar lo que se pide, es decir, que $\mathcal{H} < \mathbb{R}^* \times \mathbb{R}$, se utilizará el teorema 5; para ello, dados dos elementos $(x, -3)$ y $(y, -3) \in \mathcal{H}$, se tiene que $(y, -3)^{-1} = \left(\frac{1}{16y}, -6 + 3\right) = \left(\frac{1}{16y}, -3\right)$, con lo cual:

$$\begin{aligned}
(x, -3) \perp (y, -3)^{-1} &= (x, -3) \perp \left(\frac{1}{16y}, -3\right) \\
&= \left(\frac{4x}{16y}, -3 - 3 + 3\right) \\
&= \left(\frac{x}{4y}, -3\right)
\end{aligned}$$

que claramente pertenece a $\mathcal{H}$, pues su segunda entrada es -3; además, como $x \neq 0$ y $y \neq 0$, $\frac{x}{4y} \neq 0$. Es decir, se satisface la condición de cerradura planteada en ese teorema; así, se concluye que $\mathcal{H}$ es subgrupo de $\mathbb{R}^* \times \mathbb{R}$. ■

Ejemplo 40. *Determine todos los subgrupos de* $(P(S), \triangle)$*, donde* $S = \{a, b\}$ *y* $\triangle$ *es la diferencia simétrica.*

Solución. Para un mejor entendimiento, es importante que repase los ejemplos 12, 18 y 24. Como $o(P(S)) = 4$, es decir, el orden de $P(S)$ es 4, utilizando el teorema de Lagrange, se sabe que el orden del subgrupo puede ser 1, 2 o 4, los divisores de 4. Así, se obtiene que de orden 1 se tiene el subgrupo $\{\varnothing\}$; de orden 2, los subgrupos $\{\varnothing, \{a\}\}$ y $\{\varnothing, \{b\}\}$; de orden 4, el subgrupo $P(S)$. ■

Ejemplo 41. *Encuentre los subgrupos de* $(S_3, \circ)$.

Solución. Del ejemplo 30 se tiene que $o(S_3) = 3! = 6$, estos seis elementos de S_3 son las permutaciones:

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Así, por ejemplo, para calcular $p_2 \circ p_5$ y $p_4 \circ p_6$ se hace:

$$p_2 \circ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = p_3$$

$$p_4 \circ p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = p_2$$

Al efectuar todas las composiciones posibles, se construye la tabla de operación para este grupo:

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_4	p_1	p_2	p_6	p_5
p_4	p_4	p_3	p_6	p_5	p_1	p_2
p_5	p_5	p_6	p_2	p_1	p_4	p_3
p_6	p_6	p_5	p_4	p_3	p_2	p_1

De aquí, $e = p_1$, $p_1^{-1} = p_1$, $p_2^{-1} = p_2$, $p_3^{-1} = p_3$, $p_4^{-1} = p_5$, $p_5^{-1} = p_4$, $p_6^{-1} = p_6$. Como $o(S_3) = 6$, utilizando el teorema de Lagrange, se sabe que los posibles subgrupos podrán tener orden 1, 2, 3 y 6. Así, observando lo anterior, se tiene que el subgrupo de orden 1 es $\{p_1\}$; los tres subgrupos de orden 2 son $\{p_1, p_2\}$, $\{p_1, p_3\}$ y $\{p_1, p_6\}$; de orden 3 es $\{p_1, p_4, p_5\}$ y de orden 6 es S_3. ■

Teorema 7. *Todo subgrupo de un p-grupo es un p-grupo.*

Demostración. Sea $\mathcal{H}$ subgrupo de $\mathcal{G}$, y como $\mathcal{G}$ es un p-grupo, se tiene que $o(\mathcal{G}) = p^{\alpha}$. Por el Teorema de Lagrange se sabe que $o(\mathcal{H})$ divide a $o(\mathcal{G}) = p^{\alpha}$; así, $o(\mathcal{H}) = p^{\alpha'}$ para algún $\alpha' \leq \alpha$, y esto dice que $\mathcal{H}$ es p-grupo. $\square$

Ejemplo 42. *Como se mostró en el ejemplo 35, $U_8 = \left\{\dot{1}, \dot{3}, \dot{5}, \dot{7}\right\}$ es un grupo de orden 4 con la multiplicación módulo 8 como operación interna. Además, es subconjunto del conjunto $\mathbb{Z}_8^*$, cuya cardinalidad es 7. Observe que no se contradice el teorema de Lagrange, pues éste es válido sólo para subgrupos de un grupo y U_8 sí es grupo, pero $\mathbb{Z}_8^*$ no lo es, ya que 8 no es primo.* $\blacksquare$

Ejercicios (sección 6.4)

1. Determine todos los subgrupos de $(\mathbb{Z}_7^*, \odot)$. Utilice el ejercicio 7 de la sección 6.2.
2. Determine todos los subgrupos de $(\mathbb{Z}_6, \oplus)$.
3. Determine todos los subgrupos de $(\mathbb{Z}_{11}^*, \odot)$.
4. Determine todos los subgrupos de $(\mathbb{Z}_{12}, \oplus)$.
5. Determine todos los subgrupos de orden 4 de $(\mathbb{Z}_{17}^*, \odot)$.
6. Determine todos los subgrupos de $(U_8, \odot)$.
7. Determine todos los subgrupos de $(U_{15}, \odot)$.
8. Determine todos los subgrupos de $(P(S), \triangle)$, donde $S = \{a, b, c\}$ y $\triangle$ es la diferencia simétrica.
9. Si $M_5 = \{5k \ / \ k \in \mathbb{Z}\}$, pruebe que $(M_5, +) < (\mathbb{Z}, +)$, es decir, que el conjunto formado por los múltiplos del 5 es un subgrupo de los enteros con la adición como operación interna.

10. Sea $A = \{a, b, c, m, n, o\}$. Si se sabe que $(A, *)$ es un grupo y la tabla de operación está dada por:

$*$	a	b	c	m	n	o
a	b	c	a	n	o	m
b	c	a	b	o	m	n
c	a	b	c	m	n	o
m	n	o	m	a	b	c
n	o	m	n	b	c	a
o	m	n	o	c	a	b

(a) Determine el neutro de A y el inverso de cada elemento.

(b) Determine si $W_1 = \{c\}$ y $W_2 = \{m, c, o\}$ son subgrupos de A.

(c) Encuentre todos los subgrupos de A.

(d) Calcule el resultado de $\left(m^{-46} * o^4\right)^2 * \left(b * n^{-1}\right)^{-1}$.

11. En el ejemplo 20 se probó que $(\mathbb{R}^* \times \mathbb{R}, \perp)$ es un grupo abeliano, donde la operación interna $\perp$ es definida por:

$$(a, b) \perp (c, d) = (4ac, b + d + 3)$$

Pruebe que $\mathcal{H} = \left\{\left(\frac{1}{4}, x\right) \ / \ x \in \mathbb{R}\right\}$ es subgrupo de $\mathbb{R}^* \times \mathbb{R}$, es decir, $\mathcal{H} < \mathbb{R}^* \times \mathbb{R}$. (Puede repasar el ejemplo 39).

12. Si $W = \{a + b\sqrt{2} \ / \ a, b \in \mathbb{Z}\}$. Pruebe que $(W, +) < (\mathbb{R}, +)$, es decir, que el conjunto formado por los números de la forma $a+b\sqrt{2}$ con a y b enteros es un subgrupo de los reales con la adición como operación interna.

13. Según lo probado en el ejercicio 3, propuesto en la página 328, se sabe que $(\mathbb{R}^*, *)$ con $a * b = 4ab$ es un grupo abeliano. Pruebe que $\mathcal{H} =]-\infty, 0[$ es subgrupo de $\mathbb{R}^*$, es decir, $\mathcal{H} < \mathbb{R}^*$.

14. Según lo probado en el ejercicio 4, propuesto en la página 328, se sabe que $(\mathbb{R} \times \mathbb{R}^*, \otimes)$ es grupo, con $\otimes$ definida por:

$$(a, b) \otimes (c, d) = (a + c - 4, 2bd)$$

Pruebe que $\mathcal{H} = \{(4, x) \ / \ x \in \mathbb{R}^*\}$ es subgrupo de $\mathbb{R} \times \mathbb{R}^*$, es decir, $\mathcal{H} < \mathbb{R}^* \times \mathbb{R}$.

15. Se sabe que $(\mathbb{Z}_3, \oplus)$ y $(\mathbb{Z}_5^*, \odot)$ son grupos; considere el conjunto $\mathcal{G} = \mathbb{Z}_3 \times \mathbb{Z}_5^*$, cuya ley de composición $*$ se define como:

$$(a, b) * (c, d) = (a \oplus c, b \odot d)$$

Encuentre el neutro, el inverso de cada elemento, concluya que $\mathcal{G}$ es grupo abeliano. Además, calcule todos sus subgrupos.

16. Si $(\mathcal{G}, *)$ es un grupo, pruebe que el centro de $\mathcal{G}$ es un subgrupo de $\mathcal{G}$ (véase página 313), es decir, pruebe que $C(\mathcal{G}) < \mathcal{G}$.

17. Sobre el conjunto de funciones $\mathcal{G} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, donde $f_1 = x$, $f_2 = \frac{1}{x}$, $f_3 = 1 - x$, $f_4 = \frac{1}{1-x}$, $f_5 = \frac{x-1}{x}$, $f_6 = \frac{x}{x-1}$, y la composición de funciones como operación interna (véase ejercicio 19 de la sección 6.2 y su respectiva solución). Determine todos los subgrupos de $(\mathcal{G}, \circ)$.

18. Calcule todos los subgrupos del grupo de Klein (véase página 335).

19. Dado $(\mathcal{G}, *)$, un grupo, y $\mathcal{H}$, un subgrupo de $\mathcal{G}$. Defina para a y $b \in \mathcal{G}$ la relación $\mathcal{R}$ sobre el grupo $\mathcal{G}$ por:

$$a\mathcal{R}b \Leftrightarrow a * b^{-1} \in \mathcal{H}$$

Pruebe que la relación $\mathcal{R}$ es de equivalencia sobre $\mathcal{G}$.

6.5 Homomorfismos de grupos

En ocasiones, las relaciones biyectivas entre dos conjuntos permiten resolver un problema en uno de los conjuntos, y una vez que se resuelve este, se utiliza la biyección para devolverse al conjunto inicial. Los cambios de variables en la solución de ecuaciones o de integrales; la transformada de Laplace en la solución de ecuaciones diferenciales; en las bases de espacios vectoriales y sus transformaciones son algunas de las aplicaciones de estos principios.

Si $(\mathcal{G}, *)$ y $(\mathcal{F}, \perp)$ son dos grupos, se dice que una aplicación $f\colon \mathcal{G} \to \mathcal{F}$ es un **homomorfismo de grupos** si para todo a y b en $\mathcal{G}$ se satisface que:

$$f(a * b) = f(a) \perp f(b)$$

Si, además de ser homomorfismo,

- f es sobreyectiva, entonces f es un **epimorfismo**.
- f es inyectiva, entonces f es un **monomorfismo**.
- f es biyectiva, entonces f es un **isomorfismo**.
- $\mathcal{G} = \mathcal{F}$, entonces f es un **endomorfismo**.
- $\mathcal{G} = \mathcal{F}$ y f biyectiva, entonces f es un **automorfismo**.

Ejemplo 43. *Como ya se sabe que* $(\mathbb{R}^+, \cdot)$ *y* $(\mathbb{R}, +)$ *son grupos, y la función* $f\colon \mathbb{R}^+ \to \mathbb{R}$ *dada por* $f(x) = \ln x$ *cumple*

$$f(a \cdot b) = \ln(a \cdot b) = \ln a + \ln b = f(a) + f(b)$$

se concluye que f *es un homomorfismo de grupos. Además, se sabe que* $\ln$ *es una función biyectiva de* $\mathbb{R}^+$ *en* $\mathbb{R}$*; por lo tanto, se concluye que* f *es un isomorfismo de grupos.* ■

Teorema 8. *Sean* $(\mathcal{G}, \cdot)$ *y* $(\mathcal{F}, *)$ *dos grupos. Si* $f\colon \mathcal{G} \to \mathcal{F}$ *es un homomorfismo de grupos, si* e *es el elemento neutro de* $\mathcal{G}$ *y además* e' *es el elemento neutro de* $\mathcal{H}$*, entonces se cumple que:*

$$\begin{aligned} f(e) &= e' & (6.7) \\ f(x^{-1}) &= [f(x)]^{-1} & (6.8) \end{aligned}$$

Demostración. Para demostrar (6.7), basta observar que:

$$f(e) = f(e \cdot e) = f(e) * f(e)$$

por lo que $f(e) = e'$. Para demostrar (6.8), basta ver que:

$$e' = f(e) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$$

Para concluir que $f(x)$ y $f(x^{-1})$ son inversos entre sí, pues al operarse se obtiene el elemento neutro, con lo cual se concluye que $f(x^{-1}) = [f(x)]^{-1}$. □

Para un homomorfismo de grupos $f\colon \mathcal{G} \to \mathcal{F}$ se define el **núcleo de *f*** como el conjunto:

$$N_f = f^{-1}(\{e'\})$$

donde e' es el elemento neutro de $\mathcal{F}$. Es decir, el núcleo de un homomorfismo está formado por los elementos cuya imagen es el neutro. Además, se define la **imagen de *f*** como $\boldsymbol{Im(f) = f(\mathcal{G})}$, es decir, el ámbito de f.

Teorema 9. *Sean* $(\mathcal{G}, \cdot)$ *y* $(\mathcal{F}, *)$ *dos grupos, además, sea* e *el elemento neutro de* $\mathcal{G}$ *y* e' *el elemento neutro de* $\mathcal{F}$*. Si* $f\colon \mathcal{G} \to \mathcal{F}$ *es un homomorfismo de grupos, entonces* $N_f = \{e\}$ *si y solo si* f *es inyectiva.*

Demostración. Es necesario probar la equivalencia; para ello, se procede de la manera usual, demostrando ambas implicaciones:

"$\Rightarrow$" Como hipótesis, se tiene que $N_f = \{e\}$, se debe probar que f es una función inyectiva; para ello se utiliza el resultado (4.2):
Prueba:

$$\begin{aligned} f(a) = f(b) &\Rightarrow f(a) * [f(b)]^{-1} = e' \\ &\Rightarrow f(a) * f(b^{-1}) = e' \\ &\Rightarrow f(a \cdot b^{-1}) = e' \\ &\Rightarrow a \cdot b^{-1} \in N_f = \{e\} \\ &\Rightarrow a \cdot b^{-1} = e \\ &\Rightarrow a = b \end{aligned}$$

Con lo cual, f es inyectiva.

"$\Leftarrow$" Como hipótesis, se tiene que f es una función inyectiva, se debe probar que $N_f = \{e\}$. A partir del resultado (6.7) se cumple que $\{e\} \subseteq N_f$. Para la inclusión $N_f \subseteq \{e\}$, si $x \in N_f$, se tiene que $f(x) = e'$, y aplicando el resultado (6.7), se tiene $f(x) = f(e)$. Así, utilizando la hipótesis de que f es inyectiva, $x = e$, se ha demostrado la otra inclusión y con ello la igualdad $N_f = \{e\}$.

Con lo cual, se ha demostrado este resultado. $\square$

Ejemplo 44. *Sea $(\mathcal{G}, \cdot)$ un grupo abeliano. Demuestre que la función $h\colon \mathcal{G} \to \mathcal{G}$ definida por $h(x) = x^{-1}$ es un automorfismo.*

Solución. Como $\mathcal{G}$ es abeliano, se tiene que $y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1}$. Así, $h(x \cdot y) = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1} = h(x) \cdot h(y)$; con esto, h es un homomorfismo. Además, es claro que h es sobreyectiva ya que todo elemento $y \in \mathcal{G}$ tiene por preimagen a y^{-1} pues, $h(y^{-1}) = (y^{-1})^{-1} = y$; por otro lado, se tiene que $h(x) = e \Leftrightarrow x^{-1} = e \Leftrightarrow x = e$, con lo cual $N_h = \{e\}$. Así, es inyectiva en virtud del teorema 9; de esta forma, se ha probado que h es biyectiva y, finalmente, h es un automorfismo. $\blacksquare$

Ejemplo 45. *Sea $(H, \cdot)$ un grupo y sea a un elemento fijo en H. Demuestre que $\varphi\colon H \to H$ definida por $\varphi(x) = a^{-1}{\cdot}x{\cdot}a$ es un automorfismo de grupos.*

Solución. Primero se demuestra que es un homomorfismo:

$$\begin{aligned}
\varphi(x \cdot y) &= a^{-1} \cdot x \cdot y \cdot a \\
&= a^{-1} \cdot x \cdot e \cdot y \cdot a \\
&= a^{-1} \cdot x \cdot a \cdot a^{-1} \cdot y \cdot a \\
&= (a^{-1} \cdot x \cdot a) \cdot (a^{-1} \cdot y \cdot a) \\
&= \varphi(x) \cdot \varphi(y)
\end{aligned}$$

Sea $x \in N_\varphi$, entonces $\varphi(x) = e$, es decir, $a^{-1}{\cdot}x{\cdot}a = e$. Se multiplica a la derecha por a^{-1} y a la izquierda por a, se obtiene que $x = a \cdot e \cdot a^{-1} = e$, con lo que $N_\varphi = \{e\}$ y, por lo tanto, φ es inyectiva. Para verificar que φ es sobreyectiva, considere $y \in H$. Se tiene que:

$$\varphi(a \cdot y \cdot a^{-1}) = a^{-1} \cdot (a \cdot y \cdot a^{-1}) \cdot a = y$$

Así, $a \cdot y \cdot a^{-1}$ es preimagen de y. Se ha probado que φ es un homomorfismo biyectivo; por lo tanto, φ es un isomorfismo en donde el grupo de salida y llegada es el mismo; así, φ es un automorfismo. ■

Ejemplo 46. *Considere el espacio $\mathcal{M}_{2\times 2}$ de las matrices de 2×2 con entradas en $\mathbb{R}$, con la suma usual de matrices como operación interna. Sea $\phi\colon \mathcal{M}_{2\times 2} \to \mathcal{M}_{2\times 2}$ definida por:*

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix}$$

Pruebe que ϕ es un homomorfismo de grupos y encuentre su núcleo.

Solución. Se tiene que:

$$\begin{aligned}
\phi\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] &= \phi\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \\
&= \begin{pmatrix} a+a'-d-d' & 0 \\ 0 & b+b'-c-c' \end{pmatrix} \\
&= \begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix} + \begin{pmatrix} a'-d' & 0 \\ 0 & b'-c' \end{pmatrix} \\
&= \phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \phi\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}
\end{aligned}$$

Como el elemento neutro de $\mathcal{M}_{2\times 2}$ es $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, en el núcleo de ϕ están las matrices que satisfacen $\begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, con lo cual $a = d$ y $b = c$; por lo tanto, el núcleo de ϕ está formado por todas las matrices de la forma $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$. ■

Ejemplo 47. *Sean $(\mathcal{G},+)$ y $(\mathcal{H},+)$ grupos abelianos, y $f\colon \mathcal{G} \to \mathcal{H}$ un homomorfismo de grupos. Considere $\varphi\colon \mathcal{G}\times\mathcal{H} \to \mathcal{G}\times\mathcal{H}$ tal que:*

$$\forall\,(a,b) \in \mathcal{G}\times\mathcal{H}\colon \varphi\big((a,b)\big) = (a, b - f(a))$$

Demuestre que φ es un epimorfismo de grupos.

Solución. Para probar que φ es un homomorfismo, basta ver que:

$$\begin{aligned}
\varphi((a,b)+(c,d)) &= \varphi((a+c, b+d)) \\
&= (a+c, b+d-f(a+c)) \\
&= (a+c, b+d-f(a)-f(c)) \\
&= (a, b-f(a)) + (c, d-f(c)) \\
&= \varphi((a,b)) + \varphi((c,d))
\end{aligned}$$

Para determinar si es inyectiva, se calcula el N_φ. Si $(a,b) \in N_\varphi$, se tiene que:

$$(e,e') = \varphi(a,b) = (a, b - f(a))$$

con lo que $a = e$ y $b - f(a) = e'$, de donde se obtiene que $(a,b) = (e,e')$ y $N_\varphi = \{(e,e')\}$. De esto último, y utilizando el resultado del teorema 9, se concluye que φ es inyectiva. Por otro lado, es claro que para todo $(a,b) \in \mathcal{G} \times \mathcal{H}$ se tiene que $(a, b + f(a))$ es su preimagen, ya que se cumple:

$$\varphi\big((a, b + f(a))\big) = (a,b)$$

Así, φ es sobreyectiva, por lo que finalmente es posible concluir que φ es un epimorfismo de grupos. ■

Teorema 10. *Si $f\colon (\mathcal{G},\cdot) \to (\mathcal{F},*)$ es un homomorfismo de grupos, entonces $N_f < \mathcal{G}$.*

Demostración. Es necesario demostrar que N_f es un subgrupo de $\mathcal{G}$, para ello se utilizará el teorema 5. En primer lugar, por la misma definición de N_f es claro que $N_f \subseteq \mathcal{G}$; además, como $f(e) = e'$, se cumple que $e \in N_f$, por tanto $N_f \neq \varnothing$. Por último, si a y $b \in N_f$ se cumple que $f(a) = e'$, $f(b) = e'$, de esta forma:

$$\begin{aligned} f\left(a \cdot b^{-1}\right) &= f(a) * [f(b)]^{-1} \\ &= e' * [e']^{-1} \\ &= e' \end{aligned}$$

Por lo que se tiene que $a \cdot b^{-1} \in N_f$. □

Teorema 11. *Si $f\colon (\mathcal{G},\cdot) \to (\mathcal{F},*)$ es un homomorfismo de grupos, entonces $Im(f) < \mathcal{F}$.*

Demostración. Es necesario demostrar que $Im(f)$ es un subgrupo de $\mathcal{F}$. Para ello se utilizará el teorema 5. En primer lugar, por la misma definición $Im(f) = f(\mathcal{G})$ es claro que $Im(f) \subseteq \mathcal{F}$; además, como $e' = f(e) \in f(\mathcal{G}) = Im(f)$, se tiene que $Im(f) \neq \varnothing$. Por último, sean x, $y \in Im(f)$, por la definición existen a, $b \in \mathcal{G}$ tales que $f(a) = x$, $f(b) = y$, de esta forma:

$$\begin{aligned} x * y^{-1} &= f(a) * [f(b)]^{-1} \\ &= f(a) * f(b^{-1}) \\ &= f(a \cdot b^{-1}) \end{aligned}$$

Como $a \cdot b^{-1} \in \mathcal{G}$, finalmente se tiene que $x * y^{-1} \in Im(f)$. $\square$

Ejemplo 48. *Sea φ el homomorfismo de grupos $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}_5, \oplus)$, definido de forma natural por $\varphi(a) = \overset{\bullet}{a}$. Determine el N_φ y la $Im(\varphi)$, concluya que solo es un epimorfismo.*

Solución. Es claro que $x \in N_\varphi \Leftrightarrow \varphi(x) = \overset{\bullet}{0}$ y esto ocurre cuando x es un múltiplo de 5, es decir, $N_\varphi = \{5k \ / \ k \in \mathbb{Z}\}$, y por el teorema 9, φ no es inyectiva. Por otro lado, $Im(\varphi) = \mathbb{Z}_5$, por lo que φ es sobreyectiva. Así, es claro que es solo un epimorfismo. $\blacksquare$

Es interesante notar que, del ejemplo anterior y utilizando el teorema 10, se puede concluir que el conjunto formado por los múltiplos de 5 es un subgrupo de $(\mathbb{Z}, +)$. Sin embargo, puede comparar con el ejercicio 9 (página 340), en donde se hace la misma conclusión, pero aplicando el teorema 5.

Ejercicios (sección 6.5)

1. Pruebe que $f\colon \mathbb{R} \to \mathbb{R}^+$ dada por $f(x) = e^x$ es un homomorfismo entre los grupos $(\mathbb{R}, +)$ y $(\mathbb{R}^+, \cdot)$.

2. Pruebe que $f\colon \mathbb{R}^* \to \mathbb{R}^*$ dada por $f(x) = x^2$ es un homomorfismo entre los grupos $(\mathbb{R}^*, \cdot)$ y $(\mathbb{R}^*, \cdot)$.

3. Compruebe que $f\colon \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x + 2$ no es un homomorfismo entre los grupos $(\mathbb{R}, +)$ y $(\mathbb{R}, +)$.

4. Considere el conjunto A formado por los polinomios de la forma $ax + b$ con a, $b \in \mathbb{Z}$, con la suma de polinomios usual como la operación interna, es decir, $(ax+b)+(cx+d) = (a+c)x+(b+d)$. En el ejercicio 15 en la página 330, se prueba que $(A, +)$ es un grupo. Defina $\varphi\colon (A, +) \to (\mathbb{Z}, +)$, por medio de $\varphi(ax+b) = 3a+b$

   (a) Pruebe que es un epimorfismo de grupos.

   (b) Calcule el núcleo de φ y determine si es un monomorfismo.

5. Considere el grupo $\mathcal{F} = \mathbb{Z}$ con la suma usual de enteros, y $\mathcal{G} = \{-1, 1\}$ el subgrupo de $(\mathbb{R}^*, \cdot)$ formado sólo por estos dos elementos. Sea $\varphi\colon \mathcal{F} \to \mathcal{G}$ definida como $\varphi(n) = 1$ si n es par y $\varphi(n) = -1$ si n es impar. Compruebe que φ es un homomorfismo de grupos.

