Miguel Ángel Goberna,
Valentín Jornet, Rubén Puente
y Margarita Rodríguez

Álgebra y fundamentos

Una introducción

Ariel Ciencia

Miguel Ángel Goberna es doctor en Matemáticas por la Universidad de Valencia, donde inició su actividad docente y es, en la actualidad, catedrático en la Universidad de Alicante. Ha escrito ocho libros relacionados con la educación matemática y una monografía sobre optimización publicada por J. Wiley, habiendo editado, además, una monografía sobre el mismo tema para Kluwer Publ. Ha publicado más de cincuenta artículos en revistas especializadas en optimización, investigación operativa, álgebra y análisis aplicados, didáctica de las matemáticas y educación.

Valentín Jornet es doctor en Matemáticas por la Universidad Complutense de Madrid, siendo en estos momentos catedrático de escuela universitaria en la Universidad de Alicante. Ha publicado tres libros de texto y artículos de investigación en revistas de optimización y de investigación operativa.

Rubén Puente es doctor en Ciencias Matemáticas por la Universidad Nacional de San Luis. Ha sido profesor en la Escuela Politécnica Nacional de Quito y en las universidades nacionales de Cuyo (Mendoza) y de San Luis, de la que es, actualmente, profesor asociado exclusivo efectivo. Ha elaborado documentos didácticos para el Servicio de Publicaciones de la ESPOL y artículos de investigación en revistas de álgebra, investigación operativa y optimización.

Margarita Rodríguez es licenciada en Matemáticas por la Universidad de Santiago y ha desarrollado su actividad profesional en las universidades de Oviedo y de Alicante, donde ocupa plaza de profesora titular de escuela universitaria.

Álgebra y fundamentos

Ariel

Ariel Ciencia

Miguel Ángel Goberna,
Valentín Jornet, Rubén Puente
y Margarita Rodríguez

Álgebra y fundamentos

Una introducción

Editorial Ariel, S.A.
Barcelona

Diseño cubierta: Vicente Morales

1.ª edición: septiembre 2000

© 2000: Miguel Ángel Goberna, Valentín Jornet,
Rubén Puente y Margarita Rodríguez

Derechos exclusivos de edición en español
reservados para todo el mundo:
© 2000: Editorial Ariel, S. A.
Provença, 260 - 08008 Barcelona

ISBN: 84-344-8026-3

Depósito legal: B. 34.922 - 2000

Impreso en España

Ninguna parte de esta publicación, incluido el diseño
de la cubierta, puede ser reproducida, almacenada o transmitida
en manera alguna ni por ningún medio, ya sea eléctrico,
químico, mecánico, óptico, de grabación o de fotocopia,
sin permiso previo del editor.

ÍNDICE

Prólogo 9

CAPÍTULO 1. **Introducción a la teoría de conjuntos** 13
1.1. Cálculo proposicional 14
1.2. Las operaciones conjuntistas 18
1.3. Correspondencias 22
1.4. Relaciones binarias 26
1.5. Problemas 31

CAPÍTULO 2. **Cardinales** 37
2.1. Números cardinales 39
2.2. Los números naturales: inducción 42
2.3. Comparación de cardinales 49
2.4. Conjuntos numerables 57
2.5. El cardinal del continuo 60
2.6. Proposiciones indemostrables 65
2.7. Teorías axiomáticas 69
2.8. Problemas 74

CAPÍTULO 3. **Grupos** 81
3.1. Operaciones binarias 82
3.2. Semigrupos, monoides y grupos 84
3.3. Los números enteros 91
3.4. Problemas 98

CAPÍTULO 4. **Anillos y cuerpos** 103
4.1. Anillos: los números enteros y congruencias 104
4.2. Anillos de polinomios 110
4.3. Cuerpos de fracciones: los racionales 115
4.4. Cuerpos ordenados 118
4.5. Problemas 125

CAPÍTULO 5. **El cuerpo de los números reales** 129
5.1. Sucesiones regulares en $\mathbb{Q}$ 130
5.2. El cuerpo ordenado de los números reales 134
5.3. La propiedad arquimediana 136
5.4. Completitud de los reales 141
5.5. Epílogo 147
5.6. Problemas 150

CAPÍTULO 6. **El cuerpo de los números complejos** 155
6.1. Los números complejos 156
6.2. Formas polar y exponencial 160
6.3. Ecuaciones algebraicas con coeficientes complejos 166
6.4. Ecuaciones algebraicas con coeficientes reales 169
6.5. Problemas 172

CAPÍTULO 7. **Extensiones de cuerpos y sus aplicaciones** 175
7.1. Extensiones de cuerpos 176
7.2. La ecuación funcional de Cauchy 182
7.3. Números construibles con regla y compás 187
7.4. Imposibilidad de los tres problemas clásicos 189
7.4.1. *Duplicación del cubo* 189
7.4.2. *Trisección del ángulo* 189
7.4.3. *Cuadratura del círculo* 190
7.5. Problemas 191

Soluciones a los problemas 193
Bibliografía 209
Índice alfabético 215

PRÓLOGO

La extensión de la enseñanza obligatoria hasta los 16 años en muchos países ha tenido como primera consecuencia la proliferación de asignaturas que se corresponden con el interés inmediato de la mayoría de jóvenes (informática, técnicas audiovisuales, teatro, economía, educación para la salud, etcétera), en detrimento de las disciplinas humanísticas y científicas, cuyos horarios se han visto reducidos drásticamente. A ello hay que añadir, en el caso español, la canalización de todo el alumnado a través de una vía única, que hace compartir las aulas a estudiantes con demandas de formación contrapuestas –académica para unos, profesional para otros–, cuando no carentes de cualquier interés por aprender, como es el caso de los llamados «objetores escolares». Como consecuencia del recorte de los horarios y de la falta de diversificación curricular, los profesores de enseñanza media, a pesar de sus esfuerzos por mantener el orden en el aula y por atraer el interés de grupos tan heterogéneos, contemplan impotentes la promoción automática de alumnos con una deficiente expresión oral y escrita o que a duras penas son capaces de utilizar correctamente las operaciones aritméticas.

Por lo que se refiere a la enseñanza de las matemáticas, es un hecho constatado que muchos estudiantes acceden a la universidad sin dominar el álgebra elemental y sin la menor idea de lo que pueda ser un número complejo. También se constata la desaparición de la geometría euclídea del plano en las matemáticas no universitarias, aunque su espíritu siga planeando en el dibujo técnico que algunos estudiantes toman como asignatura optativa. Pero, con ser graves estas carencias, aún lo es más el desconocimiento generalizado del lenguaje matemático (incluido el conjuntista) y del método deductivo, pues la lógica ha sido eliminada de los programas de humanidades y las demostraciones de las proposiciones matemáticas son generalmente reemplazadas, en la enseñanza secundaria, por simples ejemplos ilustrativos.

Como su título expresa sucintamente, este pequeño libro es una **introducción al álgebra abstracta y a los fundamentos de las matemáticas**, y está concebido como texto para un curso de apreciación matemática, de los que se ofertan en los centros de formación del profesorado, o para un curso sobre fundamentos (o álgebra y fundamentos) de los que reciben los estudiantes de matemáticas, física e ingeniería. El término «introducción» que aparece en el título no hace referencia a la sencillez de los conceptos y de las demostracio-

nes, sino a la necesidad de volver a los temas aquí tratados por parte de los futuros matemáticos. En efecto, por lo que se refiere a los fundamentos, el estudiante deberá profundizar en la lógica matemática (estudiando cálculo de predicados), en los conjuntos infinitos (estudiando ordinales transfinitos) y en la teoría de conjuntos (estudiando alguna teoría axiomática); en el caso del álgebra abstracta, cuya presencia en este libro se limita al mínimo imprescindible para abordar la construcción de los sistemas numéricos y ciertos problemas clásicos, es evidente que el alumno necesitará ampliar sus conocimientos de las estructuras básicas (grupos, anillos, cuerpos y espacios vectoriales) y estudiar otras nuevas (módulos, álgebras, etc.).

El libro es fruto de la experiencia docente de los autores con alumnos de los primeros cursos en universidades españolas, argentinas y ecuatorianas, y tiene los siguientes objetivos:

1. Mejorar el conocimiento del lenguaje conjuntista y, en general, del **lenguaje matemático** (Capítulo 1).
2. Entrenar a los alumnos en el manejo del **método deductivo** (descrito en los Capítulos 1 y 2, pero utilizado a lo largo de todo el texto).
3. Introducir a los estudiantes en los **fundamentos de las matemáticas**. El estudio de los cardinales transfinitos en el Capítulo 2 puede parecer prematuro, pero el conocimiento de los conjuntos numerables es imprescindible para abordar el análisis matemático (Teorema de Lindelöf) o el cálculo de probabilidades (el conjunto de los puntos de discontinuidad de cualquier función de distribución es numerable).
4. Introducir las **estructuras algebraicas básicas**. En los Capítulos 3, 4 y 7 se estudian sucintamente los grupos, los anillos (incluyendo los anillos de polinomios), los cuerpos y los espacios vectoriales, respectivamente. Lo que se pretende es familiarizar a los alumnos con los axiomas, los conceptos y las propiedades fundamentales de estas estructuras.
5. Construir los **sistemas numéricos**, desde los números naturales (cardinales finitos) a los números complejos. En los Capítulos 3-6 se utilizan los conocimientos sobre álgebra básica para llevar a cabo la construcción de cada dominio numérico a partir del precedente (generalmente como estructura cociente). Para no recargar esta parte del libro hemos pasado de puntillas sobre los teoremas de unicidad, cuyo interés es difícil de explicar a los alumnos.
6. Proporcionar nociones básicas de **historia de las matemáticas**. Este objetivo se concreta en forma de notas históricas y en la atención prestada –a lo largo de todo el libro– a las construcciones con regla y compás, tornándose explícito en el Capítulo 7, donde se cierran negativamente tres problemas clásicos de la geometría griega mediante argumentos de álgebra básica, al tiempo que se discute la existencia de las bases infinitas (bases de Hamel) en espacios vectoriales.

En el caso de ser utilizado como texto para un curso cuatrimestral, puede ser necesario efectuar recortes en su contenido. Si los alumnos tomaron con anterioridad un curso de introducción al álgebra, pueden suprimirse totalmente las secciones 3.1 y 3.2, y parcialmente las 4.1, 4.2 y 4.3. Las secciones 2.4, 2.6, 2.7, 3.3, 4.3 y 5.5, así como el Capítulo 6 en su conjunto, son de fácil lectura, por lo que no requerirían ser expuestos en clase. El contenido de las secciones 5.3 y 5.4, relativamente difíciles, puede considerarse también propio

del análisis real, por lo que las pruebas podrían ser transferidas a la asignatura correspondiente (que posiblemente se desarrolle en paralelo). El Capítulo 7 es de lectura independiente, por lo que podría suprimirse en su totalidad (cosa que no aconsejamos por agrupar interesantes aplicaciones del álgebra abstracta a la resolución de importantes problemas clásicos de la geometría y de la teoría de funciones).

Aunque el libro contiene demostraciones de todos los resultados enunciados, excepto las relaciones entre las proposiciones indemostrables (Sección 2.6) y el Teorema Fundamental del Álgebra, puede ser conveniente eliminar algunas pruebas difíciles (como la del Teorema 2.1 –de Bernstein– o la de alguna proposición de la Sección 5.4, acerca de la completitud de la recta real) o que aporten escasas novedades metodólogicas (como algunas de la Sección 2.4, donde se discuten los diferentes casos posibles). Y es que la presentación deductiva de una materia no tiene por qué llevarse hasta sus últimas consecuencias, cuando el precio a pagar por ello es el agobio, el aburrimiento o la desmotivación del estudiante. Al profesor corresponde adaptar el contenido del curso a la madurez matemática de sus alumnos. Lo que es de todo punto imprescindible es la resolución y discusión de los ejercicios intercalados y de buena parte de los problemas seleccionados al final de cada capítulo (señalándose con un asterisco aquellos que encierran cierto grado de dificultad), que deben servir como test del aprovechamiento por parte del alumno. Para facilitar la autoevaluación, se incluyen al final las soluciones de los problemas propuestos.

LOS AUTORES

Alicante, enero de 2000

CAPÍTULO 1

INTRODUCCIÓN A LA TEORÍA DE CONJUNTOS

La teoría de conjuntos es una de las pocas disciplinas matemáticas atribuibles, en buena medida, a un solo autor, Georg Cantor, quien desarrolló, con la única ayuda de su amigo Dedekind, entre 1874 y 1899, una aritmética del infinito cuyos rudimentos se exponen en el Capítulo 2. Aunque sus resultados generaron una fuerte polémica hasta fin de siglo, geómetras como Klein (cuyo *Erlanger Programm* reducía la geometría al estudio de los grupos de transformaciones), analistas como Lebesgue (introductor de los conceptos de medida y de integral generalizada) y algebristas como Weber (autor de un famoso manual sobre álgebra abstracta) o Steinitz (artífice de importantes aportaciones a la teoría abstracta de cuerpos) convencieron a los matemáticos de las grandes ventajas que ofrecía el lenguaje conjuntista, hasta el punto de que el más famoso matemático de principios de siglo, David Hilbert, proclamó que «nadie nos arrojará del paraíso que Cantor ha creado para nosotros». Este punto de vista se impuso definitivamente con la publicación, a partir de 1938, de la gran enciclopedia estructuralista firmada por Nicolas Bourbaki, seudónimo de un grupo de grandes matemáticos franceses.

El propósito de este capítulo es introducir al lector en las formas más habituales del razonamiento matemático y, sobre todo, ampliar sus conocimientos acerca del lenguaje matemático. Este lenguaje se ha ido formando a lo largo de los siglos después de muchos intentos infructuosos. Así, de todos los sistemas de numeración introducidos a lo largo de la historia, se ha impuesto el árabe porque permite representar a cualquier número natural, por grande que sea, y facilita las operaciones aritméticas. Las civilizaciones griega y romana fueron muy avanzadas en ciertos temas, pero cuando un texto clásico habla de ejércitos con «innumerables soldados» no se trata de un tropo, sino de una carencia cultural. Suele decirse de forma un tanto abusiva que los babilonios (que utilizaban, por cierto, un sistema de numeración de base 60, nada menos) resolvían ecuaciones de primero y segundo grado cuando, de hecho, carecían de la notación que les permitiese escribirlas. En realidad, sabían resolver algorítmicamente problemas que ahora planteamos mediante ese tipo de ecuaciones. La representación actual de las ecuaciones es relativamente reciente. Así, el signo = data de 1557 (introducido por Recorde) y el uso de las letras del abecedario para representar coeficientes e incógnitas lo hemos heredado de la Italia del Renacimiento, no existiendo por entonces

una regla fija para elegir la representación de unos y otras. Viète reservó las vocales para representar las incógnitas y Descartes las últimas letras del abecedario, costumbre universalmente aceptada desde 1637. Norma tan sencilla nos ahorra preguntar cuál es la incógnita a despejar cuando se nos pide resolver una ecuación como $ax = b$. El empleo de una notación adecuada, sencilla y sugerente, facilita el cálculo y el razonamiento.

Se trata, por lo tanto, de un capítulo instrumental, repleto de definiciones y de convenios, tan formativo e ingrato como pueda serlo la gramática para un futuro escritor o el solfeo para el futuro músico. Consuélese el lector con la certeza de que le dará acceso a otros capítulos mucho más gratificantes.

1.1. Cálculo proposicional

Existe cierta semejanza entre la matemática y el ajedrez. Si nos invitan a jugar contra un programa de ordenador cuando la partida ya está iniciada, empezaremos analizando la posición que ocupan las piezas; a continuación diseñaremos un plan y lo pondremos en práctica utilizando las reglas del juego, a sabiendas de que el ordenador no aceptará movimientos ilegales. Si somos lo bastante agudos, y la posición inicial de las piezas lo permite, acabaremos por hacer jaque mate. Análogamente, si nos piden que demostremos un *teorema* (sentencia relativa a objetos matemáticos, también llamada *proposición* si se considera fácil de probar o menos importante, *corolario* si es consecuencia directa del resultado que le precede y *lema* si va a ser utilizado más tarde para demostrar otro resultado verdaderamente interesante), la *hipótesis* (condiciones que se suponen satisfechas) y la *tesis* (lo que se afirma que se cumple en esas condiciones) hacen las veces de situación inicial del tablero y jaque mate. De las condiciones contenidas en la hipótesis se irán derivando nuevas sentencias (comparables con las posiciones intermedias del tablero a lo largo de la partida) utilizando reglas lógicas de aceptación universal o convenida (como las reglas del juego en el caso del ajedrez), la última de las cuales deberá ser la tesis. Desgraciadamente, no basta con conocer las reglas del juego para ganar una partida de ajedrez, como tampoco basta con dominar las reglas lógicas para demostrar un teorema, pues, en el primer caso, podemos enfrentarnos con un rival –o programa– demasiado fuerte para nosotros y, en el segundo, la dificultad de la prueba puede ser insuperable. De lo dicho se desprende que los teoremas matemáticos son de naturaleza hipotético-deductiva en su presentación, aunque sea la inducción la que haya proporcionado la conjetura (que es al teorema lo que el embrión a la criatura), así como el esquema mental de la prueba. Hay que lamentar que los textos matemáticos casi siempre oculten –por economía del lenguaje o por mera costumbre– el papel de la inducción. Para lograr una prueba correcta es esencial tener un buen plan de acción, y para ello se requiere intuición, desarrollada ésta mediante la práctica (frecuentación de los objetos matemáticos, sobre todo analizando ejemplos) y el estudio. Sin embargo, lo primero que tiene que hacer el futuro matemático es conocer bien las reglas de la deducción y el lenguaje matemático, pues sólo así podrá optar a desarrollar las habilidades superiores. Hay que reconocer que este aprendizaje requiere esfuerzo, pero merece la pena intentarlo.

Una oración del lenguaje de la que tiene sentido afirmar que es verdadera (en cuyo caso decimos que su valor de verdad es 1) o falsa (valor 0) se denomi-

na, en lógica, **proposición**. Son proposiciones, por ejemplo, «Felipe II fue rey de España», «Las bicicletas tienen seis ruedas» o «El cuarto decimal de π es 7». Cada una de ellas es verdadera o falsa, no hay posible ambigüedad. Por el contrario, no son proposiciones las oraciones «¿Qué tal estás?», «No te asomes a la ventana» o «La función $f(x) = \cos x$ es conmutativa». Las oraciones interrogativas o imperativas no tienen ningún valor de verdad y, por otra parte, la última oración es ambigua, puesto que no existe ninguna definición aceptada de conmutatividad aplicada a las funciones (si alguna vez se estableciese dicha definición, este ejemplo se convertiría en una proposición).

Las proposiciones se combinan mediante conjunciones gramaticales (y, o, ni,...), o expresiones sustitutorias, para obtener nuevas proposiciones. Desgraciadamente, el lenguaje ordinario es ambiguo: si alguien nos dice que, en cierto lugar, hoy «llueve o hace frío», no sabemos si se excluye la posibilidad de que ocurran ambas cosas a la vez; si, alternativamente, se nos dice que «si llueve, no hace frío» podemos entender que se está afirmando la existencia de una relación causal entre ambos fenómenos o que tan sólo se constata un hecho empírico. De ahí que convenga precisar el significado de los **operadores lógicos** en función de la verdad o falsedad de las proposiciones conectadas. Así, acordaremos que la **disyunción** (denotada por $\vee$) de dos proposiciones es falsa tan sólo cuando lo son las dos proposiciones conectadas, que la **conjunción** ($\wedge$) es verdadera tan sólo cuando lo son ambas partes, que la **implicación** ($\Longrightarrow$) sólo es falsa cuando el antecedente es verdadero y el consecuente falso, mientras que la **doble implicación** o **equivalencia** ($\Longleftrightarrow$) es verdadera si, y solamente si, las dos proposiciones conectadas son simultáneamente verdaderas o falsas. Todos estos operadores son binarios por conectar dos elementos, mientras que la **negación** (que se representará superponiendo una línea) es un operador monario por afectar a una sola proposición, cuyo valor de verdad es el contrario al de la proposición negada. Estas definiciones se memorizan fácilmente recurriendo a las llamadas **tablas de verdad**, que expresan el valor de verdad (0 o 1) de la proposición compuesta en función del correspondiente a sus componentes.

Definición 1.1. *Se definen cuatro operadores lógicos binarios (disyunción, conjunción, implicación y equivalencia) y uno monario (la negación), a saber,*

p	q	$p \vee q$	$p \wedge q$	$p \Longrightarrow q$	$p \Longleftrightarrow q$
1	1	1	1	1	1
1	0	1	0	0	0
0	1	1	0	1	0
0	0	0	0	1	1

y

p	$\overline{p}$
1	0
0	1

.

Una proposición compuesta es una **tautología** cuando es siempre verdadera, cualquiera que sea el valor de verdad de las proposiciones simples que la forman (es decir, cuando la columna correspondiente en la tabla de verdad sólo contiene el valor 1).

Ejemplo 1.1. $((p \Longrightarrow q) \wedge (q \Longrightarrow p)) \Longleftrightarrow (p \Longleftrightarrow q)$ es una tautología. En efecto, teniendo en cuenta las definiciones,

p	q	$((p \Longrightarrow q) \wedge (q \Longrightarrow p))$	$((p \Longrightarrow q) \wedge (q \Longrightarrow p)) \Longleftrightarrow (p \Longleftrightarrow q)$
1	1	1 1 1	1
1	0	0 0 1	1
0	1	1 0 0	1
0	0	1 1 1	1

EJERCICIO 1.1. Demuéstrense las siguientes tautologías:

(1.1) $p \Longrightarrow p$.

(1.2) $((p \Longrightarrow q) \wedge (q \Longrightarrow p)) \Longleftrightarrow (p \Longleftrightarrow q)$.

(1.3) $((p \Longrightarrow q) \wedge (q \Longrightarrow r)) \Longrightarrow (p \Longrightarrow r)$.

(1.4) $(p \vee q) \Longleftrightarrow (q \vee p)$.

(1.5) $(p \wedge q) \Longleftrightarrow (q \wedge p)$.

(1.6) $p \Longrightarrow (p \vee q)$.

(1.7) $(p \wedge q) \Longrightarrow p$.

(1.8) $(p \vee p) \Longleftrightarrow p$.

(1.9) $(p \wedge p) \Longleftrightarrow p$.

(1.10) $\overline{\overline{p}} \Longleftrightarrow p$.

(1.11) $\overline{(p \vee q)} \Longleftrightarrow (\overline{p} \wedge \overline{q})$.

(1.12) $\overline{(p \wedge q)} \Longleftrightarrow (\overline{p} \vee \overline{q})$.

