

# Conjuntos y números



Alonso Castillo Pérez  
Alonso Castillo Ramírez  
Elba Lilia de la Cruz García  
Alfonso Manuel Hernández Magdaleno

# Conjuntos y números



EDITORIAL  
UNIVERSITARIA

Centro  
Universitario de  
Ciencias Exactas  
e Ingenierías

Universidad  
de Guadalajara



**Itzcóatl Tonatiuh Bravo Padilla**  
**Rectoría General**

**Miguel Ángel Navarro Navarro**  
**Vicerrectoría Ejecutiva**

**José Alfredo Peña Ramos**  
**Secretaría General**

**César Octavio Monzón**  
**Rectoría del Centro Universitario de Ciencias**  
**Exactas e Ingenierías**

**José Alberto Castellanos Gutiérrez**  
**Rectoría del Centro Universitario**  
**de Ciencias Económico Administrativas**

**José Antonio Ibarra Cervantes**  
**Corporativo de Empresas Universitarias**

**Edgardo Flavio López Martínez**  
**Encargado del despacho de la Editorial**  
**Universitaria**

Primera edición electrónica, 2014

#### **Textos**

© Alonso Castillo Pérez, Alonso Castillo Ramírez,  
Elba Lilia de la Cruz García y Alfonso Manuel  
Hernández Magdaleno

**Coordinación editorial**  
Sayri Karp Mitastein

**Producción**  
Jorge Orendáin Caldera

**Coordinación de diseño**  
Edgardo Flavio López Martínez

**Diseño de portada e interiores**  
Editorial Universitaria

**Formación**  
Lópx. Diseño y Comunicación Visual

**Corrección**  
David Rodríguez Álvarez

**D.R. © 2014**  
**Universidad de Guadalajara**



EDITORIAL  
UNIVERSITARIA

**Editorial Universitaria**  
José Bonifacio Andrada 2679  
Colonia Lomas de Guevara  
44657 Guadalajara, Jalisco

**01 800 834 54276**  
**www.editorial.udg.mx**

**ISBN 978 607 742 091 0**

Noviembre de 2014

Este libro se terminó de editar  
en las oficinas de la Editorial Universitaria  
José Bonifacio Andrada 2679, Lomas de Guevara  
44657, Guadalajara, Jalisco

Hecho en México  
*Made in Mexico*

Se prohíbe la reproducción, el registro o la transmisión parcial o total de esta obra por cualquier sistema de recuperación de información, sea mecánico, fotoquímico, electrónico, magnético, electroóptico, por fotocopia o cualquier otro, existente o por existir, sin el permiso por escrito del titular de los derechos correspondientes.

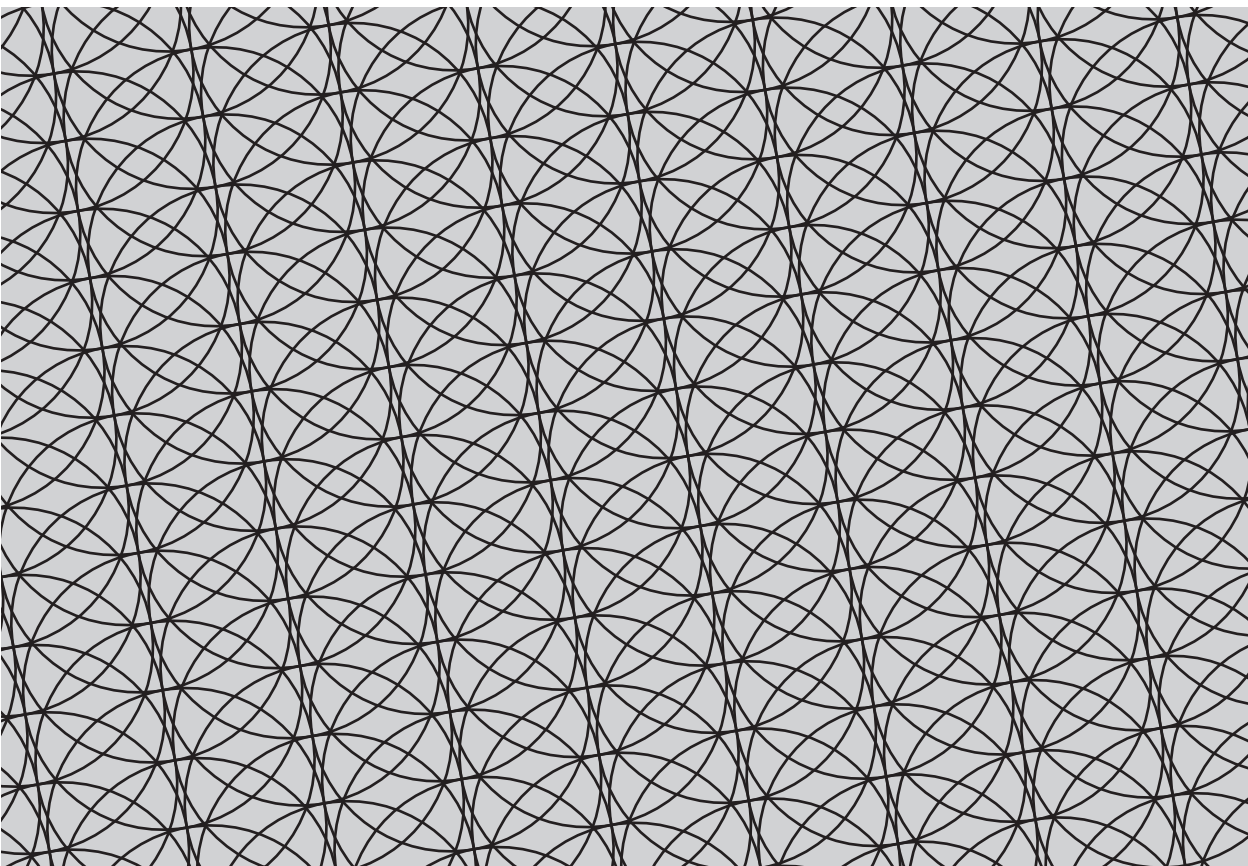
En la formación de este libro se utilizaron las familias tipográficas Meta Pro, diseñada por Erik Spiekermann, y Minion, diseñada por Robert Slimbach.

# Índice

<b>Prefacio</b>	<b>7</b>
<b>Capítulo 1. Lógica básica</b>	<b>11</b>
1.1 Proposiciones . . . . .	12
1.1.1 Ejercicios de proposiciones . . . . .	16
1.2 Negaciones y cuantificadores . . . . .	17
1.2.1 Negación . . . . .	17
1.2.2 Cuantificadores . . . . .	18
1.2.3 Ejercicios de cuantificadores . . . . .	22
1.3 Conectivos . . . . .	23
1.3.1 Conjunción y disyunción . . . . .	23
1.3.2 Condicional y bicondicional . . . . .	26
1.3.3 Tautologías y contradicciones . . . . .	30
1.3.4 Ejercicios de conectivos . . . . .	32
1.4 Métodos de demostración . . . . .	33
1.4.1 Contraejemplo y contrapuesta . . . . .	36
1.4.2 Reducción al absurdo . . . . .	37
1.4.3 Demostración de equivalencias . . . . .	38
1.4.4 Ejercicios de métodos de demostración . . . . .	40
1.5 Glosario . . . . .	41
1.6 Definiciones del capítulo . . . . .	42
<b>Capítulo 2. Conjuntos</b>	<b>43</b>
2.1 Teorías de conjuntos . . . . .	44
2.1.1 Ejercicios de teorías de conjuntos . . . . .	48
2.2 Conceptos básicos de conjuntos . . . . .	49
2.2.1 Ejercicios de conceptos básicos de conjuntos . . . . .	54
2.3 Operaciones de conjuntos . . . . .	56
2.3.1 Ejercicios de operaciones de conjuntos . . . . .	65
2.4 Definiciones del capítulo . . . . .	66
<b>Capítulo 3. Relaciones</b>	<b>67</b>
3.1 Funciones . . . . .	68
3.1.1 Relaciones binarias . . . . .	68
3.1.2 Definición de función . . . . .	72
3.1.3 Tipos de funciones . . . . .	76
3.1.4 Composición de funciones . . . . .	79
3.1.5 Ejercicios de funciones . . . . .	85

3.2	Relaciones de equivalencia . . . . .	86
3.2.1	Ejercicios de relaciones de equivalencia . . . . .	93
3.3	Relaciones de orden . . . . .	94
3.3.1	Ejercicios de relaciones de orden . . . . .	100
3.4	Definiciones del capítulo . . . . .	102
<b>Capítulo 4.</b>	<b>Números</b>	<b>103</b>
4.1	Números naturales . . . . .	104
4.1.1	Axiomas de Peano . . . . .	104
4.1.2	Inducción matemática . . . . .	107
4.1.3	Ejercicios de números naturales . . . . .	113
4.2	Números enteros . . . . .	114
4.2.1	Divisibilidad . . . . .	116
4.2.2	Ecuaciones diofánticas . . . . .	122
4.2.3	Ejercicios de números enteros . . . . .	126
4.3	Congruencias . . . . .	127
4.3.1	Ejercicios de congruencias . . . . .	131
4.4	Cardinalidad . . . . .	132
4.4.1	Comparación de cardinalidades . . . . .	132
4.4.2	Conjuntos numerables . . . . .	134
4.4.3	Números cardinales . . . . .	138
4.4.4	Ejercicios de cardinalidad . . . . .	141
4.5	Técnicas de conteo . . . . .	143
4.5.1	Ejercicios de conteo . . . . .	150
4.6	Definiciones del capítulo . . . . .	151
<b>Capítulo 5.</b>	<b>Estructuras algebraicas</b>	<b>152</b>
5.1	Grupos . . . . .	153
5.1.1	Ejercicios de grupos . . . . .	163
5.2	Campos . . . . .	164
5.2.1	Ejercicios de campos . . . . .	171
5.3	Espacios vectoriales . . . . .	173
5.3.1	Ejercicios de espacios vectoriales . . . . .	180
5.4	Polinomios . . . . .	182
5.4.1	Ejercicios de polinomios . . . . .	189
5.5	Definiciones del capítulo . . . . .	190
<b>Índice alfabético</b>		<b>194</b>

# Prefacio



La capacidad de razonamiento es el factor principal en la construcción de una civilización tecnológica y científica. Con la razón podemos interpretar, aprender, deducir y predecir fenómenos naturales para hacer cosas como curar enfermedades, construir computadoras y viajar al espacio.

Aunque es una habilidad inherente a la humanidad, con el paso de los años hemos mejorado la precisión y profundidad de nuestros razonamientos; comprendimos que los lenguajes naturales, como el español, el inglés o el francés, no son suficientes para describir situaciones complejas. Para ejemplificar esto, consideraremos dos *silogismos* aristotélicos.

*Silvestre es un gato.*  
*Los gatos son mamíferos.*  
*Silvestre es un mamífero.*

Las hipótesis y conclusión anteriores parecen adecuadas. Entonces, ¿cuál es el problema con el siguiente silogismo?

*Silvestre es un gato.*  
*Un gato puede levantar automóviles.*  
*Silvestre puede levantar automóviles.*

Después de pensarlo un poco, comprendemos que la palabra “gato” en la primera premisa se usa para referirse a un animal felino, mientras que en la segunda se usa para referirse a una herramienta hidráulica.

Las palabras de los lenguajes naturales son *polisémicas* (tienen muchos significados) y adquieren diferentes connotaciones ubicándolas en distintos contextos. Todo esto dificulta enormemente el uso del lenguaje natural para razonar de forma clara y precisa. Por tal motivo, la humanidad ha trabajado durante siglos en desarrollar otro lenguaje, uno que permita formular observaciones exactas y hacer deducciones rigurosas. Este lenguaje es la matemática.

Los términos matemáticos pretenden lograr, en cierto contexto, un significado único, preciso y total. En general, son ideas abstractas que carecen de existencia propia y sólo son lo que su definición establece. Si quisiéramos escribir una definición formal de un objeto real, por ejemplo las vacas, sería sumamente difícil. Si establecemos que las vacas son cuadrúpedos, dejaríamos fuera a las que han perdido una pata o nacieron sin ella; además, también



son cuadrúpedos los chivos, los venados, los toros, etc. ¿Qué características definen con precisión a las vacas? Afortunadamente, la definición de vaca no es indispensable ya que las reconocemos de cualquier forma. La diferencia entre un veterinario y un matemático es que el primero puede curar una vaca aunque desconozca su definición, mientras que el segundo no podría iniciar una teoría de las “vacas” si no construye primero una definición formal.

A pesar de esto, la matemática nombra sus conceptos utilizando palabras del lenguaje natural, a las cuales asigna un nuevo sentido. Dice el filósofo español José Ortega y Gasset:

Cuando el investigador descubre un fenómeno nuevo, es decir, cuando forma un nuevo concepto, necesita darle un nombre. Como una voz nueva no significaría nada para los demás, tiene que recurrir al repertorio del lenguaje usado, donde cada voz se encuentra ya adscrita a una significación. A fin de hacerse entender, elige la palabra cuyo usual sentido tenga alguna semejanza con la nueva significación.

Es particularmente complejo encontrar la relación entre el significado común de las palabras y su significado matemático. Por ejemplo, la palabra *función* en español tiene los siguientes significados:<sup>1</sup>

- 1) Capacidad de actuar propia de los seres vivos y de sus órganos, y de las máquinas o instrumentos.
- 2) Tarea que corresponde realizar a una institución o entidad, o a sus órganos o personas.
- 3) Representación de una obra teatral, o proyección de una película.

Por otro lado, en matemáticas una función es un conjunto de pares ordenados cuyas primeras coordenadas son todas distintas entre sí (ver definición 3.11). Es importante no mezclar los significados coloquiales con el matemático: en el segundo contexto, una función nunca hará referencia a una obra teatral o a la capacidad de actuar de un instrumento.

No obstante, las definiciones matemáticas tienen una historia. La formalización evoluciona; se van precisando o creando nuevos conceptos que le dan mayor alcance a una teoría. La famosa frase

---

<sup>1</sup>De acuerdo con el *Diccionario de la Real Academia de la Lengua Española*, vigésima edición.

del matemático alemán Leopold Kronecker “los números naturales los hizo Dios, todo lo demás es obra humana” puede interpretarse como que los números que se utilizan para contar son tan antiguos como la civilización misma, pero que la matemática ha trabajado permanentemente en ellos hasta llegar a su axiomatización.

Este texto fue escrito para el curso Conjuntos y Números del Centro Universitario de Ciencias Exactas e Ingenierías de la Universidad de Guadalajara. Está dirigido a estudiantes de primer semestre de la licenciatura en matemáticas. Nuestro objetivo es presentar una sólida introducción al lenguaje matemático moderno. El texto se divide en cinco capítulos principales con los temas: lógica básica, conjuntos, relaciones, números y estructuras algebraicas, cada uno de los cuales contiene varias secciones.

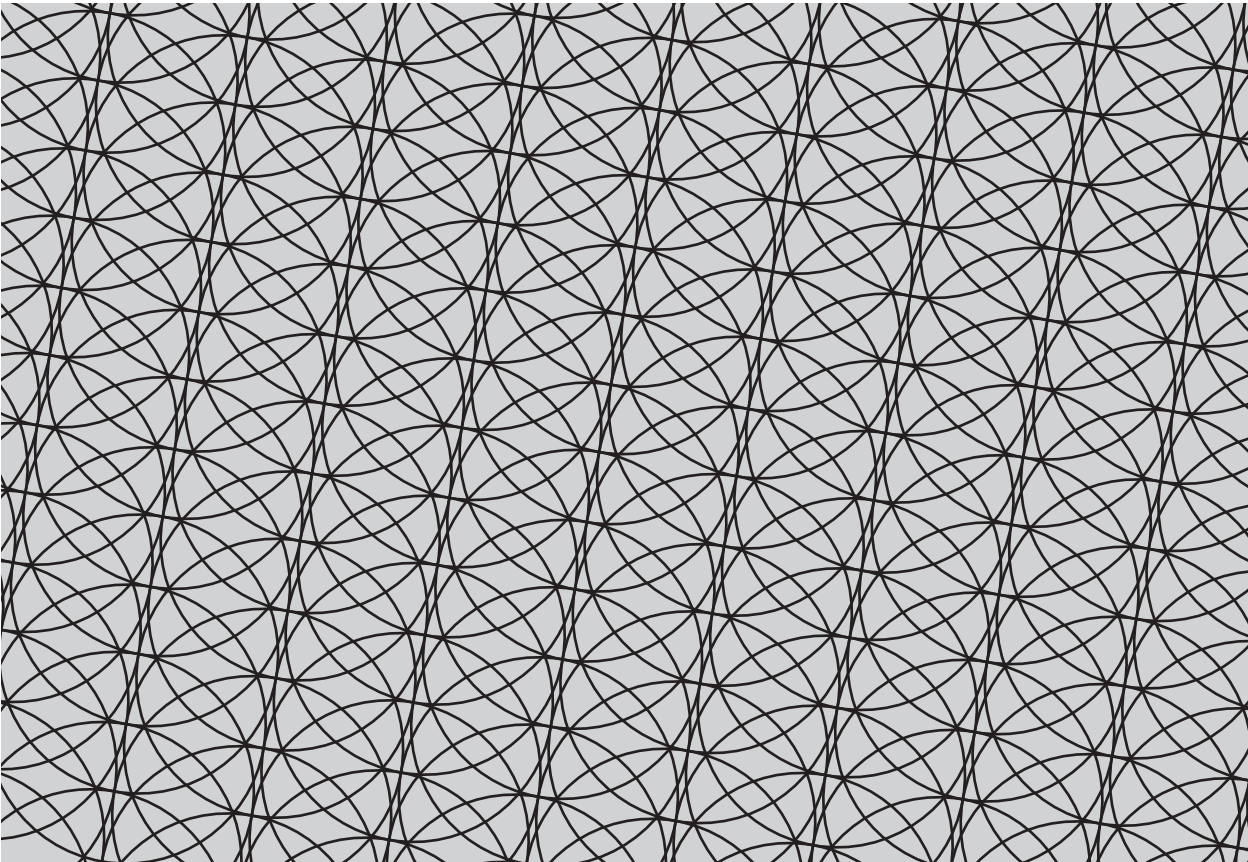
Nos enfocamos en ayudar a que el estudiante comprenda las definiciones de los objetos matemáticos tratados en cada capítulo y las demostraciones rigurosas de algunas de sus propiedades. Tomamos varias medidas para reforzar nuestro enfoque. Primero, cada capítulo incluye una sección titulada “Definiciones del capítulo”, la cual contiene una lista de conceptos. Pedimos al lector que, después de haber leído el capítulo correspondiente, recopile las definiciones de estos conceptos y encuentre un ejemplo de cada una. Cada sección incluye un párrafo final de *palabras clave*, el cual enlista los conceptos y teoremas relevantes de la sección. En el capítulo 1 exploramos diversas técnicas que brindan al estudiante las herramientas necesarias para entender las demostraciones de los capítulos posteriores y resolver los ejercicios.

Agregamos una advertencia: este texto no debe leerse como uno de historia, literatura u otra asignatura propia del bachillerato. Un texto universitario de matemáticas debe leerse asegurándose de comprender en su totalidad cada línea. Por tal motivo, recomendamos al lector hacer diagramas y notas sobre cada definición, ejemplo, proposición y teorema que encuentre. Para asimilar los conceptos abordados, también es importante resolver, o al menos intentar resolver, todos los ejercicios correspondientes a cada sección.

*¡Por el contrario! Si hubiese sido así, entonces lo sería; y siéndolo, quizá lo fuera; pero como no fue así, tampoco lo es así. ¡Es lógico!*

Lewis Carroll, Alicia en el País de las Maravillas

## Capítulo 1. Lógica básica



Durante muchos siglos, la lógica fue una rama de la filosofía dedicada al estudio del razonamiento. Aristóteles, el filósofo de la antigua Grecia, escribió el primer tratado de lógica conocido actualmente; sin embargo, la lógica comenzó a aplicarse en matemáticas hace apenas cien años con el objetivo de establecer sólidamente los fundamentos de la aritmética, la geometría y el análisis.

Irónicamente, este capítulo es el más intuitivo e informal del texto. La lógica matemática es un tema complejo y sutil; en las próximas secciones sólo abordaremos algunos de sus temas más importantes.<sup>1</sup> El concepto central de este capítulo, que presentamos en la sección 1.1, es el de *proposición*. La teoría de proposiciones tiene dos ramas: la *sintaxis*, que se ocupa de su estructura y composición; y la *semántica*, que se ocupa de su interpretación y la construcción de argumentos. Algunos conceptos relacionados con la sintaxis son los *cuantificadores* y los *conectivos*, que estudiamos en las secciones 1.2 y 1.3; profundizamos en la semántica de las proposiciones en la sección 1.4.

## 1.1 Proposiciones

Recordemos que en la gramática del español la unidad mínima de lenguaje para manifestar una idea, con su significado completo, es la oración, la cual se forma con la estructura

**sujeto + predicado.**

Cada parte de la estructura de una oración se construye combinando diversos términos. Las oraciones se dividen en las siguientes clases: declarativas, imperativas, exclamativas e interrogativas. Cuando se expresa una idea completa en una oración, cuyo predicado afirma o niega algún atributo del sujeto, se obtiene una *oración declarativa*. Esta clase de oraciones son las que abordamos en nuestro estudio de la lógica matemática.

**Ejemplo 1.1.** Consideremos los siguientes ejemplos:

- 1) ¿Fue resuelta la ecuación por Erika?. *Esta no es una oración declarativa sino interrogativa.*
- 2) Javier, apresúrese con ese problema. *Esta no es una oración declarativa sino imperativa.*

---

<sup>1</sup>Para un estudio más completo, aunque también informal, puede consultarse (Magnus, 2012).

- 3) La raíz cuadrada de 5 es menor que  $\pi$ . *Esta es una oración declarativa.*
- 4) Los lados de un triángulo no son congruentes. *Esta es una oración declarativa.*
- 5) La geometría de Riemann es una rama de las matemáticas muy interesante. *Esta es una oración declarativa.*
- 6) El promedio de  $x_1, x_2, \dots, x_N \in \mathbb{R}$

$$\frac{x_1 + x_2 + \dots + x_N}{N}.$$

*Esta es una oración declarativa.*

Cada una de las oraciones anteriores se da en un contexto implícito que determina la naturaleza de los términos involucrados. Por ejemplo, la oración 3) se da en el contexto de la aritmética de los números reales, mientras que la oración 4) se da en el contexto de la geometría euclidiana. Llamaremos a este contexto el *universo de discurso* de la oración.

Ahora podemos precisar la noción de proposición.

**Definición 1.2 (proposición).** Una proposición es una oración declarativa, la cual, en un universo de discurso dado, puede caracterizarse como verdadera o falsa, pero no puede tener ambos atributos.

En el ejemplo 1.1, sólo las oraciones 3) y 6) son proposiciones. Las oraciones 1) y 2) no son proposiciones porque no son declarativas. La oración 4) no es una proposición ya que, al no precisar el triángulo al que se hace referencia, no es posible caracterizarla como verdadera o falsa (es verdadera para algunos triángulos pero falsa para otros). La oración 5) no es una proposición ya que no se ha establecido una definición universal para el término “ser muy interesante”; por lo tanto, es una declaración subjetiva, cuya verdad o falsedad depende de gustos y opiniones.

La característica de verdad o falsedad de una proposición se denomina *valor de verdad*.

**Ejemplo 1.3.** Consideremos algunos ejemplos:

- 1) Dos es un número primo. *Esta es una proposición, ya que es una oración declarativa verdadera.*
- 2) El área del círculo es mayor que el área del cuadrado. *Esta no es una proposición, ya que no se puede determinar su valor de verdad: puede ser verdadera o falsa dependiendo del círculo y el cuadrado que se consideren.*

- 3) Siempre que  $x$  sea un número real, se cumple que  $-x < 0$ . *Esta es una proposición, ya que es una oración declarativa falsa. La razón de su falsedad recae en el uso de la palabra “siempre”: no es verdad porque podemos encontrar casos que la desmienten, por ejemplo  $-1$  es un número real tal que  $-(-1) > 0$ .*

Las proposiciones se clasifican en simples y compuestas. Las primeras se componen de *términos singulares*, los cuales hacen referencia a objetos particulares; actúan en calidad de nombre propio.

**Ejemplo 1.4 (términos singulares).** Pedro, José, 9,  $\pi$ , la constante de Euler, la ecuación de Laplace, etcétera.

**Definición 1.5 (proposición simple).** Decimos que una proposición es simple, o atómica, si está constituida por sujetos formados por términos singulares y un predicado con un verbo que expresa una acción sobre dichos sujetos.

En otras palabras, una proposición simple es aquella que no puede separarse en otros enunciados y afirma algo específico sobre un objeto particular.

**Ejemplo 1.6.** Las siguientes son proposiciones simples:

- 1) Pedro tiene los ojos negros.
- 2) El área de un círculo de radio 1 es  $\pi$ .
- 3) 3 es la raíz cuadrada de 9.
- 4)  $3 + 7 - 2 = 8$ .
- 5) 5 es un número impar.

Las proposiciones compuestas están conformadas por dos o más proposiciones simples; estudiaremos más acerca de esto en las próximas secciones.

Finalizaremos esta sección con el estudio de otro concepto importante. Un *predicado* es una expresión que establece una propiedad o característica de algún sujeto. Como mencionamos anteriormente, los predicados son una parte fundamental en la formación de oraciones. Algunos ejemplos son: “es azul”, “es mayor que” y “es un número par”.

En matemáticas, para hacer referencia a un predicado usamos variables ( $x$ ,  $y$ ,  $z$ ,  $w$ , etc.) que representan un sujeto cualquiera dentro del universo de discurso; así pues, el predicado “es azul” será denotado por

$$A(x) = (x \text{ es azul}).$$

Los predicados no son proposiciones, ya que no pueden ser caracterizados como verdaderos o falsos. Sin embargo, al *evaluar* las variables en sujetos particulares, los predicados producen proposiciones.

**Ejemplo 1.7.** Consideremos los siguientes ejemplos:

- 1) El predicado  $A(x) = (x \text{ es azul})$  evaluado en  $x = (\text{cielo})$  produce la proposición verdadera  $A(\text{cielo}) = (\text{el cielo es azul})$ .
- 2) El predicado  $P(z) = (z \text{ es un número par})$  evaluado en  $z = 5$  produce la proposición falsa  $P(5) = (5 \text{ es un número par})$ .
- 3) Consideremos el predicado  $R(x, y) = (x \leq y)$ . Entonces  $R(3, 5)$  es una proposición verdadera, mientras que  $R(7, 4)$  es una proposición falsa.

**Palabras clave de la sección:** *proposición, universo de discurso, valor de verdad, término singular, proposición simple, predicado.*

### 1.1.1 Ejercicios de proposiciones

**Ejercicio 1.8.** Determina si las siguientes expresiones son proposiciones, predicados o ninguna de las dos. Justifica tu respuesta.

- a) 5 es mayor que 9.
- b)  $m$  es un número primo.
- c) ¿Es 7 un número primo?
- d) Un triángulo tiene cuatro lados.
- e) Los matemáticos son personas inteligentes.
- f) Escribe el resultado de la ecuación.
- g) Sea  $x$  un número real mayor que cero.
- h) Existe una función que es continua pero no diferenciable.
- i) La raíz cuadrada de  $z$  es 5.

**Ejercicio 1.9.** Determina el universo de discurso de las siguientes proposiciones y escribe su valor de verdad. Justifica tu respuesta.

- a) Existen aves que no pueden volar.
- b) La ecuación  $x - 3 = 0$  tiene un número infinito de soluciones.
- c) La raíz cuadrada de 4 es 2 y la de 16 es 8.
- d) El área de un círculo es igual a  $\pi$  por el cuadrado de su radio.
- e) El número 6 es un múltiplo de 3.
- f)  $3^2 + 4^2 = 5^2$ .

**Ejercicio 1.10.** Considera los siguientes términos: ángulo, el círculo de radio 2,  $\frac{4\pi}{3}$ , humano, número real, el conjunto de números reales, Pedro y  $73^\circ$ . ¿Cuáles de estos son términos singulares? Justifica tu respuesta.

**Ejercicio 1.11.** En cada uno de los siguientes predicados, encuentra los números enteros que producen proposiciones verdaderas.

- a)  $P(x) = (x^2 = 16)$ .
- b)  $S(y) = (|y| < 3)$ .
- c)  $R(z) = (z \text{ es par y primo})$ .
- d)  $T(w, u) = (w + u = 1 \text{ y } 2u = 6)$ .



## 1.2 Negaciones y cuantificadores

En esta sección estudiaremos dos temas fundamentales ligados a la construcción de proposiciones.

### 1.2.1 Negación

Si  $P$  es una proposición cualquiera, la *negación* de  $P$ , denotada como  $\sim P$ , es una proposición cuyo valor de verdad es el opuesto al valor de verdad de  $P$ . En otras palabras, si  $P$  es verdadera, entonces  $\sim P$  es falsa, y si  $P$  es falsa, entonces  $\sim P$  es verdadera. También se usa comúnmente el símbolo  $\neg$  en lugar de  $\sim$ .

**Ejemplo 1.12.** Consideremos la proposición

$$P = (4 \text{ es igual a } 2 + 2).$$

Entonces la negación de  $P$  es

$$\sim P = (4 \text{ no es igual a } 2 + 2).$$

En este caso  $P$  es verdadera mientras que  $\sim P$  es falsa.

Además del vocablo “no”, se usa la frase “no es cierto que” para negar proposiciones.

**Ejemplo 1.13.** Si

$$Q = (\text{La raíz cuadrada de } 9 \text{ es } 2),$$

la negación de  $Q$  es

$$\sim Q = (\text{No es cierto que la raíz cuadrada de } 9 \text{ es } 2).$$

En este caso  $Q$  es falsa, mientras que  $\sim Q$  es verdadera.

Cuando el predicado de una proposición simple se representa mediante algún símbolo matemático, se acostumbra formar la negación cruzando el símbolo con una raya inclinada. De esta forma, si  $T = (5 = 4 + 1)$ , entonces la negación es  $\sim T = (5 \neq 4 + 1)$ .

La esencia de la negación de una proposición puede capturarse en una *tabla de verdad*, la cual, en este caso, consiste en un arreglo de dos renglones por dos columnas. En la primera columna se escriben los posibles valores de verdad de una proposición arbitraria

$P$	$\sim P$
$V$	$F$
$F$	$V$

Tabla 1.1: Negación

(verdadero, abreviado como V; y falso, abreviado como F). En la segunda columna se escriben los valores de verdad correspondientes a la negación de dicha proposición asumiendo el valor de verdad que se encuentra en el mismo renglón.

Específicamente, si  $P$  es una proposición arbitraria, la tabla de verdad de la negación se muestra en la tabla 1.1.

Al negar la negación de una proposición  $P$  (hacer una *doble negación*), obtenemos una proposición con el mismo valor de verdad que  $P$ . Más adelante (en el ejercicio 1.47), veremos que las proposiciones  $P$  y  $\sim(\sim P)$  son *lógicamente equivalentes* (definiremos esta idea en la sección 1.3.3). Si usamos el símbolo “ $\equiv$ ” para expresar que dos proposiciones son lógicamente equivalentes, podemos escribir

$$\sim(\sim P) \equiv P.$$

**Ejemplo 1.14.** La doble negación de  $S =$  (Lilia estudia matemáticas) es la proposición

$$\begin{aligned}\sim(\sim S) &= (\text{No es cierto que Lilia no estudia matemáticas}) \\ &\equiv (\text{Lilia estudia matemáticas}) = S.\end{aligned}$$

**Ejemplo 1.15.** La doble negación de la proposición  $P$  del ejemplo 1.12 es

$$\sim(\sim P) = (\text{No es cierto que 4 no es igual a } 2 + 2) \equiv P.$$

## 1.2.2 Cuantificadores

Sea  $P(x)$  un predicado cualquiera. En la sección anterior vimos que es posible producir proposiciones a partir de  $P(x)$  evaluando la variable  $x$ . Otra forma de producir una proposición a partir de  $P(x)$  es mediante el uso de un *cuantificador*. Hay dos tipos de cuantificadores:

- *Cuantificador existencial*, denotado por el símbolo  $\exists$ , el cual se lee como “existe”, “para algún”, “hay al menos uno” o frases equivalentes.

- *Cuantificador universal*, denotado por el símbolo  $\forall$ , el cual se lee como “para todo”, “para cada”, “para cualquier” o frases equivalentes.

Los cuantificadores son elementos clave para lograr la precisión del lenguaje requerida en la formulación de proposiciones.

Por ejemplo, consideremos el predicado

$$P(x) = (x \text{ estudia matemáticas}),$$

donde el universo de discurso es el conjunto de personas. Podemos evaluar  $P(x)$  en personas particulares para producir proposiciones verdaderas o falsas; por otro lado, podemos usar los cuantificadores previamente definidos:

- *Existencial*:

$$\exists x P(x) = (\text{Existe una persona que estudia matemáticas}).$$

- *Universal*:

$$\forall x P(x) = (\text{Todas las personas estudian matemáticas}).$$

Queda claro que el uso de los cuantificadores está restringido al universo de discurso.

Las proposiciones previas tienen significados muy distintos. La primera de ellas es verdadera porque efectivamente existe una persona que estudia matemáticas (por ejemplo, el lector de este texto). La segunda proposición es falsa ya que también podemos encontrar personas que no estudian matemáticas.

**Ejemplo 1.16.** Si el universo de discurso es el conjunto de números reales, el predicado  $Q(x) = (x^2 - 1 < 0)$  tiene dos interpretaciones:

- 1) *Existencial*: existe un número real  $x$  tal que  $x^2 - 1 < 0$ .
- 2) *Universal*: todos los números reales  $x$  satisfacen que  $x^2 - 1 < 0$ .

La proposición 1) es verdadera porque se cumple para al menos un número real (por ejemplo,  $x = 0$ ). La proposición 2) es falsa porque no se cumple para  $x = 2$  o  $x = 3$ .

**Ejemplo 1.17.** Sea  $x$  un número real. El predicado  $x^2 \geq 0$  tiene dos interpretaciones:

- 1) *Existencial*: existe un número real  $x$  tal que  $x^2 \geq 0$ .

2) *Universal*: para todo número real  $x$  se cumple que  $x^2 \geq 0$ .

Ambas proposiciones son verdaderas porque el cuadrado de cualquier número real siempre es mayor o igual que cero. De hecho, la veracidad de la segunda proposición implica la veracidad de la primera.

En el ejemplo anterior, la frase “sea  $x$  un número real” establece que el universo de discurso es el conjunto de los números reales.

Cabe señalar que la expresión “existe un  $x$  tal que” significa lo mismo que “existe al menos un  $x$  tal que”. La frase *al menos* es redundante en la mayoría de los casos. Para expresar que sólo existe un  $x$  con cierta propiedad, usamos frases como “existe exactamente uno” o “existe y es único”. Usamos el símbolo  $\exists!$  para denotar existencia y unicidad.

**Ejemplo 1.18.** Si  $z$  es un número real y  $T(z) = (2z - 7 = 0)$ , la proposición de existencia y unicidad asociada es

$\exists! T(z) = (\text{Existe exactamente un número real } z \text{ tal que } 2z - 7 = 0)$ .

En este caso, la proposición anterior es verdadera.

Las proposiciones que usan cuantificadores no son proposiciones simples; al igual que las proposiciones de la siguiente sección, son llamadas *proposiciones compuestas*.

Es importante entender cómo se obtiene la negación de una proposición cuantificada. Por ejemplo, si

$P = (\text{Todos los mexicanos son matemáticos}),$

¿cuál es la negación de  $P$ ? A simple vista, podríamos pensar que  $\sim P$  es la proposición

$Q = (\text{Todos los mexicanos no son matemáticos}),$   
 $= (\text{Ningún mexicano es matemático}).$

Sin embargo, esto es un error. Por definición,  $\sim P$  es verdadera cuando  $P$  es falsa, y viceversa. Pero esto no sucede con la proposición  $Q$ : en este caso ambas proposiciones,  $P$  y  $Q$  son falsas, ya que no es cierto que todos los mexicanos sean matemáticos, pero tampoco es cierto que ningún mexicano sea matemático. La negación correcta de  $P$  es:

$\sim P = (\text{Existen mexicanos que no son matemáticos}).$

Tal como lo esperábamos, la proposición  $\sim P$  es verdadera.

El ejemplo anterior nos ayuda a comprender que la negación de una proposición universal se obtiene negando el predicado y reemplazando el cuantificador por uno existencial. De manera similar, la negación de una proposición existencial se obtiene negando el predicado y reemplazando el cuantificador por uno universal. En símbolos, si  $P(x)$  es un predicado cualquiera:

$$\sim(\forall x P(x)) \equiv \exists x \sim P(x),$$

$$\sim(\exists x P(x)) \equiv \forall x \sim P(x).$$

**Ejemplo 1.19.** Vemos como negar una proposición existencial.

*Proposición:* Existen personas que no dicen la verdad.

*Negación:* Todas las personas dicen la verdad.

**Ejemplo 1.20.** Ahora negamos una proposición universal.

*Proposición:* Para cualquier número  $x$  tenemos que  $x^2 \geq 0$ .

*Negación:* Existe un número  $x$  tal que  $x^2 < 0$ .

**Ejemplo 1.21.** En este ejemplo se combinan, en una misma proposición, ambos cuantificadores.

*Proposición:* Para cualquier  $x$ , existe  $z$  tal que  $x + z = 0$ .

*Negación:* Existe  $x$  tal que para toda  $z$  se tiene que  $x + z \neq 0$ .

**Palabras clave de la sección:** *negación, doble negación, tabla de verdad, universo de discurso, cuantificadores existencial y universal, existencia y unicidad, negación de proposiciones cuantificadas.*

### 1.2.3 Ejercicios de cuantificadores

**Ejercicio 1.22.** En cada una de las siguientes proposiciones, identifica el predicado, nómbralo (como  $P(x)$ ,  $Q(n)$ , etc.) y reescribe la proposición usando los símbolos  $\exists$ ,  $\exists!$  y  $\forall$  apropiadamente.

- a) Existe un número positivo  $x$  tal que  $x^2 = 5$ .
- b) Para cualquier  $n$ , el número  $2n + 1$  es impar.
- c) Para toda  $k$  existe  $t$  tal que  $t = \frac{1}{k}$ .
- d) Existe exactamente un número  $x$  tal que  $5 + x = 7$ .
- e) Para todo número positivo  $n$ , tenemos que  $n + 1 > n$ .

**Ejercicio 1.23.** Escribe la negación de cada una de las siguientes proposiciones.

- a)  $7 \leq 10$ .
- b) No es cierto que  $1 + 2 = 4$ .
- c) El cuadrado de 5 no es 16.
- d) Ningún político es honesto.
- e) Existe un político que es deshonesto.
- f) Para algún número real  $x$ , se cumple que  $x^2 + 3x - 2 = 0$ .
- g) Para cualquier número real  $x$ , se cumple que  $x + 1 \leq 0$ .
- h) Existe un número natural  $n$  tal que para todo número natural  $m$  se cumple que  $n \leq m$ .

**Ejercicio 1.24.** Determina el valor de verdad de cada una de las siguientes proposiciones, donde el universo de discurso es el conjunto de los números reales. Justifica tu respuesta.

- a)  $\forall x$  tenemos que  $x \neq \pi$ .
- b)  $\exists x$  tal que  $0 \leq x \leq 1$ .
- c)  $\forall x, \forall y$  tenemos que  $xy > 0$ .
- d)  $\forall x, \exists y$  tal que  $x + y = 0$ .
- e)  $\forall x, \exists y$  tal que  $\frac{x}{y} = 1$ .

**Ejercicio 1.25.** Escribe la negación de cada una de las proposiciones del ejercicio 1.24.

## 1.3 Conectivos

En lógica existe una colección de palabras y símbolos, llamados *conectivos lógicos*, que se usan para asociar distintas proposiciones. Los conectivos de uso más frecuente son las *conjunciones*, *disyunciones*, *condicionales* y *bicondicionales*; cada uno de éstos tiene asociada una proposición compuesta.

Supongamos que  $P$  y  $Q$  son proposiciones cualesquiera. La siguiente tabla establece el símbolo usado para cada conectivo y su significado.

Nombre	Símbolo	Proposición	Significado
Conjunción	$\wedge$	$P \wedge Q$	$P$ y $Q$
Disyunción	$\vee$	$P \vee Q$	$P$ o $Q$
Condional	$\Rightarrow, \rightarrow$	$P \Rightarrow Q$	si $P$ , entonces $Q$
Bicondicional	$\Leftrightarrow, \leftrightarrow$	$P \Leftrightarrow Q$	$P$ si y sólo si $Q$

Tabla 1.2: Conectivos lógicos

En las siguientes secciones estudiaremos cada uno de estos conectivos.

### 1.3.1 Conjunción y disyunción

Si  $P$  y  $Q$  son proposiciones cualesquiera, la proposición compuesta  $P \wedge Q$  es llamada la **conjunción** de  $P$  y  $Q$ , y afirma simultáneamente lo que  $P$  y  $Q$  afirman. Veamos algunos ejemplos.

**Ejemplo 1.26.** Consideremos las proposiciones

$$P = (5 \text{ es impar}) \text{ y } Q = (5 \text{ es primo}),$$

entonces

$$P \wedge Q = (5 \text{ es impar y primo}).$$

Por razones de estilo, en ciertas ocasiones, en lugar del vocablo “y” se utilizan las palabras “pero” o “sin embargo”.

**Ejemplo 1.27.** La conjunción de las proposiciones “Los cuadrados tienen cuatro lados” y “Los triángulos tienen tres lados” es

“Los cuadrados tienen cuatro lados, pero los triángulos tres”.

Como observamos en los ejemplos anteriores, el conectivo  $\wedge$  es *conmutativo* en el sentido de que no importa el orden en el que aparezcan las proposiciones; en otras palabras,

$$P \wedge Q \equiv Q \wedge P.$$

Además, la conjunción es *asociativa* ya que, al combinar tres proposiciones  $P$ ,  $Q$  y  $T$ , tenemos que

$$(P \wedge Q) \wedge T \equiv P \wedge (Q \wedge T).$$

**Ejemplo 1.28.** Sean  $P$  y  $Q$  las proposiciones del ejemplo 1.26, y sea

$$T = (5 \text{ es un número entero}).$$

Ahora podemos observar que las proposiciones

$$(P \wedge Q) \wedge T = (5 \text{ es un número impar y primo, y entero}),$$

$$P \wedge (Q \wedge T) = (5 \text{ es un número impar, y primo y entero})$$

tienen el mismo significado.

**Ejemplo 1.29.** La conjunción de las proposiciones  $L = (6 = 3 \times 3)$  y  $M = (6 = 3 + 3)$  es

$$L \wedge M = (6 = 3 \times 3 \text{ y } 6 = 3 + 3) \equiv (3 \times 3 = 3 + 3).$$

En este caso  $L \wedge M$  es una proposición falsa debido a que  $L$  es falsa.

El ejemplo anterior nos sugiere que la conjunción de dos proposiciones es verdadera exclusivamente cuando ambas proposiciones son verdaderas; si al menos una de las proposiciones es falsa, entonces su conjunción también es falsa. La información sobre el valor de verdad de la conjunción queda claramente establecida en la tabla 1.3, en donde  $P$  y  $Q$  son proposiciones arbitrarias.

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

Tabla 1.3: Conjunción



La proposición  $P \vee Q$  es llamada la **disyunción** de  $P$  y  $Q$ , y afirma que es cierto lo que manifiesta al menos una de las proposiciones  $P$  o  $Q$ .

En lógica, el uso del vocablo “o” difiere de su uso en el lenguaje cotidiano. Cuando representa una disyunción, “o” significa “uno u otro, o ambos”. La interpretación como “uno u otro, pero no ambos” se denomina *disyunción exclusiva*, y su uso es poco común; se emplea más en estudios de informática.

El valor de verdad de la disyunción se localiza en la tabla 1.4, donde  $P$  y  $Q$  son proposiciones arbitrarias.

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

Tabla 1.4: Disyunción

Como en el caso de la conjunción, la disyunción también es conmutativa y asociativa:

$$P \vee Q \equiv Q \vee P,$$

$$(P \vee Q) \vee T \equiv P \vee (Q \vee T).$$

**Ejemplo 1.30.** Sean

$$K = (\text{El sol es una estrella})$$

$$W = (\text{El sol es un planeta}).$$

La disyunción de estas proposiciones es

$$K \vee W = (\text{El sol es una estrella o un planeta}).$$

En este caso,  $K \vee W$  es verdadera debido a que  $K$  es verdadera.

**Ejemplo 1.31.** Sean

$$J = (12 \text{ es un múltiplo de } 3)$$

$$G = (12 \text{ es un múltiplo de } 2).$$

Entonces, la disyunción

$$J \vee G = (12 \text{ es un múltiplo de } 3 \text{ o de } 2)$$

es verdadera debido a que ambas,  $J$  y  $G$ , son verdaderas.

**Ejemplo 1.32.** Sean

$$A = (8 \text{ es impar}) \text{ y } B = (2 + 2 = 5).$$

La disyunción

$$A \vee B = (8 \text{ es impar o } 2 + 2 = 5)$$

es falsa ya que ambas  $A$  y  $B$  son proposiciones falsas.

### 1.3.2 Condicional y bicondicional

Las proposiciones condicionales son las más importantes por su papel en la argumentación. A la proposición compuesta formada por un condicional se le llama *implicación*.

En la fórmula  $P \Rightarrow Q$ , la proposición  $P$  se denomina *hipótesis*, o *antecedente*, de la implicación, mientras que la proposición  $Q$  se llama *consecuente*, o *conclusión*, de la implicación. De esta forma,  $P \Rightarrow Q$  expresa que si la hipótesis es verdadera, entonces la conclusión es verdadera. El valor de verdad correspondiente a la implicación se muestra en la tabla 1.5.

$P$	$Q$	$P \Rightarrow Q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$V$
$F$	$F$	$V$

Tabla 1.5: Implicación

Existen diversas formas de expresar la implicación  $P \Rightarrow Q$  con palabras. Algunas de las más comunes son:

- 1) Si  $P$ , entonces  $Q$ .
- 2)  $P$  implica  $Q$ .
- 3)  $P$  es suficiente para  $Q$ .
- 4)  $Q$  es necesario para  $P$ .
- 5)  $Q$  si  $P$ .
- 6)  $Q$  cuando  $P$ .
- 7)  $P$  sólo si  $Q$ .

**Ejemplo 1.33.** Consideremos las proposiciones

$$P = (\text{Ser tapatío}),$$

$$Q = (\text{Ser mexicano}).$$

Las distintas formas de escribir  $P \Rightarrow Q$  son:

- 1) Si es tapatío, **entonces** es mexicano.
- 2) Ser tapatío **implica** ser mexicano.
- 3) Ser tapatío **es suficiente para** ser mexicano.
- 4) Ser mexicano **es necesario para** ser tapatío.
- 5) Es mexicano **si** es tapatío.
- 6) Es mexicano **cuando** es tapatío.
- 7) Es tapatío **sólo si** es mexicano.

Todos los enunciados anteriores son equivalentes.

**Ejemplo 1.34.** Algunos otros ejemplos de proposiciones condicionales son los siguientes. ¿Puedes identificar cuál es el antecedente y el consecuente?

- 1) Si  $x = 4$ , **entonces**  $x$  es un número par.
- 2) Que  $\theta = \pi$  es **suficiente** para que  $\sin(\theta) = 0$ .
- 3) El  $\log w$  existe **cuando**  $w$  es un número real positivo diferente de cero.

**Ejemplo 1.35.** En ocasiones las implicaciones involucran cuantificadores universales que no aparecen escritos explícitamente en su interpretación en español. Por ejemplo, en la proposición

“Si  $x$  es mayor que 1, entonces  $x^2$  es mayor que 1”,

el significado que se pretende establecer es

$$\forall x \left[ (x > 1) \Rightarrow (x^2 > 1) \right].$$

En general, si usamos una variable en el antecedente de una implicación, asumiremos que hay un cuantificador universal implícito.

Tal como su tabla de verdad lo indica, una implicación sólo es falsa cuando el antecedente es verdadero y el consecuente es falso.

Para ilustrar esto, consideremos la proposición

*“Si lees este libro, entonces aprenderás matemáticas”.*

Lo que afirma esta proposición está restringido al caso en el que lees este libro. No establece nada si no lo lees: puedes o no aprender matemáticas por otros medios. Por lo tanto, la proposición sólo es falsa en caso de que leas el libro y no aprendas matemáticas.

Sin embargo, el significado del “si-entonces” usado en español en ocasiones difiere del conectivo lógico  $\Rightarrow$ . Por ejemplo, de acuerdo con su tabla de verdad, proposiciones como

(Si las vacas vuelan)  $\Rightarrow$  (Yo soy Superman),

son verdaderas porque el antecedente es falso. Es importante comprender que  $\Rightarrow$  está definido formalmente como su tabla de verdad lo indica, aunque esto no siempre se corresponda con nuestra intuición en los lenguajes naturales.

**Definición 1.36 (implicación recíproca).** Sean  $P$  y  $Q$  proposiciones. La implicación

$$Q \Rightarrow P,$$

se llama *implicación recíproca* de  $P \Rightarrow Q$ .

**Definición 1.37 (implicación contrapuesta).** Sean  $P$  y  $Q$  proposiciones. La implicación

$$(\sim Q) \Rightarrow (\sim P),$$

se llama *implicación contrapuesta* de  $P \Rightarrow Q$ .

En general, que una implicación sea verdadera no significa que su recíproca debe ser verdadera. Por ejemplo, la implicación “si  $x = 0$ , entonces  $x$  es un número” es verdadera; sin embargo, la implicación recíproca “si  $x$  es un número, entonces  $x = 0$ ” es falsa.

Por otro lado, el valor de verdad de una implicación sí es equivalente al valor de verdad de su implicación contrapuesta: ambas proposiciones son lógicamente equivalentes. Demostraremos este hecho más adelante, en la sección 1.3.3.

La proposición formada con un conectivo **bicondicional** es llamada *equivalencia*, la cual se obtiene como la conjunción de una implicación con su recíproca; en otras palabras:

$$P \Leftrightarrow Q \text{ corresponde a } (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

En la representación escrita, usamos los vocablos “si y sólo si” o “es necesario y suficiente” para representar el bicondicional.

**Ejemplo 1.38.** Algunos ejemplos de equivalencias son las proposiciones siguientes.

- 1) Un triángulo es isósceles *si y sólo si* dos de sus lados tienen el mismo tamaño.
- 2) Para que su mamá lleve al cine a Pepe es *necesario y suficiente* que éste termine su tarea.
- 3) Una persona tiene ojos zarcos *si y sólo si* sus ojos son color azul claro.

Si  $P$  y  $Q$  son proposiciones arbitrarias, el valor de verdad de la equivalencia  $P \Leftrightarrow Q$  se localiza en la tabla 1.6.