6. Demuestre que el grupo $(\mathcal{G}, \circ)$, del ejemplo 18 de la sección 6.2, es isomorfo al grupo de Klein $(\mathcal{K}, \circ)$, definido en el ejemplo 7 de la misma sección.

7. Sea x un número racional arbitrario pero fijo, considere el grupo $(\mathbb{Z}, +)$, el conjunto de los números enteros con la suma usual, y el grupo $(\mathbb{Q}^*, \cdot)$, el conjunto de los números racionales diferentes de cero con el producto usual. Sea $\varphi\colon \mathbb{Z} \to \mathbb{Q}^*$, definida como $\varphi(n) = x^n$. Pruebe que φ es un isomorfismo de grupos.

8. Sea $\mathcal{G}$ un grupo cíclico de orden 5, con h su generador. Sea

$$\varphi\colon (\mathbb{Z}_5, +) \to (\mathcal{G}, \cdot)$$

   donde $\varphi\left(\overset{\bullet}{k}\right) = h^k$. Pruebe que φ es un isomorfismo de grupos.

9. Suponga que $(\mathcal{G}, *)$ es un grupo. Pruebe que si $f\colon \mathcal{G} \to \mathcal{G}$ dada por $f(x) = x^{-1}$ es un homomorfismo, entonces $(\mathcal{G}, *)$ es abeliano.

10. Al conjunto $\mathbb{R}$ se le dota de la ley de composición $*$ definida como:

$$x * y = \sqrt[3]{x^3 + y^3}$$

Pruebe que $(\mathbb{R}, *)$ es un grupo y que $(\mathbb{R}, *)$ es isomorfo a $(\mathbb{R}, +)$.

11. Considere el grupo $(\mathbb{R} \times \mathbb{R}, \oplus)$, donde $\oplus$ se define como:

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

Además, el grupo $(\mathbb{R} \times \mathbb{R}^*, *)$, donde $*$ se define como:

$$(a, b) * (c, d) = (a + c, bd)$$

Sea $\varphi\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}^*$ definida como $\varphi\big((x, y)\big) = (x, 2^y)$. Pruebe que φ es un isomorfismo de grupos.

12. Sean $(\mathbb{R}^+, \cdot\,)$ y $(\mathbb{R}, +)$ los grupos de números reales, y considere el conjunto $\mathbb{R}^+ \times \mathbb{R}$ con la estructura del producto cartesiano dada por la operación interna $(a, b) * (c, d) = (ac, b + d)$. Defina la aplicación $\varphi\colon \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}^+ \times \mathbb{R}$, por $\varphi(a, b) = (a, b - \ln(a))$.

    (a) Verifique que $\ln\colon (\mathbb{R}^+, \cdot\,) \to (\mathbb{R}, +)$, la función logaritmo natural, es un homomorfismo de grupos.

    (b) Pruebe que φ es un epimorfismo de grupos.

    (c) Determine el núcleo de φ.

    (d) ¿Qué puede decirse de la aplicación φ con respecto al resultado obtenido en (b) y (c)?

13. Considere $\phi\colon (\mathbb{Z}_6, +) \to (\mathbb{Z}_3, +)$ definida por $\phi([a]) = \overline{a}$, donde $[a]$ denota la clase de equivalencia módulo 6 y $\overline{a}$ denota la clase de equivalencia módulo 3.

    (a) Calcule el N_ϕ y concluya si ϕ es o no inyectiva.

    (b) Calcule el conjunto $\phi(\mathbb{Z}_6)$ y concluya si ϕ es o no sobreyectiva.

14. Sea $(\mathcal{G}, \cdot)$ un grupo. Sobre el conjunto $\mathcal{G} \times \mathcal{G}$ se define la operación $*$ como $(a, b) * (c, d) = (ac, bd)$.

    (a) Pruebe que $(\mathcal{G} \times \mathcal{G}, *)$ es un grupo.

    (b) Pruebe que la aplicación $\varphi\colon (\mathcal{G}, \cdot) \to (\mathcal{G} \times \mathcal{G}, *)$ dada por $\varphi(a) = (a, a)$ es un monomorfismo de grupos.

15. Sea $U_9 = \left\{\dot{1}, \dot{2}, \dot{4}, \dot{5}, \dot{7}, \dot{8}\right\}$ y considere la operación producto habitual de clases: $\dot{a} \odot \dot{b} = \dot{ab}$.

    (a) Demuestre que $\phi\colon U_9 \to U_9$ tal que $\phi(\dot{a}) = \left(\dot{a}\right)^2$ es un endomorfismo de grupos.

    (b) Determine N_ϕ. ¿Qué puede decirse de ϕ?

    (c) Dé por extensión el conjunto $\phi(U_9)$ y concluya si es sobreyectiva o no.

Capítulo 7
Bases y congruencias numéricas

“Si las matemáticas son
la reina de las ciencias,
la teoría de números es
la reina de las matemáticas”.

Gauss

Sistemas de numeración
Representación en bases enteras
Aritmética en distintas bases
Representación en bases fraccionarias
Congruencias numéricas
Resultados importantes

En este capítulo se introducen los sistemas de numeración en diferentes bases; además, el tema de las congruencias, y se dan algunos teoremas importantes en la teoría de números, como son los teoremas de Wilson, Fermat, Euler, entre otros. Este es un tema muy amplio, razón por la cual se hace solamente una breve introducción al tema.

Para profundizar en los temas tratados en este capítulo, consulte las referencias bibliográficas [1], [13], [20], [26] y [38].

7.1 Sistemas de numeración

Todos los pueblos, de alguna manera, empiezan a contar. Algunos controlaban sus cabezas de ganado grabando por cada unidad una marca en la corteza de un árbol; otros hacían nudos en una liana o amontonaban palos. Esta idea coincide lógica y naturalmente con el concepto matemático de la *correspondencia biunívoca.* En algunas tribus australianas, *uno* se dice *urapum*; *dos* se dice *okasa*; *tres* se convierte en *okasa urapum*, es decir, dos más uno; *cuatro* se convierte en *okasa okasa*, es decir, dos más dos; *cinco* se convierte en *okasa okasa urapum* (dos más dos más uno); *seis* se convierte en *okasa okasa okasa* (dos más dos más dos), no saben contar más de seis. Otras tribus cuentan, simplemente, *uno* y *muchos.*

Es así que un **número natural** se entiende como una *idea* asociada a un conjunto de objetos, que a la vez se puede asociar con cualquier conjunto de objetos equipotente con él. Es decir, como $A = \{\heartsuit, *, \dagger, \triangle\}$ tiene cuatro elementos, el número cuatro se asocia con todos los conjuntos equipotentes con él.

Para representar la idea de número, se utilizan los **numerales**, que son palabras o símbolos. Por ejemplo, las palabras: *cinco* en español, *five* en inglés; los símbolos 5 en el sistema indoarábigo, ||||| en egipcio, V en romano, —— en maya, ▼▼▼▼▼ en babilonio representan al mismo número, es decir, estos símbolos fueron usados en algún momento por determinado pueblo para representar la cantidad de elementos que tenía un conjunto con cinco elementos.

Un **sistema de numeración** es una colección de símbolos para representar números, y un conjunto de reglas bien definidas para combinarlos. Estas reglas son propias de cada sistema de numeración y no funcionan para otro. En un **sistema numérico** se consideran los números y sus propiedades, independientemente de los símbolos que se usan para representarlos. Las propiedades propias de los números son independientes del sistema; por ejemplo, el 5 siempre será primo; los números racionales tienen representación decimal periódica, entre otras.

El concepto de la base del sistema de numeración tiene que ver, en muchos casos, con la forma en que se contaba; así, algunos pueblos usaban base 5, base 10, base 20, que respectivamente correspondía a los dedos de una mano, dos manos, dedos de manos y pies. En el caso de un sistema posicional, tiene que ver con el **principio de agrupación**, el cual consiste en hacer, con los elementos del conjunto, otros conjuntos con determinado número de elementos.

Ejemplo 1. *Considere un conjunto con* 13 *elementos y* 2 *como base, es decir, se harán conjuntos de* 2 *elementos. Comience agrupando de dos en dos: sobra uno y se obtienen seis grupos de dos; luego, se procede a agrupar de dos en dos los seis grupos anteriores: se obtienen tres grupos; por último, estos se agrupan de dos en dos y se obtiene un grupo y sobra otro. Este agrupamiento se puede observar en la figura* 7.1. ■

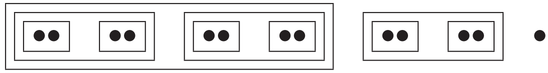


Figura 7.1: Agrupamiento de 13 en base 2.

Ejemplo 2. *Si se considera el mismo conjunto de* 13 *elementos pero ahora agrupado en conjuntos de* 3 *elementos, el agrupamiento se puede observar en la figura* 7.2. ■

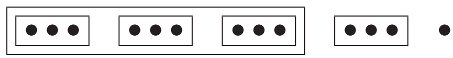


Figura 7.2: Agrupamiento de 13 en base 3.

Con base en los dos ejemplos anteriores, se ha observado que el número 13 en el sistema decimal se puede representar como 1101 en base 2, o como 111 en base 3. Es posible escribir, por comodidad, $13 = (13)_{10} = (1101)_2 = (111)_3$.

En los **sistemas de numeración no posicionales**, cada símbolo o numeral representa siempre el mismo número. El principal inconveniente de tales sistemas es su limitación, pues para representar números mayores habría que utilizar nuevos símbolos. El sistema egipcio era un sistema no posicional.

En los **sistemas de numeración posicionales** se resuelve el problema de la limitación utilizando el **principio de posición**, el cual establece que cada símbolo puede tener diferentes valores según su posición en el numeral del que forma parte. En dichos sistemas, cada símbolo tiene relacionados dos valores: uno que es independiente del lugar que ocupa en el numeral y otro que depende de su posición en el numeral. El valor de cada posición es una potencia de la base del sistema. Así por ejemplo, en el numeral 111 en el sistema decimal, el primer uno representa a una centena, el segundo representa a una decena y el último representa a una unidad, es decir, como la base es 10, se representa en potencias de la base, o sea, $111 = 1 \cdot 10^2 + 1 \cdot 10^1 + 1 \cdot 10^0$.

Algunos sistemas de numeración importantes de la antiguedad son el chino, que utilizaba dos sistemas, uno de tipo multiplicativo y otro parecido a un sistema posicional; y el egipcio, el cual se dividía en dos: el jeroglífico, de base 10 y no posicional, y el hierático, utilizado por los sacerdotes, en donde los símbolos eran sustituidos por otros especiales que representaban los números del 1 al 10 y otros símbolos para las potencias de 10.

En el sistema egipcio, por ejemplo, se disponía de siete símbolos, cada uno de los cuales se puede escribir máximo nueve veces en el mismo numeral; por esta razón, el mayor número que se puede representar es el que corresponde al número 9 999 999 en el sistema decimal.

A continuación, como ejemplo, se verán solamente los sistemas de numeración romano, griego, babilonio y maya.

7.1.1 Sistema de numeración romano

El sistema de numeración romano es uno de los más conocidos y todavía se usa en muchos ámbitos. En la siguiente tabla se presentan los numerales romanos y su equivalente al sistema decimal:

I	V	X	L	C	D	M
1	5	10	50	100	500	1000

A estos símbolos se pueden combinar siguiendo las siguientes reglas:

1. Principio aditivo: si un símbolo se escribe a la derecha de otro de mayor valor, los número se suman. Por ejemplo, VII= 7, CX= 110.

2. Principio sustractivo: si un símbolo se escribe a la izquierda de otro de mayor valor, se resta del mayor el menor de los números representados. Por ejemplo, XC= 90, CD= 400.

3. No se pueden repetir más de tres numerales iguales en forma continua, y no puede aparecer consecutivamente más de un V, más de un L, más de un D. Por ejemplo, XXX= 30, XL= 40.

4. El principio sustractivo no se aplica para los símbolos V, L, D. Por ejemplo, no se puede escribir VX ni LC.

5. Los numerales que se escriben a la izquierda para expresar resta son: I antes que V y X; X antes de L y C; C antes de D y M.

6. Un segmento horizontal sobre los numerales significa que se multiplica por 1000. Por ejemplo, $\overline{\text{XX}}\text{DCI} = 20\,601$; $\overline{\text{C}}\text{IX} = 101\,010$.

El hecho de que los romanos no tuvieran el "cero" hace que los numerales fueran muy complicados; por ejemplo 1986 =MCMLXXXVI.

7.1.2 Sistema de numeración griego

Fueron dos los más usados, ambos sistemas de base 10: el *ático* o *herodiano*, utilizado con frecuencia en las inscripciones atenienses, y el sistema *jónico* o alfabético.

Sistema ático. Los símbolos son los siguientes: el uno se representa por $|$ y se puede repetir hasta cuatro veces; $\Gamma = 5$, $\Delta = 10$, $\text{H} = 100$, $\text{X} = 1000$, $\text{M} = 10000$. Para los otros números se hacen combinaciones utilizando el principio aditivo; para algunos particulares se simplifica la notación con el principio multiplicativo. Por ejemplo, 50 no se representa con cinco deltas, sino más bien como $5 \cdot 10$ y se escribe como $\Gamma^{\Delta} = 50$, de la misma forma: $\Gamma^{\text{H}} = 500$, $\Gamma^{\text{X}} = 5000$ y $\Gamma^{\text{M}} = 50\,000$.

Ejemplo 3. *En este sistema,* 18 *se representa como* $\Delta\,\Gamma\,|||$. ■

Ejemplo 4. *El número* 34 787 *se representa en el sistema ático por medio de* $\text{M M M X X X X}\,\Gamma^{\text{H}}\,\text{H H}\,\Gamma^{\Delta}\Delta\Delta\Delta\Gamma\,||$. ■

Sistema jónico. También es un sistema aditivo en base 10, que sustituyó al ático cerca del siglo III a.C. En el cuadro 7.1 se muestran los símbolos que utilizaron, básicamente son las letras de su alfabeto.

$\alpha \to 1$	$\varsigma \to 6$	$\kappa \to 20$	$o \to 70$	$\tau \to 300$	$\omega \to 800$
$\beta \to 2$	$\zeta \to 7$	$\lambda \to 30$	$\pi \to 80$	$\upsilon \to 400$	ϡ $\to 900$
$\gamma \to 3$	$\eta \to 8$	$\mu \to 40$	ϙ $\to 90$	$\phi \to 500$	
$\delta \to 4$	$\theta \to 9$	$\nu \to 50$	$\rho \to 100$	$\chi \to 600$	
$\epsilon \to 5$	$\iota \to 10$	$\xi \to 60$	$\sigma \to 200$	$\psi \to 700$	

Tabla 7.1: Símbolos del sistema de numeración jónico.

Los múltiplos de 1000, menores que 10 000, se representaban con una comilla al lado de las unidades; por ejemplo, 9000 se escribía como $'\theta$. Los múltiplos de 10 000 se representaban escribiendo una M y sobre ella el múltiplo; por ejemplo, 40 000 se escribe como $\overset{\delta}{\mathrm{M}}$.

Ejemplo 5. *En el sistema jónico,* 189 *se representa como* $\rho\pi\theta$*.* ■

Ejemplo 6. *En este sistema,* $\overset{\gamma}{\mathrm{M}}\,'\delta\psi\pi\zeta$ *representa al número* 34 787*.* ■

7.1.3 Sistema de numeración babilonio

Hacia el año 2000 a.C., los babilonios crearon el sistema sexagesimal, posicional de base 60. Al parecer, la escogencia de esta base está relacionada con que hay aproximadamente 6 veces 60 días en un año y que una circunferencia contiene aproximadamente 6 radios. Tal sistema todavía se utiliza para la medición del tiempo y de los ángulos, pero con los símbolos del sistema decimal.

En el sistema babilónico se utilizaban dos símbolos: ▼ para el uno (una cuña) y ◀ (dos cuñas superpuestas) para el diez. Los símbolos se podían repetir hasta un máximo de nueve veces; además, para indicar el valor posicional, se dejaba un espacio entre cada grupo de símbolos. Algunos ejemplos:

1. El 3 se representa por ▼▼▼
2. El 8 se representa por ▼▼▼▼ ▼▼▼▼ o por ▼▼▼ ▼▼▼▼▼ lo importante es que se tengan 8 cuñas.
3. El 24 se representa por ◀◀ ▼▼ ▼▼
4. El 80 se representa por ▼ ◀◀ pues, como la base es 60 y el espacio del centro indica la posición, se tiene que el numeral representa a $1 \cdot 60 + 20 = 80$.
5. El 3682 se representa por ▼ ▼ ◀◀▼▼ pues la primera cuña está en la posición que corresponde a $1 \cdot 60^2$. Luego, el espacio indica que la segunda corresponde a $1 \cdot 60$ y las unidades son 22; así, el numeral dado representa a $1 \cdot 60^2 + 1 \cdot 60 + 22 = 3682$.

Los babilonios tenían un desarrollo matemático muy avanzado, manejaban los conceptos de ecuaciones en una incógnita, sistemas de ecuaciones con dos incógnitas, volúmenes y superficies, entre otros. En unas tabletas que datan del año 3000 a.C. se encuentra sobre la diagonal de un cuadrado, de lado ▼, el número

▼ ◀◀▼▼▼▼ ◀◀◀◀◀▼ ◀

Suponiendo que el punto sexagesimal está entre el 1 y el 24, representa el número

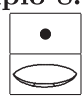
$$\begin{aligned} 1 + 24 \cdot \frac{1}{60} + 51 \cdot \frac{1}{60^2} + 10 \cdot \frac{1}{60^3} &= 1 + \frac{2}{5} + \frac{51}{3\,600} + \frac{1}{216\,000} \\ &\approx 1,4142129 \end{aligned}$$

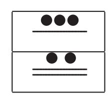
que con gran exactitud aproxima a $\sqrt{2}$.

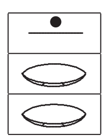
7.1.4 Sistema de numeración maya

Este sistema de numeración es, sin duda, el más notable de la antiguedad, y su importancia radica en la inclusión del cero. Hacia el siglo IV d.C., lo utilizaron con gran presición en cálculos relacionados con la astronomía, entre otros. Es un sistema posicional de base 20, y se representaba o escribía en forma vertical. Ellos utilizaron tres símbolos:  para el cero, que representaba un caracol o el ojo cerrado, que no ve nada; el • para el uno y un segmento horizontal —— para el cinco.

Ejemplo 7. *El número* 3 *se representa por* •••, *a* 13 *se le representa como*  *y el* 17 *se representa por* . ■

Ejemplo 8. *Como* $20 = 1 \cdot 20^1 + 0 \cdot 20^0$, *se tiene que* 20 *se representa como* . ■

Ejemplo 9. *El número* 172 *se representa por el numeral* , *ya que* $8 \cdot 20^1 + 12 \cdot 20^0 = 172$. ■

Ejemplo 10. *El numeral*  *representa a* 2400, *pues se tiene que* $6 \cdot 20^2 + 0 \cdot 20^1 + 0 \cdot 20^0 = 2400$. ■

Ejercicios (sección 7.1)

Escriba cada uno de los cuatro números 326, 4567, 34 788, 687 941 en los sistemas romano, griego, babilonio y maya.

7.2 Representación en bases enteras

Después de repasar los cuatro sistemas de numeración dados en la sección 7.1 y los conjuntos numéricos dados en la sección 2.2, es importante recordar que en el algoritmo de la división euclideana, los residuos son no negativos y menores que el divisor. Además, los enteros positivos se pueden representar en cualquier **base** entera $b > 1$ usando 0, 1,. . . , $b - 1$ como **dígitos**. El sistema decimal (base 10), el binario (base 2) −creado por Leibniz− y el triádico (base 3) son los más conocidos y utilizados. La representación es

$$n = (a_k a_{k-1} \ldots a_0)_b,$$

donde los a_i son los residuos de las divisiones sucesivas. Así, es posible escribir

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

y la parte decimal se toma con los exponentes negativos de b. Por otro lado, en caso de que las bases sean mayores que 10, se utilizan las letras A para el dígito 10, B para el 11, y así sucesivamente.

Ejemplo 11. *La expresión* $(A5B)_{12}$ *corresponde a:*

$$10 \cdot 12^2 + 5 \cdot 12^1 + 11 \cdot 12^0$$

Es decir, $(A5B)_{12} = 1511$. ■

Algoritmo de la división.
Dados n y b enteros positivos, existen q y r, únicos, con $0 \leq r < b$ tal que $n = qb + r$. El valor de $\boldsymbol{r}$ se conoce como **residuo**, $\boldsymbol{q}$ se conoce como **cociente**, $\boldsymbol{n}$ el **dividendo** y $\boldsymbol{b}$ el **divisor**.

Ejemplo 12. *Al efectuar la división de* 65 *por* 6*, se obtiene a* 5 *como residuo y* 10 *como cociente, y de esta manera se puede escribir la igualdad* $65 = 10 \cdot 6 + 5$. ■

Ejemplo 13. *Represente a* 26 *en base* 2 *usando, claro está, a* 0 *y* 1 *como dígitos. Recuerde que el algoritmo de la división euclideana restringe los posibles valores del residuo a enteros positivos o cero y menores que el divisor.*

$$
\begin{array}{cccccc}
26 & \multicolumn{1}{|c}{2} & & & & \\ \cline{2-2}
\mathbf{0} & 13 & \multicolumn{1}{|c}{2} & & & \\ \cline{3-3}
 & \mathbf{1} & 6 & \multicolumn{1}{|c}{2} & & \\ \cline{4-4}
 & & \mathbf{0} & 3 & \multicolumn{1}{|c}{2} & \\ \cline{5-5}
 & & & \mathbf{1} & 1 & \multicolumn{1}{|c}{2} \\ \cline{6-6}
 & & & & \mathbf{1} & 0
\end{array}
$$

Con lo que $26 = (11010)_2$. ■

Ejemplo 14. *Exprese el número* 2013 *en base* 5.

Solución. Luego de hacer las divisiones consecutivas, se obtiene:

$$
\begin{aligned}
2013 &= 402 \cdot 5 + 3 \\
&= (80 \cdot 5 + 2) \cdot 5 + 3 \\
&= 80 \cdot 5^2 + 2 \cdot 5 + 3 \\
&= (16 \cdot 5 + 0) \cdot 5^2 + 2 \cdot 5 + 3 \\
&= 16 \cdot 5^3 + 0 \cdot 5^2 + 2 \cdot 5 + 3 \\
&= (3 \cdot 5 + 1) \cdot 5^3 + 0 \cdot 5^2 + 2 \cdot 5 + 3 \\
&= 3 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 2 \cdot 5 + 3
\end{aligned}
$$

De donde $2013 = (31023)_5$. ■

El algoritmo de la división se puede utilizar para representar, de la misma forma que en los ejemplos anteriores, los enteros positivos y negativos en cualquier base entera b, con $b < -1$, utilizando los dígitos 0, 1, 2, ..., $|b| - 1$.

Ejemplo 15. *Represente ahora a* 19 *en base* -2.

Solución. Debe utilizar ahora a 0 y 1 como dígitos, observe:

$$\begin{array}{rrrrrr}
19 & \multicolumn{1}{|r}{-2} & & & & \\ \cline{2-2}
\mathbf{1} & -9 & \multicolumn{1}{|r}{-2} & & & \\ \cline{3-3}
 & \mathbf{1} & 5 & \multicolumn{1}{|r}{-2} & & \\ \cline{4-4}
 & & \mathbf{1} & -2 & \multicolumn{1}{|r}{-2} & \\ \cline{5-5}
 & & & \mathbf{0} & 1 & \multicolumn{1}{|r}{-2} \\ \cline{6-6}
 & & & & \mathbf{1} & 0
\end{array}$$

Con lo que $19 = (10111)_{-2}$. ■

Ejemplo 16. *Exprese el número* 16 *en base* -3.

Solución. Luego de hacer las divisiones consecutivas, se obtiene:

$$\begin{aligned}
16 &= (-5) \cdot (-3) + 1 = (2 \cdot (-3) + 1) \cdot (-3) + 1 \\
&= 2 \cdot (-3)^2 + 1 \cdot (-3) + 1
\end{aligned}$$

de donde $16 = (211)_{-3}$. ■

Ejemplo 17. *Represente* -51*, un número entero negativo, en la base negativa* -3.

Solución. Debe utilizar como dígitos a 0, 1 y 2.

$$\begin{array}{rrrrr}
-51 & \multicolumn{1}{|r}{-3} & & & \\ \cline{2-2}
\mathbf{0} & 17 & \multicolumn{1}{|r}{-3} & & \\ \cline{3-3}
 & \mathbf{2} & -5 & \multicolumn{1}{|r}{-3} & \\ \cline{4-4}
 & & \mathbf{1} & 2 & \multicolumn{1}{|r}{-3} \\ \cline{5-5}
 & & & \mathbf{2} & 0
\end{array}$$

Con lo que $-51 = (2120)_{-3}$. ■

Ejemplo 18. *Por último, exprese el número* -55 *en base* -3.