(1.13) $((p \Longrightarrow r) \wedge (q \Longrightarrow r)) \Longrightarrow ((p \vee q) \Longrightarrow r)$.

(1.14) $((p \vee q) \vee r) \Longleftrightarrow (p \vee (q \vee r))$.

(1.15) $((p \wedge q) \wedge r) \Longleftrightarrow (p \wedge (q \wedge r))$.

(1.16) $(p \wedge (q \vee r)) \Longleftrightarrow ((p \wedge q) \vee (p \wedge r))$.

(1.17) $(p \vee (q \wedge r)) \Longleftrightarrow ((p \vee q) \wedge (p \vee r))$.

(1.18) $(p \Longrightarrow q) \Longleftrightarrow ((p \vee q) \Longleftrightarrow q)$.

(1.19) $((p \Longrightarrow q) \wedge p) \Longrightarrow q$.

(1.20) $((p \Longrightarrow q) \wedge \overline{q}) \Longrightarrow \overline{p}$.

(1.21) $(p \Longrightarrow q) \Longleftrightarrow (\overline{q} \Longrightarrow \overline{p})$.

(1.22) $(\overline{p} \Longrightarrow (q \wedge \overline{q})) \Longrightarrow p$.

(1.23) $(p \Longrightarrow q) \Longleftrightarrow ((\overline{q} \wedge p) \Longrightarrow (r \wedge \overline{r}))$.

(1.24) $(p \Longrightarrow \overline{p}) \Longrightarrow \overline{p}$.

(1.25) $(p \Longrightarrow q) \Longleftrightarrow (q \vee \overline{p})$.

(1.26) $(p \Longrightarrow (q \vee r)) \Longleftrightarrow ((p \wedge \overline{q}) \Longrightarrow r)$.

Veamos algunas útiles consecuencias de las tautologías anteriores desde el punto de vista del razonamiento matemático:

a) Para probar (bajo cierta hipótesis) la equivalencia entre dos proposiciones matemáticas p y q, es decir, la proposición $p \Longleftrightarrow q$, bastará demostrar que $p \Longrightarrow q$ (**directo**) y $q \Longrightarrow p$ (**recíproco**) son verdaderas, de acuerdo con la tautología del Ejemplo 1.1. Además, es lo mismo probar $p \Longrightarrow q$ que probar $\overline{q} \Longrightarrow \overline{p}$, por (1.21).

b) Una **demostración por discusión de casos posibles** consiste en probar una proposición r viendo que, bajo la hipótesis, hay dos casos posibles (si son más de dos el argumento es similar); en el primero se cumple p; en el segundo se cumple q; si se demuestra que $p \Longrightarrow r$ y $q \Longrightarrow r$ son ciertas, puede concluirse que la tesis r se cumple necesariamente, por (1.13). Como $p \vee \overline{p}$ es tautología (llamada **principio del tercio excluso**), es frecuente tomar como casos posibles una proposición y su negación, aunque no es forzoso que los casos posibles se excluyan mutuamente (la negación de $p \wedge \overline{p}$ es otra tautología, llamada **principio de no contradicción**).

c) Si se prueba (siempre bajo la hipótesis) que $p \Longrightarrow q$ y se sabe que p es verdadero, entonces se cumple q por aplicación directa de (1.19). Este sencillo argumento fue denominado en el latín medieval **modus ponendo ponens** (es decir, añadiendo añades).

d) Si se prueba que $p \Longrightarrow q$ y se sabe que q es falso, entonces p es también falso, como consecuencia de (1.20). Es el denominado **modus tolendo tolens** (quitando quitas).

e) La **reducción al absurdo** consiste en probar p demostrando que su negación $\overline{p}$ implica una proposición y su contraria, es decir, una proposición del tipo $q \wedge \overline{q}$ (**contradicción**). En tal caso se cumplirá p en virtud de (1.22). También es usual para demostrar que $p \Longrightarrow q$ utilizar (1.23) y demostrar que $(\overline{q} \wedge p)$ implica una contradicción.

Ejemplo 1.2. Consideremos la proposición «si x es un número entero, entonces $x^2 \geq x$». Demostraremos que dicha proposición es verdadera por discusión de casos posibles.

Si denotamos por p y q las proposiciones «x es un número entero» y «$x^2 \geq x$», respectivamente, tendremos que demostrar que $p \Longrightarrow q$ es verdadera.

Si p es verdadera, entonces se verifica una de las siguientes proposiciones:

(i) $x < 0$, en cuyo caso $x^2 > 0 > x$ y se verifica q.

(ii) $x = 0$, por lo tanto $x^2 = 0 = x$ y también se verifica q.

(iii) $x = 1$, entonces se verifica que $x^2 = 1 = x$ y q es verdadera.

(iv) $x > 1$, por lo que $x^2 > x.1 = x$ y es verdadera q.

Ejemplo 1.3. Consideremos la proposición «si $a > 0$, entonces $1/a > 0$». Probaremos que esta proposición es verdadera por reducción al absurdo.

Denotaremos por p y q las proposiciones «$a > 0$» y «$1/a > 0$», respectivamente.

Si consideramos que p es verdadera, tenemos que probar que q también lo es. Supongamos que se verifica $\overline{q} \wedge p$, es decir, $(1/a \leq 0) \wedge (a > 0)$. Luego

$a\,(1/a) \leq a\,0$ y, por lo tanto, $1 \leq 0$, que, junto con $1 > 0$, constituye una contradicción.

Éstas son algunas de las reglas más comunes del razonamiento matemático, que se sobreentienden en las demostraciones de los textos para ahorrarle al lector los detalles aburridos (de igual forma que, al describir una partida de ajedrez a quienes ya conocen las reglas del juego, se enumeran los movimientos, pero no se explicita qué regla del juego se aplicó en cada paso). Sin embargo, un matemático tiene incorporadas en su estructura de pensamiento estas reglas y las usa correctamente, aunque no siempre sea consciente de ello. En este capítulo, excepcionalmente, presentaremos unas pocas pruebas muy detalladas.

1.2. Las operaciones conjuntistas

El concepto de **conjunto** (en inglés *set*, en alemán *Menge*, en francés *ensemble*) es tan básico que no podemos definirlo; a lo sumo podemos encontrar sinónimos como clase, colección, agregado, etc., que traen consigo ciertas connotaciones indeseables (por ejemplo, colección sugiere reunir, poner cerca, mientras que los objetos que componen un conjunto pueden estar alejados o ni siquiera estar relacionados por distancia alguna). Otro concepto primitivo (o indefinible) es la **relación de pertenencia** de un objeto o elemento a un conjunto, representada con el signo $\in$ (introducido por Peano en 1889). Nos gusta representar los conjuntos por letras latinas mayúsculas $(A, B, \ldots)$ y los elementos por letras latinas minúsculas $(a, b, \ldots)$, pero no siempre podremos hacerlo así, puesto que nada impide considerar conjuntos cuyos elementos son, a su vez, conjuntos. A un conjunto de conjuntos lo llamaremos a menudo **familia de conjuntos**, por razones fonéticas y para poner de relieve la naturaleza de sus elementos. Un conjunto se define **por extensión** si somos capaces de enunciar sus elementos: $A = \{a, b, c\}$ significa que los elementos de A son a, b y c (sólo se pueden definir por extensión conjuntos con una cantidad finita de elementos). Un conjunto se define **por comprehensión** a través de una **forma proposicional** definida sobre cierto conjunto de referencia E, es decir, mediante una expresión del lenguaje en la que aparece una variable (que suele escribirse x en la tradición de los algebristas del Renacimiento italiano) que es verdadera o falsa cuando la variable es sustituida por elementos de E: así, el conjunto de los dígitos pares es $\{0, 2, 4, 6, 8\}$; en este ejemplo el conjunto de referencia es el formado por los enteros del 0 al 9 (que forman el conjunto de los dígitos) y la forma proposicional es *x es un número par* (obsérvese que en la definición por extensión no se explicita el conjunto de referencia). Si la forma proposicional es verdadera para todos los elementos de E, entonces el conjunto que define es el propio E. Pero también podría ocurrir que la forma proposicional fuese siempre falsa; en tal caso, el conjunto carece de elementos, se denomina **vacío** y se denota $\emptyset$. Si x pertenece al conjunto A (es decir, x es elemento de A), se escribe $x \in A$. A partir de estos dos conceptos indefinibles, conjunto y pertenencia, podemos introducir las bien conocidas operaciones conjuntistas y otros conceptos que pueden ser nuevos para el lector.

Definición 1.2. *Dados dos conjuntos A y B, y un mismo conjunto de referencia E para ambos, se define su* ***unión****, $A \cup B$, como el conjunto de los elementos de E que pertenecen al menos a uno de ellos, es decir,*

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

De forma semejante se define su ***intersección****, $A \cap B$, mediante*

$$A \cap B = \{x \in E \mid x \in A \wedge x \in B\},$$

así como su ***diferencia****,*

$$A \setminus B = \{x \in E \mid x \in A \wedge \overline{x \in B}\} = \{x \in E \mid x \in A \wedge x \notin B\}.$$

El conjunto ***complementario*** *de A es $E \setminus A$. Se escribe $\overline{A}$.*

El resultado de estas operaciones binarias es independiente de cuál sea el conjunto de referencia elegido, con la condición de que contenga a ambos. Por esa razón no es necesario explicitar el conjunto de referencia, salvo en el caso del complementario.

Definición 1.3. *Si $I \neq \emptyset$ es un conjunto de índices y A_i es un conjunto para cada $i \in I$, se define la unión de la familia $\mathcal{C} = \{A_i\,,\ i \in I\}$ como el conjunto de los elementos que pertenecen al menos a uno de los conjuntos de la familia, es decir,*

$$\bigcup \mathcal{C} = \bigcup_{i \in I} A_i = \{x \mid \textit{existe } i \in I : x \in A_i\}.$$

De forma semejante, la intersección de la familia $\mathcal{C}$ es el conjunto de los elementos que pertenecen a todos los conjuntos de la familia,

$$\bigcap \mathcal{C} = \bigcap_{i \in I} A_i = \{x \mid x \in A_i \quad \textit{para todo } i \in I\}.$$

Definición 1.4. *Se dice que el conjunto A está* ***incluido*** *en B, o que B* ***contiene*** *a A, cuando $x \in A \Longrightarrow x \in B$ cualquiera que sea x. Se escribe $A \subset B$.*

Se dice que A es ***igual*** *a B si $A \subset B$ y $B \subset A$. Se escribe $A = B$.*

En matemática elemental se estudian de forma intuitiva los conjuntos numéricos $\mathbb{N}$ (naturales), $\mathbb{Z}$ (enteros), $\mathbb{Q}$ (racionales), $\mathbb{R}$ (reales) y $\mathbb{C}$ (complejos), que cumplen $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Ejemplo 1.4. Sean los conjuntos $E = \mathbb{N}$ e $I = \mathbb{N}\setminus\{1\}$. Considérese la familia de conjuntos $\{A_i\,,\ i \in I\}$, donde $A_i = \{ni \mid n \in I\}$ para $i \in I$. Es fácil comprobar que

$$\bigcap_{i \in I} A_i = \emptyset \qquad \text{y} \qquad \overline{\bigcup_{i \in I} A_i} = \{1\} \cup P,$$

donde P es el conjunto de los números primos.

Los teoremas de la teoría de conjuntos se derivan de las tautologías del cálculo proposicional. Por ejemplo, de la tautología $p \Longrightarrow p$ se deduce que $x \in A \Longrightarrow x \in A$ cualesquiera que sean x y A. De ahí que se cumpla la primera de las proposiciones conjuntistas que se enumeran en el siguiente ejercicio.

EJERCICIO 1.2. Pruébense las siguientes proposiciones de la teoría de conjuntos:

(2.1) $A \subset A$.

(2.2) $[(A \subset B) \wedge (B \subset A)] \Longleftrightarrow (A = B)$.

(2.3) $[(A \subset B) \wedge (B \subset C)] \Longrightarrow (A \subset C)$.

(2.4) $A \cup B = B \cup A$.

(2.5) $A \cap B = B \cap A$.

(2.6) $A \subset A \cup B$.

(2.7) $A \cap B \subset A$.

(2.8) $A \cup A = A$.

(2.9) $A \cap A = A$.

(2.10) $\overline{\overline{A}} = A$.

(2.11) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$.

(2.12) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.

(2.13) $[(A \subset C) \wedge (B \subset C)] \Longrightarrow [(A \cup B) \subset C]$.

(2.14) $(A \cup B) \cup C = A \cup (B \cup C)$.

(2.15) $(A \cap B) \cap C = A \cap (B \cap C)$.

(2.16) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(2.17) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(2.18) $(A \subset B) \Longleftrightarrow (A \cup B = B)$.

Algunos de estos sencillos teoremas de la teoría de conjuntos son de uso tan frecuente que reciben un nombre: (2.1), (2.2) y (2.3) son las propiedades **reflexiva**, **antisimétrica** (utilizada para probar la igualdad de dos conjuntos) y **transitiva** de la inclusión; (2.4) y (2.5) expresan las propiedades **conmutativas**, de la unión y de la intersección, respectivamente; (2.11) y (2.12) son las **leyes de complementación** o de **De Morgan**; (2.14) y (2.15) expresan la propiedad **asociativa** de la unión y de la intersección, respectivamente; para terminar, (2.16) y (2.17) son las propiedades **distributivas** de cada una de las dos operaciones respecto de la otra.

EJERCICIO 1.3. Compruébese que cualquier familia de conjuntos $\{A_i\,,\ i \in I\}$ satisface las leyes de De Morgan generalizadas:

(3.1) $\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}$.

$$(3.2) \quad \overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}\,.$$

Acabaremos esta sección con dos conceptos muy útiles. El primero es el de conjunto de las **partes de un conjunto**, que es aquel que resulta de considerar como elementos todos sus subconjuntos, incluidos el menor, $\emptyset$, y el mayor (el propio conjunto) desde el punto de vista de la inclusión. El segundo concepto es el de **producto cartesiano** de dos conjuntos dados en un cierto orden, que está formado por todos los pares ordenados que pueden formarse a partir de aquellos conjuntos. Esta noción de par ordenado puede definirse, aunque a primera vista parezca tan básica como los conceptos primitivos introducidos al comienzo de esta sección (conjunto y pertenencia).

Definición 1.5. *El conjunto de las **partes de un conjunto** A es*

$$\mathcal{P}(A) = \{X \mid X \subset A\}\,.$$

*Un conjunto que tiene un único elemento se dice que es **singular**. Un conjunto con dos elementos se dice que es una **pareja**.*

Dados dos conjuntos no vacíos A y B, y elementos respectivos $a \in A$ y $b \in B$, el conjunto

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

*es un **par ordenado**.*

*El **producto cartesiano** de* A *por* B *es*

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

Desde luego, $\{\emptyset, A\} \subset \mathcal{P}(A)$; en particular, si $A = \emptyset$ entonces $\mathcal{P}(A) = \{\emptyset\}$ es singular. Cuando $A \neq \emptyset$ son singulares los conjuntos $\{a\} \in \mathcal{P}(A)$, para cada $a \in A$.

Un par ordenado (a,b) es un conjunto, que puede ser singular (cuando $a = b$) o una pareja.

Obviamente, $A \times B = \emptyset$ si, y sólo si, uno de los dos conjuntos es vacío. En particular, cuando $B = A$, se escribe A^2 en lugar de $A \times A$ (el conjunto de los pares ordenados de elementos de A).

Proposición 1.1. *$(a,b) = (x,y)$ si, y sólo si, $x = a$ e $y = b$.*

Demostración. Como el recíproco ($\Leftarrow$) es evidente, bastará probar el directo ($\Rightarrow$). Supondremos que $(a,b) = (x,y)$. Distinguiremos dos casos posibles:

Caso 1: $a = b$. Como $\{a,b\}$ es un conjunto singular, (a,b) está formado por dos conjuntos singulares (e iguales), y lo mismo le ocurrirá a (x,y), por la hipótesis, de manera que $\{x,y\}$ también es singular y deberá ser $x = y$. Se tiene entonces

$$\{\{a\}\} = (a,b) = (x,y) = \{\{x\}\}\,. \tag{1.1}$$

De la igualdad (1.1) se sigue que $\{a\} = \{x\}$, por lo que $b = a = x = y$.

Caso 2: $a \neq b$. Ahora (a,b) está formado por el conjunto singular $\{a\}$ y la pareja $\{a,b\}$, de modo que, por la hipótesis, (x,y) también estará formado por un conjunto singular y una pareja, que deberán ser $\{x\}$ y $\{x,y\}$, debiendo cumplirse

$$\{a\} = \{x\} \tag{1.2}$$

y

$$\{a,b\} = \{x,y\}\,. \tag{1.3}$$

De (1.2) se tiene que $a = x$. Usando (1.3), al ser iguales los elementos a y x de ambas parejas, también deberán ser iguales b e y, según prueba la siguiente reducción al absurdo: si suponemos $y \neq b$, como $y \in \{a,b\}$, deberá ser $y = a = x$, y esto es imposible porque $\{x,y\}$ es pareja en este caso. □

1.3. Correspondencias

El término *correspondencia* del lenguaje ordinario es sinónimo de asociación: a cada ser humano se le pueden asociar sus progenitores vivos (con lo que a cada persona le podrán corresponder dos personas, una o, en el peor caso, ninguna); a cada ojal de una chaqueta un botón o ninguno;... Este concepto se puede definir con ayuda del producto cartesiano.

Definición 1.6. *Sean A y B dos conjuntos dados no vacíos, a los que llamaremos* ***conjunto inicial*** *(o* ***dominio****) y* ***conjunto final*** *(o* ***codominio****). Una* ***correspondencia*** *de A en B es un subconjunto no vacío G del producto cartesiano $A \times B$. Dicho subconjunto también recibe el nombre de* ***grafo de la correspondencia****.*

Sea G una correspondencia de A en B. Si $(a,b) \in G$, se dice que b es una ***imagen*** *de a, o que a es una* ***preimagen*** *de b. El* ***conjunto imagen*** *(de A) está formado por todas las imágenes de los elementos de A y el* ***conjunto preimagen*** *(de B) está formado por todas las preimágenes de los elementos de B.*

Ejemplo 1.5. Sean $A = \{a,b,c\}$ (conjunto inicial) y $B = \{\alpha,\beta,\gamma,\delta\}$ (conjunto final) para las correspondencias $G = \{(a,\alpha),(a,\beta),(b,\beta),(c,\gamma)\}$ y $F = \{(a,\alpha),(b,\beta),(c,\gamma)\}$. Representando cada par (x,y) del grafo mediante una flecha que une x con y se obtienen los diagramas sagitales de G y de F (véase Figura 1.1). En ambas correspondencias, el conjunto preimagen es A y el conjunto imagen es $\{\alpha,\beta,\gamma\}$.

Definición 1.7. *Una correspondencia de A en B tal que cada elemento de A tiene exactamente una imagen, se dice que es una* ***aplicación****. Se denotarán mediante letras latinas minúsculas seguidas de una flecha entre los conjuntos inicial y final, como*

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto f(x)\,. \end{aligned}$$

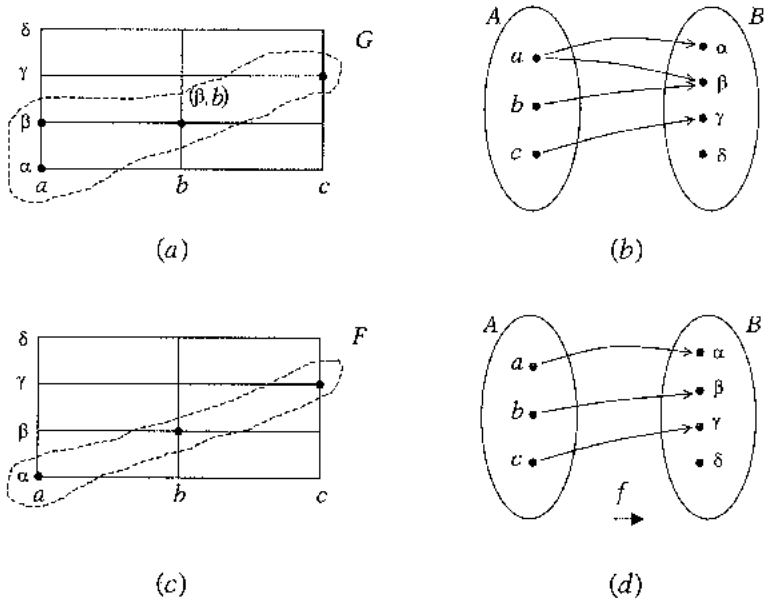

Figura 1.1. *(a) Grafo de G (cada punto de la rejilla representa un elemento de $A \times B$); (b) diagrama sagital de G; (c) grafo de F; (d) diagrama sagital de F.*

La aplicación $f : A \longrightarrow B$ es ***inyectiva*** *(o* ***uno-a-uno****) cuando elementos distintos de A tienen imágenes distintas, es decir,*

$$a_1 \neq a_2 \Longrightarrow f(a_1) \neq f(a_2),$$

cualesquiera que sean $a_1, a_2 \in A$.

La aplicación $f : A \longrightarrow B$ es ***suprayectiva*** *(o* ***sobre****) cuando para todo $b \in B$ existe al menos un $a \in A$ tal que $f(a) = b$.*

Una aplicación se dice que es ***biyectiva*** *(o* ***biunívoca****) cuando es inyectiva y suprayectiva (uno a uno y sobre).*

Dado un conjunto $A \neq \emptyset$, la correspondencia de A en sí mismo de grafo $G = \{(a,a) \mid a \in A\}$ es una aplicación biyectiva llamada ***identidad****, que denotaremos por I_A.*

Dada una aplicación $f : A \longrightarrow B$ y un subconjunto no vacío $C \subset A$, se denomina ***restricción*** *de f al subconjunto C a la aplicación $f_{|C} : C \longrightarrow B$ tal que $f_{|C}(x) = f(x)$ para todo $x \in C$.*

Si $f : A \longrightarrow B$ es una aplicación de grafo $\{(a, f(a)) \mid a \in A\} \subset A \times B$, la imagen de un subconjunto $A' \subset A$ se denota

$$f(A') = \{b \in B \mid \text{existe } a \in A' : b = f(a)\}$$

y la preimagen de $B' \subset B$ es

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}.$$

En particular, $f^{-1}(B) = A$ y la aplicación f es suprayectiva cuando $f(A) = B$.

En el Ejemplo 1.5, la correspondencia F es una aplicación (que denotaremos por f), mientras que G no lo es (puesto que a tiene dos imágenes). Además, se tiene $f(A) = \{\alpha, \beta, \gamma\} \neq B$, por lo que f no es suprayectiva ni biyectiva, aunque sí es inyectiva (véase en Figura 1.1.(d) que ningún par de flechas concurren en un mismo elemento de B).