$P$	$Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
$V$	$V$	$V$	$V$	$V$
$V$	$F$	$F$	$V$	$F$
$F$	$V$	$V$	$F$	$F$
$F$	$F$	$V$	$V$	$V$

Tabla 1.6: Equivalencia

Como podemos observar, una equivalencia es verdadera exactamente cuando ambos  $P$  y  $Q$  tienen el mismo valor de verdad (ya sean ambos verdaderos o falsos).

**Ejemplo 1.39.** La equivalencia

“Una persona es mexicana si y sólo si nació en México”

es falsa porque hay personas mexicanas que no nacieron en México.

Haremos una aclaración con respecto a la formulación de definiciones. En matemáticas, una definición es una proposición inequívoca que establece el significado preciso de una palabra, frase, concepto o símbolo matemático. Siempre asumimos que el valor de verdad de una definición es verdadero. Por razones de estilo, enunciamos las definiciones como implicaciones, aunque su significado real es el de una equivalencia. Por ejemplo, consideremos la siguiente definición.

**Definición 1.40 (número par).** Un número entero  $n$  es par si  $n = 2k$ , para algún número entero  $k$ .

La formulación anterior podría hacer pensar al lector que existen números pares que no son de la forma  $n = 2k$ . Sin embargo, esto no es así; la definición anterior establece un significado preciso y total, cuya traducción en símbolos es

$$\forall n [(n \text{ es par}) \Leftrightarrow (\exists k (n = 2k))].$$

### 1.3.3 Tautologías y contradicciones

Decimos que una proposición compuesta es una *tautología* cuando es verdadera en todas las entradas de su tabla de verdad. Por otro lado, decimos que se trata de una *contradicción* si la proposición es falsa en todas las entradas de su tabla de verdad.

**Ejemplo 1.41.** Sea  $P$  una proposición. La proposición compuesta

$$P \vee (\sim P)$$

es una tautología porque siempre es verdadera, independientemente del valor de verdad que tome  $P$  (ejercicio 1.46).

**Ejemplo 1.42.** La proposición compuesta

$$P \wedge (\sim P)$$

es una contradicción, porque siempre es falsa, independientemente del valor de verdad que tome  $P$  (ejercicio 1.46).

Cuando una equivalencia  $A \Leftrightarrow B$  es una tautología, decimos que las proposiciones  $A$  y  $B$  son *lógicamente equivalentes*; en tal caso, escribimos  $A \equiv B$ .

Por ejemplo, sean  $P$  y  $Q$  proposiciones cualesquiera, y consideremos las proposiciones compuestas

$$A = \sim[P \wedge (\sim Q)] \text{ y } B = (P \Rightarrow Q).$$

La tabla de verdad correspondiente en esta situación es:

$P$	$Q$	$A$	$B$
$V$	$V$	$V$	$V$
$V$	$F$	$F$	$F$
$F$	$V$	$V$	$V$
$F$	$F$	$V$	$V$

Ambas proposiciones,  $A$  y  $B$ , tienen siempre los mismos valores de verdad independientemente del valor de  $P$  y  $Q$ ; en otras palabras, la tabla de verdad de la proposición bicondicional  $A \Leftrightarrow B$  es una tautología:

$P$	$Q$	$A \Leftrightarrow B$
$V$	$V$	$V$
$V$	$F$	$V$
$F$	$V$	$V$
$F$	$F$	$V$

Con referencia a lo mencionado hemos demostrado que  $A$  y  $B$  son lógicamente equivalentes:

$$\sim(P \wedge \sim Q) \equiv (P \Rightarrow Q).$$

La técnica descrita en los párrafos anteriores nos permite encontrar muchas proposiciones lógicamente equivalentes. Terminamos esta sección demostrando lo siguiente.

**Proposición 1.43.** Cualquier implicación es lógicamente equivalente a su contrapuesta. En otras palabras, si  $P$  y  $Q$  son proposiciones cualesquiera, entonces

$$(P \Rightarrow Q) \equiv [(\sim Q) \Rightarrow (\sim P)].$$

**Demostración.** Construyamos la tabla de verdad correspondiente:

$P$	$Q$	$\sim Q$	$\sim P$	$P \Rightarrow Q$	$(\sim Q) \Rightarrow (\sim P)$
$V$	$V$	$F$	$F$	$V$	$V$
$V$	$F$	$V$	$F$	$F$	$F$
$F$	$V$	$F$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$V$	$V$

La implicación  $P \Rightarrow Q$  y su contrapuesta siempre tienen los mismos valores de verdad. Por lo tanto, la proposición bicondicional

$$(P \Rightarrow Q) \Leftrightarrow [(\sim Q) \Rightarrow (\sim P)]$$

es una tautología. ■

**Palabras clave de la sección:** conjunción, disyunción, condicional, implicación recíproca y contrapuesta, bicondicional, equivalencia, tautología y contradicción.

### 1.3.4 Ejercicios de conectivos

**Ejercicio 1.44.** En cada una de las siguientes implicaciones, identifica el antecedente y el consecuente, y escribe las implicaciones recíproca y contrapuesta.

- a)  $2n + 1$  es un número impar cuando  $n$  es un número entero.
- b) Puedes trabajar aquí sólo si tienes un título universitario.
- c) Es necesario que tengas gasolina para que tu automóvil encienda.
- d) Una función es continua si es diferenciable.

**Ejercicio 1.45.** Considera los predicados

$$P(x) = (x \text{ es par}), \quad Q(x) = (x \text{ es múltiplo de } 3),$$

$$T(x) = (x \text{ es múltiplo de } 6).$$

Reescribe cada una de las siguientes proposiciones usando los predicados anteriores junto con los símbolos  $\sim$ ,  $\wedge$ ,  $\vee$ ,  $\Rightarrow$  y  $\Leftrightarrow$ .

- a)  $x$  no es múltiplo de 3 o  $x$  es par.
- b) Si  $x$  es múltiplo de 6, entonces  $x$  es par.
- c)  $x$  es múltiplo de 6 si y sólo si  $x$  es par y múltiplo de 3.
- d) Si  $x$  es múltiplo de 3, entonces  $x$  es impar o es múltiplo de 6.

**Ejercicio 1.46.** Escribe las tablas de verdad de  $P \vee (\sim P)$  y  $P \wedge (\sim P)$ , donde  $P$  es una proposición cualquiera.

**Ejercicio 1.47.** Sean  $P$  y  $Q$  proposiciones. Construye una tabla de verdad para demostrar que las siguientes proposiciones son lógicamente equivalentes.

- a)  $\sim(P \wedge Q) \equiv [(\sim P) \vee (\sim Q)]$ .
- b)  $\sim(P \vee Q) \equiv [(\sim P) \wedge (\sim Q)]$ .
- c)  $\sim(P \Rightarrow Q) \equiv [P \wedge (\sim Q)]$ .
- d)  $\sim(\sim P) \equiv P$ .

**Ejercicio 1.48.** Usa las equivalencias del ejercicio anterior para escribir la negación de cada una de las siguientes proposiciones.

- a) Siete es un número primo o  $2 + 2 = 4$ .
- b) Si  $M$  es acotado, entonces  $M$  es compacto.
- c) Si las rosas son rojas y las violetas azules, entonces te amo.



## 1.4 Métodos de demostración

La lógica se interesa en los métodos y principios que permiten distinguir un razonamiento correcto de uno incorrecto. A una proposición verdadera de la cual no se tiene evidencia directa se le llama *teorema*. A la argumentación que comprueba la validez de un teorema mediante un proceso de inferencia o deducción lógica se le llama *demostración*.

En una demostración, la verdad de cualquier enunciado debe poder rastrearse hasta algún conjunto de conceptos y proposiciones iniciales. A estas proposiciones iniciales en una teoría matemática se les llama *axiomas* o *postulados*, las cuales se aceptan como verdaderas sin necesidad de ser demostradas. En cierta forma, los axiomas representan las reglas iniciales del “juego matemático” de demostrar teoremas. Hay también un conjunto de conceptos primitivos llamados *términos indefinidos*, a partir de los cuales se definen o deducen conceptos nuevos.

Típicamente, un teorema es una implicación

$$P \Rightarrow Q,$$

donde  $P$  es llamada la *hipótesis del teorema* y  $Q$  es la *conclusión del teorema*. Para demostrar su validez, suponemos siempre que la hipótesis  $P$  es verdadera (si  $P$  fuera falsa, sabemos, por su tabla de verdad, que la implicación es verdadera) y deducimos que la conclusión  $Q$  es verdadera (si  $Q$  es falsa, la implicación es falsa). Esta argumentación se realiza encontrando una secuencia de proposiciones verdaderas

$$P_1, P_2, \dots, P_m$$

tales que  $P_m = Q$  es la conclusión del teorema y puede deducirse de las proposiciones anteriores, las cuales son llamadas *premisas del argumento*. Se acostumbra que  $P_1 = P$  sea la hipótesis del teorema, mientras que las otras premisas pueden ser:

- 1) Definiciones de conceptos.
- 2) Axiomas o postulados.
- 3) Teoremas demostrados previamente.
- 4) Proposiciones que son consecuencia inmediata de las premisas anteriores.

Al construir una demostración, no hay una regla para saber qué eslabón debe emplearse en cada paso. La práctica, sin duda, ayudará al estudiante a desarrollar las habilidades e intuición necesarias para encontrar el camino adecuado.

A continuación estudiamos algunos ejemplos particulares. Recordemos que un *ángulo agudo* es un ángulo menor que  $90^\circ$ .

**Teorema 1.49.** Si  $\theta = 45^\circ$ , entonces  $\theta$  es un ángulo agudo.

**Demostración.** La cadena de premisas es:

- $(P_1)$   $\theta = 45^\circ$  (hipótesis del teorema).
- $(P_2)$  Un ángulo agudo es menor que  $90^\circ$  (definición de ángulo agudo).
- $(P_3)$   $45^\circ < 90^\circ$  (definición del orden de los números).
- $(P_4)$   $\theta$  es un ángulo agudo (conclusión del teorema, deducida de  $P_1, P_2$  y  $P_3$ ). ■

**Teorema 1.50.** Si  $n$  y  $m$  son dos números pares, entonces  $n + m$  es un número par.

Este teorema involucra un cuantificador universal implícito, el cual aparece en su traducción simbólica:

$$\forall m, n [(n, m \text{ son pares}) \Rightarrow (n + m \text{ es par})].$$

Las demostraciones de este tipo de teoremas se construyen con las condiciones abiertas, para variables arbitrarias. Evidentemente, hay que asegurarse de que cada paso de la demostración sea válido para todos los valores posibles de las variables.

**Demostración.** Primero establecemos las variables: sean  $n$  y  $m$  números enteros. La cadena de premisas es:

- $(P_1)$   $n$  y  $m$  son números pares (hipótesis del teorema).
- $(P_2)$  Un entero  $x$  es par si  $x = 2k$ , para algún entero  $k$  (definición 1.40 de número par).
- $(P_3)$   $n = 2k_1$  y  $m = 2k_2$ , para algunos enteros  $k_1$  y  $k_2$  (deducida de  $P_1$  y  $P_2$ ).
- $(P_4)$  Si  $x, y, z$  son números enteros, entonces  $xy + xz = x(y + z)$  (propiedad distributiva de los números enteros).
- $(P_5)$   $n + m = 2k_1 + 2k_2 = 2(k_1 + k_2)$  (deducida de  $P_3$  y  $P_4$ ).

( $P_6$ )  $n + m$  es un número par (conclusión del teorema, deducida de  $P_5$  y  $P_2$ ). ■

**Teorema 1.51.** Para todo número real  $x$ , si  $x > 1$ , entonces  $x^2 > x$ .

**Demostración.** Sea  $x$  un número real.

( $P_1$ )  $x > 1$  (hipótesis del teorema).

( $P_2$ )  $1 > 0$  (orden de los números).

( $P_3$ )  $x > 0$  (deducida de  $P_1$  y  $P_2$ ).

( $P_4$ ) Si  $a > 0$  y  $c > d$ , entonces  $ac > ad$  (teorema de desigualdades).

( $P_5$ )  $x^2 > x$  (conclusión del teorema, deducida de  $P_1$ ,  $P_3$  y  $P_4$ ). ■

Para demostrar un teorema con cuantificador existencial es suficiente con describir un objeto del universo de discurso que lo haga verdadero. En otras palabras, la mejor forma de demostrar que algo existe es encontrando un ejemplar.

**Ejemplo 1.52.** Consideremos los siguientes ejemplos:

- 1) El teorema “Existe un número real  $z$  tal que  $z^2 + 2z + 1 = 4$ ” es verdadero porque 1 es un ejemplar.
- 2) El teorema “Existe un número entero par que es primo” es verdadero porque 2 es un ejemplar.

Veamos otro teorema un poco más complicado.

**Teorema 1.53.** Si el número  $r$  es una raíz del polinomio

$$g(x) = x^2 + x + 1,$$

entonces  $x - r$  es un factor de  $g(x)$ .

Por definición, un polinomio  $h(x)$  es factor de  $g(x)$  si podemos encontrar un polinomio  $f(x)$  tal que  $g(x) = h(x)f(x)$ . Decimos que un número  $r$  es una raíz de  $h(x)$  si  $h(r) = 0$ .

**Demostración.** La cadena de premisas es:

( $P_1$ ) El número  $r$  es una raíz de  $g(x)$  (hipótesis del teorema).

( $P_2$ )  $g(r) = r^2 + r + 1 = 0$  (por  $P_1$  y la definición de raíz).

( $P_3$ )  $g(x) - g(r) = (x^2 + x + 1) - (r^2 + r + 1)$  (por la definición de  $g(x)$ ).

( $P_4$ )  $g(x) - g(r) = (x^2 - r^2) + (x - r)$  (reordenando los términos en  $P_3$ ).

( $P_5$ )  $g(x) - g(r) = (x + r)(x - r) + (x - r)$  (por  $P_4$  y la identidad “diferencia de cuadrados”).

( $P_6$ )  $g(x) - g(r) = (x - r)[(x + r) + 1]$  (factorizando el lado derecho de la igualdad en  $P_5$ ).

( $P_7$ )  $g(x) = g(x) - g(r) = (x - r)[(x + r) + 1]$  (por  $P_2$  y  $P_6$ ).

( $P_8$ )  $x - r$  es un factor de  $g(x)$  (conclusión del teorema, deducida de  $P_7$  y la definición de factor). ■

En la práctica no escribimos las demostraciones como una cadena explícita de proposiciones. Usualmente las demostraciones son escritas lenguaje común y es trabajo del lector identificar cada premisa.

La técnica para hacer demostraciones estudiada anteriormente se llama *demostración directa*. Existen otras estrategias más convenientes en distintas situaciones, dependiendo de la formulación del teorema. Algunas de estas estrategias son: la *demostración por contraejemplo*, la *demostración por contraposición* y la *reducción al absurdo*. A continuación estudiaremos más a detalle cada una de estas técnicas.

### 1.4.1 Contraejemplo y contraposición

La idea de la **demostración por contraejemplo** es deducir que una proposición es falsa localizando un ejemplo que la refute.

**Proposición 1.54.** Es falso que si  $m$  y  $n$  son enteros positivos y cuadrados perfectos, entonces la suma  $m + n$  es un cuadrado perfecto.

**Demostración.** Los enteros positivos 16 y 25 son cuadrados perfectos, cuya suma  $16 + 25 = 41$  no es un cuadrado perfecto. La proposición queda demostrada. ■

En el ejemplo anterior usamos la palabra “proposición” en lugar de “teorema”. El uso de estos términos para etiquetar distintos resultados es subjetivo; en general, reservamos la palabra “teorema” para resultados menos evidentes.

La **demostración por contraposición** usa el hecho de que una implicación es lógicamente equivalente a su contraposición (proposición 1.43).

**Proposición 1.55.** Si  $7m$  es un número impar, entonces  $m$  es un número impar.

**Demostración.** La proposición contrapuesta es: “Si  $m$  es un número par, entonces  $7m$  es un número par”. La cadena de premisas para demostrar esto es:

- $(P_1)$   $m$  es un número par (hipótesis de la contrapuesta).
- $(P_2)$   $m = 2k$  para algún entero  $k$  (por  $P_1$  y la definición de par).
- $(P_3)$   $7m = 7(2k)$  (por  $P_2$ ).
- $(P_4)$   $7m = 2(7k)$  (por  $P_3$  y las propiedades conmutativa y asociativa).
- $(P_5)$   $7m$  es un número par (conclusión de la contrapuesta, por  $P_4$  y la definición de par).

Esto demuestra la contrapuesta y, por equivalencia lógica, la proposición original también queda demostrada. ■

La ventaja de trabajar con la proposición contrapuesta en el ejemplo anterior se debe a que, en general, es más sencillo trabajar con números pares que con números impares. Así pues, usar la demostración por contrapuesta en  $P \Rightarrow Q$  es especialmente útil cuando resulte más fácil hacer deducciones partiendo de  $\sim Q$  que de la hipótesis  $P$ .

### 1.4.2 Reducción al absurdo

La técnica de reducción al absurdo usa un poderoso argumento que surgió en la filosofía griega hace cientos de años. La estrategia se basa en demostrar que una proposición es verdadera mostrando que asumir su falsedad implica una contradicción (de manera similar, podemos demostrar que una proposición es falsa mostrando que asumir su veracidad implica una contradicción). El fundamento lógico de esta estrategia es que una proposición debe ser, inevitablemente, falsa o verdadera, pero no ambas a la vez. Por lo tanto, si suponer que  $\sim P$  es verdadera (es decir,  $P$  es falsa) nos conduce a una contradicción, entonces  $P$  tiene que ser verdadera.

Veamos el mecanismo de esta estrategia.

**Teorema 1.56.** Si  $x$  es un número real, entonces  $x^2 \neq -1$ .

**Demostración.** Por el ejercicio 1.47 parte c), la negación del teorema es

“Existe un número real  $x$  tal que  $x^2 = -1$ ”.

Para usar la reducción al absurdo, supongamos que la negación del teorema es verdadera. Un teorema básico de los números reales establece que  $x^2 \geq 0$ . Entonces, nuestra suposición implica que  $-1 \geq 0$ , lo cual contradice el orden de los números reales. Por lo tanto, la negación es falsa y el teorema verdadero. ■

**Teorema 1.57.** El conjunto de enteros pares positivos es infinito.

**Demostración.** Supongamos que el conjunto de enteros pares positivos es *finito*. Entonces, podemos escribir una lista *completa* que contenga a todos los enteros pares positivos:  $n_1, n_2, n_3, \dots, n_r$ . Por el teorema 1.50, sabemos que  $n_1 + n_2 + n_3 + \dots + n_r$  también es un entero par positivo. Sin embargo, este número par no puede estar en nuestra lista, ya que es mayor que cada uno de sus elementos: esto contradice que nuestra lista sea completa. El teorema queda demostrado por reducción al absurdo. ■

La ventaja de usar la reducción al absurdo es que en algunas ocasiones resulta más sencillo trabajar con la negación de una proposición que con la proposición misma. Por ejemplo, en el teorema anterior no queda claro qué deducciones deben hacerse para demostrar directamente que el conjunto de enteros pares positivos es infinito; por otro lado, su negación nos permite hacer deducciones inmediatas.

### 1.4.3 Demostración de equivalencias

Para demostrar la equivalencia  $P \Leftrightarrow Q$ , es necesario demostrar la implicación  $P \Rightarrow Q$  y su recíproca  $Q \Rightarrow P$ , usando el método que sea más conveniente.

**Teorema 1.58.** Un número entero  $n$  es par si y sólo si  $n = 2m - 4$  para algún entero  $m$ .

**Demostración.** Sea  $n$  un número entero. Debemos demostrar ambas implicaciones:

- 1) Si  $n$  es par, entonces  $n = 2m - 4$  para algún entero  $m$ .
- 2) Si  $n = 2m - 4$  para algún entero  $m$ , entonces  $n$  es par.

Demostremos la primera implicación:

( $P_1$ )  $n$  es un número par (hipótesis de 1)).

( $P_2$ )  $n = 2k$  para algún entero  $k$  (por  $P_1$  y la definición de par).

( $P_3$ ) El entero  $m$  definido como  $m = k + 2$  existe (propiedad de los números enteros).

( $P_4$ )  $k = m - 2$  (por  $P_3$  y propiedad de la igualdad).

( $P_5$ )  $n = 2(m - 2)$  (por  $P_2$  y  $P_4$ ).

( $P_6$ )  $n = 2m - 4$  (conclusión de 1), por  $P_5$  y la propiedad distributiva de los enteros).

Ahora demostremos la segunda implicación:

( $Q_1$ )  $n = 2m - 4$  para algún entero  $m$  (hipótesis de 2)).

( $Q_2$ )  $n = 2(m - 2)$  (por  $Q_1$  y la propiedad distributiva).

( $Q_3$ )  $n$  es par (conclusión de 2), por  $Q_2$  y la definición de par). ■

**Palabras clave de la sección:** *teorema; hipótesis; conclusión; premisa; demostraciones directa, por contraejemplo y por contrapuesta; reducción al absurdo; demostración de equivalencias.*

### 1.4.4 Ejercicios de métodos de demostración

**Ejercicio 1.59.** Proporciona un contraejemplo de cada proposición:

- a) Todos los números pares son positivos.
- b) Todas las aves pueden volar.
- c) No existen números enteros que sean cuadrados perfectos cuya suma sea un cuadrado perfecto.

**Ejercicio 1.60.** Recordemos que un número entero  $n$  es impar si  $n = 2k + 1$ , para algún entero  $k$ . Demuestra de forma directa las siguientes proposiciones:

- a) La suma de dos números enteros impares es un entero par.
- b) La suma de un número entero par y uno impar es un entero impar.
- c) El producto de dos números enteros pares es un entero par.
- d) El producto de dos números enteros impares es un entero impar.

**Ejercicio 1.61.** Demuestra lo siguiente por reducción al absurdo:

- a) No existe un número real que sea el más pequeño.
- b) Hay un número infinito de enteros positivos.
- c) Para cualquier número real  $x$ , se cumple que  $\frac{1}{x} \neq 0$ .

**Ejercicio 1.62.** Supongamos que  $x_1$  y  $x_2$  son números reales. Usando la contrapuesta, demuestra que si  $x_1 \neq x_2$ , entonces  $3x_1 - 5 \neq 3x_2 - 5$ . Finalmente, demuestra que  $x_1 = x_2$  si y sólo si  $3x_1 - 5 = 3x_2 - 5$ .

**Ejercicio 1.63.** Demuestra que existe un número entero  $n$  tal que  $n^2 + \frac{3}{2}n = 1$ . ¿Es éste entero único?

**Ejercicio 1.64.** Sea  $x$  un número real. Demuestra que  $x$  es positivo si y sólo si  $17x$  es positivo.



## 1.5 Glosario

Aquí resumimos algunos conceptos usados frecuentemente en este capítulo. Algunos de estos términos (como *proposición*, *hipótesis* y *premisa*) tienen una definición precisa y objetiva, mientras que otros (como *teorema*, *lema* y *corolario*) son subjetivos y su uso depende, en parte, de la comunidad matemática.

- 1) **Axioma.** Proposición que, por acuerdo, se acepta como verdadera sin necesidad de ser demostrada.
- 2) **Conclusión.** La conclusión de una implicación es la proposición consecuente.
- 3) **Conjetura.** Proposición no demostrada, cuyo valor de verdad se desconoce, pero se cree que es verdadera.
- 4) **Corolario.** Proposición que se deduce fácilmente de un teorema ya demostrado.
- 5) **Definición.** Declaración inequívoca que establece el significado preciso de una palabra, frase, concepto o símbolo matemático.
- 6) **Demostración.** Secuencia de razonamientos que establecen la verdad o falsedad de una proposición.
- 7) **Hipótesis.** La hipótesis de una implicación corresponde a la proposición antecedente.
- 8) **Lema.** Proposición auxiliar que se prueba con anticipación para usarse en la demostración de uno o más teoremas.
- 9) **Proposición.** Oración declarativa que se puede clasificar como *verdadera* o *falsa*, pero no ambas. La característica de verdad o falsedad se denomina *valor de verdad* de la proposición.
- 10) **Proposición simple y compuesta.** Una proposición es *simple* si consta de un sujeto con un término singular. Una proposición es *compuesta* si involucra un cuantificador o si es una combinación de dos o más proposiciones simples.
- 11) **Premisa.** Proposición cuya validez ya ha sido establecida y se utiliza para deducir la verdad de algún teorema.
- 12) **Teorema.** Proposición demostrada como verdadera, la cual se considera importante para el desarrollo de una teoría.

## 1.6 Definiciones del capítulo

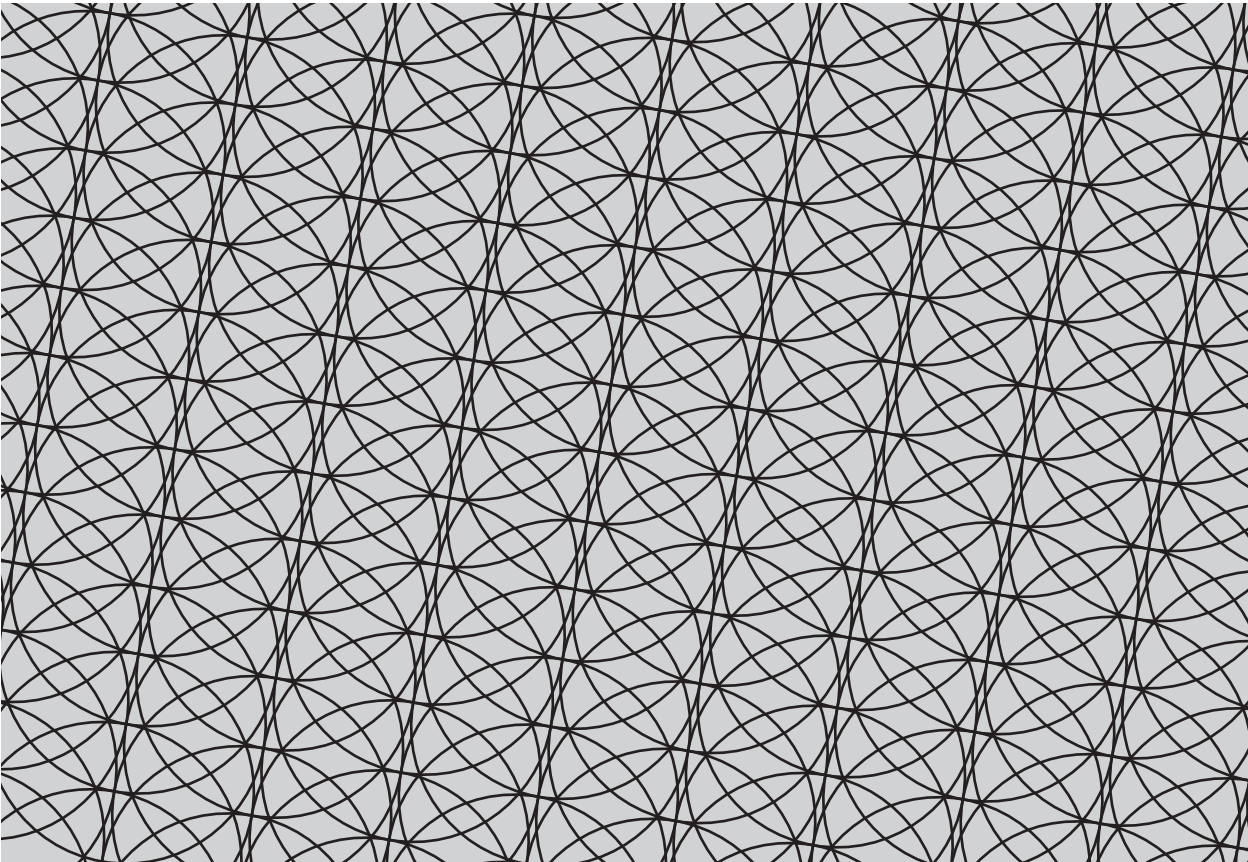
Escribe la definición y un ejemplo de cada uno de los conceptos enlistados a continuación.

- 1) Proposición.
- 2) Término singular.
- 3) Proposición simple.
- 4) Predicado.
- 5) Negación de una proposición.
- 6) Proposición con cuantificador existencial.
- 7) Proposición con cuantificador universal.
- 8) Conjunción de dos proposiciones.
- 9) Disyunción de dos proposiciones.
- 10) Implicación.
- 11) Recíproca.
- 12) Contrapuesta.
- 13) Equivalencia.
- 14) Tautología.
- 15) Contradicción.
- 16) Teorema.
- 17) Demostración.
- 18) Premisa.
- 19) Contraejemplo.
- 20) Reducción al absurdo.

*Un matemático, como un pintor o un poeta, es fabricante de modelos. Si sus modelos son más duraderos que los de estos últimos, es debido a que están hechos de ideas.*

G. H. Hardy, matemático inglés

## Capítulo 2. Conjuntos



El término *conjunto* se refiere a uno de los conceptos matemáticos fundamentales. Inevitablemente, se encuentra en todas las áreas de las matemáticas, desde las más aplicables, como la estadística y las ecuaciones diferenciales, hasta las más abstractas, como la topología y el álgebra. Sin embargo, por muchos años no existió una definición formal para este concepto.

Comenzamos en la sección 2.1 estudiando temas elementales relacionados con conjuntos, así como las paradojas que han surgido a lo largo de los años durante la búsqueda de una definición formal. En la sección 2.2 estudiamos tres conceptos básicos: igualdad de conjuntos, subconjuntos y cardinalidad. Finalmente, en la sección 2.3 estudiamos algunas de las operaciones básicas entre conjuntos, como la unión, la intersección, el complemento y el producto cartesiano.

## 2.1 Teorías de conjuntos

Comúnmente se dice que un conjunto es una colección *bien definida*. De acuerdo con esto, por ejemplo, las siguientes colecciones son conjuntos:

- La colección  $D$  de dígitos; es decir, los números 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9.
- La colección  $C$  de colores primarios: rojo, verde y azul.
- La colección  $T$  de todas las personas.

Las anteriores son colecciones bien definidas porque podemos decir con exactitud qué objetos pertenecen a ellas, y qué objetos no pertenecen a ellas. Sabemos que 3 pertenece a  $D$  pero que 15 no pertenece; sabemos que el color rojo pertenece a  $C$ , pero que el rosa no pertenece.

Por otro lado, la colección de “buenos estudiantes” no es una colección bien definida: la propiedad de ser buen estudiante no se ha establecido con claridad y por lo tanto, si examinamos a un estudiante cualquiera, no podemos determinar de manera concisa si pertenece o no a nuestra colección.

Es costumbre usar las llaves  $\{, \}$  para enlistar los elementos de un conjunto. De esta manera, escribimos al conjunto de colores primarios como

$$C = \{\text{rojo, verde, azul}\},$$

y al conjunto de dígitos como

$$D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Con esta notación, el orden en el que aparecen los elementos del conjunto no importa, ya que esto no altera los objetos que lo definen. Así pues, también podemos escribir a  $D$  como

$$D = \{7, 2, 1, 9, 5, 4, 0, 3, 6, 8\}.$$

Cada miembro que pertenece a un conjunto debe estar representado sólo una vez; la repetición de elementos no define nada nuevo. Así pues, por ejemplo,  $\{1, 1, 2\} = \{1, 2\}$ .

Cuando enlistamos los elementos de un conjunto, como en el párrafo anterior, decimos que el conjunto está dado por *extensión*. Sin embargo, esto es problemático en algunas situaciones: por ejemplo, enlistar los elementos del conjunto  $T$  de todas las personas es demasiado laborioso. En lugar de esto, es posible denotar un conjunto expresando la propiedad que deben cumplir sus elementos. Por ejemplo,

$$T = \{x : x \text{ es una persona}\}.$$

Los dos puntos se leen con la frase “tal que”. En estos casos decimos que el conjunto está dado por *comprensión*. En general, si  $P(x)$  es un predicado, podemos formar el conjunto  $\{x : P(x)\}$ .

Para expresar que un objeto *pertenece* a un conjunto usamos el símbolo  $\in$ , mientras que para expresar que un objeto *no pertenece* a un conjunto usamos  $\notin$ . Así, por ejemplo,  $4 \in D$  pero  $11 \notin D$ .

No hay restricciones para el tipo de elementos que conforman un conjunto siempre y cuando la colección esté bien definida. Por ejemplo, el conjunto

$$F = \{\clubsuit, \text{Juan}, x^2 + 3, \{1, 2\}\}$$

contiene cuatro elementos, todos de distinta índole: el símbolo de trébol  $\clubsuit$ , el nombre *Juan*, el polinomio  $x^2 + 3$  y el conjunto  $\{1, 2\}$ . Una advertencia sobre este último punto: el conjunto  $F$  contiene al conjunto  $\{1, 2\}$  y no a los números 1 y 2. En otras palabras,  $\{1, 2\} \in F$ , pero  $1 \notin F$  y  $2 \notin F$ . Es una diferencia sutil, pero importante.

A simple vista podría parecer que nuestra definición de conjunto es adecuada y no causará problemas. Así lo creyeron los matemáticos durante muchos siglos. Pero en el primer año del siglo XX, el matemático británico Bertrand Russell descubrió una *paradoja*: esto es, una contradicción verdadera, lo cual no puede ser posible porque las contradicciones siempre son falsas. La existencia de paradojas indica que una teoría no está bien sustentada en la lógica matemática. De esta forma, la paradoja de Russell puso en duda la validez de la teoría de conjuntos que se conocía en aquellos años.

Antes de explicar la paradoja de Russell, veamos un ejemplo clásico, la llamada paradoja del mentiroso:

Esta afirmación es falsa.

La afirmación de arriba es una paradoja ya que su veracidad implica su falsedad y viceversa, lo cual es una contradicción (ver ejercicio 2.4).

- Supongamos que la afirmación es verdadera. Entonces, es verdad lo que dice: es verdad que la afirmación es falsa.
- Supongamos que la afirmación es falsa. Entonces, lo que dice es falso; es decir, no es verdad que la afirmación sea falsa. Por lo tanto, la afirmación es verdadera.

Para evitar caer en paradojas, los matemáticos del siglo XX se han esforzado en crear sistemas lógicos que no permitan formular afirmaciones válidas y contradictorias. En particular, la paradoja del mentiroso fue solucionada por el matemático polaco Alfred Tarski en su teorema de la indefinibilidad.

La paradoja de Russell se originó con la creación de una colección problemática de objetos: la colección  $X$  de todos los conjuntos que no son miembros de sí mismos. Primero entenderemos lo que significa esto. Claramente, hay conjuntos que no son miembros de sí mismos; por ejemplo, el conjunto de dígitos  $D$  no es miembro de sí mismo ( $D \notin D$ ). Por otro lado, si definimos a  $D'$  como la colección de objetos matemáticos que no son dígitos, entonces  $D' \in D'$ , porque  $D'$  es un objeto matemático que no es un dígito.

No es difícil convencerse de que, bajo nuestra definición inicial,  $X$  es una colección bien definida. Es importante notar que  $X$  es una *colección de conjuntos*; es decir, todos los miembros de  $X$  son conjuntos en sí mismos. Por comprensión, escribimos  $X$  como

$$X = \{A : A \text{ es un conjunto y } A \notin A\}.$$

Por nuestra discusión del párrafo anterior, sabemos que  $D \in X$  mientras que  $D' \notin X$ . Sin embargo, las dificultades surgen cuando nos preguntamos si  $X \in X$  o  $X \notin X$ .

- Si  $X \in X$ , entonces  $X$  debe satisfacer la propiedad que lo define, es decir,  $X$  debe ser un conjunto tal que  $X \notin X$ .
- Si  $X \notin X$ , entonces  $X$  es un conjunto tal que  $X \notin X$ . Por la propiedad que lo define, debemos tener que  $X \in X$ .

Las líneas anteriores demuestran que la proposición

$$(X \in X) \Leftrightarrow (X \notin X)$$

es verdadera, pero, por el ejercicio 2.4, esto debe ser una contradicción. De esta forma, Russell creó un conjunto imposible: un objeto que pone en duda la teoría de conjuntos definida en esta sección.

Como era de esperarse, la paradoja de Russell conmocionó a la comunidad matemática, la cual hizo esfuerzos por reparar la falla. Se definió el concepto de conjunto usando la lógica formal, y se estableció una serie de reglas (*axiomas*) que todos los conjuntos debían satisfacer. Para evitar paradojas como la de Russell, se estableció que un conjunto nunca debía contenerse a sí mismo, y que colecciones de conjuntos “excesivamente grandes” no forman conjuntos.<sup>1</sup> De esta manera, colecciones como  $D'$  y  $X$  no son consideradas conjuntos. Con estas reglas, surgió una rama de las matemáticas llamada *teoría axiomática de conjuntos*, la cual contrasta con el estudio intuitivo de los conjuntos usado anteriormente. Normalmente, la teoría axiomática de conjuntos es presentada a los estudiantes de matemáticas en un curso de maestría.

Actualmente, a la teoría de conjuntos intuitiva, que no usa la lógica formal, se llama *teoría ingenua de conjuntos* (del inglés, *naïve set theory*). Afortunadamente, usada cuidadosamente, esta teoría es suficiente para entender la mayoría de los conceptos matemáticos que se estudian durante la licenciatura en matemáticas. En este texto estudiaremos la teoría desde el punto de vista ingenuo, aunque tomaremos precauciones para no crear paradojas.

**Palabras clave de la sección:** *conjunto, pertenencia, notación por extensión y comprensión, paradoja, teoría axiomática de conjuntos.*

<sup>1</sup>A este tipo de colecciones de conjuntos “excesivamente grandes” ahora se les llama *clases propias*. Por ejemplo, la colección de todos los conjuntos es una clase propia.

### 2.1.1 Ejercicios de teorías de conjuntos

**Ejercicio 2.1.** Determina cuáles de las siguientes colecciones son conjuntos. Justifica tu respuesta.

- a) La colección de estudiantes de la Universidad de Guadalajara con promedio igual o superior a 90.
- b) La colección de grandes matemáticos en la historia de la humanidad.
- c) La colección de teoremas demostrados por matemáticos mexicanos.
- d) La colección de matemáticos que no son personas.
- e) La colección de todas las ideas abstractas.

**Ejercicio 2.2.** Determina cuáles de las siguientes afirmaciones son verdaderas. Justifica tu respuesta.

- a) El conjunto  $\{c, c, c\}$  es distinto del conjunto  $\{c\}$ .
- b) El conjunto  $\{1, 2, 3\}$  es igual al conjunto  $\{2, 3, 1\}$ .
- c) Si  $V$  es el conjunto de letras vocales, entonces  $\{a\} \in V$ .
- d) Si  $T$  es el conjunto de letras consonantes, entonces  $x \in T$ .
- e) Si  $R = \{b, c, \{x, y, z\}, \{u, l\}\}$ , entonces  $\{u, l\} \in R$ .
- f) Si  $R = \{b, c, \{x, y, z\}, \{u, l\}\}$ , entonces  $x \in R$ .

**Ejercicio 2.3.** Determina si los siguientes conjuntos están dados por extensión o por comprensión. En caso de estar dados por extensión, escríbelos por comprensión, y viceversa.

- a)  $A = \{a, b, c, d, e, f, g\}$ .
- b)  $B = \{m : m = 1 \text{ o } m = 5\}$ .
- c)  $C = \{1\}$ .
- d)  $D = \{x : x \text{ es una letra del abecedario}\}$ .

**Ejercicio 2.4.** Sea  $P$  una proposición. Demuestra que  $P \Leftrightarrow (\sim P)$  es una contradicción.

**Ejercicio 2.5.** ¿Qué pasaría con la nariz de Pinocho si afirmara “*Mi nariz crecerá ahora*”? Explica por qué esto es una paradoja.



## 2.2 Conceptos básicos de conjuntos

Recordemos que un conjunto puede ser denotado por extensión o por comprensión. En ocasiones será más fácil usar una notación o la otra, y muchas veces será posible usar ambas sin problemas. A continuación presentamos algunos de los conjuntos que usaremos con frecuencia en los próximos capítulos. ¿Puedes identificar qué tipo de notación se usa en cada caso?

- El conjunto **vacío**, que no contiene a ningún elemento,

$$\emptyset = \{\}.$$

- El conjunto de los **números naturales**,

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}.$$

- El conjunto de los **números enteros**,

$$\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}.$$

- El conjunto de los **números pares**,

$$2\mathbb{Z} = \{2x : x \in \mathbb{Z}\}.$$

- El conjunto de los **números primos**,

$$P = \{2, 3, 5, 7, 11, 13, \dots\}.$$

- El conjunto de los **números racionales**,

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

- El conjunto de los **números reales**,<sup>2</sup>

$$\mathbb{R} = \{x : x \text{ representa una cantidad en la recta real}\}.$$

- El conjunto de los **números complejos**,

$$\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}.$$

---

<sup>2</sup>Consúltase (Rudin, 1976) para una definición más formal del conjunto  $\mathbb{R}$ .

La lista anterior debe mantenerse como referencia. Estudiaremos en detalle los primeros conjuntos de la lista en el capítulo 4, y el resto en el capítulo 5.

Ahora abordaremos tres ideas fundamentales relacionadas con conjuntos: igualdad, subconjunto y cardinalidad.

**Definición 2.6 (igualdad de conjuntos).** Decimos que dos conjuntos  $A$  y  $B$  son *iguales* si ambos contienen exactamente los mismos elementos. En tal caso, escribimos  $A = B$ .

**Ejemplo 2.7.** Cualquier conjunto  $A$  es igual a sí mismo:  $A = A$ .

**Ejemplo 2.8 ( $\mathbb{N}$ ).** El conjunto de números naturales  $\mathbb{N}$  es igual al conjunto de **enteros no negativos** definido como

$$\mathbb{Z}_{\geq 0} = \{x : x \in \mathbb{Z} \text{ y } x \geq 0\},$$

ya que ambos conjuntos contienen exactamente los mismos elementos.<sup>3</sup> Sin embargo, el conjunto de **enteros positivos**, definido como

$$\mathbb{Z}_{>0} = \{x : x \in \mathbb{Z} \text{ y } x > 0\},$$

es distinto de  $\mathbb{N}$ , porque  $0 \in \mathbb{N}$  pero  $0 \notin \mathbb{Z}_{>0}$ .

**Notación 2.9.** En forma equivalente, podemos definir a  $\mathbb{Z}_{\geq 0}$  como

$$\mathbb{Z}_{\geq 0} = \{x \in \mathbb{Z} : x \geq 0\},$$

ya que todos los elementos de  $\mathbb{Z}_{\geq 0}$  cumplen la propiedad  $x \in \mathbb{Z}$ . En general, si *todos* los elementos de un conjunto satisfacen cierta propiedad, podemos escribir dicha propiedad antes de los dos puntos en la definición del conjunto.

**Ejemplo 2.10 ( $\emptyset$ ).** El conjunto vacío  $\emptyset$  es igual al conjunto

$$\{x \in \mathbb{Z} : x \neq x\},$$

ya que ninguno de los dos conjuntos contiene elementos.

**Ejemplo 2.11.** Los conjuntos

$$\begin{aligned} A &= \{-1, -2, -3, -4, -5\}, \\ B &= \{x \in \mathbb{Z} : x < 0 \text{ y } x^2 \leq 30\} \end{aligned}$$

---

<sup>3</sup>Esto no es del todo cierto, ya que formalmente los números naturales y los enteros están conformados por clases distintas de objetos matemáticos.

son iguales. Como vemos, los elementos de  $B$  cumplen tres propiedades: son números enteros ( $x \in \mathbb{Z}$ ), negativos ( $x < 0$ ) y su cuadrado es menor o igual que 30 ( $x^2 \leq 30$ ). Cualquier número con estas tres propiedades pertenece a  $B$ . Por ejemplo,  $-5 \in B$  porque  $-5 \in \mathbb{Z}$ ,  $-5 < 0$  y  $(-5)^2 = 25 \leq 30$ . De hecho, todos los enteros negativos que satisfacen  $x^2 \leq 30$  son:  $-1, -2, -3, -4$  y  $-5$ . Así,  $A = B$ .

**Ejemplo 2.12.** Los conjuntos

$$J = \{1, 2\},$$

$$K = \{1, \{2\}\},$$

son distintos, ya que no contienen exactamente los mismos elementos. El conjunto  $J$  contiene dos números, mientras que  $K$  contiene un número y un conjunto. No es lo mismo el número 2 que el conjunto que contiene al número 2. Este ejemplo se puede ilustrar con la siguiente analogía: no es lo mismo un objeto que una caja que contiene a un objeto.

**Definición 2.13 (subconjunto).** Sean  $A$  y  $B$  conjuntos. Decimos que  $A$  es un subconjunto de  $B$ , y escribimos  $A \subseteq B$  si todos los elementos de  $A$  pertenecen también a  $B$ .

Utilizando símbolos lógicos,  $A \subseteq B$  si la siguiente afirmación es verdadera:

$$\forall x((x \in A) \Rightarrow (x \in B)).$$

**Ejemplo 2.14.** Consideremos el conjunto de dígitos

$$D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Algunos subconjuntos de  $D$  son  $\{0, 1, 2\}$ ,  $\{3, 4, 6, 8\}$  y  $\{7\}$ , porque todos los elementos de los conjuntos previos pertenecen a  $D$ . Sin embargo, el conjunto  $\{0, 2, 4, 9, 13\}$  no es un subconjunto de  $D$  porque  $13 \notin D$ .

**Ejemplo 2.15.** Cualquier conjunto  $A$  siempre es un subconjunto de sí mismo, ya que, obviamente, todos los elementos de  $A$  pertenecen a  $A$ .

**Ejemplo 2.16.** El conjunto vacío  $\emptyset$  siempre es subconjunto de cualquier conjunto  $A$  porque, al no tener ningún elemento, la proposición “todos los elementos de  $\emptyset$  pertenecen a  $A$ ” es trivialmente verdadera.

Si  $A$  es un subconjunto de  $B$  y  $A \neq B$ , decimos que  $A$  es un *subconjunto propio* de  $B$ . En este caso escribimos  $A \subsetneq B$ .

**Ejemplo 2.17.** Observemos que  $P \subsetneq \mathbb{N} \subsetneq \mathbb{Z}$ . Es fácil darse cuenta de que  $P \neq \mathbb{N}$  ya que, por ejemplo,  $1 \in \mathbb{N}$  pero  $1 \notin P$ . De manera similar,  $\mathbb{N} \neq \mathbb{Z}$  porque  $-1 \in \mathbb{Z}$  pero  $-1 \notin \mathbb{N}$ .

**Proposición 2.18.** Sean  $A$  y  $B$  dos conjuntos. Así,  $A = B$  si y sólo si  $A \subseteq B$  y  $B \subseteq A$ .

**Demostración.**

- ( $\Rightarrow$ ) Supongamos que  $A = B$ . Esto significa que  $A$  y  $B$  contienen exactamente los mismos elementos. En particular, todos los elementos de  $A$  son elementos de  $B$  ( $A \subseteq B$ ), y también todos los elementos de  $B$  son elementos de  $A$  ( $B \subseteq A$ ).
- ( $\Leftarrow$ ) Supongamos que  $A \subseteq B$  y  $B \subseteq A$ . Esto significa que todos los elementos de  $A$  son elementos de  $B$ , y que todos los elementos de  $B$  son elementos de  $A$ . Por lo tanto,  $A$  y  $B$  tienen exactamente los mismos elementos; esto es,  $A = B$ . ■

Decimos que un conjunto es *finito* si tiene un número finito de elementos.<sup>4</sup> Por ejemplo, el conjunto de letras del abecedario o el conjunto de dígitos son ambos finitos. En caso contrario, decimos que el conjunto es *infinito*. Por ejemplo, los conjuntos  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  y  $\mathbb{R}$  son infinitos.

**Definición 2.19 (cardinalidad).** Sea  $A$  un conjunto finito. La cardinalidad de  $A$ , denotada como  $|A|$ , es el número de elementos de  $A$ .

**Ejemplo 2.20.** Veamos algunos ejemplos:

- 1) La cardinalidad del conjunto vacío es 0.
- 2) La cardinalidad del conjunto de dígitos  $D$  es 10.
- 3) La cardinalidad del conjunto de letras del abecedario es 27.

También es posible definir el concepto de cardinalidad para conjuntos infinitos, pero no estudiaremos este tema hasta la sección 4.4.

**Proposición 2.21.** Sean  $A$  y  $B$  conjuntos finitos.

- 1) Si  $A = B$ , entonces  $|A| = |B|$ .

---

<sup>4</sup>Daremos una definición más satisfactoria de esto en la sección 4.4.

2) Si  $A \subseteq B$ , entonces  $|A| \leq |B|$ .

**Demostración.** Demostraremos cada uno de los puntos.

- 1) Si  $A = B$ , obviamente  $|A| = |B|$ , ya que  $A$  y  $B$  contienen exactamente los mismos elementos.
- 2) Si  $A \subseteq B$ , entonces todos los elementos de  $A$  están contenidos en  $B$ . De esta forma, es imposible que  $A$  pueda tener más elementos que  $B$ ; en otras palabras, esto significa que  $|A| \leq |B|$ . ■

En la siguiente definición establecemos una forma interesante de crear un conjunto a partir de otro.

**Definición 2.22 (conjunto potencia).** Sea  $A$  un conjunto. El conjunto potencia de  $A$ , denotado como  $P(A)$ , es el conjunto de todos los subconjuntos de  $A$ .

**Ejemplo 2.23.** El conjunto potencia de  $\emptyset$  es  $P(\emptyset) = \{\emptyset\}$ . En este caso  $|\emptyset| = 0$ , mientras que  $|P(\emptyset)| = 1$ .

**Ejemplo 2.24.** Si  $X = \{0, 1\}$ , el conjunto potencia de  $X$  es

$$P(X) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\},$$

donde  $|X| = 2$  y  $|P(X)| = 4$ .

**Ejemplo 2.25.** Si  $A = \{x, y, z\}$ , el conjunto potencia de  $A$  es

$$P(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, A\}.$$

En este caso  $|A| = 3$ , mientras que  $|P(A)| = 8$ .

**Palabras clave de la sección:** conjuntos de números, igualdad de conjuntos, subconjunto, conjunto finito, cardinalidad, conjunto potencia.

**2.2.1 Ejercicios de conceptos básicos de conjuntos**

**Ejercicio 2.26.** Escribe los siguientes conjuntos por extensión:

- a)  $\{x \in \mathbb{Z} : -7 \leq x \leq 2\}$ .
- b)  $\{5x : x \in \mathbb{N}\}$ .
- c)  $\{x \in \mathbb{Z} : x \notin \mathbb{N}\}$ .
- d)  $\{x \in \mathbb{Z} : x \leq -2 \text{ o } x \geq 7\}$ .

**Ejercicio 2.27.** Escribe los siguientes conjuntos por comprensión:

- a)  $\{a\}$ .
- b)  $\{6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$ .
- c)  $\{\dots, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}$ .
- d)  $\{-10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10\}$ .