Solución. Luego de hacer las divisiones consecutivas, se obtiene:

$$\begin{aligned}
-55 &= 19 \cdot (-3) + 2 \\
&= ((-6) \cdot (-3) + 1) \cdot (-3) + 2 \\
&= (-6) \cdot (-3)^2 + 1 \cdot (-3) + 2 \\
&= (2 \cdot (-3) + 0) \cdot (-3)^2 + 1 \cdot (-3) + 2 \\
&= 2 \cdot (-3)^3 + 0 \cdot (-3)^2 + 1 \cdot (-3)^1 + 2
\end{aligned}$$

de donde $-55 = (2012)_{-3}$. ■

Ejemplo 19. *En el año* 2030, *una expedición llegó a un planeta en donde se sabía que los habitantes, extintos por una catástrofe, eran seres que tenían* 4 *piernas y un tentáculo con varios dedos prensibles. En una roca encontraron unas escrituras que identificaron como la ecuación*

$$5x^2 - 50x + 125 = 0$$

y más abajo, las posibles soluciones $x_1 = 5$ *y* $x_2 = 8$. *La primera solución parece lógica, no así la segunda. Considerando que el sistema numérico de la Tierra está relacionado con el número de dedos del ser humano, ¿cuántos dedos tenían estos seres?*

Solución. Como $x_2 = 8$ es solución de la ecuación $5x^2 - 50x + 125 = 0$, se tiene que el reemplazo de x por 8 en ella provoca la igualdad:

$$5 \cdot 8^2 - 50 \cdot 8 + 125 = 0$$

Suponga que la base es b (número de dedos), la igualdad anterior se plantea como:

$$\begin{aligned}
& 5 \cdot 8^2 - (5 \cdot b^1 + 0 \cdot b^0) \cdot 8 + (1 \cdot b^2 + 2 \cdot b^1 + 5 \cdot b^0) = 0 \\
\Leftrightarrow\ & b^2 - 38b + 325 = 0 \\
\Leftrightarrow\ & b_1 = 13 \text{ ó } b_2 = 25
\end{aligned}$$

Recuerde que también $x_1 = 5$ era solución, y

$$5 \cdot 5^2 - (5 \cdot 13^1 + 0 \cdot 13^0) \cdot 5 + (1 \cdot 13^2 + 2 \cdot 13^1 + 5 \cdot 13^0) = 0$$
$$5 \cdot 5^2 - (5 \cdot 25^1 + 0 \cdot 25^0) \cdot 5 + (1 \cdot 25^2 + 2 \cdot 25^1 + 5 \cdot 25^0) = 180 \neq 0,$$

de donde la solución $b_1 = 13$ es correcta y corresponde al número de dedos de estos seres. ■

Ejercicios (sección 7.2)

1. Escriba los números dados en forma decimal en la base indicada.

   (a) 405 en base 2

   (b) 1 444 en base -3 y en base 3

   (c) 356 281 en base 5 y en base -5

   (d) 1 500 en base -6

   (e) -286 en base -6

   (f) 328 204 en base 7

2. El número 177 se representa en base b como $(2301)_b$, halle b.

3. Un monarca oriental obsequió a sus vecinos, el rey de Aulnia, el rey de Bizania y el rey de Ciria, exactamente el mismo número de caballos (inferior a doscientos). Sin embargo, el primer rey le agradeció los 222 caballos que le había obsequiado, el segundo rey hizo lo mismo por los 66 caballos y el tercero le agradeció los 22 caballos que le obsequió. Los tres reyes sabían contar bien, y ningún caballo había sido robado. ¿Puede usted dar una explicación a estos números tan diferentes? Además, ¿cuántos caballos regaló a cada uno?

7.3 Aritmética en distintas bases

Se inicia con la adición y multiplicación en el sistema binario. En la tabla 7.2 se muestran las reglas para ambas operaciones.

$+$	0	1
0	0	1
1	1	10

$\times$	0	1
0	0	0
1	0	1

Tabla 7.2: Reglas de suma y producto binario.

A partir de estas reglas, el procedimiento es análogo al que se ha aprendido para el sistema decimal; por ejemplo, $1+1=2$ en el decimal; en el binario, para $1+1$ se pone 0 y *lleva* 1. Para comprender esto, vea los siguientes ejemplos.

Ejemplo 20. *Para realizar la suma de* $(110110)_2$ *y* $(10011)_2$ *se hace:*

$$\begin{array}{r} {}^{1\ \ 11} \\ 110110 \\ +\quad 10011 \\ \hline 1001001 \end{array}$$

Por lo que $(110110)_2 + (10011)_2 = (1001001)_2$. ∎

Ejemplo 21. *Para realizar el producto* $(101101)_2 \times (101)_2$ *se hace:*

$$\begin{array}{r} 101101 \\ \times \quad 101 \\ \hline 101101 \\ 000000 \\ +\quad 101101 \\ \hline 11100001 \end{array}$$

Por lo que $(101101)_2 \times (101)_2 = (11100001)_2$. ∎

Para otras bases se procede de manera análoga; como ejemplo, en la tabla 7.3 se muestran las reglas para ambas operaciones en base 4.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Tabla 7.3: Reglas de suma y producto en base 4.

Es así como $2+3=5$ en el decimal, pero en base 4, para $2+3$ se pone 1 y *lleva* 1. Para comprender este procedimiento, vea los siguientes ejemplos.

Ejemplo 22. *Para realizar la suma de* $(223231)_4$ *y* $(10321)_4$ *se hace:*

$$\begin{array}{rr} & {\scriptstyle 1111} \\ & 223231 \\ + & 10321 \\ \hline & 300212 \end{array}$$

Por lo que $(223231)_4 + (10321)_4 = (300212)_4$. ■

Ejemplo 23. *Para realizar el producto* $(10232)_4 \times (213)_4$ *hace:*

$$\begin{array}{rr} & 10232 \\ \times & 213 \\ \hline & 32022 \\ & 10232 \\ + & 21130 \\ \hline & 2320002 \end{array}$$

Por lo que $(10232)_4 \times (213)_4 = (2320002)_4$. ■

Es interesante notar que al multiplicar por b un número dado en base b, a la representación se le debe agregar un cero a la derecha; así, $10 \cdot 243 = 2430$ en el sistema decimal; por otro lado, se cumple que $6 \cdot (31)_6 = (310)_6$ o equivalentemente, $(10)_6 \cdot (31)_6 = (310)_6$.

Ejemplo 24. *Exprese* $(0,3\overline{5})_6$ *en su forma racional canónica; además, encuentre su valor racional decimal. (Compare con el ejemplo* 28*).*

Solución. Sea $x = (0,3\overline{5})_6$, al multiplicar por 6 se obtiene la igualdad $6x = (3,5\overline{5})_6$, es decir, $(10)_6 x = (3,5\overline{5})_6$; al restar las últimas dos igualdades se tiene $5x = (3,2)_6$ o equivalentemente $(5)_6 x = (3,2)_6$; al multiplicar por 6 se obtiene la igualdad $(50)_6 x = (32)_6$, por lo que $x = \frac{(32)_6}{(50)_6}$. Finalmente, para calcular su valor racional decimal, basta ver que:

$$\begin{aligned}
(0,3\overline{5})_6 &= \frac{3}{6} + \frac{5}{6^2} + \frac{5}{6^3} + \cdots \\
&= \frac{3}{6} + \frac{5}{6^2}\left(1 + \frac{1}{6} + \frac{1}{6^2} + \cdots\right) \\
&= \frac{1}{2} + \frac{5}{6^2} \cdot \frac{1}{1 - \frac{1}{6}} \\
&= \frac{2}{3}
\end{aligned}$$

Es decir, $(0,3\overline{5})_6 = \frac{2}{3}$. Otra forma de calcular el valor es hacerlo directamente por medio de:

$$(0,3\overline{5})_6 = \frac{(32)_6}{(50)_6} = \frac{3 \cdot 6 + 2}{5 \cdot 6} = \frac{20}{30} = \frac{2}{3}$$

Y de nuevo, $(0,3\overline{5})_6 = \frac{2}{3}$. ■

Ejercicios (sección 7.3)

1. Realice las operaciones:
   (a) $(101010)_2 + (111000101)_2$
   (b) $(11101)_2 \times (110)_2$
   (c) $(321312)_4 + (123021121)_4$
   (d) $(20131)_4 \times (321)_4$
   (e) $(1123)_4 \times (302)_4 + (231)_4$
2. Construya la tabla para la suma y el producto en base 5.
3. Realice las operaciones:
   (a) $(20134)_5 + (1344210)_5$
   (b) $(12304)_5 \times (3002)_5$
   (c) $(143,01)_5 + (23,321)_5$
   (d) $(1203,4)_5 \times (3,04)_5$
   (e) $(2302)_5 - (1430)_5$
4. Construya la tabla para la suma y el producto en base 7.
5. Realice las operaciones:
   (a) $(121064)_7 + (620510)_7$
   (b) $(3025)_7 \times (612)_7$
   (c) $(3126)_7 \times (154)_7 + (2601)_7$
6. Considere el número con k unos $(11\ldots11)_2$, encuentre su cuadrado, también expresado en base 2.
7. Exprese $(2,4\overline{32})_5$ en su forma racional canónica; además, encuentre su valor racional decimal.
8. Exprese $(3,25\overline{123})_7$ en su forma racional canónica; además, encuentre su valor racional decimal.

7.4 Representación en bases fraccionarias

Algunos números tienen representación en bases fraccionarias. En el siguiente ejemplo se plantea el conocido "problema de los cocos", (véase [4]). Su solución se desarrolla de una manera general para así, de esta forma, esbozar el algoritmo para la representación en este tipo de bases.

Ejemplo 25. *Cinco náufragos, en una isla desierta, han recogido un montón de cocos. Pero antes de poder repartírselos sobreviene la noche y optan por acostarse a descansar. La luz de la luna, de madrugada, despierta a uno de ellos. Desconfiado de sus compañeros, decide, por si acaso, hacerse con su parte. Reparte equitativamente los cocos en cinco montones. Al hacerlo, sobra un coco, que arroja lejos. Vuelve a agrupar cuatro de los montones en uno solo, se lleva el quinto montón junto a su lecho y, ya tranquilo, vuelve a dormirse. Un segundo náufrago se despierta un poco más tarde. Se dirige hasta el montón colectivo y se sirve, procediendo como el primero. También ahora sobra un coco, que tira lejos. Los otros tres compañeros actúan de igual manera: cada uno se apodera de una quinta parte del montón, que disminuye en cada operación, sobrando siempre, tras cada reparto, un coco. ¿Cuántos cocos habían recogido inicialmente los náufragos?*

Solución. Suponga que n_0 es la cantidad inicial de cocos, n_1 la cantidad después del segundo reparto, n_2 la cantidad después del tercer reparto, etc. Antes de la j-ésima división, el náufrago de turno dispone de n_{j-1} cocos. Procede a distribuirlos en $r = 5$ montones iguales y arroja lejos los a_{j-1} cocos restantes. Se apropia de $h = 1$ montón de entre los 5. Reagrupa lo que queda de sus $s = 4$ montones, formando un nuevo montón de n_j cocos, es decir:

$$n_j = s \cdot \left(\frac{n_{j-1} - a_{j-1}}{r} \right) \tag{7.1}$$

Al despejar:

$$n_{j-1} = a_{j-1} + n_j \cdot \frac{r}{s}$$

Suponiendo que el proceso sigue mientras hayan cocos disponibles, en un momento dado el número de cocos n_k será inferior a r, con lo que $a_k = n_k$ y $n_{k+1} = 0$, y a partir de ahí ya no es posible el reparto. Las fórmulas son:

$$\begin{aligned} n_0 &= a_0 + n_1 \cdot \frac{r}{s} \\ n_1 &= a_1 + n_2 \cdot \frac{r}{s} \\ n_2 &= a_2 + n_3 \cdot \frac{r}{s} \\ \vdots & \quad \vdots \end{aligned}$$

Al hacer la sustitución hacia atrás:

$$\begin{aligned} n_0 &= a_0 + n_1 \cdot \frac{r}{s} \\ &= a_0 + \left(a_1 + n_2 \cdot \frac{r}{s}\right) \cdot \frac{r}{s} \\ &= a_0 + a_1 \cdot \frac{r}{s} + \left(a_2 + n_3 \cdot \frac{r}{s}\right) \cdot \left(\frac{r}{s}\right)^2 \\ \vdots & \quad \vdots \\ &= a_0 + a_1 \cdot \frac{r}{s} + a_2 \cdot \left(\frac{r}{s}\right)^2 + \cdots + a_k \cdot \left(\frac{r}{s}\right)^k \end{aligned}$$

Con lo cual se ha encontrado que la cantidad inicial de cocos n_0 es una representación en la base 5/4, es decir:

$$n_0 = (a_k a_{k-1} \dots a_0)_{5/4}$$

Recuerde que en este ejemplo $a_1 = a_2 = a_3 = a_4 = a_5 = 1$, así:

$$n_0 = (* * \cdots * * 11111)_{5/4}$$

Como además se sabe que los náufragos hacen solo un reparto, la escogencia de los a_i con $i \geq 5$ puede ser cualquiera, que se indica con el símbolo $*$. Claro que se debe tener en cuenta que $n_0 + 4$ es un número con residuo cero en las cinco primeras divisiones, con lo que $n_0 + 4$ es divisible por $5^5 = 3125$. El menor n_0 posible es entonces 3121 (otras posibles soluciones son 6246, 9371, etc.). Como un ejercicio, se puede ver que:

$$3121 = (432\,103\,134\,003\,434\,321\,021\,011\,111)_{5/4}$$

■

Ejemplo 26. *Utilice la fórmula recursiva dada por la ecuación* (7.1) *para representar a* $n_0 = 17$ *en la base* $\frac{3}{2}$*, donde los posibles residuos son* 0, 1 *y* 2*; además,* $s = 2$ *y* $r = 3$*. Primero se plantea:*

$$n_1 = 2 \cdot \left(\frac{17 - a_0}{3}\right),$$

de donde se concluye que $a_0 = 2$*, pues con* 0 *o con* 1 *no se obtiene un número entero. Así,* $n_1 = 2 \cdot \left(\frac{17-2}{3}\right) = 10$*. Con este resultado se plantea:*

$$n_2 = 2 \cdot \left(\frac{10 - a_1}{3}\right),$$

de donde se concluye que $a_1 = 1$*, pues con* 0 *o con* 2 *no es posible obtener un número entero. Así,* $n_2 = 2 \cdot \left(\frac{10-1}{3}\right) = 6$*. Con este resultado se plantea:*

$$n_3 = 2 \cdot \left(\frac{6 - a_2}{3}\right),$$

de donde se concluye que $a_2 = 0$*, y se obtiene que* $n_3 = 2 \cdot \left(\frac{6-0}{3}\right) = 4$*. Análogamente se plantea,* $n_4 = 2 \cdot \left(\frac{4-a_3}{3}\right)$*, y se obtiene* $a_3 = 1$ *y* $n_4 = 2$*. Luego* $n_5 = 2 \cdot \left(\frac{2-a_4}{3}\right)$*, y se obtiene* $a_4 = 2$ *y* $n_5 = 0$*, con lo cual se termina el proceso y es posible escribir:*

$$17 = (21012)_{3/2}$$

■

Ejercicios (sección 7.4)

1. Escriba los siguientes números en la base indicada.

   (a) 31 en base 3/2
   (b) 23 en base 5/4
   (c) 27 en base 5/3

2. En el libro *El Hombre que Calculaba*, de Malba Tahan [34], se plantea el problema de los tres marineros, cuyo enunciado es: *Un navío que volvía de Ceilán, trayendo gran cantidad de especias, fue alcanzado por un violento temporal. La embarcación habría sido destruida por las olas si no hubiera sido por el esfuerzo de tres marineros. El capitán, queriendo recompensarlos, les dio cierto número de monedas, más de doscientos y menos de trescientos. Las monedas fueron colocadas en una caja para que al día siguiente, al desembarcar, se repartieran entre los tres valientes. Sucedió que, durante la noche, uno de los tres marineros se despertó y pensó: "sería mejor que retirase mi parte. Así no tendré oportunidad de discutir con mis amigos". Y sin decir nada repartió las monedas en tres partes iguales y notó que la división no era exacta, ya que sobraba una moneda, la cual arrojó al mar. Retiró su parte y dejó el resto en el mismo lugar. Horas después, un segundo marinero tuvo la misma idea: repartió en tres partes, sobró una que tiró, tomó su parte y dejó el resto en el mismo lugar. El tercero, sin saber lo sucedido, tuvo la misma idea, y sucedió lo mismo que con los otros dos. Al día siguiente, el capitán tomó las monedas, las dividió en tres partes y, al darse cuenta de que sobraba una moneda, la guardó como retribución de su trabajo. ¿Cuántas eran las monedas?, ¿cuánto recibió cada uno?*
   La respuesta, sin justificación alguna, que se da en el libro, es que se tenían inicialmente 241 monedas. Plantee el problema y concluya esta solución.

7.5 Congruencias numéricas

Un concepto muy importante en la teoría de números es el de las congruencias numéricas. Fue el gran matemático alemán Carl Friedrich Gauss quien, en su monumental obra *Disquisitiones arithmeticae*, publicada en 1801, en analogía con el "=" para la igualdad, introdujo el símbolo "≡" para denotar que dos números son "congruentes". En aquella época (inicios del siglo XIX), no existían las computadoras ni calculadoras electrónicas, y los cálculos eran totalmente manuales, o bien, con el uso del ábaco.

Leonard Euler demostró que la conjetura de Fermat, según la cual los números de la forma $2^{2^n}+1$ eran primos para todo $n \in \mathbb{N}$, era falsa. Esto se cumple para $n = 1, 2, 3, 4$, pero no para todo natural. Euler demostró que $2^{2^5}+1 = 2^{32}+1 = 641 \times 6\,700\,417$. Dicho resultado se puede verificar actualmente con base en las congruencias, o rápidamente con ayuda de una calculadora sencilla. Euler lo hizo manualmente. Aún así, hay números que son tan grandes, como $2^{1000000}$, que se necesitaría algo más que una calculadora para obtener, por ejemplo, el residuo de la división de este número por otro.

> Sean a, b, $m \in \mathbb{Z}$, con $m > 0$. Se dice que a es **congruente** a b módulo m y se escribe $a \equiv b \bmod m$ si y solo si m divide a $a - b$.

Ejemplo 27. *Se tiene que* $91 \equiv 1 \bmod 5$, *pues* 5 *divide a* 90. ■

Ejemplo 28. *Dado que* 7 *divide a* 35, *se tiene que* $43 \equiv 8 \bmod 7$, *y además* $31 \equiv -4 \bmod 7$. ■

Ejemplo 29. *Si* x *es cualquier número impar, entonces* $x^2 \equiv 1 \bmod 4$.

Solución. Como x es impar, entonces $\exists n \in \mathbb{Z}$ tal que $x = 2n+1$; así, $x^2 = (2n+1)^2 = 4n^2+4n+1 = 4(n^2+n)+1$. Por lo tanto, $x^2 - 1 = 4k$

con $k \in \mathbb{Z}$, esto dice que 4 divide a $x^2 - 1$, con lo cual se concluye que $x^2 \equiv 1 \bmod 4$. ■

Teorema 1. *Si $a \equiv b \bmod m$, entonces $a^n \equiv b^n \bmod m$, $\forall n \in \mathbb{N}$.*

Demostración. Se sabe que $a - b$ divide a $a^n - b^n$ (véase ejercicio 14, en la página 292), por lo que $a^n - b^n = (a - b) \cdot M$, para algún M en $\mathbb{Z}$. Como $a \equiv b \bmod m$, se tiene que $a - b = km$, de donde $a^n - b^n = k \cdot m \cdot M = (kM) \cdot m$, con lo cual m divide a $a^n - b^n$; así, se concluye que $a^n \equiv b^n \bmod m$. □

Teorema 2. *Si $a \equiv b \bmod m$ y $p(x)$ es un polinomio con coeficientes enteros, entonces $p(a) \equiv p(b) \bmod m$.*

Demostración. Sea $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, de donde

$$p(b) - p(a) = a_n(b^n - a^n) + \cdots + a_1(b - a)$$

Como $a \equiv b \bmod m$, por teorema 1 se tiene que $m|(b^i - a^i)$ para todo $i = 1, \ldots, n$, de donde $m|(p(b) - p(a))$; así, $p(a) \equiv p(b) \bmod m$. □

Teorema 3. *Si $a \equiv b \bmod m$ y además $\alpha \equiv \beta \bmod m$, entonces $a\alpha \equiv b\beta \bmod m$.*

Demostración. Ejercicio para el lector. □

Teorema 4. *Si $a \equiv b \bmod m$ y $a \equiv b \bmod n$ con* m.c.d.$(m, n) = 1$*, se cumple $a \equiv b \bmod m \cdot n$.*

Demostración. Ejercicio para el lector. □

Los siguientes ejemplos, de los cuales se podrían resolver algunos utilizando solamente los conceptos de divisibilidad, son muy ilustrativos con respecto a cómo ayudan las congruencias para simplificar la solución de problemas que involucran números grandes.

Ejemplo 30. *Calcule el residuo de dividir* $(17^{70}+37^{28})^{54}$ *por* 7.

Solución. Primero note que $17 \equiv 3 \bmod 7$, así, al elevar a la dos y luego a la cinco, se obtiene $17^2 \equiv 3^2 \bmod 7 \equiv 2 \bmod 7$ y $17^{10} \equiv 2^5 \bmod 7 \equiv 4 \bmod 7$; por último, al elevar a la siete:

$$17^{70} \equiv 4^7 \bmod 7 \equiv 4 \bmod 7$$

De forma análoga se obtiene que $37^{28} \equiv 2 \bmod 7$. Así, al sumar ambas congruencias, se obtiene que:

$$17^{70}+37^{28} \equiv 4+2 \bmod 7 \equiv -1 \bmod 7$$

Luego de elevar a la 54, se obtiene que $(17^{70}+37^{28})^{54} \equiv (-1)^{54} \bmod 7 \equiv 1 \bmod 7$. De esta manera, el residuo es 1. ■

Ejemplo 31. *¿Para cuáles valores enteros de* n *el número* $1996^{1997n}+1$ *es divisible por* 1997*?*

Solución. Como $1996 \equiv -1$ mod 1997, se tiene que:

$$\begin{aligned} 1996^{1997n} &\equiv (-1)^{1997n} \text{ mod } 1997 \\ &\equiv (-1)^{n} \text{ mod } 1997 \end{aligned}$$

de donde $1996^{1997n}+1 \equiv (-1)^n + 1$ mod 1997, que sería divisible por 1997 si el residuo $(-1)^n+1$ diera cero, y esto ocurre solamente si n es un número impar. ■

Ejemplo 32. *Calcule el residuo de dividir* $(33^{45}+45^{33})^{27}+1$ *por* 10. *Concluya que este número no puede ser un cuadrado perfecto.*

Solución. Primero note que $33 \equiv 3 \bmod 10$, así, al elevar a la cinco se obtiene $33^5 \equiv 3^5 \bmod 10 \equiv 1 \bmod 10$ y $33^{45} \equiv 1^{15} \bmod 10 \equiv 1 \bmod 10$; análogamente se tiene que $45^{33} \equiv 5 \bmod 10$. De esto, al sumar, se obtiene que $33^{45}+45^{33} \equiv 1+5 \bmod 10 \equiv 6 \bmod 10$, y luego de elevar a la tres y luego a la nueve, se obtiene que $(33^{45}+45^{33})^{27} \equiv 6 \bmod 10$. De esta manera se tiene que:

$$(33^{45}+45^{33})^{27}+1 \equiv 6+1 \bmod 10 \equiv 7 \bmod 10$$

Con lo cual el número de unidades es 7, y como ningún cuadrado perfecto termina en 7, se concluye que no es un cuadrado perfecto. ■

Ejemplo 33. *Calcule el residuo de dividir* $(51+22^{24})^{25}$ *por* 5.

Solución. Note que $51 \equiv 1 \bmod 5$; además, $22 \equiv 2 \bmod 5$. Así, $22^6 \equiv 2^6 \bmod 5 \equiv 4 \bmod 5$ y $22^{24} \equiv 4^4 \bmod 5 \equiv 1 \bmod 5$, de donde:

$$\begin{aligned} 51+22^{24} &\equiv 2 \bmod 5 \\ \left(51+22^{24}\right)^5 &\equiv 2^5 \bmod 5 \equiv 32 \bmod 5 \equiv 2 \bmod 5 \\ \left(51+22^{24}\right)^{25} &\equiv 2^5 \bmod 5 \equiv 32 \bmod 5 \equiv 2 \bmod 5 \end{aligned}$$

Con lo que el residuo es 2. ■

Teorema 5. *Si* $ax \equiv ay \bmod m$ *y además* $\text{m.c.d.}(a,m)=g$, *entonces* $x \equiv y \bmod m/g$.

Demostración. Dado que $ax \equiv ay \bmod m$, se tiene que $m|a(x-y)$. Como $\text{m.c.d.}(a,m)=g$, se tiene que $a=ga'$ y $m=gm'$; al sustituir estos valores, se obtiene que $gm'|ga'(x-y)$; por lo tanto, $m'|a'(x-y)$ con $\text{m.c.d.}(a',m')=1$. Se concluye, por el lema de Euclides, que $m'|(x-y)$, es decir, $x \equiv y \bmod m' \equiv y \bmod m/g$. □

El siguiente resultado, que se obtiene inmediatamente del anterior cuando $g=1$, se conoce como **ley de cancelación** para congruencias.

Corolario 2. *Si* $ax \equiv ay \bmod m$ *y además* $\text{m.c.d.}(a,m)=1$, *entonces* $x \equiv y \bmod m$.