Cuando los conjuntos inicial y final están formados por números, la aplicación se llama **función**.

Si $A \subset \mathbb{R}$ y $B \subset \mathbb{R}$, la función $f : A \longrightarrow B$ es una **función real de variable real**, que es la clase de funciones que se estudia en la enseñanza media. En tal caso, $f \subset A \times B \subset \mathbb{R}^2$ es un conjunto de pares ordenados de números reales que se representan en el plano cartesiano, con ejes ortogonales, de la forma conocida. El grafo de tal correspondencia se denomina **gráfica** de f, y cumple la condición de que las rectas verticales por los puntos del conjunto A (representado sobre el eje de abscisas) contienen un único punto de la gráfica. Además, el conjunto imagen $f(A) \subset B$ se visualiza proyectando la gráfica sobre el eje de ordenadas. Por otro lado, f es inyectiva si toda recta horizontal intersecta a la gráfica a lo sumo en un punto y es suprayectiva si toda recta horizontal por los puntos de B (sobre el eje de ordenadas) intersecta a la gráfica en al menos un punto.

Ejemplo 1.6. La expresión $f(x) = \sqrt{1 - x^2}$ define informalmente una función cuyo dominio se sobreentiende que está formado por los números reales que al ser sustituidos en la expresión producen un número real, es decir, $A = \{x \in \mathbb{R} \mid 1 - x^2 \geq 0\} = [-1, 1]$, mientras que el codominio es, implícitamente, $\mathbb{R}$. Es fácil probar que $(x, y) \in \mathbb{R}^2$ pertenece a la gráfica de f si, y sólo si, es un punto de la circunferencia unidad $x^2 + y^2 = 1$ (de centro en el origen de coordenadas y radio unidad) y del semiplano superior $y \geq 0$ (véase Figura 1.2). Por lo tanto, $f(A) = [0, 1]$, y f no es inyectiva ni suprayectiva. En cambio, $f_{|[0,1]}$ es inyectiva.

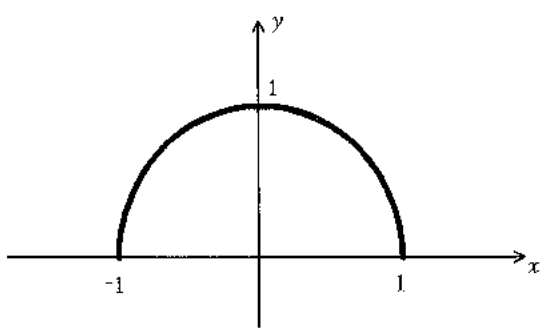

Figura 1.2. *Gráfica de* $f(x) = \sqrt{1 - x^2}$.

Definición 1.8. *Sean F y G dos correspondencias de A en B y de B en C, respectivamente. El conjunto*

$$\{(a, c) \in A \times C \mid \textit{existe } b \in B : (a, b) \in F \wedge (b, c) \in G\},$$

si no es vacío, define una correspondencia de A en C denominada ***composición*** *de F y G. Se denota $G \circ F$ (obsérvese el orden).*

Definición 1.9. *Dada una correspondencia G de A en B, se define la* ***correspondencia inversa*** *G^{-1} de B en A por*

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

Si $A \subset \mathbb{R}$ y $B \subset \mathbb{R}$, entonces el grafo de G^{-1} es el conjunto simétrico del grafo de G respecto de la recta $y = x$ (bisectriz del primer cuadrante). Para la función $f_{|[0,1]}$ del Ejemplo 1.6, su inversa es ella misma.

Proposición 1.2. *Dadas las aplicaciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$, las siguientes proposiciones son ciertas:*

(i) *$g \circ f$ es aplicación. Además, se cumple que $(g \circ f)(x) = g(f(x))$, para todo $x \in A$.*

(ii) *f^{-1} es aplicación si, y sólo si, f es biyectiva.*

(iii) *Si f y g son inyectivas (suprayectivas, biyectivas), entonces $g \circ f$ es, asimismo, inyectiva (suprayectiva, biyectiva, respectivamente).*

(iv) *Si f y g son biyectivas, se tiene $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Demostración. (i) Dado $a \in A$ arbitrario, existe un único $b \in B$ tal que $(a,b) \in f$. Para dicho b también existe un único $c \in C$ tal que $(b,c) \in g$. Entonces, existe un único $c \in C$ tal que $(a,c) \in g \circ f$. Por lo tanto, $g \circ f$ es aplicación. Como $b = f(a)$, $c = g(b) = g(f(a))$ y también $c = (g \circ f)(a)$, se tiene que

$$(g \circ f)(a) = g(f(a)) \tag{1.4}$$

para todo $a \in A$ (ya que a era arbitrario).

(ii) Probaremos, en primer lugar, el directo. Supongamos que f no es inyectiva. Entonces existen dos elementos $x \neq y$ en A, tales que $f(x) = f(y) = z \in B$. Se tiene entonces que $(x,z) \in f$ y $(y,z) \in f$, por lo que $(z,x) \in f^{-1}$ y $(z,y) \in f^{-1}$. En ese caso, z tendría dos imágenes y f^{-1} no sería aplicación. Así pues, si f^{-1} es aplicación, f es inyectiva. También f es suprayectiva, ya que para $b \in B$ arbitrario existe un único $a \in A$ tal que $(b,a) \in f^{-1}$, luego $(a,b) \in f$, es decir, existe $a \in A$ tal que $f(a) = b$.

Para probar el recíproco supondremos que f es biyectiva. Sea $b \in B$ arbitrario. Por ser f suprayectiva, existe $a \in A$ tal que $f(a) = b$, es decir, $(a,b) \in f$. Por ser f inyectiva, dicho a es único. En otras palabras, para cada $b \in B$ existe un único $a \in A$ tal que $(b,a) \in f^{-1}$, de modo que f^{-1} es aplicación.

(iii) Supongamos que f y g son inyectivas. Dados dos elementos $x \neq y$ en A, se tiene que $f(x) \neq f(y)$. Entonces, usando (1.4) y la inyectividad de g,

$$(g \circ f)(x) = g(f(x)) \neq g(f(y)) = (g \circ f)(y).$$

Supongamos ahora que f y g son suprayectivas. Dado $c \in C$ existe $b \in B$ tal que $g(b) = c$ y también existe $a \in A$ tal que $f(a) = b$. Puesto que

$$(g \circ f)(a) = g(f(a)) = g(b) = c,$$

se concluye que todo elemento de C tiene preimagen por $g \circ f$.

Que la composición de aplicaciones biyectivas lo es también, es consecuencia de las dos afirmaciones previas.

(iv) Usando (ii), f^{-1} y g^{-1} son aplicaciones, luego la composición $f^{-1} \circ g^{-1}$ también lo es. Por (iii) se tiene que $(g \circ f)^{-1}$ es una aplicación. Para demostrar la igualdad bastará con ver que proporcionan la misma imagen para cualquier $c \in C$. En efecto, sea $b = g^{-1}(c)$ y sea $a = f^{-1}(b)$. Como $(g \circ f)(a) = c$, se tiene

$$(g \circ f)^{-1}(c) = a = f^{-1}\left(g^{-1}(c)\right) = \left(f^{-1} \circ g^{-1}\right)(c).$$

Es decir, $(c,a) \in (g \circ f)^{-1}$ si, y sólo si, $(c,a) \in \left(f^{-1} \circ g^{-1}\right)$, por lo que ambas aplicaciones tienen igual grafo. Por lo tanto $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

1.4. Relaciones binarias

Definición 1.10. *Una **relación binaria** G sobre un conjunto $A \neq \emptyset$, que denotaremos (A,G), es una correspondencia G de A en A, es decir, G es un subconjunto de A^2.*

Una relación binaria (A,G) se dice que es:

$$\begin{cases} \text{(R)}\textbf{\textit{reflexiva:}}\ (x,x) \in G \text{ para todo } x \in A; \\ \text{(T)}\textbf{\textit{transitiva:}}\ [(x,y) \in G \wedge (y,z) \in G] \Longrightarrow (x,z) \in G \text{ para todo } x,y,z \in A; \\ \text{(S)}\textbf{\textit{simétrica:}}\ (x,y) \in G \Longrightarrow (y,x) \in G \text{ para todo } x,y \in A; \\ \text{(A)}\textbf{\textit{antisimétrica:}}\ [(x,y) \in G \wedge (y,x) \in G] \Longrightarrow x = y, \text{ para todo } x,y \in A. \end{cases}$$

La noción de relación binaria es de gran importancia en matemáticas, en particular en temas como teoría de la decisión, teoría de elección social o teoría de votaciones, disciplinas que pretenden explicar el comportamiento de los agentes (especialmente económicos), tanto individuales como colectivos, que eligen o deciden en función de sus preferencias sobre un conjunto de elecciones posibles. Nos concentraremos en las relaciones binarias de equivalencia y de orden, que usaremos en nuestra fundamentación de los conjuntos numéricos, y que son de utilidad también en álgebra y en análisis.

Definición 1.11. *Una relación binaria que es reflexiva, transitiva y simétrica se dice que es una **relación de equivalencia** (**RBE** para abreviar).*

Si en un conjunto de personas se considera la relación consistente en compartir el signo zodiacal, o el municipio de nacimiento, tenemos una relación de equivalencia. En el conjunto de las fracciones con numerador entero y denominador entero positivo se pueden relacionar a/b y c/d cuando $ad = bc$. Esto define una relación de equivalencia sobre tales fracciones (obsérvese que 1/2 está relacionado con 2/4, pero son fracciones diferentes a pesar de que representan el mismo número racional).

Definición 1.12. *Si G define una RBE sobre A, y $(x,y) \in G$, se dice que x e y son* ***equivalentes****. Es común escribir, entonces, $x \sim y$, por lo que nos referiremos indistintamente al par (A, G) o al par $(A, \sim)$. El conjunto de todos los elementos de A que son equivalentes a $x \in A$ es la* ***clase de equivalencia*** *de x, que se denota por $[x]$, es decir, $[x] = \{y \in A \mid x \sim y\}$. Cualquier elemento de una clase se denomina* ***representante*** *de dicha clase.*

El conjunto cuyos elementos son las clases de equivalencia de $(A, \sim)$ se denomina ***conjunto cociente****. Se denota mediante $A/\sim$, o bien por*

$$A/G = \{[x] \mid x \in A\}.$$

Cuando se consideran los seres humanos relacionados a través de su signo zodiacal, el conjunto cociente tiene 12 elementos (clases de equivalencia), pudiéndose hacer afirmaciones del siguiente tenor acerca de los elementos de una clase: «los aries son belicosos», «los leo son ambiciosos», etc. Con respecto a las fracciones, cada clase de equivalencia representa, según sabemos, un número racional: $[1/2] = \{1/2, 2/4, 3/6, \ldots\}$. En este caso, el conjunto cociente es el conjunto de los números racionales $\mathbb{Q}$.

Ejemplo 1.7. Se define sobre $\mathbb{R}$ la siguiente relación de equivalencia: dos números reales x e y están relacionados si $x = y + 2k\pi$ para algún entero k, es decir,

$$x \sim y \Longleftrightarrow (x - y)/2\pi \in \mathbb{Z}.$$

Por lo tanto, en cada clase de equivalencia se identifican todos los números reales que se diferencian en un múltiplo entero de 2π. Es posible, entonces, pensar que cada clase de equivalencia es un ángulo. Si denotamos por S^1 la circunferencia unidad $x^2 + y^2 = 1$ en el plano, la aplicación biyectiva

$$\begin{aligned} f : \mathbb{R}/\sim &\longrightarrow S^1 \\ [x] &\longmapsto (\cos x, \operatorname{sen} x) \end{aligned}$$

está bien definida (no depende de representantes) y permite identificar S^1 con $\mathbb{R}/\sim$ (véase Figura 1.3).

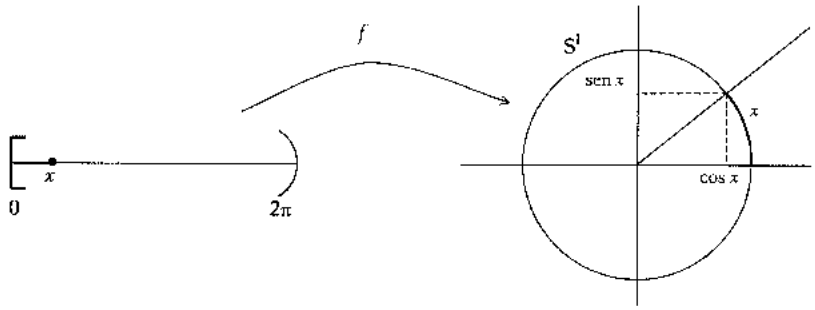

Figura 1.3. *Todo número real tiene un representante $x \in [0, 2\pi[$, y $f([x])$ es el punto $(\cos x, \operatorname{sen} x) \in S^1$.*

Proposición 1.3. *Toda RBE sobre A define una* ***partición*** *de A, es decir, la unión de todas las clases de equivalencia es A y dos clases diferentes cualesquiera son disjuntas. Recíprocamente, toda partición de A da lugar a una RBE sobre A cuyas clases de equivalencia son los conjuntos de la partición.*

Demostración. Empezaremos probando que las clases de equivalencia constituyen una partición de A.

Por la propiedad reflexiva (R), cada elemento de A pertenece a la clase de equivalencia que define, es decir $x \in [x]$. Por lo tanto $A \subset \cup_{x \in A} [x]$, mientras que el recíproco, $\cup_{x \in A} [x] \subset A$, se cumple trivialmente.

Si $[x] \cap [y] \neq \emptyset$ entonces existe $z \in A$ tal que $z \in [x] \cap [y]$. Esto significa que $x \sim z$ y que $y \sim z$. Por (S) y (T) se tiene $x \sim y$, de modo que, si $w \in [y]$ se tendrá $y \sim w$, por lo que $x \sim w$ y, con ello, $w \in [x]$. Hemos probado así que $[y] \subset [x]$. Como los papeles de x y de y son intercambiables, se tiene también $[x] \subset [y]$, de donde $[x] = [y]$. Por lo tanto, si $[x] \neq [y]$ entonces $[x] \cap [y] = \emptyset$.

Supongamos, para terminar la prueba, que $\mathcal{C}$ es una familia de conjuntos no vacíos, disjuntos dos a dos tal que su unión es A. Sea $G \subset A^2$ la relación binaria definida por

$$(x, y) \in G \Longleftrightarrow \text{existe } B \in \mathcal{C} : x \in B \wedge y \in B. \tag{1.5}$$

Es fácil comprobar que la relación G definida en (1.5) es RBE (en la que dos elementos de A son equivalentes si, y sólo si, pertenecen a un mismo conjunto de la partición). □

Definición 1.13. *Una relación binaria sobre un conjunto A que es reflexiva, transitiva y antisimétrica se dice que es una* ***relación de orden*** *(**RBO** para abreviar). Se dice entonces que A está ordenado por dicha RBO.*

Las RBE anteriores no son RBO. La relación binaria $\leq$ sobre las fracciones con denominador positivo, definida por $a/b \leq c/d$ cuando $ad \leq bc$, no es RBE ni RBO por fallar (S) (ya que $1/3 \leq 1/2$, pero no es cierto que $1/2 \leq 1/3$), al igual que (A) (pues $2/4 \leq 1/2$ y $1/2 \leq 2/4$, pero son fracciones diferentes, aunque representan el mismo número racional). Sin embargo, el orden conocido sobre los números racionales, $\leq$, establece una RBO sobre $\mathbb{Q}$.

Para cualquier conjunto E, la relación de inclusión en $\mathcal{P}(E)$ produce una RBO (véase Figura 1.4).

Si G define una RBO sobre A, suele escribirse el par $(A, \preceq)$ en lugar de (A, G), reemplazando $(x, y) \in G$ por $x \preceq y$.

Para cada RBO $(A, \preceq)$ se define una relación binaria asociada, $\prec$, por

$$x \prec y \Longleftrightarrow (x \preceq y \wedge x \neq y). \tag{1.6}$$

La relación definida en (1.6) no es RBO (ni, por supuesto, RBE), pero cumple (T) y satisface otra propiedad, denominada **antirreflexiva**: $x \not\prec x$ para todo $x \in A$.

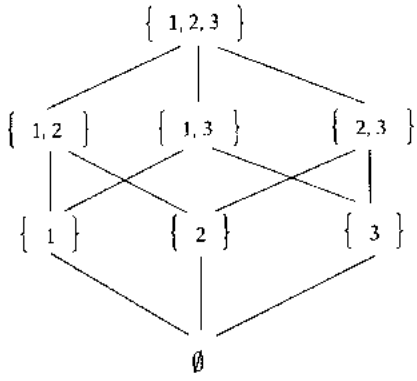

Figura 1.4. *El diagrama ilustra la ordenación de* $(\mathcal{P}(\{1,2,3\}), \subset)$.

Definición 1.14. *En un conjunto ordenado* $(A, \preceq)$ *pueden existir elementos notables. Decimos que* $a \in A$ *es:*

$$\begin{cases} \textbf{\textit{mínimo}} \text{ (o } \textbf{primer elemento}\text{) de } A \text{ si } a \preceq x, \text{ para todo } x \in A. \\ \textbf{\textit{máximo}} \text{ (o } \textbf{último elemento}\text{) de } A \text{ si } x \preceq a, \text{ para todo } x \in A. \\ \textbf{\textit{minimal}}\text{: } x \preceq a \Longrightarrow x = a, \text{ para todo } x \in A \text{ (no hay elemento anterior a } a\text{).} \\ \textbf{\textit{maximal}}\text{: } a \preceq x \Longrightarrow x = a, \text{ para todo } x \in A \text{ (no hay elemento posterior a } a\text{).} \end{cases}$$

$(\mathbb{Q}, \leq)$ carece de tales elementos. En cambio, $(\mathcal{P}(E), \subset)$ tiene a $\emptyset$ como mínimo y minimal, y a E como máximo y maximal. Como consecuencia de la propiedad antisimétrica (A), el máximo y el mínimo son únicos cuando existen, y son maximal y minimal respectivamente. Si no existe máximo (o mínimo), los elementos maximales (minimales) no son necesariamente únicos: si E es un conjunto con al menos dos elementos, $(\mathcal{P}(E) \setminus \{\emptyset\}, \subset)$ es ordenado y todos los conjuntos singulares son minimales, pero ya no existe mínimo (comparar con Figura 1.4).

Definición 1.15. *Supóngase que* (A, G) *es un conjunto ordenado,* $B \subset A$ *y* $G \cap B^2 \neq \emptyset$. *Entonces* $G \cap B^2$ *define un orden sobre* B *que se dice que está* ***inducido*** *por el de* A. *También se dice que el orden sobre* A ***extiende*** *el orden sobre* B. *Ambos se representan de la misma forma; por ejemplo,* $(A, \preceq)$ *y* $(B, \preceq)$.

Definición 1.16. *Para un conjunto ordenado* $(A, \preceq)$ *y un subconjunto* $B \subset A$, *decimos que un elemento* $a \in A$ *es:*

$$\begin{cases} \textbf{\textit{cota superior}} \text{ de } B \text{ cuando } b \preceq a, \text{ para todo } b \in B. \\ \textbf{\textit{cota inferior}} \text{ de } B \text{ cuando } a \preceq b, \text{ para todo } b \in B. \end{cases}$$

Ejemplo 1.8. La relación binaria en el plano $\mathbb{R}^2$ definida por:

$$(x_1, y_1) \preceq (x_2, y_2) \Longleftrightarrow (x_2 - x_1 \geq 0 \wedge y_2 - y_1 \geq 0),$$

es una RBO. Se denomina **orden parcial**, ya que, por ejemplo, los elementos $(1, 2)$ y $(2, 1)$ no son comparables entre sí (véase Figura 1.5). Ambos elementos son cotas superiores para el círculo unidad $x^2 + y^2 \leq 1$. Una cota inferior para la pareja $\{(1, 2), (2, 1)\}$ es el elemento $(1, 1)$.

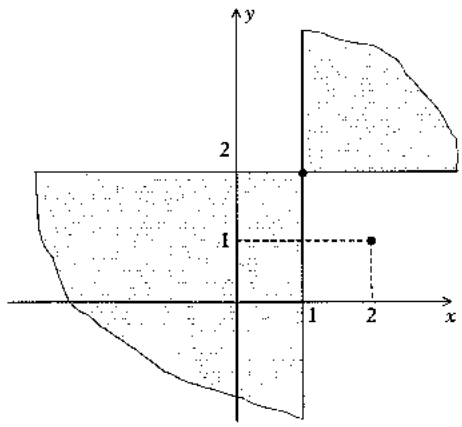

Figura 1.5. *La región sombreada muestra los elementos comparables con (1,2).*

Definición 1.17. *Dado un conjunto ordenado $(A, \preceq)$, se dice que está* ***totalmente ordenado*** *cuando dos elementos arbitrarios $x, y \in A$ siempre son comparables, lo que equivale a decir que se cumple una, y sólo una, de las condiciones $x \prec y$, $x = y$ o $y \prec x$ (**ley de tricotomía**).*

Definición 1.18. *Un conjunto ordenado $(A, \preceq)$, se dice que está* ***bien ordenado*** *cuando todo subconjunto no vacío, con el orden inducido, tiene primer elemento.*

Desde luego, todo conjunto bien ordenado está totalmente ordenado (considérense las parejas como subconjuntos), pero el recíproco no es cierto; por ejemplo, $(\mathbb{Q}, \leq)$ está totalmente ordenado pero no está bien ordenado. Cualquier subconjunto finito $A \subset \mathbb{Q}$, con el orden inducido está bien ordenado.

$(\mathcal{P}(E), \subset)$ está bien (totalmente) ordenado si, y sólo si, E es singular, puesto que ninguna pareja de subconjuntos singulares está relacionada (véase Figura 1.4).

El conjunto de los números enteros con el orden usual no está bien ordenado. Sin embargo, es posible definir un orden especial que resulte ser un buen orden: $0 \preceq -1 \preceq 1 \preceq -2 \preceq 2 \preceq -3 \preceq \ldots$

En próximos capítulos fijaremos nuestra atención en las propiedades del orden usual sobre los conjuntos numéricos, que son básicas en análisis. La existencia, o no, de algún buen orden particular sobre cualquier conjunto es una cuestión de extraordinaria importancia y dificultad en la fundamentación de las matemáticas, y a ella nos referiremos brevemente en el próximo capítulo.