**Ejercicio 2.28.** Definimos al conjunto de números impares como

$$\mathbb{I} = \{\dots, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, \dots\}$$

Escribe este conjunto por comprensión, de dos formas distintas.

**Ejercicio 2.29.** Determina cuáles de los siguientes conjuntos son iguales a  $\mathbb{N}$ . Justifica tu respuesta.

- a)  $\{x \in \mathbb{Z} : -x \leq 0\}$ .
- b)  $\{x \in \mathbb{N} : x \notin 2\mathbb{Z}\}$ .
- c)  $\{x \in \mathbb{N} : x \neq 5\}$ .
- d)  $\{x \in \mathbb{Z} : 2^x \geq 1\}$ .

**Ejercicio 2.30.** Determina cuáles de los siguientes conjuntos son iguales entre sí. Justifica tu respuesta.

- a)  $\{0, 1, 4, 9, 16, 25, 36\}$ .
- b)  $\emptyset$ .
- c)  $\{n^2 : n \in \mathbb{Z}, 0 \leq n \leq 6\}$ .
- d)  $\{x \in 2\mathbb{Z} : 0 \leq x \leq 36\}$ .
- e)  $\{x \in \mathbb{N} : x \leq -3\}$ .

**Ejercicio 2.31.** Determina cuáles de los siguientes conjuntos son subconjuntos de  $\mathbb{N}$ . Justifica tu respuesta.

- a)  $\{-4, -2, 0, 2, 4\}$ .
- b)  $\{\{0\}, \{1\}, \{2\}, \{3\}, \dots\}$ .
- c)  $\{x \in \mathbb{Z} : x < 0 \text{ y } x > 0\}$ .
- d)  $\{x \in \mathbb{Z} : x^2 \geq 0\}$ .
- e)  $\{x \in \mathbb{Z} : x^3 \geq 0\}$ .

**Ejercicio 2.32.** Determina si los siguientes conjuntos son finitos o infinitos. En caso de ser finitos, escribe su cardinalidad. Justifica tu respuesta.

- a)  $\{-7, -3, 0, 4, 6, 7, 88, 460\}$ .
- b)  $\{x \in \mathbb{Z} : x^2 \leq x\}$ .
- c)  $I_n = \{x \in \mathbb{Z} : -n \leq x \leq n\}$  donde  $n$  es un número natural fijo.
- d)  $P(\mathbb{N})$ .
- e)  $\{x \in \mathbb{Z} : x \notin \mathbb{N}\}$ .

**Ejercicio 2.33.** Encuentra el conjunto potencia de  $Y = \{\mathcal{Y}\}$ .

**Ejercicio 2.34.** Encuentra el conjunto potencia de  $Z = \{1, 2, 3, 4\}$ .  
¿Cuál es la cardinalidad de  $P(Z)$ ?

## 2.3 Operaciones de conjuntos

En esta sección estudiaremos distintas formas de construir conjuntos nuevos a partir de dos o más conjuntos dados. A estas técnicas que producen nuevos conjuntos las llamamos *operaciones de conjuntos*. Hay cuatro operaciones básicas: la unión, la intersección, el complemento y el producto cartesiano. Es indispensable para un futuro matemático entender estas cuatro operaciones y sus propiedades básicas.

La **unión** es la operación que nos permite, dados dos o más conjuntos, definir un conjunto que contenga a ambos.

**Definición 2.35 (unión).** Sean  $A$  y  $B$  conjuntos. La *unión* de  $A$  y  $B$ , denotada como  $A \cup B$ , es el conjunto de elementos que pertenecen a  $A$  o pertenecen a  $B$ . En otras palabras,

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}$$

donde  $\vee$  es el conectivo lógico de disyunción.

El *diagrama de Venn* es una representación gráfica que muestra todas las relaciones lógicas posibles entre una colección finita de conjuntos. El diagrama de Venn que representa la unión de dos conjuntos es el siguiente:

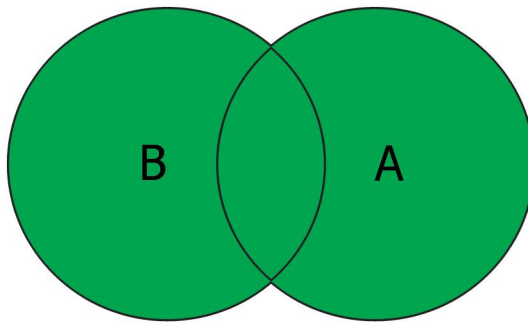


Figura 2.1: Unión de  $A$  y  $B$ .

**Ejemplo 2.36.** Consideremos el conjunto de enteros negativos

$$\mathbb{Z}_{<0} = \{x \in \mathbb{Z} : x < 0\}.$$

Entonces

$$\mathbb{N} \cup \mathbb{Z}_{<0} = \{x \in \mathbb{Z} : (x \geq 0) \vee (x < 0)\} = \mathbb{Z}.$$



**Proposición 2.37 (unión).** Sean  $A$ ,  $B$  y  $C$  conjuntos. La unión de conjuntos cumple las siguientes propiedades:

- 1)  $A \cup \emptyset = A$ .
- 2) *Conmutatividad.*  $A \cup B = B \cup A$ .
- 3) *Asociatividad.*  $(A \cup B) \cup C = A \cup (B \cup C)$ .
- 4) *Idempotencia.*  $A \cup A = A$ .

**Demostración.** Demostraremos cada uno de los puntos.

- 1) Por definición,  $A \cup \emptyset = \{x : (x \in A) \vee (x \in \emptyset)\}$ . Sin embargo, la condición  $x \in \emptyset$  nunca se cumple, porque  $\emptyset$  no tiene ningún elemento. De esta forma, es posible omitir esta condición y escribir  $A \cup \emptyset = \{x : x \in A\} = A$ .
- 2)  $A \cup B = \{x : (x \in A) \vee (x \in B)\} = \{x : (x \in B) \vee (x \in A)\} = B \cup A$ , ya que el conectivo lógico  $\vee$  es conmutativo.
- 3) Como el conectivo lógico  $\vee$  es asociativo, tenemos que

$$\begin{aligned} (A \cup B) \cup C &= \{x : x \in A \vee x \in B\} \cup C \\ &= \{x : [x \in A \vee x \in B] \vee x \in C\} \\ &= \{x : x \in A \vee [x \in B \vee x \in C]\} \\ &= A \cup (B \cup C). \end{aligned}$$

- 4)  $A \cup A = \{x : (x \in A) \vee (x \in A)\} = \{x : x \in A\} = A$ . ■

**Ejemplo 2.38.** Sean

$$L = \{0, 1, 2\}, M = \{1, 2, 3\} \text{ y } N = \{0, 2, 3\}.$$

Por la asociatividad que se demostró en la proposición anterior, podemos escribir  $L \cup M \cup N$  sin paréntesis, ya que no importa qué unión de conjuntos calculemos primero. En este caso,

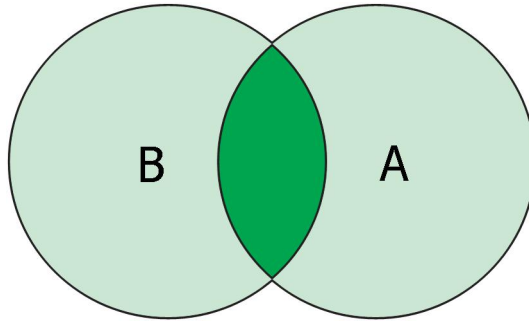
$$L \cup M \cup N = \{x : (x \in L) \vee (x \in M) \vee (x \in N)\} = \{0, 1, 2, 3\}.$$

La **intersección** es la segunda operación que estudiaremos.

**Definición 2.39 (intersección).** Sean  $A$  y  $B$  conjuntos. La *intersección* de  $A$  y  $B$ , denotada como  $A \cap B$ , es el conjunto de elementos que simultáneamente pertenecen a ambos,  $A$  y  $B$ . En otras palabras,

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\},$$

donde  $\wedge$  es el conectivo lógico de conjunción.

Figura 2.2: Intersección de  $A$  y  $B$ .

La intersección de dos conjuntos está representada por el área más oscura en el diagrama de Venn de la figura 2.2.

**Ejemplo 2.40.** Observemos que

$$2\mathbb{Z} \cap \mathbb{N} = \{x : x \in 2\mathbb{Z} \text{ y } x \in \mathbb{N}\} = \{0, 2, 4, 6, 8, 10, \dots\}.$$

**Proposición 2.41 (intersección).** Sean  $A$ ,  $B$  y  $C$  conjuntos. La intersección de conjuntos cumple las siguientes propiedades.

- 1)  $A \cap \emptyset = \emptyset$ .
- 2) *Conmutatividad.*  $A \cap B = B \cap A$ .
- 3) *Asociatividad.*  $(A \cap B) \cap C = A \cap (B \cap C)$ .
- 4) *Idempotencia.*  $A \cap A = A$ .

**Demostración.** La demostración de esta proposición es consecuencia de las propiedades del conectivo lógico  $\wedge$ , así que se deja como ejercicio. ■

**Ejemplo 2.42.** Sean  $L = \{0, 1, 2\}$ ,  $M = \{1, 2, 3\}$  y  $N = \{0, 2, 3\}$ . Entonces

$$\begin{aligned} L \cap M &= \{x : (x \in L) \wedge (x \in M)\} = \{1, 2\}, \\ L \cap N &= \{x : (x \in L) \wedge (x \in N)\} = \{0, 2\}, \\ M \cap N &= \{x : (x \in M) \wedge (x \in N)\} = \{2, 3\}, \\ L \cap M \cap N &= \{x : (x \in L) \wedge (x \in M) \wedge (x \in N)\} = \{2\}. \end{aligned}$$

**Ejemplo 2.43.** Si  $A$ ,  $B$  y  $C$  son tres conjuntos, la intersección  $A \cap B \cap C$  está representada por el área más oscura en el diagrama de Venn de la figura 2.3.

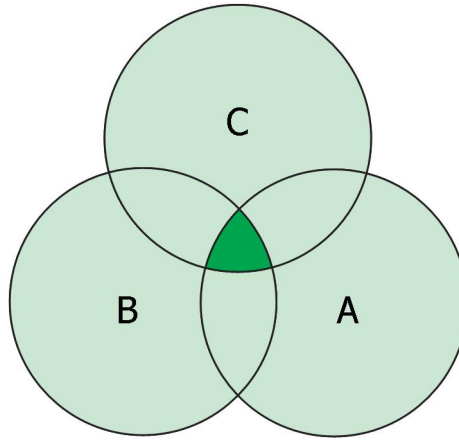


Figura 2.3: Intersección de  $A$ ,  $B$  y  $C$ .

**Definición 2.44 (conjuntos disjuntos).** Decimos que dos conjuntos  $A$  y  $B$  son disjuntos si  $A \cap B = \emptyset$ .

**Ejemplo 2.45.** Los conjuntos

$$A = \{1, 2, 3\} \text{ y } B = \{4, 5, 6\}$$

son disjuntos.

Ahora definiremos el **complemento** de un conjunto en otro.

**Definición 2.46 (complemento).** Sean  $A$  y  $B$  conjuntos. El *complemento* de  $A$  en  $B$ , denotado como  $B \setminus A$ , es el conjunto de elementos de  $B$  que no pertenecen a  $A$ .

$$B \setminus A = \{x \in B : \sim (x \in A)\} = \{x \in B : x \notin A\},$$

donde  $\sim$  es el conectivo lógico de negación.

**Ejemplo 2.47.** Consideremos los conjuntos

$$A = \{a, b, c, d, e\} \text{ y } B = \{a, e, i, o, u\}.$$

Entonces, el complemento de  $A$  en  $B$  es

$$B \setminus A = \{i, o, u\},$$

mientras que el complemento de  $B$  en  $A$  es

$$A \setminus B = \{b, c, d\}.$$

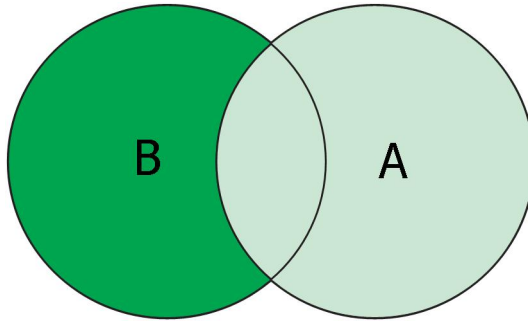


Figura 2.4: Complemento de A en B.

El complemento de A en B está representado por el área más oscura en el diagrama de Venn de la figura 2.4.

**Ejemplo 2.48.** Consideremos los conjuntos  $\mathbb{Z}$  y  $2\mathbb{Z}$ . En este caso, tenemos que

$$\mathbb{Z} \cup 2\mathbb{Z} = \{x : x \in \mathbb{Z} \text{ o } x \in 2\mathbb{Z}\} = \mathbb{Z}$$

$$\mathbb{Z} \cap 2\mathbb{Z} = \{x : x \in 2\mathbb{Z} \text{ y } x \in \mathbb{Z}\} = 2\mathbb{Z}$$

$$\mathbb{Z} \setminus 2\mathbb{Z} = \{x \in \mathbb{Z} : x \notin 2\mathbb{Z}\} = \mathbb{I}$$

$$2\mathbb{Z} \setminus \mathbb{Z} = \{x \in 2\mathbb{Z} : x \notin \mathbb{Z}\} = \emptyset$$

donde  $\mathbb{I}$  es el conjunto de enteros impares.

En los ejemplos anteriores observamos que la operación complemento no es conmutativa: en general,  $(B \setminus A) \neq (A \setminus B)$ .

En ciertas situaciones, todos los conjuntos que consideramos son subconjuntos de un conjunto  $U$ , al que llamamos *universo* (en muchos ejemplos anteriores, el universo ha sido  $\mathbb{Z}$ ). En tales casos, si  $A \subseteq U$ , denotamos al complemento de A en U de una forma especial: escribimos  $A'$  en lugar de  $U \setminus A$  para simplificar la notación.

**Proposición 2.49 (complemento).** Sea A un subconjunto de U. El complemento de A en U cumple las siguientes propiedades.

- 1)  $(A')' = A$ .
- 2)  $\emptyset' = U$  y  $U' = \emptyset$ .
- 3)  $A \cap A' = \emptyset$  y  $A \cup A' = U$ .

**Demostración.** Demostraremos cada uno de los puntos.

1) Observemos que

$$\begin{aligned}(A')' &= \{x \in U : \sim (x \in A')\} \\ &= \{x \in U : \sim (\sim (x \in A))\} \\ &= \{x \in U : x \in A\} \\ &= A,\end{aligned}$$

usando el ejercicio 1.47 d).

2) Por definición,

$$\emptyset' = \{x \in U : x \notin \emptyset\}.$$

Debido a que la condición  $x \notin \emptyset$  es universalmente cierta, podemos omitirla. Por lo tanto,

$$\emptyset' = \{x \in U\} = U.$$

Por otro lado,

$$U' = \{x \in U : x \notin U\} = \emptyset.$$

3) Demostraremos que  $A \cap A' = \emptyset$ , y se dejará como ejercicio demostrar que  $A \cup A' = U$ . Por definición, tenemos que

$$A \cap A' = \{x \in U : (x \in A) \wedge (x \notin A)\}.$$

Debido a que es imposible que un elemento simultáneamente pertenezca y no pertenezca a  $A$ , concluimos que  $A \cap A' = \emptyset$ . ■

Es posible combinar las operaciones de conjuntos definidas anteriormente para formar nuevos conjuntos. El siguiente teorema describe la interacción de las uniones e intersecciones con el complemento.

**Teorema 2.50 (leyes de De Morgan).** Sean  $A$  y  $B$  subconjuntos de  $U$ . Entonces se cumple que

$$(A \cup B)' = A' \cap B' \text{ y } (A \cap B)' = A' \cup B'.$$

**Demostración.** Por el ejercicio 1.47, sabemos que

$$\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q) \text{ y } \sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q),$$

donde  $P$  y  $Q$  son proposiciones cualesquiera. Usando estas identidades, no es difícil completar la demostración del teorema (ejercicio 2.58). ■

El siguiente ejemplo ilustra el conjunto obtenido al combinar la intersección con el complemento.

**Ejemplo 2.51.** Si  $A$ ,  $B$  y  $C$  son conjuntos, el conjunto  $(B \cap C) \setminus A$  está representado por el área más oscura en el diagrama de Venn de la figura 2.5.

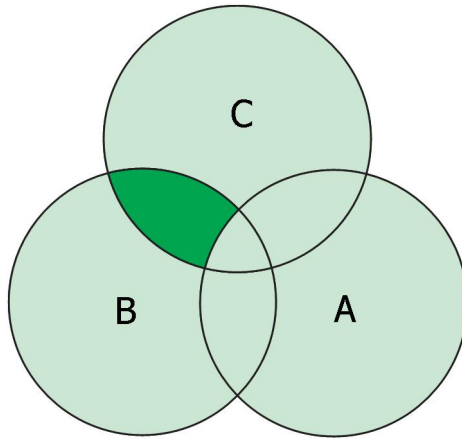


Figura 2.5:  $(B \cap C) \setminus A$ .

La siguiente proposición estudia el caso de cuando se operan dos conjuntos  $A$  y  $B$  tales que  $A \subseteq B$ . Recomendamos al lector visualizar cada una de las afirmaciones de esta proposición en un diagrama de Venn.

**Proposición 2.52.** Sean  $A$  y  $B$  subconjuntos de  $U$ . Las siguientes afirmaciones son equivalentes:

- 1)  $A \subseteq B$ .
- 2)  $A \cup B = B$ .
- 3)  $B' \subseteq A'$ .
- 4)  $A \cap B = A$ .

La técnica más común para demostrar este tipo de proposiciones consiste en demostrar que la afirmación 1) implica 2), que 2) implica 3), que 3) implica 4), y finalmente, que 4) implica 1). Esto demuestra que todas las afirmaciones son equivalentes entre sí.

**Demostración.**

- 1) → 2) Ejercicio 2.59.
- 2) → 3) Supongamos que  $A \cup B = B$ . Sea  $x \in U$ . Si  $x \notin B$ , entonces  $x \notin A \cup B$ , lo que implica que  $x \notin A$ . Por lo tanto, si  $x \in B'$ , entonces  $x \in A'$ . Esto quiere decir que cualquier elemento de  $B'$  pertenece a  $A'$ ; en otras palabras,  $B' \subseteq A'$ .
- 3) → 4) Supongamos que  $B' \subseteq A'$ . Debemos demostrar que  $A \cap B = A$ . Es claro que, por definición,  $A \cap B \subseteq A$ . Demostraremos que  $A \subseteq A \cap B$ , y usaremos la proposición 2.18. Sea  $x \in U$  cualquier elemento tal que  $x \in A$ . Para demostrar que  $x \in A \cap B$ , debemos probar que  $x \in B$ . Por reducción al absurdo, si  $x \notin B$ , entonces  $x \in B'$ , así que  $x \in A'$  (ya que  $B' \subseteq A'$ ). Pero esto contradice que  $x \in A$ , así que  $x \in B$ , como queríamos demostrar.
- 4) → 1) Ejercicio 2.60. ■

Finalmente, estudiaremos una nueva forma de definir un conjunto a partir de otros, sin usar los conectivos lógicos como pieza fundamental. Antes de esto, recordaremos al lector el concepto de *par ordenado*.

Consideremos dos objetos matemáticos  $x$  y  $y$ . Una manera de crear un nuevo objeto matemático, que involucre a  $x$  y  $y$ , es formar el conjunto  $\{x, y\}$ . En esta situación no consideramos ningún orden especial; es decir,  $\{x, y\} = \{y, x\}$ . El par ordenado  $(x, y)$  es la construcción natural que surge cuando nos interesa considerar el orden en el que aparecen los objetos. En este caso distinguimos que  $x$  es el primer elemento del par (o *primera coordenada*) y que  $y$  es el segundo elemento del par (o *segunda coordenada*). Así, a diferencia del caso de los conjuntos,

$$(x, y) \neq (y, x),$$

a menos que  $x = y$ . La propiedad más característica de los pares ordenados es que dos de ellos son iguales si y sólo si las primeras y segundas coordenadas coinciden. En símbolos:

$$((x, y) = (z, w)) \Leftrightarrow ((x = z) \wedge (y = w)).$$

**Definición 2.53 (producto cartesiano).** Sean  $A$  y  $B$  conjuntos. El *producto cartesiano* de  $A$  y  $B$ , denotado como  $A \times B$ , es el conjunto de todos los pares ordenados formados por los elementos de  $A$  y  $B$ :

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

**Ejemplo 2.54.** Consideremos los conjuntos

$$X = \{w, x, y, z\} \text{ y } Y = \{1, 2, 3\}.$$

Entonces,

$$X \times Y = \left\{ \begin{array}{l} (w, 1), (x, 1), (y, 1), (z, 1), (w, 2), (x, 2), \\ (y, 2), (z, 2), (w, 3), (x, 3), (y, 3), (z, 3) \end{array} \right\}.$$

Observemos que  $|X| = 4$  y  $|Y| = 3$ , mientras que  $|X \times Y| = 12$ . Además el producto cartesiano

$$Y \times X = \left\{ \begin{array}{l} (1, w), (1, x), (1, y), (1, z), (2, w), (2, x), \\ (2, y), (2, z), (3, w), (3, x), (3, y), (3, z) \end{array} \right\},$$

es distinto de  $X \times Y$  porque las coordenadas de los pares aparecen en el orden opuesto. De manera similar, podemos calcular el producto

$$X \times X = \left\{ \begin{array}{l} (w, w), (w, x), (w, y), (w, z), (x, w), \\ (x, x), (x, y), (x, z), (y, w), (y, x), \\ (y, y), (y, z), (z, w), (z, x), (z, y), (z, z) \end{array} \right\},$$

y el producto

$$Y \times Y = \left\{ \begin{array}{l} (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), \\ (2, 3), (3, 1), (3, 2), (3, 3) \end{array} \right\}.$$

**Palabras clave de la sección:** *unión, intersección, conjuntos disjuntos, complemento, diagrama de Venn, par ordenado, producto cartesiano.*



### 2.3.1 Ejercicios de operaciones de conjuntos

**Ejercicio 2.55.** Considera los conjuntos

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\},$$

$$B = \{2, 4, 6, 8\} \text{ y } C = \{-1, 0, 1\}.$$

- Escribe por extensión las uniones  $B \cup C$  y  $A \cup B \cup C$ .
- Escribe por extensión las intersecciones  $A \cap B$ ,  $A \cap C$  y  $B \cap C$ .
- Escribe por extensión los complementos  $A \setminus B$ ,  $B \setminus A$  y  $C \setminus A$ .
- Escribe por extensión el conjunto  $(A \cap C) \cup B$ .
- Si  $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ , encuentra los conjuntos  $(A \cup B)'$  y  $A' \cap B'$ , y comprueba que son iguales. Esto ejemplifica el teorema de las leyes de De Morgan.
- Escribe por extensión los productos cartesianos  $B \times C$  y  $C \times C$ .

**Ejercicio 2.56.** Demuestra la proposición 2.41 que establece las propiedades básicas de la intersección de conjuntos.

**Ejercicio 2.57.** Sean  $A$  y  $B$  conjuntos disjuntos.

- Demuestra que  $A \setminus B = A$  y  $B \setminus A = B$ .
- Explica por qué, si  $A$  y  $B$  son finitos,

$$|A \cup B| = |A| + |B|.$$

**Ejercicio 2.58.** Escribe una demostración completa para el teorema 2.50 de las leyes de De Morgan.

**Ejercicio 2.59.** Sean  $A$  y  $B$  subconjuntos de  $U$ . Demuestra que si  $A \subseteq B$ , entonces  $A \cup B = B$ .

**Ejercicio 2.60.** Sean  $A$  y  $B$  subconjuntos de  $U$ . Demuestra que si  $A \cap B = A$  entonces  $A \subseteq B$ .

**Ejercicio 2.61.** Escribe un ejemplo donde los conjuntos  $A \times B$  y  $B \times A$  no sean iguales. Escribe también un ejemplo donde  $A \times B = B \times A$ .

## 2.4 Definiciones del capítulo

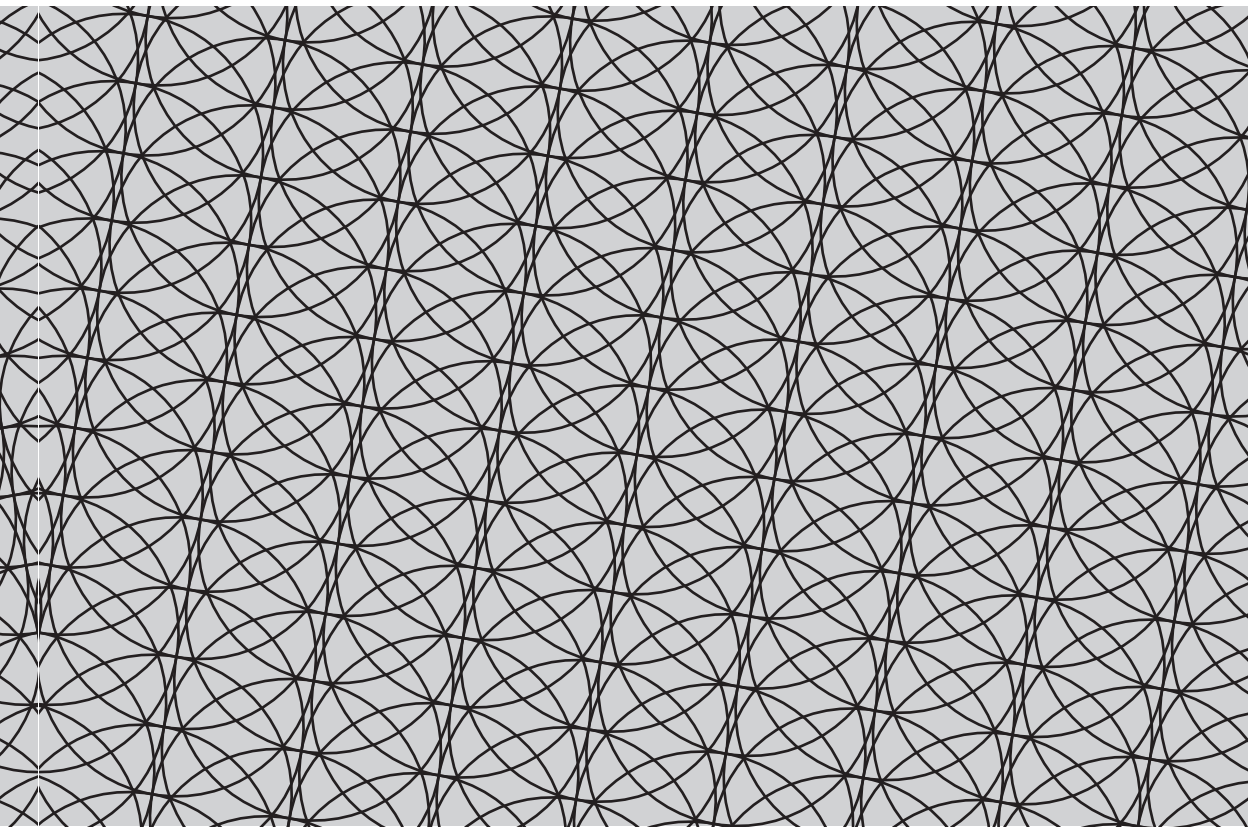
Escribe la definición y un ejemplo de cada uno de los conceptos enlistados a continuación.

- 1) Paradoja.
- 2) Notación por extensión de un conjunto.
- 3) Notación por comprensión de un conjunto.
- 4) Igualdad de conjuntos.
- 5) Subconjunto.
- 6) Cardinalidad de un conjunto finito.
- 7) Conjunto potencia.
- 8) Unión de dos conjuntos.
- 9) Intersección de dos conjuntos.
- 10) Conjuntos disjuntos.
- 11) Complemento de un conjunto en otro.
- 12) Primera y segunda coordenadas de un par ordenado.
- 13) Producto cartesiano de dos conjuntos.

*Los matemáticos no estudian objetos, sino las relaciones entre objetos.*

H. Poincaré, matemático francés

## Capítulo 3. Relaciones



Las *relaciones* matemáticas representan la formalización de las conexiones e interacciones entre diversos objetos matemáticos; por tal motivo, tienen una importancia crucial en todas las ramas de esta ciencia.

En este capítulo daremos una definición formal del concepto de relación, y el cual, advertimos, no debe ser confundido su significado en español. Como explicaremos, una relación establece un vínculo entre dos conjuntos, o de un conjunto consigo mismo. Los tres tipos de relaciones matemáticas más importantes son: las *funciones*, las *relaciones de equivalencia* y las *relaciones de orden*. Este capítulo está dedicado al estudio de estos tres conceptos.

## 3.1 Funciones

### 3.1.1 Relaciones binarias

La definición de función que usamos actualmente apareció por primera vez en el libro *Axiomatic set theory* (1960) de Patrick Suppes. El siguiente es un extracto del texto:

Aún hoy muchos textos de cálculo diferencial e integral no dan una definición de función matemáticamente satisfactoria. Una definición precisa y completamente general es inmediata dentro de nuestro enfoque teórico de conjuntos. Una función es simplemente una relación de muchos a uno, esto es, una relación tal que cualquier elemento de su dominio se relaciona exactamente con un elemento de un recorrido.<sup>1</sup>

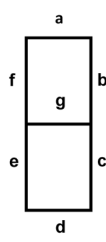
No deja de sorprender que la frase escrita por Suppes en 1960 siga vigente: aún hoy existen muchos textos de cálculo que reproducen la definición de función que en 1923 escribió el matemático francés Edouard Goursat en su célebre obra *Curso de análisis matemático*:

Se dice que  $y$  es una función de  $x$  si a cada valor de  $x$  le corresponde un valor de  $y$ . Esta correspondencia se indica mediante la ecuación  $y = f(x)$ .

La definición anterior pone énfasis en la correspondencia entre las variables y no en la idea de conjunto. Sin embargo, ha sido a partir de la definición conjuntista que el concepto de función se ha

---

<sup>1</sup>Tomado de la versión en español de Hernando Alfonso Castillo, profesor de la Universidad Pedagógica Nacional, Bogotá, Editorial Norma (1968).



Número	Segmentos encendidos	Número	Segmentos encendidos
0	a, b, c, d, e, f	5	a, f, g, c, d
1	b, c	6	a, f, g, c, d, e
2	a, b, g, e, d	7	a, b, c
3	a, b, g, c, d	8	a, b, c, d, e, f, g
4	b, c, f, g	9	a, b, c, d, f, g

Figura 3.1: Relación *display*.

vuelto fundamental en todos los campos de la matemática. Incluso podría decirse que en la matemática actual el concepto de función es más fundamental que el de número.

En la definición de Suppes se utilizan tres conceptos que requieren una definición: *relación*, *dominio* y *recorrido* (también llamado *rango*).

**Definición 3.1 (relación).** Una *relación* es un conjunto en el cual todos sus elementos son pares ordenados.

Una relación formada por pares también suele llamarse *relación binaria*, ya que el concepto puede generalizarse: un conjunto en el cual todos sus elementos son *n-tuplas ordenadas*  $(a_1, a_2, a_3, \dots, a_n)$  se llama *relación n-aria*. En este texto nos enfocamos en estudiar relaciones binarias.

**Ejemplo 3.2.** El conjunto

$$R_1 = \{(\clubsuit, \odot), (\boxplus, \times), (\otimes, a)\}$$

es una relación, ya que se trata de un conjunto de pares ordenados.

**Ejemplo 3.3.** El *display* que usan algunos equipos electrónicos para representar los dígitos está formado por siete segmentos que, a base de encenderse o apagarse, dan forma a cada número.

Con esto, definimos una relación  $R_2$  como el conjunto de pares  $(a, b)$ , donde  $a$  es un dígito y  $b$  es el número de segmentos que se encienden en el *display* para mostrar el dígito  $a$ . Escrita por extensión, la relación es

$$R_2 = \left\{ \begin{array}{l} (0, 6), (1, 2), (2, 5), (3, 5), (4, 4), \\ (5, 5), (6, 6), (7, 3), (8, 7), (9, 6) \end{array} \right\}.$$

En el capítulo 2 definimos el producto cartesiano  $A \times B$  como el conjunto de todos los pares cuyas primeras y segundas coordenadas son elementos de  $A$  y  $B$  respectivamente. Por lo tanto, cualquier subconjunto de un producto cartesiano es siempre una relación.

**Definición 3.4 (relación de  $A$  en  $B$ ).** Sean  $A$  y  $B$  conjuntos. Una *relación de  $A$  en  $B$*  es un subconjunto del producto cartesiano  $A \times B$ .

En otras palabras,  $R$  es una relación de  $A$  en  $B$  si y sólo si  $R \subseteq A \times B$ . En símbolos, denotamos a una relación  $R$  de  $A$  en  $B$  como

$$R : A \rightarrow B.$$

No debemos confundir esta notación con el conectivo lógico condicional. Si  $A = B$ , decimos que  $R : A \rightarrow A$  es una relación *sobre*  $A$ .

**Ejemplo 3.5.** Sean  $A = \{a, b\}$  y  $B = \{1, 2, 3\}$ . El producto cartesiano de estos conjuntos es

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}.$$

Así, por ejemplo,

$$R = \{(a, 1), (a, 3), (b, 2)\}$$

es una relación de  $A$  en  $B$ . Todas las relaciones de  $A$  en  $B$  se muestran en la tabla 3.1. Hay 64 relaciones distintas, cada una de las cuales corresponde a un subconjunto de  $A \times B$ .

**Definición 3.6 (dominio).** Sea  $R$  una relación. El conjunto de todas las primeras coordenadas de los pares ordenados de una relación  $R$  se llama *dominio de  $R$* . En otras palabras,

$$\text{dom}(R) = \{a : \exists b \text{ tal que } (a, b) \in R\}.$$

Para cualquier relación  $R$  de  $A$  en  $B$ , tenemos que  $\text{dom}(R) \subseteq A$ .

**Ejemplo 3.7.** El dominio de la relación  $R_1$  del ejemplo 3.2 es

$$\text{dom}(R_1) = \{\clubsuit, \boxplus, \odot\},$$

mientras que el dominio de la relación  $R_2$  del ejemplo 3.3 es

$$\text{dom}(R_2) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

$R_0 = \{\}$	$R_{32} = \{(a, 2), (a, 3), (b, 1)\}$
$R_1 = \{(a, 1)\}$	$R_{33} = \{(a, 2), (a, 3), (b, 2)\}$
$R_2 = \{(a, 2)\}$	$R_{34} = \{(a, 2), (a, 3), (b, 3)\}$
$R_3 = \{(a, 3)\}$	$R_{35} = \{(a, 2), (b, 1), (b, 2)\}$
$R_4 = \{(b, 1)\}$	$R_{36} = \{(a, 2), (b, 1), (b, 3)\}$
$R_5 = \{(b, 2)\}$	$R_{37} = \{(a, 2), (b, 2), (b, 3)\}$
$R_6 = \{(b, 3)\}$	$R_{38} = \{(a, 3), (b, 1), (b, 2)\}$
$R_7 = \{(a, 1), (a, 2)\}$	$R_{39} = \{(a, 3), (b, 1), (b, 3)\}$
$R_8 = \{(a, 1), (a, 3)\}$	$R_{40} = \{(a, 3), (b, 2), (b, 3)\}$
$R_9 = \{(a, 1), (b, 1)\}$	$R_{41} = \{(b, 1), (b, 2), (b, 3)\}$
$R_{10} = \{(a, 1), (b, 2)\}$	$R_{42} = \{(a, 1), (a, 2), (a, 3), (b, 1)\}$
$R_{11} = \{(a, 1), (b, 3)\}$	$R_{43} = \{(a, 1), (a, 2), (a, 3), (b, 2)\}$
$R_{12} = \{(a, 2), (a, 3)\}$	$R_{44} = \{(a, 1), (a, 2), (a, 3), (b, 3)\}$
$R_{13} = \{(a, 2), (b, 1)\}$	$R_{45} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
$R_{14} = \{(a, 2), (b, 2)\}$	$R_{46} = \{(a, 1), (a, 2), (b, 1), (b, 3)\}$
$R_{15} = \{(a, 2), (b, 3)\}$	$R_{47} = \{(a, 1), (a, 2), (b, 2), (b, 3)\}$
$R_{16} = \{(a, 3), (b, 1)\}$	$R_{48} = \{(a, 1), (a, 3), (b, 1), (b, 2)\}$
$R_{17} = \{(a, 3), (b, 2)\}$	$R_{49} = \{(a, 1), (a, 3), (b, 1), (b, 3)\}$
$R_{18} = \{(a, 3), (b, 3)\}$	$R_{50} = \{(a, 1), (a, 3), (b, 2), (b, 3)\}$
$R_{19} = \{(b, 1), (b, 2)\}$	$R_{51} = \{(a, 1), (b, 1), (b, 2), (b, 3)\}$
$R_{20} = \{(b, 1), (b, 3)\}$	$R_{52} = \{(a, 2), (a, 3), (b, 1), (b, 2)\}$
$R_{21} = \{(b, 2), (b, 3)\}$	$R_{53} = \{(a, 2), (a, 3), (b, 1), (b, 3)\}$
$R_{22} = \{(a, 1), (a, 2), (a, 3)\}$	$R_{54} = \{(a, 2), (a, 3), (b, 2), (b, 3)\}$
$R_{23} = \{(a, 1), (a, 2), (b, 1)\}$	$R_{55} = \{(a, 2), (b, 1), (b, 2), (b, 3)\}$
$R_{24} = \{(a, 1), (a, 2), (b, 2)\}$	$R_{56} = \{(a, 3), (b, 1), (b, 2), (b, 3)\}$
$R_{25} = \{(a, 1), (a, 2), (b, 3)\}$	$R_{57} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2)\}$
$R_{26} = \{(a, 1), (a, 3), (b, 1)\}$	$R_{58} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 3)\}$
$R_{27} = \{(a, 1), (a, 3), (b, 2)\}$	$R_{59} = \{(a, 1), (a, 2), (a, 3), (b, 2), (b, 3)\}$
$R_{28} = \{(a, 1), (a, 3), (b, 3)\}$	$R_{60} = \{(a, 1), (a, 2), (b, 1), (b, 2), (b, 3)\}$
$R_{29} = \{(a, 1), (b, 1), (b, 2)\}$	$R_{61} = \{(a, 1), (a, 3), (b, 1), (b, 2), (b, 3)\}$
$R_{30} = \{(a, 1), (b, 1), (b, 3)\}$	$R_{62} = \{(a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$
$R_{31} = \{(a, 1), (b, 2), (b, 3)\}$	$R_{63} = \{a, b\} \times \{1, 2, 3\}$

 Tabla 3.1: Relaciones de  $\{a, b\}$  en  $\{1, 2, 3\}$ .

**Definición 3.8 (rango).** El conjunto de todas las segundas coordenadas de los pares ordenados de una relación  $R$  se llama *rango* de  $R$ :

$$\text{ran}(R) = \{b : \exists a \text{ tal que } (a, b) \in R\}.$$

Si  $R$  es una relación de  $A$  en  $B$ , tenemos que  $\text{ran}(R) \subseteq B$ . El conjunto  $B$  es llamado *codominio* o *contradominio* de la relación.

**Ejemplo 3.9.** El rango de  $R_1$  del ejemplo 3.2 es

$$\text{ran}(R_1) = \{\odot, \times, a\},$$

mientras que el rango de  $R_2$  del ejemplo 3.3 es

$$\text{ran}(R_2) = \{2, 3, 4, 5, 6, 7\}.$$

Las definiciones 3.1 y 3.4 son en realidad equivalentes, ya que cualquier conjunto  $R$  de pares ordenados puede verse como un subconjunto del producto cartesiano  $\text{dom}(R) \times \text{ran}(R)$ . En conclusión, todo conjunto de pares ordenados es una relación y toda relación es subconjunto de algún producto cartesiano.

**Ejemplo 3.10.** La relación  $R_2$  del ejemplo 3.3 es un subconjunto de

$$\text{dom}(R_2) \times \text{ran}(R_2) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \times \{2, 3, 4, 5, 6, 7\}.$$

Si  $D$  es el conjunto de dígitos, también tenemos que

$$R \subseteq D \times D.$$

Además,  $R \subseteq \mathbb{N} \times \mathbb{N}$  y  $R \subseteq \mathbb{Z} \times \mathbb{Z}$ . Esto ejemplifica que una relación puede ser subconjunto de diversos productos cartesianos.

### 3.1.2 Definición de función

Con los conceptos revisados, finalmente podemos enunciar la definición de función.

**Definición 3.11 (función).** Sean  $A$  y  $B$  conjuntos. Una *función de  $A$  en  $B$*  es una relación  $F : A \rightarrow B$  tal que:

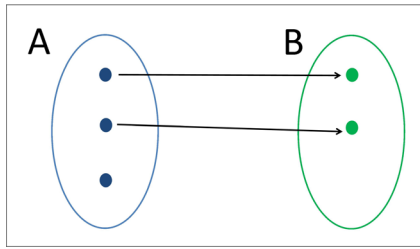
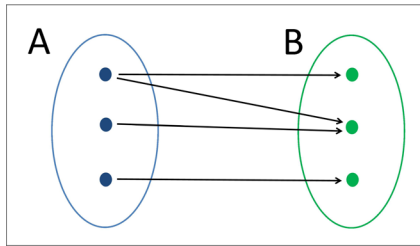
- 1)  $\text{dom}(F) = A$ .
- 2) Si  $(a, b_1) \in F$  y  $(a, b_2) \in F$ , entonces  $b_1 = b_2$ .

Queda establecido que las funciones son un tipo especial de relaciones. La propiedad 2) de la definición 3.11 significa que a cada elemento  $a \in \text{dom}(F)$  le corresponde un único elemento del rango, comúnmente denotado como  $F(a)$ .

**Ejemplo 3.12.** Consideremos las relaciones  $K_1$  y  $K_2$  definidas por las figuras 3.3 y 3.2. Las flechas  $\rightarrow$  en los diagramas indican que el par conformado por el punto inicial y el punto final de la flecha pertenecen a la relación.

- 1) La relación  $K_1$  no es una función porque hay un punto en  $A$  del cual no parte ninguna flecha; es decir,  $\text{dom}(K_1) \neq A$ .




 Figura 3.2: Relación  $K_1$ .

 Figura 3.3: Relación  $K_2$ .

- 2) La relación  $K_2$  no es una función porque al primer punto del dominio le corresponden dos puntos distintos del rango.

**Ejemplo 3.13.** Sea  $D$  el conjunto de dígitos. Consideremos la relación *display* del ejemplo 3.3 (a la cual renombramos con la letra  $G$ ):

$$G = \left\{ \begin{array}{l} (0, 6), (1, 2), (2, 5), (3, 5), (4, 4), \\ (5, 5), (6, 6), (7, 3), (8, 7), (9, 6) \end{array} \right\}.$$

Esta relación es una función sobre  $D$  porque:

- 1) Todos los dígitos aparecen como primera coordenada de algún par en la relación. Así,  $\text{dom}(G) = D$ .
- 2) No existen pares con primeras coordenadas iguales y segundas coordenadas distintas.

Desde ahora, llamaremos a esta relación  $G$  la “función *display*”.

**Ejemplo 3.14.** La relación

$$U = \{(1, 2), (3, 4), (3, 5)\},$$

no es una función porque no se cumple la propiedad 2) de la definición 3.11. La razón de esto es que 3 es un elemento del dominio al que le corresponden dos elementos distintos del rango: 4 y 5.

**Ejemplo 3.15.** Sólo nueve de las relaciones de la tabla 3.1 son funciones. Explícitamente, estas funciones son:

$$R_9, R_{10}, R_{11}, R_{13}, R_{14}, R_{15}, R_{16}, R_{17} \text{ y } R_{18}.$$

¿Por qué las otras 55 relaciones de la tabla no son funciones?

**Ejemplo 3.16.** Consideremos la relación  $F : \mathbb{R} \rightarrow \mathbb{R}$  definida como

$$F = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}.$$

Entonces,  $F$  es una función:

- 1)  $\text{dom}(F) = \mathbb{R}$ , porque para cualquier  $a \in \mathbb{R}$  tenemos que  $(a, a^2) \in F$ .
- 2) Si  $(a, b), (a, c) \in F$ , entonces  $b = a^2$  y  $c = a^2$ . Por lo tanto,  $b = c$ .

En el ejemplo anterior fue sencillo expresar en símbolos la regla que define a la función  $F$ ; en tales casos es común identificar a la función misma con su regla definitoria. Será frecuente escribir expresiones como: “sea  $F(x) = x^2$  una función”, para referirse a la función definida por tal regla.

**Ejemplo 3.17.** Consideremos la relación  $K : \mathbb{R} \rightarrow \mathbb{R}$  definida como

$$K = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y^2\}.$$

En este caso  $K$  no es una función porque existen números reales a los que corresponden dos elementos distintos del rango. Por ejemplo, si  $x = 4$ , entonces  $(4, 2) \in K$  y  $(4, -2) \in K$ .

Definiremos algunos conceptos relacionados con funciones.

**Definición 3.18 (imagen y preimagen).** Sea  $F : A \rightarrow B$  una función y sea  $(a, b) \in F$ . Decimos que  $b$  es la *imagen* de  $a$  bajo  $F$ , y escribimos  $b = F(a)$ . También decimos que  $F$  está definida en  $a$ , y que  $a$  es una *preimagen* de  $b$ .

Es claro que, por definición, la imagen de cualquier elemento bajo cualquier función debe ser única, y que todos los pares de la función  $F$  pueden escribirse como  $(a, F(a))$ , donde  $a \in \text{dom}(F)$ .

**Definición 3.19 (rango).** El *rango* de la función  $F : A \rightarrow B$  es el conjunto de todas las posibles imágenes de los elementos de  $A$ :

$$\text{ran}(F) = \{F(a) \in B : a \in A\}.$$

La definición del rango de una función  $F$  coincide con la definición del rango de  $F$  vista como relación.

**Ejemplo 3.20.** Sea  $G$  la función *display* del ejemplo 3.13. El dominio y el codominio de  $G$  son iguales al conjunto de dígitos  $D$ . El rango de la función es

$$\text{ran}(G) = \{2, 3, 4, 5, 6, 7\}.$$

**Ejemplo 3.21.** Consideremos la función  $F : \mathbb{R} \rightarrow \mathbb{R}$  del ejemplo 3.16. El rango de  $F$  es

$$\text{ran}(F) = \{x^2 : x \in \mathbb{R}\} = \{y \in \mathbb{R} : y \geq 0\},$$

ya que cualquier número real mayor o igual que cero puede escribirse como el cuadrado de otro número real.

**Definición 3.22 (imagen de un conjunto).** Sea  $F : A \rightarrow B$  una función y  $C \subseteq A$ . Definimos la *imagen del conjunto*  $C$  como

$$F(C) = \{F(a) \in B : a \in C\}.$$

Claramente,  $F(C) \subseteq \text{ran}(F)$ . Con la notación anterior, el uso de los símbolos  $F(A)$  y  $\text{ran}(F)$  es intercambiable; es decir, para cualquier función  $F : A \rightarrow B$  se cumple que  $F(A) = \text{ran}(F)$ .

**Definición 3.23 (preimagen de un conjunto).** Sea  $F : A \rightarrow B$  una función y  $E \subseteq B$ . Se llama *preimagen del conjunto*  $E$  al conjunto

$$F^{-1}(E) = \{a \in A : F(a) \in E\}.$$

El conjunto  $F^{-1}(E)$  coincide con la imagen de  $E$  bajo la *relación inversa* de  $F$ , la cual definiremos más adelante.

**Ejemplo 3.24.** Sea  $F : A \rightarrow B$  una función. Si  $b \in B$ , entonces

$$F^{-1}(\{b\}) = \{a \in A : F(a) = b\};$$

es decir,  $F^{-1}(\{b\})$  es el conjunto de las preimágenes de  $b$ . Para simplificar la notación, escribimos simplemente  $F^{-1}(b)$ .

**Ejemplo 3.25.** Sea  $G$  la función *display* del ejemplo 3.13,

$$G = \left\{ \begin{array}{l} (0, 6), (1, 2), (2, 5), (3, 5), (4, 4), \\ (5, 5), (6, 6), (7, 3), (8, 7), (9, 6) \end{array} \right\}.$$

1) Las imágenes de cada  $x \in \text{dom}(G)$  son:

$$G(0) = G(6) = G(9) = 6,$$

$$G(1) = 2,$$

$$G(2) = G(3) = G(5) = 5,$$

$$G(4) = 4,$$

$$G(7) = 3,$$

$$G(8) = 7.$$

2) Sea  $C = \{0, 6, 9\} \subseteq \text{dom}(G)$ . La imagen del conjunto  $C$  es

$$G(C) = \{6\} \subseteq \text{ran}(G).$$

3) Sea  $E = \{5, 6\} \subseteq \text{ran}(G)$ . La preimagen del conjunto  $E$  es

$$G^{-1}(E) = \{0, 2, 3, 5, 6, 9\} \subseteq \text{dom}(G).$$

### 3.1.3 Tipos de funciones

**Definición 3.26 (función inyectiva).** Decimos que una función

$$F : A \rightarrow B$$

es *inyectiva* si  $(a_1, b), (a_2, b) \in F$  implica que  $a_1 = a_2$ .

Otras formas lógicamente equivalentes de formular la definición de función inyectiva son:

1)  $F$  es inyectiva si y sólo si  $F(a_1) = F(a_2)$  implica que  $a_1 = a_2$ .

2)  $F$  es inyectiva si y sólo si  $a_1 \neq a_2$  implica que  $F(a_1) \neq F(a_2)$ .

3)  $F$  es inyectiva si y sólo si cada elemento del dominio de  $F$  tiene una imagen distinta en el rango.

**Definición 3.27 (función sobreyectiva).** Decimos que una función  $F : A \rightarrow B$  es *sobreyectiva* si para toda  $b \in B$  existe  $a \in A$  tal que  $b = F(a)$ . En otras palabras,  $F$  es sobreyectiva si  $\text{ran}(F) = B$ .

La definición de función sobreyectiva depende del conjunto al que consideremos como codominio. Por ejemplo, la función

$$F_0 : \{0, 1\} \rightarrow \{a, b, c\}, F_0 = \{(0, a), (1, b)\}$$

no es sobreyectiva porque  $c$  no tiene ninguna preimagen. Sin embargo, modificando el codominio definimos una función sobreyectiva como

$$F_1 : \{0, 1\} \rightarrow \{a, b\}, F_1 = \{(0, a), (1, b)\}.$$

A pesar de que ambas funciones,  $F_1$  y  $F_0$ , están definidas exactamente por los mismos pares, una es sobreyectiva y la otra no. La conclusión es que para determinar si una función es sobreyectiva es importante conocer el codominio de la función.