Teorema 6. *Para $a \in \mathbb{Z}$, si $x \equiv y \bmod m$, entonces $ax \equiv ay \bmod m$.*

Demostración. Como $x \equiv y \bmod m$, se tiene que m divide a $x - y$; además, divide a cualquier múltiplo entero de él. Por lo tanto, $m|a(x-y)$ y se concluye que $ax \equiv ay \bmod m$. □

Teorema 7. *Si $a \equiv b \bmod m$ y $\alpha \equiv \beta \bmod m$, entonces para todos x, y enteros se cumple que $(ax + \alpha y) \equiv (bx + \beta y) \bmod m$.*

Demostración. Dado que $a \equiv b \bmod m$ y $x \equiv x \bmod m$, al aplicar el teorema 3 se obtiene que $ax \equiv bx \bmod m$, análogamente $\alpha y \equiv \beta y \bmod m$. Así, m divide a $ax - bx$ y m divide a $\alpha y - \beta y$; por lo tanto, m divide a $ax + \alpha y - bx - \beta y$, y de allí se concluye la demostración. □

Ejemplo 34. *Pruebe que todo número de Fermat termina con dígito 7.*

Solución. Es claro que, en el sistema decimal, un número entero m termina en 7 si $m \equiv 7$ mod 10; por lo tanto, se probará que todo número de Fermat satisface esta condición. En el caso $n = 2$, se tiene que $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$, y claramente, $F_2 \equiv 7$ mod 10; con lo que la proposición se cumple para $n = 2$. Analice el caso $n > 2$, se sabe que $2^{2^2} = 16$, con lo cual $2^{2^2} \equiv 6$ mod 10, se elevan ambos lados de esta congruencia al exponente 2^{n-2},

$$\left(2^{2^2}\right)^{2^{n-2}} \equiv 6^{2^{n-2}} \text{ mod } 10 \tag{7.2}$$

Se utiliza primero la propiedad de las potencias $\left(a^n\right)^m = a^{nm}$, y se efectúa $\left(2^{2^2}\right)^{2^{n-2}} = 2^{2^2 \cdot 2^{n-2}}$; luego se hace uso de la propiedad $a^n a^m = a^{n+m}$ y se obtiene $2^{2^{2+n-2}} = 2^{2^n}$; por último, el hecho de que cualquier potencia entera y positiva de 6 termina en 6, es decir, $6^k \equiv 6$ mod 10. Con lo cual, se obtiene a partir de (7.2) la congruencia $2^{2^n} \equiv 6$ mod 10; sumando 1 a ambos lados, se concluye que $2^{2^n} + 1 \equiv 7$ mod 10. ■

Ejemplo 35. *Probar que un entero positivo n es divisible por 3 si y solo si la suma de los dígitos de su expresión decimal es divisible por 3.*

Solución. Sea $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$, donde $a_0, \ldots, a_k$ pertenecen a $\{0, 1, \ldots, 9\}$ con $a_k \neq 0$. Es claro que $n = p(10)$ para $p(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$. Como $10 \equiv 1 \bmod 3$, por el teorema 2, se tiene que:

$$\begin{aligned} n = p(10) &\equiv p(1) \bmod 3 \\ &\equiv (a_k + a_{k-1} + \cdots + a_1 + a_0) \bmod 3 \end{aligned}$$

Por lo que $3|n$ si y solo si $3|(a_k + a_{k-1} + \cdots + a_1 + a_0)$. ■

Ejemplo 36. *Demuestre que $\forall n \in \mathbb{N}$ se cumple que $10^n + 3 \cdot 4^{n+2} + 5$ es divisible por 9.*

Solución. Se probará que $10^n + 3 \cdot 4^{n+2} + 5 \equiv 0 \bmod 9$. En primer término, como $10 \equiv 1 \bmod 9$, se tiene que $10^n \equiv 1 \bmod 9$. Además, como $4 \equiv 1 \bmod 3$, se tiene que $4^{n+2} \equiv 1 \bmod 3$, y al multiplicar por 3 toda la congruencia, se obtiene que $3 \cdot 4^{n+2} \equiv 3 \bmod 9$. Finalmente, como $5 \equiv 5 \bmod 9$, al sumar las tres congruencias se tiene que:

$$10^n + 3 \cdot 4^{n+2} + 5 \equiv (1 + 3 + 5) \bmod 9 \equiv 0 \bmod 9$$

Por lo tanto, $10^n + 3 \cdot 4^{n+2} + 5$ es divisible por 9. ■

Ejemplo 37. *Calcule el menor valor positivo de k para que 5 sea divisor de $(37 - 48^{30})^{16} + k^2$.*

Solución. Primero, averigüe cuál es el residuo de dividir $(37 - 48^{30})^{16}$ por 5. Para ello observe que $37 \equiv 2 \bmod 5$, además, $48 \equiv 3 \bmod 5$; así, $48^3 \equiv 3^3 \bmod 5 \equiv 2 \bmod 5$ y $48^{15} \equiv 2^5 \bmod 5 \equiv 2 \bmod 5$, de donde:

$$\begin{aligned} 37 - 48^{30} &\equiv 2 - 4 \bmod 5 \equiv 3 \bmod 5 \\ \left(37 - 48^{30}\right)^4 &\equiv 3^4 \bmod 5 \equiv 81 \bmod 5 \equiv 1 \bmod 5 \\ \left(37 - 48^{30}\right)^{16} &\equiv 1^4 \bmod 5 \equiv 1 \bmod 5 \end{aligned}$$

Con lo que el residuo es 1 y así k debe ser 2. ■

Ejemplo 38. *Pruebe que* $9589^{2222} + 6051^{1111}$ *es divisible por* 17.

Solución. Primero note que $9589 \equiv 1 \bmod 17$, así se obtiene:

$$9589^{2222} \equiv 1^{2222} \bmod 17 \equiv 1 \bmod 17$$

Análogamente, como $6051 \equiv 16 \bmod 17 \equiv -1 \bmod 17$, se tiene que:

$$6051^{1111} \equiv (-1)^{1111} \bmod 17 \equiv -1 \bmod 17$$

De esto, al sumar, se obtiene que $9589^{2222} + 6051^{1111} \equiv 0 \bmod 17$; de esta manera se tiene que el residuo es cero, y con ello el número dado es divisible por 17. ■

Ejercicios (sección 7.5)

1. Pruebe que cualquier cuarta potencia de un número debe tener como dígito de las unidades a 0, 1, 5 o 6.

2. ¿Cuáles son los dos últimos dígitos en la expansión de 3^{400}?

3. Halle el mínimo valor positivo de k, para el cual $7077^{377} - k$ es divisible por 11.

4. Calcule el residuo que se obtiene al dividir $2^{1000000} + 1\,000\,000!$ por 77.

5. Calcule el residuo que se obtiene al dividir $(23^{24} + 2\,000)^{40}$ por 7.

6. Calcule el residuo de dividir $(2346 + 4321^{300})^3$ por 7.

7. Pruebe que cualquier número que sea un cuadrado perfecto debe tener como dígito de las unidades a 0, 1, 4, 5, 6 o 9.

8. Pruebe que $2001^{1999} + 27! + 123456$ no es un cuadrado perfecto.

9. Halle el residuo de dividir el número $\left(116 + 17^{17}\right)^{21}$ por 8.

10. Pruebe que $9589^{2222} + 6051^{1111}$ es divisible por 17.

11. Halle el residuo de dividir el número $\left(1234^{77} - 37^{99}\right)^{44}$ por 7.

12. Analice si existe k tal que $k^2 = 1989^{1988} + 6$.

13. Pruebe, sin utilizar inducción, que para todo natural n:

    (a) $3^{2n+1} + 4 \cdot 23^n$ es divisible por 7.
    (b) $4^{2n+1} + 3^{n+2}$ es divisible por 13.
    (c) $2^{4n+1} - 2^{2n} - 1$ es divisible por 9.
    (d) $a^{2n+1} + (a-1)^{n+2}$ es divisible por $a^2 - a + 1$, para $a \in \mathbb{N}$.

14. Verifique, utilizando congruencias, que la conjetura propuesta por Fermat de que los números de la forma $2^{2^n} + 1$ son primos, es falsa para $n = 5$.

15. Sea $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_0$. Pruebe que $11|n$ si y solo si $11|(a_0 - a_1 + a_2 + \cdots + (-1)^k a_k)$.

16. Sea n un número de cuatro cifras, es decir, $n = 1000a_3 + 100a_2 + 10a_1 + a_0$. Pruebe que $7|n$ si y solo si $7|(a_0 + 3a_1 + 2a_2 + 6a_3)$.

7.6 Resultados importantes

Dentro de los resultados sobre congruencias, se tiene:

Teorema de Wilson. Para p primo, se cumple:

$$(p-1)! \equiv -1 \bmod p$$

Teorema de Fermat. Si p es primo, todo entero a satisface $a^p \equiv a \bmod p$ y todo entero a no divisible por p satisface $a^{p-1} \equiv 1 \bmod p$, es decir, $a^{p-1} - 1$ es divisible por p.

Ejemplo 39. *Si a no es divisible por p y $n \equiv m \bmod (p-1)$, entonces $a^n \equiv a^m \bmod p$.*

Solución. Suponga que $n > m$. Como $p-1|n-m$, se tiene que $n-m = c(p-1)$ para algún entero positivo c. Como a no es divisible por p, del teorema de Fermat se tiene que $a^{p-1} \equiv 1 \bmod p$ y $(a^{p-1})^c \equiv 1 \bmod p$; así $a^{n-m} \equiv 1 \bmod p$, como $a^m \equiv a^m \bmod p$ resulta que $a^{n-m}a^m \equiv a^m \bmod p$ con lo que se obtiene el resultado $a^n \equiv a^m \bmod p$. ■

Ejemplo 40. *Para encontrar el residuo de la división de $2^{1\,000\,000}$ por 7, es posible utilizar el resultado del ejemplo anterior. Como $1\,000\,000 \equiv 4 \bmod 6$, se tiene $2^{1\,000\,000} \equiv 2^4 \bmod 7 \equiv 16 \bmod 7 \equiv 2 \bmod 7$; así, el residuo es 2.* ■

Ejemplo 41. *Demuestre que $N = n^{13} - n$ es múltiplo de $2\,730$, $\forall n \in \mathbb{N}$.*

Solución. Como N se puede factorizar como $N = n\left(n^{12} - 1\right)$, se tiene que N es divisible por 13; como N se puede factorizar como:

$$N = n\left(n^6 + 1\right)\left(n^6 - 1\right),$$

se tiene que N es divisible por 7. Además, N se puede factorizar como:

$$N = n\left(n^6+1\right)\left(n^4+n^2+1\right)\left(n^2-1\right)$$

y se obtiene que N es divisible por 3. Análogamente,

$$N = n\left(n^6+1\right)\left(n^4+n^2+1\right)(n+1)(n-1),$$

por lo que es divisible por 2; por último:

$$N = n\left(n^8+n^4+1\right)\left(n^4-1\right)$$

Con lo cual, N es divisible por 5. Resumiendo: a partir del Teorema de Fermat, se ha probado que N es divisible por 13, 7, 3, 2 y 5. Además, como todos ellos son números primos, N es divisible por su producto; así, N es divisible por $13 \cdot 7 \cdot 3 \cdot 2 \cdot 5 = 2\,730$. ■

Un resultado que es natural y lógico pero, a su vez, muy importante y útil, es el conocido **principio del palomar** o principio de las casillas. Establece que si $n+1$ palomas viven en n casitas, entonces al menos 2 palomas viven en la misma casita.

En los dos ejemplos siguientes se muestra la utilidad de este principio, ellos son de la autoría del famoso matemático Paul Erdös.

Ejemplo 42. *Dados n enteros, pruebe que uno de ellos es múltiplo de n o se pueden sumar varios de ellos para dar un múltiplo de n.*

Solución. Llame $a_1, a_2, \ldots, a_n$ los n enteros. Si uno de ellos es múltiplo de n, ya se cumple la conclusión y no habría nada que probar. Suponga que esto no ocurre, considere $S_i = a_1+a_2+\cdots+a_i$. Los posibles restos de la división de los S_i por n son solamente $1, 2, \ldots, n-1$, y como se tienen n números S_i, por el *principio del palomar*, habrá dos donde el residuo da el mismo valor, llámelos S_j y S_{j+k}, de donde $S_j \equiv S_{j+k} \mod n$, es decir $S_{j+k} - S_j = a_{j+1} + a_{j+2} + \cdots + a_{j+k}$ es divisible por n. ■

Ejemplo 43. *Sean* a_1, $a_2, \ldots, a_{n+1}$ *enteros menores o iguales que* $2n$*, pruebe que al menos uno de ellos es divisible por otro.*

Solución. Note que $a_r = c_r \cdot 2^{k_r}$ con c_r impar y menor que $2n$, pues todo número entero se puede escribir como una potencia de 2 por un número impar. Dado que la cantidad de enteros impares menores que $2n$ es n y se tienen $n+1$ números, por el *principio del palomar* se concluye que dos de estos impares se repiten, llámelos c_i y c_j. Es claro que si $k_i \geq k_j$, se tendría que a_j divide a a_i, y si $k_i < k_j$, a_i divide a a_j. ■

Si a y b son números enteros, el **máximo común divisor** de a y b es el mayor de todos los divisores comunes de a y b, y se denotará por m.c.d.(a, b). Además, se dice que dos números enteros a y b son **primos relativos** si y solo si m.c.d.$(a, b) = 1$.

Antes de enunciar el siguiente resultado, se define la función **φ de Euler** para valores enteros de n como el número de enteros no negativos $b < n$ tal que m.c.d.$(b, n) = 1$. Una forma sencilla de calcular el valor de esta función para n es con base en la factorización en factores primos de n, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$; de esta forma, se tiene que:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right)$$

Ejemplo 44. *La factorización en factores primos de* 3500 *es* $2^2 \cdot 5^3 \cdot 7$*. Así,* $\varphi(3500) = 3500\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 1200$. ■

El siguiente teorema es la "Generalización del Teorema de Fermat" y se conoce como el Teorema de Euler, ya que fue él quien lo demostró.

Teorema de Euler. Si m.c.d.$(a, n) = 1$, entonces:

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Ejemplo 45. *Se sabe que* $\varphi(20) = 8$*, observe que* $3^8 - 1 = 6\,560 = 328 \cdot 20$*, es decir,* $3^{\varphi(20)} \equiv 1 \bmod 20$. ■

Ejemplo 46. *¿Será el número* $10^{5^{10^{5^{10}}}} + 5^{10^{5^{10^{5}}}}$ *divisible por* 11*?*

Solución. Del Teorema de Fermat se sabe que $5^{10} \equiv 1 \bmod 11$, y dado que $10^{5^{10^5}}$ es múltiplo de 10, resulta que:

$$5^{10^{5^{10^{5}}}} \equiv 1 \bmod 11.$$

Además, dado que toda potencia de 5 es impar, y $10 \equiv -1 \bmod 11$, se tiene:

$$10^{5^{10^{5^{10}}}} \equiv -1 \bmod 11,$$

de donde

$$10^{5^{10^{5^{10}}}} + 5^{10^{5^{10^{5}}}} \equiv -1 + 1 \bmod 11 \equiv 0 \bmod 11.$$

Es decir, sí es divisible por 11. ■

Apéndice A

Solución de algunos ejercicios

"Cada problema que resolví
se volvió una regla,
que sirvió más tarde,
para resolver otros problemas".

Descartes

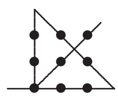
Sección 1.1, página 35

3. Cama suiza de roble en 1875, mesa austriaca de cedro en 1825 y silla francesa de fresno en 1850.

4. Tomando en cuenta como orden el tercero, el segundo y el primero, los posibles acomodos de los sombreros son: BBB, BBR, BRB, RBB, RRB, RBR, BRR. De los cuales se descarta BRR, pues si el primero hubiera visto los dos sombreros rojos de adelante, no hubiera dudado en decir que el suyo era blanco. Además, se descarta BBR y RBR, pues si el segundo ve un sombrero rojo delante de él y sabe, además, que el tercero no vio dos rojos delante de él, el segundo hubiera podido asegurar que su sombrero era blanco. Al descartar estos tres casos, en los cuatro casos restantes se ve que necesariamente el sombrero del primero es blanco.

5. En forma de una estrella de 5 puntas, con un niño en cada punta y en cada intersección de los segmentos 

6. Piense en una pirámide con base triangular.

7. 

8. El niño tiene el pelo rojo.

9. Sin tomar en cuenta la portada y contraportada, la polilla atravesó 102 hojas en total.

10a. $X = 10$. Aumentan progresivamente en 1, 2, 3, 4 . . .

10b. $X = 11$. Cada paso multiplica por 3 y alterna sumar 2 y restar 2.

10c. $X = 27$. Alternan dos series, una se suma 5 y la otra resta 3.

10d. $X = 174$. Se suma 3 y se multiplica por 3 en forma alternada.

10e. $X = 14$. Se divide por 2 y se resta 2 en forma alternada.

10f. $X = 253$. Los elementos de la segunda fila se obtienen sumando o multiplicando (en forma alternada) los de la columna anterior.

11. Observe la simetría axial con una recta vertical en cada término, el sexto será un número seis y su reflejo.

12. Si hay 70 inteligentes y 70 guapos, serían 140 entre ambos, pero como son 100, debe haber al menos 40 que sean inteligentes y guapos a la vez. Luego, al haber 40 inteligentes y guapos y 70 buenos, serían 110, pero como son 100, debe haber como mínimo 10 que sean inteligentes, guapos y buenos a la vez.

13. Se llena la de 4 y se vacía en la grande. Se llena de nuevo la de 4 y se vacía parte del contenido hasta llenar la grande, por lo que en la jarra pequeña quedará 1 litro. Luego, se vacía la grande y el litro de la pequeña se vacía en la de 7 litros. Se llena de nuevo la pequeña y se vierte el agua en la grande; así, en la grande se tienen 5 litros.

14. Si A fuese mentiroso, lo que dijo sería mentira, con lo cual la verdad sería "B es mentiroso y yo soy sincero", pero esto es imposible, ya que se estaría afirmando que A es mentiroso y sincero a la vez. Por lo tanto, se concluye que A es sincero, y con ello, lo que dice

es verdad, de donde B es sincero. Se concluye que tanto A como B son sinceros.

18. Llame A, B y C al primero, segundo y tercer vacilonio respectivamente. Se analizarán los dos casos posibles: A es sincero y A es mentiroso. En el primer caso, es decir, si A es sincero, entonces C debe ser mentiroso, puesto que C dijo que A era mentiroso; además, A debería haber respondido que él era sincero, por lo que B dijo la verdad y eso lo convierte en sincero. Resumiendo, en este primer caso se tiene que A y B son sinceros y C es mentiroso. En el segundo caso, si A es mentiroso, C dijo la verdad y esto lo convierte en sincero; además, A debería de haber contestado que él no era mentiroso, pues como mentiroso que es, debería de haber mentido, de donde se sigue que B dijo la verdad y, por lo tanto, es sincero. En este segundo caso, se ha visto que A es mentiroso, B y C son sinceros. Es decir, en ambos casos se ha concluido que B es sincero y siempre hay un mentiroso.

19. Es claro que un sincero no puede afirmar "yo soy un mentiroso", pues estaría mintiendo; además, un mentiroso tampoco puede afirmar "yo soy un mentiroso", pues estaría diciendo la verdad, es decir, aunque no se sabe lo que dijo A, es seguro que no afirmó que era mentiroso. Por lo tanto, B mentía cuando dijo que A había dicho que era un mentiroso. Por lo tanto, B es mentiroso. Por último, C dice que B está mintiendo, lo cual es cierto; por lo tanto C es sincero.

21. Si A es sincero, lo que dijo sería verdad; sin embargo, afirma que es mentiroso, pero no puede darse que sea sincero y mentiroso a la vez. Por lo tanto, A es mentiroso y lo que dijo: "Ambos somos mentirosos(as)" es mentira, es decir, lo cierto es "alguno es sincero", y como A no es sincero, se desprende que B debe ser sincero y, en consecuencia, lo que dijo es verdad. Por lo tanto, A es una mujer mentirosa y B es una mujer sincera.

22. Se encontraron el jueves.

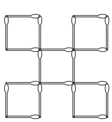
24. Alicia es costurera y tiene un Fiat; Bárbara es dentista y tiene un Mercedes; Carolina es bióloga y tiene un Toyota; Diana es abogada y tiene un Subarú.

25. $T = 3$, $R = 5$, $E = 6$, $S = 2$, $N = 1$, $U = 0$, $V = 8$.

26. Para iniciar, debe observar y concluir (desechando los otros casos) que M debe ser 1; luego, S debe ser 9; luego O debe ser 0, etc. Para obtener finalmente que la suma es:
$$\begin{array}{ccccc} & 9 & 5 & 6 & 7 \\ + & 1 & 0 & 8 & 5 \\ \hline 1 & 0 & 6 & 5 & 2 \end{array}$$

27. El culpable es Rafael.

28. Se colocan los dos primeros interruptores encendidos y los dos últimos apagados, es decir, $EEAA$. Se espera unos minutos, se colocan en $EAEA$ y entra a la habitación: si el bombillo está caliente y encendido, el interruptor correcto es el primero; si el bombillo está caliente y apagado, el interruptor es el segundo; si está frío y encendido, es el tercero, y por último, si está frío y apagado, es el cuarto interruptor el que enciende el bombillo.

29. 

30. Se puede lograr con una sola pesada. Coloque una moneda del primer saco, 2 monedas del segundo saco, 3 del tercero y así sucesivamente hasta 8 monedas del octavo saco.

31. La botella más pequeña les permite adelantar hacia la piedra, y la del extremo derecho los llevará hacia atrás.

32. Para A, B, C las posibles edades, se tienen 8 casos posibles:

	A	B	C
1	1	1	36
2	1	2	18
3	1	3	12
4	1	4	9
5	1	6	6
6	2	2	9
7	2	3	6
8	3	3	4

Sólo en los casos 5 y 6 se obtiene una suma igual, de manera que si le faltaba un dato, el amigo vive en la casa número 13. En ambos casos hay mellizos, pero sólo en el caso 6 se puede hablar de *el mayor*; por lo tanto, las edades son 2, 2, 9.

33. Sean: x la edad que yo tengo y y la edad que tú tienes. Se plantea el sistema de ecuaciones lineales:

$$\left\{ \begin{array}{rcl} 2(y-(x-y)) & = & x \\ (x+(x-y))+(y+(x-y)) & = & 63 \end{array} \right.$$

Al resolverlo, se obtiene que yo tengo 28 y tú 21 años.

34b. El origen de la paradoja de Protágoras reside en el hecho de que tanto Protágoras como su alumno primero aceptan la autoridad del tribunal, pero después, si el veredicto no les favorece, deciden no someterse. Dicho de otra manera: más que una paradoja, este es un caso de mala fe por parte de maestro y alumno. La finalidad del pleito es resolver el conflicto entre las partes. Pero deja de tener sentido si estas condicionan su acatamiento al resultado. Conclusión: Si no van a juicio, pues no hay paradoja. Si van a juicio, tendrán que acatar sin discusión lo que decida el tribunal.

34c. Si no se afeita a sí mismo, será una de las personas de la ciudad que no se afeitan a sí mismas, con lo cual debería de afeitarse, siendo, por tanto, una de las personas que se afeitan a sí mismas, no debiendo por tanto afeitarse.

Sección 1.2, página 53

3. Tome A, B verdaderas y C, D, E falsas.

11. (a). $P \rightarrow (Q \wedge R)$
    (b). $(Q \wedge R) \rightarrow P$
    (c). $\neg S \leftrightarrow (Q \rightarrow P)$
    (d). $(\neg Q \vee \neg R) \rightarrow (\neg P \wedge S)$
    (e). $Q \vee (S \leftrightarrow \neg P)$.

13. La tabla de verdad de $(P \mid Q) \mid (P \mid Q)$ es:

P	Q	$P \mid Q$	$(P \mid Q) \mid (P \mid Q)$
V	V	F	V
V	F	V	F
F	V	V	F
F	F	V	F

Con lo cual se tiene que $(P \mid Q) \mid (P \mid Q) \equiv P \wedge Q$.