1.5. Problemas

Problema 1.1. Demuestre las siguientes tautologías:

a) $(p \vee q) \Longleftrightarrow [(p \Longrightarrow q) \Longrightarrow q]$;
b) $[(p \Longrightarrow q) \wedge (q \Longrightarrow r)] \vee (r \Longrightarrow p)$;
c) $[(p \Longrightarrow q) \wedge (r \Longrightarrow s)] \Longrightarrow [(p \vee r) \Longrightarrow (q \vee s)]$.

Problema 1.2. Pruebe que $B \subset C$ implica $B \cup A \subset C \cup A$, así como $B \cap A \subset C \cap A$.

Problema 1.3. Pruebe las siguientes proposiciones:

a) $A \subset B$ si y sólo si $\overline{B} \subset \overline{A}$;
b) $A = B$ si y sólo si $\overline{B} = \overline{A}$.

Problema 1.4. Demuestre que $(A \cap B) \cup (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (\overline{A} \cap \overline{B}) = E$.

Problema 1.5. Demuestre que $(A \cap \overline{B}) \cup (\overline{A} \cap B) = B$ si, y sólo si, $A = \emptyset$.

Problema 1.6. Demuestre que $(A \cup B) \cap \overline{B} = A$ si, y sólo si, $A \cap B = \emptyset$.

Problema 1.7. Pruebe las siguientes propiedades del producto cartesiano:

a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
c) $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$;
d) $A \times B = B \times A$ si, y sólo si, $A = B$.

Problema 1.8. Se define la **diferencia simétrica** de dos conjuntos A y B como $A \Delta B = (A \backslash B) \cup (B \backslash A)$. Pruebe que dicha operación conjuntista satisface:

a) $A \Delta A = \emptyset$;
b) $A \Delta \emptyset = A$;
c) $A \Delta B = (A \cup B) \setminus (A \cap B)$.

Problema 1.9. Considérense los conjuntos $A = \{x \in \mathbb{R} \mid -2 \leq x < 4\}$, $B = [-1, 5]$ y $C = \{z \in \mathbb{Z} \mid -2 \leq z < 1\}$. Calcule las uniones, las intersecciones y el producto cartesiano de las parejas de conjuntos A y B, A y C y, finalmente, B y C.

Problema 1.10. Se considera la correspondencia de $\mathbb{N}$ en $\mathbb{N}$ cuyo grafo es $G = \{(x, y) \mid 2x + y = 16\}$. Se pide:

a) describir G por extensión;
b) determinar su conjunto preimagen y su conjunto imagen.

Problema 1.11. Sean $A = \{\alpha, \beta, \gamma\}$, $B = \{a, b, c, d\}$ y $C = \{1, 2\}$. Considérense las correspondencias

$$F = \{(\alpha, a), (\beta, b), (\gamma, d), (\beta, c)\}$$

y

$$G = \{(a, 1), (b, 2), (c, 2), (d, 1)\}.$$

Clasifique F, G y $G \circ F$ (como aplicaciones o no; y si lo son, de qué tipo).

Problema 1.12. Clasifique las siguientes funciones reales de variables real (como inyectiva, suprayectiva, biyectiva o ninguna de las tres cosas):

a) $f(x) = ax + b$, con $a \neq 0$;
b) $f(x) = ax^2 + bx + c$, con $a \neq 0$.

Problema 1.13.* Clasifique $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definida como $f(x, y) = (x, xy - y^3)$.

Problema 1.14. Sea $f : A \longrightarrow B$ una aplicación. Demuestre que las siguientes proposiciones son ciertas cuando f es biyectiva, pero no para aplicaciones cualesquiera:

a) $f(\overline{X}) = \overline{f(X)}$ cualquiera que sea $X \subset A$;
b) f^{-1} es también biyectiva;
c) $\left(f^{-1}\right)^{-1} = f$.

Problema 1.15. Sea $f : A \longrightarrow B$ una aplicacion. Pruebe las siguientes proposiciones, y dé ejemplos que demuestren que las inclusiones que se afirman no son necesariamente igualdades, aunque también podrían serlo:

a) $A_1 \subset A_2 \subset A \Longrightarrow f(A_1) \subset f(A_2)$;
b) $B_1 \subset B_2 \subset B \Longrightarrow f^{-1}(B_1) \subset f^{-1}(B_2)$;
c) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, siendo $A_i \subset A, i = 1, 2$;
d) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$, siendo $A_i \subset A, i = 1, 2$;
e) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, siendo $B_i \subset B, i = 1, 2$;
f) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$, siendo $B_i \subset B, i = 1, 2$.

Problema 1.16.* Demuestre que $f : A \longrightarrow B$ es inyectiva si y sólo si $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$, para cualquier par de conjuntos $A_i \subset A, i = 1, 2$.

Problema 1.17.* Pruebe las siguientes proposiciones acerca de $f : A \longrightarrow B$:

a) f es inyectiva si y sólo si $X = f^{-1}(f(X))$ cualquiera que sea $X \subset A$;
b) f es suprayectiva si y sólo si $Y = f\left(f^{-1}(Y)\right)$ cualquiera que sea $Y \subset B$.

Problema 1.18. Si G es una correspondencia de A en B y A' es un subconjunto no vacío de A, entonces

$$G' := \left\{(x, y) \in G \mid x \in A'\right\}$$

es una correspondencia de A' en B llamada «restricción de G a A'». Pruebe que, si f es una aplicación de A en B, su restricción a A' es también una aplicación (que se denota mediante $f_{|A'}$). Además, si f es inyectiva, $f_{|A'}$ también lo es. Sin embargo, la suprayectividad no siempre es heredada por la restricción.

Problema 1.19.* Dado un número natural fijo n se define en $\mathbb{Z}$ la relación binaria $G = \{(x,y) \mid \text{existe } z \in \mathbb{Z} : x - y = zn\}$. Pruebe que es una relación de equivalencia e identifique el conjunto cociente.

Problema 1.20. Sea $f : E \longrightarrow \mathbb{N}$ una aplicación. Definimos sobre E la relación binaria $G = \{(x,y) \mid f(x) \leq f(y)\}$. Pruebe que G no define, en general, una relación de orden sobre E, a menos que f sea inyectiva.

Problema 1.21. Pruebe que la siguiente relación binaria define sobre $\mathbb{R}^2$ una relación de orden total (denominada **orden lexicográfico** sobre el plano), que no es un buen orden:

$$(x,y) \preceq (z,t) \Longleftrightarrow (x < z) \vee [(x = z) \wedge (y \leq t)].$$

Encuentre cota superior e inferior (si las hubiera) para el conjunto B definido así:

$$B = \{(x,y) \in \mathbb{R}^2 \mid 0 < x < 1\}.$$

Pruebe que el orden lexicográfico inducido sobre el subconjunto $\mathbb{N}^2 \subset \mathbb{R}^2$ es un buen orden.

Problema 1.22. Dado un conjunto E, se dice que un conjunto $\emptyset \neq G \subset E^2$ define una relación binaria circular sobre E cuando

$$[(a,b) \in G \wedge (b,c) \in G] \Longrightarrow (c,a) \in G,$$

cualesquiera que sean los elementos a, b y c tomados en E. Pruebe las siguientes proposiciones:

a) toda relación de equivalencia es circular;
b) si una relación es circular y reflexiva, entonces es de equivalencia.

Problema 1.23.* Vamos a dar un argumento que justifique la siguiente proposición: «la propiedad reflexiva de una relación binaria es consecuencia de las propiedades simétrica y transitiva» (de ser verdadera, bastaría verificar que una relación binaria satisface (S) y (T) para clasificarla, directamente, como RBE).

Supongamos $\emptyset \neq G \subset E^2$ satisfaciendo (S) y (T). Se tendrá:

(1) $(x,y) \in G \Longrightarrow (y,x) \in G$, para todo $(x,y) \in E^2$, debido a (S).
(2) $(x,y) \in G \Longrightarrow (x,x) \in G$, para todo $(x,y) \in E^2$, debido a (1) y (T).
(3) $(x,x) \in G$, para todo $x \in E$, como consecuencia de (2).

De (3) se sigue que G define una RBE sobre E. ¿Es correcta la prueba? ¿Es verdadera la proposición?

Problema 1.24. Enumere las relaciones de equivalencia y de orden total que pueden definirse sobre el conjunto $E = \{1, 2, 3\}$. De las relaciones de orden total que ha encontrado diga cuáles son un buen orden sobre E. Dé un ejemplo de orden parcial sobre E, pero que no sea total.

Problema 1.25.* Definimos sobre $\mathbb{N}$ una relación binaria a través del grafo $G = G_1 \cup G_2 \cup G_3$, donde

$$\begin{aligned} G_1 &= \{(x,y) \mid x \text{ e } y \text{ son impares tales que } x \leq y\}, \\ G_2 &= \{(x,y) \mid x \text{ e } y \text{ son pares tales que } x \leq y\} \text{ y} \\ G_3 &= \{(x,y) \mid x \text{ es impar e } y \text{ es par}\}. \end{aligned}$$

a) Demuestre que G define una relación de orden sobre $\mathbb{N}$, diciendo si es orden total o buen orden.

b) ¿Qué subconjuntos de $\mathbb{N}$ tienen máximo?

Problema 1.26. Definimos sobre $\mathbb{N}^2$ una relación binaria a través del grafo

$$G = \{((a,b),(c,d)) \in \mathbb{N}^2 \times \mathbb{N}^2 \mid a \text{ divide a } c \text{ y } b \text{ es múltiplo de } d\}$$

a) Demuestre que G define una relación de orden sobre $\mathbb{N}^2$, diciendo si es orden total o buen orden.

b) Si consideramos el subconjunto de $\mathbb{N}^2$

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

estudie los elementos maximales, minimales, máximo y mínimo de A.

Problema 1.27. Definimos sobre $\mathbb{R}^2$ la siguiente relación binaria:

$$(a,b) \sim (c,d) \Longleftrightarrow a + d = b + c.$$

Estudie si se trata de una relación de equivalencia y, en caso afirmativo, halle el conjunto cociente.

Problema 1.28. En el conjunto $\mathbb{R}^2$ de los puntos del plano se considera un punto fijo O y se define la relación binaria

$$A \sim B \Longleftrightarrow d(O,A) = d(O,B),$$

siendo d la distancia euclídea entre dos puntos. Se pide:

a) ¿Es una relación de equivalencia?

b) En caso afirmativo, ¿cuáles son las clases de equivalencia y el conjunto cociente?

Problema 1.29. Sea U el conjunto de todos los rectángulos del plano y consideremos U ordenado por la relación de inclusión. Sea D el subconjunto de U que indica la Figura 1.6, $D = \{A_1, A_2, A_3, B_1, B_2\}$. Estudie los elementos maximales, minimales, máximo y mínimo de D.

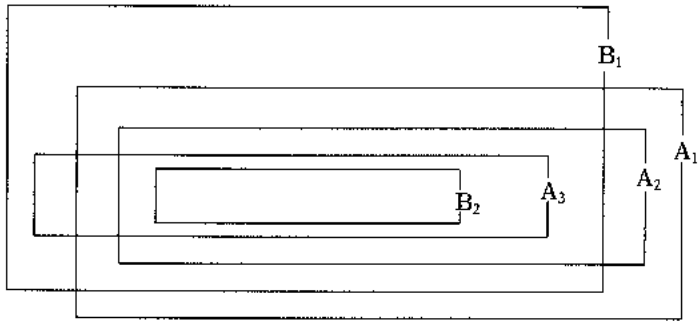

Figura 1.6. *Representación del conjunto D.*

Problema 1.30. Para la RBO en el plano $\mathbb{R}^2$ definida en el Ejemplo 1.8 así:

$$(x_1, y_1) \preceq (x_2, y_2) \Longleftrightarrow (x_2 - x_1 \geq 0 \wedge y_2 - y_1 \geq 0),$$

encuentre un subconjunto infinito $B \subset \mathbb{R}^2$ tal que B, con el orden inducido, esté totalmente ordenado.

Problema 1.31.* Supóngase que $(A, \preceq)$ es un conjunto ordenado, para el que existe un único elemento maximal $a_1 \in A$. ¿Se puede afirmar que a_1 es el máximo de A? (Ayuda: intente demostrarlo).

CAPÍTULO 2

CARDINALES

Los conjuntos se clasifican como finitos (aquellos para los que es cierto el famoso aforismo de Bergson «el todo es mayor que la parte») e infinitos, cuya existencia puede parecer paradójica. Los conjuntos finitos se clasifican, a su vez, atendiendo a su tamaño (referido aquí a la abundancia de elementos) mediante los números naturales. Análogamente, los conjuntos infinitos se clasifican a través de la noción de cardinal transfinito, concepto introducido, no sin polémica, por Cantor a finales de siglo XIX. El menor cardinal transfinito es precisamente el del conjunto de los números naturales, que se llama cardinal numerable. Los conjuntos que tienen cardinal numerable se llaman también numerables, y sus propiedades son muy importantes en varias ramas de la matemática. Aunque nos limitaremos a introducir los números cardinales, y no los ordinales, conviene saber que los números, además de ser útiles para contar, sirven también para ordenar conjuntos. En el caso de los conjuntos finitos, con los naturales hacemos ambas cosas: cuando le indicamos al ascensorista nuestro deseo de ascender hasta el piso 20, en realidad nos estamos refiriendo a la vigésima planta del edificio. En el caso de los conjuntos infinitos las cosas no son tan simples y es necesario diferenciar los números para contar (cardinales) de los números para ordenar (ordinales) (por ejemplo, al cardinal numerable le corresponden infinitos números ordinales distintos).

Casi todas las civilizaciones han conocido los primeros números naturales y, algunas de ellas, también números grandes cuando su sistema de numeración se lo permitía. La posibilidad de operar sin ábacos también estaba condicionada al sistema de numeración. El que utilizamos actualmente, sistema de numeración de posición, con base 10 es originario de la India (siglo VI d.C.), si bien 0 no era interpretado como un número, sino como un artificio para rellenar huecos; así, el número natural que consta de dos centenas y de tres unidades es el 203, de tal forma que «0» indica en este caso, por su posición, ausencia de decenas. Los árabes introdujeron este sistema de numeración, y las consiguientes reglas de cálculo en la Europa medieval. Es aquí donde comienza la comparación de conjuntos infinitos. Por ejemplo, Alberto de Sajonia demostró que una viga de longitud infinita tiene el mismo volumen que todo el espacio tridimensional. La definición de conjunto infinito podría deberse a Bolzano, ya en 1847. Suele tomarse 1874 como fecha de nacimiento de la teoría de conjuntos por publicarse, en el *Journal de Crelle*, el primer artículo

sobre el tema, obra de Cantor, quien se había dedicado con anterioridad a la teoría de números y al estudio de las series trigonométricas. En dicho artículo se habla de conjuntos que pueden ponerse en correspondencia biyectiva con los números naturales. En esa época, Cantor no usa el término *numerable* para estos conjuntos, palabra que se introduce en 1883. Se demuestra (véase el Problema 2.23) que no pueden ponerse en biyección con los números reales y Cantor señala que esto prueba un teorema debido a Liouville: que existen infinitos números trascendentes (el argumento en la Proposición 2.11 es también de Cantor, pero posterior, de 1891). La noción de conjuntos equipotentes y la demostración de la equipotencia de $\mathbb{R}$ y $\mathbb{R}^n$ aparecen en otro artículo publicado en la misma revista en 1878. A partir de aquí publica Cantor una serie de seis artículos en *Mathematische Annalen* (1879-1884), donde se introduce el concepto de buen orden y se desarrollan las aritméticas de los cardinales y de los ordinales transfinitos. Sus ideas revolucionarias encuentran la radical oposición de quienes solamente aceptan aquellos objetos matemáticos que pueden ser construidos, tras un número finito de pasos, a partir de los números naturales. Este grupo lo lideraba el prestigioso Kronecker, quien, respecto a la demostración de la trascendencia de π realizada por Lindemann en 1882, dijo: «¿Para qué sirve su bella investigación de π si los números irracionales no existen?» También a Kronecker se le atribuye la afirmación: «Dios ha creado los números naturales. Todo lo demás es obra del hombre.» La controversia afectó a Cantor hasta el punto de provocarle una crisis mental de la que salió, en 1886, afectado para siempre. A pesar de todo siguió investigando hasta 1899. En su último tratado, publicado en 1897, ya se utiliza el lenguaje conjuntista actual; allí prueba Cantor la propiedad antisimétrica del orden en conjuntos de cardinales transfinitos (la prueba del Teorema 2.3, más simple que la suya, aunque nada trivial, es de Bernstein).

Suele considerarse a Grassmann como el primer matemático en ocuparse de la fundamentación de la aritmética, en 1861. Frege definió en 1879 el «ancestral» y, por medio de esta noción de la lógica, la clase de los números naturales. La construcción del conjunto de los números naturales, $\mathbb{N}$, a partir de la teoría general de cardinales se debe al propio Cantor y a Dedekind. Sin embargo, muchos contemporáneos de Cantor, escépticos con respecto a sus propuestas revolucionarias, prefirieron descripciones axiomáticas de tipo material: se supone dado un conjunto, llamado $\mathbb{N}$, cuyos elementos satisfacen una lista de axiomas (proposiciones que son aceptadas por convenio). La más célebre axiomatización de $\mathbb{N}$ fue iniciada por Peano en 1889 y completada en su «Formulario» de 1897-1899 (véase el Problema 2.32). Los axiomas adoptados por Peano eran teoremas en la versión de Dedekind (1888). Las paradojas que aparecían en la teoría intuitiva de conjuntos, como la descubierta por Cantor en 1899 (véase la Proposición 2.5), o la de Russell en 1902 (descubierta independientemente por Zermelo en 1901) (véase Problema 2.29), eran evitadas mediante la formulación de sistemas axiomáticos (Hilbert, 1900; Zermelo, 1908 y 1930; Fraenkel, 1925; Von Neumann, 1925 y 1928).

Aunque a lo largo de los próximos capítulos nos proponemos revisar los conjuntos numéricos, desde los números naturales hasta los números complejos, supondremos que el lector los conoce intuitivamente, tal y como se estudian en matemáticas elementales. De esa manera podremos ilustrar adecuadamente muchos de los conceptos del capítulo.

2.1. Números cardinales

En el campeonato social del Club de Tenis Halmos, que se disputa por el sistema de copa (en cada ronda se sortean los emparejamientos y siguen adelante los vencedores), se han inscrito 1.024 socios. ¿Cuántos partidos deberán jugarse?: 512 partidos en la primera ronda, 256 en la segunda y así sucesivamente. La respuesta es la suma de la progresión geométrica $512+256+\cdots+1$. Se llega a la misma conclusión por la vía conjuntista: como existe una biyección entre el conjunto de partidos y el de perdedores (todos los inscritos menos el ganador), la respuesta es 1.023.

Definición 2.1. *Dos conjuntos, A y B, son* ***equipotentes*** *cuando existe una aplicación biyectiva entre A y B. En tal caso se escribe $A \sim B$. Por las propiedades de las biyecciones, la equipotencia ($\sim$) es relación de equivalencia sobre cualquier familia de conjuntos, y cada clase de equivalencia se llama* ***número cardinal****. Suelen representarse con letras del alfabeto griego o hebreo: $\alpha = \operatorname{card}(A)$. En particular, en nuestro sistema de numeración escribimos* $\operatorname{card}(\emptyset) = 0$, $\operatorname{card}(\{x\}) = 1$ *y* $\operatorname{card}(\{x,y\}) = 2$ *si* $x \neq y$.

Ejemplo 2.1. Dados dos números reales $a < b$, la aplicación

$$f : [0,\ 1] \to [a,b]$$

tal que $f(x) = (1-x)a + xb$ es biyectiva. En efecto, si $f(x) = f(y)$, se tiene $(x-y)(a-b) = 0$ y, al ser $a \neq b$, necesariamente $x = y$. Se concluye que f es inyectiva. También es fácil demostrar que f es suprayectiva: cualquiera que sea $c \in [a,b]$, el lector puede comprobar que $f(x) = c$ si se toma

$$x = \frac{c-a}{b-a} \in [0,\ 1].$$

Se concluye, por lo tanto, que ambos intervalos, a pesar de tener diferente longitud, son equipotentes, es decir, que se tiene $[0,\ 1] \sim [a,b]$.

El mismo argumento permite probar que $]0,\ 1[\sim]a,b[$.

Ejemplo 2.2. Veremos que $]-1,\ 1[\sim \mathbb{R}$, puesto que somos capaces de construir una aplicación

$$f :]-1,\ 1[\to \mathbb{R}$$

que es biyectiva. Definiremos f gráficamente (véase Figura 2.1), aunque podríamos hacerlo también analíticamente (lo que se deja como ejercicio para el lector).

Las operaciones con cardinales se definen por medio de representantes. A tal fin, es imprescindible probar que para cardinales α y β cualesquiera existen representantes disjuntos. En efecto, si A y B son conjuntos tales que $\operatorname{card}(A) = \alpha$, $\operatorname{card}(B) = \beta$, los conjuntos disjuntos $A \times \{1\}$ y $B \times \{2\}$ son representantes de los mismos cardinales, ya que las aplicaciones

$$\begin{array}{rcl} A & \longrightarrow & A \times \{1\} \\ a & \longmapsto & (a, 1) \end{array}$$

y

$$\begin{array}{rcl} B & \longrightarrow & B \times \{2\} \\ b & \longmapsto & (b, 2) \end{array}$$

son biyectivas.

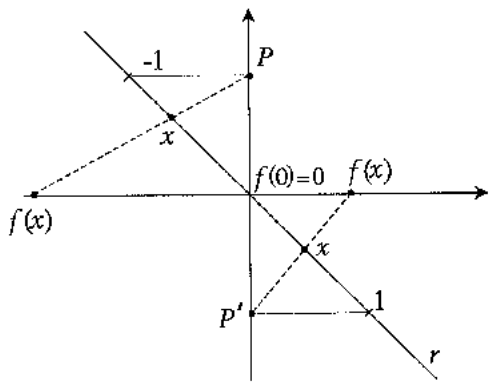

Figura 2.1. *Para definir la biyección $f :]-1, 1[\longrightarrow \mathbb{R}$, se dibuja en el plano cartesiano una recta graduada r cuyo origen coincida con el origen de coordenadas. Sean P y P' los pies de las perpendiculares al eje de ordenadas trazadas desde los puntos ∓ 1 de r. Se define $f(0) = 0$ y, si $x > 0$ ($x < 0$), $f(x)$ está determinado por la intersección del eje de abscisas con la semirrecta que parte de P' (de P) y pasa por el punto $x \in]-1, 1[$.*

Observemos también que, si A y B son representantes disjuntos de α y β, y A' y B' también lo son, entonces $A' \cup B' \sim A \cup B$. En efecto, si $f : A \longrightarrow A'$ y $g : B \longrightarrow B'$ son biyecciones, la aplicación $h : A \cup B \longrightarrow A' \cup B'$ tal que

$$h(x) = \begin{cases} f(x), & x \in A \\ g(x), & x \in B \end{cases}$$

es también una biyección.