**Definición 3.28 (función biyectiva).** Decimos que una función es *biyectiva* si es a la vez inyectiva y sobreyectiva.

**Ejemplo 3.29.** Las funciones  $R_{10}, R_{11}, R_{13}, R_{15}, R_{16}$  y  $R_{17}$  de la tabla 3.1 son inyectivas. ¿Puedes explicar por qué las funciones  $R_9, R_{14}$  y  $R_{18}$  no lo son?

**Ejemplo 3.30.** Ninguna de las funciones del ejemplo 3.15 es sobreyectiva.

**Ejemplo 3.31.** Consideremos las funciones definidas en los siguientes diagramas. Las flechas determinan la imagen de los puntos del dominio.

- 1) La función de la figura 3.4 no es inyectiva porque dos flechas llegan a un mismo punto del codominio ni sobreyectiva porque hay un punto en el codominio al que no llega ninguna flecha.
- 2) La función de la figura 3.5 es inyectiva porque a ningún elemento del codominio llega más de una flecha.
- 3) La función de la figura 3.6 es sobreyectiva porque a todos los puntos del codominio llega al menos una flecha.
- 4) La función de la figura 3.7 es biyectiva.

**Ejemplo 3.32.** Todas las funciones definidas sobre  $A = \{a, b\}$  son:

$$F_1 = \{(a, a), (b, a)\}, F_2 = \{(a, a), (b, b)\},$$

$$F_3 = \{(a, b), (b, a)\}, F_4 = \{(a, b), (b, b)\}.$$

En este caso, sólo  $F_2$  y  $F_3$  son biyectivas.

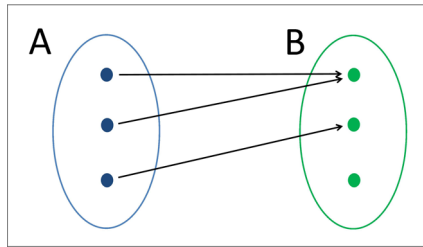


Figura 3.4: Función no inyectiva ni sobreyectiva.

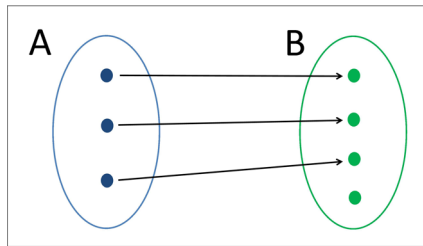


Figura 3.5: Función inyectiva no sobreyectiva.

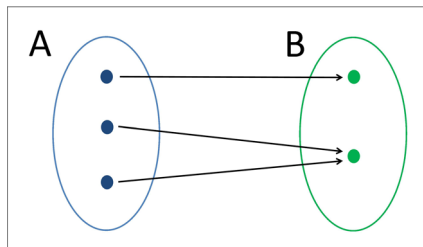


Figura 3.6: Función sobreyectiva no inyectiva.

**Ejemplo 3.33.** Si  $A = \{1, 2, 3\}$  y  $B = \{a, b\}$ , todas las funciones de  $A$  en  $B$  son:

$$H_1 = \{(1, a), (2, a), (3, a)\}, \quad H_2 = \{(1, a), (2, a), (3, b)\},$$

$$H_3 = \{(1, a), (2, b), (3, a)\}, \quad H_4 = \{(1, b), (2, a), (3, a)\},$$

$$H_5 = \{(1, a), (2, b), (3, b)\}, \quad H_6 = \{(1, b), (2, a), (3, b)\},$$

$$H_7 = \{(1, b), (2, b), (3, a)\}, \quad H_8 = \{(1, b), (2, b), (3, b)\}.$$

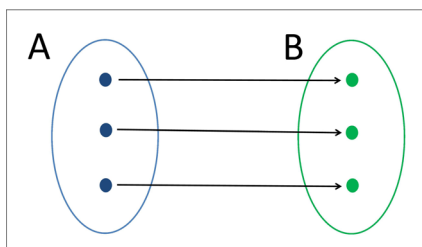


Figura 3.7: Función biyectiva.

Todas estas funciones, excepto  $H_1$  y  $H_8$ , son sobreyectivas; sin embargo, ninguna es inyectiva. Compara esto con las funciones del ejemplo 3.15.

### 3.1.4 Composición de funciones

**Definición 3.34 (composición de funciones).** Sean  $F : A \rightarrow B$  y  $G : B \rightarrow C$  funciones. La *composición de  $F$  con  $G$*  es la función

$$G \circ F : A \rightarrow C,$$

definida como

$$G \circ F = \{ (a, G(F(a))) : a \in A \}.$$

Recordemos que si  $F : A \rightarrow B$  es una función, la imagen de  $a \in A$  es  $F(a) \in \text{ran}(F) \subseteq B$ . Para formar la composición de  $F$  con alguna otra función  $G$  es necesario que  $F(a)$  siempre sea un elemento del dominio de  $G$ ; en tal caso tiene sentido escribir  $G(F(a)) \in \text{ran}(G)$ . Si, por otro lado,  $H$  es una función tal que  $\text{ran}(F) \not\subseteq \text{dom}(H)$ , entonces no es posible formar la composición de  $F$  con  $H$ .

En resumen,

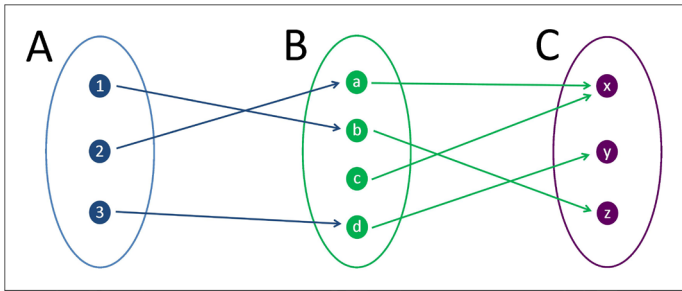
$$G \circ F \text{ existe} \iff \text{ran}(F) \subseteq \text{dom}(G).$$

**Ejemplo 3.35.** Sean  $A = \{1, 2, 3\}$ ,  $B = \{a, b, c, d\}$  y  $C = \{x, y, z\}$ . Consideremos las funciones  $F : A \rightarrow B$  y  $G : B \rightarrow C$  definidas como

$$F = \{(1, b), (2, a), (3, d)\} \text{ y } G = \{(a, x), (b, z), (c, x), (d, y)\}.$$

Entonces, la composición de  $F$  con  $G$  es:

$$G \circ F = \{(1, z), (2, x), (3, y)\}.$$

Figura 3.8: Composición de  $F$  con  $G$ .

La forma de hacer esta composición se ilustra en la Figura 3.8.

En este ejemplo es claro que no podemos formar la composición opuesta,  $F \circ G$ , debido a que expresiones como  $F(G(a))$  no tienen sentido (en este caso,  $G(a) = x$  pero  $F$  no está definida en  $x$ ).

**Ejemplo 3.36.** Sea  $F$  la función cuyos pares  $(x, y)$  se forman de la siguiente manera:  $x$  es un dígito escrito en sistema binario, mientras que  $y$  es el mismo dígito escrito en sistema decimal. Entonces:

$$F = \left\{ \begin{array}{l} (0000, 0), (0001, 1), (0010, 2), (0011, 3), (0100, 4), \\ (0101, 5), (0110, 6), (0111, 7), (1000, 8), (1001, 9) \end{array} \right\}.$$

Sea  $G$  la función *display*

$$G = \left\{ \begin{array}{l} (0, 6), (1, 2), (2, 5), (3, 5), (4, 4), \\ (5, 5), (6, 6), (7, 3), (8, 7), (9, 6) \end{array} \right\}.$$

La composición de  $F$  con  $G$  asigna a cada dígito escrito en sistema binario el número de segmentos que se encienden en el *display* para mostrar dicho número en decimal. Explícitamente, los pares de  $G \circ F$  son:

$$G \circ F = \left\{ \begin{array}{l} (0000, 6), (0001, 2), (0010, 5), (0011, 5), (0100, 4), \\ (0101, 5), (0110, 6), (0111, 3), (1000, 7), (1001, 6) \end{array} \right\}.$$

**Ejemplo 3.37.** Consideremos las funciones  $F : \mathbb{R} \rightarrow \mathbb{R}$  y  $G : \mathbb{R} \rightarrow \mathbb{R}$  definidas como  $F(x) = x^2$  y  $G(x) = x^3$  para  $x \in \mathbb{R}$ . Entonces,

$$(G \circ F)(x) = G(F(x)) = G(x^2) = (x^2)^3 = x^6.$$

La siguiente definición hace referencia a relaciones en general, aunque nuestro interés principal estará en el caso particular de las funciones.



**Definición 3.38 (relación inversa).** Sea  $R : A \rightarrow B$  una relación. La *relación inversa de  $R$* , denotada como  $R^{-1}$ , es la relación

$$R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}.$$

Por definición, el dominio de  $R$  coincide con el rango de  $R^{-1}$ , y viceversa:

$$\begin{aligned} \text{dom}(R^{-1}) &= \text{ran}(R), \\ \text{ran}(R^{-1}) &= \text{dom}(R). \end{aligned}$$

**Proposición 3.39.** Sea  $R : A \rightarrow B$  una relación. Entonces,

$$(R^{-1})^{-1} = R.$$

**Demostración.** Por definición,

$$(R^{-1})^{-1} = \{(a, b) \in A \times B : (b, a) \in R^{-1}\}.$$

Nuevamente por definición, sabemos que

$$(b, a) \in R^{-1} \iff (a, b) \in R;$$

por lo tanto, podemos reemplazar la propiedad que define al conjunto  $(R^{-1})^{-1}$  para obtener que

$$(R^{-1})^{-1} = \{(a, b) \in A \times B : (a, b) \in R\} = R.$$

■

**Ejemplo 3.40.** Sea  $F$  la función del ejemplo 3.36. Su relación inversa es:

$$F^{-1} = \left\{ \begin{array}{l} (0, 0000), (1, 0001), (2, 0010), (3, 0011), (4, 0100), \\ (5, 0101), (6, 0110), (7, 0111), (8, 1000), (9, 1001) \end{array} \right\}.$$

Observemos que en este caso  $F^{-1}$  es también una función.

En general, la inversa de una relación es una relación; sin embargo, no siempre se cumple que la inversa de una función sea una función.

**Ejemplo 3.41.** Sea  $G$  la función display del ejemplo 3.13. La relación inversa de  $G$  es

$$G^{-1} = \left\{ \begin{array}{l} (2, 1), (3, 7), (4, 4), (5, 2), (5, 3), \\ (5, 5), (6, 0), (6, 6), (6, 9), (7, 8) \end{array} \right\}.$$

En este caso,  $G^{-1}$  no es una función ya que, por ejemplo,  $5 \in \text{dom}(G^{-1})$  tiene tres imágenes distintas.

**Ejemplo 3.42.** Las inversas de las funciones  $F_2 = \{(a, a), (b, b)\}$  y  $F_3 = \{(a, b), (b, a)\}$  del ejemplo 3.32 son funciones:

$$F_2^{-1} = \{(a, a), (b, b)\},$$

$$F_3^{-1} = \{(a, b), (b, a)\}.$$

El siguiente teorema examina una clase de funciones cuya inversa siempre es una función. Más adelante veremos que esta clase es la única donde sucede.

**Teorema 3.43.** Sea  $F : A \rightarrow B$  una función biyectiva. Entonces, la relación inversa de  $F$  es una función y es biyectiva.

**Demostración.** Para demostrar que  $F^{-1} : B \rightarrow A$  es una función debemos comprobar dos cosas: 1)  $\text{dom}(F^{-1}) = B$ , y 2) si  $(b, a_1), (b, a_2) \in F^{-1}$ , entonces  $a_1 = a_2$ .

- 1) La relación inversa de  $F$  cumple que  $\text{dom}(F^{-1}) = \text{ran}(F)$ . Como  $F$  es sobreyectiva,  $\text{ran}(F) = B$ . Por lo tanto,  $\text{dom}(F^{-1}) = B$ .
- 2) Si  $(b, a_1), (b, a_2) \in F^{-1}$ , por definición de inversa, tenemos que  $(a_1, b), (a_2, b) \in F$ . Como  $F$  es inyectiva, concluimos que  $a_1 = a_2$ .

Ahora, para demostrar que  $F^{-1}$  es biyectiva tenemos que comprobar dos cosas: 3)  $F^{-1}$  es inyectiva, y 4)  $F^{-1}$  es sobreyectiva.

- 3) Si  $(b_1, a), (b_2, a) \in F^{-1}$ , por definición de inversa, tenemos que  $(a, b_1), (a, b_2) \in F$ . Como  $F$  es una función, concluimos que  $b_1 = b_2$ .
- 4) La relación inversa de  $F$  cumple que  $\text{ran}(F^{-1}) = \text{dom}(F)$ . Como  $F$  es una función,  $\text{dom}(F) = A$ . Por lo tanto,  $\text{ran}(F^{-1}) = A$ . ■

Para cualquier conjunto  $A$ , la *función identidad en  $A$* , denotada como  $I_A : A \rightarrow A$ , es la función definida por la regla  $I_A(a) = a$ ,  $\forall a \in A$ ; en otras palabras,

$$I_A = \{(a, a) : a \in A\}.$$

Claramente, si  $F : A \rightarrow B$  es una función, la identidad  $I_A$  cumple que

$$F \circ I_A = F,$$

mientras que la identidad  $I_B$  cumple que

$$I_B \circ F = F.$$

**Teorema 3.44.** Sea  $F : A \rightarrow B$  una función y supongamos que  $F^{-1} : B \rightarrow A$  es también una función. Entonces,

$$F \circ F^{-1} = I_B \text{ y } F^{-1} \circ F = I_A.$$

**Demostración.** Sabemos que  $(a, b) \in F$  si y sólo si  $(b, a) \in F^{-1}$ . En otras palabras,  $F(a) = b$  si y sólo si  $F^{-1}(b) = a$ . Con esto, vemos que

$$F \circ F^{-1}(b) = F(F^{-1}(b)) = F(a) = b.$$

para toda  $b \in B$ . Por lo tanto,  $F \circ F^{-1} = I_B$ . De manera similar,

$$F^{-1} \circ F(a) = F^{-1}(F(a)) = F^{-1}(b) = a,$$

para toda  $a \in A$ . Por lo tanto,  $F^{-1} \circ F = I_A$ . ■

**Teorema 3.45.** Sean  $F : A \rightarrow B$  y  $G : B \rightarrow A$  funciones.

- 1) Si  $G \circ F = I_A$ , entonces  $F$  es inyectiva.
- 2) Si  $F \circ G = I_B$ , entonces  $F$  es sobreyectiva.

**Demostración.** Demostraremos cada una de las afirmaciones.

- 1) Supongamos que  $F(a_1) = F(a_2)$  donde  $a_1, a_2 \in A$ . Aplicando la función  $G$  y usando la hipótesis  $G \circ F = I_A$ , vemos que:

$$\begin{aligned} F(a_1) = F(a_2) &\Rightarrow G(F(a_1)) = G(F(a_2)) \\ &\Rightarrow (G \circ F)(a_1) = (G \circ F)(a_2) \\ &\Rightarrow I_A(a_1) = I_A(a_2) \\ &\Rightarrow a_1 = a_2. \end{aligned}$$

Esto demuestra que  $F$  es inyectiva.

- 2) Debemos demostrar que para toda  $b \in B$  existe  $a \in A$  tal que  $F(a) = b$ . Sea  $b \in B$  un elemento arbitrario de  $B$ . Definamos  $a = G(b) \in A$ . Entonces, por hipótesis

$$\begin{aligned} F(a) &= F(G(b)) \\ &= (F \circ G)(b) \\ &= I_B(b) = b. \end{aligned}$$

Esto demuestra que  $F$  es sobreyectiva. ■

**Corolario 3.46.** Sea  $F : A \rightarrow B$  una función tal que su relación inversa es también una función. Entonces  $F$  es biyectiva.

**Demostración.** Por el teorema 3.44, la función  $F$  satisface las hipótesis del teorema 3.45 con  $G = F^{-1}$ . Así,  $F$  es inyectiva y sobreyectiva, y por lo tanto, biyectiva. ■

De esta manera el corolario 3.46 y el teorema 3.43 implican el siguiente teorema.

**Teorema 3.47 (función inversa).** Una función es biyectiva si y sólo si su relación inversa es una función.

**Palabras clave de la sección:** *relación; dominio; codominio; imagen; función; función inyectiva, sobreyectiva y biyectiva; composición de funciones; relación inversa; función identidad.*

### 3.1.5 Ejercicios de funciones

**Ejercicio 3.48.** Encuentra todas las relaciones de  $A = \{0, 1\}$  en  $B = \{a, b\}$ . ¿Cuáles de estas relaciones son funciones? Determina cuáles son funciones de los siguientes tipos:

- a) No inyectivas ni sobreyectivas.
- b) Inyectivas pero no sobreyectivas.
- c) Sobreyectivas pero no inyectivas.
- d) Biyectivas.

**Ejercicio 3.49.** Considera las funciones

$$F = \{(0, 0), (1, 2), (2, 4), (3, 6), (4, 8), (5, 10), (6, 12)\},$$

$$G = \left\{ \begin{array}{l} (0, 0), (1, 1), (2, 0), (3, 1), (4, 0), \\ (5, 1), (6, 0), (8, 0), (12, 0) \end{array} \right\}.$$

- a) Encuentra las imágenes  $F(3)$ ,  $F(4)$ ,  $G(0)$  y  $G(8)$ .
- b) Encuentra los conjuntos  $\text{dom}(F)$ ,  $\text{ran}(F)$ ,  $\text{dom}(G)$  y  $\text{ran}(G)$ .
- c) Si  $J = \{0, 3, 5\}$ , encuentra  $F(J)$  y  $G(J)$ .
- d) Encuentra  $F^{-1}(\{10, 12\})$ ,  $F^{-1}(0)$  y  $G^{-1}(0)$ .
- e) Determina si  $F$  y  $G$  son funciones inyectivas. Justifica.
- f) Determina si es posible hacer las composiciones  $G \circ F$ ,  $F \circ G$  y, en caso de que sea posible escríbelas. Justifica tu respuesta.
- g) Encuentra las relaciones inversas de  $F$  y  $G$ . Determina si estas relaciones son funciones.

**Ejercicio 3.50.** Considera las funciones  $F_i : \mathbb{R} \rightarrow \mathbb{R}$  definidas por las siguientes reglas:

$$F_1(x) = x^2, \quad F_2(x) = x^3, \quad F_3(x) = 2^x, \quad F_4(x) = 5x + 1.$$

Responde lo siguiente justificando en cada caso:

- a) ¿Cuáles de estas funciones son inyectivas?
- b) ¿Cuáles de estas funciones son sobreyectivas?
- c) ¿Cuáles de estas funciones son biyectivas? Encuentra la función inversa de cada una de estas funciones biyectivas.
- d) Encuentra las siguientes composiciones:

$$F_3 \circ F_1, \quad F_2 \circ F_3, \quad F_1 \circ F_4, \quad F_4 \circ F_3 \quad \text{y} \quad F_3 \circ F_2 \circ F_1.$$

## 3.2 Relaciones de equivalencia

Parte del trabajo de un matemático es hacer *generalizaciones*; es decir, encontrar y describir las propiedades de objetos particulares para estudiarlas en una variedad de objetos más amplia.

Tomando como ejemplo al conjunto de números, en esta sección generalizamos una de sus relaciones más importantes: la igualdad. ¿Cuáles son las propiedades esenciales de la igualdad entre números?

Nos enfocamos en estudiar relaciones *sobre* conjuntos (recordemos que  $R$  es una relación sobre  $A$  si  $R \subseteq A \times A$ ). Una forma alternativa para denotar que  $(a, b) \in R$  es escribir  $aRb$ .

**Definición 3.51.** Sea  $R$  una relación sobre  $A$ .

- 1) Decimos que  $R$  es *reflexiva* si  $aRa$  para toda  $a \in A$ .
- 2) Decimos que  $R$  es *simétrica* si  $aRb$  implica que  $bRa$ .
- 3) Decimos que  $R$  es *transitiva* si  $aRb$  y  $bRc$  implica que  $aRc$ .

**Definición 3.52 (relación de equivalencia).** Sea  $R$  una relación sobre  $A$ . Decimos que  $R$  es una *relación de equivalencia sobre  $A$*  si  $R$  es reflexiva, simétrica y transitiva.

**Ejemplo 3.53.** La relación de igualdad entre números reales, denotada como “=”, es de equivalencia. Estrictamente, esta relación es igual al conjunto

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y\},$$

pero, como en el caso de las funciones, nos referimos a ella simplemente por la regla que la define.

La igualdad es la relación de equivalencia arquetípica: sus propiedades son la fuente de inspiración de la definición general.

- 1) La igualdad es *reflexiva* porque  $x = x$  para toda  $x \in \mathbb{R}$ .
- 2) La igualdad es *simétrica* porque si  $x = y$  entonces  $y = x$ .
- 3) La igualdad es *transitiva* porque si  $x = y$ ,  $y = z$  entonces  $x = z$ .

Observemos que la relación de igualdad coincide con la función identidad en  $\mathbb{R}$ .

**Ejemplo 3.54.** Consideremos la siguiente relación sobre  $\{1, 2, 3, 4\}$ :

$$R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (3, 4), (4, 3)\}.$$

Demostraremos que  $R_1$  se trata de una relación de equivalencia.

- 1) La relación es *reflexiva* porque todos los pares  $(1, 1)$ ,  $(2, 2)$ ,  $(3, 3)$  y  $(4, 4)$  pertenecen a  $R_1$ .
- 2) La relación es *simétrica* porque los pares  $(1, 2)$ ,  $(2, 1)$ ,  $(3, 4)$  y  $(4, 3)$  pertenecen a  $R_1$ .
- 3) La relación es *transitiva* porque  $(a, b), (b, c) \in R_1$  implica que  $(a, c) \in R_1$ .

**Ejemplo 3.55.** Consideremos la relación sobre el conjunto de personas definida por la regla: “A tiene el mismo color de ojos que B”.

- 1) Esta relación es reflexiva porque cualquier persona tiene el mismo color de ojos que ella misma.
- 2) Es simétrica porque si A tiene el mismo color de ojos que B, entonces B tiene el mismo color de ojos que A.
- 3) Es transitiva porque si A tiene el mismo color de ojos que B, y B tiene el mismo color de ojos que C, entonces A tiene el mismo color de ojos que C.

**Ejemplo 3.56.** Las siguientes relaciones no son de equivalencia:

- 1) La relación “ $x$  es menor o igual que  $y$ ”, denotada como  $\leq$ , sobre los números reales, no es simétrica.
- 2) La relación “A es compañero de clase de B”, sobre el conjunto de estudiantes, no es ni reflexiva ni transitiva.
- 3) La relación “A es padre de B”, sobre el conjunto de personas, no es ni reflexiva, ni simétrica, ni transitiva.

**Definición 3.57 (clase de equivalencia).** Sea  $R$  una relación de equivalencia sobre  $A$ . La *clase de equivalencia* de un elemento  $a \in A$ , denotada como  $[a]$ , es el subconjunto de  $A$  definido como

$$[a] = \{x \in A : xRa\}.$$

Debido a que cualquier relación de equivalencia es reflexiva, tenemos que  $a \in [a]$  para toda  $a \in A$ .

**Definición 3.58 (conjunto cociente).** Sea  $R$  una relación de equivalencia sobre  $A$ . El *conjunto cociente* de  $A$  por  $R$ , denotado como  $A/R$ , es el conjunto de clases de equivalencia de los elementos de  $A$ . En otras palabras,

$$A/R = \{[a] : a \in A\}.$$

La idea detrás de la definición del conjunto cociente  $A/R$  es la de considerar a todos los elementos de  $A$  que no sean equivalentes entre sí.

**Proposición 3.59.** Sea  $R$  una relación de equivalencia sobre  $A$ . Las clases de equivalencia  $[a]$  y  $[b]$  son iguales si y sólo si  $aRb$ .

**Demostración.**

- ( $\Rightarrow$ ) Supongamos que  $[a] = [b]$ . Como  $a \in [a]$ , tenemos que  $a \in [b]$ . La definición de clase de equivalencia implica que  $aRb$ .
- ( $\Leftarrow$ ) Supongamos que  $aRb$ . Usaremos la proposición 2.18. Primero demostraremos que  $[a] \subseteq [b]$ . Sea  $x \in [a]$  un elemento arbitrario. Entonces  $xRa$ , y por transitividad,  $xRb$ . Por lo tanto,  $x \in [b]$ , lo que demuestra que  $[a] \subseteq [b]$ . Sea ahora  $y \in [b]$  un elemento arbitrario. Entonces  $yRb$ . Por simetría, como  $aRb$ , tenemos que  $bRa$ . Luego, por transitividad,  $yRa$  y  $y \in [a]$ . Esto demuestra que  $[b] \subseteq [a]$ . Por lo tanto  $[a] = [b]$ . ■

**Ejemplo 3.60.** La relación  $R_1$  del ejemplo 3.54 tiene dos clases de equivalencia: la clase de 1 (que es igual a la clase de 2 porque  $(1, 2) \in R_1$ ) y la clase de 3 (que es igual a la clase de 4). Por lo tanto,

$$A/R_1 = \{ [1], [3] \},$$

donde

$$[1] = [2] = \{1, 2\} \text{ y } [3] = [4] = \{3, 4\}.$$

**Ejemplo 3.61.** Todas las clases de equivalencia de la relación de igualdad sobre  $\mathbb{R}$  contienen sólo un número; es decir,  $[x] = \{x\}$ ,  $\forall x \in \mathbb{R}$ .

**Ejemplo 3.62.** Las clases de equivalencia de la relación “ $A$  tiene el mismo color de ojos que  $B$ ” sobre el conjunto de personas, están determinadas por los posibles colores de ojos. Así pues, si Juan tiene ojos negros, Elisa ojos cafés, Daniela ojos verdes y Pedro ojos



azules, entonces (considerando cierta variación en los colores), el conjunto cociente en este caso es igual a

$$\{[Juan], [Elisa], [Daniela], [Pedro]\}.$$

Si Hugo también tiene ojos verdes, el representante de su clase es intercambiable (proposición 3.59); es decir,  $[Daniela] = [Hugo]$ .

La siguiente definición no hace referencia a relaciones de equivalencia; su relevancia se establecerá en los últimos teoremas de esta sección.

**Definición 3.63 (partición).** Sea  $A$  un conjunto. Una *partición* de  $A$  es un conjunto  $P$  tal que:

- 1) Los elementos de  $P$  son subconjuntos no vacíos de  $A$ .
- 2) La unión de los elementos de  $P$  es igual a  $A$ .
- 3) La intersección de cualquier par de elementos distintos de  $P$  es vacía.

**Ejemplo 3.64.** Consideremos el conjunto de dígitos,

$$D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Dos particiones distintas de  $D$  son:

$$P_1 = \{\{0, 1\}, \{2, 3, 7\}, \{5, 9\}, \{4, 6\}, \{8\}\},$$

$$P_2 = \{\{0, 1, 2, 3, 4, 5\}, \{6\}, \{7\}, \{8\}, \{9\}\}.$$

Es sencillo comprobar que  $P_1$  y  $P_2$  cumplen las propiedades 1) – 3) de la definición 3.63: claramente, la unión de sus elementos es  $D$ , mientras que la intersección de cualquier par de elementos distintos es vacía.

**Ejemplo 3.65.** Sea  $2\mathbb{Z}$  el conjunto de enteros pares e  $\mathbb{I}$  el conjunto de enteros impares,

$$2\mathbb{Z} = \{2n : n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \dots\},$$

$$\mathbb{I} = \{2n + 1 : n \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \dots\}.$$

El conjunto

$$P = \{2\mathbb{Z}, \mathbb{I}\}$$

es una partición de  $\mathbb{Z}$ , ya que  $2\mathbb{Z} \cup \mathbb{I} = \mathbb{Z}$  mientras que  $2\mathbb{Z} \cap \mathbb{I} = \emptyset$ .

**Ejemplo 3.66.** Consideremos la relación de equivalencia  $R_1$  sobre  $A = \{1, 2, 3, 4\}$  del ejemplo 3.54. El conjunto cociente

$$A/R_1 = \{[1], [3]\} = \{\{1, 2\}, \{3, 4\}\},$$

es una partición de  $A$  porque

$$A = \{1, 2\} \cup \{3, 4\} \text{ y } \{1, 2\} \cap \{3, 4\} = \emptyset.$$

El ejemplo anterior ilustra un hecho más general.

**Teorema 3.67.** Sea  $R$  una relación de equivalencia sobre  $A$ . Entonces el conjunto cociente  $A/R$  es una partición de  $A$ .

**Demostración.** Demostraremos que se cumplen las tres propiedades de la definición de partición de un conjunto:

- 1) Los elementos de  $A/R$  son subconjuntos no vacíos de  $A$  porque las clases de equivalencia son subconjuntos no vacíos de  $A$ .
- 2) Debemos demostrar que  $A$  es igual a la unión de todas sus clases de equivalencia; en símbolos,

$$A = \bigcup_{a \in A} [a].$$

Claramente,  $\cup_{a \in A} [a] \subseteq A$  porque todos los elementos de cualquier clase de equivalencia son elementos de  $A$ . Para demostrar que  $A \subseteq \cup_{a \in A} [a]$ , sea  $x \in A$  un elemento arbitrario. Debido a que  $x \in [x]$ , tenemos que  $x \in \cup_{a \in A} [a]$ . La igualdad queda demostrada.

- 3) Demostraremos que la intersección de dos clases de equivalencia distintas es vacía. Sean  $[a], [b] \in A/R$  clases de equivalencia,  $[a] \neq [b]$ . Usaremos reducción al absurdo. Supongamos que

$$[a] \cap [b] \neq \emptyset.$$

Entonces, existe  $c \in [a] \cap [b]$ . Por definición,  $c \in [a]$  y  $c \in [b]$ , así que  $cRa$  y  $cRb$ . Por simetría y transitividad, tenemos que  $aRb$ . Pero ahora, la proposición 3.59 implica que  $[a] = [b]$ , lo que contradice que las clases sean distintas. Por lo tanto,  $[a] \cap [b] = \emptyset$ . ■

El siguiente teorema describe cómo es posible definir una relación de equivalencia sobre un conjunto usando una partición del conjunto.

**Teorema 3.68.** Sea  $P$  una partición de un conjunto  $A$ . Entonces la relación  $R_P$  sobre  $A$  definida como

$$R_P = \{(a, b) \in A \times A : a, b \in E \text{ para algún } E \in P\}$$

es una relación de equivalencia. Además, se cumple que  $P = A/R_P$ .

**Demostración.** Demostraremos que la relación  $R_P$  es reflexiva, simétrica y transitiva:

- 1) *Reflexividad.* Como la unión de los elementos de  $P$  es igual a  $A$ , para cualquier  $a \in A$  existe  $E \in P$  tal que  $a \in E$ . Por lo tanto,  $aR_P a$  para toda  $a \in A$ .
- 2) *Simetría.* Si  $aR_P b$ , entonces  $a, b \in E$  para algún  $E \in P$ . Claramente, también se cumple que  $b, a \in E$ , así que  $bR_P a$ .
- 3) *Transitividad.* Supongamos que  $aR_P b$  y  $bR_P c$ . Entonces, existen  $E_1, E_2 \in P$  tales que  $a, b \in E_1$  y  $b, c \in E_2$ . Como  $b \in E_1 \cap E_2$ , la intersección de  $E_1$  y  $E_2$  es no vacía. Por la propiedad 3) de las particiones, deducimos que  $E_1 = E_2$ . Por lo tanto,  $a, c \in E_1 = E_2$ , lo que significa que  $aR_P c$ .

Se deja como ejercicio comprobar que  $P = A/R_P$ . ■

**Ejemplo 3.69.** Consideremos la partición  $P = \{2\mathbb{Z}, \mathbb{I}\}$  de  $\mathbb{Z}$ . La relación de equivalencia  $R_P$  sobre  $\mathbb{Z}$  inducida por esta partición es

$$R_P = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : (a, b \in 2\mathbb{Z}) \vee (a, b \in \mathbb{I})\} = (2\mathbb{Z} \times 2\mathbb{Z}) \cup (\mathbb{I} \times \mathbb{I}).$$

En otras palabras,  $R_P$  relaciona a los números pares con los pares y a los números impares con los impares.

**Ejemplo 3.70.** Sea  $R_1$  la relación de equivalencia sobre

$$A = \{1, 2, 3, 4\}$$

del ejemplo 3.54. Consideremos la siguiente partición de  $A$ :

$$P = \{\{1, 2\}, \{3, 4\}\} = A/R_1.$$

La relación de equivalencia  $R_P$  inducida por esta partición es:

$$\begin{aligned} R_P &= \{(a, b) \in A \times A : (a, b \in \{1, 2\}) \vee (a, b \in \{3, 4\})\} \\ &= \{(1, 1), (2, 2), (1, 2), (2, 1), (3, 3), (4, 4), (3, 4), (4, 3)\}. \end{aligned}$$

Observemos que  $R_P = R_1$ .

No es difícil darse cuenta de que si  $P = \{E_1, E_2, \dots, E_n\}$  es una partición de  $A$ , entonces

$$R_P = (E_1 \times E_1) \cup (E_2 \times E_2) \cup \dots \cup (E_n \times E_n).$$

**Palabras clave de la sección:** *relación reflexiva, simétrica y transitiva; relación de equivalencia; clase de equivalencia; conjunto cociente; partición de un conjunto.*

### 3.2.1 Ejercicios de relaciones de equivalencia

**Ejercicio 3.71.** Determina si las siguientes relaciones son reflexivas, simétricas o transitivas. Justifica tu respuesta.

- a) La relación “ $A$  es hermano de  $B$ ” sobre el conjunto de personas.
- b) La relación  $R = \{(a, b) \in \mathbb{R} \times \mathbb{R} : a \cdot b = 1\}$ .
- c) La relación “ $A$  es subconjunto de  $B$ ” sobre el conjunto potencia de  $\mathbb{N}$ .
- d) La relación  $K = \{(a, b) \in \mathbb{R} \times \mathbb{R} : a^2 = b^2\}$ .

**Ejercicio 3.72.** Define relaciones sobre conjuntos tales que:

- a) La relación sea reflexiva, pero no simétrica ni transitiva.
- b) La relación sea reflexiva y simétrica, pero no transitiva.
- c) La relación sea transitiva, pero no reflexiva ni simétrica.
- d) La relación sea simétrica y transitiva, pero no reflexiva.

**Ejercicio 3.73.** Demuestra que cada una de las siguientes relaciones es de equivalencia y describe el conjunto cociente. ¿Cuál es la cardinalidad de estos conjuntos cociente?

- a) La relación “ $A$  cumple años el mismo día que  $B$ ” sobre el conjunto de personas.
- b) La relación  $L = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a - b \in 2\mathbb{Z}\}$ .
- c) La relación  $J = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a = \pm b\}$ .

**Ejercicio 3.74.** Determina cuáles de los siguientes conjuntos son particiones de  $\mathbb{Z}$ . Justifica tu respuesta en cada caso.

- a)  $P_1 = \{\{a \in \mathbb{Z} : a \leq 0\}, \{a \in \mathbb{Z} : a \geq 0\}\}$ .
- b)  $P_2 = \{\{a \in \mathbb{Z} : a^2 + 2a + 1 = 0\}, \{a \in \mathbb{Z} : (a \leq 2) \wedge (a \geq 2)\}, \{0, 1\}\}$ .
- c)  $P_3 = \{\{a \in \mathbb{Z} : (a \leq 2) \vee (a \geq 2)\}, \{a \in \mathbb{Z} : a^3 - a = 0\}\}$ .

**Ejercicio 3.75.** Encuentra una partición de  $\mathbb{Z}$  conformada por exactamente tres conjuntos infinitos y describe la relación de equivalencia inducida.

**Ejercicio 3.76.** Si  $P$  es una partición de  $A$ , demuestra que  $P = A/R_P$ .

### 3.3 Relaciones de orden

En esta sección generalizamos otra de las relaciones más importantes entre números: la relación  $\leq$  que los ordena. Al igual que antes, estamos interesados en relaciones *sobre* conjuntos.

**Definición 3.77 (relación antisimétrica).** Una relación  $R$  sobre un conjunto  $A$  es *antisimétrica* si  $aRb$  y  $bRa$  implica que  $a = b$ .

En otras palabras,  $R$  es antisimétrica si siempre que  $(a, b) \in R$ ,  $a \neq b$ , tenemos que  $(b, a) \notin R$ .

**Ejemplo 3.78.** La relación  $\leq$  sobre los números reales es antisimétrica: si  $x \leq y$ ,  $y \leq x$ , entonces  $x = y$ .

**Ejemplo 3.79.** Si  $X$  es un conjunto, la relación  $\subseteq$  sobre el conjunto potencia  $P(X)$  es antisimétrica: si  $B \subseteq C$  y  $C \subseteq B$ , entonces  $B = C$  (proposición 2.18).

La siguiente definición generaliza los ejemplos anteriores.

**Definición 3.80 (relación de orden).** Sea  $R$  una relación sobre  $A$ . Decimos que  $R$  es una *relación de orden* sobre  $A$  si  $R$  es reflexiva, antisimétrica y transitiva.

**Ejemplo 3.81.** La relación  $\leq$  sobre los números reales es una relación de orden, ya que es reflexiva, antisimétrica y transitiva.

**Definición 3.82 (conjunto ordenado).** Un *conjunto ordenado*<sup>2</sup> es un par  $(A, R)$ , donde  $A$  es un conjunto y  $R$  una relación de orden sobre  $A$ .

En lo sucesivo, cuando  $R$  sea una relación de orden, en lugar de escribir  $aRb$  para indicar que  $(a, b) \in R$ , escribiremos  $a \leq b$ . Esta notación está inspirada en la relación  $\leq$ . Como es usual, escribimos  $a < b$  cuando  $a \leq b$  y  $a \neq b$ .

Con esta nueva notación, las propiedades de una relación de orden sobre  $A$  son:

- 1) *Reflexividad.* Para cualquier  $a \in A$ , se cumple que  $a \leq a$ .
- 2) *Antisimetría.* Si  $a \leq b$  y  $b \leq a$  entonces  $a = b$ .
- 3) *Transitividad.* Si  $a \leq b$  y  $b \leq c$  entonces  $a \leq c$ .

---

<sup>2</sup>Algunos autores usan el término *conjunto parcialmente ordenado* para distinguirlo de los conjuntos *totalmente ordenados*, que se definirán más adelante.

**Ejemplo 3.83.** Sea  $X$  un conjunto. La relación  $\subseteq$  sobre el conjunto potencia  $P(X)$  es una relación de orden. Verifiquemos cada propiedad:

- 1) *Reflexividad.* Para cualquier  $B \in P(X)$ , se cumple que  $B \subseteq B$ .
- 2) *Antisimetría.* Si  $B \subseteq C$  y  $C \subseteq B$ , entonces  $B = C$ .
- 3) *Transitividad.* Si  $B \subseteq C$  y  $C \subseteq D$ , entonces  $B \subseteq D$ .

Llamamos *relación de inclusión* a esta relación de orden.

**Definición 3.84 (comparable).** Si  $(A, \leq)$  es un conjunto ordenado, decimos que dos elementos  $a, b \in A$  son *comparables* si  $a \leq b$  o  $b \leq a$ .

En general, pueden existir elementos de  $A$  que no sean comparables; es decir,  $a, b \in A$  tales que ni  $a \leq b$  ni  $b \leq a$ .

**Ejemplo 3.85.** Consideremos el conjunto ordenado  $(P(X), \subseteq)$  donde

$$X = \{w, x, y, z\}.$$

Los subconjuntos  $\{x, y\}$  y  $\{x, y, z\}$  son comparables porque

$$\{x, y\} \subseteq \{x, y, z\}.$$

Sin embargo, también existen subconjuntos de  $X$  que no son comparables. Por ejemplo,  $\{w, x\}$  y  $\{y, z\}$  no son comparables ya que

$$\{w, x\} \not\subseteq \{y, z\} \text{ y } \{y, z\} \not\subseteq \{w, x\}.$$

Cuando cualquier par de elementos es comparable, el conjunto ordenado  $(A, \leq)$  recibe un nombre especial.

**Definición 3.86 (orden total).** Sea  $(A, \leq)$  un conjunto ordenado. Decimos que  $\leq$  es una relación de *orden total*, o que  $(A, \leq)$  está *totalmente ordenado*, si cualquier par de elementos de  $A$  es comparable.

**Ejemplo 3.87.** La relación  $\leq$  sobre los números reales es de orden total: para cualesquiera  $x, y \in \mathbb{R}$  se cumple que  $x \leq y$  o  $y \leq x$ .

Una *cadena* de  $(A, \leq)$  es un subconjunto totalmente ordenado.

**Ejemplo 3.88.** Tomemos en cuenta el conjunto ordenado  $(P(X), \subseteq)$  del ejemplo 3.85. El subconjunto  $C$  de  $P(X)$  definido como

$$C = \{\{x, y, z\}, \{x, y\}, \{x\}\},$$

es una cadena, ya que cualquier par de elementos de  $C$  es comparable.

Ahora estudiaremos diferentes elementos especiales en conjuntos ordenados.

**Definición 3.89 (elemento maximal / minimal).** Sea  $(A, \leq)$  un conjunto ordenado.

- Un elemento  $m \in A$  es un *elemento maximal* de  $(A, \leq)$  si no existe ningún  $x \in A$  tal que  $m < x$ .
- Un elemento  $s \in A$  es un *elemento minimal* de  $(A, \leq)$  si no existe ningún  $x \in A$  tal que  $x < s$ .

**Ejemplo 3.90.** El conjunto  $(\mathbb{R}, \leq)$  no tiene elementos maximales ni minimales. Por otro lado, 0 es el único elemento minimal de  $(\mathbb{N}, \leq)$ .

**Ejemplo 3.91.** Sea  $X$  un conjunto y  $(P(X), \subseteq)$  el conjunto potencia ordenado por inclusión. Entonces, el conjunto vacío es el único elemento minimal y  $X$  es el único elemento maximal.

**Ejemplo 3.92.** Sea  $X = \{a, b, c\}$ . Observemos que el par

$$(P(X) \setminus \{\emptyset\}, \subseteq)$$

es un conjunto ordenado por inclusión cuyos elementos son los subconjuntos no vacíos de  $X$ . En este caso,  $X$  es el único elemento maximal, pero existen tres elementos minimales:  $\{a\}$ ,  $\{b\}$  y  $\{c\}$ .

Como vimos en los ejemplos anteriores, un conjunto ordenado puede no tener elementos maximales ni minimales y, si los tiene, éstos pueden no ser únicos. Sin embargo, para el caso de los conjuntos totalmente ordenados, tenemos el siguiente resultado.

**Proposición 3.93.** Sea  $(A, \leq)$  un conjunto totalmente ordenado. Si  $(A, \leq)$  tiene un elemento maximal, entonces éste es único.

**Demostración.** Por hipótesis existe un elemento maximal  $m \in A$ . Para demostrar su unicidad, sea  $m' \in A$  otro elemento maximal. Como el orden es total, debe cumplirse que  $m \leq m'$  o  $m' \leq m$ . Si  $m \leq m'$ , entonces  $m = m'$ , ya que no es posible que  $m < m'$  por definición de maximal. De manera similar, si  $m' \leq m$ , entonces  $m' = m$ . Esto demuestra que  $m$  es único. ■

Existe una proposición análoga a la anterior para los elementos minimales (ejercicio 3.107).

**Definición 3.94 (máximo / mínimo absoluto).** Sea  $(A, \leq)$  un conjunto ordenado.



- Un elemento  $m \in A$  es un *máximo absoluto* si  $x \preceq m, \forall x \in A$ .
- Un elemento  $s \in A$  es un *mínimo absoluto* si  $s \preceq x, \forall x \in A$ .

La diferencia clave entre un elemento maximal y un máximo absoluto es que el segundo debe ser comparable con *todos* los elementos. Claramente, un máximo absoluto también es un elemento maximal, pero un elemento maximal no siempre es un máximo absoluto. Además, un máximo absoluto, si existe, es único. Afirmaciones análogas se cumplen para los mínimos absolutos.

**Ejemplo 3.95.** Consideremos el conjunto

$$K = \{\{x\}, \{x, y\}, \{w, x, y, z\}, \{y, z\}\}$$

ordenado por inclusión. Los conjuntos  $\{x\}$  y  $\{y, z\}$  son los únicos elementos minimales de  $K$  (porque no existen elementos menores que ellos), pero ninguno es el mínimo absoluto de  $K$ , porque  $\{x\}$  y  $\{y, z\}$  no se pueden comparar entre sí. Por lo tanto,  $K$  no tiene un mínimo absoluto, pero sí tiene un máximo absoluto:  $\{w, x, y, z\}$ .

**Definición 3.96 (cota superior / inferior).** Sea  $B$  un subconjunto del conjunto ordenado  $(A, \preceq)$ .

- Un elemento  $k \in A$  es una *cota superior de  $B$*  si  $b \preceq k, \forall b \in B$ .
- Un elemento  $r \in A$  es una *cota inferior de  $B$*  si  $r \preceq b, \forall b \in B$ .

Si  $k$  es una cota superior de  $B$ , entonces cualquier otro elemento  $k' \in A$  tal que  $k \preceq k'$  también es una cota superior de  $B$ . Además, cualquier cota superior de  $B$  es una cota superior de cualquier subconjunto de  $B$ . Afirmaciones análogas se cumplen para las cotas inferiores.

**Ejemplo 3.97.** El número 0 es una cota inferior del subconjunto  $\mathbb{N}$  de  $(\mathbb{R}, \leq)$ , ya que  $0 \leq n, \forall n \in \mathbb{N}$ . Sin embargo,  $\mathbb{N}$  no tiene cotas superiores.

**Ejemplo 3.98.** Consideremos el subconjunto  $B = \{3, 5, 11, 121, 240\}$  de  $(\mathbb{R}, \leq)$ . Entonces  $-30, -7, 0$  y  $3$  son cotas inferiores de  $B$ , mientras que  $240, 300$  y  $973$  son algunos ejemplos de cotas superiores de  $B$ .

**Definición 3.99 (supremo / ínfimo).** Sea  $B$  un subconjunto de un conjunto ordenado  $(A, \preceq)$ .

- El *supremo de  $B$* , denotado como  $\sup_A B$ , es la mínima cota superior de  $B$ .

- El *ínfimo* de  $B$ , denotado como  $\inf_A B$ , es la máxima cota inferior de  $B$ .

**Ejemplo 3.100.** Consideremos al subconjunto

$$B = \{3, 5, 11, 121, 240\}$$

de  $(\mathbb{N}, \leq)$ . La mínima cota superior de  $B$  es 240, mientras que la máxima cota inferior es 3. Por lo tanto,  $\sup_{\mathbb{N}} B = 240$  e  $\inf_{\mathbb{N}} B = 3$ . En este caso, el supremo e ínfimo de  $B$  coinciden con el máximo y mínimo absoluto de  $B$ , respectivamente.

**Ejemplo 3.101.** Probablemente el estudiante sabrá que  $\pi$  es un número real cuya aproximación decimal es 3.14159265. Consideremos el siguiente conjunto de números reales:

$$B = \{3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \dots\}.$$

Los elementos de  $B$  son números racionales que se aproximan a  $\pi$  (el cual es un número irracional), pero  $\pi \notin B$ . Claramente, el ínfimo de  $B$  es 3, el cual coincide con el mínimo absoluto de  $B$ . Sin embargo, a pesar de no tener un máximo absoluto, el supremo de  $B$  es  $\pi$ . Esto ocurre debido a que los elementos de  $B$  se aproximan a  $\pi$  “tanto como queramos”, pero nunca llegan a ser iguales a él.

**Definición 3.102 (conjunto bien ordenado).** Decimos que un conjunto ordenado  $(A, \leq)$  está *bien ordenado* si cualquier subconjunto no vacío de  $(A, \leq)$  tiene un mínimo absoluto.

**Ejemplo 3.103.** El conjunto  $(\mathbb{N}, \leq)$  está bien ordenado. Cualquier subconjunto de  $\mathbb{N}$  tiene un mínimo absoluto.

**Proposición 3.104.** Cualquier conjunto bien ordenado está totalmente ordenado.

**Demostración.** Sea  $(A, \leq)$  un conjunto bien ordenado. Tenemos que demostrar que cualquier par de elementos de  $A$  se puede comparar. Sean  $a, b \in A$ . Por la definición de conjunto bien ordenado, el subconjunto  $\{a, b\}$  debe tener un mínimo absoluto. Esto significa que  $a \leq b$  o  $b \leq a$ , y por lo tanto  $a$  y  $b$  son comparables. Esto demuestra que  $(A, \leq)$  está totalmente ordenado. ■

La proposición recíproca de la proposición anterior no es verdad, como lo demuestra el siguiente ejemplo.

**Ejemplo 3.105.** El conjunto  $(\mathbb{Z}, \leq)$  está totalmente ordenado (ya que cualquier par de elementos se puede comparar), pero no es un conjunto bien ordenado debido a que  $\mathbb{Z}$  no tiene un mínimo absoluto.

**Palabras clave de la sección:** *relación antisimétrica, relación de orden, elementos maximales y minimales, cotas superiores e inferiores, máximos y mínimos absolutos, supremo e ínfimo, conjunto bien ordenado.*

### 3.3.1 Ejercicios de relaciones de orden

**Ejercicio 3.106.** Considera el conjunto

$$H = \{\{a, b\}, \{a, b, c\}, \{a, b, d\}, \{a, b, f\}, \{a, b, e, f\}, \{a, b, c, d, e\}\}$$

ordenado por inclusión.

- Explica por qué  $H$  no es un conjunto totalmente ordenado. Encuentra un subconjunto de  $H$  que sí esté totalmente ordenado (una cadena).
- Encuentra todos los elementos minimales y maximales de  $H$ .
- Determina si  $H$  tiene un máximo o un mínimo absoluto.
- Si  $\mathbf{A}$  es el conjunto potencia de las letras del abecedario, encuentra  $\inf_{\mathbf{A}} H$  y  $\sup_{\mathbf{A}} H$ . (Sugerencia: considera uniones e intersecciones de los elementos de  $H$ .)

**Ejercicio 3.107.** Demuestra que si  $(A, \preceq)$  es un conjunto totalmente ordenado y  $s \in A$  es un elemento minimal, entonces  $s$  es único.

**Ejercicio 3.108.** Sea  $\leq$  la relación de orden usual sobre  $\mathbb{N}$ . Definamos la relación de *orden lexicográfico* sobre  $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$  de la siguiente forma:

$$L = \{((a, b), (c, d)) \in \mathbb{N}^2 \times \mathbb{N}^2 : (a < c) \vee [(a = c) \wedge (b \leq d)]\}.$$

Si  $((a, b), (c, d)) \in L$  escribimos  $(a, b) \preceq (c, d)$ . Determina si las siguientes afirmaciones son verdaderas o falsas. Justifica tu respuesta.