Sección 1.3, página 61

1. $P \vee R$

2. $(P \leftrightarrow R) \wedge \neg(\neg P \vee R) \equiv (\neg P \vee R) \wedge (\neg R \vee P) \wedge (P \wedge \neg R) \equiv (\neg P \vee R) \wedge [(\neg R \vee P) \wedge P] \wedge \neg R \equiv \neg(P \wedge \neg R) \wedge (P \wedge \neg R) \equiv F_0$

3. $P \vee S$

4. $[(\neg P \vee Q) \wedge P] \rightarrow Q \equiv [(\neg P \wedge P) \vee (Q \wedge P)] \rightarrow Q \equiv [F_0 \vee (Q \wedge P)] \rightarrow Q \equiv (Q \wedge P) \rightarrow Q \equiv \neg(Q \wedge P) \vee Q \equiv \neg Q \vee \neg P \vee Q \equiv (\neg Q \vee Q) \vee \neg P \equiv V_0 \vee \neg P \equiv V_0$

5. F_0

6. $\neg P$

7. $[(\neg P \vee Q) \wedge \neg R] \to [(\neg Q \wedge R) \vee P] \equiv [(P \wedge \neg Q) \vee R] \vee [(\neg Q \wedge R) \vee P] \equiv [(P \wedge \neg Q) \vee P] \vee [(\neg Q \wedge R) \vee R] \equiv P \vee R$

8. $(\neg P \wedge Q) \vee [\neg P \wedge \neg(Q \wedge R)] \vee \neg(R \to P) \equiv (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R) \vee (R \wedge \neg P) \equiv [(\neg P \wedge Q) \vee (\neg P \wedge \neg Q)] \vee [(\neg P \wedge \neg R) \vee (R \wedge \neg P)] \equiv [\neg P \wedge (Q \vee \neg Q)] \vee [\neg P \wedge (\neg R \vee R)] \equiv [\neg P \wedge V_0] \vee [\neg P \wedge V_0] \equiv \neg P$

9. $[P \to (Q \wedge P)] \vee [\neg Q \wedge (P \vee Q)] \equiv [\neg P \vee (Q \wedge P)] \vee [\neg Q \wedge (P \vee Q)] \equiv [\neg P \vee (Q \wedge P)] \vee [(\neg Q \wedge P) \vee (\neg Q \wedge Q)] \equiv [\neg P \vee (Q \wedge P)] \vee [(\neg Q \wedge P) \vee F_0] \equiv \neg P \vee [(Q \wedge P) \vee (\neg Q \wedge P)] \equiv \neg P \vee [(Q \vee \neg Q) \wedge P] \equiv \neg P \vee (V_0 \wedge P) \equiv \neg P \vee P \equiv V_0$

10. $\neg Q \vee \neg \Big[\big[\neg[(P \wedge Q) \vee (P \wedge \neg Q)] \vee Q\big] \wedge P \Big] \equiv \neg Q \vee \neg \Big[\big[\neg[P \wedge (Q \vee \neg Q)] \vee Q\big] \wedge P \Big] \equiv \neg Q \vee \neg \big[(\neg P \vee Q) \wedge P\big] \equiv \neg Q \vee \neg \big[(\neg P \wedge P) \vee (Q \wedge P)\big] \equiv \neg Q \vee \neg[(Q \wedge P)] \equiv \neg Q \vee \neg Q \vee \neg P \equiv \neg Q \vee \neg P$

14. $\neg P \wedge \neg Q$

Sección 1.4, página 71

1d. Se parte de las premisas 1. $P \to Q$, 2. $Q \to R \wedge S$, 3. $\neg R \vee \neg T \vee U$, 4. $P \wedge T$, se debe probar que es válida U.

5.	P	Simpl. a 4.
6.	T	Simpl. a 4.
7.	Q	MP a 1 y 5.
8.	$R \wedge S$	MP a 2 y 7.
9.	R	Simpl. a 8.
10.	$\neg T \vee U$	SD a 3 y 9.
11.	U	SD a 6 y 10.

1f. Se parte de las premisas 1. $V \to (R \vee P)$, 2. $R \to \neg V$, 3. $L \to \neg P$, 4. V, se debe probar que es válida $\neg(L \wedge D)$

5.	$\neg R$	MT a 2 y 4.
6.	$R \vee P$	Separación a 1 y 4.
7.	P	SD a 5 y 6.
8.	$\neg L$	MT a 3 y 7.
9.	$\neg L \vee \neg D$	Adición de $\neg D$ a 7.
10.	$\neg(L \wedge D)$	De Morgan a 9.

1p. Se debe simbolizar correctamente si, por ejemplo, se toman las proposiciones $P : x = 5$, $Q : z > x$, $R : x < 7$, $S : x < 6$, $T : x = 3$, $U : z = 8$. Para finalizar, usted debe demostrar la validez del argumento:

$$\begin{array}{ll} 1. & Q \to R \\ 2. & (S \vee T) \to Q \\ 3. & S \wedge U \\ 4. & \neg R \vee P \\ \hline & \therefore P \end{array}$$

2a. Se debe probar que las premisas 1. $P \to Q$, 2. $P \vee (T \wedge S)$, 3. $Q \to R$, 4. $\neg R$, implican lógicamente a la conclusión S

5.	$P \to R$	SH a 1 y 3.
6.	$\neg P$	MT a 4 y 5.
7.	$T \wedge S$	SD a 2 y 6.
8.	S	Simplificación a 7.

3g. Considere las proposiciones: M: matriculo Matemática discreta; G: gano los otros cuatro cursos matriculados; C: cambio de carrera; N: me he decidido; D: quiero estudiar computación. Se debe probar $\neg N$.

1.	$\neg M \to G$	Premisa
2.	$G \vee C$	Premisa
3.	$M \wedge C \to \neg N$	Premisa
4.	$\neg(G \wedge \neg D)$	Premisa
5.	$\neg D$	Premisa
6.	$\neg G \vee D$	DM. a 4.
7.	$\neg G$	SD a 5 y 6.
8.	M	MT a 1 y 7. y DN.
9.	C	SD. a 2 y 7.
10.	$M \wedge C$	Adj. a 8 y 9.
11.	$\neg N$	MP. a 3 y 10.

3j. Considere las proposiciones P: Leo es un muchacho y las variables x: la edad de Leo y y: la edad de Juan. Así, la proposición "*Si Leo es un muchacho, entonces Leo es más joven que Juan*" se simboliza como $P \to x < y$. Luego de simbolizar todo el argumento, usted concluirá que "*Leo es una muchacha*".

3k. Considere las proposiciones:
P: le pago al sastre; D: tengo dinero; B: puedo llevar a mi novia al baile; T: tengo traje; E: mi novia se enojará conmigo.

1.	$P \to \neg D$	Premisa
2.	$B \to D$	Premisa
3.	$\neg B \to E$	Premisa
4.	$\neg P \to \neg T$	Premisa
5.	$\neg T \to \neg B$	Premisa
6.	$\neg D \vee \neg T$	LC. a 1, 4.
7.	$\neg D \to \neg B$	contrapositiva a 2.
8.	$\neg B \vee \neg B$	DC a 5, 6 y 7.
9.	$\neg B$	Idemp. a 8.
10.	E	MP a 3 y 9.

4. Basta encontrar una asignación de valores de verdad para cada proposición atómica, de manera que las premisas sean verdaderas y la conclusión sea falsa.

5. Considere las proposiciones:
   P : Usted es un niño; Q : Usted es ilógico; R : Usted puede domar un cocodrilo; S : Usted es despreciado.
   La proposición "Los niños son ilógicos" se simboliza como: $P \to Q$; la proposición "Nadie es despreciado cuando puede domar un cocodrilo" se simboliza como: $R \to \neg S$; y por último, la proposición "Las personas ilógicas son despreciadas" es $Q \to S$. De estas tres premisas, usted puede inferir como conclusión $P \to \neg R$, que en palabras diría: "Si usted es un niño, no puede domar un cocodrilo" o, como el mismo Lewis Carroll escribiera, "Los niños no pueden domar cocodrilos".

7. En Vacilonia no llueve, las vacas vuelan, sus habitantes son altos y tienen cinco ojos.

8. Aquí solamente se probaron MIM y MIU; para abreviar, indicó sobre la flecha la regla que se utiliza:

   $$\text{MI} \xrightarrow{1} \text{MIMIMI} \xrightarrow{4} \text{MIMIMUI} \xrightarrow{5} \text{MIMIUI} \xrightarrow{2} \text{MIMIIII} \xrightarrow{3} \text{MIM}$$

   Como ya se probó que MIM es admisible, se puede utilizar para probar MIU:

   $$\text{MIM} \xrightarrow{4} \text{MIMU} \xrightarrow{5} \text{MIU}$$

   Para el resto de las palabras, usted debe encontrar el procedimiento correcto. Por último, para probar que MU no se puede probar, observe que con cualquiera de las reglas que se aplican se mantiene que la cantidad de I que aparecen será siempre impar, y como MU no tiene cantidad impar, nunca se podrá deducir.

9. Recuerde que $a \geq b$ es equivalente a escribir $a > b \vee a = b$. Debe aplicar la distributividad en $(a > b \vee a = b) \wedge a \leq b$, luego la Ley

de Inversos, distributividad, e Inversos nuevamente para concluir entonces que $a = b$. Además, tome en cuenta que la proposición $a > b \ \wedge \ a \leq b$ es una contradicción.

Sección 1.5, página 80

1c. Se escribe la expresión como una disyunción de conjunciones:

$\neg\big[\neg(\neg P \wedge \neg Q) \vee \neg(Q \to R)\big] \wedge \neg(R \to P)$	**Justific.**
$\equiv (\neg P \wedge \neg Q) \wedge (Q \to R) \wedge \neg(R \to P)$	DM y DC.
$\equiv (\neg P \wedge \neg Q) \wedge (\neg Q \vee R) \wedge (R \wedge \neg P)$	DM.
$\equiv \big[(\neg P \wedge \neg Q \wedge \neg Q) \vee (\neg P \wedge \neg Q \wedge R)\big] \wedge (R \wedge \neg P)$	Aso., Dist.
$\equiv (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$	Dist., Idem.

1e. $(P \vee R) \wedge (P \vee S \vee T) \wedge (Q \vee R) \wedge (Q \vee S \vee T)$.

Sección 1.6, página 91

1a. $(\forall a, b \in \mathbb{R}^+)(\exists n \in \mathbb{Z})\big[na \geq b\big]$

1d. $(\forall x \in \mathbb{R}^+)(\exists n \in \mathbb{N}^*)\big[\frac{1}{n} < x\big]$

1e. Considere las proposiciones abiertas $P(a, b)$: a y b son primos relativos, y $M(a, b)$: el máximo común divisor a y b es 1, por lo que la proposición se simboliza como:

$$(\forall a \in \mathbb{N})(\forall b \in \mathbb{N})\,[P(a, b) \leftrightarrow M(a, b)]$$

O simplemente $\forall a, b \in \mathbb{N} \ \ [P(a, b) \leftrightarrow M(a, b)]$

1g. $\neg\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [y < x] \equiv \forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\, [y \geq x]$

3a. $(\exists n \in \mathbb{N})\big[n^2 - 2n + 5 < 4\big]$

4b. Al menos un miembro del club tiene 30 años o menos.

5. (a). V pues $x = 9$ cumple; (b). V pues $x = 7$ cumple; (c). V pues todos cumplen; (d). F pues $x = 7$ no cumple.

6. (a). F (b). V (c). F (d) V (e). V

8. $P(x) : x$ gusta de la poesía; $Q(x) : x$ es domesticable.
"Ningún conejo que gusta de la poesía es indomesticable" se simboliza como $\neg\exists x\big[P(x)\wedge\neg Q(x)\big]$ y es equivalente a las proposiciones $\forall x\big[\neg P(x) \vee Q(x)\big]$ o $\forall x\big[P(x) \to Q(x)\big]$

10b. Se debe probar que si n es impar, entonces n^2 es impar. Si n es impar, existe $k \in \mathbb{Z}$ tal que $n = 2k + 1$, esto implica que:

$$n^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1 = 2k' + 1,$$

con $k' \in \mathbb{Z}$, con lo cual n^2 es impar.

10e. Si $n + m$ es par, entonces, por la parte 10a, $(n + m)^2$ también es par. Desarrolle la fórmula notable y concluya.

13. $(\exists\epsilon > 0)(\forall\delta > 0)\big[x < \delta \wedge f(x) \ \geq \ \epsilon\big]$

17. Su demostración se hará probando la validez de su contrapositiva:

$$\neg(x = 0 \ \wedge \ y = 0) \to \neg\big[(\forall\, a, b \in \mathbb{R})\ ax + by = 0\big],$$

que es equivalente a:

$$(x \neq 0 \ \vee \ y \neq 0) \to \big[(\exists\, a, b \in \mathbb{R})\ ax + by \neq 0\big]$$

Basta tomar $x \neq 0$, $a = 1$, $b = 0$.

18. Sea P la proposición del enunciado. Así, su negación es:

$$\neg P \equiv (\exists\, a, b \in \mathbb{R})\ \big[ax + by = 0 \ \wedge \ (x \neq 0 \ \vee \ y \neq 0)\big],$$

que es verdadera al tomar $a = 0$, $b = 0$, por lo que la proposición P es falsa.

19. Observe que para cada valor ϵ positivo se puede tomar $\delta = \frac{\epsilon}{3}$ y se cumple la proposición.

Sección 1.7, página 98

1b.

1.	$\forall x\, \big[\neg Q(x) \to \neg P(x)\big]$	Premisa
2.	$\forall x\, \big[Q(x) \to (R(x) \wedge S(x))\big]$	Premisa
3.	$\nexists x\, \big[\neg P(x) \vee \neg T(x)\big]$	Premisa
4.	$\forall x\, \neg\big[\neg P(x) \vee \neg T(x)\big]$	(1.5) a 3.
5.	$\forall x\, \big[P(x) \wedge T(x)\big]$	De Morgan a 4.
6.	$\forall x\, P(x)$	Simplificación a 5.
7.	$\forall x\, \big[P(x) \to Q(x)\big]$	Contrapositiva a 1.
8.	$\forall x\, Q(x)\big]$	MT a 6 y 7.
9.	$\forall x\, \big[R(x) \wedge S(x)\big]$	MT a 2 y 8.
10.	$\forall x\, S(x)$	Simplificación a 9.

Sección 2.1, página 121

3. $B \times A = \big\{(1, \varnothing), (1, 2), (1, \{2\}), (\{2\}, \varnothing), (\{2\}, 2), (\{2\}, \{2\})\big\}$
   $P(A) = \big\{\varnothing, \{\varnothing\}, \{2\}, \{\{2\}\}, \{\varnothing, 2\}, \{\varnothing, \{2\}\}, \{2, \{2\}\}, A\big\}$
   $A \cap B = \big\{\{2\}\big\}$
   $B - A = \{1\}$

5. $(A \cup C) \bigtriangleup B = \{a, c\}$
   $P(\overline{A} \cap \overline{B}) = \big\{\varnothing, \{e\}, \{f\}, \{e, f\}\big\}$
   $(C \times B) - (A \times C) = \big\{(a, b), (a, c), (d, b), (d, c), (d, d)\big\}$

8. $P(P(A)) = P\left(\{\varnothing, \{a\}\}\right) = \Big\{\varnothing, \{\varnothing\}, \{\{a\}\}, \{\varnothing, \{a\}\}\Big\}$
   $P(A) \times P(A) = \big\{(\varnothing, \varnothing), (\varnothing, \{a\}), (\{a\}, \varnothing), (\{a\}, \{a\})\big\}$

10. $C - (A \bigtriangleup B) = \{4\}$
    $P(A) - P(B) = \big\{\{2\}, \{2, 3\}, \{2, 4\}, \{2, 3, 4\}\big\}$
    $(A \cap C) \times \overline{(B \cup C)} = \{(2, 0), (2, 5), (4, 0), (4, 5)\}$

12. $A = \{2, 3, 4, 6, 8, 9, 10\}$, $B = \{6\}$, $C = \{2, 3, 4, 8, 9, 10\}$

14. Es claro que cualquier elemento de A se puede escribir como un elemento de B; para ello observe que $3n - 2 = 3n - 2 + 4 - 4 = 3n - 6 + 4 = 3(n - 2) + 4 = 3m + 4$, donde $m = n - 2$ es entero. Análogamente, cualquier elemento de B se puede escribir como un elemento de A. Por lo tanto, $A = B$ es una proposición verdadera.

23. Si la palabra *heterológica* fuera autológica, entonces cumple con lo que ella significa; por lo tanto, es heterológica. Por otro lado, si la palabra *heterológica* fuera heterológica, cumpliría lo que significa; por lo tanto, sería autológica. En ambos casos se tiene una contradicción. Observe que el razonamiento es análogo al de la paradoja de Russell.

Sección 2.2, página 131

2e. $5,22\overline{681} = \frac{522681-522}{99900} = \frac{174053}{33300}$

2g. $267,3457\overline{68923} = \frac{133671547733}{499995000}$

4a. $56,23\overline{374} = \frac{5623374-5623}{(10^3-1)(10^2)} = \frac{5617751}{99900}$.

Sección 2.3, página 135

2. La única verdadera es la segunda.

Sección 2.4, página 140

1.

$$\begin{aligned}
\overline{[(\overline{A} \cup B) \cap A]} \cup B &= \overline{[(\overline{A} \cap A) \cup (A \cap B)]} \cup B \\
&= \overline{[\varnothing \cup (A \cap B)]} \cup B \\
&= \overline{A \cap B} \cup B \\
&= \overline{A} \cup \overline{B} \cup B \\
&= \overline{A} \cup \mathcal{U} = \mathcal{U}
\end{aligned}$$

2.

$$
\begin{aligned}
\left[A\cup\overline{(\overline{B}\cup\overline{C})}\right]\cup(\overline{B}\cap C) &= [A\cup(B\cap C)]\cup(\overline{B}\cap C)\\
&= A\cup[(B\cap C)\cup(\overline{B}\cap C)]\\
&= A\cup[(B\cup\overline{B})\cap C]\\
&= A\cup[\mathcal{U}\cap C]\\
&= A\cup C
\end{aligned}
$$

6. $\mathcal{U}$

7. $A\cup B$

8. $B\cap C$

Sección 2.5, página 146

4. 1100 solo guitarra; 100 solo saxofón; 900 guitarra y saxofón; 2250 solo un instrumento.

5. Solo fútbol 150 personas; 180 solo atletismo y 250 solo ciclismo.

8. $|P(A)\times P(B)| = 32$, por otro lado, $|P(A\times B)| = 64$.

10. (a). 16 (b). 32 (c). 16

12. $3\cdot 2^5 = 96$

13. (a). 12 (b). $2^{4\cdot 6} = 2^{24}$

14. (a). $3\cdot 2^5 = 96$ (b). $2^{3\cdot 7} = 2^{21}$

15. 496.

16. $6\cdot 2^7 = 768$

17. 17a. $A = \{\varnothing\}$; 17b. $A = \{1,2,3,4,5,6\}$; 17c. $A = \{1\}$; 17d. $A = \{1,2\}$; 17e. $A = \{\varnothing, 1\}$; 17f. $A = \{\varnothing,1,2,3\}$.

18. Se utiliza la fórmula 2.1 y las leyes a la expresión $|A \cup (B \cup C)|$:

$$\begin{aligned}
&= |A| + |B \cup C| - |A \cap (B \cup C)| \\
&= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \\
&= |A| + |B| + |C| - |B \cap C| \\
&\quad - \Big(|A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|\Big) \\
&= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|
\end{aligned}$$

Sección 2.6, página 153

3. $A = [2, 5[$ y $B = [3, 4]$.

Sección 2.7, página 162

1b. $S \in P(A) \cup P(B) \Rightarrow S \in P(A) \vee S \in P(B) \Rightarrow S \subseteq A \vee S \subseteq B \Rightarrow S \subseteq A \cup B \Rightarrow S \in P(A \cup B)$

1c. $(a, b) \in \overline{A} \times \overline{B} \Rightarrow a \in \overline{A} \wedge b \in \overline{B} \Rightarrow a \notin A \wedge b \notin B \Rightarrow (a, b) \notin A \times B \Rightarrow (a, b) \in \overline{A \times B}$

1d. $x \in B - A \Rightarrow x \in B \wedge x \notin A \Rightarrow x \in B \Rightarrow x \notin A \vee x \in B \Rightarrow \neg(x \in A \wedge x \notin B) \Rightarrow \neg(x \in A - B) \Rightarrow x \in \overline{A - B}$

2a. Suponga que $A \cap (B - A) \neq \varnothing \Rightarrow \exists x$ tal que $x \in A \cap (B - A) \Rightarrow x \in A \wedge x \in (B - A) \Rightarrow x \in A \wedge x \in B \wedge x \notin A \Rightarrow x \in A \wedge x \notin A (\Rightarrow\Leftarrow)$; por lo tanto, $A \cap (B - A) = \varnothing$

2d. $a \in (A - B) - C \Leftrightarrow a \in A - B \wedge a \notin C \Leftrightarrow (a \in A \wedge a \notin B) \wedge a \notin C \Leftrightarrow a \in A \wedge (a \notin B \wedge a \notin C) \Leftrightarrow a \in A \wedge \neg(a \in B \vee a \in C) \Leftrightarrow a \in A \wedge \neg(a \in B \cup C) \Leftrightarrow a \in A \wedge (a \notin B \cup C) \Leftrightarrow a \in A - (B \cup C)$

2o. $(a, b) \in A \times (\overline{B \cap C}) \Leftrightarrow a \in A \wedge b \in \overline{B \cap C} \Leftrightarrow a \in A \wedge b \notin B \cap C \Leftrightarrow a \in A \wedge (b \notin B \vee b \notin C) \Leftrightarrow (a \in A \wedge b \in \overline{B}) \vee (a \in A \wedge b \in \overline{C}) \Leftrightarrow (a, b) \in A \times \overline{B} \vee (a, b) \in A \times \overline{C} \Leftrightarrow (a, b) \in (A \times \overline{B}) \cup (A \times \overline{C})$

2r. A partir de la definición, se sabe que $A \triangle B = (A-B) \cup (B-A)$; por lo tanto, basta probar que $(A-B) \cup (B-A) = (A \cup B) - (A \cap B)$:

$$\begin{aligned}
x \in (A-B) \cup (B-A) &\Leftrightarrow\ x \in (A-B)\ \vee\ x \in (B-A) \\
&\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \\
&\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A) \\
&\quad\ \wedge (x \notin B \vee x \in B) \wedge (x \notin B \vee x \notin A) \\
&\Leftrightarrow (x \in A \cup B) \wedge T_0 \wedge x \notin (A \cap B) \\
&\Leftrightarrow (x \in A \cup B) \wedge x \notin (A \cap B) \\
&\Leftrightarrow x \in (A \cup B) - (A \cap B)
\end{aligned}$$

2s. Se probará que $\forall x\ [x \in A - (B \cup C) \Leftrightarrow x \in (A-B) \cap \overline{C}]$

$$\begin{aligned}
x \in A - (B \cup C) &\Leftrightarrow\ x \in A\ \wedge\ x \notin B \cup C \\
&\Leftrightarrow\ x \in A\ \wedge\ (x \notin B\ \wedge\ x \notin C) \\
&\Leftrightarrow\ (x \in A \wedge x \notin B)\ \wedge\ x \notin C \\
&\Leftrightarrow\ x \in A - B\ \wedge\ x \in \overline{C} \\
&\Leftrightarrow\ x \in (A-B) \cap\ \overline{C}
\end{aligned}$$

3g. Se debe probar, bajo la hipótesis $D \subseteq A - B\ \wedge\ E \subseteq A \cap B$, que se cumple $D \cap E = \varnothing$. Se efectúa la prueba por contradicción, es decir, suponga que $D \cap E \neq \varnothing$; a partir de esta proposición, se sigue que:

$$\begin{aligned}
\exists a \in D \cap E \quad &\Rightarrow \quad (a \in D)\ \wedge\ (a \in E) \\
&\Rightarrow \quad (a \in A - B)\ \wedge\ (a \in A \cap B) \\
&\Rightarrow \quad (a \in A\ \wedge\ a \notin B)\ \wedge\ (a \in A\ \wedge\ a \in B) \\
&\Rightarrow \quad (a \notin B\ \wedge\ a \in B) \quad (\Rightarrow\Leftarrow)
\end{aligned}$$

La última proposición es una contradicción que se obtuvo al suponer $D \cap E \neq \varnothing$, con lo cual, esta suposición es falsa y se concluye que $D \cap E = \varnothing$ es verdadera.

3l. Para este ejercicio, debe recordar la Ley de exportación, con lo cual, es claro que se tienen dos hipótesis:

$$
\begin{array}{ll}
1. & A \neq \varnothing \text{ es decir, } \exists x \ / \ \ x \in A \\
2. & A \times B \subseteq A \times C
\end{array}
$$

Bajo estas dos hipótesis se debe demostrar que $B \subseteq C$.
Prueba:

$$
\begin{aligned}
b \in B \quad & \Rightarrow \quad (x, b) \in A \times B \\
& \Rightarrow \quad (x, b) \in A \times C \\
& \Rightarrow \quad x \in A \wedge b \in C \\
& \Rightarrow \quad b \in C
\end{aligned}
$$

3m. Se parte de las premisas:

$$
\begin{array}{ll}
1. & A \cap B \subseteq \overline{D} \\
2. & \overline{B} \cap D = \varnothing
\end{array}
$$

Es necesario probar que $A \subseteq \overline{D}$. Suponga, por contradicción, que $A \not\subseteq \overline{D}$:

3.	$\exists x \ / \ \ x \in A \ \wedge \ x \notin \overline{D}$	Definición
4.	$x \in A$	Simplificación a 3.
5.	$x \notin \overline{D}$	Simplificación a 3.
6.	$x \notin A \cap B$	Contrapositiva a 1.
7.	$x \notin A \ \vee \ x \notin B$	De Morgan a 6.
8.	$x \notin B$	Silogismo disjuntivo a 4 y 7.
9.	$x \notin B \ \wedge \ x \notin \overline{D}$	Adjunción de 5 y 8.
10.	$x \in \overline{B} \ \wedge \ x \in D$	Definición de complemento a 9.
11.	$x \in \overline{B} \cap D$	Definición de intersección a 10.

Lo cual es una contradicción con la premisa 2.; por lo tanto, se concluye que $A \not\subseteq \overline{D}$ es falsa, es decir, que $A \subseteq \overline{D}$ es verdadera.

4h. En el ejemplo 68 se probó "$\Rightarrow$". Para probar "$\Leftarrow$", suponga que $A \cap B \neq \varnothing$, se sigue que $\exists x \in A \cap B \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in \overline{B} \ \wedge \ x \in B$ ($\Rightarrow\Leftarrow$); por lo tanto, $A \cap B = \varnothing$.

5c. Si $A = \{1, 2\}$, $B = \{2\}$ y $C = \{3\}$, se tiene que $A - (B \cap C) = \{1, 2\}$; además, $(A - B) \cap (A - C) = \{1\}$ y es claro que $A - (B \cap C) \nsubseteq (A - B) \cap (A - C)$.