Definición 2.2. *Dados los cardinales α y β, se define su* ***suma*** *como el cardinal de la unión de dos de sus representantes disjuntos. En otras palabras, $\alpha + \beta :=$ card $(A \cup B)$ siempre que $\alpha =$ card (A), $\beta =$ card (B) y $A \cap B = \emptyset$.*

La definición previa es «buena» al haberse demostrado que siempre existen representantes disjuntos y que el cardinal de su unión es independiente de los representantes disjuntos elegidos.

Las siguientes propiedades de la suma son de comprobación inmediata:

(i) *Conmutatividad* (por ser conmutativa la intersección y la unión de conjuntos).

(ii) *Asociatividad* (por ser asociativa la unión de conjuntos).

(iii) $\alpha + 0 = 0 + \alpha = \alpha$, puesto que

$$A \cup \emptyset = \emptyset \cup A = A.$$

Se dice que el elemento 0 es el *neutro* para la suma de cardinales.

Definición 2.3. *Dados α y β, cardinales representados por A y B, se define su* ***producto*** *como el cardinal del producto cartesiano $A \times B$. Se escribe $\alpha \times \beta =$* card $(A \times B)$.

La definición de producto de dos cardinales también es «buena» porque el cardinal del producto cartesiano no depende de los representantes elegidos. En efecto, si A' y B' son representantes de α y β, existen biyecciones

$$f : A \longrightarrow A'$$

y

$$g : B \longrightarrow B',$$

en cuyo caso la aplicación

$$\begin{array}{ccc} A \times B & \longrightarrow & A' \times B' \\ (a,b) & \longmapsto & (f(a), g(b)) \end{array}$$

es, asimismo, biyectiva.

Las propiedades del producto de cardinales son semejantes a las de la suma:

(i) *Conmutatividad*, por ser biyectiva la aplicación

$$\begin{array}{c} A \times B \longrightarrow B \times A \\ (a,b) \longmapsto (b,a) \end{array}$$

(ii) *Asociatividad*, puesto que la aplicación

$$\begin{array}{c} A \times (B \times C) \longrightarrow (A \times B) \times C \\ (a,(b,c)) \longmapsto ((a,b),c) \end{array}$$

también es biyectiva.

(iii) $\alpha \times 1 = 1 \times \alpha = \alpha$, lo que se expresa diciendo que 1 es el *neutro* para el producto de cardinales.

A las propiedades específicas de las operaciones binarias suma y producto enumeradas arriba hay que añadir la siguiente, que relaciona ambas operaciones:

(iv) *Distributividad* del producto respecto de la suma:

$$\alpha \times (\beta + \gamma) = \alpha \times \beta + \alpha \times \gamma.$$

En efecto, si A, B y C representan a α, β y γ, y $B \cap C = \emptyset$, entonces

$$A \times (B \cup C) = (A \times B) \cup (A \times C),$$

con $(A \times B) \cap (A \times C) = \emptyset$.

La tercera operación con cardinales que definiremos es monaria (relativa a un solo cardinal), y se basa en el concepto de conjunto de partes de un conjunto A: $\mathcal{P}(A) = \{X \mid X \subset A\}$. En combinatoria elemental se demuestra, usando la fórmula del binomio de Newton, que un conjunto de n elementos tiene 2^n subconjuntos. Esto motiva la siguiente definición.

Definición 2.4. *Si A es un representante del cardinal α, se define la* ***potencia*** *de α en base 2 como el cardinal del conjunto de las partes de A. En símbolos,* $2^\alpha := \operatorname{card}(\mathcal{P}(A))$.

Una vez más se demuestra que la definición es «buena». En efecto, si A' es otro representante de α, existe una aplicación biyectiva

$$f : A \longrightarrow A'.$$

Entonces la aplicación definida por

$$\begin{aligned} \Phi : \mathcal{P}(A) &\longrightarrow \mathcal{P}(A'), \\ X &\longmapsto f(X) \end{aligned}$$

es también biyectiva, de modo que 2^α es independiente de representantes.

2.2. Los números naturales: inducción

Como introducción a los conjuntos infinitos relataremos el ejemplo conocido como «el hotel de Hilbert». Este hipotético hotel tiene la particularidad de poseer un número tan grande de habitaciones que van numeradas consecutivamente, sin alcanzar un final. Un día llega a él un cliente nuevo y se decepciona al saber que, a pesar de extenderse hasta el infinito, todas las habitaciones del hotel están ocupadas. Hilbert, el recepcionista, medita por unos momentos y tranquiliza al recién llegado asegurándole que logrará una habitación para él. Pide a todos los clientes ya instalados que se muden a la habitación que sigue a la que ocupan ahora, de manera que el de la habitación número uno se muda a la dos, el de la dos a la tres, etc. Todos los que ya estaban en el hotel siguen teniendo una habitación y eso permite que el recién llegado ocupe la habitación número uno, ahora vacante.

La noche siguiente, Hilbert tiene que enfrentarse a un problema mucho mayor. El hotel continúa completo cuando llega un ómnibus infinitamente

largo de nuevos clientes. Hilbert permanece imperturbable y se frota las manos pensando en la cantidad infinita de dinero que podrá cobrar. Pide a sus clientes ya instalados que se muden de nuevo, pero esta vez a la habitación cuyo número sea el doble del que tiene la que ahora ocupan. Todos los que estaban en el hotel siguen teniendo una habitación y ahora un número infinito de habitaciones, todas las impares, han quedado vacantes para los recién llegados.

Definición 2.5. *Un conjunto A (o su cardinal correspondiente) es* ***infinito*** *cuando es equipotente a una parte propia (un subconjunto B de A tal que $\emptyset \subsetneq B \subsetneq A$). De lo contrario, el conjunto (o su correspondiente cardinal) es* ***finito****.*

Se llaman ***números naturales*** *a los cardinales de los conjuntos finitos no vacíos. El conjunto de todos los números naturales se denota por $\mathbb{N}$.*

Debemos comprobar que la definición de cardinal infinito es independiente de representantes. En efecto, supongamos que $f : A \longrightarrow A'$ es una aplicación biyectiva, que $g : A \longrightarrow B \subsetneq A$ es inyectiva y que $a \in A \backslash B$. Entonces, la aplicación $f \circ \left(g \circ f^{-1}\right) : A' \longrightarrow A'$ es inyectiva (al ser composición de aplicaciones inyectivas) pero no es suprayectiva, ya que, como el lector probará, $f(a)$ no pertenece a su conjunto imagen.

La definición de cardinal finito también es independiente de representantes.

De acuerdo con esta definición, el *cero* no es un número natural.

Desde luego, todos los conjuntos singulares y todas las parejas son conjuntos finitos, de modo que los cardinales 1 y 2 son números naturales.

Probaremos que cualquier subconjunto de un conjunto finito es también finito mediante el contrarrecíproco (tautología 1.21). Supongamos que $A \subset B$ y que A es infinito. Existe entonces una aplicación biyectiva

$$f : A \longrightarrow C,$$

tal que $\emptyset \subsetneq C \subsetneq A$. En tal caso podemos definir una biyección $g : B \longrightarrow (B \backslash A) \cup C$ (subconjunto propio de B) como sigue:

$$g(x) = \begin{cases} f(x), & x \in A \\ x, & x \in B \backslash A. \end{cases}$$

La conclusión es que B es infinito.

El siguiente resultado, de enunciado tan intuitivo que puede parecer obvio, tiene importantes consecuencias, según veremos más adelante.

Proposición 2.1. *Si $n \in \mathbb{N}$, entonces $n + 1 \in \mathbb{N}$.*

Demostración. Sea A finito tal que $\operatorname{card}(A) = n$, y sea $z \notin A$ (z es un objeto arbitrario no perteneciente al conjunto A). Por definición de suma de cardinales,

$$n + 1 = \operatorname{card}(A \cup \{z\}).$$

Supondremos que $A \cup \{z\}$ es infinito y llegaremos a una contradicción (argumento por reducción al absurdo).

Estamos suponiendo que existe una aplicación biyectiva

$$f : A \cup \{z\} \longrightarrow B,$$

donde $B \subsetneqq A \cup \{z\}$. Pueden darse tres casos:

Caso 1: $z \notin B$. Entonces

$$f_{|A} : A \longrightarrow B \setminus \{f(z)\}$$

es biyección, con $B \setminus \{f(z)\} \subsetneqq A$, por lo que A sería infinito (véase Figura 2.2).

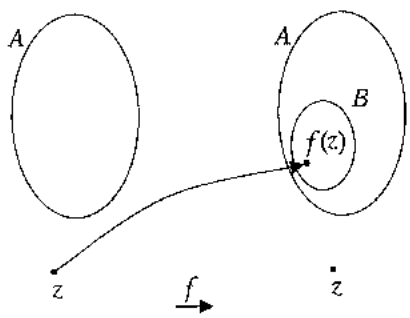

Figura 2.2. *Ilustración del caso 1.*

Caso 2: $f(z) = z$. De nuevo

$$f_{|A} : A \longrightarrow B \setminus \{f(z)\}$$

es biyección, con $B \setminus \{z\} \subsetneqq A$, y se concluye también que A es infinito (véase Figura 2.3).

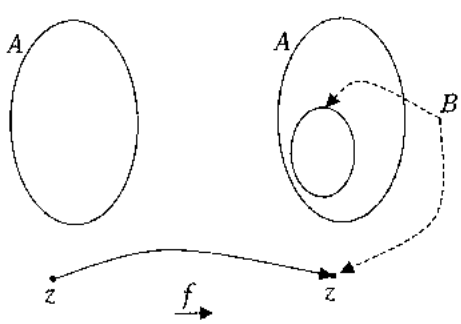

Figura 2.3. *Ilustración del caso 2.*

Caso 3: $f(z) \neq z \in B$. Sea $a \in A$ tal que $f(a) = z$. Se define la aplicación

$$g : A \longrightarrow B \setminus \{z\}$$

(véase Figura 2.4) tal que

$$g(x) = \begin{cases} f(x), & x \neq a \\ f(z), & x = a. \end{cases}$$

Como g es biyección y $B \setminus \{z\} \subsetneq A$, concluimos que A es infinito. □

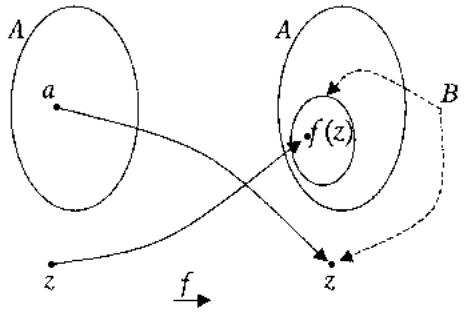

Figura 2.4. *Ilustración del caso 3.*

El siguiente teorema es la versión formal del procedimiento adoptado por Hilbert ante la llegada de un nuevo cliente a su hotel, relatado al inicio de esta sección.

Teorema 2.1 ***(1° de Peano).*** *La aplicación* ***(función sucesor)***

$$\begin{aligned} s : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n+1 \end{aligned}$$

es inyectiva y $s(\mathbb{N}) \subsetneq \mathbb{N}$.

Demostración. Supongamos que $s(n) = s(m)$, es decir, $n+1 = m+1$. Si A y B representan a los cardinales n y m, y se eligen dos objetos z y t tales que $z \notin A$ y $t \notin B$, entonces $A \cup \{z\}$ y $B \cup \{t\}$ representarán a $n+1$ y a $m+1$, debiendo ser equipotentes (por la hipótesis). Sea

$$f : A \cup \{z\} \longrightarrow B \cup \{t\}$$

biyectiva. Dos casos son posibles:

Caso 1: $f(z) = t$. Entonces $f_{|A} : A \longrightarrow B$ es biyección y $n = m$.

Caso 2: $f(z) \neq t$. Sea $a \in A$ tal que $f(a) = t$. Se define $g : A \longrightarrow B$ tal que

$$g(x) = \begin{cases} f(x), & x \neq a \\ f(z), & x = a \end{cases}.$$

Como g es biyectiva, $n = m$ (véase Figura 2.5).

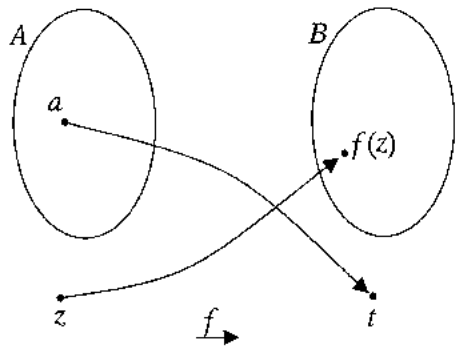

Figura 2.5. *Ilustración del caso 2.*

Terminaremos probando que $1 \notin s(\mathbb{N})$. En efecto, dado $n \in \mathbb{N}$, consideramos A tal que $\operatorname{card}(A) = n$. Consideramos también $x \in A$ (tal x existe porque $A \neq \emptyset$) y un objeto arbitrario $z \notin A$. Como $A \cup \{z\}$ contiene a la pareja $\{x, z\}$ (no puede ser un conjunto singular porque $x \neq z$), se tiene

$$s(n) = n + 1 = \operatorname{card}(A \cup \{z\}) \neq 1.$$

Así, $s(\mathbb{N}) \subsetneq \mathbb{N}$. □

Corolario 2.1. *El conjunto de los números naturales es infinito.*

Demostración. Como la función sucesor s es inyectiva, $\mathbb{N}$ y $s(\mathbb{N})$ son equipotentes; además, $s(\mathbb{N})$ es un subconjunto propio de $\mathbb{N}$. □

Teorema 2.2 *(2° de Peano).* *Sea $A \subset \mathbb{N}$ un subconjunto cualquiera con las siguientes propiedades*

(i) $1 \in A$.
(ii) $n \in A \Longrightarrow s(n) \in A$, *para todo* $n \in \mathbb{N}$.

Entonces $A = \mathbb{N}$.

En la Sección 2.6 se exhibe una demostración del Teorema 2.2, compatible con el enfoque adoptado en este texto (véase el Teorema 2.7 y la nota que le sigue). Aceptémoslo de momento.

El conjunto de los números naturales posee las propiedades enunciadas en los Teoremas de Peano. Más aún, estas propiedades *caracterizan* al conjunto de los números naturales, en el siguiente sentido: si K es un conjunto cualquiera con una aplicación (sucesor) $s : K \longrightarrow K$ inyectiva pero no suprayectiva (Teorema 2.1) y tal que los subconjuntos de K verifican la propiedad enunciada en el Teorema 2.2, entonces K es el conjunto de los números naturales (salvo por cuestiones de notación).

El Teorema 2.2, convenientemente reformulado, se usa como un método de demostración de proposiciones referidas a números naturales, conocido en la literatura como el **principio de inducción matemática**.

Supongamos que $p(n)$ es una ecuación en la que aparece la variable n (véase el Problema 2.1), y se desea probar que las infinitas proposiciones $p(1)$, $p(2), p(3), \ldots$ son todas ciertas. Podemos imaginar infinitas fichas de dominó erguidas, cada una portando escrita en su cara una de estas ecuaciones; una vez comprobada la validez de una ecuación particular derribamos la ficha correspondiente. Para derribar una a una todas las fichas, no alcanzaría toda una vida. Sin embargo, si las fichas están cuidadosamente dispuestas, al caer la primera, ésta derribará a la segunda, que a su vez hará caer la tercera, y así caerán todas. El principio de inducción, versión matemática del efecto dominó, podemos enunciarlo como sigue:

Si $p(n)$ es una forma proposicional sobre $\mathbb{N}$ tal que:

(i) $p(1)$ se cumple y, además,
(ii) $p(n) \Longrightarrow p(n+1)$, para todo $n \in \mathbb{N}$,

entonces es cierta la proposición $p(n)$ para todo $n \in \mathbb{N}$.

La inducción matemática fue usada, y explícitamente reconocida, por Pascal en 1654 y Fermat en 1659, y conservó la condición de axioma aritmético último hasta 1879, cuando Frege definió la clase de los números naturales a partir de conceptos lógicos. En contraposición al significado habitual del término, la *inducción* (siempre en el sentido de arriba) es un método deductivo de demostración que garantiza la validez de la proposición $p(n)$ para todo $n \in \mathbb{N}$, sin ninguna excepción. El uso del término proviene del hecho de que para elaborar una conjetura (la proposición $p(n)$ para todo $n \in \mathbb{N}$, que se cree cierta) se suele proceder por observación de varios casos, como en las ciencias experimentales.

De inmediato veremos cuán importante es el principio de inducción cuando se trata de probar propiedades de números naturales. Empezaremos demostrando que la suma y el producto de elementos de $\mathbb{N}$ son, asimismo, elementos de $\mathbb{N}$ (de donde obtendremos que la unión y el producto cartesiano de conjuntos finitos son también finitos).

Proposición 2.2. *La suma y el producto de dos números naturales es también un número natural.*

Demostración. Empezaremos probándolo para la suma y luego, en base a esta propiedad, para el producto.

(i) Dado $m \in \mathbb{N}$ (número natural fijo), consideramos la siguiente forma proposicional sobre $\mathbb{N}$: $p(n) \equiv m + n \in \mathbb{N}$. Acabamos de ver que $p(1)$ es verdad (Proposición 2.1). Suponiendo cierto $p(n)$, tenemos $m + n \in \mathbb{N}$ y, por la misma proposición y por la asociatividad de la suma, se tiene

$$m + (n + 1) = (m + n) + 1 \in \mathbb{N}.$$

Por lo tanto, $p(n) \Longrightarrow p(n+1)$, cualquiera que sea $n \in \mathbb{N}$, y se concluye, por inducción, que $n+m \in \mathbb{N}$ para todo $n \in \mathbb{N}$. Como m es arbitrario, $m+n \in \mathbb{N}$ cualesquiera que sean los números naturales m y n.

(ii) Dado $m \in \mathbb{N}$ (otra vez fijo), consideramos ahora la forma proposicional $p(n) \equiv nm \in \mathbb{N}$ (es costumbre prescindir del signo $\times$ para representar el producto de números naturales). También ahora $p(1)$ es cierto, porque $m1 = \operatorname{card}(A \times \{z\}) = \operatorname{card}(A) = m \in \mathbb{N}$. Suponiendo cierto $p(n)$, y utilizando propiedades de cardinales ya demostradas, se obtiene

$$m(n+1) = mn + m1 = mn + m \in \mathbb{N}.$$

Por lo tanto, $p(n) \Longrightarrow p(n+1)$ para todo $n \in \mathbb{N}$ y se concluye, como antes, que $mn \in \mathbb{N}$ para todo $n \in \mathbb{N}$. Así pues, $mn \in \mathbb{N}$ cualesquiera que sean los números naturales m y n. □

Corolario 2.2. *La unión y el producto cartesiano de dos conjuntos finitos es un conjunto finito.*

Demostración. La afirmación es trivialmente cierta cuando al menos uno de los dos conjuntos es vacío, por lo que supondremos que los conjuntos finitos dados, A y B, son no vacíos. Sean $m = \operatorname{card}(A)$ y $n = \operatorname{card}(B)$.

Para el producto es inmediato, ya que $\operatorname{card}(A \times B) = mn \in \mathbb{N}$.

Por lo que se refiere a la unión, es inmediato si A y B son disjuntos o $A = B$. De no ser así, como $A \cup B = A \cup (B \backslash A)$ y estos dos conjuntos son finitos, no vacíos y disjuntos, se tiene que $p = \operatorname{card}(B \backslash A)$ es también un número natural y $\operatorname{card}(A \cup B) = m + p \in \mathbb{N}$. □

Corolario 2.3. *La unión finita de conjuntos finitos es finita.*

Demostración. Probaremos por inducción que la unión de cualquier familia de n conjuntos finitos es un conjunto finito, para todo $n \in \mathbb{N}$. Es obvio que para $n = 1$ el resultado es cierto. Supongamos que la propiedad es cierta para una familia de n elementos y sean $A_1, A_2, \ldots, A_{n+1}$ conjuntos finitos. Por la asociatividad se puede escribir la unión de la familia como

$$\bigcup_{i=1}^{n+1} A_i = \left(\bigcup_{i=1}^{n} A_i \right) \cup A_{n+1}$$

que es una unión de dos conjuntos finitos (el primero es finito por hipótesis de inducción). Aplicando el Corolario 2.2 se completa la prueba. □

Proposición 2.3. *Si A es un conjunto finito, entonces $\mathcal{P}(A)$ también es finito.*

Demostración. Probaremos la proposición por inducción sobre $\operatorname{card}(A) = n \in \mathbb{N}$ (el caso $A = \emptyset$ es trivial, ya que $\mathcal{P}(\emptyset) = \{\emptyset\}$ es unitario). A tal fin, cuando $\operatorname{card}(A) = 1$ se tiene que $\operatorname{card}(\mathcal{P}(A)) = 2$, que es finito. Supongamos que $\mathcal{P}(A)$ es finito cuando $\operatorname{card}(A) = n$, y sea B un conjunto tal que $\operatorname{card}(B) = n+1$. Siendo $B \neq \emptyset$, sea $b \in B$ arbitrario y consideremos las siguientes familias de

subconjuntos de B :

$$\mathcal{B}_1 = \{X \in \mathcal{P}(B) \mid b \in X\} \quad \text{y} \quad \mathcal{B}_2 = \{X \in \mathcal{P}(B) \mid b \notin X\}.$$

Evidentemente, $\mathcal{B}_1 \cup \mathcal{B}_2 = \mathcal{P}(B)$ y $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$. Además, $\mathcal{B}_2 = \mathcal{P}(B \setminus \{b\})$ y la aplicación

$$\begin{aligned} f: \quad \mathcal{B}_1 &\longrightarrow \mathcal{B}_2 \\ X &\longmapsto X \setminus \{b\} \end{aligned}$$

es una biyección (demuéstrelo). Como card $(B \setminus \{b\}) = n$, aplicando la hipótesis de inducción se tiene que $\mathcal{B}_2$ es finito, por lo que $\mathcal{B}_1$ también lo es. La conclusión se obtiene aplicando el Corolario 2.2. □

Otra de las propiedades «evidentes» de $\mathbb{N}$, que demostraremos por inducción y utilizaremos más adelante, es la **ley de cancelación** para la suma de números naturales. Conviene recordar que, como la función sucesor es inyectiva, si $m + 1 = n + 1$, entonces $m = n$ (cancelación de la unidad).