- $(3, 4) \preceq (1, 7)$ .
- $(5, 9) \preceq (5, 11)$ .
- $L$  es una relación de orden sobre  $\mathbb{N}^2$ .
- $(\mathbb{N} \times \mathbb{N}, \preceq)$  no es un conjunto totalmente ordenado.
- $(\mathbb{N} \times \mathbb{N}, \preceq)$  es un conjunto bien ordenado.

**Ejercicio 3.109.** Considera la relación

$$K = \{(n, m) \in \mathbb{N} \times \mathbb{N} : \exists k \in \mathbb{N} \text{ tal que } m = kn\},$$

para la cual, si  $(n, m) \in K$ , decimos que  $n$  divide a  $m$  y escribimos  $n \mid m$ .

- a) Demuestra que  $K$  es una relación de orden sobre  $\mathbb{N}$ .
- b) Determina si  $(\mathbb{N}, |)$  es un conjunto totalmente ordenado.
- c) Encuentra todos los elementos maximales y minimales de  $(\mathbb{N}, |)$ .
- d) Determina si  $(\mathbb{N}, |)$  es un conjunto bien ordenado.

### 3.4 Definiciones del capítulo

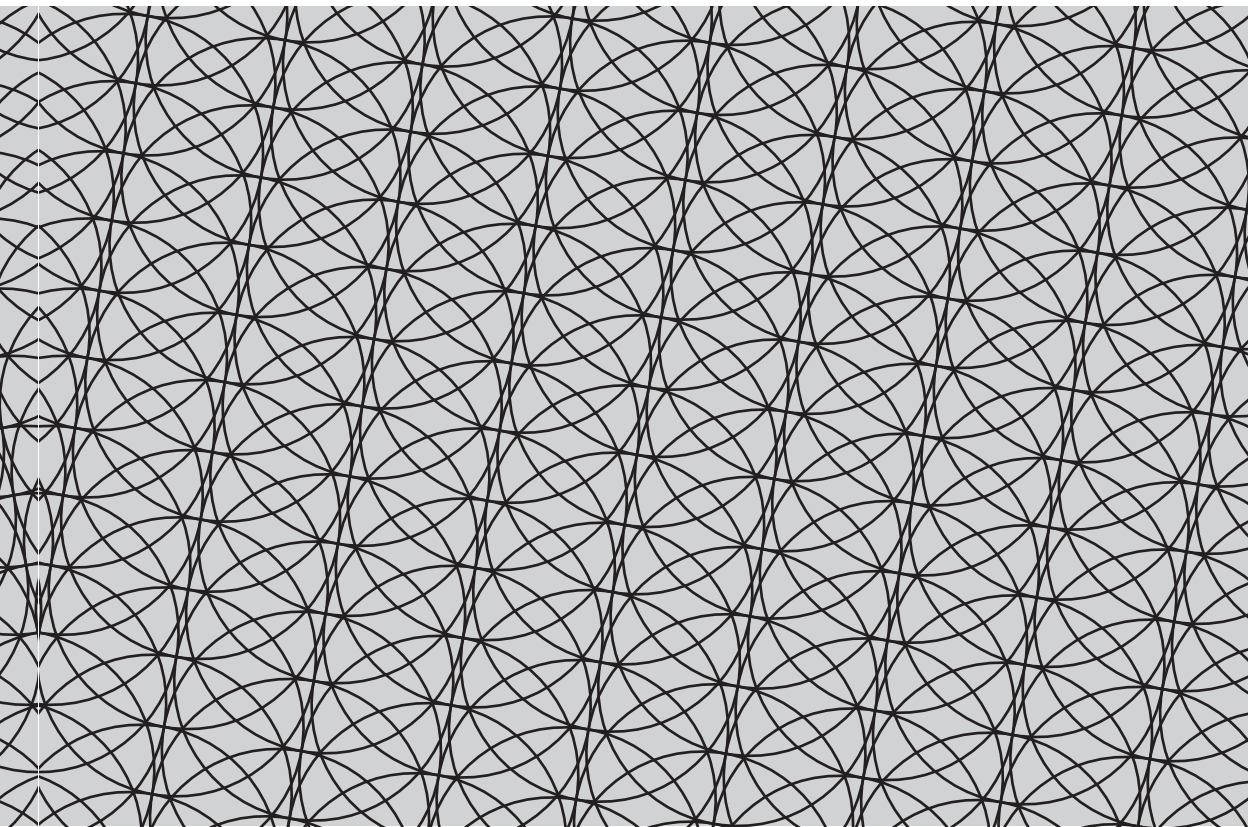
Escribe la definición y un ejemplo de cada uno de los conceptos enlistados a continuación.

- 1) Relación.
- 2) Dominio de una relación.
- 3) Rango de una relación.
- 4) Función.
- 5) Imagen de un conjunto bajo una función.
- 6) Preimagen de un conjunto bajo una función.
- 7) Función inyectiva.
- 8) Función sobreyectiva.
- 9) Función biyectiva.
- 10) Composición de dos funciones.
- 11) Relación inversa.
- 12) Relación de equivalencia.
- 13) Clase de equivalencia.
- 14) Conjunto cociente de una relación de equivalencia.
- 15) Partición de un conjunto.
- 16) Relación de orden.
- 17) Relación de orden total.
- 18) Elemento minimal.
- 19) Cota inferior.
- 20) Mínimo absoluto.
- 21) Ínfimo.
- 22) Conjunto bien ordenado.

*Dondequiera que haya un número está la  
belleza.*

Proclo, filósofo griego

## Capítulo 4. Números



Originalmente, los números surgieron de la necesidad práctica de contar objetos. Los primeros humanos contaban con ayuda de los medios disponibles: dedos, piedras, marcas talladas, etc. Le tomó cientos de años a la humanidad establecer conceptos como la infinitud de los números, la existencia del cero<sup>1</sup> y los números negativos.

En este capítulo estudiamos el concepto matemático de número desde diversos puntos de vista. En la sección 4.1, estudiamos las propiedades básicas de los números naturales y el *principio de inducción matemática*, el cual nos proporciona una nueva y poderosa técnica de demostración. En la sección 4.2 examinamos los conceptos importantes relacionados con los números enteros, como la divisibilidad y las ecuaciones diofánticas. Las congruencias módulo  $n$  son definidas después, en la sección 4.3. Luego, en la sección 4.4 abordamos el concepto de cardinalidad de un conjunto, ya sea finito o infinito. Finalmente, en la sección 4.5 presentamos algunas técnicas para contar cardinalidades de conjuntos finitos.

## 4.1 Números naturales

En los capítulos anteriores desarrollamos un buen bagaje de herramientas lógicas, las cuales aplicamos al estudio de conjuntos, relaciones y funciones. A pesar de haber trabajado con números constantemente, no hemos dicho con precisión qué es un número. ¿Cuál es la esencia de los números? ¿Qué propiedades básicas los definen?

El primer paso es definir al conjunto de los números naturales. Existen diversas formas de lograr esto: la más aceptada actualmente se basa en la teoría axiomática de conjuntos, la cual define a  $\mathbb{N}$  como un sistema especial de conjuntos. Aunque este enfoque es elegante, también es complicado y abstracto. En este capítulo adoptaremos otro enfoque, uno más clásico: definiremos a  $\mathbb{N}$  usando los *axiomas de Peano*.

### 4.1.1 Axiomas de Peano

Recordemos que los axiomas son proposiciones aceptadas como verdaderas sin necesidad de ser demostradas. Podemos decir que los axiomas, junto con las definiciones, son las reglas del “juego

---

<sup>1</sup>Durante el primer siglo antes de Cristo, las culturas olmeca y maya fueron las primeras en considerar al cero como un número.



matemático”, de las cuales debemos partir para comenzar la construcción de una enorme red lógica formada por teoremas, lemas y proposiciones.

Es muy importante establecer de forma clara y explícita las reglas del juego, pues en caso contrario, a la larga, éstas se podrían tornar confusas.

Los axiomas de Peano fueron introducidos por el matemático italiano Giuseppe Peano en el siglo XIX.

**Axioma 4.1 (axiomas de Peano).** Existe un conjunto  $\mathbb{N}$ , llamado el *conjunto de los números naturales*, que satisface las siguientes propiedades:

- 1) Existe un símbolo constante 0, llamado *cero*, que pertenece a  $\mathbb{N}$ .
- 2) Para cualquier  $n \in \mathbb{N}$ , existe un elemento  $s(n) \in \mathbb{N}$ , llamado el *sucesor* de  $n$ .
- 3) No existe ningún  $n \in \mathbb{N}$  tal que  $s(n) = 0$ .
- 4) Si  $s(n) = s(m)$ ,  $n, m \in \mathbb{N}$ , entonces  $m = n$ .
- 5) Si  $S \subseteq \mathbb{N}$  es un subconjunto tal que:
  - a)  $0 \in S$ ,
  - b)  $\forall k \in S, s(k) \in S$ ,

entonces  $S = \mathbb{N}$ .

Los axiomas anteriores fueron las reglas más importantes que, según Peano, capturan la esencia de los números naturales; tal vez la observación más característica es la existencia del “sucesor” de un número.

En los siguientes párrafos explicaremos cómo los axiomas de Peano conducen a la representación más familiar de los números naturales.

El conjunto  $\mathbb{N}$  no es vacío porque  $0 \in \mathbb{N}$  (axioma 1)). Implícitamente, Peano definió una función

$$s : \mathbb{N} \rightarrow \mathbb{N}$$

llamada la *función sucesor* (axioma 2)). Hasta ahora no conocemos la regla que define esta función, pero eso no importa: saber de su existencia es suficiente.

Aplicando la función sucesor a 0, obtenemos un número  $s(0) \in \mathbb{N}$ . Observemos que  $s(0) \neq 0$  por el axioma 3). Ahora, consideremos

también al número  $s(s(0)) \in \mathbb{N}$ , para el cual  $0 \neq s(s(0))$  (axioma 3)). Además,

$$s(0) \neq s(s(0)),$$

ya que de lo contrario, si  $s(0) = s(s(0))$ , entonces, por el axioma 4),  $0 = s(0)$ , lo cual es una contradicción. Por lo tanto

$$\{0, s(0), s(s(0))\}$$

es un subconjunto de  $\mathbb{N}$  con tres elementos distintos.

Repitamos el argumento anterior para formar el subconjunto

$$S = \{0, s(0), s(s(0)), s(s(s(0))), \dots\} \subseteq \mathbb{N}.$$

Este conjunto  $S$  satisface las condiciones del axioma 5), así que

$$\mathbb{N} = \{0, s(0), s(s(0)), s(s(s(0))), \dots\}.$$

Finalmente, para establecer la notación usual, simplemente renombramos a los elementos de  $\mathbb{N}$ :

$$1 = s(0), \quad 2 = s(s(0)), \quad 3 = s(s(s(0))), \quad \dots$$

Con esta nueva notación, la regla de la función sucesor puede escribirse como  $s(n) = n + 1$ ,  $n \in \mathbb{N}$ .

El quinto axioma de Peano es muy importante ya que, además de ayudar a establecer la construcción usual de  $\mathbb{N}$ , nos permite hacer uso de un método de demostración llamado *inducción matemática*. Estudiaremos de cerca esta técnica en la siguiente sección.

Las dos operaciones básicas de  $\mathbb{N}$  (la adición y la multiplicación) pueden definirse en términos de la función sucesor. No escribiremos las definiciones formales en este texto, pero enlistaremos las propiedades que estas operaciones satisfacen.

#### **Adición en $\mathbb{N}$ .**

Para todo  $a, b, c \in \mathbb{N}$  se cumplen las siguientes propiedades:

- 1) *Cerradura*:  $a + b \in \mathbb{N}$ .
- 2) *Conmutatividad*:  $a + b = b + a$ .
- 3) *Asociatividad*:  $(a + b) + c = a + (b + c)$ .
- 4) *Identidad aditiva*: el cero satisface que  $a + 0 = a$ .

#### **Multiplicación en $\mathbb{N}$ :**

Para todo  $a, b, c \in \mathbb{N}$  se cumplen las siguientes propiedades:

- 5) *Cerradura*:  $a \cdot b \in \mathbb{N}$ .
- 6) *Conmutatividad*:  $a \cdot b = b \cdot a$ .
- 7) *Asociatividad*:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
- 8) *Identidad multiplicativa*: el sucesor del cero, denotado como 1, satisface que  $a \cdot 1 = a$ .

Existe además una propiedad que involucra a ambas operaciones:

- 9) *Distributividad*:  $a \cdot (b + c) = a \cdot b + a \cdot c$ , para cualesquiera  $a, b, c \in \mathbb{N}$ .

Observemos que ni la resta ni la división de dos números naturales están siempre definidas en  $\mathbb{N}$ ; por ejemplo,  $3 - 8 \notin \mathbb{N}$  y  $\frac{3}{8} \notin \mathbb{N}$ .

### 4.1.2 Inducción matemática

La inducción matemática es una técnica de demostración para proposiciones que involucran al conjunto de los números naturales. Algunos ejemplos de proposiciones de este tipo son:

- 1) Para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ , la igualdad  $1 + 3 + 5 + \cdots + (2n - 1) = n^2$  se cumple.
- 2) Para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ , la igualdad  $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$  se cumple.
- 3) Para toda  $n \in \mathbb{N}$ , el número  $n^2 + n + 41$  es primo.

Para refutar alguna de las proposiciones anteriores basta con encontrar un número natural que no satisfaga la afirmación. Sin embargo, demostrar la veracidad de estas proposiciones sin las herramientas adecuadas podría parecer una tarea casi imposible. Comprobar que la afirmación es verdadera para diez, cien o un millón de números no es suficiente: es necesario demostrar que es verdadera para *todos* los números naturales.

Por ejemplo, podemos comprobar que la proposición 3) de la lista es verdadera para los primeros doce números naturales; los

números primos que se obtienen son:

$$\begin{array}{ll} 0^2 + 0 + 41 = 41, & 1^2 + 1 + 41 = 43, \\ 2^2 + 2 + 41 = 47, & 3^2 + 3 + 41 = 53, \\ 4^2 + 4 + 41 = 61, & 5^2 + 5 + 41 = 71, \\ 6^2 + 6 + 41 = 83, & 7^2 + 7 + 41 = 97, \\ 8^2 + 8 + 41 = 113, & 9^2 + 9 + 41 = 131, \\ 10^2 + 10 + 41 = 151, & 11^2 + 11 + 41 = 173. \end{array}$$

Podríamos seguir aplicando la fórmula  $n^2 + n + 41$  para los siguientes veintiocho números naturales para obtener más números primos; sin embargo, al sustituir  $n = 40$  obtenemos

$$40^2 + 40 + 41 = 1681,$$

el cual no es primo porque es divisible entre 41. Esto demuestra que la proposición 3) es falsa.

Incluso cuando tenemos una proposición que es válida para muchos casos particulares, no podemos afirmar que sea verdadera en general. En proposiciones como las de nuestra lista es imposible analizar todos los casos, ya que  $\mathbb{N}$  es un conjunto infinito. Entonces, ¿qué técnica debemos aplicar en estas situaciones? La respuesta es usar el razonamiento conocido como *método de inducción matemática*, el cual se basa en el quinto axioma de Peano. Debido a su importancia, reescribimos este axioma a continuación y lo llamamos *principio de inducción matemática*.

**Axioma 4.2 (principio de inducción matemática).** Sea  $S$  un subconjunto de  $\mathbb{N}$  que tiene las siguientes propiedades:

- 1)  $0 \in S$ ,
- 2) Para toda  $k \in S$ , se cumple que  $k + 1 \in S$ .

Entonces,  $S = \mathbb{N}$ .

Veamos un ejemplo donde aplicamos este principio.

**Proposición 4.3.** Para cualquier  $n \in \mathbb{N}$ , se cumple que  $n^2 \geq 0$ .

**Demostración.** Consideremos el subconjunto de  $\mathbb{N}$  definido como

$$S = \{n \in \mathbb{N} : n^2 \geq 0\}.$$

En otras palabras,  $S$  es el conjunto de todos los números naturales cuyo cuadrado es mayor o igual que cero. Demostraremos que este conjunto cumple con las condiciones del principio de inducción matemática:

- 1) Debido a que  $0^2 \geq 0$ , tenemos que  $0 \in S$ .
- 2) Supongamos que  $k \in S$ . Por la propiedad que define a  $S$ , tenemos que  $k^2 \geq 0$ , y como  $k \in \mathbb{N}$ , tenemos que  $2k \geq 0$ . Esto implica que

$$(k + 1)^2 = k^2 + 2k + 1 \geq 0.$$

Entonces,  $k + 1 \in S$ .

Por lo tanto,  $S = \mathbb{N}$ . Esto demuestra que  $n^2 \geq 0$ , para toda  $n \in \mathbb{N}$ . ■

De manera informal, la inducción matemática se basa en lo siguiente. Una vez que sabemos que una afirmación se cumple para 0 y para el sucesor de cualquier número natural, deducimos que debe cumplirse para 1 (porque es el sucesor de 0). Luego, la afirmación también debe cumplirse para 2 (que es el sucesor 1), y para 3, y para 4, etc. Por lo tanto, la afirmación debe cumplirse para todos los números naturales.

Los pasos generales para demostrar una proposición por inducción son estándar y, hasta cierto punto, rutinarios. Por tal motivo, no es necesario construir explícitamente el conjunto  $S$  como en la proposición 4.3. Este conjunto puede mantenerse implícito para que la demostración se enfoque en los pasos más importantes de la inducción: verificar las condiciones 1) y 2) del principio de inducción matemática. En resumen, si  $P(m)$  es un predicado que depende de un número natural, la forma estándar de demostrar la proposición “ $\forall m \in \mathbb{N}, P(m)$ ” es la siguiente:

- 1) *Base de la inducción*. Comprobar la validez de la proposición para un caso base, normalmente  $P(0)$  o  $P(1)$ .
- 2) *Hipótesis de la inducción*. Suponer la validez de  $P(k)$ , donde  $k$  es un número natural fijo arbitrario.
- 3) Demostrar que  $P(k + 1)$  es verdadera, tomando en consideración la validez supuesta de  $P(k)$ .

El paso base de la inducción puede variar, incluso puede ser distinto de  $P(0)$  o  $P(1)$ . Si cambiamos el número del paso base por cualquier otro número natural  $r \neq 0$ , el principio de inducción matemática demuestra la validez de  $P(n)$ , para toda  $n \geq r$ .

Demostremos las proposiciones 1) y 2) de nuestra lista inicial.

**Proposición 4.4.** Para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ , se cumple la igualdad

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2. \quad (4.1)$$

**Demostración.** Usaremos el principio de inducción matemática.

- 1) *Base de la inducción.* La fórmula (4.1) con  $n = 1$  es  $1 = 1^2$ , la cual claramente es válida.
- 2) *Hipótesis de la inducción.* Supongamos que la fórmula (4.1) se cumple para  $k \in \mathbb{N}$ :

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2.$$

- 3) Debemos demostrar que la fórmula (4.1) es válida para  $k + 1$ . Usando la hipótesis de la inducción, tenemos que

$$1 + 3 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1).$$

Factorizando el lado derecho de la igualdad, obtenemos que

$$1 + 3 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2.$$

Esto demuestra la validez de la fórmula para  $k + 1$ . ■

**Proposición 4.5.** Para cualquier  $n \in \mathbb{N}$ ,  $n \neq 0$ , se cumple la igualdad

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

**Demostración.** Denotemos la suma como  $S(n)$ :

$$S(n) = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)}.$$

Usaremos el principio de inducción matemática.

- 1) *Base de la inducción.* Observemos que  $S(1) = \frac{1}{2}$  por definición, así que  $S(1) = \frac{1}{1+1}$ .
- 2) *Hipótesis de la inducción.* Supongamos que la igualdad se cumple para  $k \in \mathbb{N}$ ; es decir,

$$S(k) = \frac{k}{k+1}.$$

- 3) Demostraremos que

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

Por definición de  $S(k+1)$  y  $S(k)$ , tenemos que

$$\begin{aligned} S(k+1) &= \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)}, \\ &= S(k) + \frac{1}{(k+1)(k+2)}. \end{aligned}$$

Por consiguiente, según la hipótesis de inducción,

$$\begin{aligned} S(k+1) &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k^2 + 2k + 1}{(k+1)(k+2)} \\ &= \frac{k+1}{k+2}. \end{aligned}$$

■

**Proposición 4.6.** Para cualquier  $n \in \mathbb{N}$ ,  $n \neq 0$ , se cumple que

$$n \leq 2^{n-1}. \quad (4.2)$$

**Demostración.** Usaremos el principio de inducción matemática.

- 1) *Base de la inducción.* La desigualdad (4.2) es verdadera para 1, porque  $1 \leq 2^{1-1}$ .
- 2) *Hipótesis de la inducción.* Supongamos que la desigualdad (4.2) se cumple para  $k \in \mathbb{N}$ :

$$k \leq 2^{k-1}. \quad (4.3)$$

- 3) Demostraremos que la desigualdad también es válida para  $k+1$ . Multiplicando ambos lados de la desigualdad (4.3) por 2:

$$2k \leq 2 \cdot 2^{(k-1)} = 2^k.$$

Por el ejercicio 4.9, sabemos que  $(k+1) \leq 2k$ . Así, por la transitividad de  $\leq$  tenemos que

$$k+1 \leq 2^k.$$

■

**Proposición 4.7.** Sea  $\alpha$  un número positivo. Entonces, para toda  $n \in \mathbb{N}$ ,  $n \geq 2$ , se cumple la desigualdad de Bernoulli:

$$(1 + \alpha)^n > 1 + \alpha n. \quad (4.4)$$

**Demostración.** Usaremos el principio de inducción matemática.

- 1) *Base de la inducción.* El caso base de la inducción es para 2 (ya que no se cumple en los casos anteriores). Observemos que

$$\begin{aligned}(1 + \alpha)^2 > 1 + 2\alpha &\iff 1 + 2\alpha + \alpha^2 > 1 + 2\alpha \\ &\iff \alpha^2 > 0.\end{aligned}$$

Esta última desigualdad siempre es verdadera, y por consiguiente,  $(1 + \alpha)^2 > 1 + 2\alpha$  se cumple.

- 2) Supongamos que la desigualdad de Bernoulli es válida para un número natural fijo  $k$ ; es decir,

$$(1 + \alpha)^k > 1 + \alpha k. \quad (4.5)$$

- 3) Demostraremos que la desigualdad

$$(1 + \alpha)^{k+1} > 1 + \alpha(k + 1) \quad (4.6)$$

es válida. Multiplicando ambos lados de la desigualdad (4.5) por el número positivo  $(1 + \alpha)$  obtenemos que

$$(1 + \alpha)^{k+1} > (1 + \alpha k)(1 + \alpha) \quad (4.7)$$

Observemos ahora que

$$(1 + \alpha k)(1 + \alpha) > 1 + \alpha(k + 1) \iff \alpha^2 k > 0. \quad (4.8)$$

Esta última desigualdad siempre es válida para  $\alpha$  y  $k$  positivos. Por lo tanto, por (4.7) y (4.8), obtenemos la validez de la desigualdad (4.6). ■

**Palabras clave de la sección:** *axiomas de Peano, sucesor de un número natural, propiedades de las operaciones de los números naturales, principio de inducción matemática.*



### 4.1.3 Ejercicios de números naturales

**Ejercicio 4.8.** Considera la función sucesor  $s : \mathbb{N} \rightarrow \mathbb{N}$  definida por los axiomas de Peano. Determina si las siguientes afirmaciones son verdaderas o falsas. Justifica tu respuesta.

- a)  $s(s(3)) = 6$ .
- b) La función  $s$  es inyectiva.
- c) La función  $s$  es sobreyectiva.
- d) El rango de la función  $s$  es  $\mathbb{N} \setminus \{0\}$ .

**Ejercicio 4.9.** Demuestra, usando el principio de inducción matemática, que  $n + 1 \leq 2n$  se cumple para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ .

**Ejercicio 4.10.** El alemán Carl Friedrich Gauss fue uno de los más grandes matemáticos de la historia. Cuenta la leyenda que cuando aún cursaba la primaria descubrió la fórmula

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$

Demuestra, usando el principio de inducción matemática, que la fórmula de Gauss es válida para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ .

**Ejercicio 4.11.** Demuestra, usando el principio de inducción matemática, las siguientes proposiciones:

- a) Para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ , se cumple que

$$2^n \leq 1 \cdot 2 \cdot \dots \cdot (n+1).$$

- b) Para toda  $n \in \mathbb{N}$ , tenemos que

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2.$$

- c) Para toda  $n \in \mathbb{N}$ ,  $n \neq 0$ , tenemos que

$$1^2 - 2^2 + 3^2 - \dots + (-1)^{n+1} n^2 = (-1)^{n+1} \frac{n(n+1)}{2}.$$

- d) Para toda  $n \in \mathbb{N}$ , el número  $5^{2n} - 1$  es divisible entre 8 (sugerencia: recuerda que la suma de dos números divisibles entre 8 es divisible entre 8).

## 4.2 Números enteros

Dentro del conjunto de los números naturales, ecuaciones como

$$x + a = b, \text{ donde } a, b \in \mathbb{N},$$

no siempre tienen solución. Por ejemplo, si  $a = 8$  y  $b = 5$ , entonces no existe un número natural  $x$  tal que

$$x + 8 = 5.$$

Para resolver tales ecuaciones es necesario ampliar nuestro sistema de números: debemos considerar al conjunto  $\mathbb{Z}$  de los *números enteros*. Este conjunto puede construirse a partir de  $\mathbb{N}$  sin agregar más axiomas, como mostraremos a continuación.

En un primer intento, un número entero negativo podría definirse como un par ordenado de números naturales. Por ejemplo, podríamos identificar a  $-3$  con  $(5, 8)$ , ya que, en  $\mathbb{Z}$ , sabemos que  $-3 = 5 - 8$ . Sin embargo, como  $-3 = 4 - 7$  y  $-3 = 11 - 14$ , también podríamos identificar a  $-3$  con  $(4, 7)$  y  $(11, 14)$ . De hecho, podríamos identificar a  $-3$  con un número infinito de pares. Por tal motivo, esta definición no es satisfactoria.

Para resolver este problema, estudiaremos una relación de equivalencia sobre  $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ , y definiremos los números enteros como clases de equivalencia.

Sea  $R$  la relación sobre  $\mathbb{N}^2$  definida como:

$$(a, b)R(c, d) \text{ si y sólo si } a + d = b + c.$$

No podemos escribir " $a - b = c - d$ " en lugar de " $a + d = b + c$ " porque la resta no está bien definida sobre  $\mathbb{N}$ ; sin embargo, sabemos que ambas expresiones son en realidad equivalentes en  $\mathbb{Z}$ .

**Proposición 4.12.** La relación  $R$ , definida arriba, es de equivalencia.

**Demostración.**

- 1) *Reflexividad.* Claramente,  $(a, b)R(a, b)$  porque  $a + b = a + b$ .
- 2) *Simetría.* Si  $(a, b)R(c, d)$ , entonces  $a + d = b + c$ . Por la conmutatividad de la suma,  $c + b = d + a$ , así que  $(c, d)R(a, b)$ .
- 3) *Transitividad.* Supongamos que  $(a, b)R(c, d)$  y  $(c, d)R(e, f)$ . Entonces  $a + d = b + c$  y  $c + f = d + e$ . Por lo tanto,

$$\begin{aligned} a + d = b + c &\Rightarrow a + d + e = b + c + e \\ &\Rightarrow a + c + f = b + c + e \\ &\Rightarrow a + f = b + e. \end{aligned}$$

Esto demuestra que  $(a, b)R(e, f)$ . ■

Definimos a  $\mathbb{Z}$  como el conjunto cociente de  $R$ :

$$\mathbb{Z} = \mathbb{N}^2 / R = \{[(a, b)] : a, b \in \mathbb{N}\}.$$

Y definimos a la suma de clases de equivalencia de la siguiente forma:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)].$$

Es importante observar que en cualquier clase de equivalencia podemos encontrar un representante de la forma  $(n, 0)$  o  $(0, n)$ ,  $n \in \mathbb{N}$ . Por ejemplo, en la clase  $[(3, 8)]$  encontramos el representante  $(0, 5)$  porque  $3 + 5 = 0 + 8$ . De esta forma,

$$\mathbb{Z} = \{[(n, 0)], [(0, n)] : n \in \mathbb{N}\}.$$

Para regresar a la notación usual, identificamos a  $n$  con la clase  $[(n, 0)]$ , y a  $-n$  con la clase  $[(0, n)]$ . Esta notación cumple la propiedad usual:

$$n + (-n) = [(n, 0)] + [(0, n)] = [(n, n)] = [(0, 0)] = 0.$$

Así pues, por ejemplo,  $-3$  es igual a la clase de equivalencia de todos los pares  $(a, b) \in \mathbb{N}$  tales que  $a = b + 3$ . Con esta nueva notación, consideramos que  $\mathbb{N}$  es un subconjunto de  $\mathbb{Z}$ .

**Ejemplo 4.13.** Las clases de equivalencia de  $\mathbb{Z}$  que se muestran a continuación son iguales:

$$\begin{aligned} [(5, 8)] &= [(4, 7)] = [(11, 14)] = [(2, 5)] = -3, \\ [(15, 10)] &= [(25, 20)] = [(8, 3)] = [(6, 1)] = 5, \\ [(5, 11)] &= [(14, 20)] = [(11, 17)] = [(0, 6)] = -6, \\ [(5, 4)] &= [(4, 3)] = [(11, 10)] = [(6, 5)] = 1, \\ [(n, n)] &= 0, \quad \forall n \in \mathbb{N}. \end{aligned}$$

La suma y la multiplicación en  $\mathbb{Z}$  cumplen las propiedades asociativa, conmutativa y distributiva; además, 0 y 1 son las identidades aditiva y multiplicativa, respectivamente. El conjunto  $\mathbb{Z}$  tiene una nueva propiedad respecto a la suma:

10) *Inverso aditivo.* Para cualquier  $a \in \mathbb{Z}$  existe  $b \in \mathbb{Z}$  tal que  $a + b = 0$ .

### 4.2.1 Divisibilidad

La ecuación  $x + a = b$ ,  $a, b \in \mathbb{Z}$  tiene solución en  $\mathbb{Z}$ . Sin embargo,  $\mathbb{Z}$  es aún insuficiente para resolver ecuaciones como

$$ax = b, \quad a, b \in \mathbb{Z}, \quad a \neq 0,$$

las cuales tienen solución entera si y sólo si  $a$  es un *divisor* de  $b$ .

**Definición 4.14 (divisor).** Sean  $a, b \in \mathbb{Z}$ , con  $a \neq 0$ . Decimos que  $a$  es un *divisor* de  $b$ , y escribimos  $a \mid b$ , si existe  $t \in \mathbb{Z}$  tal que  $at = b$ .

Si  $a \mid b$ , también decimos que  $a$  es un *factor* de  $b$ , o que  $b$  es *múltiplo* de  $a$ , o que  $b$  es *divisible* entre  $a$ .

La definición de divisor involucra a la multiplicación y no a la división, como su nombre podría sugerir. La razón es que la división no es una operación bien definida en  $\mathbb{Z}$ ; es decir, la división de dos números enteros no siempre es un entero. De cualquier forma, en ocasiones resulta cómodo pensar que  $a$  es un divisor de  $b$  si  $b/a$  es un número entero. Por ejemplo,  $5 \mid 10$  porque  $10 = 5 \cdot 2$  o, en forma equivalente, porque  $10/5 = 2 \in \mathbb{Z}$ .

**Ejemplo 4.15.** Consideremos los siguientes ejemplos:

- 1)  $1 \mid n$  para toda  $n \in \mathbb{Z}$ , porque  $n = 1 \cdot n$ .
- 2)  $n \mid 0$  para toda  $n \in \mathbb{Z}$ , porque  $0 = 0 \cdot n$ .
- 3) Si  $2n \in 2\mathbb{Z}$  es un número par, claramente  $2 \mid 2n$ .

Los números enteros que no pueden ser factorizados reciben un nombre especial.

**Definición 4.16 (número primo).** Sea  $p \in \mathbb{Z}$ ,  $p > 1$ . Decimos que  $p$  es un *número primo* si sus únicos divisores positivos son 1 y él mismo.

**Definición 4.17 (compuesto).** Si  $t \in \mathbb{Z}$ ,  $t > 1$  no es un número primo, decimos que  $t$  es un *número compuesto*.

Los primeros números primos son bastante conocidos:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

El misterioso comportamiento de esta secuencia ha obsesionado a los matemáticos durante siglos. Numerosos esfuerzos fallidos se

han hecho por encontrar alguna fórmula que describa su comportamiento. Nosotros descubriremos su relevancia primordial más adelante, cuando abordemos el *teorema fundamental de la aritmética*.

Las siguientes son algunas propiedades fundamentales de la divisibilidad.

**Lema 4.18 (divisibilidad).** Sean  $a, b, c \in \mathbb{Z}$ . Las siguientes afirmaciones son verdaderas:

- 1) Si  $a \mid b$  y  $b \mid c$ , entonces  $a \mid c$ .
- 2) Si  $c \mid a$  y  $c \mid b$  entonces  $c \mid (au + bv)$  para todo  $u, v \in \mathbb{Z}$ .
- 3)  $a \mid b$  y  $b \mid a$  si y sólo si  $a = \pm b$ .

**Demostración.**

- 1) Si  $a \mid b$  y  $b \mid c$ , entonces  $b = t_1 a$  y  $c = t_2 b$  para algunos  $t_1, t_2 \in \mathbb{Z}$ . Sustituyendo la primera relación en la segunda,  $c = t_2(t_1 a) = (t_2 t_1) a$ , por lo que  $a \mid c$ .
- 2) Si  $c \mid a$  y  $c \mid b$ , entonces  $a = t_1 c$  y  $b = t_2 c$  para algunos  $t_1, t_2 \in \mathbb{Z}$ . Así, para cualquier  $u, v \in \mathbb{Z}$  tenemos que  $au = t_1 cu$  y  $bv = t_2 cv$ . Sumando las dos relaciones anteriores:

$$\begin{aligned} au + bv &= t_1 cu + t_2 cv, \\ &= (t_1 u + t_2 v) c. \end{aligned}$$

Por lo tanto,  $c \mid (au + bv)$ .

- 3) Si  $a = \pm b$ , entonces es claro que  $a = q_1 b$  y  $b = q_2 a$  donde  $q_1 = q_2 = \pm 1$ . Luego,  $a \mid b$  y  $b \mid a$ . Supongamos ahora que  $a \mid b$  y  $b \mid a$ . De esta manera,  $a = q_1 b$  y  $b = q_2 a$  para algunos  $q_1, q_2 \in \mathbb{Z}$ . Sustituyendo la segunda ecuación en la primera y cancelando:

$$a = q_1 q_2 a \implies 1 = q_1 q_2.$$

La única forma de que el producto de dos enteros sea igual a 1 es que  $q_1 = q_2 = \pm 1$ . Por lo tanto,  $a = \pm b$ . ■

El siguiente es un resultado importante, cuya demostración se estudia normalmente en un curso de teoría de números elemental ver (Burton, 1980).

**Teorema 4.19 (algoritmo de la división).** Sean  $a, b \in \mathbb{Z}$ ,  $b > 0$ . Existen enteros únicos  $q$  y  $r$  tales que

$$a = bq + r,$$

donde  $0 \leq r < b$ .

En el algoritmo de la división, el entero  $q$  es llamado el *cociente* de  $a$  entre  $b$ , mientras que  $r$  es llamado el *residuo*.

**Ejemplo 4.20.** Consideremos los siguientes ejemplos:

- 1) Si  $a = -5$  y  $b = 2$ , entonces  $a = -3b + 1$ .
- 2) Si  $a = 0$  y  $b = 250$ , entonces  $a = 0b + 0$ .
- 3) Si  $a = 23$  y  $b = 5$ , entonces  $a = 4b + 3$ .

**Definición 4.21 (máximo común divisor).** Sean  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ ,  $b \neq 0$ . Decimos que  $d \in \mathbb{Z}$ ,  $d \geq 1$  es el máximo común divisor de  $a$  y  $b$ , si se cumplen las siguientes propiedades:

- 1) Es divisor común:  $d \mid a$  y  $d \mid b$ .
- 2) Si  $c$  es un entero tal que  $c \mid a$  y  $c \mid b$ , entonces  $c \mid d$ .

Denotamos al máximo común divisor de  $a$  y  $b$  como  $\text{mcd}(a, b)$ .

**Definición 4.22 (primos relativos).** Decimos que  $a, b \in \mathbb{Z}$  son *primos relativos* si  $\text{mcd}(a, b) = 1$ .

Una forma de obtener el máximo común divisor de dos números es escribir todos los divisores de ambos números e identificar al mayor de los divisores comunes. Por ejemplo, para encontrar  $\text{mcd}(12, 18)$  escribimos:

Divisores de 12 : 1, 2, 3, 4, 6, 12.

Divisores de 18 : 1, 2, 3, 6, 9, 18.

El máximo de los divisores comunes es 6, así que  $\text{mcd}(12, 18) = 6$ . Sin embargo, este procedimiento puede ser muy lento si se usan números más grandes. Un método más eficiente es el llamado *algoritmo de Euclides*, pero antes de presentarlo demostraremos algunos teoremas.

**Lema 4.23 (Bézout).** Para toda  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ ,  $b \neq 0$ , existen  $s_1, s_2 \in \mathbb{Z}$  tales que

$$\text{mcd}(a, b) = as_1 + bs_2.$$

**Demostración.** Consideremos el conjunto

$$S = \{ax_1 + bx_2 \in \mathbb{N} \setminus \{0\} : x_1, x_2 \in \mathbb{Z}\}.$$

Como  $S \subseteq \mathbb{N}$  y  $\mathbb{N}$  es un conjunto bien ordenado, sabemos que  $S$  tiene un mínimo absoluto. Sea  $d = as_1 + bs_2$  el mínimo absoluto de  $S$ . Demostraremos que  $d = \text{mcd}(a, b)$ .

- 1) Por el algoritmo de la división, existen  $q, r \in \mathbb{Z}$  tales que  $a = qd + r$  donde  $0 \leq r < d$ . Si  $r \neq 0$ , entonces

$$r = a - qd = a - q(as_1 + bs_2) = (1 - qs_1)a + (-qs_2)b \in S.$$

Como  $r < d$ , esto contradice que  $d$  sea el mínimo absoluto de  $S$ . Por lo tanto,  $r = 0$  y  $d \mid a$ . De manera similar, demostramos que  $d \mid b$ .

- 2) Si  $c$  es un entero tal que  $c \mid a$  y  $c \mid b$ , entonces  $c \mid (as_1 + bs_2) = d$  por el lema 4.18, 2). ■

**Corolario 4.24.** Sean  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ ,  $b \neq 0$ . Entonces  $\text{mcd}(a, b) = 1$  si y sólo si existen  $s_1, s_2 \in \mathbb{Z}$  tales que  $as_1 + bs_2 = 1$ .

**Demostración.**

( $\Rightarrow$ ) Si  $\text{mcd}(a, b) = 1$ , entonces  $as_1 + bs_2 = 1$  para algunos  $s_1, s_2 \in \mathbb{Z}$  por el lema de Bézout.

( $\Leftarrow$ ) Supongamos que  $1 = as_1 + bs_2$  para algunos  $s_1, s_2 \in \mathbb{Z}$ . Sea  $d = \text{mcd}(a, b)$ . Como  $d \mid a$  y  $d \mid b$ , el lema 4.18, 2) implica que

$$d \mid (as_1 + bs_2) \Rightarrow d \mid 1.$$

Claramente,  $1 \mid d$  por el ejemplo 4.15, 1), así que el lema 4.18, 3) implica que  $d = \pm 1$ . Por definición,  $d > 0$ , así que  $d = 1$ . ■

**Lema 4.25.** Si  $a = qb + r$ , entonces  $\text{mcd}(a, b) = \text{mcd}(b, r)$ .

**Demostración.** Sean  $c = \text{mcd}(a, b)$  y  $d = \text{mcd}(b, r)$ . El lema 4.18 2) implica que

$$c \mid (qb + r) = a \text{ y } c \mid (a - qb) = r.$$

Por definición de máximo común divisor, tenemos que

$$\begin{aligned} d \mid a \text{ y } d \mid b &\Rightarrow d \mid \text{mcd}(a, b) = c, \\ c \mid b \text{ y } c \mid r &\Rightarrow c \mid \text{mcd}(b, r) = d. \end{aligned}$$

Por el lema 4.18 3), obtenemos que  $d = \pm c$ , lo que implica que  $d = c$ , ya que el máximo común divisor siempre es positivo. ■

Euclides fue un matemático griego nacido en Alejandría hacia el año 325 antes de Cristo. A pesar de que prácticamente no se sabe nada sobre su vida, es uno de los iconos matemáticos más conocidos actualmente. En su obra más importante, *Elementos*, desarrolla

de manera axiomática la geometría y la aritmética. Fue uno de los primeros matemáticos en utilizar la técnica de reducción al absurdo.

El **algoritmo de Euclides** es una forma rápida y eficiente de encontrar el máximo común divisor de dos números  $a, b \in \mathbb{Z}$ . Podemos asumir que  $a > 0$  y  $b > 0$  ya que  $\text{mcd}(a, b) = \text{mcd}(\pm a, \pm b)$ . La idea principal del procedimiento es el uso repetido del algoritmo de la división:

$$\begin{aligned} a &= bq_1 + r_1 \text{ donde } 0 < r_1 < b, \\ b &= r_1q_2 + r_2 \text{ donde } 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3 \text{ donde } 0 < r_3 < r_2, \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k \text{ donde } 0 < r_k < r_{k-1}, \\ r_{k-1} &= r_kq_{k+1} + 0. \end{aligned}$$

Como  $b > r_1 > r_2 > \dots \geq 0$ , debemos obtener un residuo  $r_k = 0$  después de un máximo de  $b$  pasos. Ahora, afirmamos que

$$r_k = \text{mcd}(a, b).$$

Para demostrar esto, observemos que, por el lema 4.25,

$$\text{mcd}(a, b) = \text{mcd}(b, r_1) = \text{mcd}(r_1, r_2) = \dots = \text{mcd}(r_{k-1}, r_k).$$

De la última ecuación, vemos que  $r_k \mid r_{k-1}$ , así que  $\text{mcd}(r_{k-1}, r_k) = r_k$ .

**Ejemplo 4.26.** Usaremos el algoritmo de Euclides para obtener el máximo común divisor entre 236 y 112:

$$\begin{aligned} 236 &= 112 \cdot 2 + 12, \\ 112 &= 12 \cdot 9 + 4, \\ 12 &= 4 \cdot 3 + 0. \end{aligned}$$

Por lo tanto,  $\text{mcd}(236, 112) = 4$ .

El algoritmo de Euclides también permite encontrar los enteros  $s_1$  y  $s_2$  del lema de Bézout. El procedimiento consiste en reescribir la penúltima ecuación:

$$r_k = r_{k-2} - r_{k-1}q_k,$$



y sustituir en las ecuaciones anteriores:

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1},$$

$$r_{k-2} = r_{k-4} - r_{k-3}q_{k-2},$$

$$\vdots$$

hasta llegar a una expresión que contenga  $a$  y  $b$ .

**Ejemplo 4.27.** Usaremos el algoritmo de Euclides para obtener el máximo común divisor de 15 y 49.

$$49 = 15 \cdot 3 + 4,$$

$$15 = 4 \cdot 3 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

Por lo tanto  $\text{mcd}(15, 49) = 1$ . Despejando los residuos:

$$1 = 4 - 3 \cdot 1,$$

$$3 = 15 - 4 \cdot 3,$$

$$4 = 49 - 15 \cdot 3.$$

Ahora podemos escribir 1 como combinación lineal de 15 y 49.

$$\begin{aligned} 1 &= 4 - 3 \cdot 1, \\ &= 4 - (15 - 4 \cdot 3) \cdot 1, \\ &= 4 \cdot 4 - 15, \\ &= (49 - 15 \cdot 3) \cdot 4 - 15, \\ &= 49 \cdot 4 - 15 \cdot 13. \end{aligned}$$

Además del algoritmo, el siguiente lema lleva el nombre de Euclides.

**Lema 4.28 (Euclides).** Sean  $a, b \in \mathbb{Z}$ . Si  $p$  es un primo tal que  $p \mid ab$  entonces  $p \mid a$  o  $p \mid b$ .

**Demostración.** Supongamos que  $p \nmid a$ . Demostraremos que  $p \mid b$ . Como  $p \nmid a$ , tenemos que  $\text{mcd}(p, a) = 1$ , y por el lema de Bézout, existen  $s_1, s_2 \in \mathbb{Z}$  tales que

$$1 = ps_1 + as_2.$$

Multiplicando por  $b$ , obtenemos que

$$b = ps_1b + abs_2.$$

Como  $p \mid abs_2$  y  $p \mid ps_1b$ , tenemos que  $p \mid b$  por el lema 4.18 2). ■

Una forma alternativa de enunciar el lema de Euclides es decir que si  $p \mid ab$ , donde  $p$  es primo relativo con  $a$ , entonces  $p \mid b$ .

Es un error pensar que el lema de Euclides se cumple si  $p$  no es un número primo. Por ejemplo,  $6 \mid 3 \cdot 4$  pero  $6 \nmid 3$  y  $6 \nmid 4$ .

El siguiente teorema revela la gran importancia de los números primos.

**Teorema 4.29 (teorema fundamental de la aritmética).** Para cualquier entero mayor que 1 es un número primo o un producto de números primos. Además, este producto es único excepto por el orden de los factores.

**Ejemplo 4.30.** La factorización de 30 en números primos es

$$30 = 2 \cdot 3 \cdot 5.$$

Esta factorización es única excepto por el orden de los factores.

## 4.2.2 Ecuaciones diofánticas

**Definición 4.31 (ecuación diofántica).** Una ecuación diofántica lineal en las variables  $x, y$  es una ecuación de la forma

$$ax + by = c, \text{ donde } a, b, c \in \mathbb{Z}.$$

Veamos una aplicación de este tipo de ecuaciones.

**Ejemplo 4.32.** Supongamos que tenemos \$430 y queremos comprar bolígrafos que cuestan \$20 y cuadernos que cuestan \$50. ¿Podemos gastar todo nuestro dinero comprando bolígrafos y cuadernos? En otras palabras, buscamos las soluciones enteras no negativas de la ecuación

$$20x + 50y = 430,$$

donde  $x, y$  son el número de bolígrafos y cuadernos, respectivamente.

La siguiente proposición establece las condiciones bajo las cuales una ecuación diofántica tiene soluciones enteras.

**Teorema 4.33.** Sean  $a, b, c \in \mathbb{Z}$ . La ecuación diofántica

$$ax + by = c$$

tiene soluciones enteras si y sólo si  $\text{mcd}(a, b) \mid c$ .

**Demostración.** Sea  $d = \text{mcd}(a, b)$ .

( $\Rightarrow$ ) Si la ecuación tiene soluciones enteras, existen  $u, v \in \mathbb{Z}$  tales que  $au + bv = c$ . Entonces  $d \mid c$  por el lema 4.18, 2).

( $\Leftarrow$ ) Supongamos que  $d \mid c$ . Por definición, existe  $r \in \mathbb{Z}$  tal que  $c = dr$ . Por el lema de Bézout 4.23, existen  $s_1, s_2 \in \mathbb{Z}$  tales que

$$as_1 + bs_2 = d.$$

Multiplicando la igualdad anterior por  $r$ , obtenemos que

$$r(as_1 + bs_2) = dr = c.$$

Por la propiedad distributiva,

$$a(s_1r) + b(s_2r) = c.$$

Esto demuestra que  $x = s_1r$ ,  $y = s_2r$  es una solución de la ecuación. ■

El siguiente teorema nos muestra un método para encontrar todas las soluciones enteras de una ecuación diofántica.

**Teorema 4.34.** Sean  $a, b, c \in \mathbb{Z}$ , y  $d = \text{mcd}(a, b)$ . Supongamos que  $x_0, y_0 \in \mathbb{Z}$  es una solución particular de la ecuación diofántica  $ax + by = c$ . Entonces, todas las soluciones enteras de esta ecuación son

$$x_n = x_0 + \frac{b}{d}n, \quad y_n = y_0 - \frac{a}{d}n, \quad \text{donde } n \in \mathbb{Z}. \quad (4.9)$$

**Demostración.** Observemos que  $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$ , ya que  $d = \text{mcd}(a, b)$ . Como  $x_0, y_0$  es una solución particular de  $ax + by = c$ , los enteros dados en (4.9) también son soluciones:

$$\begin{aligned} a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) &= ax_0 + by_0 + \frac{b}{d}an - \frac{a}{d}bn \\ &= ax_0 + by_0 = c. \end{aligned}$$

Ahora demostraremos que todas las soluciones tienen esta forma. Supongamos que  $\hat{x}, \hat{y} \in \mathbb{Z}$  es una solución de  $ax + by = c$ . Entonces,

$$a\hat{x} + b\hat{y} = c = ax_0 + by_0 \Rightarrow a(\hat{x} - x_0) = b(y_0 - \hat{y}).$$

Dividiendo la igualdad anterior entre  $d$ , obtenemos que

$$\frac{a}{d}(\hat{x} - x_0) = \frac{b}{d}(y_0 - \hat{y}). \quad (4.10)$$

Por el ejercicio 4.42,  $\frac{a}{d}$  y  $\frac{b}{d}$  son primos relativos. Luego, la igualdad (4.10) y el lema de Euclides 4.28 implican que

$$\frac{a}{d} \mid (y_0 - \hat{y}).$$

Por lo tanto, existe  $n \in \mathbb{Z}$  tal que

$$y_0 - \hat{y} = \frac{a}{d}n \implies \hat{y} = y_0 - \frac{a}{d}n.$$

Finalmente, sustituyendo en la igualdad (4.10), obtenemos que

$$\hat{x} = x_0 + \frac{b}{d}n.$$

Esto demuestra que  $\hat{x}$ ,  $\hat{y}$  tienen la forma requerida. ■

**Ejemplo 4.35.** Resolveremos la ecuación del ejemplo 4.32,

$$20x + 50y = 430. \quad (4.11)$$

Como  $\text{mcd}(20, 50) = 10$ , y 10 divide a 430, sabemos, por el teorema 4.33, que la ecuación (4.11) tiene soluciones enteras. Una solución particular puede encontrarse usando el algoritmo de Euclides. Veamos que

$$50 = 2 \cdot 20 + 10 \implies 10 = -2 \cdot 20 + 1 \cdot 50.$$

Multiplicando por 43, tenemos que

$$430 = -86 \cdot 20 + 43 \cdot 50.$$

Esto demuestra que  $x_0 = -86$ ,  $y_0 = 43$  es una solución particular.