5f. Si $A = \{1\}$ y $B = \{2\}$, se tiene que $A \cup B = \{1, 2\}$, así, $P(A \cup B) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$, mientras que $P(A) \cup P(B) = \{\varnothing, \{1\}, \{2\}\}$ y es claro que $P(A \cup B) \nsubseteq P(A) \cup P(B)$.

5h. Para $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{1, 2\}$ es claro que $A - B \neq \varnothing$ y $B - C \neq \varnothing$ son verdaderas, pero $A - C \neq \varnothing$ es falsa.

Sección 3.1, página 174

4. $G_{\mathcal{R}} = \{(1,2), (1,3), (2,1), (2,3), (2,4), (3,1), (3,2), (3,4), (3,5), (4,2), (4,3), (4,5), (5,3), (5,4)\}$,
   $G_{\mathcal{S}} = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3), (5,1), (5,2), (5,3), (5,4)\}$
   $G_{(\mathcal{S} \circ \mathcal{R}) - (\mathcal{R} \circ \mathcal{S})} = \{(1,1), (1,2), (2,1)\}$

Sección 3.2, página 183

2. Las matrices pedidas son:

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad M_{\mathcal{S}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$M_{\overline{\mathcal{R} \cup \mathcal{S}}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad M_{\mathcal{S} \circ \mathcal{R}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

5. $M_{\mathcal{R}} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ y se tiene que:

   $G_{\mathcal{R}} = \{(\sharp,\sharp),(\sharp,a),(a,\sharp),(a,0),(2,\sharp),(0,\sharp),(0,a),(0,2),(0,0)\}$

   Por último, $G_{\overline{\mathcal{R}}-\mathcal{R}^{-1}} = \big\{(a,a),(a,2),(2,a),(2,2)\big\}$.

6. $M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ $M_{\mathcal{S}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$

8. $n = 4$, además, $M_{\mathcal{R}^{2006}} = M_{\mathcal{R}^2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Sección 3.3, página 193

1a. $\mathcal{R}_1$ es no reflexiva, simétrica, transitiva, antisimétrica y no total.

1b. $\mathcal{R}_2$ es reflexiva, no simétrica, transitiva, antisimétrica y no total.

1e. $\mathcal{R}_5$ es reflexiva, simétrica, transitiva, no antisimétrica y no total.

5. $G = \{(1,1),(2,2),(3,3)\}$

19a. Por hipótesis, A es finito y tiene n elementos, por lo cual es posible suponer que $A = \{a_1, a_2, \ldots, a_n\}$.

“$\Rightarrow$” Suponga que $\mathcal{R}$ es reflexiva, se debe probar que $I_n \leq M_{\mathcal{R}}$, es decir, que la entrada ij de la matriz I_n es menor o igual que la entrada ij de la matriz $M_{\mathcal{R}}$.
Prueba: como se asume que $\mathcal{R}$ es reflexiva, se tiene que $a_i\mathcal{R}a_i$, por lo que $M_{\mathcal{R}}[i,i] = 1$; así se cumple que $I_n[i,i] = 1 = M_{\mathcal{R}}[i,i]$. Además, es claro que si $i \neq j$, se tiene que $I_n[i,j] = 0 \leq M_{\mathcal{R}}[i,j]$. De donde se concluye que $I_n \leq M_{\mathcal{R}}$.

"$\Leftarrow$" Asumiendo que $I_n \leq M_{\mathcal{R}}$ como hipótesis, se debe probar que $\mathcal{R}$ es reflexiva.
Prueba: como por hipótesis se asume que $I_n \leq M_{\mathcal{R}}$, se tiene que $1 = I_n[i,i] \leq M_{\mathcal{R}}[i,i]$, con lo cual $1 = M_{\mathcal{R}}[i,i]$ y se concluye que $a_i \mathcal{R} a_i$; por lo tanto, $\mathcal{R}$ es reflexiva.

10c. Es claro que no es reflexiva, pues $A - A = \varnothing$. Tampoco es simétrica, pues $A - B \neq \varnothing$ no implica necesariamente que $B - A \neq \varnothing$. Tampoco es transitiva (repase el ejercicio 5h de la sección 2.7). Por último, verifique que no es antisimétrica ni total.

11e. Se asume $\mathcal{R}$ antisimétrica, se prueba que $\mathcal{R} \cap \mathcal{R}^{-1}$ es antisimétrica.

$$
\begin{aligned}
a\mathcal{R} \cap \mathcal{R}^{-1} b \ \wedge \ b\mathcal{R} \cap \mathcal{R}^{-1} a \quad & \Rightarrow \quad (a\mathcal{R}b \wedge a\mathcal{R}^{-1}b) \wedge (b\mathcal{R}a \wedge b\mathcal{R}^{-1}a) \\
& \Rightarrow \quad (a\mathcal{R}b \wedge b\mathcal{R}a) \ \wedge \ (b\mathcal{R}a \wedge a\mathcal{R}b) \\
& \Rightarrow \quad a = b \ \wedge \ a = b \\
& \Rightarrow \quad a = b
\end{aligned}
$$

12c. Considere $A = \{1, 2\}$ y sea $\mathcal{R}$ de manera que $G_{\mathcal{R}} = \{(1, 2)\}$. Se tiene que $G_{\mathcal{R}^{-1}} = \big\{(2, 1)\big\}$; además, $G_{\mathcal{R} \cup \mathcal{R}^{-1}} = \big\{(1, 2), (2, 1)\big\}$. Es claro que tanto $\mathcal{R}$ como $\mathcal{R}^{-1}$ son antisimétricas, pero $\mathcal{R} \cup \mathcal{R}^{-1}$ no.

14. Aplicando las definiciones y la hipótesis de que $\mathcal{R}$ y $\mathcal{S}$ son transitivas, se obtiene:

$$
\begin{aligned}
a(\mathcal{R} \cap \mathcal{S})b \wedge b(\mathcal{R} \circ \mathcal{S})a \quad & \Rightarrow \quad a\mathcal{R}b \wedge a\mathcal{S}b \wedge [\exists c \in A \ / \ \ b\mathcal{S}c \wedge c\mathcal{R}a] \\
& \Rightarrow \quad (a\mathcal{S}b \ \wedge \ b\mathcal{S}c) \ \wedge \ (c\mathcal{R}a \ \wedge \ a\mathcal{R}b) \\
& \Rightarrow \quad a\mathcal{S}c \ \wedge \ c\mathcal{R}b \\
& \Rightarrow \quad a(\mathcal{R} \circ \mathcal{S})b
\end{aligned}
$$

17a. Considere la relación con gráfico es $G = \big\{(a, a), (a, b), (b, c), (c, b)\big\}$.

21a. Como $\mathcal{R} = (G, A, B)$ y $\mathcal{S} = (H, B, C)$, $\mathcal{S} \circ \mathcal{R} = (H \circ G, A, C)$:

$$
(\mathcal{S} \circ \mathcal{R})^{-1} = ((H \circ G)^{-1}, C, A) \tag{A.1}
$$

Además, como $\mathcal{S}^{-1} = (H^{-1}, C, B)$ y $\mathcal{R}^{-1} = (G^{-1}, B, A)$:

$$\mathcal{R}^{-1} \circ \mathcal{S}^{-1} = (G^{-1} \circ H^{-1}, C, A) \tag{A.2}$$

Como las relaciones en (A.1) y (A.2) tienen el mismo conjunto de salida y el mismo de llegada, basta ver que sus gráficos son iguales, es decir, basta probar que $(H \circ G)^{-1} = G^{-1} \circ H^{-1}$:

$$\begin{aligned} (c,a) \in (H \circ G)^{-1} &\Leftrightarrow (a,c) \in H \circ G \\ &\Leftrightarrow (\exists b \in B) \left[(a,b) \in G \ \wedge \ (b,c) \in H\right] \\ &\Leftrightarrow (\exists b \in B) \left[(c,b) \in H^{-1} \ \wedge \ (b,a) \in G^{-1}\right] \\ &\Leftrightarrow (c,a) \in G^{-1} \circ H^{-1} \end{aligned}$$

Con lo cual, ambas relaciones son iguales.

22b. $a \in D_{\mathcal{R}\cap\mathcal{S}} \Rightarrow (\exists b \in B)\ [a\mathcal{R} \cap \mathcal{S}b] \Rightarrow (\exists b \in B)\ [a\mathcal{R}b \wedge a\mathcal{S}b] \Rightarrow (a \in D_{\mathcal{R}} \ \wedge \ a \in D_{\mathcal{S}}) \Rightarrow a \in D_{\mathcal{R}} \cap D_{\mathcal{S}}$

22f. Se debe probar que $\forall b \left[b \in \mathcal{R}[A] - \mathcal{S}[A] \Rightarrow b \in (\mathcal{R} - \mathcal{S})[A]\right]$:

$$\begin{aligned} b \in \mathcal{R}[A] - \mathcal{S}[A] &\Rightarrow b \in \mathcal{R}[A] \ \wedge \ b \notin \mathcal{S}[A] \\ &\Rightarrow \left[\exists a \in A \ / \ \ a\mathcal{R}b\right] \ \wedge \ \left[\forall c \in A \ / \ \ c\not{\mathcal{S}}b\right] \\ &\Rightarrow a\mathcal{R}b \ \wedge \ a\not{\mathcal{S}}b \\ &\Rightarrow a(\mathcal{R} - \mathcal{S})b \\ &\Rightarrow b \in (\mathcal{R} - \mathcal{S})[A] \end{aligned}$$

Sección 3.4, página 201

1. $\dot{a} = \{a, b\}$, además, $A/\mathcal{R} = \left\{\dot{a}, \dot{c}, \dot{d}, \dot{f}\right\}$.

2. Si $A = \{1, 2, 3, 4\}$, las posibles matrices se relacionan con las posibles particiones de A. Asociada a la partición $\left\{\{1, 2\}, \{3, 4\}\right\}$ se tiene la matriz $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$. Las otras dos posibles matrices se obtienen de las particiones $\left\{\{1, 3\}, \{2, 4\}\right\}$ y $\left\{\{1, 4\}, \{2, 3\}\right\}$.

11. $\overset{\bullet}{(4,9)}= \{(2k, 3k+3) \ / \ \ k \in \mathbb{Z}\}$.

13. $G=\{(1,1),(1,4),(4,1),(4,4),(3,3),(3,5),(5,3),(5,5),(2,2),(6,6)\}$

15. La familia K sí es una partición de $\mathbb{R}$, pues $\bigcup\limits_{i\in\mathbb{Z}}[i, i{+}1[= \mathbb{R}$; además, son disjuntos dos a dos, pues $[n, n+1[\cap[m, m+1[= \varnothing$ si $n \neq m$.

16. La familia K no es una partición de $\mathbb{R}$, pues aunque sí se cumple $\bigcup\limits_{i\in\mathbb{Z}}[i, i+1[= \mathbb{R}$, los elementos de la familia no son disjuntos dos a dos; por ejemplo, $[1,3[\cap[2,4[= [2,3[\neq \varnothing$.

20b. $\overset{\bullet}{\frac{5}{3}}= \{\frac{k}{3} \ / \ \ k \in \mathbb{Z}\}$ y en $\overset{\bullet}{\frac{1}{2}}$, la clase de $\frac{1}{2}$, están los números racionales de la forma $\frac{k}{6}$ con $k \in \mathbb{Z}$, k impar.

21. Para comprobar que 11 es organizado, basta ver que los cuatro conjuntos $A_1 = \{1\}$, $A_2 = \{2,4\}$, $A_3 = \{3,6,7\}$ y $A_4 = \{5,8,9,10,11\}$ forman una partición de A, y además, $|A_1| = 1$, $|A_2| = 2$, $|A_3| = 3$ y $|A_4| = 5$. Ahora, para comprobar que 21 es organizado, observe que $21 = 1+2+3+7+8$.

Sección 3.5, página 211

2. $G = \{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3)(3,1),(2,3),(3,2)\}$.

Sección 4.1, página 226

5. Existen $6^4 = 1296$ funciones diferentes de A en B; además, existen $6 \cdot 5 \cdot 4 \cdot 3 = 360$ funciones inyectivas de A en B.

6. $f(\{a,c\}) = 2$, $f\big(\{\{a\},\{a,b\},\{b\}\}\big) = \{1,2\}$. Por otro lado, la imagen inversa del conjunto $\{2,4\}$ está formado por las preimágenes de 2 y de 4; así, $f^{-1}\big(\{2,4\}\big) = \big\{\{a,b\},\{a,c\},\{b,c\}\big\}$. No es inyectiva, pues el 2 tiene varias (tres) preimágenes; no es sobreyectiva, pues el elemento 4 no tiene preimagen.

8. $D_f = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$, el ámbito es $A_f = \{1,3,4\}$, su codominio es B. No es sobreyectiva, pues el codominio y ámbito no son iguales. No es inyectiva, pues $(1,2)$ y $(2,3)$ tienen como imagen a 1, es decir, el 1 tiene más de una preimagen. Por último, $f^{-1}\big(\{2\}\big) = \varnothing$, $f^{-1}\big(\{3\}\big) = \{(2,1),(3,1),(3,2)\}$.

11. Al calcular $E_2(45!) = 41$ y $E_5(45!) = 10$ y notando que para tener un cero final se necesita divisibilidad por $10 = 2 \cdot 5$. Se concluye que el número de ceros al final es 10.

12. (a). 5760 (b). 9801 (c). 58 176

13. $E_2(75!) = \left\lfloor \frac{75}{2} \right\rfloor + \left\lfloor \frac{75}{4} \right\rfloor + \left\lfloor \frac{75}{8} \right\rfloor + \left\lfloor \frac{75}{16} \right\rfloor + \left\lfloor \frac{75}{32} \right\rfloor + \left\lfloor \frac{75}{64} \right\rfloor = 37+18+9+4+2+1 = 71$.

14. (a). $p = 4$, $p = -1$ (b). $p = 2$, $p = -2$, $p = 1$.

17b. Sea $h(x) = f(x)g(x)$ con f y g impares, basta ver que $h(-x) = f(-x)g(-x) = (-f(x)) \cdot (-g(x)) = f(x)g(x) = h(x)$

18. Si la función f es par e impar a la vez, se debe cumplir que $f(x) = f(-x) = -f(x)$, de donde $f(x) = -f(x)$ y se obtiene que la función buscada es la función nula $f(x) = 0$ para todo x en el dominio que se tome.

20. $f\,([0,4]) = [1,3]$, $f^{-1}\,([0,4]) = [-1,+\infty[$.

22. $f\left(\left[\frac{1}{2},1\right[\right) = \{3\}$, $f^{-1}\left(\left[0,3\right[\right) = [-3,-2[$. Para las imágenes se evalúa: $f(-2) = 3$, $f(1) = 3$, $f(3) = 4$. La preimagen de -5 es -4, es decir, $f^{-1}(\{-5\}) = \{-4\}$. Por último, $f^{-1}\big(\{3\}\big) = \{-2\} \cup [0,2]$

23. La función $\chi_\varnothing$ corresponde a la función constante cero y χ_E a la función constante uno. Para probar las igualdades funcionales que se dan, en cada caso, analice los diferentes conjuntos disjuntos que forman el universo E. Por ejemplo, para verificar que la identidad

$\chi_{A\cup B}(x) = \chi_A(x)+\chi_B(x)-\chi_A(x)\cdot\chi_B(x)$ es verdadera, considere los siguientes cuatro casos: $x \in A \wedge x \in B$, $x \notin A \wedge x \in B$, $x \in A \wedge x \notin B$, $x \notin A \wedge x \notin B$, y verifique que en cada uno de ellos se cumple la igualdad. Por último, al utilizar las equivalencias anteriores, para $x \in E$ se obtiene que $\chi_{A\triangle B}(x) = \chi_A(x)+\chi_B(x)-2\chi_A(x)\chi_B(x)$.

24b. Se debe probar que $\forall b \left[b \in f(D\cap E) \Rightarrow b \in f(D)\cap f(E)\right]$:

$$\begin{aligned}
b \in f(D\cap E) \quad &\Rightarrow \quad \exists a \in D\cap E \ / \ f(a)=b \\
&\Rightarrow \quad a \in D \wedge a \in E \ / \ f(a)=b \\
&\Rightarrow \quad \left[a \in D \ / \ f(a)=b\right] \wedge \left[a \in E \ / \ f(a)=b\right] \\
&\Rightarrow \quad b \in f(D) \wedge b \in f(E) \\
&\Rightarrow \quad b \in f(D)\cap f(E)
\end{aligned}$$

24c. Asumiendo que f es inyectiva, se debe probar la igualdad $f(D\cap E) = f(D)\cap f(E)$, es decir, se deben probar ambas inclusiones. En el ejercicio 24b se probó la inclusión $f(D\cap E) \subseteq f(D)\cap f(E)$, solo faltaría probar la inclusión $f(D)\cap f(E) \subseteq f(D\cap E)$:

$$\begin{aligned}
& b \in f(D)\cap f(E) \\
\Rightarrow\ & b \in f(D) \wedge b \in f(E) \\
\Rightarrow\ & \left[\exists a \in D \ / \ f(a)=b\right] \wedge \left[\exists a' \in E \ / \ f(a')=b\right] \\
\Rightarrow\ & f(a) = f(a') \\
\Rightarrow\ & a = a' \\
\Rightarrow\ & a \in D \wedge a \in E \ / \ f(a)=b \\
\Rightarrow\ & a \in D\cap E \ / \ f(a)=b \\
\Rightarrow\ & b \in f(D\cap E)
\end{aligned}$$

Es interesante que se compare con el ejemplo 20.

24d. Se debe probar que $\forall b \left[b \in f(D) - f(E) \Rightarrow b \in f(D-E)\right]$:

$$\begin{aligned} b \in f(D) - f(E) &\Rightarrow b \in f(D) \ \wedge \ b \notin f(E) \\ &\Rightarrow \left[\exists a \in D \ / \ \ f(a) = b\right] \wedge \left[\forall x \in E \ / \ \ f(x) \neq b\right] \\ &\Rightarrow a \in (D-E) \ \wedge \ f(a) = b \\ &\Rightarrow b \in f(D-E) \end{aligned}$$

Sección 4.2, página 236

2. $f([2,5[) = \left]0, \frac{3}{2}\right]$, $f^{-1}([2,5[) =]-5, 1]$

3. Aproximadamente $4,9$ metros.

4. $f(x) = \frac{-3}{4}x^2 - \frac{3}{2}x + \frac{45}{4}$.

5. $f(x) = \frac{9}{25}x^2 - \frac{54}{25}x - \frac{144}{25}$

Sección 4.3, página 241

2. Si f es lineal, su criterio debe ser de la forma $f(x) = ax+b$. Como se debe cumplir que $f(f(x)) = a(ax+b)+b = a^2x+ab+b = 4x+1$, al igualar coeficientes se debe resolver el sistema de ecuaciones

$$\begin{cases} a^2 &= 4 \\ ab+b &= 1 \end{cases}$$

Para finalmente obtener las dos posibles funciones $f_1(x) = 2x + \frac{1}{3}$, $f_2(x) = -2x - 1$.

3. $f(x) = -2x + \frac{5}{3}$

5. $g(x) = \sqrt[3]{5-x}$

6. $f(x) = x^2 - 5x + 6$

9a. Podría ser $f(x) = x^4$, $g(x) = 2x+3$, cuya composición satisface lo pedido; sin embargo, g es lineal, por lo que se debe descartar. Se tienen muchas posibilidades, una que sí satisface lo pedido es, por ejemplo, $f(x) = x^2$, $g(x) = (2x+3)^2$.

9b. Observe que $4x^4 + 4x^2 + 1 = (2x^2+1)^2$, de esta forma, $f(x) = x^2$, $g(x) = 2x^2 + 1$ es una posibilidad; otra opción trivial es $f(x) = x+1$, $g(x) = 4x^4 + 4x^2$.

9d. Observe que se puede reescribir el criterio de h como:

$$h(x) = \frac{x+3}{x^2+2x} - 2x + 4 = \frac{(x+1)+2}{(x+1)^2-1} - 2(x+1) + 6$$

De esta manera, una posibilidad sería tomar $f(x) = \frac{x+2}{x^2-1} - 2x + 6$, $g(x) = x+1$.

10. (a). $]-\infty, 2] - \{-4, 1\}$ (c). $]-\infty, -2[\cup [-1, 3[$ (d). $[-3, 0] \cup [2, 3]$

11. El criterio de la suma es:

$$(f+g)(x) = \begin{cases} x^2 + 3x - 1 & \text{si } x \geq 2 \\ x^2 + 4 & \text{si } x < 2 \end{cases}$$

Y el criterio de la composición de f y g es:

$$(f \circ g)(x) = \begin{cases} -x^2 - x & \text{si } -1 < x < 0 \\ 2x^2 + 2x + 1 & \text{si } x \leq -1 \vee x \geq 0 \end{cases}$$

12. El criterio de la suma es:

$$(f+g)(x) = \begin{cases} x+3 & \text{si } x \leq 1 \\ -3x+3 & \text{si } 1 < x \leq 3 \\ -x-4 & \text{si } x > 3 \end{cases}$$

El de la composición es:

$$(f \circ g)(x) = \begin{cases} 2x-3 & \text{si } x < 1 \\ -2x+5 & \text{si } 1 \leq x \leq 3 \\ 2x-9 & \text{si } 3 < x \leq 6 \\ -2x+11 & \text{si } x > 6 \end{cases}$$

15b. Se debe probar que g es sobreyectiva, es decir, mostrar que todo c en C tiene preimagen por la función g, o sea, es necesario probar que existe x en B tal que $g(x) = c$. La prueba es:

$$c \in C \Rightarrow \exists k \in A \ / \ \ g \circ f(k) = c,$$

pues $g \circ f$ es sobre por hipótesis, es decir, $\exists k \in A \ / \ \ g(f(k)) = c$, basta tomar a x como $f(k)$, que claramente pertenece a B.

15c. Tomando como hipótesis que $g \circ f$ es inyectiva y f es sobreyectiva, se debe probar que g es inyectiva, es decir, mostrar que para a y b en B, si $g(a) = g(b)$, entonces $a = b$. Como f es sobreyectiva, existen x y y en A tales que $f(x) = a$ y $f(y) = b$, por lo que:

$$\begin{aligned} g(a) = g(b) \quad &\Rightarrow \quad g(f(x)) = g(f(y)) \\ &\Rightarrow \quad (g \circ f)(x) = (g \circ f)(y) \\ &\overset{\text{hip.}}{\Rightarrow} \quad x = y \\ &\Rightarrow \quad a = f(x) = f(y) = b \end{aligned}$$

Con lo cual se ha probado que g es inyectiva.

15d. Se debe probar que f es sobreyectiva, es decir, mostrar que todo b en B tiene preimagen por la función f. La prueba es:

$$\begin{aligned} b \in B \Rightarrow g(b) \in C \quad &\Rightarrow \quad \exists a \in A \ / \ \ g \circ f(a) = g(b) \\ &\Rightarrow \quad \exists a \in A \ / \ \ g(f(a)) = g(b) \\ &\Rightarrow \quad \exists a \in A \ / \ \ f(a) = b \end{aligned}$$

Analice en cuál paso de la demostración anterior se han utilizado las dos premisas o hipótesis y, por supuesto, observe que la primera implicación es posible por el hecho de que g es función.

Sección 4.4, página 249

2. Primero se calcula que $(f \circ f \circ f)(x) = -27x + 7$, luego, con el despeje usual, se calcula $(f \circ f \circ f)^{-1}(x) = \frac{7-x}{27}$.

3. $(g \circ f)^{-1}(x) = \frac{17-x}{18}$.

4. $(H^{-1} \circ G \circ H)(x) = \frac{15x-4}{9x}$, $(H \circ G^{-1})(x) = \frac{16x-4}{1-x}$.

6. $k = \frac{9}{2}$.

10. $f^{-1}(x) = \frac{7+6x}{3-9x}$, además, $(f \circ f)(x) = \frac{7+6x}{3-9x}$.

12. Note que f es una función cuadrática cuyo gráfico es una parábola con vértice en $(-2,-3)$. Si se toma el conjunto $[-2,+\infty[$ como dominio de f, f será inyectiva, y si se toma el conjunto $[-3,+\infty[$ como codominio de f, f será sobreyectiva; entonces, f es biyectiva. Por último, al despejar se obtiene que $f^{-1}(x) = \sqrt{x+3} - 2$.

13. $f^{-1}\colon]-\infty, 0[\cup[3,+\infty[\to \mathbb{R}$ con $f^{-1}(x) = \begin{cases} \frac{x-1}{2} & \text{si } x \geq 3 \\ x+1 & \text{si } x < 0 \end{cases}$

14. $f^{-1}(x) = \begin{cases} -\sqrt{1-x} & \text{si } x \leq 1 \\ x-1 & \text{si } x > 1 \end{cases}$, además, f y f^{-1} se intersecan solamente en el punto $\left(\frac{-1-\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}\right)$.