Proposición 2.4. *Cualesquiera que sean los números naturales m, n y q, si $m + n = q + n$, entonces $m = q$.*

Demostración. Dados $m \in \mathbb{N}$ y $q \in \mathbb{N}$ (fijos), se considera la siguiente forma proposicional sobre $\mathbb{N}$:

$$p(n) \equiv (m + n = q + n \Longrightarrow m = q).$$

La proposición $p(1) \equiv (m + 1 = q + 1 \Longrightarrow m = q)$ es la cancelación de 1, que es una proposición verdadera (Teorema 2.1).

Suponiendo cierto $p(n)$, así como $m + (n + 1) = q + (n + 1)$ (el antecedente de $p(n + 1)$), se tiene, como consecuencia de la asociatividad de la suma de cardinales, que $(m + n) + 1 = (q + n) + 1$. Como puede cancelarse la unidad, se obtiene $m + n = q + n$ y, usando la hipótesis de inducción $p(n)$, se tiene entonces $m = q$.

En conclusión, $p(n) \Longrightarrow p(n + 1)$ cualquiera que sea $n \in \mathbb{N}$, lo que completa la segunda parte de la prueba por inducción (cualquiera que sea $n \in \mathbb{N}$, n puede cancelarse).

Como m y q eran arbitrarios se tiene lo que se quería probar. □

2.3. Comparación de cardinales

El ejemplo del hotel de Hilbert relatado al inicio de la sección anterior parece insinuar que un infinito es tan extenso como cualquier otro, porque varios infinitos caben a la vez en el mismo hotel infinito; el cardinal del conjunto de los números naturales pares es igual al cardinal del conjunto de los números naturales. Sin embargo, unos infinitos son, en realidad, mayores que otros. Por ejemplo, todo intento de emparejar uno a uno cada número racional con otro irracional acaba en el fracaso y, de hecho, se puede demostrar que el

cardinal de los números irracionales es mayor que el cardinal de los números racionales.

Definición 2.6. *Dados dos cardinales α y β, con representantes respectivos A y B, se dice que $\alpha \leq \beta$ si existe una aplicación inyectiva $f : A \longrightarrow B$ o, alternativamente, si $A = \emptyset$.*

Se define $\alpha < \beta$ cuando $\alpha \leq \beta$ y $\alpha \neq \beta$ (es decir, existe al menos una aplicación inyectiva $f : A \longrightarrow B$, pero ninguna de ellas es suprayectiva, o bien $\alpha = 0$ y $\beta \neq 0$).

Es fácil comprobar que la definición de $\alpha \leq \beta$ es independiente de representantes. En efecto, si $A \neq \emptyset$ (ya que el resultado es obvio cuando $A = \emptyset$), supongamos que $A' \sim A$ y $B' \sim B$, por lo que existen sendas aplicaciones biyectivas $g : A' \longrightarrow A$ y $h : B \longrightarrow B'$. Entonces $h \circ (f \circ g) : A' \longrightarrow B'$ es inyectiva (al ser composición de aplicaciones inyectivas).

La definición de $\alpha < \beta$ también es independiente de representantes.

Obsérvese que, si $\alpha \leq \beta$, se tiene $\alpha + \gamma \leq \beta + \gamma$ cualquiera que sea el cardinal γ. Por eso se dice que la relación $\leq$ entre cardinales es **compatible** con la suma.

Ejemplo 2.3. (i) Si $A \subset B$, se tiene $\operatorname{card}(A) \leq \operatorname{card}(B)$ (por la inyectividad de la aplicación que asocia cada elemento de A consigo mismo). En particular, si $A \subsetneq B$ y B es finito, entonces $\operatorname{card}(A) < \operatorname{card}(B)$.

(ii) Recordando que $2^\alpha = \operatorname{card}(\mathcal{P}(A))$ cuando $\alpha = \operatorname{card}(A)$, también se cumple $\alpha \leq 2^\alpha$ cualquiera que sea el cardinal α, puesto que la siguiente aplicación es inyectiva cuando $A \neq \emptyset$:

$$\begin{aligned} A &\longrightarrow \mathcal{P}(A) \\ x &\longrightarrow \{x\} . \end{aligned}$$

En particular, $n < 2^n$ para todo cardinal finito n. Pronto veremos que $\alpha < 2^\alpha$ siempre (Teorema de Cantor).

Ejemplo 2.4. En toda reunión hay siempre dos participantes que ya conocían al mismo número de personas.

En efecto, si representamos por B el conjunto de participantes en la reunión ($\operatorname{card}(B) = n \geq 2$), se pregunta a cada elemento $b \in B$ cuántos participantes conocía (se supone que conoce al menos a uno, sin contarse a sí mismo). Sea $f(b) \in \mathbb{N}$ su respuesta. Si

$$A := f(B) = \{f(b) \mid b \in B\},$$

se tiene

$$A \subset \{1, \ldots, \operatorname{card}(B) - 1\},$$

por lo que $\operatorname{card}(A) < \operatorname{card}(B)$ (véase Problema 2.5). Si se demuestra que $\leq$ es una RBO (antisimétrica), $f : B \longrightarrow A$ no podrá ser inyectiva y existirán

dos elementos distintos en B (dos participantes) que tienen la misma imagen (conocían al mismo número de personas).

Este ejemplo ilustra el *principio del palomar*: si tenemos n nidos y $n+1$ palomas, entonces hay un nido en el que duermen al menos dos palomas. Este principio (muy utilizado en matemática discreta) es una de las consecuencias de que la relación binaria $\leq$ satisfaga las propiedades reflexiva, transitiva y antisimétrica sobre cualquier conjunto de cardinales. La demostración –nada simple– de esta última propiedad se conoce como Teorema de Bernstein, de Cantor-Bernstein o de Schröder-Bernstein, pues fue demostrado independientemente por esos tres autores. La herramienta de la prueba consiste en la construcción de cierta sucesión de conjuntos.

Definición 2.7. *Una* ***sucesión*** *en A es una aplicación $f : \mathbb{N} \longrightarrow A$, que denotaremos simplemente por $\{a_n\}_{n=1}^{\infty}$* cuando $a_n = f(n)$.

La notación $\{a_n\}_{n=1}^{\infty}$ (o incluso $\{a_n\}$, para abreviar) podría dar lugar a confundir una sucesión con el conjunto imagen de la aplicación f, pero son dos cosas diferentes.

En la prueba de Bernstein se construye una sucesión de conjuntos, $\{E_n\}$ de la siguiente forma. Se define E_1 directamente y, para cualquier $n \in \mathbb{N}$, si se supone dado E_n se definirá E_{n+1} a partir de E_n. De esa forma, si $p(n)$ es la forma proposicional «E_n está bien definido», se tendrá, por el principio de inducción, que se cumple $p(n)$ para todo $n \in \mathbb{N}$, es decir, que $\{E_n\}$ es una sucesión de conjuntos bien definida. Las sucesiones así definidas se llaman **recursivas** (volveremos a utilizarlas más adelante).

Teorema 2.3. *La relación $\leq$ es de orden sobre cualquier conjunto de cardinales.*
Propuse una condición para subsanar que e
Demostración. Propiedad reflexiva: si $\alpha = \operatorname{card}(A)$, como $I_A : A \longrightarrow A$ es inyectiva (y biyectiva), $\alpha \leq \alpha$.

Propiedad transitiva: si $\alpha = \operatorname{card}(A)$, $\beta = \operatorname{card}(B)$ y $\gamma = \operatorname{card}(C)$, y suponemos que $\alpha \leq \beta$ y que $\beta \leq \gamma$, deberán existir aplicaciones inyectivas $f : A \longrightarrow B$ y $g : B \longrightarrow C$. Entonces $g \circ f : A \longrightarrow C$ es también inyectiva y, por lo tanto, $\alpha \leq \gamma$.

Propiedad antisimétrica (**Teorema de Bernstein**): supondremos que $\alpha \leq \beta$ y que $\beta \leq \alpha$, siendo $\alpha = \operatorname{card}(A)$ y $\beta = \operatorname{card}(B)$. Estamos admitiendo que existen aplicaciones inyectivas $f : A \longrightarrow B$ y $g : B \longrightarrow A$. Probaremos que existe una aplicación biyectiva $h : A \longrightarrow B$ recurriendo a una sucesión recursiva de conjuntos.

El primer elemento de dicha sucesión será

$$E_1 := A \backslash g(B) \tag{2.1}$$

(véase Figura 2.6). Si $E_1 = \emptyset$, entonces g es suprayectiva y, como es inyectiva, $\alpha = \beta$ y la demostración termina (esto sucede cuando A es finito, por ejemplo).

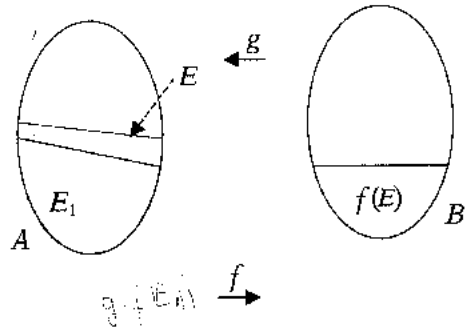

Figura 2.6. *Definición del conjunto E.*

Supongamos, entonces, $E_1 \neq \emptyset$. Los restantes elementos de la sucesión se obtienen, cada uno a partir del anterior, como sigue:

$$E_2 := g\{f(E_1)\} \neq \emptyset, \ldots, E_{n+1} := g\{f(E_n)\} \neq \emptyset, \ldots$$

La sucesión recursiva de conjuntos $\{E_n\}_{n=1}^{\infty}$ está bien definida, por el principio de inducción. Denotaremos por E la unión de todos los conjuntos de dicha sucesión, es decir, $E := \bigcup_{n=1}^{\infty} E_n$.

Consideremos ahora la aplicación $h : A \longrightarrow B$ dada por la expresión

$$h(x) := \begin{cases} f(x), & x \in E \\ g^{-1}(x), & x \in A \backslash E \end{cases}, \tag{2.2}$$

que está bien definida. En efecto, si $x \in A\backslash E$, como $A\backslash E \subset A\backslash E_1 = g(B)$, $x \in g(B)$ y, al ser g inyectiva, x tiene imagen inversa única $g^{-1}(x)$. Si probamos que h es biyectiva podremos concluir que $\alpha = \beta$.

(*a*) *h es inyectiva*: debemos probar que $x \neq y$ implica $h(x) \neq h(y)$. Para ello distinguimos los tres casos posibles siguientes:

Caso 1: $\{x, y\} \subset E$ (véase Figura 2.7).

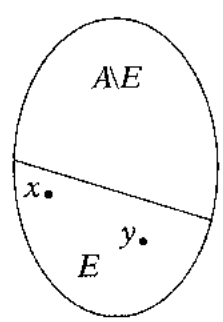

Figura 2.7. *h es inyectiva (caso 1).*

Como $x \neq y$ y f es inyectiva, se tiene $h(x) = f(x) \neq f(y) = h(y)$.

Caso 2: $\{x, y\} \subset A \backslash E$ (véase Figura 2.8).

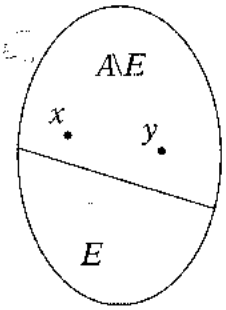

Figura 2.8. *h es inyectiva (caso 2).*

Si fuese $h(x) = h(y)$, se tendría $g^{-1}(x) = g^{-1}(y)$ y, al ser g aplicación, debería ser $x = y$.

Caso 3: $x \in E$ e $y \in A \backslash E$ (véase Figura 2.9).

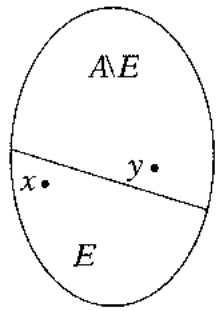

Figura 2.9. *h es inyectiva (caso 3).*

Suponiendo, de nuevo, que $h(x) = h(y)$ se tiene, recordando la definición de h en (2.2), que $f(x) = g^{-1}(y)$. Entonces obtenemos $y = g\{f(x)\} \in E$, en contradicción con $y \in A \backslash E$. En efecto, si $x \in E_n$ (x debe pertenecer a cierto conjunto de la sucesión cuya unión es E), se tendrá $g\{f(x)\} \in E_{n+1} \subset E$.

(*b*) *h es suprayectiva*: dado $z \in B$, se busca $x \in A$ tal que $h(x) = z$. Para ello conviene distinguir dos casos posibles.

Caso 1: $z \in f(E)$ (véase Figura 2.10).

En virtud de la hipótesis existirá un $x \in E \subset A$ tal que $f(x) = z$. Entonces, recordando (2.2), se tendrá $h(x) = z$.

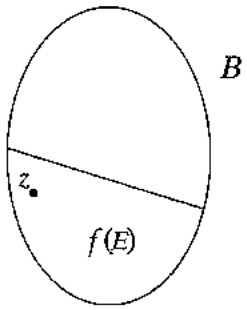

Figura 2.10. *h es suprayectiva (caso 1).*

Caso 2: $z \notin f(E)$ (véase Figura 2.11).

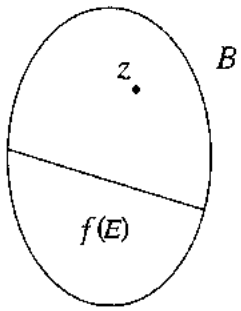

Figura 2.11. *h es suprayectiva (caso 2).*

Veremos que $x = g(z)$ satisface la condición requerida.

Como suponemos $z \notin f(E)$, se tiene que $z \notin f(E_n)$, $n = 1, 2, \ldots$ Entonces, al ser g inyectiva, deberá ser también

$$g(z) \notin g\{f(E_n)\} = E_{n+1}, n = 1, 2, \ldots$$

Además, por la definición de E_1 dada en (2.1), $g(z) \notin E_1$. En consecuencia,

$$g(z) \notin \bigcup_{n=1}^{\infty} E_n = E.$$

Como $g(z) \in A \backslash E$, usando nuevamente (2.2), tenemos

$$h[g(z)] = g^{-1}[g(z)] = z.$$

De esta forma, la prueba ha quedado completada. □

Teorema 2.4 ***(de Cantor).*** *$\alpha < 2^{\alpha}$ para todo cardinal α.*

Demostración. Sea $\alpha = \operatorname{card}(A)$. Desde luego, $\alpha \leq 2^\alpha$ como consecuencia de que la aplicación

$$\begin{aligned} A &\longrightarrow \mathcal{P}(A) \\ x &\longrightarrow \{x\} \end{aligned}$$

es inyectiva (el caso $A = \emptyset$ es trivial). Probaremos ahora que $\alpha = 2^\alpha$ es imposible (reducción al absurdo).

Sea $f : A \longrightarrow \mathcal{P}(A)$ una aplicación biyectiva. Consideramos el conjunto

$$M := \{x \in A \mid x \notin f(x)\} \tag{2.3}$$

(en principio, podría ser $M = \emptyset$ o $M = A$). En cualquier caso, $M \in \mathcal{P}(A)$, por lo que existirá un único elemento $a \in A$ tal que $f(a) = M$. Entonces, usando la definición de M dada en (2.3), se tienen las dos implicaciones siguientes cuya conjunción es siempre falsa:

$$\begin{cases} a \in M \Longrightarrow a \notin f(a) = M \\ a \notin M = f(a) \Longrightarrow a \in M\,. \end{cases}$$

Tenemos, pues, la deseada contradicción. □

Del Teorema de Cantor se sigue que no puede haber un cardinal mayor que todos los demás. Veremos, a continuación, la llamada **Paradoja de Cantor**, que niega la existencia de un conjunto «universal» U, es decir, la existencia de un conjunto que incluya a cualquier otro conjunto imaginable.

Proposición 2.5. *No existe un conjunto universal.*

Demostración. Si hubiese un conjunto universal U que contuviese a cualquier otro conjunto, se tendría $\mathcal{P}(U) \subset U$ y, por lo tanto, $2^\alpha \leq \alpha$ para $\alpha = \operatorname{card}(U)$, en contradicción con el Teorema de Cantor. □

Como consecuencia de la Proposición 2.5, dado un conjunto arbitrario A, siempre existe x tal que $x \notin A$. Un lector muy atento notará que esto ya fue usado en la Sección 2.2 (por ejemplo, en la demostración del Teorema 2.1). Sin embargo, no hemos incurrido en un círculo vicioso, pues en el Teorema de Cantor no se usa ningún resultado sobre números naturales.

Está claro que no podemos admitir como conjuntos colecciones cualesquiera de objetos, como el «conjunto universal» U o la colección de todos los cardinales (otra colección «demasiado grande» de objetos). Sólo en el contexto de una teoría formal de conjuntos puede especificarse cuándo una colección de objetos es un conjunto, pero tales teorías son excesivamente complejas y áridas para ser incluidas en un curso introductorio.

Como los cardinales finitos no son tantos (aunque no baste toda una vida para enumerarlos), aceptaremos que $\mathbb{N}$ es un conjunto (como lo son casi todas las colecciones de objetos que se consideran en matemáticas). De lo dicho hasta aquí se desprende que $(\mathbb{N}, \leq)$ es un conjunto ordenado. Veremos un par de propiedades interesantes del mismo antes de terminar esta sección.

Proposición 2.6. *Sean m y n números naturales. Entonces $m < n$ si, y sólo si, existe $p \in \mathbb{N}$ tal que $m + p = n$.*

Demostración. Sean A y B representantes de m y de n, respectivamente. Estamos suponiendo que existe una aplicación $f : A \longrightarrow B$ que es inyectiva, pero que no podrá ser suprayectiva. Sea

$$C = B \backslash f(A) \neq \emptyset.$$

Obviamente, C es finito, ya que B es finito y $C \subset B$. Como $A \sim f(A)$ y $B = f(A) \cup C$, con $f(A) \cap C = \emptyset$, se tiene entonces $n = m + \operatorname{card}(C)$. Tomando $p = \operatorname{card}(C)$, se concluye que $m + p = n$.

Recíprocamente, si $m + p = n$, entonces existen representantes A, C y B de m, p y n, respectivamente, que pueden suponerse disjuntos dos a dos, tales que $A \cup C \sim B$. Luego existe una biyección $g : A \cup C \longrightarrow B$ cuya restricción

$$g_{|A} : A \longrightarrow B$$

es inyectiva y, por lo tanto, $m \leq n$. Además, si fuera $m = n$ se tendría que $n = m + p = n + p$, es decir, se cumpliría $n = n + p$ para algún natural p. No es difícil demostrar, por inducción sobre n, que $n \neq n + p$ para todo $n, p \in \mathbb{N}$ (Problema 2.3). Por lo tanto, $m \neq n$ y, en consecuencia, $m < n$. □

Proposición 2.7. $(\mathbb{N}, \leq)$ *es un buen orden.*

Demostración. Recordando la Definición 1.18 (buen orden), consideremos un subconjunto no vacío $A \subset \mathbb{N}$ y supongamos que A no tiene mínimo (reducción al absurdo). Entonces $1 \notin A$ (ya que de lo contrario sería el mínimo), por lo que

$$1 \in \mathbb{N} \backslash A = \overline{A}. \tag{2.4}$$

Probaremos por inducción que $\overline{A} = \mathbb{N}$, lo que contradice la hipótesis $\emptyset \subsetneq A \subset \mathbb{N}$ y termina la demostración.

Consideremos la forma proposicional

$$p(n) \equiv \{1, 2, \ldots, n\} \subset \overline{A}.$$

Sabemos que $p(1)$ es verdadera por (2.4). Supongamos que para algún n natural se cumple $p(n)$ pero no $p(n+1)$, es decir,

$$\{1, 2, \ldots, n\} \subset \overline{A}$$

pero

$$\{1, 2, \ldots, n, n+1\} \not\subseteq \overline{A}.$$

Entonces $n + 1 \in A$ sería el mínimo de A (véase Problema 2.4), contradiciendo el supuesto de que A no tiene mínimo. Por lo tanto, $p(n) \Rightarrow p(n+1)$, lo que completa la prueba por inducción de que $\overline{A} = \mathbb{N}$. □

Obviamente, $(\mathbb{N}, \leq)$ es un orden total. Obsérvese que 1 es el elemento mínimo de $\mathbb{N}$, mientras que $\mathbb{N}$ carece de máximo: para todo $n \in \mathbb{N}$ se tiene que $n+1 \in \mathbb{N}$ y que $n < n+1$ (porque existe $p \in \mathbb{N}$ tal que $n+p = n+1$), con lo que ningún natural n puede ser el máximo de $\mathbb{N}$.

2.4. Conjuntos numerables

Definición 2.8. *Un conjunto A es* ***numerable*** *si $A \sim \mathbb{N}$. El cardinal de tales conjuntos,* $\operatorname{card}(\mathbb{N}) = \aleph_0$, *es el cardinal numerable ($\aleph$, símbolo que se lee «aleph», es la primera letra del alfabeto hebreo). Un conjunto A (o su cardinal) es* ***a lo sumo numerable*** *si es finito o numerable* ($\operatorname{card}(A) \leq \aleph_0$).

Todo conjunto numerable es infinito. Si A es numerable y $f : \mathbb{N} \longrightarrow A$ es biyectiva, denotando $a_n = f(n)$, puede escribirse $A = \{a_n \mid n \in \mathbb{N}\}$, que es una **enumeración** de los elementos de A (en la sucesión $\{a_n\}$ están todos los elementos de A una vez, y sólo una).

Obsérvese que cualquier conjunto numerable admite infinitas enumeraciones (reordenando los n primeros elementos de $\mathbb{N}$ se obtienen $n!$ enumeraciones de $\mathbb{N}$).

Ejemplo 2.5. (*i*) El conjunto de los números enteros, $\mathbb{Z}$, es numerable porque $\{0, 1, -1, 2, -2, \ldots\}$ es una enumeración de $\mathbb{Z}$, con $a_n = (-1)^n \lfloor n/2 \rfloor$ donde $\lfloor n/2 \rfloor$ representa la parte entera por defecto ($\lfloor 1/2 \rfloor = 0$).

(*ii*) $\mathbb{N}^2$ es numerable porque podemos enumerar sus elementos recorriendo de la manera indicada el camino que aparece en la Figura 2.12, que pasa una sola vez por todos los puntos del plano cuyas coordenadas son números naturales (existen, desde luego, otros muchos caminos que satisfacen esta condición. Véase, por ejemplo, el Problema 2.15).