Por el teorema 4.34, todas las soluciones enteras de la ecuación (4.11) son

$$x_n = -86 + 5n, \quad y_n = 43 - 2n, \quad n \in \mathbb{Z}.$$

En este ejemplo estamos interesados en las soluciones positivas porque el número de bolígrafos y cuadernos son enteros positivos. La ecuación tiene cinco soluciones enteras positivas:

$$\begin{aligned} x_{18} &= 4, & y_{18} &= 7, \\ x_{19} &= 9, & y_{19} &= 5, \\ x_{20} &= 14, & y_{20} &= 3, \\ x_{21} &= 19, & y_{21} &= 1. \end{aligned}$$

**Ejemplo 4.36.** ¿Será posible llenar exactamente un depósito de agua de 55 litros si sólo tenemos recipientes de 6 y 9 litros? Para responder a esta pregunta debemos encontrar las soluciones enteras de la ecuación diofántica

$$6x + 9y = 55.$$

Sin embargo,  $\text{mcd}(6, 9) = 3$  y 3 no divide a 55, así que, por el teorema 4.33, sabemos que no existen soluciones enteras. En otras palabras, no es posible llenar exactamente el depósito con los recipientes mencionados.

**Palabras clave de la sección:** *divisor, número primo, algoritmo de la división, máximo común divisor, lema de Bézout, algoritmo de Euclides, lema de Euclides, teorema fundamental de la aritmética, ecuación diofántica.*

### 4.2.3 Ejercicios de números enteros

**Ejercicio 4.37.** Demuestra que 13 divide a  $4^{2n+1} + 3^{n+2}$ , para toda  $n \in \mathbb{N}$  (sugerencia: usa el principio de inducción matemática).

**Ejercicio 4.38.** Demuestra que si  $p$  es primo,  $a \in \mathbb{Z}$  y  $n \in \mathbb{N}$  tal que  $p \mid a^n$ , entonces  $p \mid a$  (sugerencia: usa el principio de inducción matemática y el lema de Euclides).

**Ejercicio 4.39.** Sean  $p_1, p_2, \dots, p_n$  números primos. Demuestra que el número  $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$  no es divisible entre ninguno de los primos  $p_i$  para toda  $i = 1, 2, \dots, n$ . Usa este hecho y el teorema fundamental de la aritmética para demostrar, por reducción al absurdo, que hay un número infinito de primos.

**Ejercicio 4.40.** Investiga qué es la *criba de Eratóstenes* y úsala para encontrar todos los números primos menores que cien.

**Ejercicio 4.41.** Para cada uno de los siguientes valores de  $a$  y  $b$ , usa el algoritmo de Euclides para calcular  $\text{mcd}(a, b)$  y expresarlo en la forma  $\text{mcd}(a, b) = as_1 + bs_2$ ,  $s_1, s_2 \in \mathbb{Z}$ .

- a)  $a = 16, b = 8$ .
- b)  $a = 63, b = 49$ .
- c)  $a = 619, b = 93$ .
- d)  $a = 52163, b = 2187$ .

**Ejercicio 4.42.** Sean  $a, b \in \mathbb{Z}$  y  $d = \text{mcd}(a, b)$ . Demuestra que

$$\frac{a}{d}, \frac{b}{d} \in \mathbb{Z},$$

son primos relativos.

**Ejercicio 4.43.** Encuentra todas las soluciones enteras de las siguientes ecuaciones diofánticas:

- a)  $9x - 12y = 10$ .
- b)  $2x + 3y = 7$ .
- c)  $21x - 35y = -14$ .

**Ejercicio 4.44.** ¿De cuántas formas es posible tener \$325 en monedas de \$5 y \$10?

## 4.3 Congruencias

**Definición 4.45 (congruencia módulo  $m$ ).** Sea  $m \in \mathbb{N}$ ,  $m \neq 0$ . Dos números enteros  $a, b \in \mathbb{Z}$  son *congruentes módulo  $m$*  si  $m \mid (a - b)$ .

Usamos la notación

$$a \equiv b \pmod{m}$$

para indicar que  $a$  y  $b$  son congruentes módulo  $m$ . Si no son congruentes, escribimos

$$a \not\equiv b \pmod{m}.$$

En particular,  $a \equiv 0 \pmod{m}$  si y sólo si  $a$  es múltiplo de  $m$ .

**Ejemplo 4.46.** Consideremos los siguientes ejemplos:

- 1)  $14 \equiv 6 \pmod{4}$  ya que  $4 \mid (14 - 6) = 8$ .
- 2)  $10 \equiv 15 \pmod{5}$  ya que  $5 \mid (10 - 15) = -5$ .
- 3)  $12 \equiv 6 \pmod{3}$  ya que  $3 \mid (12 - 6) = 6$ .
- 4)  $22 \not\equiv 6 \pmod{5}$  ya que  $(22 - 6) = 16$  no es múltiplo de 5.

El lenguaje de las congruencias fue inventado por el matemático alemán Carl Friedrich Gauss en su libro *Disquisitiones arithmeticae* en 1801. Actualmente se usa constantemente en la vida cotidiana; por ejemplo, las manecillas de un reloj indican la hora módulo 12.

**Teorema 4.47.** Sea  $m \in \mathbb{N}$ ,  $m \neq 0$ . La relación de congruencia módulo  $m$  es una relación de equivalencia sobre  $\mathbb{Z}$ .

**Demostración.**

- 1) *Reflexividad.* Claramente,  $a \equiv a \pmod{m}$ , para toda  $a \in \mathbb{Z}$ , ya que  $m$  siempre divide a  $a - a = 0$ .
- 2) *Simetría.* Sean  $a, b \in \mathbb{Z}$  y supongamos que  $a \equiv b \pmod{m}$ . Entonces  $m \mid a - b$ , lo que significa que  $a - b = km$  para algún  $k \in \mathbb{Z}$ . Multiplicando por  $-1$  obtenemos que  $b - a = (-k)m$ . Luego,  $m \mid b - a$  y  $b \equiv a \pmod{m}$ .
- 3) *Transitividad.* Sean  $a, b, c \in \mathbb{Z}$  tales que  $a \equiv b \pmod{m}$  y  $b \equiv c \pmod{m}$ . Entonces se cumple que  $a - b = k_1m$  y  $b - c = k_2m$  para algunos  $k_1, k_2 \in \mathbb{Z}$ . Sumando las igualdades anteriores obtenemos que  $a - c = (k_1 + k_2)m$ , lo que implica que  $a \equiv c \pmod{m}$ . ■

La suma y multiplicación de enteros tienen un buen comportamiento con respecto a las congruencias módulo  $m$ .

**Teorema 4.48.** Sea  $m \in \mathbb{N}$ ,  $m \neq 0$ . Sean  $a, a', b, b' \in \mathbb{Z}$  tales que  $a \equiv a' \pmod{m}$  y  $b \equiv b' \pmod{m}$ . Entonces:

- 1)  $(a + b) \equiv (a' + b') \pmod{m}$ .
- 2)  $ab \equiv a'b' \pmod{m}$ .

**Demostración.**

- 1) Si  $a \equiv a' \pmod{m}$  y  $b \equiv b' \pmod{m}$ , sabemos que existen  $r, s \in \mathbb{Z}$ , tales que  $(a - a') = rm$  y  $(b - b') = sm$ . Entonces

$$(a + b) - (a' + b') = (a - a') + (b - b') = (r + s)m.$$

Por lo tanto,  $(a + b) \equiv (a' + b') \pmod{m}$ .

- 2) En forma análoga, tenemos que

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= (a - a')b + a'(b - b') \\ &= rbm + sa'm \\ &= (rb + sa')m. \end{aligned}$$

Por lo tanto,  $ab \equiv a'b' \pmod{m}$ . ■

Las clases de equivalencia de la relación módulo  $m$  forman una partición de  $\mathbb{Z}$  (teorema 3.67). Denotamos como  $\mathbb{Z}_m$  al conjunto cociente de esta relación.

**Ejemplo 4.49.** Hay dos clases de equivalencia en la relación módulo 2 sobre  $\mathbb{Z}$ . Una de estas clases contiene a los números divisibles entre 2 (los pares) y la otra contiene a los números que no son divisibles entre 2 (los impares). Explícitamente,

$$\begin{aligned} [0] &= \{0, \pm 2, \pm 4, \dots\} = \{2n : n \in \mathbb{Z}\}, \\ [1] &= \{\pm 1, \pm 3, \pm 5, \dots\} = \{2n + 1 : n \in \mathbb{Z}\}. \end{aligned}$$

Por lo tanto, el conjunto cociente es

$$\mathbb{Z}_2 = \{[0], [1]\}.$$

Compara esto con el ejemplo 3.69.



**Ejemplo 4.50.** En este ejemplo encontramos  $\mathbb{Z}_3$ . Si  $a \in \mathbb{Z}$ , el algoritmo de la división implica que existen enteros  $q$  y  $r$  tales que

$$a = 3q + r,$$

donde  $0 \leq r < 3$ . Por lo tanto,  $3 \mid (a - r)$  y

$$a \equiv r \pmod{3}, \text{ donde } 0 \leq r < 3.$$

Esto significa que cualquier número entero siempre es congruente módulo 3 con 0, 1 o 2. Por lo tanto,  $\mathbb{Z}_3$  contiene exactamente tres clases de equivalencia:

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

donde

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

En general, dado cualquier número  $a \in \mathbb{Z}$ , podemos usar el algoritmo de la división para encontrar un entero  $r$ ,  $0 \leq r < m$ , tal que  $a \equiv r \pmod{m}$ . Esto significa que las clases de equivalencia módulo  $m$  siempre tienen representantes  $0, 1, 2, \dots, m - 1$ .

**Ejemplo 4.51.** Consideremos la clase de equivalencia de 243 en la relación módulo 11. Debido a que  $11k \equiv 0 \pmod{11}$ ,  $\forall k \in \mathbb{Z}$ , el teorema 4.48 implica que

$$243 \equiv (243 + 11) \equiv (243 + 22) \equiv (243 - 11) \pmod{11}.$$

En otras palabras, podemos sumar y restar múltiplos de 11 para obtener otros números en la misma clase:

$$[243] = [254] = [265] = [232].$$

Para encontrar un representante menor que 11, usamos el algoritmo de la división:

$$243 = 11 \cdot 22 + 1.$$

Por lo tanto,  $1 \equiv 243 \pmod{11}$ , y  $[243] = [1]$ .

Las congruencias tienen varias aplicaciones. Una de las más elementales consiste en la obtención de reglas de divisibilidad, como las que se muestran en las siguientes proposiciones.

**Proposición 4.52.** Un número entero es divisible entre 9 si y sólo si la suma de sus cifras es divisible entre 9.

**Demostración.** Sea  $x \in \mathbb{Z}$  y sean  $x_0, x_1, \dots, x_n$  sus cifras decimales, esto es

$$x = x_0 + x_1 10 + x_2 10^2 + \dots + x_n 10^n,$$

donde  $n \in \mathbb{N}$ .

Por el ejercicio 4.57, tenemos que  $10^k \equiv 1 \pmod{9}$  para cualquier  $k \in \mathbb{N}$ . Entonces, por el teorema 4.48, deducimos que

$$x \equiv x_0 + x_1 10 + \dots + x_n 10^n \equiv x_0 + x_1 + \dots + x_n \pmod{9}.$$

En particular, 9 divide a  $x$  si y sólo si  $x \equiv 0 \pmod{9}$ , lo cual es cierto si y sólo si

$$x_0 + x_1 + \dots + x_n \equiv 0 \pmod{9}.$$

Esto último significa que  $x_0 + x_1 + \dots + x_n$  es divisible entre 9. ■

**Proposición 4.53.** Un número entero es divisible entre 3 si y sólo si la suma de sus cifras es divisible entre 3.

**Demostración.** Debido a que  $10^k \equiv 1 \pmod{3}$  para cualquier  $k \in \mathbb{N}$ , el resultado se deduce con un razonamiento similar al usado para demostrar la proposición 4.52. La demostración formal de esta proposición se deja como ejercicio. ■

**Ejemplo 4.54.** El número entero 19731 es divisible entre 3 pero no entre 9, porque la suma  $1 + 9 + 7 + 3 + 1 = 21$  es divisible entre 3 pero no entre 9.

**Palabras clave de la sección:** congruencia módulo  $m$ , propiedades de sumas y productos de congruencias módulo  $m$ , conjunto cociente  $\mathbb{Z}_m$ , reglas de divisibilidad entre 3 y 9.

### 4.3.1 Ejercicios de congruencias

**Ejercicio 4.55.** Encuentra los conjuntos cocientes  $\mathbb{Z}_6$  y  $\mathbb{Z}_7$ , describiendo brevemente cada una de las clases de equivalencia que contienen.

**Ejercicio 4.56.** Sea  $a \in \mathbb{Z}$  y  $m \in \mathbb{N}$ ,  $m \neq 0$ . Encuentra un entero  $r$ ,  $0 \leq r < m$ , tal que  $a \equiv r \pmod{m}$  en los siguientes casos:

- a) Con  $a = 7$  y  $m = 10$ .
- b) Con  $a = -15$  y  $m = 7$ .
- c) Con  $a = 126$  y  $m = 6$ .
- d) Con  $a = 160$  y  $m = 13$ .

**Ejercicio 4.57.** Demuestra, por inducción, que  $10^k \equiv 1 \pmod{9}$  para toda  $k \in \mathbb{N}$ .

**Ejercicio 4.58.** Demuestra que si  $a \in \mathbb{Z}$ , entonces  $a^2$  es congruente con 0 o 1 módulo 4.

**Ejercicio 4.59.** Sea  $p \in \mathbb{N}$  un número primo. Demuestra que si  $ab \equiv 0 \pmod{p}$  entonces  $a \equiv 0 \pmod{p}$  o  $b \equiv 0 \pmod{p}$ .

**Ejercicio 4.60.** Sean  $a, b, c \in \mathbb{Z}$  y  $m \in \mathbb{N}$ ,  $m \neq 0$ . Demuestra que si  $ac \equiv bc \pmod{m}$  entonces  $a \equiv b \pmod{\frac{m}{d}}$  donde  $d = \text{mcd}(c, m)$ .

**Ejercicio 4.61.** Demuestra la proposición 4.53.

**Ejercicio 4.62.** Escribe un número entero  $x$  de ocho cifras tal que:

- a)  $x$  sea divisible entre 3, pero no entre 9.
- b)  $x$  sea divisible entre 2 y 3.
- c)  $x$  sea divisible entre 5 y 9. ¿Es  $x$  también divisible entre 3?

## 4.4 Cardinalidad

### 4.4.1 Comparación de cardinalidades

En esta sección estudiamos cómo comparar el tamaño de dos conjuntos. Cuando ambos conjuntos son finitos, la forma más razonable de comparar sus tamaños es contar el número de sus elementos y usar la relación de orden en  $\mathbb{N}$ . Sin embargo, ¿qué podemos hacer en el caso de los conjuntos infinitos? La forma de resolver esto es usando funciones inyectivas.

**Definición 4.63.** Sean  $S$  y  $T$  conjuntos, finitos o infinitos.

- 1) Decimos que *la cardinalidad de  $S$  es menor o igual que la de  $T$* , y escribimos

$$|S| \leq |T|,$$

si existe una función inyectiva de  $S$  en  $T$ .

- 2) Decimos que  $S$  y  $T$  tienen *la misma cardinalidad*, y escribimos

$$|S| = |T|,$$

si existe una función biyectiva de  $S$  en  $T$ .

Cuando  $S$  y  $T$  tienen la misma cardinalidad, también decimos que son conjuntos *equipotentes*. Como es usual,  $|S| < |T|$  significa que  $|S| \leq |T|$  y  $|S| \neq |T|$ .

**Proposición 4.64.** Sea  $\mathcal{F}$  una colección de conjuntos. La relación de igualdad entre cardinalidades es una relación de equivalencia sobre  $\mathcal{F}$ .

**Demostración.**

- 1) *Reflexividad.* Cualquier conjunto  $S \in \mathcal{F}$  satisface que  $|S| = |S|$ , puesto que la identidad en  $S$  es una función biyectiva sobre  $S$ .
- 2) *Simetría.* Sean  $S, T \in \mathcal{F}$ . Si  $f : S \rightarrow T$  es una función biyectiva, su inversa  $f^{-1} : T \rightarrow S$  también es una función biyectiva (teorema 3.43). Esto implica que si  $|S| = |T|$ , entonces  $|T| = |S|$ .
- 3) *Transitividad.* Sean  $T, S, U \in \mathcal{F}$ . Si  $|S| = |T|$  y  $|T| = |U|$ , existen funciones biyectivas  $f : S \rightarrow T$  y  $g : T \rightarrow U$ . Es sencillo demostrar que la composición  $g \circ f : S \rightarrow U$  también es una función biyectiva (ejercicio 4.82). Por lo tanto  $|S| = |U|$ . ■

La proposición anterior debe restringirse a una colección de conjuntos puesto que, como discutimos en la sección 2.1, la colección de *todos* los conjuntos no es un conjunto.

Originalmente, el matemático alemán Georg Cantor definió la *cardinalidad* de un conjunto  $S$  como la clase de equivalencia

$$[S] = \{X : |X| = |S|\}.$$

Sin embargo, esta definición no funciona en las teorías axiomáticas modernas debido a que  $[S]$  es un conjunto “demasiado grande” (es decir, es una *clase propia*). La definición formal de cardinalidad está fuera del alcance de este texto: nos enfocaremos más en comparar cardinalidades que en definir el concepto de cardinalidad mismo.

En el siguiente teorema establecemos algunas de las propiedades básicas relacionadas con la comparación de cardinalidades.

**Teorema 4.65.** Sean  $S$ ,  $T$  y  $U$  conjuntos.

- 1) Si  $S \subseteq T$ , entonces  $|S| \leq |T|$ .
- 2)  $|S| \leq |S|$ .
- 3) Si  $|S| \leq |T|$  y  $|T| \leq |U|$ , entonces  $|S| \leq |U|$ .

**Demostración.**

- 1) Si  $S \subseteq T$  la función de inclusión  $i : S \rightarrow T$  definida por  $i(s) = s$ , para todo  $s \in S$ , es inyectiva.
- 2) Ejercicio 4.83.
- 3) Ejercicio 4.84. ■

Las partes 2) y 3) del teorema anterior son las propiedades reflexiva y transitiva de la relación  $\leq$  entre cardinalidades. El siguiente teorema establece que la relación  $\leq$  entre cardinalidades es también antisimétrica, y por lo tanto, una relación de orden.

**Teorema 4.66 (de Schroeder-Bernstein).** Sean  $S$  y  $T$  dos conjuntos. Si  $|S| \leq |T|$  y  $|T| \leq |S|$ , entonces  $|S| = |T|$ .

A simple vista, el teorema de Schroeder-Bernstein podría parecer obvio; sin embargo, hay que tener presente que  $|S| \leq |T|$  significa que existe una función inyectiva de  $S$  en  $T$ , mientras que  $|T| \leq |S|$  significa que existe una función inyectiva de  $T$  en  $S$ . Por esto, especialmente cuando  $S$  y  $T$  son infinitos, no es trivial demostrar que  $|T| = |S|$  (es decir, que existe una función biyectiva de  $T$  en  $S$ ). En vista de esto, omitimos la demostración de este teorema.

Si  $n \in \mathbb{N}$ , denotamos al conjunto de los primeros  $n$  números naturales como:

$$\mathbf{n} = \{0, 1, 2, \dots, n-1\}.$$

Así, por ejemplo,  $2 = \{0, 1\}$  y  $5 = \{0, 1, 2, 3, 4\}$ . Si  $n = 0$ , definimos  $0 = \{\}$ .

**Definición 4.67 (conjunto finito).** Un conjunto  $S$  es *finito* si  $|S| = |\mathbf{n}|$ , para algún  $n \in \mathbb{N}$ .

De manera más intuitiva,  $|S| = |\mathbf{n}|$  significa que el conjunto  $S$  tiene precisamente  $n$  elementos. Si un conjunto no es finito, decimos que es *infinito*.

**Proposición 4.68.** Todo subconjunto de un conjunto finito es finito.

**Demostración.** Sea  $S$  un conjunto finito. Si  $S = \emptyset$ , el único subconjunto de  $S$  es  $S$  mismo, así que la proposición es verdadera en este caso. Supongamos que  $S \neq \emptyset$ . Por definición, existe una función biyectiva  $f : S \rightarrow \mathbf{n}$ , para algún  $n \in \mathbb{N}$ ,  $n \neq 0$ . Sea  $T$  un subconjunto no vacío de  $S$ . La imagen de  $T$  es un conjunto de números naturales:

$$f(T) = \{f(t_1), f(t_2), \dots, f(t_k)\} \subseteq \mathbf{n},$$

para algún  $k \in \mathbb{N}$ ,  $k \leq n$ . Ahora, podemos definir una función biyectiva  $g : T \rightarrow \mathbf{k}$  como  $g(t_i) = i$  donde  $i \in \mathbf{k}$ . Esto demuestra que  $T$  es finito. ■

#### 4.4.2 Conjuntos numerables

El ejemplo más claro de un conjunto infinito es  $\mathbb{N}$ .

**Proposición 4.69.** El conjunto de los números naturales es infinito.

**Demostración.** Por reducción al absurdo, supongamos que  $|\mathbb{N}| = |\mathbf{n}|$  para algún  $n \in \mathbb{N}$ . Por definición, existe una función biyectiva

$$f : \{0, 1, \dots, n-1\} \rightarrow \mathbb{N}.$$

El rango de esta función es  $\text{ran}(f) = \{f(0), f(1), \dots, f(n-1)\} = \mathbb{N}$ . Sea  $s \in \mathbb{N}$  el sucesor del máximo absoluto de  $\text{ran}(f)$ . Entonces,  $s \notin \text{ran}(f)$ , porque  $s$  es estrictamente mayor que cada uno de los elementos de  $\text{ran}(f)$ . Por lo tanto,  $\text{ran}(f) \neq \mathbb{N}$ , lo que implica que la función  $f$  no es sobreyectiva. Esta contradicción demuestra que  $\mathbb{N}$  es infinito. ■

Los conjuntos cuya cardinalidad es menor o igual que la cardinalidad de  $\mathbb{N}$  reciben un nombre especial.

**Definición 4.70 (numerable).** Decimos que un conjunto  $S$  es *numerable* si  $|S| \leq |\mathbb{N}|$ .

En otras palabras, un conjunto  $S$  es numerable si existe una función inyectiva de  $S$  en  $\mathbb{N}$ . En particular, es claro que cualquier conjunto finito es numerable.

**Definición 4.71 (infinito numerable).** Decimos que un conjunto  $S$  es *infinito numerable* si  $|S| = |\mathbb{N}|$ .

Si  $S$  es finito, entonces  $|S| < |\mathbb{N}|$ .

**Ejemplo 4.72.** El conjunto  $2\mathbb{N}$ , de números pares, es un subconjunto propio de  $\mathbb{N}$  porque  $1 \in \mathbb{N}$  pero  $1 \notin 2\mathbb{N}$ . Sin embargo,  $\mathbb{N}$  y  $2\mathbb{N}$  tienen la misma cardinalidad: la función  $f : \mathbb{N} \rightarrow 2\mathbb{N}$  definida por  $f(n) = 2n$  es biyectiva, por lo que

$$|2\mathbb{N}| = |\mathbb{N}|.$$

Si  $S$  es un conjunto numerable, entonces, por definición, existe una función inyectiva  $f : S \rightarrow \mathbb{N}$ . Esta función provee una forma de enumerar los elementos de  $S$  usando las imágenes bajo  $f$ : si  $f(s) = k \in \mathbb{N}$ , escribimos  $s = s_k$ . Luego,

$$S = \{s_1, s_2, s_3, \dots\} = \{s_n : n \in \mathbb{N}\}.$$

Esta habilidad de enlistar los elementos de un conjunto caracteriza a los conjuntos numerables. Si la lista termina, entonces el conjunto es finito; en caso contrario,  $S$  es infinito numerable.

**Teorema 4.73.** Cualquier subconjunto de un conjunto numerable es numerable.

**Demostración.** Sea  $S$  un conjunto numerable y  $T \subseteq S$ . Por el teorema 4.65 parte 1), tenemos que  $|T| \leq |S|$ . Como  $S$  es numerable,  $|S| \leq |\mathbb{N}|$ . El teorema 4.65 parte 3) implica que  $|T| \leq |\mathbb{N}|$ , lo que significa que  $T$  es numerable. ■

Usando el teorema 4.73, deducimos otro criterio para determinar cuándo un conjunto es numerable.

**Teorema 4.74.** Un conjunto  $S$  es numerable si y sólo si existe una función sobreyectiva de  $\mathbb{N}$  en  $S$ .

**Demostración.**

( $\Rightarrow$ ) Supongamos que  $S$  es numerable. Por definición, existe una función inyectiva  $f : S \rightarrow \mathbb{N}$ . Claramente,  $f$  es una función biyectiva de  $S$  en  $f(S)$ , así que  $f^{-1} : f(S) \rightarrow S$  es una función biyectiva. Usaremos  $f^{-1}$  para construir una función sobreyectiva. Sea  $s \in S$  cualquier elemento fijo. Definamos  $g : \mathbb{N} \rightarrow S$  como

$$g(n) = \begin{cases} f^{-1}(n), & \text{si } n \in f(S), \\ s, & \text{si } n \notin f(S). \end{cases}$$

Esta función es sobreyectiva porque

$$g(f(S)) = f^{-1}(f(S)) = S \text{ y } g(\mathbb{N} \setminus f(S)) = \{s\},$$

lo que implica que  $\text{ran}(g) = S$ .

( $\Leftarrow$ ) Supongamos que existe una función sobreyectiva  $g : \mathbb{N} \rightarrow S$ . Definamos  $h : S \rightarrow \mathbb{N}$  como  $h(s) = n$ , donde  $n$  es el mínimo absoluto del conjunto  $g^{-1}(s)$  de las preimágenes de  $s \in S$ ; en otras palabras,  $n$  es el número natural más pequeño tal que  $g(n) = s$ . La función  $h$  está definida en todo el conjunto  $S$  porque  $g$  es sobreyectiva. Además,  $h$  es inyectiva porque

$$h(s_1) = h(s_2) \Rightarrow g(h(s_1)) = g(h(s_2)) \Rightarrow s_1 = s_2.$$

Esto demuestra que  $|S| \leq |\mathbb{N}|$ , y  $S$  es numerable por definición. ■

**Proposición 4.75.** Sean  $S$  y  $T$  conjuntos numerables. Entonces:

- 1)  $S \cup T$  es numerable.
- 2)  $S \times T$  es numerable.

**Demostración.**

- 1) Por el teorema 4.74 existen funciones sobreyectivas  $f : \mathbb{N} \rightarrow S$  y  $g : \mathbb{N} \rightarrow T$ . Entonces, la función  $h : \mathbb{N} \rightarrow S \cup T$  definida como

$$h(n) = \begin{cases} f\left(\frac{n+1}{2}\right), & \text{si } n \text{ es impar,} \\ g\left(\frac{n}{2}\right), & \text{si } n \text{ es par,} \end{cases}$$

es sobreyectiva (ejercicio 4.85), lo que demuestra que  $S \cup T$  es numerable.



- 2) Por definición, existen funciones inyectivas  $f : S \rightarrow \mathbb{N}$  y  $g : T \rightarrow \mathbb{N}$ . Entonces la función  $r : S \times T \rightarrow \mathbb{N}$  definida como

$$r(s, t) = 2^{f(s)} \cdot 3^{g(t)}, \text{ donde } s \in S \text{ y } t \in T,$$

es inyectiva (ejercicio 4.85). Luego,  $S \times T$  es numerable. ■

**Ejemplo 4.76.** El conjunto  $\mathbb{Z}_{\geq 0}$  de los enteros no negativos es numerable porque la función  $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{N}$  definida como  $f(n) = n$ ,  $n \in \mathbb{Z}_{\geq 0}$ , es inyectiva. El conjunto  $\mathbb{Z}_{< 0}$  de los enteros negativos es numerable porque la función  $g : \mathbb{Z}_{< 0} \rightarrow \mathbb{N}$  definida como  $g(n) = -n$ ,  $n \in \mathbb{Z}_{< 0}$ , es inyectiva. Debido a que

$$\mathbb{Z} = \mathbb{Z}_{\geq 0} \cup \mathbb{Z}_{< 0},$$

la proposición 4.75, 1) implica que  $\mathbb{Z}$  es numerable. En otras palabras,

$$|\mathbb{Z}| = |\mathbb{N}|.$$

**Ejemplo 4.77.** En este ejemplo demostraremos que  $|\mathbb{Q}| = |\mathbb{N}|$ . Cada elemento de  $\mathbb{Q}$  puede identificarse con un par de números enteros (el numerador y el denominador). Por la proposición 4.75, 2), el conjunto  $\mathbb{Z} \times \mathbb{Z}$  es numerable porque  $\mathbb{Z}$  lo es. Como  $\mathbb{Q}$  es un subconjunto de  $\mathbb{Z} \times \mathbb{Z}$  bajo la identificación previa, el teorema 4.73 implica que  $\mathbb{Q}$  es numerable.

No todos los conjuntos tienen cardinalidad menor o igual que  $\mathbb{N}$ ; en otras palabras, existen conjuntos infinitos que no son numerables.

**Teorema 4.78.** El conjunto de los números reales no es numerable.

**Demostración.** Puesto que cualquier subconjunto de un conjunto numerable es numerable (Teorema 4.73), es suficiente demostrar que el intervalo  $J = (0, 1) \subseteq \mathbb{R}$  no es numerable. Por reducción al absurdo, supongamos que  $J$  es numerable, así que podemos enlistar sus elementos

$$J = \{x_1, x_2, x_3, \dots\} = \{x_n : n \in \mathbb{N}\}. \quad (4.12)$$

Mostraremos que esto conduce a una contradicción mediante la construcción de un número real  $y$  en  $J = (0, 1)$  distinto de todos

los números  $x_n$  de la lista. Cada elemento de  $J = (0, 1)$  tienen una expansión decimal de la forma:

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13} \cdots, \\ x_2 &= 0.a_{21}a_{22}a_{23} \cdots, \\ x_3 &= 0.a_{31}a_{32}a_{33} \cdots, \\ &\vdots \end{aligned}$$

donde  $a_{ij} \in \{0, 1, 2, \dots, 9\}$ . Definamos  $y = 0.b_1b_2b_3 \cdots$  donde

$$b_n = \begin{cases} 1, & \text{si } a_{nn} \neq 1, \\ 2, & \text{si } a_{nn} = 1. \end{cases}$$

Claramente  $y \in J$ . Sin embargo,  $y \neq x_i$  para toda  $i$ , porque  $y$  difiere de  $x_i$  en el  $i$ -ésimo decimal. Esto contradice la suposición de que la lista (4.12) incluye a todos los elementos de  $J$ . Por lo tanto,  $J$  no es numerable. ■

El teorema anterior demuestra que  $|\mathbb{R}| > |\mathbb{N}|$ .

### 4.4.3 Números cardinales

De manera informal, decimos que un *número cardinal* es un objeto matemático usado para medir la cardinalidad o el tamaño de un conjunto. Como es de esperarse, conjuntos que tengan la misma cardinalidad (en el sentido de la definición 4.63) deben tener asignado el mismo número cardinal. Además, establecemos un orden en estos números cardinales de acuerdo con el orden de las cardinalidades de sus respectivos conjuntos.

El número cardinal asociado con  $\mathbf{n} = \{0, \dots, n-1\}$  es simplemente el número natural  $n \in \mathbb{N}$ ; esto significa que  $n$  es el número cardinal asociado con cualquier conjunto finito de  $n$  elementos.

El número cardinal asociado con el conjunto  $\mathbb{N}$  es  $\aleph_0$ .<sup>2</sup> Por lo tanto, el número cardinal asociado con cualquier conjunto infinito numerable es también  $\aleph_0$ .

Por otro lado, el número cardinal asociado con  $\mathbb{R}$  es  $\mathfrak{c}$ . Puesto que  $\mathbb{R}$  es un conjunto infinito no numerable, debemos tener que  $\aleph_0 < \mathfrak{c}$ .

<sup>2</sup>El símbolo  $\aleph_0$  se lee “alef-sub-cero”. Alef es la primera letra del alfabeto hebreo.

Los números cardinales asociados con conjuntos infinitos, como  $\aleph_0$  y  $\mathfrak{c}$ , son llamados *cardinales transfinitos*. ¿Existen otros cardinales transfinitos además de  $\aleph_0$  y  $\mathfrak{c}$ ? La respuesta es un rotundo sí, como lo muestra el siguiente teorema.

**Teorema 4.79 (Cantor).** Para cualquier conjunto  $S$ ,

$$|S| < |P(S)|,$$

donde  $P(S)$  es el conjunto potencia de  $S$ .

**Demostración.** La función  $g : S \rightarrow P(S)$  dada por  $g(s) = \{s\}$  es claramente inyectiva, por lo que  $|S| \leq |P(S)|$ . Esta función no es sobreyectiva porque  $\emptyset$  no pertenece al rango de  $g$ . Para probar que  $|S| \neq |P(S)|$  debemos mostrar que ninguna función de  $S$  en  $P(S)$  puede ser sobreyectiva (por lo tanto, ninguna función de  $S$  en  $P(S)$  puede ser una biyección).

Sea  $f : S \rightarrow P(S)$  una función. Como  $f(x) \in P(S)$  es un subconjunto de  $S$ , tiene sentido preguntarse si  $x \in f(x)$  o  $x \notin f(x)$ . Definamos

$$T = \{x \in S : x \notin f(x)\}.$$

En particular,  $T \in P(S)$  porque  $T \subseteq S$ . Demostraremos que  $T \notin \text{ran}(f)$ , lo que implica que  $f$  no es sobreyectiva. Por reducción al absurdo, supongamos que  $T \in \text{ran}(f)$ . Entonces,  $T = f(y)$  para alguna  $y \in S$ . Esto genera una paradoja, ya que:

$$(y \in T) \Leftrightarrow (y \notin f(y)) \Leftrightarrow (y \notin T).$$

Por lo tanto, no es posible que  $T \in \text{ran}(f)$  y el teorema queda demostrado. ■

Aplicando el teorema 4.79 repetidamente obtenemos una secuencia infinita de cardinales transfinitos, cada uno mayor que el anterior:

$$\aleph_0 = |\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| < |P(P(P(\mathbb{N})))| < \dots$$

En el ejercicio 4.89 esbozamos la demostración de que  $|P(\mathbb{N})| = \mathfrak{c}$ .

Usando el *axioma de elección*, es posible demostrar que cualquier conjunto infinito contiene un subconjunto numerable, así que  $\aleph_0$  es el cardinal transfinito más pequeño. Sabemos que  $\aleph_0 < \mathfrak{c}$ , pero ¿existirá cardinal transfinito  $\lambda$  tal que  $\aleph_0 < \lambda < \mathfrak{c}$ ? Más concretamente, ¿existirá un subconjunto  $X \subseteq \mathbb{R}$  tal que  $|\mathbb{N}| < |X| < |\mathbb{R}|$ ? La experiencia nos sugiere que no, porque nunca se ha encontrado

ningún conjunto como este. La conjetura de que existe un conjunto  $X$  con tal característica fue propuesta por Georg Cantor y es conocida como la *hipótesis del continuo*.

En 1900, David Hilbert incluyó la demostración de la hipótesis del continuo como el primero de sus famosos 23 problemas sin resolver. En 1938, Kurt Godel demostró que el suponer verdadera la hipótesis del continuo no contradice ninguno de los axiomas de la teoría de conjuntos. Por otro lado, en 1963, Paul Cohen demostró que el suponer falsa la hipótesis del continuo tampoco contradice los axiomas. Por lo tanto, la hipótesis del continuo es *independiente* de los axiomas aceptados en la actualidad: no se puede demostrar ni refutar.

**Palabras clave de la sección:** *comparación de cardinalidades; conjuntos finitos, infinitos y numerables; números cardinales; teorema de Cantor; hipótesis del continuo.*

### 4.4.4 Ejercicios de cardinalidad

**Ejercicio 4.80.** Determina cuáles de los siguientes conjuntos son finitos, infinitos numerables, o no numerables. Justifica tu respuesta.

- a) El conjunto de números enteros que son divisibles entre 3.
- b) El conjunto de números naturales menores o iguales que 100.
- c) El conjunto de los números primos.
- d) El conjunto de los números complejos.

**Ejercicio 4.81.** Determina si las siguientes afirmaciones son falsas o verdaderas. Justifica tu respuesta.

- a) Dos conjuntos  $S$  y  $T$  tienen la misma cardinalidad si existe una función biyectiva  $f : S \rightarrow T$ .
- b) Si  $T$  y  $S$  son conjuntos numerables, entonces  $T \cap S$  es numerable.
- c) Si  $A$  y  $B$  son conjuntos,  $|A| = 7$ ,  $|B| = 5$ , entonces existe una función biyectiva de  $A$  en  $B$ .
- d) Si  $A$  y  $B$  son conjuntos,  $|A| = 7$ ,  $|B| = 5$ , entonces existe una función inyectiva de  $B$  en  $A$ .

**Ejercicio 4.82.** Demuestra que si  $f : S \rightarrow T$  y  $g : T \rightarrow U$  son funciones biyectivas, entonces  $g \circ f : S \rightarrow U$  también es biyectiva.

**Ejercicio 4.83.** Demuestra la parte 2) del teorema 4.65.

**Ejercicio 4.84.** Demuestra la parte 3) del teorema 4.65.

**Ejercicio 4.85.** Considera las funciones  $h : \mathbb{N} \rightarrow S \cup T$  y  $r : S \times T \rightarrow \mathbb{N}$  definidas en la demostración de la proposición 4.75. Demuestra que  $h$  es sobreyectiva y que  $r$  es inyectiva.

**Ejercicio 4.86.** Muestra que los siguientes pares de conjuntos tienen la misma cardinalidad encontrando una función biyectiva en cada caso:

- a)  $S = [0, 1]$  y  $T = [1, 3]$ .
- b)  $S = (0, 1)$  y  $T = (0, \infty)$ .
- c)  $S = (0, 1)$  y  $T = \mathbb{R}$ .

**Ejercicio 4.87.** Demuestra que:

- a) Si  $|S| \leq |T|$ , entonces  $|P(S)| \leq |P(T)|$ .  
 b) Si  $|S| = |T|$ , entonces  $|P(S)| = |P(T)|$ .

**Ejercicio 4.88.** Investiga qué dice el *axioma de elección* y escribe un argumento intuitivo que muestre que cualquier conjunto infinito contiene un subconjunto numerable.

**Ejercicio 4.89.** Esbozaremos cómo demostrar que  $|P(\mathbb{N})| = \mathfrak{c}$ , usando el teorema de Schroder-Bernstein.

- a) Debemos demostrar que  $|P(\mathbb{N})| \leq \mathfrak{c}$ . Sea  $f: P(\mathbb{N}) \rightarrow \mathbb{R}$  la función definida como

$$f(A) = 0.a_1a_2a_3 \cdots a_n \cdots ,$$

donde  $A \in P(\mathbb{N})$  y

$$a_n = \begin{cases} 0, & \text{si } n \notin A \\ 1, & \text{si } n \in A. \end{cases}$$

Demuestra que  $f$  es inyectiva.

- b) Debemos demostrar que  $\mathfrak{c} \leq |P(\mathbb{N})|$ . Por el ejercicio 4.87, sabemos que  $|P(\mathbb{N})| = |P(\mathbb{Q})|$ , debido a que  $|\mathbb{N}| = |\mathbb{Q}|$ . Por lo tanto, es suficiente demostrar que  $\mathfrak{c} \leq |P(\mathbb{Q})|$ . Consideremos la función  $g: \mathbb{R} \rightarrow P(\mathbb{Q})$  definida como

$$g(x) = \{y \in \mathbb{Q} : y < x, x \in \mathbb{R}\}.$$

Demuestra que  $g$  es inyectiva usando el hecho de que dados  $a, b \in \mathbb{R}$ , siempre existe  $r \in \mathbb{Q}$  tal que  $a < r < b$ .

## 4.5 Técnicas de conteo

En este capítulo estudiamos más a fondo las cardinalidades de conjuntos finitos. En particular, estamos interesados en encontrar métodos efectivos para “contar” las cardinalidades de conjuntos que resultan al operar dos o más conjuntos finitos.

**Teorema 4.90 (principio fundamental de conteo).** Sean  $A$  y  $B$  conjuntos finitos. Entonces:

- 1)  $|A \cup B| = |A| + |B| - |A \cap B|$ .
- 2)  $|A \times B| = |A| \times |B|$ .

### Demostración.

- 1) Si  $A$  y  $B$  son conjuntos disjuntos, es decir  $A \cap B = \emptyset$ , es claro que  $|A \cup B| = |A| + |B|$ . Este resultado también es válido si se considera la unión de más de dos conjuntos disjuntos. Ahora, veamos que los conjuntos  $A$ ,  $B$  y  $A \cup B$  tienen la siguiente descomposición en conjuntos disjuntos (recomendamos visualizar cada igualdad en un diagrama de Venn):

$$\begin{aligned} A &= (A \setminus B) \cup (A \cap B), \\ B &= (B \setminus A) \cup (A \cap B), \\ A \cup B &= (A \setminus B) \cup (B \setminus A) \cup (A \cap B). \end{aligned}$$

Al ser uniones de conjuntos disjuntos, obtenemos que

$$\begin{aligned} |A| &= |A \setminus B| + |A \cap B|, \\ |B| &= |B \setminus A| + |A \cap B|, \\ |A \cup B| &= |A \setminus B| + |B \setminus A| + |A \cap B|. \end{aligned}$$

Sumando las dos primeras igualdades obtenemos que

$$|A| + |B| = (|A \setminus B| + |B \setminus A| + |A \cap B|) + |A \cap B|.$$

Finalmente, sustituyendo  $|A \cup B|$  obtenemos la igualdad requerida:

$$|A| + |B| = |A \cup B| + |A \cap B|.$$

- 2) Sean  $|A| = n$  y  $|B| = m$ . Sin perder generalidad, supongamos que  $A = \{a_1, a_2, \dots, a_n\}$ . Ahora, descomponemos  $A \times B$  como la unión de los siguientes  $n$  conjuntos disjuntos:

$$A \times B = \{(a_1, b) : b \in B\} \cup \{(a_2, b) : b \in B\} \cup \dots \cup \{(a_n, b) : b \in B\}.$$

Al ser disjuntos, se cumple que

$$|A \times B| = |\{(a_1, b) : b \in B\}| + \dots + |\{(a_n, b) : b \in B\}|.$$

Cada uno de los conjuntos  $\{(a_i, b) : b \in B\}$  tiene la misma cardinalidad que  $B$  (la cual es  $m$ ); por lo tanto,

$$|A \times B| = m + m + \dots + m = nm. \quad \blacksquare$$

No es difícil generalizar el teorema anterior: si  $A_1, A_2, \dots, A_r$  son conjuntos finitos, entonces

$$|A_1 \times A_2 \times \dots \times A_r| = |A_1| |A_2| \dots |A_r|.$$

El siguiente teorema calcula el número de funciones de  $A$  en  $B$ .

**Teorema 4.91.** Sean  $A$  y  $B$  conjuntos finitos. El número de funciones de  $A$  en  $B$  que existen es  $|B|^{|A|}$ .

**Demostración.** Sea  $A = \{a_1, \dots, a_n\}$ . Cualquier función  $f : A \rightarrow B$  está completamente determinada por las imágenes de cada uno de los elementos de  $A$ . En otras palabras,  $f$  está determinada por la  $n$ -tupla:

$$(f(a_1), f(a_2), \dots, f(a_n)) \in B \times B \times \dots \times B.$$

Cualquier  $n$ -tupla diferente determinará una función diferente. Por lo tanto, el número de funciones de  $A$  en  $B$  es igual a la cardinalidad del producto cartesiano,

$$|B \times B \times \dots \times B| = |B|^n, \text{ donde } n = |A|. \quad \blacksquare$$

El teorema anterior puede aplicarse a una situación en la que sea necesario elegir  $n$  elementos de un conjunto  $B$ , lo que permite la repetición de los elementos y considera el orden (o hace una distinción) en cada elección. El siguiente ejemplo ilustra esta situación.



**Ejemplo 4.92.** En una clase de 15 estudiantes, hay que elegir un comité de un presidente, un secretario y un tesorero. Supongamos que un mismo estudiante puede ocupar dos o más puestos distintos. ¿De cuántas maneras distintas se puede formar el comité?

Sea  $C$  el conjunto de estudiantes. Etiquetemos a cada estudiante con un número del 1 al 15. Si

$$P = (\text{presidente}), S = (\text{secretario}), T = (\text{tesorero}),$$

entonces el número de comités posibles es igual al número de funciones de  $\{P, S, T\}$  en  $C$ . Por ejemplo, una función  $f : \{P, S, T\} \rightarrow C$  definida como

$$f : \begin{cases} P \mapsto 4 \\ S \mapsto 8 \\ T \mapsto 4 \end{cases}$$

representa el comité donde el estudiante 4 es el presidente y el tesorero, mientras que el 8 es el secretario. Por el teorema 4.91, el número de funciones de este tipo es

$$|C|^3 = 15^3 = 3,375.$$

Luego, hay 3,375 maneras de formar el comité.

Ahora contaremos el número de funciones inyectivas de  $A$  en  $B$ .

**Teorema 4.93.** Sean  $A$  y  $B$  conjuntos finitos,  $|A| = n$  y  $|B| = m$ . El número de funciones inyectivas de  $A$  en  $B$  es:

- 1) 0, si  $n > m$ .
- 2)  $P(m, n) = m \cdot (m - 1) \cdot \dots \cdot (m - n + 1)$ , si  $n \leq m$ .

**Demostración.** La primera parte del teorema se conoce como el *principio del palomar* y se deja como ejercicio. Supongamos que  $n \leq m$  y sea  $A = \{a_1, a_2, \dots, a_n\}$ . Una función inyectiva  $f : A \rightarrow B$  puede verse como una  $n$ -tupla “inyectiva”:

$$(f(a_1), f(a_2), \dots, f(a_n)), \text{ donde } f(a_i) \neq f(a_j) \text{ para } i \neq j.$$

Demostraremos el teorema por inducción sobre  $n$ .

- 1) *Base de la inducción.* Es claro que hay  $m$  funciones inyectivas de  $\{a_1\}$  en  $B$ , una por cada elemento de  $B$ . Esto concuerda con que  $P(m, 1) = m$ .
- 2) *Hipótesis de la inducción.* Para un natural fijo  $k$ , supongamos que hay  $P(m, k)$  funciones inyectivas de  $A$  en  $B$ .

3) Tenemos que contar las  $(k + 1)$ -tuplas inyectivas de la forma

$$(f(a_1), f(a_2), \dots, f(a_k), f(a_{k+1})),$$

donde  $f(a_i) \neq f(a_j)$  para  $i \neq j$ . Fijemos  $f(a_{k+1}) = b \in B$ . Por hipótesis de inducción, el número de funciones inyectivas de  $A \setminus \{a_{k+1}\}$  en  $B \setminus \{b\}$  es  $P(m - 1, k)$ . Cada una de estas funciones se extiende a una función inyectiva de  $A$  en  $B$  definiendo  $f(a_{k+1}) = b$ . Si cambiamos  $f(a_{k+1}) = b' \in B$ ,  $b' \neq b$ , de nuevo por hipótesis sabemos que el número de funciones inyectivas de  $A \setminus \{a_{k+1}\}$  en  $B \setminus \{b'\}$  es  $P(m - 1, k)$ , cada una de las cuales se extiende a una función inyectiva de  $A$  en  $B$ . Podemos continuar este proceso  $m$  veces para cada uno de los elementos de  $B$ . Por lo tanto, obtenemos que el número total de funciones inyectivas de  $A$  en  $B$  es

$$P(m - 1, k) + \dots + P(m - 1, k) = m \cdot P(m - 1, k).$$

Ahora simplemente debemos observar que

$$m \cdot P(m - 1, k) = m \cdot (m - 1) \cdot \dots \cdot (m - (k + 1) + 1) = P(m, k + 1).$$

■

El resultado anterior se aplica en la siguiente situación. Supongamos que tenemos un conjunto  $B$  del cual queremos elegir  $n$  elementos sin repetirlos y considerando el orden (o haciendo una distinción) en cada elección. Este planteamiento es equivalente a contar el número de funciones inyectivas de  $\{1, \dots, n\}$  en  $B$ .

**Ejemplo 4.94.** En una clase de 15 estudiantes, hay que elegir un comité de un presidente, un secretario y un tesorero. En este caso, supongamos que no es posible que un mismo estudiante ocupe dos puestos distintos. ¿De cuántas maneras se puede formar el comité?

Con la notación del ejemplo 4.92, debemos contar las funciones inyectivas de  $\{P, S, T\}$  en  $C$ . Por el teorema 4.93, el número de funciones inyectivas de este tipo es

$$P(15, 3) = 15 \cdot 14 \cdot 13 = 2,730.$$

Por lo tanto, hay 2,730 formas distintas de formar el comité bajo las suposiciones previas.

El siguiente teorema nos dice cuál es la cardinalidad del conjunto potencia de un conjunto finito.

**Teorema 4.95.** Sea  $A$  un conjunto finito,  $|A| = n$ . Entonces la cardinalidad del conjunto potencia de  $A$  es

$$|P(A)| = 2^n.$$

**Demostración.** Recordemos que  $P(A)$  es el conjunto de todos los subconjuntos de  $A$ . Para cada  $S \in P(A)$ , podemos asociar una función  $\phi_S : A \rightarrow \{0, 1\}$  definida como

$$\phi_S(a) = \begin{cases} 1, & \text{si } a \in S \\ 0, & \text{si } a \notin S. \end{cases}$$

Cada una de estas funciones determina un subconjunto de  $A$  distinto; es decir, si  $\phi_S = \phi_T$ ,  $S, T \in P(A)$ , entonces

$$S = \phi_S^{-1}(1) = \phi_T^{-1}(1) = T.$$

Esto demuestra que el número de subconjuntos de  $A$  es igual al número de funciones de  $A$  en  $\{0, 1\}$ . Por el teorema 4.91, este número es

$$|\{0, 1\}|^{|A|} = 2^{|A|}.$$

■

**Ejemplo 4.96.** Si  $A = \{a, b, c\}$ , de acuerdo con el teorema 4.95,

$$|P(A)| = 2^3 = 8.$$

Comprobamos esto obteniendo directamente el conjunto potencia:

$$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}.$$

Las funciones biyectivas sobre  $A$  reciben un nombre especial.

**Definición 4.97 (permutación).** Sea  $A$  un conjunto finito. Una permutación de  $A$  es una biyección  $\alpha : A \rightarrow A$ .

Denotamos como  $\text{Sym}(A)$  al conjunto de las permutaciones de  $A$ .