15. Para la inyectividad,

$$\begin{aligned} f(a) = f(b) \quad &\Rightarrow \quad \frac{a^2+1}{a} = \frac{b^2+1}{b} \\ &\Rightarrow \quad a^2b + b = ab^2 + a \\ &\Rightarrow \quad a^2b + b - ab^2 - a = 0 \\ &\Rightarrow \quad ab(a-b) - (a-b) = 0 \\ &\Rightarrow \quad (a-b)(ab-1) = 0 \\ &\Rightarrow \quad (a=b) \ \vee \ (a=b=1) \\ &\Rightarrow \quad a = b \end{aligned}$$

Para la sobreyectividad se debe probar que todo elemento b en $[2,+\infty[$ posee una preimagen a en $[1,+\infty[$, es decir, $f(a) = b$;

para ello, se logra despejar como sigue:

$$\begin{aligned}\frac{a^2+1}{a}=b \quad &\Leftrightarrow \quad a^2-ba+1=0\\ &\Leftrightarrow \quad \left(a-\frac{b}{2}\right)^2+1-\frac{b^2}{4}=0\\ &\Leftrightarrow \quad a-\frac{b}{2}=\sqrt{\frac{b^2}{4}-1}\Leftrightarrow a=\frac{b}{2}+\frac{\sqrt{b^2-4}}{2}\end{aligned}$$

Por último, la función inversa es $f^{-1}(x)=\frac{x+\sqrt{x^2-4}}{2}$.

19. Son $\mathcal{O}(1)=\{1,2\}$, $\mathcal{O}(3)=\{3,4,6\}$, $\mathcal{O}(5)=\{5,7,9\}$, $\mathcal{O}(8)=\{8\}$.

20. Para la inyectividad, $f_a(x)=f_a(y)\Rightarrow f(ax)=f(ay)\Rightarrow ax=ay\Rightarrow x=y$. Para la sobreyectividad, se debe probar que:

$$\forall y\in\mathbb{R}\ \exists x\in\mathbb{R}\ [f_a(x)=y]$$

Para probarlo, sea $y\in\mathbb{R}$, como f es sobreyectiva, se sabe que existe z tal que $f(z)=y$; por lo tanto, se garantiza que $f_a\left(\frac{z}{a}\right)=y$, con lo que basta tomar $x=\frac{z}{a}$ y se verifica que existe x, que es preimagen de y. Por último, considere $g(x)=\frac{1}{a}f^{-1}(x)$ y compruebe que $(f_a\circ g)(x)=x$ y $(g\circ f_a)(x)=x$, de donde se concluye que g es la inversa de f_a.

21a. Para iniciar, recuerde la definición de imagen inversa:

$$f^{-1}(F)=\{a\in A \ / \ \exists b\in F \ \text{ tal que } \ b=f(a)\}$$

Sustituyendo F por $f(D)$, se tiene:

$$f^{-1}(f(D))=\{a\in A \ / \ \exists b\in f(D) \ \text{ tal que } \ b=f(a)\}$$

Ahora, para demostrar que $D\subseteq f^{-1}(f(D))$, nos damos $a\in D$ y es necesario probar que $a\in f^{-1}(f(D))$. Como f es función, se tiene que $f(a)\in f(D)$, y tomando $b=f(a)$, se ve claramente que $\exists b\in f(D)$ tal que $b=f(a)$ es verdadera, con lo cual $a\in f^{-1}(f(D))$.

Sección 4.5, página 259

2. Obtenga la función lineal (que se puede probar es biyectiva) que pasa por los puntos $(2,4)$ y $(5,3)$.

Sección 4.6, página 263

1. Son 25 000 placas con la posibilidad de repetir, y 14 400 sin repetir.

2. Se utilizan las combinaciones y la regla del producto; de esta manera se tiene: $C(7,3) \cdot C(8,3) = 35 \cdot 56 = 1960$.

3. Para A hay $C(11,4) = 330$; para B se tienen $C(7,3) = 35$; para C son $C(4,2) = 6$ y para D solo $C(2,2) = 1$. Así, utilizando la regla del producto, se tienen $330 \cdot 35 \cdot 6 \cdot 1 = 69\,300$ formas de repartir estos regalos.

4. Basta observar que esta palabra tiene 9 letras, pero se tienen 3 repeticiones en la R, dos en la A, dos en la E. Se calcula $\frac{9!}{3!\,2!\,2!} = 15\,120$ y se concluye que son 15 120 las posibles palabras.

5. (a) 210 (b) 90 (c) 5040.

6. 255.

8. (a) 1250 (b) 1800 (c) 50.

9. (a) 1680 (b) 280.

11. (a) 81 (b) 60 (c) 120 (d) 5^{24}.

Sección 5.1, página 274

1. (1f) $\displaystyle\sum_{i=2}^{10}(i - i^3)$ (1g) $\displaystyle\prod_{i=2}^{11}\sum_{j=1}^{i} i^2$

2. (a) 131 (c) $-105\,600$ (e) $\frac{2552}{45}$ (f) 370.

Sección 5.2, página 287

1f. Para el paso inductivo, observe que:

$$\begin{aligned}
1^2+2^2+\cdots+n^2+(n+1)^2 &\overset{H.I.}{=} \frac{n(n+1)(2n+1)}{6}+(n+1)^2\\
&= \frac{n(n+1)(2n+1)+6(n+1)^2}{6}\\
&= \frac{(n+1)(2n^2+7n+6)}{6}\\
&= \frac{(n+1)(n+2)(2n+3)}{6}
\end{aligned}$$

1m. Para el paso inductivo, observe que:

$$\begin{aligned}
\frac{1}{1\cdot 3}+\cdots+\frac{1}{(2n+1)(2n+3)} &\overset{H.I.}{=} \frac{n}{2n+1}+\frac{1}{(2n+1)(2n+3)}\\
&= \frac{2n^2+3n+1}{(2n+1)(2n+3)}=\frac{n+1}{2n+3}
\end{aligned}$$

1s. Para el paso inductivo, observe que:

$$\begin{aligned}
\sum_{i=1}^{n+1} i(i!) &= \sum_{i=1}^{n} i(i!)+(n+1)(n+1)!\\
&\overset{H.I.}{=} (n+1)!-1+(n+1)(n+1)!\\
&= (n+1)!(n+2)-1\\
&= (n+2)!-1
\end{aligned}$$

2b. Para el paso inductivo y utilizando la distributividad, se cumple:

$$\begin{aligned}
(n+1)(n+2)(n+3) &= n(n+1)(n+2)+3(n+1)(n+2)\\
&\overset{H.I.}{=} 6k+3\cdot 2k'\\
&= 6(k+k')=6k''
\end{aligned}$$

Para lo anterior, observe que dados dos números consecutivos $n+1$ y $n+2$, mayores que 2, uno de ellos es par.

2d. Para $n = 1$ es válido, pues $1^7 - 1 = 1 - 1 = 0$, y 0 es divisible por 7. Se asume que existe $k \in \mathbb{Z}$ tal que $n^7 - n = 7k$. Para el paso inductivo, observe que:

$$\begin{aligned}
& (n+1)^7 - (n+1) \\
= \quad & n^7 + 7n^6 + 21n^5 + 35n^4 + 35n^3 + 21n^2 + 7n + 1 - n - 1 \\
= \quad & n^7 - n + 7(n^6 + 3n^5 + 5n^4 + 5n^3 + 3n^2 + n) \\
\overset{H.I.}{=} \quad & 7k + 7k' \\
= \quad & 7k''
\end{aligned}$$

2g. Para $n = 1$ es válido, pues $3^1 + 7^1 - 2 = 8$, y 8 es divisible por 8. Se asume que existe $k \in \mathbb{Z}$ tal que $3^n + 7^n - 2 = 8k$, es decir, $3^n = 8k - 7^n + 2$. Se prueba la validez de la proposición para $n+1$:

$$\begin{aligned}
3^{n+1} + 7^{n+1} - 2 &= 3 \cdot 3^n + 7 \cdot 7^n - 2 \\
&\overset{H.I.}{=} 3(8k - 7^n + 2) + 7 \cdot 7^n - 2 \\
&= 24k - 3 \cdot 7^n + 6 + 7 \cdot 7^n - 2 \\
&= 24k + 4(7^n + 1)
\end{aligned}$$

Ahora, note que 7^n será impar para todo n natural; así, $7^n + 1$ será par y se tiene que $24k + 4(7^n + 1) = 24k + 4 \cdot (2k') = 8(3k + k') = 8k''$.

3j. Para $n = 1$ es válido, pues $2 \leq 2$ es cierto. Se asume la validez para n, es decir, que $\dfrac{4^n}{n+1} \leq \dfrac{(2n)!}{(n!)^2}$. Para el paso inductivo se debe probar que:

$$\frac{4^{n+1}}{n+2} \leq \frac{(2n+2)!}{((n+1)!)^2}$$

Para ello, observe que:

$$\frac{(2n+2)!}{((n+1)!)^2} = \frac{(2n+2)(2n+1)(2n)!}{(n!)^2(n+1)^2} \overset{H.I.}{\geq} \frac{4^n}{n+1} \frac{(2n+2)(2n+1)}{(n+1)^2}$$

Así, basta verificar que se cumple que $\frac{4^n}{n+1} \frac{(2n+2)(2n+1)}{(n+1)^2} \geq \frac{4^{n+1}}{n+2}$ y el resultado se concluye aplicando la transitividad.

6. La fórmula es $\displaystyle\sum_{i=1}^{n} 2i = n(n+1)$.

8. La fórmula es $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

9a. Observe que $1{\cdot}2+2{\cdot}3+\cdots+(n-1)n = \displaystyle\sum_{i=1}^{n-1} i(i+1) = \sum_{i=1}^{n-1} i^2 + \sum_{i=1}^{n-1} i = \frac{(n-1)n(2n-1)}{6} + \frac{(n-1)n}{2} = \frac{(n-1)n(n+1)}{3}$

10. (a) 338 350 (ver ejercicio 1f con $n = 100$); (b) $\frac{16}{33}$ (ver ejercicio 1m con $n = 16$); (c) 9920 (ver ejercicio 9a); (d) 76 176 (ver ejercicio 1g); (e) $\frac{3}{16}\left(\frac{7^{20}-1}{7^{20}}\right)$; (f) ver ejercicio 1t, así, la suma es $\frac{100}{401} - \frac{4}{17} = \frac{96}{6817}$.

11b. $S = \frac{1+2+3+\cdots+n^2}{n} = \frac{\frac{n^2(n^2+1)}{2}}{n} = \frac{n(n^2+1)}{2}$.

12a. Observe que:

$$\begin{aligned} a_n &= \sum_{i=1}^{n} a_i - \sum_{i=1}^{n-1} a_i \\ &= \frac{n^2+3n}{2} - \frac{(n-1)^2+3(n-1)}{2} \\ &= \frac{n^2+3n-n^2+2n-1-3n+3}{2} \\ &= \frac{2n+2}{2} = n+1 \end{aligned}$$

Por lo que $a_i = i + 1$.

12b. $a_i = i^2 - i + 1$

13. Análogo al ejemplo 27, se obtiene la ecuación:

$$(n+1)^5 = 1 + 5S_4 + 10S_3 + 10S_2 + 5S_1 + n$$

Al sustituir las fórmulas conocidas para S_1, S_2, S_3, despejar y simplificar, se obtiene:

$$S_4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

15. $S_n = \dfrac{8n^3 - 8n + 3}{3}$

18. Sea $P(x) = 1 + x + x^2 + \cdots + x^{100}$ y $D(x) = x^2 - x - 2$. Es claro que el grado del residuo debe ser menor que el grado del divisor, y como el grado del divisor $D(x)$ es dos, se tiene que el grado del residuo es 1, es decir, $R(x) = ax + b$. Así, existe un polinomio $Q(x)$ tal que:

$$P(x) = Q(x)(x^2 - x - 2) + (ax + b)$$

Al evaluar en $x = -1$ se obtiene la ecuación $1 = -a + b$; al evaluar en $x = 2$ y utilizar la fórmula del ejercicio 1k, se obtiene la ecuación $2^{101} - 1 = 2a + b$. Al resolver el sistema de dos ecuaciones lineales con dos incógnitas, se obtienen los valores exactos de a y b, para finalmente concluir que $R(x) = \left(\frac{2^{101}-2}{3}\right)x + \frac{2^{101}+1}{3}$.

19. Se procederá por inducción sobre la cardinalidad n del conjunto. En primer lugar, si $|A| = 0$, se tiene que $A = \varnothing$, $P(A) = \{\varnothing\}$; así, se tiene que $|P(A)| = 1 = 2^0$ y el resultado se cumple.
Asuma que el resultado es válido para n, es decir, si $|A| = n$, entonces $|P(A)| = 2^n$. Para el paso inductivo, sea B un conjunto tal que $|B| = n + 1$, tome un elemento arbitrario x de A.
Es claro que todos los subconjuntos de B se pueden separar en dos clases disjuntas: los que contienen a x y los que no la contienen. Los que no la contienen resultan ser los subconjuntos de $B - \{x\}$, es decir, los elementos de $P(B - \{x\})$, pero como $B - \{x\}$ tiene n elementos, por H.I. se concluye que la cantidad de conjuntos que no contienen a x es 2^n.

Por otro lado, se debe determinar la cantidad de conjuntos que contienen a x, pero resulta evidente que cada conjunto que lo contiene se puede descomponer como uno que no lo contiene unido con $\{x\}$, es decir, la cantidad de conjuntos que lo contienen es 2^n. Por lo tanto, $|P(B)| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

Sección 5.3, página 304

2a. $a_n = \frac{1}{7} \cdot 6^n + \frac{13}{7} \cdot (-1)^n$ para $n \geq 0$.

3b. $b_n = 2 \cdot 3^n + (-2)^n + 3n(-2)^n$ para $n \geq 0$.

3c. $U_n = 2 \cdot (-1)^n + n(-1)^n + 3 \cdot 2^n$ para $n \geq 0$.

3e. $a_n = 1 - 2(-1)^n + 3 \cdot 2^n$ para $n \geq 0$.

3f. $a_n = 2 + 3n + 4(-1)^n$ para $n \geq 0$.

3g. $b_n = 3 \cdot 2^n + n2^n - 4n^2 2^n$ para $n \geq 1$.

4a. $a_n = 2^n - n2^n + n^2 2^n + (-1)^n$ para $n \geq 0$.

4b. $a_n = 2(-1)^n + n(-1)^n + 2(-3)^n - n(-3)^n$ para $n \geq 0$.

5a. El término $(-3)^n$ induce la raíz $x = -3$, pero además está repetida, pues aparece el término $n(-3)^n$; así, la ecuación característica es $(x+3)^2 = x^2 + 6x + 9 = 0$ y se obtiene $U_n = -6a_{n-1} - 9a_{n-2}$, con $U_1 = 9$, $U_2 = -72$.

5b. $a_n = -a_{n-1} + 2a_{n-2}$ con $a_0 = 6$, $a_1 = 3$.

5d. $a_n = 8a_{n-1} - 25a_{n-2} + 38a_{n-3} - 28a_{n-4} + 8a_{n-5}$ si $n \geq 5$, $a_0 = 4$, $a_1 = 12$, $a_2 = 43$, $a_3 = 144$, $a_4 = 441$.

6. $a_n = -3 \cdot 2^n + 2 \cdot 3^n$, $a_4 = 114$, $a_7 = 3990$.

8. La ecuación asociada es $x^2 - x - 1 = 0$, cuyas dos soluciones son $S_1 = \frac{1+\sqrt{5}}{2}$ y $S_2 = \frac{1-\sqrt{5}}{2}$. Utilizando las condiciones dadas y resolviendo el sistema de ecuaciones se verifica lo pedido.

9. Es claro que $F_5 = 5$ y es impar, $F_{12} = 144$ y es par. Para clasificar F_{4311} no es conveniente calcularlo, pues es bastante el cálculo; sin embargo, se observa que los ciclos de repetición son F_1 impar, F_2 impar, F_3 par, F_4 impar, F_5 impar, F_6 par.... Así, aparece un F_n par cada vez que $n = 3k$, y como $4311 = 3 \cdot 1437$, se concluye que F_{4311} es par.

14. Se puede despejar de varias maneras, para obtener, por ejemplo: $x = \sqrt[5]{8 - 2x^3}$, $x = \sqrt[3]{\frac{8-x^5}{2}}$ o $x = \frac{8}{x^4+2x^2}$. Con cualquier función, la solución con 5 decimales axactos es $1,29559$.

15a. La solución exacta es $1,51598022769$.

15b. La solución exacta es $1,29559774252$.

Sección 6.1, página 317

3. El elemento 1 es el elemento neutro. El elemento 0 es el elemento absorbente por la izquierda, no tiene absorbente por la derecha; por lo tanto, la estructura no tiene elemento absorbente. La estructura no es conmutativa, pues $5 * 7 = 5 \neq 1 = 7 * 5$. Tampoco es asociativa, pues $(5 * 7) * 5 = 5 * 5 = 0$, mientras que $5 * (7 * 5) = 5 * 1 = 5$, es decir, $(5 * 7) * 5 \neq 5 * (7 * 5)$.

4b. El neutro es $\frac{1}{5}$; los involutivos son $\frac{-1}{5}$ y $\frac{1}{5}$ y el idempotente es $\frac{1}{5}$.

6. Los únicos elementos centrales son b y d, pues se puede verificar que tanto b como d conmutan con todos los elementos de $\mathcal{E}$. Por lo tanto, se concluye que $C(\mathcal{E}) = \{b, d\}$.

7. Es claro que si a, $b \in [0, +\infty[$, $a * b = \sqrt{a^2 + b^2} \in [0, +\infty[$, con lo que la operación es cerrada. Si a, b, $c \in [0, +\infty[$ se cumple que:

$$\begin{aligned} a * (b * c) &= a * \sqrt{b^2 + c^2} \\ &= \sqrt{a^2 + \left(\sqrt{b^2 + c^2}\right)^2} = \sqrt{a^2 + b^2 + c^2} \end{aligned}$$

Análogamente, $(a*b)*c = \sqrt{a^2+b^2+c^2}$ y se cumple que $a*(b*c) = (a*b)*c$, es decir, la asociatividad. Para la conmutatividad basta ver que $a*b = \sqrt{a^2+b^2} = \sqrt{b^2+a^2} = b*a$; por último, el neutro es el 0, pues $a*0 = \sqrt{a^2+0^2} = \sqrt{a^2} = |a| = a$.

10. Se debe resolver $a\perp(b\perp c) = (a\perp b)\perp c$, para ello se calcula:

$$\begin{aligned} & a\perp(b\perp c) = a\perp(bc+kb+kc+42) \\ = \quad & a(bc+kb+kc+42)+ka+k(bc+kb+kc+42)+42 \end{aligned}$$

Análogamente se calcula $(a\perp b)\perp c = abc+kac+kbc+42c+kab+k^2a+k^2b+42k+kc+42$. Al igualar ambas expresiones y factorizar, se obtiene la ecuación $(a-c)(k^2-k-42) = 0$; al resolverla, se obtiene que los posibles valores son $k=7$ o $k=-6$.

13. Analice el ejemplo 12 de la página 314. La tabla se construye de forma análoga y es claro que es conmutativa y que $\varnothing$ es el elemento neutro; además, cada elemento es su propio inverso; por ejemplo, $\{b,c\}^{-1} = \{b,c\}$, pues $\{b,c\} \bigtriangleup \{b,c\} = \varnothing$.

Sección 6.2, página 328

2. Para probar que $(\mathbb{R},*)$ es un grupo abeliano, compare con el ejemplo 19. Se debe notar que en esta operación se tiene que $e=4$, además $a^{-1} = 8-a$; de esta manera se obtiene que:

$$\begin{aligned} 3^3 * \left[7 * \left(2 * \frac{1}{4}\right)^{-2}\right]^4 &= 1 * \left[7 * \left(\frac{-7}{4}\right)^{-2}\right]^4 \\ &= 1 * \left[7 * \frac{31}{2}\right]^4 \\ &= 1 * \left[\frac{37}{2}\right]^4 = 1*62 = 59 \end{aligned}$$

3. Para probar que $(\mathbb{R}^*,*)$ es un grupo abeliano, compare con el ejemplo 19. Se debe notar que en esta operación se tiene que

$e = \frac{1}{4}$, además $a^{-1} = \frac{1}{16a}$; al efectuar los respectivos cálculos, se obtiene que: $3^3 * \left[7 * \left(2 * \frac{1}{4}\right)^{-2}\right]^4 = \frac{64\,827}{4096}$.

4. Para probar que $(\mathbb{R} \times \mathbb{R}^*, \otimes)$ es un grupo abeliano, compare con el ejemplo 20. Concluya que $e = (4, \frac{1}{2})$ es el elemento neutro y $(a, b)^{-1} = (8 - a, \frac{1}{4b})$ es el inverso de (a, b). Por último:

$$\begin{aligned}(2,-1)^3 \otimes \left[\left(0, \frac{1}{3}\right) \otimes (1,-1)^{-1}\right]^2 &= (-2,-4) \otimes \left[\left(3, \frac{-1}{6}\right)\right]^2 \\ &= (-2,-4) \otimes \left(2, \frac{1}{18}\right) \\ &= \left(-4, \frac{-4}{9}\right)\end{aligned}$$

5. $\left(18, \frac{5}{192}\right)$

7. A partir de la siguiente tabla de operación, se observa que $e = \dot{1}$, los inversos son $\left(\dot{1}\right)^{-1} = \dot{1}$, $\left(\dot{2}\right)^{-1} = \dot{4}$, $\left(\dot{3}\right)^{-1} = \dot{5}$, $\left(\dot{4}\right)^{-1} = \dot{2}$, $\left(\dot{5}\right)^{-1} = \dot{3}$ y $\left(\dot{6}\right)^{-1} = \dot{6}$.

$\odot$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{2}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{1}$	$\dot{3}$	$\dot{5}$
$\dot{3}$	$\dot{3}$	$\dot{6}$	$\dot{2}$	$\dot{5}$	$\dot{1}$	$\dot{4}$
$\dot{4}$	$\dot{4}$	$\dot{1}$	$\dot{5}$	$\dot{2}$	$\dot{6}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{3}$	$\dot{1}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{6}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Es claro que $\left(\dot{3}\right)^4 = \dot{4}$ y $\left(\dot{3}\right)^{-4} = \dot{2}$. Por último, utilizando las reglas de potencias, se calcula $\left(\dot{2}\right)^{-409} = \left(\dot{2}^3\right)^{-137} \odot \left(\dot{2}\right)^2 = \dot{4}$.

8. A partir de la tabla de operación, se tiene que $e = \dot{1}$; además, $\left(\dot{1}\right)^{-1} = \dot{1}$, $\left(\dot{2}\right)^{-1} = \dot{6}$, $\left(\dot{3}\right)^{-1} = \dot{4}$, $\left(\dot{4}\right)^{-1} = \dot{3}$, $\left(\dot{5}\right)^{-1} = \dot{9}$, $\left(\dot{6}\right)^{-1} = \dot{2}$, $\left(\dot{7}\right)^{-1} = \dot{8}$, $\left(\dot{8}\right)^{-1} = \dot{7}$, $\left(\dot{9}\right)^{-1} = \dot{5}$, $\left(\dot{10}\right)^{-1} = \dot{10}$.

   El resultado exacto de la parte 8c) es $\dot{6}$.

9. Es claro que la operación es cerrada. Si a, b, $c \in \mathbb{R}$, se cumple que $a * (b * c) = a * \sqrt[3]{b^3 + c^3} = \sqrt[3]{a^3 + \left(\sqrt[3]{b^3 + c^3}\right)^3} = \sqrt[3]{a^3 + b^3 + c^3}$ análogamente $(a*b)*c = \sqrt[3]{a^3 + b^3 + c^3}$ y se cumple que $a*(b*c) = (a*b)*c$, es decir, la asociatividad. Para la conmutatividad basta ver que $a * b = \sqrt[3]{a^3 + b^3} = \sqrt[3]{b^3 + a^3} = b * a$. El neutro es el 0, pues $a * 0 = \sqrt[3]{a^3 + 0^3} = \sqrt[3]{a^3} = a$. Por último, para b el inverso de a se requiere que $a * b = 0 \Leftrightarrow \sqrt[3]{a^3 + b^3} = 0 \Leftrightarrow b = -a$, con lo cual, el inverso existe siempre y es $a^{-1} = -a$.

10c. Es un monoide conmutativo.

10d. Si a, b, $c \in \mathbb{R} - \{-1\}$, se cumple que $a * (b * c) = a * (b + c + bc) = a+b+c+bc+a(b+c+bc) = a+b+c+ab+ac+bc+abc$ análogamente $(a*b)*c = a+b+c+ab+ac+bc+abc$ y se cumple que $a*(b*c) = (a*b)*c$ por lo que es asociativa. Para el neutro e se requiere que $a * e = a \Leftrightarrow a + e + ae = a \Leftrightarrow e(1 + a) = 0 \Leftrightarrow e = 0 \vee a = -1$, pero $a \neq -1$, por lo que el neutro es $e = 0$. Fácilmente se comprueba que es conmutativa. Por último, para b el inverso de a se requiere que $a * b = 0 \Leftrightarrow a + b + ab = 0 \Leftrightarrow b(1 + a) = -a \Leftrightarrow b = \frac{-a}{1+a}$, así, $a^{-1} = \frac{-a}{1+a}$. Por lo anterior, la estructura es un grupo abeliano.

10i. Es un grupo abeliano con $e = (-3, \frac{1}{4})$ como elemento neutro y $(a, b)^{-1} = (-6 - a, \frac{1}{16b})$ como el inverso de (a, b).

10j. Es un grupo abeliano con $e = (0, -2)$ como elemento neutro y $(a, b)^{-1} = \left(\frac{-a}{1+a}, -4 - b\right)$ como el inverso de (a, b).

13a. Es un monoide conmutativo.