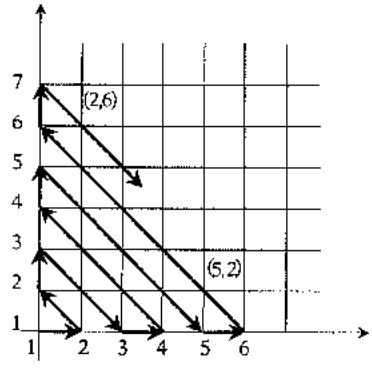

Figura 2.12. *Enumeración de $\mathbb{N}^2$.*

(*iii*) El conjunto de los racionales positivos, $\mathbb{Q}^+$, es numerable porque todo racional positivo se expresa de forma única como fracción m/n (con m, $n \in \mathbb{N}$ y primos entre sí). Entonces la aplicación

$$\begin{aligned} \mathbb{Q}^+ &\longrightarrow \mathbb{N}^2 \\ \frac{m}{n} &\longmapsto (m,n) \end{aligned}$$

es inyectiva y, por lo tanto,

$$\operatorname{card}(\mathbb{Q}^+) \leq \operatorname{card}(\mathbb{N}^2) = \aleph_0.$$

Como, además, $\mathbb{N} \subset \mathbb{Q}^+$, también se tiene que $\aleph_0 \leq \operatorname{card}(\mathbb{Q}^+)$ y, por la propiedad antisimétrica del orden, se concluye que

$$\operatorname{card}(\mathbb{Q}^+) = \aleph_0.$$

Proposición 2.8. *Para cualquier cardinal α, $\aleph_0 \leq \alpha$ si, y solamente si, α es infinito.*

Demostración. Debemos probar las dos afirmaciones del enunciado.

(a) Si $\aleph_0 \leq \alpha$ y $\operatorname{card}(A) = \alpha$, entonces existe una aplicación inyectiva $f : \mathbb{N} \longrightarrow A$. Como $f(\mathbb{N}) \sim \mathbb{N}$ y $f(\mathbb{N}) \subset A$, A contiene un conjunto infinito, de modo que A es también infinito.

(b) Suponiendo que A es infinito, existe una aplicación $g : A \longrightarrow A$ que es inyectiva pero no suprayectiva.

A partir de un elemento $a \in A \backslash g(A)$ arbitrario y usando la función g, definimos una sucesión recursiva $\{a_n\}_{n=1}^{\infty}$ como sigue:

$$a_1 := a;\ a_2 := g(a_1);\ \ldots;\ a_{n+1} := g(a_n);\ldots$$

Desde luego $a_{n+1} \in g(A)$, de manera que, para todo $n \in \mathbb{N}$, se tiene

$$a_{n+1} \neq a_1 = a. \tag{2.4}$$

Probaremos por inducción que $a_{n+1} \notin \{a_1, \ldots, a_n\}$ para todo $n \in \mathbb{N}$. Para $n = 1$, usando (2.4), se cumple la afirmación $a_2 \notin \{a_1\}$. Supongamos ahora que $a_{n+1} \notin \{a_1, \ldots, a_n\}$ y analicemos el elemento a_{n+2}. Por la inyectividad de g se tiene

$$a_{n+2} = g(a_{n+1}) \notin \{g(a_1), \ldots, g(a_n)\} = \{a_2, \ldots, a_{n+1}\}.$$

Como además, nuevamente por (2.4), se cumple que $a_{n+2} \neq a_1$, obtenemos $a_{n+2} \notin \{a_1, \ldots, a_{n+1}\}$, con lo que concluye la demostración por inducción.

Esto prueba que la aplicación $f : \mathbb{N} \longrightarrow A$, con $f(n) = a_n$, es inyectiva. En efecto, si $m \neq n$, deberá ser $m < n$ o $n < m$ (Proposición 2.7). En el primer caso

$$f(n) \notin \{f(1), \ldots, f(n-1)\},$$

conjunto que contiene a $f(m)$, por lo que $f(n) \neq f(m)$, llegándose a la misma conclusión en el segundo caso.

Al ser $f: \mathbb{N} \longrightarrow A$ inyectiva, $\aleph_0 \leq \operatorname{card}(A)$, que es la conclusión deseada. □

Corolario 2.4. *Para cualquier cardinal α, $\alpha < \aleph_0$ si, y solamente si, α es finito.*

Demostración. Demostraremos el directo por reducción al absurdo (tautología 1.23). Supongamos $\alpha < \aleph_0$ y α infinito. Entonces, por la Proposición 2.8, $\aleph_0 \leq \alpha$. Pero $(\alpha < \aleph_0) \wedge (\aleph_0 \leq \alpha)$ es una contradicción debido a que la relación entre cardinales es RBO.

Supongamos ahora que α es finito. El caso $\alpha = 0$ es trivial. En otro caso, α es un número natural, por lo que

$$\alpha = n = \operatorname{card}(\{1, 2, \ldots, n\}) < \operatorname{card}(\mathbb{N}) = \aleph_0. \ \square$$

La prueba de los dos siguientes corolarios se deja como ejercicio.

Corolario 2.5. *Un conjunto es infinito si, y sólo si, contiene un subconjunto numerable.*

Corolario 2.6. *Todo subconjunto de un conjunto numerable es a lo sumo numerable.*

Probaremos a continuación algunas propiedades de los conjuntos numerables, empezando por justificar las decisiones tomadas por Hilbert para alojar a los recién llegados a su hotel.

Proposición 2.9. $\aleph_0 + \alpha = \aleph_0$, *para todo cardinal* $\alpha \leq \aleph_0$.

Demostración. Si $\mathbb{Z}^-$ denota al conjunto de los enteros negativos, entonces $\mathbb{Z}^- \sim \mathbb{N}$, puesto que

$$\begin{aligned} \mathbb{N} &\longrightarrow \mathbb{Z}^- \\ n &\longmapsto -n \end{aligned}$$

es una biyección. Considerando, además, que $\emptyset = \mathbb{Z}^- \cap \{1, 2, \ldots, n\} = \mathbb{Z}^- \cap \mathbb{N}$ y

$$\mathbb{Z}^- \subset \mathbb{Z}^- \cup \{1, 2, \ldots, n\} \subset \mathbb{Z}^- \cup \mathbb{N} \subset \mathbb{Z},$$

tenemos

$$\aleph_0 \leq \aleph_0 + n \leq \aleph_0 + \aleph_0 \leq \aleph_0,$$

para todo $n \in \mathbb{N}$, llegándose a la conclusión deseada al aplicar el Teorema de Bernstein. □

Corolario 2.7. *La unión de dos conjuntos a lo sumo numerables, es a lo sumo numerable.*

Demostración. Sean A y B conjuntos finitos o numerables. Definimos el conjunto $C := B \backslash A \subset B$ que es a lo sumo numerable por el Corolario 2.6. Entonces $A \cup B = A \cup C$, con $A \cap C = \emptyset$, por lo que

$$\operatorname{card}(A \cup B) = \operatorname{card}(A \cup C) = \operatorname{card}(A) + \operatorname{card}(C) \leq \aleph_0 ,$$

siendo la última desigualdad consecuencia del Corolario 2.4, cuando A y B son finitos, y de la Proposición 2.9 en otro caso. □

Proposición 2.10. $\aleph_0 \times \aleph_0 = \aleph_0$. *Por lo tanto, el producto cartesiano de dos conjuntos numerables es también numerable.*

Demostración. $\operatorname{card}(\mathbb{N}^2) = \aleph_0 \times \aleph_0$ y vimos en el Ejemplo 2.5*ii*) que $\operatorname{card}(\mathbb{N}^2) = \aleph_0$. La segunda afirmación es consecuencia inmediata de

$$\operatorname{card}(A) \times \operatorname{card}(B) = \operatorname{card}(A \times B) . \ \square$$

Las Proposiciones 2.9 y 2.10 muestran que las operaciones con cardinales no satisfacen las leyes de cancelación (a menos que dichos cardinales sean naturales).

Ejemplo 2.6. $\mathbb{Q}$ es numerable. En efecto, llamando $\mathbb{Q}^-$ a los racionales negativos y $\mathbb{Q}^+$ a los positivos, $\mathbb{Q}^- \sim \mathbb{Q}^+ \sim \mathbb{N}$ y se tiene entonces

$$\operatorname{card}(\mathbb{Q}) = \operatorname{card}(\mathbb{Q}^- \cup [\{0\} \cup \mathbb{Q}^+]) = \aleph_0 + \aleph_0 = \aleph_0.$$

Teorema 2.5. *La unión numerable de conjuntos numerables es numerable.*

En la Sección 2.6 se dará una prueba de este resultado que es compatible con el enfoque adoptado en este libro (véase Teorema 2.8). Nos limitaremos a utilizar el Teorema 2.5 para obtener el siguiente útil resultado cuya prueba se deja como ejercicio.

Corolario 2.8. *Una unión a lo sumo numerable de conjuntos a lo sumo numerables es a lo sumo numerable.*

2.5. El cardinal del continuo

En matemáticas elementales se afirma que, al representar los números reales sobre una recta graduada (con origen y longitud unidad), no quedan agujeros. En otras palabras, los números reales tienen una representación continua sobre la recta. Esta propiedad, que se precisará en el Capítulo 5, motiva la siguiente definición.

Definición 2.9. *Un conjunto se dice que tiene el* ***cardinal del continuo*** *si es equipotente al conjunto de los números reales,* $\mathbb{R}$. *Se denota por* $c = \operatorname{card}(\mathbb{R})$.

Ejemplo 2.7. Veamos que todos los intervalos propios de números reales tienen el cardinal del continuo.

(a) Si $a < b$, entonces

$$\operatorname{card}(]a,b[) = c$$

porque hemos visto en los Ejemplos 2.1 y 2.2 que todos los intervalos propios son equipotentes entre sí y que $]-1,\ 1[\sim \mathbb{R}$.

(b) Todo intervalo propio I (cerrado o no por sus extremos, de longitud mayor que cero, finita o no) contiene un intervalo de la forma $]a,b[$ con $a < b$. Como $]a,b[\subset I \subset \mathbb{R}$, se tiene

$$c \leq \operatorname{card}(I) \leq c,$$

es decir,

$$\operatorname{card}(I) = c.$$

Como $\mathbb{N} \subset \mathbb{R}$ sabemos que $\aleph_0 \leq c$. Vamos a clasificar el cardinal del continuo comparando un intervalo de longitud uno de la recta real con el conjunto $\{0,\ 1\}^{\mathbb{N}}$ de todas las sucesiones con valores en la pareja $\{0,\ 1\}$.

Lema 2.1. *Existe una aplicación inyectiva* $f : [0,\ 1[\longrightarrow \{0,\ 1\}^{\mathbb{N}}$. *Por lo tanto,* $c \leq \operatorname{card}\left(\{0,\ 1\}^{\mathbb{N}}\right)$.

Demostración. Para cada número real $x \in [0,\ 1[$ construiremos una sucesión $\{x_n\}_{n=1}^{\infty}$ con valores 0 ó 1. Para ello, partimos $[0,\ 1[$ en dos subintervalos semiabiertos disjuntos $[0, \frac{1}{2}[$ y $[\frac{1}{2}, 1[$. Entonces, $x \in [0, \frac{1}{2}[$ o bien $x \in [\frac{1}{2}, 1[$, y definimos el primer término de la sucesión así:

$$x_1 := \begin{cases} 0, & \text{si } x \in [0, \frac{1}{2}[\\ 1, & \text{si } x \in [\frac{1}{2}, 1[\,. \end{cases}$$

Ahora, partimos $[0,\ 1[$ en cuatro subintervalos semiabiertos de longitud $1/4$ que enumeramos consecutivamente al recorrerlos de izquierda a derecha. Definimos entonces $x_2 = 0$, si x pertenece al primer o tercer intervalo, o bien $x_2 = 1$, cuando x pertenece al segundo o al cuarto. En general, partiendo $[0,\ 1[$ en 2^n subintervalos consecutivos de longitud $1/2^n$, definimos $x_n = 0$ si x pertenece a un subintervalo impar, o $x_n = 1$ si x pertenece a un subintervalo par (véase Figura 2.13).

Definimos, entonces, la aplicación

$$\begin{aligned} f : [0,\ 1[&\longrightarrow \{0,\ 1\}^{\mathbb{N}} \\ x &\longmapsto \{x_n\}\,. \end{aligned}$$

A dos números reales diferentes $x, y \in [0,\ 1[$ se les asignan sucesiones también diferentes, pues ambos números reales no pueden pertenecer, para todo $n \in \mathbb{N}$, a los mismos subintervalos de longitud $1/2^n$ (como se verá en la

Sección 5.3, esto se debe a la propiedad arquimediana de los reales). Por lo tanto, la aplicación f es inyectiva y $c \leq \operatorname{card}\left(\{0,1\}^{\mathbb{N}}\right)$. □

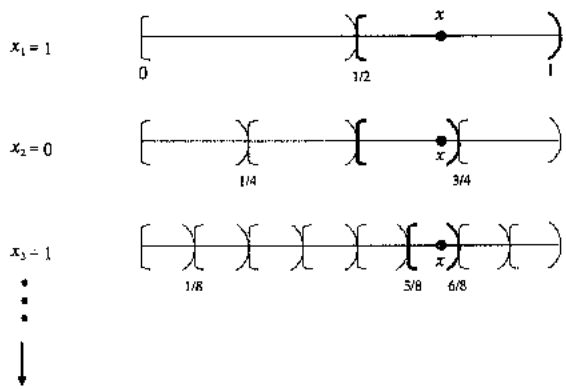

Figura 2.13. *Definición de $\{x_n\}$ a partir de x.*

La sucesión construida en el Lema 2.1 produce una expresión *en cifras binarias* del número real x $(0{,}x_1x_2x_3\cdots)$, análoga a la conocida expresión *decimal*. El desarrollo decimal se tratará en el Capítulo 5 (Teorema 5.1 (*ii*), Proposición 5.6 y Teorema 5.7).

Lema 2.2. *Existe una aplicación inyectiva $g : \{0,1\}^{\mathbb{N}} \longrightarrow [0,1]$.* Por lo tanto, $\operatorname{card}\left(\{0,1\}^{\mathbb{N}}\right) \leq c$.

Demostración. Dada una sucesión $\{x_n\}_{n=1}^{\infty}$ de ceros y unos definiremos primeramente una sucesión recursiva $\{I_n\}$ de intervalos cerrados encajados. Para ello partimos el intervalo cerrado $[0,1]$ en tres subintervalos disjuntos consecutivos de longitud 1/3: $[0,\frac{1}{3}]$, $]\frac{1}{3},\frac{2}{3}[$ y $[\frac{2}{3},1]$, y eliminamos el intervalo abierto central. Definimos el primer término de la sucesión por

$$I_1 = [a_1, b_1] := \begin{cases} \left[0, \frac{1}{3}\right], & \text{si } x_1 = 0 \\ \left[\frac{2}{3}, 1\right], & \text{si } x_1 = 1\,. \end{cases}$$

Ahora partimos I_1 en tres subintervalos disjuntos consecutivos de longitud 1/9, eliminamos el intervalo abierto central y definimos I_2 como el subintervalo de la izquierda o el de la derecha dependiendo de si $x_2 = 0$ ó $x_2 = 1$. En cualquier caso, $I_2 \subset I_1$ y la longitud de I_2 es 1/9.

En general, I_{n+1} será el tercio izquierdo del intervalo cerrado I_n, si $x_{n+1} = 0$, o bien el tercio derecho, si $x_{n+1} = 1$. En cualquier caso, $I_{n+1} \subset I_n$ y la longitud de I_n es $b_n - a_n = (1/3)^n$ (véase Figura 2.14).

La sucesión $\{I_n\}$ así construida es de intervalos cerrados encajados y la longitud $b_n - a_n$ tiende a 0, cuando n tiende a infinito. Veremos en el Capítulo 5 que, bajo estas condiciones, existe un único número real $z \in \bigcap_{n=1}^{\infty} I_n$ (principio de encaje de intervalos).

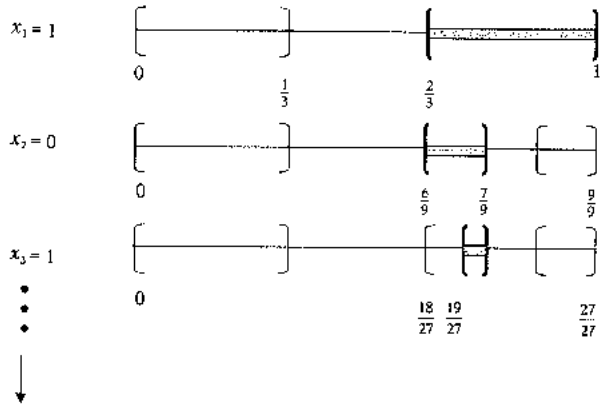

Figura 2.14. *Definición de $\{I_n\}$ a partir de $\{x_n\}$.*

Resumiendo, hemos demostrado la existencia de una aplicación

$$\begin{array}{rcl} g : \{0, 1\}^{\mathbb{N}} & \longrightarrow & [0, 1] \\ \{x_n\} & \longmapsto & z \end{array} .$$

Es claro que g es una aplicación inyectiva y, por lo tanto, $\operatorname{card}\left(\{0, 1\}^{\mathbb{N}}\right) \leq c$. □

La siguiente relación entre $\aleph_0$ y c es particularmente interesante.

Proposición 2.11. $2^{\aleph_0} = \operatorname{card}\left(\{0, 1\}^{\mathbb{N}}\right) = c$.

Demostración. La segunda igualdad se obtiene inmediatamente de los Lemas 2.1 y 2.2 y del Teorema de Bernstein.

Para la primera probaremos que

$$\operatorname{card}(\mathcal{P}(\mathbb{N})) = \operatorname{card}\left(\{0, 1\}^{\mathbb{N}}\right).$$

Para ello es suficiente señalar que a cada sucesión $\{x_n\}_{n=1}^{\infty}$ de ceros y unos se le puede asignar, de manera natural, el subconjunto $A \subset \mathbb{N}$ definido por

$$A = \{n \in \mathbb{N} \mid x_n = 1\} ,$$

y, recíprocamente, dado un subconjunto cualquiera $A \subset \mathbb{N}$ se define una sucesión $\{x_n\}_{n=1}^{\infty}$ así:

$$x_n = \begin{cases} 1, & \text{si } n \in A \\ 0, & \text{si } n \notin A . \end{cases}$$

Habiendo establecido una aplicación biyectiva entre $\mathcal{P}(\mathbb{N})$ y $\{0, 1\}^{\mathbb{N}}$, ambos conjuntos son equipotentes. □

Como consecuencia de la Proposición 2.11 y del teorema de Cantor se tiene que $\aleph_0 < c$. Este resultado, probado por Cantor en 1874, le sugirió la clasificación de los conjuntos –por su tamaño– a través de la noción de cardinal, introducida en 1878.

Enunciaremos a continuación algunas propiedades casi inmediatas de esta curiosa «aritmética» de cardinales.

Proposición 2.12. $c + \aleph_0 = c$.

Demostración. Consecuencia de que $\mathbb{R}^+ \subset \mathbb{R}^+ \cup \mathbb{Z}^- \subset \mathbb{R}$ y del Teorema de Bernstein. □

Proposición 2.13. $c + c = c$.

Demostración. Usando que $\mathbb{R}_+ \cup \mathbb{R}^- = \mathbb{R}$. □

Proposición 2.14. $c \times \aleph_0 = c$.

Demostración. Resulta de considerar la siguiente aplicación biyectiva:

$$\begin{aligned} f : [0, 1[\times \mathbb{Z} &\longrightarrow \mathbb{R} \\ (x, n) &\longmapsto x + n. \end{aligned}$$ □

Proposición 2.15. $c \times c = c$.

Demostración. Probaremos que $\{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}} \sim \{0, 1\}^{\mathbb{N}}$.

Una de las desigualdades es trivial, ya que

$$\{0, 1\}^{\mathbb{N}} \sim \{0, 1\}^{\mathbb{N}} \times \{s\} \subset \{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}},$$

para cualquier conjunto singular $\{s\} \subset \{0, 1\}^{\mathbb{N}}$.

Para la otra desigualdad, será suficiente probar que existe una aplicación inyectiva

$$f : \{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}} \longrightarrow \{0, 1\}^{\mathbb{N}}.$$

Con tal fin, para cada par de sucesiones $\{x_n\}$ e $\{y_n\}$ en $\{0, 1\}^{\mathbb{N}}$ se define la sucesión intercalada

$$\{z_n\}_{n=1}^{\infty} = \{x_1, y_1, x_2, y_2, \ldots\ldots\}.$$

Se comprueba fácilmente que esta aplicación es inyectiva. □

Como consecuencia, el plano cartesiano $\mathbb{R}^2$ tiene el cardinal del continuo. Esta propiedad sorprendió a los matemáticos contemporáneos a Cantor, provocando una fuerte polémica entre ellos. Afortunadamente, la equipotencia entre recta y plano no causa en la actualidad ninguna controversia.

No menos fuerte es la polémica que surge de la pregunta, natural por cierto, sobre la existencia de conjuntos con cardinales intermedios, entre $\aleph_0$ y $2^{\aleph_0}$. Reservamos un análisis de esta cuestión para la siguiente sección.

2.6. Proposiciones indemostrables

Acabaremos este capítulo introduciendo, de modo muy superficial, algunas ideas sobre aspectos complejos de la teoría de conjuntos. Empezaremos por referirnos a ciertas proposiciones que no pueden demostrarse, como tampoco pueden serlo sus negaciones. De hecho, todas ellas fueron introducidas por famosos matemáticos que creyeron que eran verdaderas, en algunos casos dándose incluso una «prueba» que contenía un círculo vicioso. Una de estas proposiciones involucra el concepto de producto cartesiano de una familia (posiblemente infinita) de conjuntos. Para motivar este concepto, que generaliza el producto cartesiano de dos conjuntos, observemos que $\mathbb{R}^2$ es equipotente al conjunto $\mathbb{R}^{\{1,2\}}$ de las aplicaciones de $\{1, 2\}$ en $\mathbb{R}$, pues basta asociar a cada par ordenado $(a_1, a_2) \in \mathbb{R}^2$ la aplicación $f: \{1, 2\} \longrightarrow \mathbb{R}$ dada por

$$f(x) = \begin{cases} a_1, & x = 1 \\ a_2, & x = 2 \end{cases},$$

de modo que

$$(a_1, a_2) = (f(1), f(2)).$$

Por esa razón se define el producto cartesiano de $\mathbb{R}$ por sí mismo n veces, $\mathbb{R}^n$, como $\mathbb{R}^{\{1,\dots,n\}}$, conjunto de las aplicaciones $f : \{1, \dots, n\} \longrightarrow \mathbb{R}$, que se identifican con las n-plas $(f(1), f(2), \dots, f(n))$. Más en general, dados n conjuntos no vacíos $A_1, \dots, A_n$ arbitrarios,

$$A_1 \times \cdots \times A_n = \{f : \{1, \dots, n\} \longrightarrow (A_1 \cup \cdots \cup A_n) \mid f(i) \in A_i, i = 1, \dots, n\}.$$

Bajo estas condiciones, $A_1 \times A_2 \neq \emptyset$, y se demuestra por inducción que $A_1 \times \cdots \times A_n \neq \emptyset$, cualquiera sea $n \in \mathbb{N}$. Ya estamos en condiciones de definir el producto cartesiano de una familia, finita o infinita, de conjuntos.