**Teorema 4.98.** Sea  $A$  un conjunto finito,  $|A| = n$ . El número de permutaciones de  $A$  que existen es

$$|\text{Sym}(A)| = n! = n \cdot (n - 1) \cdot \dots \cdot 2 \cdot 1.$$

**Demostración.** Este teorema es un resultado directo del teorema 4.93, ya que cualquier función inyectiva sobre  $A$  es de hecho biyectiva (ejercicio 4.104) y  $P(n, n) = n!$ . ■

Permutación	Tríada corresp.	Permutación	Tríada corresp.
$\beta_1 : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases}$	(1, 2, 3)	$\beta_4 : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases}$	(1, 3, 2)
$\beta_2 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases}$	(2, 1, 3)	$\beta_5 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$	(2, 3, 1)
$\beta_3 : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases}$	(3, 2, 1)	$\beta_6 : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases}$	(3, 1, 2)

Tabla 4.1: Permutaciones de  $\{1, 2, 3\}$ 

Veamos ahora algunos ejemplos.

**Ejemplo 4.99.** Consideremos el conjunto  $A = \{1, 2, 3\}$ . Una permutación de  $A$  es la función biyectiva

$$\beta_5 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1, \end{cases}$$

la cual se corresponde con la tríada (o 3-tupla)

$$(\beta(1), \beta(2), \beta(3)) = (2, 3, 1).$$

Por el teorema 4.98, hay  $3! = 6$  permutaciones de  $A$ . Todas estas permutaciones aparecen en la tabla 4.1.

Como pudimos observar en el ejemplo anterior, una permutación de un conjunto finito puede verse como un “arreglo” de los elementos del conjunto, en el cual no se permiten repeticiones e importa el orden en el que aparecen los elementos.

Si  $A$  es cualquier conjunto, un  $k$ -subconjunto de  $A$  es un subconjunto de  $A$  de cardinalidad  $k$ .

**Teorema 4.100.** Sea  $A$  un conjunto finito,  $|A| = n$ . Si  $k \in \mathbb{N}$ ,  $k \leq n$ , entonces el número de  $k$ -subconjuntos de  $A$  es

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

**Demostración.** El teorema 4.93 implica que el número de  $k$ -tuplas inyectivas formadas por distintos elementos de  $A$  es  $P(n, k)$ . Sin embargo, estas  $k$ -tuplas no representan  $k$ -subconjuntos porque en un  $k$ -subconjunto no importa el orden en el que aparecen los elementos.

Digamos que dos  $k$ -tuplas

$$(a_1, \dots, a_k) \text{ y } (b_1, \dots, b_k)$$

son equivalentes si existe una permutación  $\beta : A \rightarrow A$  tal que  $\beta(a_i) = b_i$  para toda  $i$ . Esto define una relación de equivalencia (ejercicio 4.105). Por el teorema 4.98, la cardinalidad de cada clase de equivalencia es  $k!$ . Como las clases de equivalencia forman una partición de las  $k$ -tuplas, deducimos que hay

$$\frac{P(n, k)}{k!}$$

clases de equivalencia distintas. El teorema queda demostrado observando que cada clase de equivalencia corresponde a un  $k$ -subconjunto distinto de  $A$ , y que

$$\frac{P(n, k)}{k!} = \frac{P(n, k)(n - k)!}{k!(n - k)!} = \frac{n!}{k!(n - k)!}.$$

■

La expresión  $\binom{n}{k}$  del teorema anterior se llama *coeficiente binomial*, ya que también determina el  $k$ -ésimo coeficiente del binomio  $(x + y)^n$ .

**Ejemplo 4.101.** En una clase de 15 estudiantes hay que elegir un comité formado por tres representantes. ¿Cuántos comités diferentes se pueden formar?

Como no hay distinción alguna entre los representantes que forman el comité, la pregunta anterior es equivalente a encontrar el número de subconjuntos de cardinalidad 3 del conjunto de 15 estudiantes. Por el teorema 4.100, el número de estos subconjuntos es

$$\binom{15}{3} = \frac{15!}{3!(15 - 3)!} = 455.$$

**Palabras clave de la sección:** principio fundamental de conteo, número de funciones inyectivas, cardinalidad del conjunto potencia, permutación,  $k$ -subconjunto, coeficiente binomial.

### 4.5.1 Ejercicios de conteo

**Ejercicio 4.102.** Demuestra que si  $A_1, A_2, \dots, A_r$  son conjuntos finitos, entonces

$$|A_1 \times A_2 \times \dots \times A_r| = |A_1| |A_2| \dots |A_r|.$$

(sugerencia: usa inducción sobre  $r$  y el teorema 4.90).

**Ejercicio 4.103.** *Principio del palomar:* demuestra que no hay funciones inyectivas de  $A$  en  $B$  si  $|A| > |B|$ .

**Ejercicio 4.104.** Sea  $A$  un conjunto finito. Explica por qué cualquier función inyectiva sobre  $A$  es también sobreyectiva.

**Ejercicio 4.105.** Comprueba que la relación definida en la demostración del teorema 4.100 sobre las  $k$ -tuplas es una relación de equivalencia.

**Ejercicio 4.106.** Sea  $A$  un conjunto de cardinalidad 8. Encuentra lo siguiente y justifica tu respuesta:

- a) La cardinalidad del conjunto potencia  $P(A)$ .
- b) El número de permutaciones de  $A$ .
- c) El número de 5-subconjuntos de  $A$ .
- d) La cardinalidad del producto cartesiano  $A \times A$ .
- e) El número de relaciones sobre  $A$  (recuerda que una relación sobre  $A$  es un subconjunto de  $A \times A$ .)
- f) El número de subconjuntos  $X$  de  $A$  tales que  $|X| \leq 3$ .

**Ejercicio 4.107.** Con las letras de la palabra *LIBRO*, ¿cuántos arreglos de letras distintos se pueden hacer?

**Ejercicio 4.108.** Un profesor quiere repartir 4 libros entre 10 estudiantes de una clase. Determina el número de formas diferentes en las que se pueden repartir si:

- a) Los cuatro libros son distintos, y los estudiantes pueden recibir más de un libro.
- b) Los cuatro libros son distintos, y los estudiantes no pueden recibir más de un libro.
- c) Los cuatro libros son iguales, y los estudiantes no pueden recibir más de un libro.

## 4.6 Definiciones del capítulo

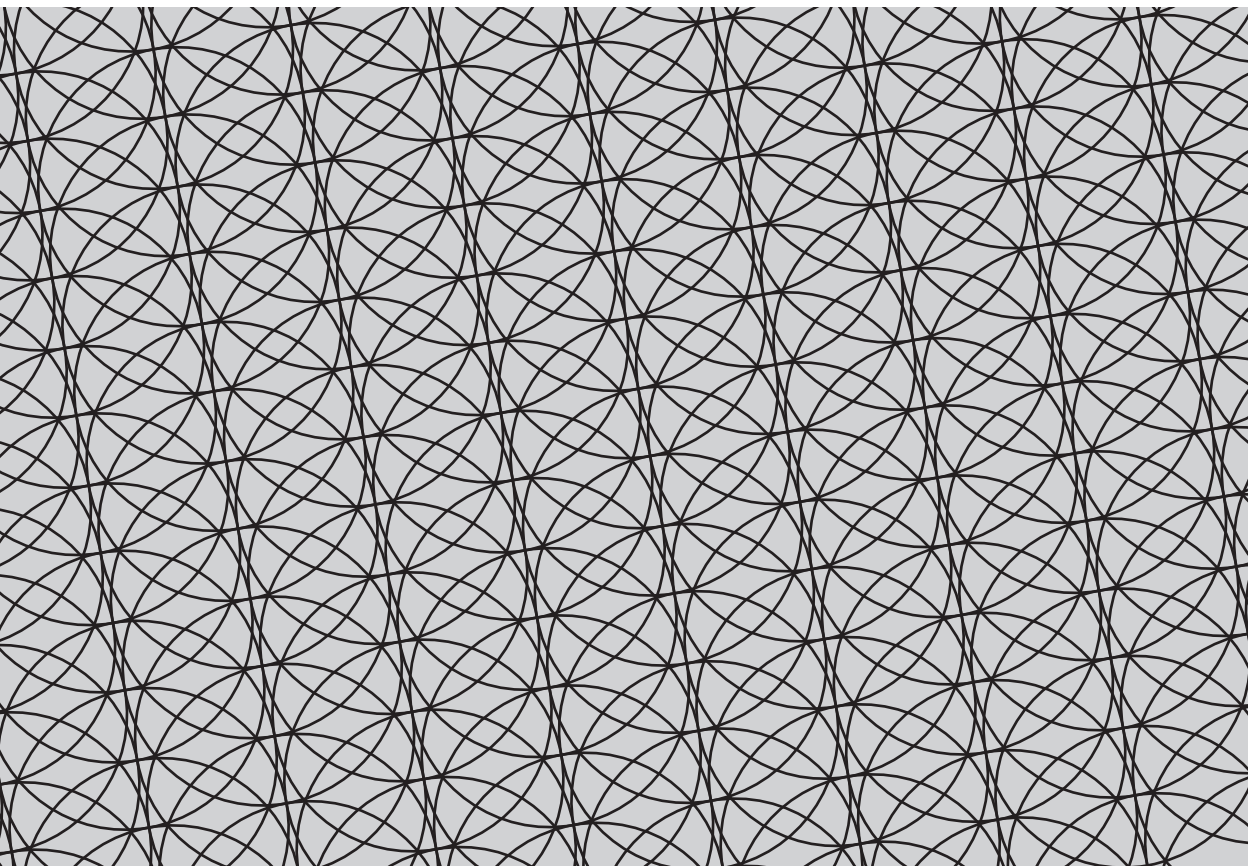
Escribe la definición y un ejemplo de cada uno de los conceptos enlistados a continuación.

- 1) Números naturales.
- 2) Números enteros.
- 3) Divisor.
- 4) Número primo.
- 5) Número compuesto.
- 6) Máximo común divisor.
- 7) Primos relativos.
- 8) Ecuación diofántica.
- 9) Congruencia módulo  $n$ .
- 10) Igualdad de cardinalidades.
- 11) Cardinalidad menor o igual que.
- 12) Conjunto finito.
- 13) Conjunto numerable.
- 14) Permutación.
- 15)  $k$ -subconjunto.
- 16) Coeficiente binomial.

*Las estructuras son las armas del matemático.*

Nicolás Bourbaki, grupo de matemáticos franceses

## Capítulo 5. Estructuras algebraicas





Los objetos principales de estudio del álgebra universitaria son las *estructuras algebraicas*. Dicho brevemente, una estructura algebraica involucra uno o más conjuntos junto con una o más *operaciones* que satisfacen ciertas propiedades. Estas operaciones pueden variar considerablemente, dependiendo de los conjuntos sobre las que estén definidas. Algunos ejemplos comunes son la suma y la multiplicación usual de números, la multiplicación de matrices y la composición de funciones.

Cada estructura algebraica recibe un nombre especial, dependiendo del número de conjuntos y operaciones involucradas y de las propiedades que éstas satisfagan; así pues, pueden ser llamadas grupos, campos, espacios vectoriales o anillos, entre muchas otras. En las siguientes secciones definiremos algunas de estas estructuras y examinamos algunos ejemplos elementales.

## 5.1 Grupos

Antes de definir formalmente lo que es un grupo, presentamos el concepto de *operación binaria*.

**Definición 5.1 (operación binaria).** Sea  $G$  un conjunto no vacío. Una *operación binaria* de  $G$  es una función de la forma  $f : G \times G \rightarrow G$ .

**Ejemplo 5.2.** Si  $G = \mathbb{Z}$ , la función  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  definida como

$$f(n, m) = n + m \in \mathbb{Z}, \text{ donde } n, m \in \mathbb{Z},$$

es una operación binaria llamada *suma usual* de  $\mathbb{Z}$ .

En general, para verificar que  $f$  es una operación binaria bien definida en  $G$  hay que asegurarse de que realmente  $f(a, b) \in G$  para cualquier par  $(a, b) \in G \times G$ . Comúnmente llamamos a esto propiedad de *cerradura* de la operación.

**Ejemplo 5.3.** Consideremos el conjunto de números racionales distintos de cero, denotado como  $\mathbb{Q}^*$ :

$$\mathbb{Q}^* = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, a \neq 0, b \neq 0 \right\}.$$

La función

$$f\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}\right) = \frac{a_1 a_2}{b_1 b_2}, \text{ donde } \frac{a_i}{b_i} \in \mathbb{Q}^*,$$

es una operación binaria de  $\mathbb{Q}$ . Para comprobar la cerradura, notemos que si  $a_i \neq 0$  y  $b_i \neq 0$ , entonces  $a_1 a_2 \neq 0$  y  $b_1 b_2 \neq 0$ , y por lo tanto

$$\frac{a_1 a_2}{b_1 b_2} \in \mathbb{Q}^*.$$

Esta operación es llamada *multiplicación usual* de números racionales.

**Ejemplo 5.4.** Consideremos el conjunto

$$\mathbb{I} = \{2n + 1 : n \in \mathbb{Z}\}.$$

La función

$$f(a, b) = a + b, \text{ donde } a, b \in \mathbb{I},$$

no es una operación binaria de  $\mathbb{I}$  porque no se cumple la cerradura: la suma de dos enteros impares no es un entero impar.

En el ejemplo anterior, ¿qué ocurre si consideramos al conjunto de enteros pares en lugar del conjunto de enteros impares? ¿Es la suma en este caso una operación binaria? (ejercicio 5.25).

Cuando los elementos de  $G$  son clases de equivalencia imponemos la condición de que una operación binaria  $f$  de  $G$  debe ser independiente de los representantes que se elijan en cada clase; más precisamente,  $f$  debe cumplir que si  $[a] = [a']$  y  $[b] = [b']$ , entonces  $f([a], [b]) = f([a'], [b'])$ . El siguiente ejemplo ilustra esta situación.

**Ejemplo 5.5.** Sea  $n \in \mathbb{N}$ ,  $n \neq 0$ . Consideremos el conjunto cociente de la relación módulo  $n$ :

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}.$$

La función

$$f([m], [k]) = [m + k] \in \mathbb{Z}_n, \text{ donde } [m], [k] \in \mathbb{Z}_n,$$

es una operación binaria de  $\mathbb{Z}_n$ . Claramente,  $f$  cumple la cerradura, pero en este caso también es necesario verificar que  $f$  es independiente de los representantes de clase. Esto queda establecido por el teorema 4.48, el cual demuestra que si  $[m] = [m']$  y  $[k] = [k']$ , entonces  $[m + k] = [m' + k']$ .

**Notación 5.6.** En general, escribimos un punto  $\cdot$  para denotar una operación binaria cualquiera. Además, es costumbre escribir la imagen del par  $(a, b) \in G \times G$  como  $a \cdot b$ .

Un *grupo* es una estructura algebraica que consiste en un conjunto y una operación binaria que cumple tres propiedades. El concepto surgió por primera vez en el siglo XIX en las investigaciones del matemático francés Évariste Galois. A pesar de haber sido asesinado en un duelo a la corta edad de 20 años, Galois desarrolló una de las teorías matemáticas más brillantes de la historia.

**Definición 5.7 (grupo).** Sea  $G$  un conjunto no vacío y  $\cdot$  una operación binaria de  $G$ . El par  $(G, \cdot)$  es un *grupo* si se cumplen las siguientes propiedades:

G1 *Asociatividad.* Para toda  $a, b, c \in G$ , se cumple que

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

G2 *Identidad.* Existe un elemento  $e \in G$  tal que  $e \cdot a = a \cdot e = a$  para toda  $a \in G$ .

G3 *Inversos.* Para cualquier  $a \in G$ , existe un elemento  $b \in G$  tal que  $a \cdot b = b \cdot a = e$ .

El elemento  $e \in G$  de la propiedad G2 es llamado *identidad* de  $G$ . El elemento  $b \in G$  de la propiedad G3, que cumple que  $a \cdot b = b \cdot a = e$ , es llamado *inverso de  $a$*  y es denotado como  $a^{-1}$ . Más adelante demostramos que estos elementos son únicos.

**Ejemplo 5.8.** Sea  $+$  la suma usual de  $\mathbb{Z}$ . El par  $(\mathbb{Z}, +)$  es un grupo:

G1 Para toda  $n, m, k \in \mathbb{Z}$ , se cumple que  $(n + m) + k = n + (m + k)$ .

G2 La identidad es  $0 \in \mathbb{Z}$  porque  $0 + n = n + 0 = n$ , para toda  $n \in \mathbb{Z}$ .

G3 El inverso de cualquier  $n \in \mathbb{Z}$  es  $-n \in \mathbb{Z}$  porque  $n + (-n) = (-n) + n = 0$ .

**Ejemplo 5.9.** Consideremos un conjunto con sólo un elemento  $\{e\}$  y una operación binaria  $\cdot$  definida como  $e \cdot e = e$ . El par  $(\{e\}, \cdot)$  es un grupo: las propiedades G1-G3 se cumplen obviamente. Llamamos a  $(\{e\}, \cdot)$  *grupo trivial*.

**Ejemplo 5.10.** Sea  $\cdot$  la multiplicación usual de  $\mathbb{Q}^*$ . El par  $(\mathbb{Q}^*, \cdot)$  es un grupo:

G1 Sabemos que la multiplicación de números enteros es asociativa. Por lo tanto:

$$\begin{aligned} \frac{a_1}{b_1} \cdot \left( \frac{a_2}{b_2} \cdot \frac{a_3}{b_3} \right) &= \frac{a_1(a_2a_3)}{b_1(b_2b_3)} \\ &= \frac{(a_1a_2)a_3}{(b_1b_2)b_3} \\ &= \left( \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \right) \cdot \frac{a_3}{b_3}, \end{aligned}$$

para cualquier  $\frac{a_i}{b_i} \in \mathbb{Q}^*$ .

G2 La identidad es  $\frac{1}{1} \in \mathbb{Q}^*$  porque  $\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b} \cdot \frac{1}{1} = \frac{a}{b}$ , para toda  $\frac{a}{b} \in \mathbb{Q}^*$ .

G3 El inverso de cualquier  $\frac{a}{b} \in \mathbb{Q}^*$  es  $\frac{b}{a} \in \mathbb{Q}^*$  porque  $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1}$ .

**Ejemplo 5.11.** Consideremos un triángulo con vértices

$$V = \{v_1, v_2, v_3\}.$$

Sea  $\text{Sym}(V)$  el conjunto de permutaciones de  $V$  (funciones biyectivas sobre  $V$ ). A estas permutaciones también se les llama *simetrías* del triángulo. Por ejemplo, la permutación

$$\rho : \begin{cases} v_1 \mapsto v_2 \\ v_2 \mapsto v_3 \\ v_3 \mapsto v_1 \end{cases}$$

puede verse como una rotación de 120 grados (figura 5.1).

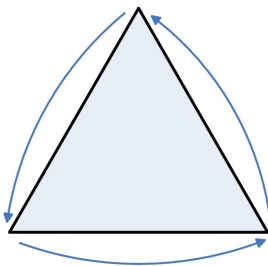


Figura 5.1: Rotación de 120 grados.

De manera similar, la permutación

$$\sigma : \begin{cases} v_1 \mapsto v_1 \\ v_2 \mapsto v_3 \\ v_3 \mapsto v_2 \end{cases}$$

puede verse como una reflexión del triángulo a través del eje que pasa por  $v_1$  (figura 5.2).

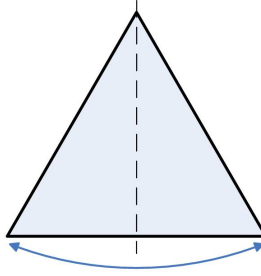


Figura 5.2: Reflexión del triángulo.

Por el ejercicio 5.29, la composición de funciones  $\circ$  es una operación binaria de  $\text{Sym}(V)$ . Además, el par  $(\text{Sym}(D), \circ)$  es un grupo:

G1 La asociatividad de  $\circ$  se deduce directamente de la definición 3.34.

G2 La permutación

$$id : \begin{cases} v_1 \mapsto v_1 \\ v_2 \mapsto v_2 \\ v_3 \mapsto v_3 \end{cases}$$

es la identidad porque  $id \circ \phi = \phi \circ id = \phi$ , para toda  $\phi \in \text{Sym}(V)$ .

G3 Debido a que los elementos de  $\text{Sym}(V)$  son funciones biyectivas, cualquier elemento tiene un inverso.

**Ejemplo 5.12.** Sea  $+$  la operación binaria de  $\mathbb{Z}_n$  del ejemplo 5.5. Entonces, el par  $(\mathbb{Z}_n, +)$  es un grupo (ejercicio 5.25).

Ahora demostramos algunos resultados básicos.

**Lema 5.13 (cancelación derecha).** Sea  $(G, \cdot)$  un grupo y  $a, b, c \in G$ . Si  $a \cdot c = b \cdot c$ , entonces  $a = b$ .

**Demostración.** Usando las propiedades de la definición de grupo,

$$\begin{aligned}
 a \cdot c = b \cdot c &\implies (a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1}, \\
 &\implies a \cdot (c \cdot c^{-1}) = b \cdot (c \cdot c^{-1}), & (G1) \\
 &\implies a \cdot e = b \cdot e, & (G3) \\
 &\implies a = b. & (G2)
 \end{aligned}$$

■

También es posible demostrar la cancelación izquierda (ejercicio 5.26).

**Teorema 5.14 (unicidad de los inversos).** Sea  $(G, \cdot)$  un grupo. El inverso de cualquier elemento de  $G$  es único.

**Demostración.** Sea  $a \in G$  y supongamos que  $b, d \in G$  cumplen que  $a \cdot b = b \cdot a = e$  y  $a \cdot d = d \cdot a = e$ . Demostramos que  $b = d$ :

$$\begin{aligned}
 b &= b \cdot e & (G2) \\
 &= b \cdot (a \cdot d) & (\text{hipótesis}) \\
 &= (b \cdot a) \cdot d & (G1) \\
 &= e \cdot d & (\text{hipótesis}) \\
 &= d. & (G2)
 \end{aligned}$$

■

También es posible demostrar que la identidad de cualquier grupo es única (ejercicio 5.26).

Un grupo  $(G, \cdot)$  es *finito* si  $G$  es un conjunto finito. Cuando  $|G| = m$ , podemos escribir una tabla, llamada *tabla de Cayley* de  $(G, \cdot)$ , con  $m$  filas y  $m$  columnas, que determina completamente el comportamiento de la operación del grupo. Para esto ordenamos de manera arbitraria los elementos del grupo,  $G = \{g_1, g_2, \dots, g_m\}$ , y escribimos  $g_i \cdot g_j$  en la entrada  $(i, j)$  de la tabla.

**Ejemplo 5.15.** Consideremos el grupo  $(\mathbb{Z}_5, +)$ , donde

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}.$$

En este caso, la tabla de Cayley es la siguiente:

La famosa frase “el orden de los factores no altera el producto” sólo es verdadera en grupos *abelianos*.

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

 Tabla 5.1: Tabla de Cayley de  $(\mathbb{Z}_5, +)$ 

**Definición 5.16 (grupo abeliano).** Decimos que un grupo  $(G, \cdot)$  es *abeliano* si se cumple la siguiente propiedad:

G4 *Conmutatividad.* Para toda  $a, b \in G$ , tenemos que  $a \cdot b = b \cdot a$ .

El término “abeliano” hace referencia al matemático noruego de principios del siglo XIX, Neils Henrik Abel.

**Ejemplo 5.17.** Los grupos  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}^*, \cdot)$  y  $(\mathbb{Z}_n, +)$  son abelianos.

**Ejemplo 5.18.** El grupo  $(\text{Sym}(V), \circ)$  de simetrías del triángulo no es abeliano. Para observar esto, sean  $\rho$  y  $\sigma$  las simetrías del ejemplo 5.11. Entonces,

$$\rho \circ \sigma : \begin{cases} v_1 \mapsto v_2 \\ v_2 \mapsto v_1 \\ v_3 \mapsto v_3 \end{cases}$$

mientras que,

$$\sigma \circ \rho = \begin{cases} v_1 \mapsto v_3 \\ v_2 \mapsto v_2 \\ v_3 \mapsto v_1 \end{cases}$$

Por lo tanto,  $\rho \circ \sigma \neq \sigma \circ \rho$ .

Si  $(G, \cdot)$  es un grupo y  $H$  un subconjunto de  $G$ , denotemos por  $\cdot_H$  la restricción de  $\cdot$  en  $H$ ; en otras palabras,  $\cdot_H$  es la función  $\cdot_H : H \times H \rightarrow G$  definida como

$$a \cdot_H b = a \cdot b, \text{ donde } a, b \in H.$$

**Definición 5.19 (subgrupo).** Sea  $(G, \cdot)$  un grupo y  $H \subseteq G$ . Decimos que  $(H, \cdot_H)$  es un *subgrupo* de  $(G, \cdot)$  si  $(H, \cdot_H)$  es en sí mismo un grupo.

Decimos que  $(H, \cdot_H)$  es un subgrupo propio de  $(G, \cdot)$  si  $H \subsetneq G$ .

**Ejemplo 5.20.** El grupo trivial  $(\{e\}, \cdot)$  es un subgrupo de cualquier grupo  $(G, \cdot)$ .

**Teorema 5.21 (test del subgrupo).** Sea  $(G, \cdot)$  un grupo y  $H \subseteq G$ . El par  $(H, \cdot_H)$  es un subgrupo de  $(G, \cdot)$  si y sólo si se cumplen las siguientes propiedades:

- S1 Se cumple la cerradura en  $H$ ; es decir,  $a \cdot b \in H$  para toda  $a, b \in H$ .
- S2 La identidad del grupo  $(G, \cdot)$  está contenida en  $H$ .
- S3 Para cualquier  $a \in H$ , tenemos que  $a^{-1} \in H$ .

**Demostración.**

( $\Rightarrow$ ) Si  $(H, \cdot_H)$  es un subgrupo, claramente se cumplen las propiedades **S1-S3**.

( $\Leftarrow$ ) Supongamos que el par  $(H, \cdot_H)$  cumple las propiedades **S1-S3**. La propiedad **S1** garantiza que  $\cdot_H$  es una función de la forma  $H \times H \rightarrow H$ , así que es una operación binaria de  $H$ . Las propiedades **S2** y **S3** implican directamente que **G2** y **G3** se cumplen. Finalmente,  $(H, \cdot_H)$  también cumple **G1** porque, para cualquier  $a, b, c \in H$ ,

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

Por lo tanto,  $(H, \cdot_H)$  es un grupo en sí mismo. ■

Para simplificar notación, si  $(H, \cdot_H)$  es un subgrupo de  $(G, \cdot)$ , denotamos la operación  $\cdot_H$  con el mismo símbolo que la operación de  $(G, \cdot)$ .

**Ejemplo 5.22.** Sea  $n \in \mathbb{N}$ ,  $n \neq 0$ . Consideremos al conjunto de los múltiplos enteros de  $n$ :

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}.$$

Claramente,  $n\mathbb{Z}$  es un subconjunto de  $\mathbb{Z}$  (un subconjunto propio si  $n \neq 1$ ). Además,  $(n\mathbb{Z}, +)$  es un subgrupo de  $(\mathbb{Z}, +)$ :

- S1 Sean  $a, b \in n\mathbb{Z}$ . Entonces  $a = nk_1$  y  $b = nk_2$ , para algunos  $k_1, k_2 \in \mathbb{Z}$ . Por lo tanto,

$$a + b = nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}.$$

- S2 El conjunto  $n\mathbb{Z}$  contiene a 0 porque  $0 = n0$ .



S3 Si  $a \in n\mathbb{Z}$ , entonces  $a = nk$ , para algún  $k \in \mathbb{Z}$ , así que  $-a = n(-k) \in n\mathbb{Z}$ .

Hay un método sencillo para encontrar un subgrupo de un grupo finito  $(G, \cdot)$ . Primero, tomamos cualquier elemento  $g \in G$  distinto de la identidad, y lo operamos consigo mismo:

$$(g \cdot g), (g \cdot g \cdot g), (g \cdot g \cdot g \cdot g), \dots$$

El proceso termina cuando encontramos que

$$(g \cdot g \cdot \dots \cdot g) = e.$$

Esto siempre sucede dado que  $G$  es un conjunto finito. Para simplificar notación, escribimos  $g^i = (g \cdot \dots \cdot g)$ , donde  $g$  está operado consigo mismo  $i$  veces, y  $g^0 = e$ . Sea  $n \in \mathbb{N}$  el entero positivo más pequeño tal que  $g^n = e$ , y definamos

$$\langle g \rangle = \{e, g, g^2, g^3, \dots, g^{n-1}\}.$$

Veremos que  $(\langle g \rangle, \cdot)$  es un subgrupo de  $(G, \cdot)$ , llamado *grupo cíclico generado por  $g$* .

**Teorema 5.23 (subgrupo cíclico).** Con la notación de arriba,  $(\langle g \rangle, \cdot)$  es un subgrupo de  $(G, \cdot)$ .

**Demostración.** Usaremos el test del subgrupo (teorema 5.21).

S1 Sean  $g^k, g^s \in \langle g \rangle$ ,  $1 \leq k, s < n$ . Observemos que

$$g^k \cdot g^s = (g \cdot \dots \cdot g) \cdot (g \cdot \dots \cdot g) = g^{k+s}.$$

Si  $(k + s) < n$ , es claro que  $g^{k+s} \in \langle g \rangle$ . Por otro lado, si  $(k + r) > n$ , usamos el algoritmo de la división para encontrar enteros  $q, r \in \mathbb{Z}$  tales que

$$(k + s) = qn + r, \text{ donde } 0 \leq r < n.$$

Por lo tanto,

$$\begin{aligned} g^{k+s} &= g^{qn+r} \\ &= g^n \cdot g^n \cdot \dots \cdot g^n \cdot g^r \\ &= e \cdot e \cdot \dots \cdot e \cdot g^r \\ &= g^r \in \langle g \rangle. \end{aligned}$$

S2 Por definición,  $e = g^0 \in \langle g \rangle$ .

S3 Ejercicio 5.27.



**Ejemplo 5.24.** Consideremos la clase  $[2]$  en el grupo  $(\mathbb{Z}_6, +)$ . Observemos que

$$\begin{aligned}[2] + [2] &= [4], \\ [2] + [2] + [2] &= [0].\end{aligned}$$

Por lo tanto,

$$(\{[0], [2], [4]\}, +)$$

es un subgrupo de  $(\mathbb{Z}_6, +)$ . Consideremos ahora  $[3]$  en  $(\mathbb{Z}_6, +)$  y veamos que  $[3] + [3] = [0]$ . Por lo tanto,

$$(\{[0], [3]\}, +),$$

es un subgrupo de  $(\mathbb{Z}_6, +)$ .

**Palabras clave de la sección:** *operación binaria, grupo, identidad, inverso, grupo abeliano, subgrupo, subgrupo cíclico.*

### 5.1.1 Ejercicios de grupos

**Ejercicio 5.25.** ¿Cuáles de los siguientes pares son grupos? Si el par es un grupo, demuestra que se cumple la cerradura y **G1-G3**. En caso contrario, determina qué propiedad es la que no se cumple.

- a)  $(\mathbb{Z}_n, +)$ , donde  $+$  es la suma de clases de equivalencia.
- b)  $(2\mathbb{Z}, +)$ , donde  $+$  es la suma usual de números.
- c)  $(\mathbb{N}, +)$ , donde  $+$  es la suma usual de números.
- d)  $(\mathbb{Q}, \cdot)$ , donde  $\cdot$  es la multiplicación usual de fracciones.

**Ejercicio 5.26.** Sea  $(G, \cdot)$  un grupo. Demuestra lo siguiente:

- a) Sean  $a, b, c \in G$ . Si  $c \cdot a = c \cdot b$ , entonces  $a = b$ .
- b) La identidad de  $(G, \cdot)$  es única.

**Ejercicio 5.27.** Sea  $(G, \cdot)$  un grupo,  $g \in G$ ,  $g \neq e$ . Si

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

es el conjunto definido en esta sección, con  $g^n = e$ , demuestra que  $(\langle g \rangle, \cdot)$  cumple la propiedad **S3** del teorema 5.21.

**Ejercicio 5.28.** Encuentra todos los subgrupos cíclicos de  $\mathbb{Z}_3$ ,  $\mathbb{Z}_4$ ,  $\mathbb{Z}_5$  y  $\mathbb{Z}_8$ . ¿Puedes encontrar subgrupos cíclicos propios no triviales en  $\mathbb{Z}_3$  o  $\mathbb{Z}_5$ ? ¿A qué crees que se deba esto?

**Ejercicio 5.29.** Sea  $(\text{Sym}(V), \circ)$  el grupo de simetrías del triángulo con vértices  $V = \{v_1, v_2, v_3\}$ .

- a) Explica por qué la composición de funciones  $\circ$  es una operación binaria de  $\text{Sym}(V)$ .
- b) ¿Cuántos elementos hay en  $\text{Sym}(V)$ ? Escríbelos todos usando la notación del ejemplo 5.11.
- c) Encuentra la tabla de Cayley de  $(\text{Sym}(V), \circ)$ .
- d) Encuentra dos subgrupos propios no triviales de  $(\text{Sym}(V), \circ)$ .

**Ejercicio 5.30.** Sea  $V = \{v_1, v_2, v_3, v_4\}$ .

- a) Demuestra que  $(\text{Sym}(V), \circ)$  es un grupo, donde  $\circ$  es la composición de funciones.
- b) ¿Cuántos elementos hay en  $\text{Sym}(V)$ ? Escríbelos todos con la notación usada en el ejemplo 5.11.
- c) Encuentra la tabla de Cayley de  $(\text{Sym}(V), \circ)$

## 5.2 Campos

En esta sección definimos una nueva estructura algebraica que involucra dos operaciones binarias.

**Definición 5.31 (campo).** Sea  $F$  un conjunto no vacío. Sean  $+$  y  $\cdot$  dos operaciones binarias de  $F$ . La tríada  $(F, +, \cdot)$  es un *campo* si se cumplen las siguientes propiedades:

- C1  $(F, +)$  es un grupo abeliano con identidad  $e_0$ .
- C2 Sea  $F^* = F \setminus \{e_0\}$ . El par  $(F^*, \cdot)$  es un grupo abeliano con identidad  $e_1 \neq e_0$ .
- C3 *Distributividad*. Para toda  $a, b, c \in F$ ,  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ .

Las operaciones  $+$  y  $\cdot$  en un campo son llamadas “suma” y “multiplicación”, respectivamente. Esto no significa que  $+$  y  $\cdot$  sean la suma y multiplicación usual de números; de hecho, el conjunto  $F$  podría no contener números. Al elemento  $e_0$  se le llama *identidad aditiva* del campo, mientras que a  $e_1$  se le llama *identidad multiplicativa*.

Si  $(F, +, \cdot)$  es un campo, es costumbre denotar como  $-a$  al inverso aditivo de  $a \in F$ , y como  $\frac{1}{a}$  al inverso multiplicativo de  $a$ , siempre y cuando  $a \neq e_0$ . Para simplificar notación, si  $a, b \in F$ , escribimos  $a - b$  en lugar de  $a + (-b)$ . Como ambas operaciones  $+$  y  $\cdot$  forman grupos abelianos, es claro que  $a + b = b + a$  y que  $a \cdot b = b \cdot a$  para toda  $a, b \in F$ .

De hecho, podemos decir que una tríada  $(F, +, \cdot)$  es un campo si las operaciones binarias  $+$  y  $\cdot$  cumplen todas las propiedades básicas de la aritmética.

**Proposición 5.32.** Sea  $(F, +, \cdot)$  un campo. Para cualquier  $a \in F$ , tenemos que  $e_0 \cdot a = e_0$ .

**Demostración.** Usando las propiedades de la definición,

$$(e_0 \cdot a) + e_0 = e_0 \cdot a \quad (\text{C1})$$

$$= (e_0 + e_0) \cdot a \quad (\text{C1})$$

$$= (e_0 \cdot a) + (e_0 \cdot a). \quad (\text{C3})$$

Por lo tanto,  $e_0 = e_0 \cdot a$  por cancelación izquierda en el grupo  $(F, +)$ . ■

Usando la proposición anterior es posible deducir que la identidad aditiva  $e_0 \in F$  no tiene inverso multiplicativo: es decir, que no está permitido dividir entre cero en un campo (ejercicio 5.43).

**Proposición 5.33.** Sea  $(F, +, \cdot)$  un campo. Para toda  $a, b \in F$ , tenemos que

$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b).$$

**Demostración.** El elemento  $-(a \cdot b)$  es, por definición, el inverso aditivo del producto  $a \cdot b \in F$ . Observemos que

$$\begin{aligned} (a \cdot b) + ((-a) \cdot b) &= (a + (-a)) \cdot b & (C3) \\ &= e_0 \cdot b & (C1) \\ &= e_0. & (\text{proposición 5.32}) \end{aligned}$$

Por lo tanto,  $(-a) \cdot b$  también es el inverso aditivo de  $a \cdot b$ , así que  $(-a) \cdot b = -(a \cdot b)$  por la unicidad de los inversos en  $(F, +)$ . De forma similar, podemos demostrar que  $a \cdot (-b) = -(a \cdot b)$ . ■

**Ejemplo 5.34.** El campo más pequeño que existe es  $(\mathbb{Z}_2, +, \cdot)$  donde  $\mathbb{Z}_2 = \{[0], [1]\}$ . La identidad aditiva es  $e_0 = [0]$  y la identidad multiplicativa es  $e_1 = [1]$ . En este caso, el grupo  $(\mathbb{Z}_2^*, \cdot)$  es el grupo trivial, donde  $[1] \cdot [1] = [1]$ .

**Ejemplo 5.35.** El conjunto de los números racionales

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\},$$

junto con la suma usual de fracciones, definida como

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2},$$

y multiplicación usual de fracciones, es un campo:

C1 Ejercicio 5.44.

C2 Por el ejemplo 5.10,  $(\mathbb{Q}^*, \cdot)$  es un grupo abeliano con identidad multiplicativa  $e_1 = \frac{1}{1}$ .

C3 Para cualquier  $\frac{a_i}{b_i} \in \mathbb{Q}$ , tenemos que

$$\begin{aligned} \frac{a_1}{b_1} \cdot \left( \frac{a_2}{b_2} + \frac{a_3}{b_3} \right) &= \frac{a_1}{b_1} \cdot \left( \frac{a_2 b_3 + a_3 b_2}{b_2 b_3} \right) \\ &= \frac{a_1 (a_2 b_3 + a_3 b_2)}{b_1 (b_2 b_3)} \\ &= \frac{a_1 a_2 b_3 + a_1 a_3 b_2}{b_1 b_2 b_3}. \end{aligned}$$

Por otro lado,

$$\begin{aligned}
 \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) + \left(\frac{a_1}{b_1} \cdot \frac{a_3}{b_3}\right) &= \frac{a_1 a_2}{b_1 b_2} + \frac{a_1 a_3}{b_1 b_3} \\
 &= \frac{a_1 a_2 (b_1 b_3) + a_1 a_3 (b_1 b_2)}{b_1 b_2 (b_1 b_3)} \\
 &= \frac{b_1 (a_1 a_2 b_3 + a_1 a_3 b_2)}{b_1 (b_1 b_2 b_3)} \\
 &= \frac{a_1 a_2 b_3 + a_1 a_3 b_2}{b_1 b_2 b_3}.
 \end{aligned}$$

Por lo tanto,

$$\frac{a_1}{b_1} \cdot \left(\frac{a_2}{b_2} + \frac{a_3}{b_3}\right) = \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) + \left(\frac{a_1}{b_1} \cdot \frac{a_3}{b_3}\right).$$

**Ejemplo 5.36.** La tríada  $(\mathbb{Z}, +, \cdot)$  no es un campo porque  $(\mathbb{Z} \setminus \{0\}, \cdot)$  no es un grupo: ningún elemento  $a \in \mathbb{Z}$ ,  $a \neq \pm 1$  tiene inverso multiplicativo en  $\mathbb{Z}$ .

**Ejemplo 5.37.** La tríada  $(\mathbb{R}, +, \cdot)$  es un campo, con identidad aditiva 0 e identidad multiplicativa 1, llamado *campo de los números reales*.

El conjunto de los *números complejos* es el producto cartesiano de los números reales:

$$\mathbb{C} = \{(x, y) : x, y \in \mathbb{R}\} = \mathbb{R} \times \mathbb{R}$$

La primera coordenada de  $\mathbb{C}$  se llama *coordenada real*, mientras que la segunda se llama *coordenada imaginaria*. El número complejo  $(x, y) \in \mathbb{C}$  es llamado *real puro* si  $y = 0$ , o *imaginario puro* si  $x = 0$ .

Nuestro objetivo es definir dos operaciones binarias  $+$  y  $\cdot$  de  $\mathbb{C}$  tales que la tríada  $(\mathbb{C}, +, \cdot)$  sea un campo. Llamamos a  $+$  la *suma usual de números complejos* y la definimos como

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \in \mathbb{C},$$

donde  $(x_i, y_i) \in \mathbb{C}$ . Por otro lado, llamamos a  $\cdot$  la *multiplicación usual de números complejos* y la definimos como

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \in \mathbb{C},$$

donde  $x_i y_j$  representa la multiplicación usual de números reales.

Si  $(x_1, 0)$  y  $(x_2, 0)$  son reales puros, las operaciones definidas previamente coinciden con la suma y multiplicación usual de números reales:

$$\begin{aligned}(x_1, 0) + (x_2, 0) &= (x_1 + x_2, 0), \\ (x_1, 0) \cdot (x_2, 0) &= (x_1 x_2, 0).\end{aligned}$$

Observemos que, para cualquier  $(x, y) \in \mathbb{C}$ ,

$$(x, y) = (x, 0) \cdot (1, 0) + (y, 0) \cdot (0, 1).$$

Para simplificar notación, identificamos a  $(x, 0)$  y  $(y, 0)$  con los números reales  $x, y \in \mathbb{R}$ , respectivamente. Si definimos

$$i = (0, 1) \in \mathbb{C},$$

podemos denotar al número complejo  $(x, y)$  como

$$x + yi \in \mathbb{C}.$$

El imaginario puro  $i = (0, 1)$  es llamado *unidad imaginaria* y cumple que

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0),$$

al cual identificamos con  $-1 \in \mathbb{R}$ . Es por esta razón que comúnmente se dice que “ $i$  es una raíz cuadrada de  $-1$ ”.

Con esta nueva notación, la suma y multiplicación de números complejos puede escribirse como

$$\begin{aligned}(x_1 + y_1 i) + (x_2 + y_2 i) &= x_1 + x_2 + (y_1 + y_2)i, \\ (x_1 + y_1 i) \cdot (x_2 + y_2 i) &= x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1)i.\end{aligned}$$

**Ejemplo 5.38.** Consideremos los números complejos  $5 + i$  y  $2 + 4i$ . Entonces,

$$\begin{aligned}(5 + i) + (2 + 4i) &= (5 + 2) + (1 + 4)i = 7 + 5i, \\ (5 + i) \cdot (2 + 4i) &= (10 - 4) + (20 + 2)i = 6 + 22i.\end{aligned}$$

Usando la notación propuesta y las propiedades de los números reales, no es difícil demostrar que  $(\mathbb{C}, +, \cdot)$  es un campo. Sin embargo, la demostración es algo laboriosa, así que se deja como ejercicio.

Ahora tomemos en cuenta un campo con un número finito de elementos.

**Ejemplo 5.39.** La tríada  $(\mathbb{Z}_5, +, \cdot)$  es un campo finito, donde  $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ . La operación  $\cdot$  está definida como

$$[k] \cdot [s] = [ks] \in \mathbb{Z}_5 \text{ donde } k, s \in \mathbb{Z}.$$

Por el ejercicio 5.45, esta es una operación de clases bien definida. Por el ejercicio 5.25,  $(\mathbb{Z}_5, +)$  es un grupo. Claramente,  $(\mathbb{Z}_5, +)$  es abeliano porque

$$[k] + [s] = [k + s] = [s + k] = [s] + [k].$$

Demostraremos que también  $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$  es un grupo abeliano:

G1 La operación es asociativa: para toda  $m, k, s \in \mathbb{Z}$ ,

$$[m] \cdot ([k] \cdot [s]) = [m(ks)] = [(mk)s] = ([m] \cdot [k]) \cdot [s].$$

G2 La identidad multiplicativa es  $[1]$  porque  $[1] \cdot [s] = [1s] = [s]$ .

G3 Demostramos la existencia del inverso multiplicativo de  $[s] \in \mathbb{Z}_5$  usando el lema de Bézout. Como  $5 \in \mathbb{Z}$  es un número primo, sabemos que  $\text{mcd}(s, 5) = 1$ . Por lo tanto, existen enteros  $x, y \in \mathbb{Z}$  tales que

$$1 = sx + 5y.$$

De esta forma,  $[x] \in \mathbb{Z}_5$  es el inverso multiplicativo de  $[s]$  porque

$$[s] \cdot [x] = [sx] = [1 - 5y] = [1].$$

G4 La operación es conmutativa: para toda  $m, k, s \in \mathbb{Z}$ ,

$$[k] \cdot [s] = [ks] = [sk] = [s] \cdot [k].$$

Si  $(F, +, \cdot)$  es un campo y  $R \subseteq F$ , decimos que  $R$  es un *subcampo* si  $(R, +, \cdot)$  es un campo en sí mismo.

**Ejemplo 5.40.** La tríada  $(\mathbb{Q}, +, \cdot)$  es un subcampo de  $(\mathbb{R}, +, \cdot)$ . A su vez,  $(\mathbb{R}, +, \cdot)$  es un subcampo de  $(\mathbb{C}, +, \cdot)$ .

**Proposición 5.41 (test del subcampo).** Sea  $(F, +, \cdot)$  un campo y  $R \subseteq F$ . Entonces,  $(R, +, \cdot)$  es un subcampo de  $(F, +, \cdot)$  si y sólo si se cumplen las siguientes propiedades:

SC1 Las identidades del campo pertenecen a  $R$ ; es decir,  $e_0, e_1 \in R$ .



SC2 Para toda  $a, b \in R$ , tenemos que  $a + b \in R$  y  $-a \in R$ .

SC3 Para toda  $a, b \in R^*$ , tenemos que  $ab \in R^*$  y  $\frac{1}{a} \in R^*$ .

**Demostración.** Ejercicio 5.48. ■

**Ejemplo 5.42.** Consideremos el conjunto

$$\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} : x, y \in \mathbb{R}\}.$$

Demostraremos que la tríada

$$(\mathbb{Q}(\sqrt{2}), +, \cdot),$$

es un subcampo de  $(\mathbb{R}, +, \cdot)$ .

SC1 Las identidades  $0 = 0 + 0\sqrt{2}$  y  $1 = 1 + 0\sqrt{2}$  pertenecen a  $\mathbb{Q}(\sqrt{2})$ .

SC2 Si  $x_i + y_i\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ , entonces

$$\begin{aligned} (x_1 + y_1\sqrt{2}) + (x_2 + y_2\sqrt{2}) &= (x_1 + x_2) \\ &\quad + (y_1 + y_2)\sqrt{2} \in \mathbb{Q}(\sqrt{2}). \end{aligned}$$

El inverso aditivo de  $x + y\sqrt{2}$  es

$$-(x + y\sqrt{2}) = (-x) + (-y)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

SC3 Si  $x_i + y_i\sqrt{2} \in \mathbb{Q}(\sqrt{2})^* = \mathbb{Q}(\sqrt{2}) \setminus \{0\}$ , tenemos que

$$\begin{aligned} (x_1 + y_1\sqrt{2}) \cdot (x_2 + y_2\sqrt{2}) &= (x_1x_2 + 2y_1y_2) \\ &\quad + (x_1y_2 + x_2y_1)\sqrt{2} \end{aligned}$$

es un elemento de  $\mathbb{Q}(\sqrt{2})^*$ . El inverso multiplicativo de  $x + y\sqrt{2} \neq 0$  en  $\mathbb{R}$  es

$$\frac{1}{x + y\sqrt{2}},$$

aunque no está claro si este es un elemento de  $\mathbb{Q}(\sqrt{2})^*$ . Para demostrar que el inverso tiene la forma requerida, racionalizamos el denominador:

$$\begin{aligned}\frac{1}{x + y\sqrt{2}} &= \frac{1}{x + y\sqrt{2}} \frac{x - y\sqrt{2}}{x - y\sqrt{2}} \\ &= \frac{x - y\sqrt{2}}{x^2 - 2y^2} \\ &= \left( \frac{x}{x^2 - 2y^2} \right) - \left( \frac{y}{x^2 - 2y^2} \right) \sqrt{2} \in \mathbb{Q}(\sqrt{2})^*.\end{aligned}$$

**Palabras clave de la sección:** *campo, números racionales, números reales, números complejos, campo finito, subcampo.*

### 5.2.1 Ejercicios de campos

**Ejercicio 5.43.** Sea  $(F, +, \cdot)$  un campo. Explica por qué la identidad aditiva  $e_0 \in F$  no tiene inverso multiplicativo en  $F$ .

**Ejercicio 5.44.** Demuestra que los siguientes pares son grupos abelianos.

- a)  $(\mathbb{Q}, +)$ , donde  $+$  es la suma de números racionales definida en esta sección.
- b)  $(\mathbb{C}, +)$ , donde  $+$  es la suma de números complejos.
- c)  $(\mathbb{C}^*, \cdot)$ , donde  $\cdot$  es la multiplicación de números complejos.

**Ejercicio 5.45.** Sea  $n \in \mathbb{N}$ ,  $n \neq 0$ . Si  $[k], [s] \in \mathbb{Z}_n$ , demuestra que la operación binaria  $[k] \times [s] = [ks]$  no depende de los representantes  $k$  y  $s$ . Concluye que  $\times$  es una operación binaria de  $\mathbb{Z}_n$  bien definida.

**Ejercicio 5.46.** ¿Cuáles de las siguientes tríadas son campos? Justifica tu respuesta detalladamente.

- a)  $(\mathbb{C}, +, \cdot)$ , donde  $+$  y  $\cdot$  son las operaciones usuales de  $\mathbb{C}$ .
- b)  $(\mathbb{N}, +, \cdot)$ , donde  $+$  y  $\cdot$  son las operaciones usuales de  $\mathbb{N}$ .
- c)  $(\mathbb{Z}, +, \cdot)$ , donde  $+$  y  $\cdot$  son las operaciones usuales de  $\mathbb{Z}$ .
- d)  $(\mathbb{Z}_3, +, \times)$ , donde  $+$  y  $\times$  son las operaciones usuales de clases.
- e)  $(\mathbb{Z}_4, +, \times)$ , donde  $+$  y  $\times$  son las operaciones usuales de clases.

**Ejercicio 5.47.** Sea  $p \in \mathbb{N}$  un número primo. Demuestra que

$$(\mathbb{Z}_p, +, \times)$$

es un campo finito.

**Ejercicio 5.48.** Demuestra la proposición 5.32 usando el test del subgrupo 5.21.

**Ejercicio 5.49.** Si  $i$  es la unidad imaginaria, definamos

$$\mathbb{Q}(i) = \{x + yi : x, y \in \mathbb{Q}\}.$$

Demuestra que  $(\mathbb{Q}(i), +, \cdot)$  es un subcampo de  $(\mathbb{C}, +, \cdot)$  distinto de  $(\mathbb{R}, +, \cdot)$ .