14. El único elemento que falta en la tercera fila es b; así, $a{*}a = b$. Con este, el único elemento que falta en la tercera columna es d; así, $c{*}a = d$. Por otro lado, $c{*}d = a$ y $c{*}a = d$. Así, sustituyendo, se tiene que $c{*}c{*}a = a$, con lo cual, $c{*}c = e$. Con estos datos, se debe cumplir que $c * b = b \vee c * b = f$, pero es imposible que $c * b = b$ sea verdadero, pues esto implicaría que $c = e$; por lo tanto, se debe cumplir $c * b = f$ (observe cómo se utilizó el silogismo disyuntivo). Continuando con razonamientos análogos, se obtiene:

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

16. Para la cerradura, basta ver que para a, b, c, d números racionales se cumple $\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right) = (ac+2bd)+(bc+ad)\sqrt{2}$, donde $ac + 2bd$, $bc + ad$ son racionales. Es claro que la asociatividad y conmutatividad se cumplen, pues son números reales. El elemento neutro es $1 = 1 + 0\sqrt{2}$. Para los inversos, se debe cumplir que:

$$\begin{aligned}
\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right) = 1 \quad &\Leftrightarrow \quad (ac+2bd)+(bc+ad)\sqrt{2} = 1 \\
&\Leftrightarrow \quad ac+2bd = 1 \ \wedge \ bc+ad = 0 \\
&\Leftrightarrow \quad c = \frac{a}{a^2-2b^2} \ \wedge \ d = \frac{b}{2b^2-a^2}
\end{aligned}$$

Por lo tanto, $\left(a+b\sqrt{2}\right)^{-1} = \frac{a}{a^2-2b^2} + \frac{b}{2b^2-a^2}\sqrt{2}$.

17. Es claro que es cerrado, pues la composición de funciones biyectivas es biyectiva (ver ejercicio 14 de la sección 4.1). Para verificar la asociatividad, se debe probar que dadas f, g, h en $\mathcal{G}$ se satisface

$(f \circ g) \circ h = f \circ (g \circ h)$. Por supuesto, lo anterior debería ser cierto para todo $x \in A$; su prueba es:

$$\begin{aligned} & \big((f \circ g) \circ h\big)(x) = \big(f \circ (g \circ h)\big)(x) \\ \Leftrightarrow \quad & (f \circ g)\big(h(x)\big) = f\big((g \circ h)(x)\big) \\ \Leftrightarrow \quad & f\big(g(h(x))\big) = f\big(g(h(x))\big) \end{aligned}$$

El elemento neutro es la función identidad. Si $f \in \mathcal{G}$ es biyectiva y por lo tanto existe f^{-1}, también se sabe que la composición de funciones no es conmutativa.

19. La tabla de operación es:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

De aquí se observa que el elemento neutro es $e = f_1$; además, los elementos inversos son $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_5$, $f_5^{-1} = f_4$, $f_6^{-1} = f_6$.

Sección 6.3, página 335

1. Un generador es $\dot{3}$, ya que $(\dot{3})^1 = \dot{3}$, $(\dot{3})^2 = \dot{2}$, $(\dot{3})^3 = \dot{6}$, $(\dot{3})^4 = \dot{4}$, $(\dot{3})^5 = \dot{5}$, $(\dot{3})^6 = \dot{1}$. Note que $\dot{5}$, el inverso de $\dot{3}$, también genera.

2. Tome $\beta = 6$ y compruébelo.

3. $U_9 = \left\{\dot{1}, \dot{2}, \dot{4}, \dot{5}, \dot{7}, \dot{8}\right\}$ es un grupo de orden 6. Como cada elemento se puede expresar como una potencia de $\dot{2}$, esto comprobaría que es un grupo cíclico generado por $\dot{2}$. El otro posible generador es solamente $\dot{5}$.

7. El elemento neutro es e, cada elemento del grupo es su propio inverso.

Sección 6.4, página 340

1. A partir del ejercicio 7 de la sección anterior, y como el orden de $\mathbb{Z}_7^*$ es 6, del Teorema de Lagrange se sabe que el orden de sus subgrupos puede ser 1, 2, 3 o 6. Así, de orden 1 es $\left\{\overset{\bullet}{1}\right\}$; de orden 2 es $\left\{\overset{\bullet}{1},\overset{\bullet}{6}\right\}$; de orden 3 es $\left\{\overset{\bullet}{1},\overset{\bullet}{2},\overset{\bullet}{4}\right\}$; de orden 6 es $\mathbb{Z}_7^*$.

2. A partir de la siguiente tabla se tiene que $e = \overset{\bullet}{0}$, $\left(\overset{\bullet}{0}\right)^{-1} = \overset{\bullet}{0}$, $\left(\overset{\bullet}{1}\right)^{-1} = \overset{\bullet}{5}$, $\left(\overset{\bullet}{2}\right)^{-1} = \overset{\bullet}{4}$, $\left(\overset{\bullet}{3}\right)^{-1} = \overset{\bullet}{3}$, $\left(\overset{\bullet}{4}\right)^{-1} = \overset{\bullet}{2}$, $\left(\overset{\bullet}{5}\right)^{-1} = \overset{\bullet}{1}$.

$\oplus$	$\overset{\bullet}{0}$	$\overset{\bullet}{1}$	$\overset{\bullet}{2}$	$\overset{\bullet}{3}$	$\overset{\bullet}{4}$	$\overset{\bullet}{5}$
$\overset{\bullet}{0}$	$\overset{\bullet}{0}$	$\overset{\bullet}{1}$	$\overset{\bullet}{2}$	$\overset{\bullet}{3}$	$\overset{\bullet}{4}$	$\overset{\bullet}{5}$
$\overset{\bullet}{1}$	$\overset{\bullet}{1}$	$\overset{\bullet}{2}$	$\overset{\bullet}{3}$	$\overset{\bullet}{4}$	$\overset{\bullet}{5}$	$\overset{\bullet}{0}$
$\overset{\bullet}{2}$	$\overset{\bullet}{2}$	$\overset{\bullet}{3}$	$\overset{\bullet}{4}$	$\overset{\bullet}{5}$	$\overset{\bullet}{0}$	$\overset{\bullet}{1}$
$\overset{\bullet}{3}$	$\overset{\bullet}{3}$	$\overset{\bullet}{4}$	$\overset{\bullet}{5}$	$\overset{\bullet}{0}$	$\overset{\bullet}{1}$	$\overset{\bullet}{2}$
$\overset{\bullet}{4}$	$\overset{\bullet}{4}$	$\overset{\bullet}{5}$	$\overset{\bullet}{0}$	$\overset{\bullet}{1}$	$\overset{\bullet}{2}$	$\overset{\bullet}{3}$
$\overset{\bullet}{5}$	$\overset{\bullet}{5}$	$\overset{\bullet}{0}$	$\overset{\bullet}{1}$	$\overset{\bullet}{2}$	$\overset{\bullet}{3}$	$\overset{\bullet}{4}$

El orden de $\mathbb{Z}_6$ es 6. Del Teorema de Lagrange se sabe que el orden del subgrupo puede ser 1, 2, 3 o 6. Así, de orden 1 es $\left\{\overset{\bullet}{0}\right\}$; de orden 2 es $\left\{\overset{\bullet}{0},\overset{\bullet}{3}\right\}$; de orden 3 es $\left\{\overset{\bullet}{0},\overset{\bullet}{2},\overset{\bullet}{4}\right\}$; de orden 6 es $\mathbb{Z}_6$.

3. El orden de $\mathbb{Z}_{11}^*$ es 10. Del Teorema de Lagrange se sabe que el orden del subgrupo puede ser 1, 2, 5 o 10. Así, de orden 1, el subgrupo es $\left\{\overset{\bullet}{1}\right\}$; de orden 2 es $\left\{\overset{\bullet}{1},\overset{\bullet}{10}\right\}$; de orden 5 es solamente $\left\{\overset{\bullet}{1},\overset{\bullet}{3},\overset{\bullet}{4},\overset{\bullet}{5},\overset{\bullet}{9}\right\}$; de orden 11 es $\mathbb{Z}_{11}^*$.

4. El orden de $\mathbb{Z}_{12}$ es 12; así, el orden de los subgrupos puede ser 1, 2, 3, 4, 6 o 12. Todos los subgrupos son: $\left\{\overset{\bullet}{0}\right\}$ de orden 1 , $\left\{\overset{\bullet}{0}, \overset{\bullet}{6}\right\}$ de orden 2 , $\left\{\overset{\bullet}{0}, \overset{\bullet}{4}, \overset{\bullet}{8}\right\}$ de orden 3 , $\left\{\overset{\bullet}{0}, \overset{\bullet}{3}, \overset{\bullet}{6}, \overset{\bullet}{9}\right\}$ de orden 4 , $\left\{\overset{\bullet}{0}, \overset{\bullet}{2}, \overset{\bullet}{4}, \overset{\bullet}{6}, \overset{\bullet}{8}, \overset{\bullet}{10}\right\}$ de orden 6 y $\mathbb{Z}_{12}$ de orden 12 .

8. Repase la solución del ejemplo 40 y el ejercicio 13 de la sección 6.1 (página 319), para así obtener los subgrupos de orden 1, 2, 4 y 8.

17. Como $o(\mathcal{G}) = 6$, los posibles subgrupos podrán tener orden 1, 2, 3 y 6. Así, observando la tabla y los inversos dados en la solución del ejercicio 19 (página 331), se tiene que el subgrupo de orden 1 es $\{f_1\}$; de orden 2 son $\{f_1, f_2\}$, $\{f_1, f_3\}$, $\{f_1, f_6\}$; de orden 3 es $\{f_1, f_4, f_5\}$ y de orden 6 es $\mathcal{G}$.

18. Los subgrupos: de orden 1 es $\{e\}$; de orden 2 son $\{e, r\}$, $\{e, h\}$, $\{e, v\}$ y de orden 4 es $\{r, h, v, e\}$.

19. Es claro que la relación $\mathcal{R}$ sobre el grupo $\mathcal{G}$ es reflexiva, pues dado $a \in \mathcal{G}$ se cumple que $a * a^{-1} = e$ y $e \in \mathcal{H}$ por ser subgrupo; así, $a\mathcal{R}a$. Para verificar que es reflexiva, si $a\mathcal{R}b$, entonces $a * b^{-1} \in \mathcal{H}$, pero por ser subgrupo, su inverso estará también; así, $\left(a * b^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1} * a^{-1} = b * a^{-1} \in \mathcal{H}$, y esto dice que $b\mathcal{R}a$. La transitividad es sencilla, dado que si $a\mathcal{R}b$ y $b\mathcal{R}c$, se tiene que $a * b^{-1} \in \mathcal{H}$ y $b * c^{-1} \in \mathcal{H}$. Al operar ambos elementos, y dado que $\mathcal{H}$ es subgrupo, se tiene que $\left(a * b^{-1}\right) * \left(b * c^{-1}\right) = a * c^{-1} \in \mathcal{H}$, que prueba $a\mathcal{R}c$.

Sección 6.5, página 349

1. Basta ver que se cumple $f(a + b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b)$.

5. Para $\varphi(n + m)$, basta analizar los posibles 4 casos si n y m son pares o impares.

10. Para probar que $(\mathbb{R}, *)$ es un grupo vea la solución del ejercicio 9 de la sección 6.2 dada en la página 430. Para probar que son isomorfos, se debe definir una función que sea un isomorfismo, para ello, defina $\phi\colon (\mathbb{R}, *) \to (\mathbb{R}, +)$ como $\phi(x) = x^3$; así, se tiene que:
$$\phi(x * y) = \phi(\sqrt[3]{x^3 + y^3}) = x^3 + y^3 = \phi(x) + \phi(y)$$
Para la biyección, note que $N_\phi = \{0\}$, y además, $y = \sqrt[3]{x}$ es una preimagen de x, con lo que ϕ es un isomorfismo.

15. ϕ es endomorfismo, pues $\phi([a][b]) = \phi([ab]) = [ab]^2 = [a][b][a][b] = [abab] = [a^2][b^2] = [a]^2[b]^2 = \phi([a])\phi([b])$. Para ver cuál es su núcleo, note que $a \in N_\phi$ si cumple $[1] = \phi(a) = [a]^2 = [a^2]$, es decir $a^2 \equiv 1 \bmod 9 \Rightarrow a = 1$ o $a = 8$; así, $N_\phi = \{[1], [8]\}$. De esto es posible concluir que ϕ no es inyectiva. Por último, $Im(\phi) = \phi(U_9) = \{[1], [4], [7]\} \neq U_9$, con lo cual no es sobreyectiva.

Sección 7.2, página 367

1a. $405 = (110010101)_2$

1b. $1444 = (2001221)_{-3} = (1222111)_3$

1c. $356281 = (42400111)_5 = (113100241)_{-5}$

1d. $1500 = (25020)_{-6}$

1e. $-286 = (2402)_{-6}$

2. $b = 4$.

3. La explicación es sencilla, cada uno de los tres reyes tiene una base de numeración distinta, por lo que, en realidad, se debe cumplir que $(222)_a = (66)_b = (22)_c$. Luego de plantear las ecuaciones asociadas, $3b + 2 = c$ y $b = \frac{a^2+a-2}{3}$, y recordando que $b > 6$, usted obtiene que las ecuaciones se satisfacen si $a = 7$, $b = 18$ y $c = 56$, con lo cual cada rey recibió 114 (ciento catorce) caballos.

Sección 7.3, página 371

2. Las tablas de adición y multiplicación en base 5 son:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

3b. $(12304)_5 \times (3002)_5 = (43002113)_5$

3d. $(1203,4)_5 \times (3,04)_5 = (4230,001)_5$

3e. $(2302)_5 - (1430)_5 = (322)_5$

5a. $(121064)_7 + (620510)_7 = (1041604)_7$

5b. $(3025)_7 \times (612)_7 = (2461533)_7$

6. Al utilizar la fórmula dada en el ejercicio (1j) (página 288), se tiene $(11\ldots11)_2 = 1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$, su cuadrado es:

$$\begin{aligned}(2^k - 1)^2 &= 2^{2k} - 2^{k+1} + 1\\ &= 2^{k+1}(2^{k-1} - 1) + 1\\ &= 2^{k+1}(2^{k-2} + \cdots + 1) + 1\\ &= 2^{2k-1} + 2^{2k-2} + \cdots + 2^{k+1} + 1\end{aligned}$$

Es decir, $[(\underbrace{11\ldots11}_{k \text{ unos}})_2]^2 = (\underbrace{111\ldots11}_{k-1 \text{ unos}}\underbrace{00\ldots00}_{k \text{ ceros}}1)_2$

7. La fracción racional de $(2,4\overline{32})_5$ es $\frac{(2403)_5}{(440)_5}$ y la decimal $\frac{353}{120}$.

Sección 7.4, página 375

1c. $27 = (3402)_{5/3}$

Sección 7.5, página 382

2. Sugerencia: verifique que $3^{20} \equiv 1 \bmod 100$.

3. $k = 5$.

4. 23.

5. Primero note que $23 \equiv 2 \bmod 7$; así, al elevar a la tres se obtiene $23^3 \equiv 2^3 \bmod 7 \equiv 1 \bmod 7$ y $23^{24} \equiv 1 \bmod 7$. Análogamente se tiene que $2\,000 \equiv 5 \bmod 7$. De esto, al sumar, se obtiene que $(23^{24} + 2\,000) \equiv (1 + 5) \bmod 7 \equiv -1 \bmod 7$, y luego de elevar a la 40 se obtiene que $(23^{24} + 2\,000)^{40} \equiv (-1)^{40} \bmod 7 \equiv 1 \bmod 7$. De esta manera, el residuo es 1.

6. Es claro que $2346 \equiv 1 \bmod 7$. Además, vea que $4321 \equiv 2 \bmod 7$, al elevar a la tres se obtiene $4321^3 \equiv 2^3 \bmod 7 \equiv 1 \bmod 7$, por lo que $4321^{300} \equiv 1^{100} \bmod 7 \equiv 1 \bmod 7$. De esto, al sumar, se obtiene que $2346 + 4321^{300} \equiv 1 + 1 \bmod 7 \equiv 2 \bmod 7$, y luego de elevar a la tres, se obtiene que $(2346 + 4321^{300})^3 \equiv 2^3 \bmod 7 \equiv 1 \bmod 7$. De esta manera, el residuo es 1.

8. Como $2001^{1999} \equiv 1 \bmod 10$; además, $27! \equiv 0 \bmod 10$, pues $27!$ tiene a 10 como factor; por último, $123456 \equiv 6 \bmod 10$. Por lo tanto, se tiene que $2001^{1999} + 27! + 123456 \equiv 7 \bmod 10$. Con lo que el número de unidades de este número es 7 y, por el ejercicio 7 de esta lista, como ningún cuadrado perfecto termina en 7, se tiene que no es un cuadrado perfecto.

9. El residuo es 5.

12. Se prueba que $1989^{1988} + 6 \equiv 7 \bmod 10$; esto significa que $1989^{1988} + 6$ tiene un 7 en las unidades. Como ningún cuadrado perfecto termina en 7, no existe tal k.

13c. Una primera forma de probar este resultado es hacer casos sobre n, analizando para $n = 3k$, $n = 3k+1$, $n = 3k+2$ y probando que en cada caso se obtiene un residuo de 0 en la división por 9. Otra forma de probar el resultado propuesto es factorizando en la forma $\left(2^{2n}-1\right)\left(2^{2n+1}+1\right)$ y luego verificar, utilizando congruencias, que cada uno de estos dos factores es divisible por 3.

14. Pruebe que $2^{32}+1 \equiv 0 \bmod 641$.

15. Pruebe que $\displaystyle\sum_{i=0}^{n} a_i 10^i - \sum_{i=0}^{n} (-1)^i a_i \equiv 0 \bmod 11$, luego analice qué debe darse para que un número divida a una diferencia.

16. Se verifica que $994 \equiv 0 \bmod 7$, $98 \equiv 0 \bmod 7$ y $7 \equiv 0 \bmod 7$.

"$\Rightarrow$" Como $7|n$, se tiene:

$$\begin{aligned}
&\Rightarrow \quad 1000a_3 + 100a_2 + 10a_1 + a_0 \equiv 0 \bmod 7\\
&\Rightarrow \quad (994+6)a_3 + (98+2)a_2 + (7+3)a_1 + a_0 \equiv 0 \bmod 7\\
&\Rightarrow \quad 6a_3 + 2a_2 + 3a_1 + a_0 \equiv 0 \bmod 7
\end{aligned}$$

"$\Leftarrow$" Como $994a_3 + 98a_2 + 7a_1 \equiv 0 \bmod 7$, se tiene:

$$\begin{aligned}
&\Rightarrow \quad (1000-994)a_3 + (100-98)a_2 + (10-7)a_1 + a_0\\
&\qquad \equiv 0 \bmod 7\\
&\Rightarrow \quad 1000a_3 + 100a_2 + 10a_1 + a_0 - (994a_3 + 98a_2 + 7a_1)\\
&\qquad \equiv 0 \bmod 7\\
&\Rightarrow \quad 1000a_3 + 100a_2 + 10a_1 + a_0 \equiv 0 \bmod 7
\end{aligned}$$

Bibliografía

[1] Barrantes, Hugo *et al. Introducción a la Teoría de Números.* Editorial de la Universidad Estatal a Distancia. Costa Rica, 1998.

[2] Barrantes, Hugo. *Introducción a la Matemática.* Editorial de la Universidad Estatal a Distancia. Costa Rica, 2002.

[3] Bogart, Kenneth. *Matemáticas Discretas.* LIMUSA. México, 1998.

[4] Burde, Klaus. *Numeración fraccionaria.* Revista Investigación y Ciencia, Num. 227. España, 1995.

[5] Camacho, Luis. *Introducción a la Lógica.* Libro Universitario Regional (LUR). 2002.

[6] Calderón, Silvia & Morales, Mario. *Análisis Combinatorio.* Editorial Tecnológica de Costa Rica, 1992.

[7] Carreño, Ximena & Cruz, Ximena. *Álgebra.* Publicaciones Cultural. México, 2003.

[8] Carroll, Lewis. *Alicia en el país de las maravillas.* 1865. Disponible en www.infotematica.com.ar.

[9] Díaz Navarro, Pedro. *Reflexiones sobre el concepto de infinito.* Revista digital Matemática, Educación e Internet. Disponible en: www.cidse.itcr.ac.cr/revistamate/MundoMatematicas/index.html

[10] Gardner, M. *Circo Matemático.* Alianza Editorial. Madrid, 1985.

[11] Gómez, Pedro & Gómez, Cristina. *Sistemas formales, informalmente.* Grupo Editorial Iberoamérica. México, 2000.

[12] Góngora, E. *Introducción al Pensamiento Lógico Matemático*. Editorial de la Universidad Estatal a Distancia. Costa Rica, 1979.

[13] González, Fabio. *Álgebra I*. Editorial de la Universidad Estatal a Distancia. Costa Rica, 1994.

[14] Grassmann, W. & Tremblay, J.P. *Matemática Discreta y Lógica*. Prentice Hall. Madrid, 1996.

[15] Grimaldi, R. *Matemáticas Discreta y Combinatoria*. Addison Wesley, Tercera Edición. México, 1998.

[16] Herstein, I.N. *Álgebra Abstracta*. Grupo Editorial Iberoamérica. México, 1986.

[17] Hofstadter, Douglas R. *Gödel, Escher, Bach*. Vintage Books, Random House. New York, 1980.

[18] Huete de Guevara, María. *Matemática Elemental*. Vol 2. Editorial de la Universidad Estatal a Distancia. Costa Rica, 2000.

[19] Kleiman, A. & Kleiman, E. *Conjuntos*. Editorial LIMUSA. México, 1974.

[20] Kolman, B. *et al. Estructuras de Matemáticas Discretas para la Computación*, Tercera Edición. Prentice Hall. México, 1996.

[21] Marranghello, Leonardo. *Introducción a la Matemática*. CAEM, Escuela de Matemática, Universidad de Costa Rica, 1983.

[22] www.mersenne.org

[23] Micha, E. *Matemáticas Discretas*. Editorial LIMUSA. México, 1999.

[24] Miller, Charles & Heeren, Vern. *Introducción al pensamiento matemático*, Primera Edición. Editorial Trillas. México, 1979.

[25] Murillo, Manuel *et al. Matemática básica con aplicaciones*. Editorial de la Universidad Estatal a Distancia. Costa Rica, 2000.

[26] Murillo, Manuel & González, Fabio. *Teoría de los números*. Editorial Tecnológica de Costa Rica, 2006.

[27] Murillo T. Manuel *et al. Un mosaico de ajedrez*. Educación, matemática e Internet. Costa Rica, 2001.
www.itcr.ac.cr/revistamate/ContribucionesN12001/ajedrez/pag1.html

[28] Perero, Mariano. *Historia e Historias de Matemáticas*. Grupo Editorial Iberoamérica. México, 1994.

[29] Rodríguez, Rodolfo. *El mundo de la lógica: de la paradoja a la verdad*. Las Matemáticas y su Enseñanza, Num. 8, Vol. 3, 1991.

[30] Ross, K. & Wright, Ch. *Matemáticas Discretas*, Segunda Edición. Prentice Hall. México, 1990.

[31] Ruiz, Ángel. *Historia y Filosofía de las Matemáticas*. Editorial de la Universidad Estatal a Distancia. Costa Rica, 2003.

[32] Scheinerman, Edward. *Matemáticas Discretas*. Editorial Thomson. México, 2001.

[33] Smullyan, Raymond. *¿Cómo se llama este libro?*. Ediciones Cátedra. Madrid, 1985.

[34] Tahan, Malba (Seudónimo). *El hombre que calculaba*. Editorial Crear. Venezuela, 1985.

[35] Tsijli, Teodora. *Geometría Euclídea I*. Editorial de la Universidad Estatal a Distancia. Costa Rica, 1994.

[36] www.cimm.ucr.ac.cr/aruiz/Historia%20y%20Filosofia/Secciones/Biografias.htm

[37] www.itcr.ac.cr/revistamate/

[38] Vinográdov, I. *Fundamentos de la Teoría de Números*. Editorial MIR. Moscú, 1987.

Índice temático

F

N

O

P

U

V

W

Z

Sobre el autor

Obtuvo su licenciatura en Matemática en la Universidad de Costa Rica, y una Maestría en Educación en la Universidad Americana. Inició su labor como docente en la Universidad de Costa Rica en 1987; en la actualidad es profesor catedrático de la Universidad Estatal a Distancia y del Instituto Tecnológico de Costa Rica.

Autor de los libros: *Una introducción a la teoría de números* (1998), *Matemática básica con aplicaciones* (2000), ambos de la Editorial de la Universidad Estatal a Distancia; *El ajedrez en Costa Rica* (2003), *Antología del ajedrez costarricense* (2003), ambos de la Editorial de la Universidad de Costa Rica; *Introducción a la matemática discreta* (2004), *Teoría de los números* (2006), ambos de la Editorial Tecnológica de Costa Rica. Además, cuenta con más de 30 publicaciones en el campo de las matemáticas y sus aplicaciones en Chile, Nicaragua, Guatemala, Cuba y Costa Rica. Participante y expositor en más de 35 eventos académicos en Cuba, Centroamérica, Puerto Rico, México y Grecia.

Es miembro adjunto del Comité Latinoamericano de Matemática Educativa desde el 2006. Premio Jorge Volio 2007 en el área de Filosofía, segundo lugar por su obra *De valores, pecados y otros mitos.* Premio Jorge Volio 2008 en el área de Ciencias Exactas, mención de honor por su obra *Teoría de los números.*

Teléfonos: (506)2550-2225, (506)2550-2493

Correos electrónicos: *mmurillo@itcr.ac.cr*, *mmurillo@costarricense.cr*