**Ejercicio 5.50.** Sea  $F = \{O, I, \alpha, \beta\}$ . Considera dos operaciones binarias de  $F$  definidas por las siguientes tablas de Cayley:

$+$	$O$	$I$	$\alpha$	$\beta$	$\times$	$O$	$I$	$\alpha$	$\beta$
$O$	$O$	$I$	$\alpha$	$\beta$	$O$	$O$	$O$	$O$	$O$
$I$	$I$	$O$	$\beta$	$\alpha$	$I$	$O$	$I$	$\alpha$	$\beta$
$\alpha$	$\alpha$	$\beta$	$O$	$I$	$\alpha$	$O$	$\alpha$	$\beta$	$I$
$\beta$	$\beta$	$\alpha$	$I$	$O$	$\beta$	$O$	$\beta$	$I$	$\alpha$

Demuestra que  $(F, +, \times)$  es un campo finito.

### 5.3 Espacios vectoriales

Otra de las estructuras algebraicas más importantes son los *espacios vectoriales*. En esta sección damos una breve introducción a las propiedades básicas de los espacios vectoriales; un estudio más detallado puede encontrarse en (Rose, 2002) o (Fraleigh y Beauregard, 1994).

**Definición 5.51 (espacio vectorial real).** Sea  $V$  un conjunto no vacío. Sean  $+$  una operación binaria de  $V$  y  $*$  :  $\mathbb{R} \times V \rightarrow V$  una función. La triada  $(V, +, *)$  es un *espacio vectorial real* si para toda  $\alpha, \beta \in \mathbb{R}$   $v, w \in V$  se cumplen las siguientes propiedades:

- V1  $(V, +)$  es un grupo abeliano con identidad  $e_0$ .
- V2 *Distributividad 1:*  $\alpha * (v + w) = \alpha * v + \alpha * w$ .
- V3 *Distributividad 2:*  $(\alpha + \beta) * v = \alpha * v + \beta * v$ .
- V4 *Asociatividad:*  $(\alpha\beta) * v = \alpha * (\beta * v)$ .
- V5 *Identidad:*  $1 * v = v$ .

Los elementos de un espacio vectorial real son comúnmente llamados *vectores*. La operación binaria  $+$  es llamada “suma”, mientras que la operación  $*$  es llamada “multiplicación por escalar”.

El campo de los números reales usado en la definición 5.51 puede reemplazarse por cualquier otro campo  $F$  para definir un espacio vectorial *sobre*  $F$ . Aunque es común trabajar con espacios vectoriales sobre el campo de los números complejos o incluso sobre algún campo finito, nos enfocaremos en espacios vectoriales reales.

**Ejemplo 5.52 ( $\mathbb{R}^n$ ).** Consideremos el conjunto

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) : x, y, z \in \mathbb{R}\}.$$

Definamos la suma en  $\mathbb{R}^3$  como

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2) \in \mathbb{R}^3,$$

y la multiplicación por escalar como

$$\alpha * (x, y, z) = (\alpha x, \alpha y, \alpha z) \in \mathbb{R}^3,$$

donde  $\alpha \in \mathbb{R}$ . La tríada  $(\mathbb{R}^3, +, *)$  es un espacio vectorial real:

V1 ejercicio 5.62.

V2 Si  $\alpha \in \mathbb{R}$ , entonces

$$\begin{aligned}\alpha * [(x_1, y_1, z_1) + (x_2, y_2, z_2)] \\&= \alpha * (x_1 + x_2, y_1 + y_2, z_1 + z_2) \\&= (\alpha(x_1 + x_2), \alpha(y_1 + y_2), \alpha(z_1 + z_2)) \\&= (\alpha x_1 + \alpha x_2, \alpha y_1 + \alpha y_2, \alpha z_1 + \alpha z_2) \\&= (\alpha x_1, \alpha y_1, \alpha z_1) + (\alpha x_2, \alpha y_2, \alpha z_2) \\&= \alpha * (x_1, y_1, z_1) + \alpha * (x_2, y_2, z_2).\end{aligned}$$

V3 Si  $\alpha, \beta \in \mathbb{R}$ , entonces

$$\begin{aligned}(\alpha + \beta) * (x, y, z) &= ((\alpha + \beta)x, (\alpha + \beta)y, (\alpha + \beta)z) \\&= (\alpha x + \beta x, \alpha y + \beta y, \alpha z + \beta z) \\&= (\alpha x, \alpha y, \alpha z) + (\beta x, \beta y, \beta z) \\&= \alpha * (x, y, z) + \beta * (x, y, z).\end{aligned}$$

V4 Si  $\alpha, \beta \in \mathbb{R}$ , entonces

$$\begin{aligned}(\alpha\beta) * (x, y, z) &= ((\alpha\beta)x, (\alpha\beta)y, (\alpha\beta)z) \\&= (\alpha(\beta x), \alpha(\beta y), \alpha(\beta z)) \\&= \alpha * (\beta x, \beta y, \beta z) \\&= \alpha * (\beta * (x, y, z)).\end{aligned}$$

V5 Claramente,

$$1 * (x, y, z) = (1x, 1y, 1z) = (x, y, z).$$

**Ejemplo 5.53** ( $M_2(\mathbb{R})$ ). Consideremos el conjunto de matrices

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} : a_i \in \mathbb{R} \right\}.$$

Definamos la suma de matrices como

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix},$$

y la multiplicación por escalar como

$$\alpha * \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha a_1 & \alpha a_2 \\ \alpha a_3 & \alpha a_4 \end{pmatrix}, \text{ donde } \alpha \in \mathbb{R}.$$

La tríada  $(M_2(\mathbb{R}), +, *)$  es un espacio vectorial real (ejercicio 5.63).

**Ejemplo 5.54.** Consideremos el conjunto de funciones reales

$$\text{Fun} = \{f : \mathbb{R} \rightarrow \mathbb{R}\}.$$

Definamos la suma de dos funciones  $f$  y  $g$  como la función

$$(f \oplus g) \in \text{Fun},$$

dada por

$$(f \oplus g)(x) = f(x) + g(x), \text{ para } x \in \mathbb{R}.$$

Definamos la multiplicación de  $f$  por el escalar  $\alpha \in \mathbb{R}$  como la función  $\alpha * f \in \text{Fun}$  dada por

$$(\alpha * f)(x) = \alpha f(x), \text{ para } x \in \mathbb{R}.$$

La tríada  $(\text{Fun}, \oplus, *)$  es un espacio vectorial real. Demostraremos V1 y se deja como ejercicio demostrar V2-V5.

V1 (G1) La operación  $\oplus$  es asociativa porque

$$\begin{aligned} [f \oplus (g \oplus h)](x) &= f(x) + (g \oplus h)(x) \\ &= f(x) + [g(x) + h(x)] \\ &= [f(x) + g(x)] + h(x) \\ &= (f \oplus g)(x) + h(x) \\ &= [(f \oplus g) \oplus h](x), \end{aligned}$$

para toda  $x \in \mathbb{R}$ . Como dos funciones son iguales si y sólo si coinciden en todos sus valores, tenemos que

$$f \oplus (g \oplus h) = (f \oplus g) \oplus h.$$

V1 (G2) Sea  $i_0 : \mathbb{R} \rightarrow \mathbb{R}$  la función definida como  $i_0(x) = 0$ , para toda  $x \in \mathbb{R}$ . Entonces,

$$\begin{aligned} (f \oplus i_0)(x) &= f(x) + i_0(x) \\ &= f(x) + 0 \\ &= f(x), \end{aligned}$$

para toda  $x \in \mathbb{R}$ , lo que implica que

$$f \oplus i_0 = f.$$

Esto demuestra que  $i_0$  es la identidad de  $(\text{Fun}, \oplus)$ .

V1 (G3) El inverso aditivo de una función  $f \in \text{Fun}$  es la función  $(-f) : \mathbb{R} \rightarrow \mathbb{R}$  definida como  $(-f)(x) = -f(x)$ . Así,

$$\begin{aligned}(f \oplus (-f))(x) &= f(x) + (-f)(x) \\ &= f(x) - f(x) \\ &= 0 = i_0(x),\end{aligned}$$

para toda  $x \in \mathbb{R}$ , así que

$$f \oplus (-f) = i_0.$$

V1 (G4) La operación  $\oplus$  es conmutativa porque

$$\begin{aligned}(f \oplus g)(x) &= f(x) + g(x) \\ &= g(x) + f(x) \\ &= (g \oplus f)(x),\end{aligned}$$

para toda  $x \in \mathbb{R}$ , así que

$$f \oplus g = g \oplus f.$$

**Proposición 5.55.** Sea  $(V, +, *)$  un espacio vectorial real. Para toda  $v \in V$ ,  $\alpha \in \mathbb{R}$ , tenemos que:

- 1)  $0 * v = e_0$ .
- 2)  $\alpha * e_0 = e_0$ .
- 3)  $(-\alpha) * v = -(\alpha * v)$ .

**Demostración.** Demostraremos cada punto.

1) Observemos que

$$0 * v + e_0 = 0 * v \tag{V1}$$

$$= (0 + 0) * v$$

$$= 0 * v + 0 * v. \tag{V3}$$

Por cancelación izquierda en el grupo  $(V, +)$ , tenemos que  $e_0 = 0 * v$ .



- 2) Si  $\alpha = 0$ ,  $\alpha * e_0 = e_0$  por la parte 1) de esta proposición. Si  $\alpha \neq 0$ , entonces, para cualquier  $w \in V$ ,

$$\alpha * e_0 = \alpha * e_0 + e_0 \quad (V1)$$

$$= \alpha * e_0 + \frac{\alpha}{\alpha} * e_0 \quad (V5)$$

$$= \alpha * e_0 + \alpha * \left( \frac{1}{\alpha} * e_0 \right) \quad (V4)$$

$$= \alpha * \left[ e_0 + \left( \frac{1}{\alpha} * e_0 \right) \right] \quad (V2)$$

$$= \alpha * \left( \frac{1}{\alpha} * e_0 \right) \quad (V1)$$

$$= \frac{\alpha}{\alpha} * e_0 \quad (V4)$$

$$= 1 * e_0 = e_0. \quad (V5)$$

- 3) Ejercicio 5.64.

■

Un subconjunto  $W$  de un espacio vectorial real  $(V, +, *)$  es un subespacio vectorial si  $(W, +, *)$  es un espacio vectorial real en sí mismo.

**Teorema 5.56 (test del subespacio).** Sea  $(V, +, *)$  un espacio vectorial real y  $W \subseteq V$ . Entonces  $(W, +, *)$  es un subespacio vectorial si y sólo si se cumplen las siguientes propiedades:

SV1  $e_0 \in W$ .

SV2 Para toda  $u, v \in W$ , tenemos que  $u + v \in W$ .

SV3 Para toda  $v \in W$ ,  $\alpha \in \mathbb{R}$ , tenemos que  $\alpha * v \in W$ .

**Demostración.**

( $\Rightarrow$ ) Es claro que si  $(W, +, *)$  es un subespacio vectorial, las propiedades SV1-SV3 deben cumplirse.

( $\Leftarrow$ ) Supongamos que  $W$  satisface las propiedades SV1-SV3. Demostremos que  $(W, +, *)$  es un espacio vectorial en sí mismo. El par  $(W, +)$  es un subgrupo abeliano de  $(V, +)$ :

S1 Por la hipótesis SV1, la identidad aditiva  $e_0$  pertenece a  $W$ .

S2 Por la hipótesis SV2,  $u + v \in W$  para toda  $u, v \in W$ .

S3 Si  $v \in W$ , por SV3, sabemos que  $(-1) * v \in W$ . Como  $(-1) * v = -(1 * v) = -v$ , por la proposición 5.55 3), tenemos que  $-v \in W$ .

La hipótesis SV3 implica que la multiplicación por escalar está bien definida en  $W$ . Luego, las propiedades V2-V5 de espacio vectorial se cumplen para  $(W, +, *)$  al ser un caso particular de las propiedades V2-V5 de  $(V, +, *)$ . Por lo tanto,  $(W, +, *)$  es un espacio vectorial en sí mismo. ■

**Definición 5.57 (combinación lineal).** Sea  $(V, +, *)$  un espacio vectorial real. Una *combinación lineal* de los vectores  $v_1, v_2, \dots, v_n \in V$  es un vector de la forma

$$w = \alpha_1 * v_1 + \alpha_2 * v_2 + \dots + \alpha_n * v_n, \text{ donde } \alpha_i \in \mathbb{R}.$$

**Definición 5.58 (espacio generado).** Sea  $(V, +, *)$  un espacio vectorial real y  $A = \{v_1, \dots, v_n\}$  un subconjunto finito de  $V$ . El conjunto

$$\text{gen}(A) = \{\alpha_1 * v_1 + \alpha_2 * v_2 + \dots + \alpha_n * v_n : \alpha_i \in \mathbb{R}\}$$

es llamado *espacio generado* por  $A$ .

En otras palabras,  $\text{gen}(A)$  es el conjunto de combinaciones lineales de los vectores de  $A$ .

**Proposición 5.59.** Sea  $(V, +, *)$  un espacio vectorial real y

$$A = \{v_1, \dots, v_n\} \subseteq V.$$

La tríada  $(\text{gen}(A), +, *)$  es un subespacio vectorial de  $(V, +, *)$ .

**Demostración.** Usaremos el test del subespacio.

SV1 Por la proposición 5.55, 1), tenemos que

$$0 * v_1 + 0 * v_2 + \dots + 0 * v_n = e_0 + e_0 + \dots + e_0 = e_0,$$

por lo que  $e_0 \in \text{gen}(A)$ .

SV2 Consideremos dos elementos arbitrarios de  $\text{gen}(A)$ :

$$\alpha_1 * v_1 + \dots + \alpha_n * v_n \text{ y } \beta_1 * v_1 + \dots + \beta_n * v_n,$$

donde  $\alpha_i, \beta_i \in \mathbb{R}$ . Por la propiedad V3, la cual se cumple en  $(V, +, *)$ , tenemos que

$$\begin{aligned} & (\alpha_1 * v_1 + \dots + \alpha_n * v_n) + (\beta_1 * v_1 + \dots + \beta_n * v_n) \\ &= (\alpha_1 + \beta_1) * v_1 + \dots + (\alpha_n + \beta_n) * v_n \in \text{gen}(A). \end{aligned}$$

SV3 La propiedad V2 implica que

$$\begin{aligned} & \alpha * (\alpha_1 * v_1 + \dots + \alpha_n * v_n) \\ &= \alpha * (\alpha_1 * v_1) + \dots + \alpha * (\alpha_n * v_n) \end{aligned} \quad (V2)$$

$$= (\alpha\alpha_1) * v_1 + \dots + (\alpha\alpha_n) * v_n \in \text{gen}(A) \quad (V4)$$

■

**Ejemplo 5.60.** Consideremos el subconjunto

$$A = \{(1, 0, 0), (0, 1, 1)\} \subseteq \mathbb{R}^3.$$

El espacio generado por  $A$  es

$$\begin{aligned} \text{gen}(A) &= \{\alpha_1(1, 0, 0) + \alpha_2(0, 1, 1) : \alpha_i \in \mathbb{R}\} \\ &= \{(\alpha_1, 0, 0) + (0, \alpha_2, \alpha_2) : \alpha_i \in \mathbb{R}\} \\ &= \{(\alpha_1, \alpha_2, \alpha_2) : \alpha_i \in \mathbb{R}\}. \end{aligned}$$

**Ejemplo 5.61.** Consideremos el subconjunto

$$B = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \subseteq \mathbb{R}^3.$$

El espacio generado por  $B$  es

$$\begin{aligned} \text{gen}(A) &= \{\alpha_1(1, 0, 0) + \alpha_2(0, 1, 0) + \alpha_3(0, 0, 1) : \alpha_i \in \mathbb{R}\} \\ &= \{(\alpha_1, \alpha_2, \alpha_3) : \alpha_i \in \mathbb{R}\} \\ &= \mathbb{R}^3. \end{aligned}$$

**Palabras clave de la sección:** *espacio vectorial real, subespacio, combinación lineal, espacio generado.*

### 5.3.1 Ejercicios de espacios vectoriales

**Ejercicio 5.62.** Demuestra que  $(\mathbb{R}^3, +)$  es un grupo abeliano.

**Ejercicio 5.63.** Demuestra que las siguientes tríadas son espacios vectoriales reales:

- a)  $(M_2(\mathbb{R}), +, *)$ , donde  $M_2(\mathbb{R})$  es el conjunto de matrices definido anteriormente.
- b)  $(\mathbb{R}^n, +, *)$ , donde  $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R}$ ,  $n \in \mathbb{N}$ .
- c)  $(\text{Fun}, \oplus, *)$ , donde  $\text{Fun}$  es el conjunto de funciones sobre  $\mathbb{R}$ .

**Ejercicio 5.64.** Sea  $(V, +, *)$  un espacio vectorial real. Demuestra que  $(-\alpha) * v = -(\alpha * v)$ , para toda  $\alpha \in \mathbb{R}$ ,  $v \in V$ .

**Ejercicio 5.65.** Supongamos que la multiplicación  $\cdot$  de elementos de  $\mathbb{R}^3$  está definida como

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = (x_1 y_1, x_2 y_2, x_3 y_3) \in \mathbb{R}^3,$$

donde  $x_i, y_i \in \mathbb{R}$ . Si  $*$  es la multiplicación por escalar usual, ¿es la tríada  $(\mathbb{R}^3, \cdot, *)$  un espacio vectorial real? Justifica tu respuesta.

**Ejercicio 5.66.** Demuestra las siguientes afirmaciones:

- a)  $W = \{(x, 0, z) : x, z \in \mathbb{R}\}$  es un subespacio de

$$(\mathbb{R}^3, +, *).$$

- b)  $\text{Fun}_0 = \{f : \mathbb{R} \rightarrow \mathbb{R} : f(0) = 0\}$  es un subespacio de

$$(\text{Fun}, \oplus, *).$$

- c)  $\text{Fun}_1 = \{f : \mathbb{R} \rightarrow \mathbb{R} : f(1) = 1\}$  no es un subespacio de

$$(\text{Fun}, \oplus, *).$$

**Ejercicio 5.67.** Encuentra el espacio generado por los siguientes subconjuntos de  $\mathbb{R}^3$ :

$$A_1 = \{(7, 0, 0)\},$$

$$A_2 = \{(2, 0, 0), (0, 0, 0), (1, 0, 0), (0, 0, 1)\},$$

$$A_3 = \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}.$$

**Ejercicio 5.68.** Sean

$$W_1 = \{(\alpha_1, \alpha_2, -\alpha_2) : \alpha_i \in \mathbb{R}\},$$

$$W_2 = \{(\alpha_1, 0, 0) : \alpha_1 \in \mathbb{R}\},$$

$$W_3 = \{(\alpha_1, \alpha_2, 3\alpha_1 - 5\alpha_2) : \alpha_i \in \mathbb{R}\}.$$

Encuentra subconjuntos de vectores  $A_i$  en  $\mathbb{R}^3$  tales que  $\text{gen}(A_i) = W_i$ . Concluye que  $(W_i, +, *)$  es un subespacio de  $(\mathbb{R}^3, +, *)$  para cada  $i$ .

## 5.4 Polinomios

En esta sección presentamos formalmente uno de los conceptos más importantes usados en álgebra. Muy probablemente el lector ya está familiarizado con el uso de polinomios por haber recibido de cursos previos de álgebra básica. Aquí abordaremos nuevamente muchos temas elementales relacionados con polinomios y discutiremos el tipo de estructura algebraica que forman.

A partir de ahora, si  $(F, +, \cdot)$  es un campo, denotaremos sus identidades aditiva  $e_0 \in F$  y multiplicativa  $e_1 \in F$  simplemente como 0 y 1, respectivamente. La razón de esto es que generalmente estaremos pensando en los campos de números racionales, reales o complejos.

Sea  $(F, +, \cdot)$  un campo. Decimos que  $f(x)$  es un *polinomio* sobre  $F$  en la variable  $x$ , si  $f(x)$  es una expresión de la forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

donde  $a_i \in F$ ,  $n \in \mathbb{N}$ . Esta no es la definición formal de polinomio debido a que no hemos establecido con precisión el término “variable  $x$ ”. Sin embargo, la definición anterior será suficiente para nuestros propósitos.

Denotamos como  $F[x]$  al conjunto de polinomios sobre  $F$  en la variable  $x$ . Los elementos  $a_i \in F$  de un polinomio  $f(x)$  son llamados sus *coeficientes*. Si  $a_n \neq 0$  y  $a_i = 0$  para toda  $i > n$ , decimos que  $f(x)$  es de *grado*  $n$  y escribimos  $\deg f(x) = n$ . En este caso el coeficiente  $a_n \in F$  es llamado *coeficiente principal* de  $f(x)$ . Observemos que no asociamos ningún grado con el polinomio  $0 \in F[x]$

**Definición 5.69 (polinomio constante).** Un polinomio  $f(x) \in F[x]$  es llamado *constante* si  $f(x) = 0$  o  $\deg f(x) = 0$ .

Los polinomios constantes de  $F[x]$  coinciden con los elementos de  $F$ .

Definimos la suma y la multiplicación de polinomios de la siguiente manera. Sean  $f(x), g(x) \in F[x]$  polinomios

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0.$$

donde  $a_i, b_i \in F$ . Sin perder generalidad, supongamos que  $n \geq m$ . Definimos la suma de  $f(x)$  y  $g(x)$  como

$$f(x) + g(x) = a_n x^n + \dots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + \dots + (a_0 + b_0).$$

Por otro lado, definimos la multiplicación de  $f(x)$  y  $g(x)$  como

$$\begin{aligned} f(x)g(x) &= a_nb_mx^{n+m} + (a_{n-1}b_m + a_nb_{m-1})x^{n+m-1} \\ &\quad + \dots + (a_1b_0 + a_0b_1)x + (a_0 + b_0) \\ &= \sum_{k=0}^{n+m} \left( \sum_{i+j=k} a_ib_j \right) x^k. \end{aligned}$$

La definición anterior podría parecer poco natural; sin embargo, si prestamos atención podemos darnos cuenta de que se trata de la multiplicación usual de polinomios estudiada en cursos de álgebra básica.

**Ejemplo 5.70.** Consideremos los polinomios

$$f(x) = x^2 + 3x + 2 \text{ y } g(x) = x - 1,$$

en  $\mathbb{Q}[x]$ . El grado de  $f(x)$  es 2 y sus coeficientes son  $a_2 = 1$ ,  $a_1 = 3$  y  $a_0 = 2$ . El grado de  $g(x)$  es 1 y sus coeficientes son  $b_1 = 1$ ,  $b_0 = -1$ . La suma y producto de estos polinomios son:

$$\begin{aligned} f(x) + g(x) &= a_2x^2 + (a_1 + b_1)x + (a_0 + b_0) \\ &= x^2 + 4x + 1 \in \mathbb{Q}[x], \end{aligned}$$

$$\begin{aligned} f(x)g(x) &= a_2b_1x^3 + (a_2b_0 + a_1b_1)x^2 + (a_1b_0 + a_0b_1)x \\ &\quad + a_0b_0 \\ &= x^3 + 2x^2 - x - 2 \in \mathbb{Q}[x]. \end{aligned}$$

La tríada  $(F[x], +, \cdot)$  no es un campo ya que muchos polinomios no tienen inverso multiplicativo en  $F[x]$ . Por ejemplo,  $x \in F[x]$  no tiene inverso multiplicativo en  $F[x]$  porque expresiones como  $\frac{1}{x}$  no son polinomios. De hecho, ningún polinomio no constante tiene inverso multiplicativo en  $F[x]$  (ejercicio 5.87).

Sin embargo,  $(F[x], +, \cdot)$  satisface muchas otras propiedades:

- 1)  $(F[x], +)$  es un grupo abeliano (ejercicio 5.84).
- 2) La multiplicación  $\cdot$  es asociativa y conmutativa.
- 3) Existe la identidad multiplicativa: el polinomio constante  $1 \in F[x]$ .
- 4) La propiedad distributiva se cumple.

Una tríada  $(A, +, \cdot)$  que satisface las propiedades anteriores es llamada *anillo conmutativo*; estas estructuras algebraicas se estudian normalmente en cursos más avanzados de álgebra abstracta, ver (Hernández Magdaleno y Castillo Ramírez, 2012).

La tríada  $(F[x], +, \cdot)$  comparte muchas propiedades con  $(\mathbb{Z}, +, \cdot)$ . La siguiente definición es análoga al caso de los números enteros.

**Definición 5.71 (factor).** Sean  $f(x), h(x) \in F[x]$ . Decimos que  $f(x)$  es un *factor* de  $h(x)$ , o que  $f(x)$  *divide* a  $h(x)$ , si  $h(x) = f(x)g(x)$  para algún  $g(x) \in F[x]$ .

**Ejemplo 5.72.** Con respecto al ejemplo 5.70, el polinomio  $f(x) = x^2 + 3x + 2$  divide a  $h(x) = x^3 + 2x^2 - x - 2$  porque  $h(x) = f(x)g(x)$ , donde  $g(x) = x - 1$ .

En la sección 5.2 estudiamos el algoritmo de la división en  $\mathbb{Z}$ . Este resultado también se cumple para polinomios.

**Teorema 5.73 (algoritmo de la división).** Sea  $F$  un campo y

$$f(x), g(x) \in F[x] \text{ con } g(x) \neq 0.$$

Existen polinomios únicos  $q(x)$  y  $r(x)$  en  $F[x]$  tales que

$$f(x) = g(x)q(x) + r(x),$$

donde  $r(x) = 0$  o  $\deg r(x) < \deg g(x)$ .

Omitimos la demostración del teorema anterior ya que involucra algunos conceptos que no hemos definido en este texto. Al igual que en el caso de los enteros,  $q(x)$  se llama *cociente* y  $r(x)$  se llama *residuo* de la división de  $f(x)$  entre  $g(x)$ .

**Ejemplo 5.74.** Consideremos los polinomios

$$f(x) = 2x^4 + x \text{ y } g(x) = x^2 + 2x + 1 \text{ en } \mathbb{Q}[x].$$

La forma de encontrar el cociente y el residuo de la división de  $f(x)$  entre  $g(x)$  es la llamada “división larga”:

$$\begin{array}{r} 2x^2 - 4x + 6 \\ x^2 + 2x + 1 \overline{) 2x^4 + x} \\ \underline{-2x^4 - 4x^3 - 2x^2} \phantom{+ 6} \\ -4x^3 - 2x^2 + x \phantom{+ 6} \\ \underline{4x^3 + 8x^2 + 4x} \phantom{+ 6} \\ 6x^2 + 5x \phantom{+ 6} \\ \underline{-6x^2 - 12x - 6} \\ -7x - 6 \end{array}$$



El procedimiento se detiene cuando encontramos un residuo de grado menor que  $\deg g(x) = 2$ . De esta manera, el cociente de la división es  $q(x) = 2x^2 - 4x + 6$  y el residuo es  $r(x) = -7x - 6$ . Se deja como ejercicio comprobar que  $f(x) = q(x)g(x) + r(x)$  (ejercicio 5.88).

**Definición 5.75 (irreducible).** Sea  $f(x) \in F[x]$  un polinomio no constante. Decimos que  $f(x)$  es *irreducible* si  $f(x)$  no puede ser factorizado como el producto de dos polinomios no constantes de  $F[x]$ .

Es posible demostrar que cualquier polinomio no constante de  $F[x]$  puede ser escrito de forma esencialmente única como el producto de polinomios irreducibles. Por lo tanto, en cierta forma, los polinomios irreducibles son análogos a los números primos. También es posible estudiar conceptos como el máximo común divisor, el algoritmo de Euclides y el lema de Bézout para polinomios.

Ahora nos enfocaremos en estudiar otros conceptos importantes relacionados con polinomios. Si

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0,$$

y  $\alpha \in F$  es un elemento del campo, definimos a  $f(\alpha) \in F$  como

$$f(\alpha) = a_n (\alpha)^n + a_{n-1} (\alpha)^{n-1} + \dots + a_0.$$

En otras palabras,  $f(\alpha)$  es el elemento del campo que resulta al sustituir  $x$  por  $\alpha$  en el polinomio  $f(x)$ .

**Ejemplo 5.76.** Sean

$$f(x) = 2x^2 + ix + 1 \in \mathbb{C}[x] \text{ y } \alpha = 2i \in \mathbb{C}.$$

Entonces  $f(2i)$  es igual a

$$\begin{aligned} f(2i) &= 2(2i)^2 + i(2i) + 1 \\ &= 8i^2 + 2i^2 + 1 = -9 \in \mathbb{C}, \end{aligned}$$

ya que  $i^2 = -1$  en  $\mathbb{C}$ .

**Definición 5.77 (raíz).** Sea  $f(x) \in F[x]$ . Decimos que un número  $\alpha \in F$  es una *raíz* de  $f(x)$  si  $f(\alpha) = 0$ .

**Ejemplo 5.78.** Si  $h(x) = x^3 + 2x^2 - x - 2$ , entonces 1 es una raíz de  $h(x)$  porque

$$h(1) = (1)^3 + 2(1)^2 - 1 - 2 = 0.$$

Debido a la forma en la que están definidas las operaciones de polinomios, si tenemos  $f(x), g(x), h(x), s(x) \in F[x]$  tales que

$$h(x) = f(x)g(x) \text{ y } s(x) = f(x) + g(x),$$

entonces  $h(\alpha) = f(\alpha)g(\alpha)$  y  $s(\alpha) = f(\alpha) + g(\alpha)$  para cualquier  $\alpha \in F$ . En otras palabras, da igual sumar o multiplicar polinomios y luego evaluarlos que evaluar polinomios y luego sumar o multiplicar los resultados.

**Ejemplo 5.79.** Sean  $f(x) = x^2 + 3x + 2$ ,  $g(x) = x - 1$ , y  $h(x) = x^3 + 2x^2 - x - 2$ . Observemos que

$$h(x) = (x^2 + 3x + 2)(x - 1) = f(x)g(x).$$

Evaluemos estos polinomios en  $\alpha = 3$ :

$$f(3) = 3^2 + 3 \cdot 3 + 2 = 20,$$

$$g(3) = 3 - 1 = 2,$$

$$h(3) = 3^3 + 2 \cdot 3^2 - 3 - 2 = 40.$$

Así, comprobamos que

$$f(3)g(3) = 20 \cdot 2 = 40 = h(3).$$

**Teorema 5.80 (factor).** Sea  $f(x) \in F[x]$ . Un número  $\alpha \in F$  es una raíz de  $f(x)$  si y sólo si  $x - \alpha$  es un factor de  $f(x)$ .

**Demostración.**

( $\Rightarrow$ ) Supongamos que  $\alpha \in F$  es una raíz de  $f(x)$ . Por el algoritmo de la división, con  $g(x) = x - \alpha \in F[x]$ , tenemos que

$$f(x) = q(x)(x - \alpha) + r(x),$$

para algunos  $q(x), r(x) \in F[x]$ , donde

$$r(x) = 0 \text{ o } \deg r(x) < \deg g(x) = 1.$$

Luego,  $r(x)$  es un polinomio constante. Como  $f(\alpha) = 0$ , sabemos que

$$\begin{aligned} 0 &= f(\alpha) \\ &= q(\alpha)(\alpha - \alpha) + r(\alpha) \\ &= r(\alpha). \end{aligned}$$

Debido a que  $r(x)$  es constante,  $r(x) = r(\alpha) = 0$ , lo que implica que  $f(x) = q(x)(x - \alpha)$ . Por lo tanto,  $x - \alpha$  es factor de  $f(x)$ .

( $\Leftarrow$ ) Supongamos que  $x - \alpha \in F[x]$  es factor de  $f(x) \in F[x]$ . Por definición, tenemos que

$$f(x) = q(x)(x - \alpha),$$

para algún  $q(x) \in F[x]$ . Así,

$$f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha) \cdot 0 = 0.$$

Por lo tanto,  $\alpha$  es una raíz de  $f(x)$ . ■

En general, no es verdad que todos los polinomios de  $F[x]$  tienen una raíz en  $F$ .

**Ejemplo 5.81.** Ningún polinomio constante distinto de cero tiene raíces. Por ejemplo,  $f(x) = 5$  no puede tener ninguna raíz ya que  $f(\alpha) = 5 \neq 0$  para toda  $\alpha \in F$ .

La siguiente proposición nos brinda un ejemplo más interesante.

**Proposición 5.82.** El polinomio

$$f(x) = x^2 - 2 \in \mathbb{Q}[x],$$

no tiene ninguna raíz en  $\mathbb{Q}$ .

**Demostración.** Por reducción al absurdo, supongamos que  $\alpha^2 - 2 = 0$  para algún  $\alpha \in \mathbb{Q}$ . En forma equivalente, escribimos  $\alpha^2 = 2$ . Como  $\alpha \in \mathbb{Q}$ , tenemos que  $\alpha = \frac{m}{n}$ , donde  $m, n \in \mathbb{Z}$ ,  $n \neq 0$ . Podemos asumir que  $m$  y  $n$  no tienen factores comunes (excepto 1), ya que éstos pueden ser cancelados en la fracción. Además  $n \neq 1$  porque no existe ningún entero  $\frac{m}{1} = m$  tal que  $m^2 = 2$ .

Por el teorema fundamental de la aritmética,

$$m = p_1 \dots p_r,$$

$$n = q_1 \dots q_s,$$

donde  $p_i, q_j \in \mathbb{Z}$ , son números primos distintos. Entonces,

$$\left(\frac{m}{n}\right)^2 = \frac{p_1^2 \dots p_r^2}{q_1^2 \dots q_s^2} = 2,$$

lo que implica que

$$p_1^2 \dots p_r^2 = 2q_1^2 \dots q_s^2.$$

Por unicidad de la factorización en primos,  $p_k = 2$  para alguna  $k$ , y cancelando

$$p_1^2 \dots p_k \dots p_r^2 = q_1^2 \dots q_s^2.$$

Pero ahora, de nuevo por la unicidad de la factorización, tenemos que  $p_k = q_d$ , para alguna  $d$ , lo cual contradice que los primos  $p_i$  y  $q_j$  son distintos. Por lo tanto, no existe ningún  $\alpha \in \mathbb{Q}$  tal que  $\alpha^2 - 2 = 0$ . ■

La proposición anterior también implica que  $\sqrt{2} \notin \mathbb{Q}$ .

Si  $F = \mathbb{C}$ , entonces sí es verdad que cualquier polinomio no constante en  $\mathbb{C}[x]$  tiene una raíz en  $\mathbb{C}$ . Este hecho es llamado *teorema fundamental del álgebra*.

**Teorema 5.83.** Sea  $f(x) \in \mathbb{C}[x]$  un polinomio no constante. Entonces  $f(x)$  tiene una raíz en  $\mathbb{C}$ .

La demostración de este teorema está fuera del alcance de este texto; normalmente se estudia en un texto de *análisis complejo*, por ejemplo (Marsden y Hoffman, 1999).

**Palabras clave de la sección:** *polinomio, grado, polinomio constante, factor, algoritmo de la división para polinomios, polinomio irreducible, raíz de un polinomio, teorema fundamental del álgebra.*

### 5.4.1 Ejercicios de polinomios

**Ejercicio 5.84.** Demuestra que  $(F[x], +)$  es un grupo abeliano.

**Ejercicio 5.85.** Sean  $f(x), g(x) \in F[x]$  polinomios de grado  $n$  y  $m$ , respectivamente. Demuestra que

$$\deg(f(x) + g(x)) = \max\{n, m\},$$

y que  $\deg(f(x)g(x)) = n + m$ .

**Ejercicio 5.86.** Encuentra la suma y la multiplicación de los polinomios  $f(x) = 2x^3 - x + 3$  y  $g(x) = x^2 + x - 1$ .

**Ejercicio 5.87.** Demuestra que todos los polinomios constantes tienen inverso multiplicativo en  $F[x]$ , pero que ningún polinomio no constante tiene inverso multiplicativo en  $F[x]$ . (Sugerencia: usa el Ejercicio 5.85.)

**Ejercicio 5.88.** Comprueba que  $f(x) = q(x)g(x) + r(x)$ , donde  $f(x)$ ,  $q(x)$ ,  $g(x)$  y  $r(x)$  son los polinomios definidos en el ejemplo 5.74.

**Ejercicio 5.89.** Sean  $f(x) = x + 2$  y  $g(x) = x^4 + 3x^2 + x - 1$  polinomios en  $\mathbb{Q}[x]$ . Encuentra el cociente y residuo de la división de  $f(x)$  entre  $g(x)$ .

**Ejercicio 5.90.** Sean  $f(x), g(x), s(x) \in F[x]$  polinomios tales que  $s(x) = f(x) + g(x)$ . Demuestra que  $s(\alpha) = f(\alpha) + g(\alpha)$  para cualquier  $\alpha \in F$ .

**Ejercicio 5.91.** Demuestra que el polinomio  $f(x) = x^2 - 3 \in \mathbb{Q}[x]$  no tiene ninguna raíz en  $\mathbb{Q}$ .

**Ejercicio 5.92.** Sea  $f(x) = ax^2 + bx + c \in \mathbb{C}[x]$ , donde  $a, b, c \in \mathbb{C}$ ,  $a \neq 0$ . Demuestra que si

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ y } \beta = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

entonces  $f(x) = (x - \alpha)(x - \beta)$ . Concluye que  $\alpha$  y  $\beta$  son raíces de  $f(x)$ .

**Ejercicio 5.93.** Usa el ejercicio 5.92 para encontrar las raíces de los polinomios  $f(x) = 3x^2 + 6x - 1$  y  $g(x) = x^2 + x + 4$ .

## 5.5 Definiciones del capítulo

Escribe la definición y un ejemplo de cada uno de los conceptos enlistados a continuación.

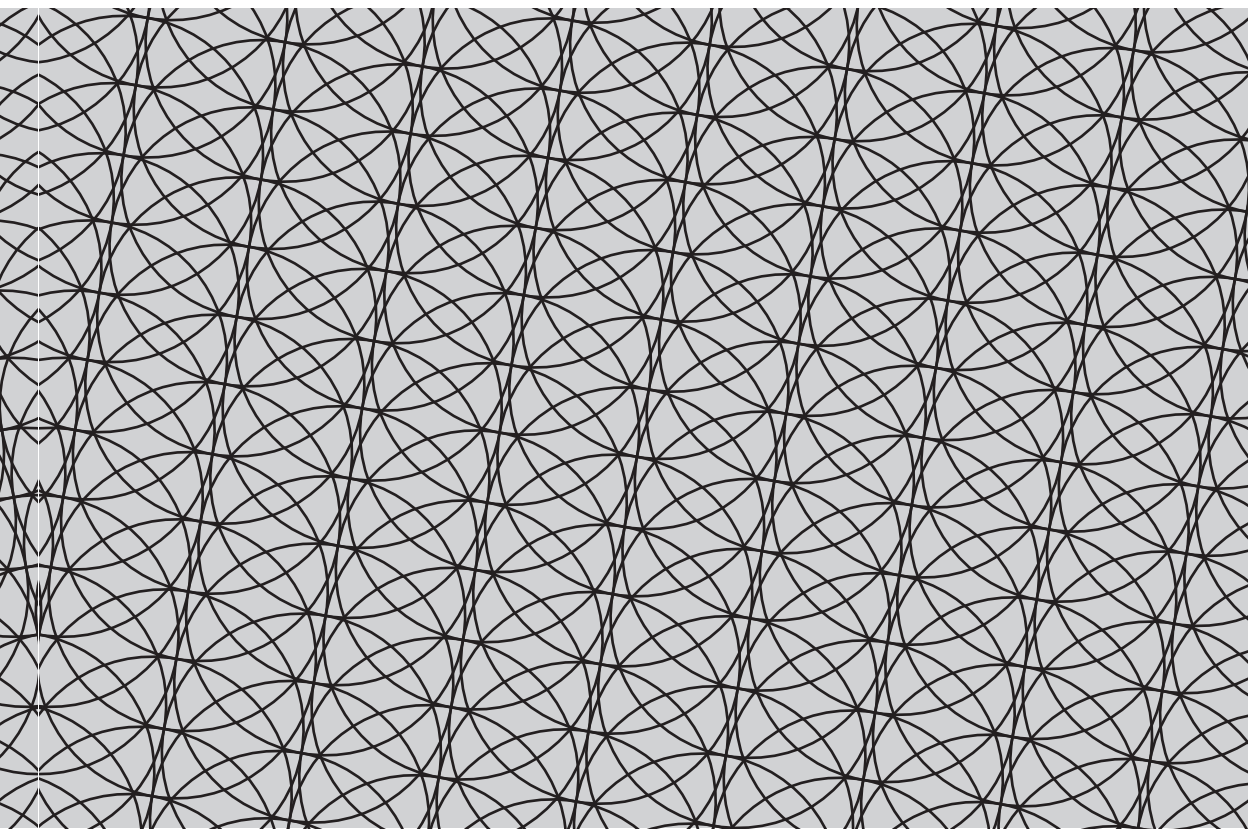
- 1) Operación binaria.
- 2) Grupo.
- 3) Grupo abeliano.
- 4) Subgrupo.
- 5) Grupo trivial.
- 6) Subgrupo cíclico.
- 7) Campo.
- 8) Números racionales.
- 9) Números complejos.
- 10) Espacio vectorial real.
- 11) Combinación lineal.
- 12) Espacio generado.
- 13) Polinomio.
- 14) Coeficientes de un polinomio.
- 15) Grado de un polinomio.
- 16) Polinomio mónico.
- 17) Polinomio constante.
- 18) Factor de un polinomio.
- 19) Polinomio irreducible.
- 20) Raíz de un polinomio.

- Bloch, E. D. (2000). *Proofs and fundamentals: a first course in abstract mathematics*. Basel: Birkhäuser.
- Burton, D. M. (1980). *Elementary number theory*. Boston: Allyn & Bacon, Inc.
- Cameron, P. J. (1995). *Combinatorics: topics, techniques, algorithms*. Cambridge: Cambridge University Press.
- Church, A. (1970). *Introduction to mathematical logic (vol. 1)*. New Jersey: Princeton University Press.
- Copi, I. M., y Cohen, C. (1995). *Introducción a la lógica*. México : Editorial Limusa.
- Cupillari, A. (2005). *The nuts and bolts of proofs*. Amsterdam: Elsevier Academic Press.
- Dunham, W. (1990). *Journey through genius: the great theorems of mathematics*. New Jersey: John Wiley & Sons.
- Enderton, H. B. (2001). *A mathematical introduction to logic*. New York and London: Harcourt Academic Press.
- Fraleigh, J. B. (1998). *A first course in abstract algebra*. New Jersey: Prentice Hall.
- Fraleigh, J. B., y Bearegard, R. A. (1994). *Linear algebra*. Pearson.
- Gallian, J. A. (2004). *Contemporary abstract algebra*. Massachusetts: Houghton Mifflin.
- Halmos, P. R. (1998). *Naïve set theory*. Springer Undergraduate Texts in Mathematics.
- Hernández Magdaleno, A. M., y Castillo Ramírez, A. (2012). *Álgebra moderna: anillos y campos*. Guadalajara: Editorial Universitaria.
- Herstein, I. N. (1983). *Álgebra moderna*. México: Trillas.
- Jones, G. A., y Josephine, J. M. (1998). *Elementary number theory*. Springer.
- Lay, S. R. (2001). *Analysis with an introduction to proof*. Prentice Hall.
- Liebeck, M. W. (2001). *A concise introduction to pure mathematics*. CRC Press Inc.
- Maddox, R. B. (2008). *A transition to abstract mathematics, learning mathematical thinking and writing*. Amsterdam: Elsevier Academic Press.
- Magnus, P. D. (2012). *Forallx: An introduction to formal logic*. Recuperado de <http://www.fecundity.com/codex/forallx.pdf>.
- Marsden, J. E., y Hoffman, M. J. (1999). *Basic complex analysis*. San Francisco: W. H. Freeman.

- Rose, H. E. (2002). *Linear algebra: a pure mathematical approach*. Birkhäuser.
- Rudin, W. (1976). *Principles of mathematical analysis*. McGraw-Hill Higher Education.
- Schramm, M. J. (2008). *Introduction to real analysis*. New York: Dover.
- Stewart, I. (2008). *Belleza y verdad: una historia de la simetría*. Editorial Crítica.
- Stewart, I., y Tall, D. (1977). *The foundations of mathematics*. Oxford: Oxford University Press.
- Velleman, D. J. (1995). *How to prove it: a structured approach*. Cambridge: Cambridge University Press.
- Zubieta, G. (1974). *Manual de lógica para estudiantes de matemáticas*. México: Editorial Trillas.



# Índice alfabético



# Índice alfabético

## A

Algoritmo

de Euclides, 120

de la división, 117

Axioma de Peano, 105

## B

Bézout

lema de, 118

## C

Campo, 164

Clase de equivalencia, 87

Codominio, 71

Coefficiente binomial, 149

Complemento

de subconjuntos de un universo  $U$ , 60

de un conjunto en otro, 59

Composición de funciones, 79

Conclusión del teorema, 33

Congruencia módulo  $m$ , 127

Conjunción, 23

Conjunto(s), 44

cociente de una relación de equivalencia, 88

bien ordenado, 98

cociente  $\mathbb{Z}_m$  130, 128

finito, 134

igualdad de, 50

imagen de un, 75

infinito, 134

intersección de, 57

numerable, 135

partición de un, 89

potencia, 53

preimagen de un, 75

unión de, 56

Contradicción, 30

Contradominio, 71

Cota

inferior, 97

superior, 97  
Cuantificador, 18  
existencial, 18  
universal, 19

## D

Demostración  
de equivalencias, 38  
directa, 36  
por contraejemplo, 36  
por contraposición, 36  
reducción al absurdo, 37  
Diagrama de Venn, 56  
Disyunción, 25  
Divisor, 116  
Dominio, 70

## E

Ecuación diofántica, 122  
Elemento  
maximal, 96  
minimal, 96  
Euclides  
algoritmo de, 120  
lema de, 121  
Existencia y unicidad, 20

## F

Función, 72  
biyectiva, 77  
identidad, 83  
inyectiva, 76  
sobreyectiva, 76

## G

Grupo, 155  
abeliano, 159

## H

Hipótesis  
del continuo, 140  
de un teorema, 33

## **I**

### **Identidad**

- aditiva del campo, 164
- en un grupo, 155
- multiplicativa del campo, 164

### **Imagen, 74**

### **Implicación, 26**

- contrapuesta, 28
- recíproca, 28

### **Inducción matemática, 106**

### **Ínfimo, 97**

### **Inverso**

- en un grupo, 155

## **L**

### **Lema**

- de Bézout, 118
- de Euclides, 121

### **Leyes de De Morgan, 61**

## **M**

### **Máximo absoluto, 96**

### **Máximo común divisor, 118**

### **Mínimo absoluto, 96**

## **N**

### **Número**

- cardinal, 138
- compuesto, 116
- primo, 116

### **Negación, 17**

- doble, 18
- tabla de verdad, 18
- de proposiciones cualificadas, 20

### **Notación**

- por comprensión, 45
- por extensión, 45

## **O**

### **Operación binaria, 153**

### **Orden total, 95**

## **P**

### **Par ordenado, 63**

Paradoja, 45  
Partición de un conjunto, 89  
Permutación, 147  
Predicado, 14  
Premisa del argumento, 33  
Primos relativos, 118  
Principio fundamental de conteo, 143  
Producto cartesiano, 63  
Proposición, 13  
Proposición simple, 14

## **R**

Rango, 71  
Relación, 69  
    antisimétrica, 94  
    de equivalencia, 86  
    de orden, 94  
    inversa, 81  
    reflexiva, 86  
    simétrica, 86  
    transitiva, 86

## **S**

Subcampo, 168  
    test de, 168  
Subconjunto, 51  
Subgrupo, 159  
    cíclico, 161  
    test de, 160  
Sucesor de un número, 105  
Supremo, 97

## **T**

Término singular, 14  
Tabla  
    de Caley, 158  
    de la bicondicional, 29  
    de la conjunción, 24  
    de la disyunción, 25  
    de la implicación, 26  
    de la negación, 18  
    de verdad, 17  
    símbolos de los conectivos lógicos, 23

Tautología, 30

Teorema, 33

de Cantor, 139

fundamental de la aritmética, 122

## **U**

Universo de discurso, 13

## **V**

Valor de verdad, 13

# Acerca de los autores

**Alonso Castillo Pérez** es ingeniero en comunicaciones y electrónica por la Universidad de Guadalajara. Obtuvo el grado de maestro en ingeniería eléctrica en la misma institución. Ha sido profesor en programas de licenciatura, maestría y doctorado, en los que fundamentalmente ha impartido cursos relacionados con diferentes campos de la matemática y las ciencias computacionales. Se desempeñó como ingeniero en la Comisión Federal de Electricidad, donde desarrolló *software* para la simulación de problemas muy variados. Es autor de textos de matemáticas, ingeniería eléctrica e historia de la educación.

e-mail: gauss@cencar.udg.mx

**Alonso Castillo Ramírez** es licenciado en matemáticas por la Universidad de Guadalajara. Fue reconocido en la XXXVIII Ceremonia de Reconocimiento y Estímulo a Estudiantes Sobresalientes (CREES) en dicha institución. En 2010 obtuvo el grado de maestro en ciencias en matemáticas puras con distinción en el Imperial College de Londres. Recientemente le fue otorgada la Beca Internacional Imperial College para realizar el doctorado en matemáticas bajo la supervisión del profesor Alexander Ivanov. Su línea de investigación es la de representaciones de Majorana de grupos finitos.

e-mail: ac1209@imperial.ac.uk

**Elba Lilia de la Cruz García** egresó de la licenciatura en matemáticas de la Universidad de Guadalajara, en 2001. Fue reconocida en la XXII Ceremonia de Reconocimiento y Estímulo a Estudiantes Sobresalientes (CREES) en dicha institución. En 2005 obtuvo el grado de maestra en ciencias en matemáticas bajo la dirección del doctor Alexander Yakhno, en la Universidad de Guadalajara. Actualmente labora como profesora de tiempo completo del Centro Universitario de Ciencias Exactas e Ingenierías de la Universidad de Guadalajara y cuenta con perfil Promep.

e-mail: elba\_lilia@hotmail.com

***Alfonso Manuel Hernández Magdaleno*** se graduó de la licenciatura y la maestría en matemáticas de la Universidad de Guadalajara, en 1998 y 2003, respectivamente. Doctorado en ciencias en física por la Universidad de Guadalajara en 2008, bajo la dirección del doctor Vladimir N. Efremov. Es miembro del Sistema Nacional de Investigadores en el nivel de candidato y cuenta con perfil Promep. Actualmente es profesor de tiempo completo del Centro Universitario de Ciencias Exactas e Ingenierías de la Universidad de Guadalajara. Su línea de investigación es topología de dimensiones bajas y teoría del campo.  
e-mail: 137mag@gmail.com