Definición 2.10. *Dada una familia $\{A_i, i \in I\}$ de conjuntos no vacíos se define el* ***producto cartesiano*** *de dicha familia como el conjunto de las aplicaciones que asocian a cada índice un elemento del conjunto correspondiente al mismo, es decir,*

$$\prod_{i \in I} A_i := \left\{ f : I \longrightarrow \bigcup_{i \in I} A_i \mid f(i) \in A_i, \text{ para todo } i \in I \right\}.$$

Ahora podemos enunciar las conjeturas (o proposiciones indemostrables) más célebres de la teoría de conjuntos. Los nombres obedecen a razones históricas.

Axioma de elección. *Si $\{A_i, i \in I\}$ es una familia (posiblemente infinita) de conjuntos no vacíos, entonces* $\prod_{i \in I} A_i \neq \emptyset$.

Hemos visto que para una familia finita no es necesario este axioma.

En el Problema 2.24 se muestran otras maneras de formularlo.

Hay conjuntos no vacíos cuyos elementos son tan raros que no se conoce ninguno. Se sabe, por ejemplo, que existen funciones que son continuas en un intervalo pero que oscilan (ni son crecientes ni decrecientes) en cualquier subintervalo, pero nadie ha sido capaz de encontrar una de tales funciones. Algo parecido ocurre con productos cartesianos infinitos.

Hipótesis del continuo. *El cardinal que sigue a $\aleph_0$ es c, es decir,*

$$c = \min \{\alpha \mid \aleph_0 < \alpha\}.$$

Si se acepta la Hipótesis del continuo se justifica la notación $\aleph_1$ para el cardinal del continuo.

Hipótesis del continuo generalizada (Tarski). *Si α es un cardinal infinito (o transfinito), el cardinal que le sigue es 2^α.*

Así, los primeros cardinales serían

$$1, 2, \ldots\ldots; \aleph_0; \aleph_1 = 2^{\aleph_0}; \aleph_2 = 2^{\aleph_1}; \ldots\ldots$$

Teorema de Zermelo. *Todo conjunto no vacío puede ser bien ordenado.*

Zermelo probó este enunciado a partir del siguiente axioma.

Lema de Zorn. *Sea $(A, \preceq)$ un conjunto no vacío ordenado. Si todo subconjunto $S \subset A$, tal que $(S, \preceq)$ es totalmente ordenado con el orden inducido, tiene cota superior en A, entonces existe al menos un elemento maximal de A.*

Buena ordenación de cardinales. *Todo conjunto de cardinales está bien ordenado con el orden natural (existencia de aplicación inyectiva entre representantes).*

Una base de Hamel de un espacio vectorial (de dimensión posiblemente infinita) es un subconjunto generador y linealmente independiente (volveremos sobre dichas bases en la Sección 7.1).

Existencia de bases de Hamel. *Todo espacio vectorial tiene al menos una base de Hamel.*

Se han establecido las siguientes relaciones entre estas proposiciones «indemostrables»:

$$\text{H. continuo general} \begin{array}{l} \nearrow \text{ H. del continuo} \\ \searrow \text{ Axioma de elección} \\ \qquad \Updownarrow \\ \text{Teorema de Zermelo} \\ \qquad \Updownarrow \\ \text{Lema de Zorn} \\ \qquad \Updownarrow \\ \text{Buena ordenación de cardinales} \\ \qquad \Updownarrow \\ \text{Existencia de bases de Hamel} \end{array} \Rightarrow \begin{array}{c} \text{A. de elección numerable} \\ \Updownarrow \\ \text{Unión numerable de conjuntos numerables es numerable} \end{array}$$

El Axioma de Elección (AE para abreviar), y sus varias equivalencias, es probablemente el más discutido axioma de la matemática, después del postulado de las paralelas de Euclides. La *consistencia* de AE con los axiomas de Zermelo-Fraenkel (ZF para abreviar), que fundamentan la teoría de conjuntos, fue demostrada por Gödel en 1938. La *independencia* de AE respecto de la axiomática ZF fue demostrada por Paul Cohen en 1963. La dificultad para su aceptación estriba en que AE (o cualquiera de sus equivalencias) afirma la existencia de un objeto matemático sin exhibirlo ni proporcionar ninguna pista sobre cómo construirlo. AE puede parecer intuitivamente evidente, pero su aceptación obliga a aceptar también, por ejemplo, que el conjunto de los números reales puede ser bien ordenado, hecho para nada evidente. Por eso, los matemáticos siempre tratan de evitar el uso de estas conjeturas, salvo que sea imposible dar una prueba alternativa, advirtiendo expresamente su eventual utilización. Por ejemplo, del axioma de elección se sigue que todo conjunto equipotente a una parte propia contiene un subconjunto numerable, pero es preferible una prueba por inducción (como la dada en la Proposición 2.8 (*b*)).

A efectos ilustrativos demostraremos una de las implicaciones más sencillas. Aceptando lo afirmado en el Teorema de Zermelo probaremos el axioma de elección. En la Sección 7.1 se probará, suponiendo el Lema de Zorn, la existencia de bases de Hamel en espacios vectoriales.

Teorema 2.6. *Si todo conjunto no vacío puede ser bien ordenado, entonces, para cualquier familia de conjuntos no vacíos* $\mathcal{C} = \{A_i, i \in I\}$, *se cumple* $\prod_{i \in I} A_i \neq \emptyset$.

Demostración. Debemos probar que existe una aplicación

$$f : I \longrightarrow \bigcup \mathcal{C}$$

tal que $f(i) \in A_i$ para cada $i \in I$. Por hipótesis, existe un buen orden $\leq$ en el conjunto $\bigcup \mathcal{C}$. Cada A_i es un subconjunto no vacío de $\bigcup \mathcal{C}$, por lo que tiene (un único) primer elemento $a_i = \min A_i$, con respecto al orden $\leq$ restringido. Entonces, está bien definida una aplicación f que, a cada $i \in I$, le asigna el

primer elemento de A_i. Hemos establecido directamente la existencia de una aplicación $f \in \prod_{i \in I} A_i$. □

Concluiremos esta sección con las pruebas aplazadas de los Teoremas 2.2 y 2.5, basadas en la buena ordenación de cualquier conjunto de cardinales y en el axioma de elección, respectivamente. Como los nuevos enunciados añaden la correspondiente hipótesis se renumeran dichos teoremas.

Teorema 2.7. *Supongamos que todo conjunto de cardinales está bien ordenado con el orden natural. Entonces, si un subconjunto $A \subset \mathbb{N}$ satisface las propiedades*

(*i*) $1 \in A$; *y*
(*ii*) $n \in A \Longrightarrow n+1 \in A$ *para todo* $n \in \mathbb{N}$

se cumple la igualdad $A = \mathbb{N}$.

Demostración. Supongamos que $A \subsetneq \mathbb{N}$. Por hipótesis, el conjunto de cardinales $\mathbb{N} \backslash A \neq \emptyset$, tiene un primer cardinal $p = \min\,(\mathbb{N} \backslash A)$. Naturalmente, $p \neq 1$, pues $1 \in A$ por la hipótesis (*i*). Sea P un conjunto (finito) tal que $\operatorname{card}(P) = p$. Como $P \neq \emptyset$, sea $x \in P$ y consideramos el conjunto $Q = P \backslash \{x\} \subsetneq P$. Entonces, $q = \operatorname{card}(P \backslash \{x\}) \neq 0$ y

$$q = \operatorname{card}(P \backslash \{x\}) \leq \operatorname{card}(P) = p.$$

Como P es finito, q también es un número natural. Si fuera $q = p$, P sería equipotente a una parte propia, contradiciendo su carácter finito. Por lo tanto, $q < p$, y siendo p el mínimo de $\mathbb{N} \backslash A$, se tiene que $q \notin \mathbb{N} \backslash A$, es decir, $q \in A$. Usando la hipótesis (*ii*), $q + 1 \in A$. Pero

$$q + 1 = \operatorname{card}(P \backslash \{x\}) + \operatorname{card}\,(\{x\}) = \operatorname{card}(P) = p.$$

Esto implica que $p \in A$, lo cual es una contradicción. □

Nota al Teorema 2.7. En la demostración del teorema anterior se supone que el orden entre cardinales es RBO, propiedad que fuera demostrada en el Teorema 2.3 (de Bernstein). En dicha prueba hemos usado inducción, pero sólo para el caso de cardinales infinitos. Como el Teorema 2.7 se refiere a números naturales (cardinales finitos), no hemos incurrido en un círculo vicioso.

Por otro lado, parece que el principio de inducción fuera consecuencia del axioma de elección. Esto requiere una aclaración. Con la definición de número natural adoptada en este texto (cardinal de un conjunto no equipotente a una parte propia), el axioma de elección se hace indispensable. Sin embargo, hay otras construcciones conjuntistas de los números naturales en las que el principio de inducción se demuestra sin usar el axioma de elección. Existe, por ejemplo, una construcción muy similar a la del texto (pero más difícil), basada en la definición de conjunto finito según Tarski (véase Problema 2.18), que no

lo necesita. Pero en esa versión es un teorema la afirmación «un conjunto no finito (Tarski) es equipotente a una parte propia», y, para demostrarlo, sí se requiere el axioma de elección.

Teorema 2.8. *Suponiendo que se cumple el axioma de elección, entonces la unión numerable de conjuntos numerables es numerable.*

Demostración. Sea $\{A_n \mid n \in \mathbb{N}\}$ una familia numerable de conjuntos numerables, y sea $B := \cup_{n=1}^{\infty} A_n$.

Cada conjunto A_n puede ser enumerado de infinitas maneras distintas. Sea E_n el conjunto de todas las enumeraciones de A_n. Una aplicación de $\Pi_{n=1}^{\infty} E_n$ proporciona la enumeración simultánea de todos los elementos de la familia $\{A_n \mid n \in \mathbb{N}\}$.

Sea, pues, $A_n = \{a_{nm}, m \in \mathbb{N}\}$, $n = 1, 2, \ldots$ La aplicación definida por

$$\begin{array}{rccc} g: & \mathbb{N}^2 & \longrightarrow & B \\ & (n,m) & \longmapsto & a_{nm} \end{array}$$

es, obviamente, suprayectiva, por lo que $\{g^{-1}(b) \mid b \in B\}$ es una familia de conjuntos no vacíos contenidos en $\mathbb{N}^2$.

Sea $f \in \Pi_{b \in B} g^{-1}(b)$. Desde luego, $f : B \longrightarrow \mathbb{N}^2$ y $f(b) \in g^{-1}(b)$ (es decir, $g[f(b)] = b$) para todo $b \in B$.

Es fácil probar que f es inyectiva. En efecto, si se cumple $f(b) = f(b')$ para $b, b' \in B$, se tiene $g[f(b)] = g[f(b')]$, es decir, $b = b'$.

Por la inyectividad de f,

$$\operatorname{card}(B) \leq \operatorname{card}(\mathbb{N}^2) = \aleph_0$$

(Proposición 2.10), mientras que $A_1 \subset B$ implica $\aleph_0 \leq \operatorname{card}(B)$. Aplicando, una vez más el Teorema de Bernstein, se concluye que $\operatorname{card}(B) = \aleph_0$. □

En la prueba del Teorema 2.8 el AE se usa dos veces, siendo esencial tan sólo la primera de ellas (al ser $\mathbb{N}^2$ numerable, está bien ordenado y puede definirse $f(b)$ como el mínimo de $g^{-1}(b)$, y esto para todo $b \in B$).

2.7. Teorías axiomáticas

La teoría intuitiva de conjuntos da lugar a paradojas inadmisibles, las más célebres de las cuales fueron descubiertas por Cantor en 1899 (Proposición 2.5) y por Russell en 1902 (Problema 2.29), ambas surgidas al considerar conjuntos «demasiado grandes». La única estrategia capaz de evitar las paradojas consiste en axiomatizar la teoría de conjuntos, de tal forma que la definición de un conjunto por comprehensión, es decir, mediante cualquier forma proposicional, esté regulada por reglas restrictivas que permitan obtener unos conjuntos a partir de otros sólo si se cumplen determinadas condiciones.

Pocos autores han sido capaces de describir de forma tan simple la naturaleza de un sistema axiomático formal como Jean Dieudonné, señalado miembro del grupo Bourbaki, de cuyo artículo «Les méthodes axiomatiques

modernes et les fondements des mathématiques» (*Actualités Scientifiques et Industrielles*, 77, pp. 224-232) traducimos un fragmento:

«Se trata de fundar las matemáticas sobre bases indiscutibles, es decir, que los términos que figuran en un texto matemático deben tener el mismo sentido para todos los lectores, y que, por otra parte, debe existir un método objetivo que permita discernir si dicho texto es correcto sin réplica posible. La tesis esencial de Hilbert, que hemos hecho nuestra, es que no cabe hablar de pensamiento claro más que tratando de objetos determinados y en número finito (...).

Pero si queremos permanecer en lo finito, ¿podemos todavía hacer la mayor parte de los razonamientos matemáticos? ¿Podemos incluso enunciar la mayor parte de las proposiciones sin pérdida de sentido? Cuando enunciamos la siguiente proposición, concerniente a los números reales, 'cualesquiera que sean x e y se tiene $x+y=y+x$', ¿no estamos expresando el hecho de que las sumas son iguales para todos los números reales que podrían reemplazar a x e y? Se puede muy bien, como enseña el método axiomático, hacer abstracción de toda intuición sobre la naturaleza propia de los números reales y razonar sobre ellos como si fuesen seres indeterminados cuyas propiedades, enunciadas en los axiomas, son las únicas que se tienen en cuenta; pero no puedo impedir que el lector piense que mi proposición es de un orden diferente de la que se formularía al reemplazar sucesivamente en la relación $x+y=y+x$, la pareja (x,y) por parejas de números reales determinados, por numerosos que sean, uniendo las proposiciones obtenidas con el signo $\wedge$. ¿No parece inevitable la introducción de la noción de infinito?

Hilbert escapa a este dilema de una manera tan simple como original. Sin duda existe una antinomia entre el contenido de la proposición anterior y la idea de que los razonamientos deben reposar sobre lo determinado; pero no existe ninguna contradicción entre este punto de vista y la escritura de la proposición

$$\forall x, y \in \mathbb{R} \quad x+y=y+x,$$

que aparece como un ensamblaje, en un cierto orden, de los signos $\forall$ (léase «para todo») x, y, $\in$, $\mathbb{R}$, $+$ e $=$, signos bien determinados y en número bien pequeño. Parece imposible eludir la noción de infinito mientras se considere que lo esencial de una proposición es su contenido, es decir, la representación mental que simboliza; pero la dificultad se desvanece si se admite que lo esencial de la proposición es su forma; en otras palabras, es inútil que una proposición evoque una representación mental distinta de la percepción de los signos con los cuales ha sido escrita.

Esta posición es tan extraña y paradójica a primera vista que no parece digna de un examen: ¿se puede sostener la posibilidad de llevar un razonamiento sin comprender una palabra de lo que se dice? En suma, ¿qué son las palabras del lenguaje y los signos matemáticos, destinados como están a comunicar representaciones mentales, y cómo se les puede desarraigar de esas representaciones sin convertirlos en ininteligibles?

Ésta es, sin embargo, la idea fundamental de Hilbert; en el enunciado de las proposiciones matemáticas, los signos empleados son signos puros, desnudos de toda significación. Para ver cómo puede uno ver las cosas desde

esa perspectiva tomaremos como término de comparación un juego, el ajedrez por ejemplo; con las piezas de este juego, que tienen formas y colores diversos a fin de poder distinguirlas, se forman sobre el tablero ensamblajes que se suceden siguiendo un proceso sometido a ciertas reglas establecidas de una vez por todas pero de manera que, cuando son igualmente posibles, en virtud de las reglas, diversos movimientos, la elección del más conveniente se deja al arbitrio del jugador. Lo que es esencial observar es que, para jugar al ajedrez correctamente, no es necesario asociar a la percepción de cada movimiento del juego una nueva representación mental, de la que el movimiento considerado sería el símbolo; basta asegurarse de que las reglas han sido respetadas.

Transponiendo lo dicho a las matemáticas tendremos la concepción de Hilbert; las matemáticas se convierten en un juego, cuyas piezas son los signos gráficos, que se distinguen entre sí por su forma; con estos signos se constituyen ensamblajes que, según su forma, serán llamados relaciones o proposiciones; en virtud de ciertas reglas, algunas proposiciones son calificadas *a priori* como verdaderas, mientras que otras reglas permiten fabricar nuevas proposiciones verdaderas, bien sea a partir de relaciones cualesquiera, bien sea a partir de otras proposiciones verdaderas; y el punto esencial consiste en que estas reglas permiten verificar su observancia sin más que examinar el ensamblaje.

Conviene subrayar que las palabra *verdadero*, *relación* y *proposición* no tienen en esta concepción más que un significado puramente convencional; se pueden comparar estos términos con los del ajedrez, donde *jaque mate* y *enroque* son empleados para caracterizar, de manera abreviada, ciertas situaciones o ciertos movimientos del juego que las reglas describen con mayor longitud; de forma semejante, los términos matemáticos de los que acabamos de hablar son abreviaturas cuya constitución está precisada por las reglas. En todo caso, no se puede hablar de verdad absoluta de las proposiciones, ni de las reglas que permiten pasar de una proposición 'verdadera' a otra; se puede afirmar que las matemáticas, así concebidas, no recurren a más nociones ni hipótesis metafísicas que el juego del ajedrez, por insistir en el ejemplo. De igual forma que todos los jugadores admiten disponer de un método objetivo para reconocer si un movimiento es correcto en una partida de ajedrez, se dispondrá de un método para reconocer si un texto matemático es correcto o no.

Así se encontrará completamente resuelto el problema de los fundamentos de las matemáticas. (...)»

Este plan de fundamentación axiomática de todas las matemáticas, comenzando por la teoría de conjuntos, fue llevado a la práctica con relativo éxito por el propio Hilbert y por sus discípulos Zermelo y Fraenkel (teoría formulada entre 1908 y 1930), así como por Von Neumann, Bernays y Gödel (1925-1940), entre otros. Gödel puso en evidencia las limitaciones de cualquier teoría axiomática formal, demostrando, con sus teoremas de imposibilidad (1931), que el objetivo planteado por Hilbert no es alcanzable. Un inconveniente de todos los **sistemas axiomáticos formales** es su considerable dificultad técnica, de manera que resulta muy laborioso trasladar al marco formal argumentos intuitivamente válidos. De ahí que la gran mayoría de los matemáticos prefiere trabajar en el marco «ingenuo» de la teoría intuitiva de conjuntos, en la confianza de que sus eventuales descubrimientos podrían

ser «traducidos» al riguroso, sí, pero también tedioso, marco de una teoría axiomática formal. El famoso algebrista G. Birkhoff ha narrado con sorna su experiencia personal, según relata E. L. Lawler («Old stories», en *History of Mathematical Programming*, Lenstra *et al.* (eds.), North-Holland, 1989):

«Hace mucho tiempo, allá por los años 30, pensé que me interesaban los fundamentos de las matemáticas. Incluso escribí un par de trabajos en ese área. Teníamos en el claustro de profesores (de la Universidad de Harvard) un brillante lógico que estaba labrándose una gran reputación. El azar quiso que durante cierto semestre mis clases siguieran a las suyas, por lo que, antes de borrar la pizarra cada día, echaba un vistazo a lo que acababa de explicar. En septiembre empezó con el Teorema 1. Poco antes de Navidad llegó al Teorema 747. Y, ¿sabes lo que decía?: <Si $x \leq y$ e $y \leq z$, entonces $x \leq z$! Algo se quebró de repente en mí. Hay algunas cosas en matemáticas que debe uno admitir, me dije. Y, a partir de ese momento, nunca más he vuelto a preocuparme por los fundamentos de las matemáticas.»

Nos valdremos de un par de ejemplos de **sistemas axiomáticos materiales**, que son los más utilizados en matemáticas desde los tiempos de Euclides, para ilustrar la diferencia con los sistemas axiomáticos formales.

Alrededor del año 300 a.C., Euclides escribió sus célebres *Elementos*, el libro de texto matemático más famoso de la historia, que está compuesto por 13 grandes capítulos. Aunque los *Elementos* organizaron todo el saber geométrico y aritmético acumulado por los griegos, los babilonios y los egipcios, su mayor logro consistió en mostrar cómo un resultado puede ser deducido a partir de otras proposiciones mediante una sucesión de razonamientos lógicos. La geometría desarrollada por Euclides es la primera teoría axiomática de tipo material que se conoce.

En la axiómatica de la geometría euclídea se consideran tres clases de objetos no definidos: puntos, rectas y planos. A estos términos no definidos sólo se les pueden atribuir las propiedades derivadas de los axiomas o postulados (cuya aceptación es un acuerdo entre Euclides y sus lectores). Los 15 axiomas se distribuyen en 5 grupos:

a) Postulados de incidencia:

1. Por dos puntos pasa una recta única.
2. Toda recta contiene, por lo menos, dos puntos.
3. Existen, por lo menos, tres puntos no alineados.

b) Postulados de orden.
c) Postulados de congruencia.
d) Postulado de completitud.
e) Postulado de las paralelas:

15. Por un punto exterior a una recta (es decir, no perteneciente a la misma) se puede trazar una sola recta paralela.

El axioma de las paralelas fue, durante mucho tiempo, el más controvertido. Muchos geómetras pensaban que este postulado era consecuencia lógica

de los anteriores y que, por tanto, se podía eliminar. Sin embargo, fueron vanos los esfuerzos por demostrarlo. Ya en el siglo XIX se demostró su independencia al encontrar modelos geométricos que cumplían todos los postulados menos el de las paralelas.

De hecho, si consideramos sólo los postulados de incidencia y el de las paralelas, y definimos como rectas paralelas aquellas que no se cortan, podemos encontrar un modelo muy simple de geometría que cumple los cuatro axiomas y otro modelo que sólo cumple los tres primeros.

Ejemplo 2.8. Consideremos la geometría cuyos elementos no definidos son los puntos P_i, $i = 1, \ldots, 4$ y las rectas r_j, $j = 1, \ldots, 6$ de la Figura 2.15. Se comprueba que dicha geometría verifica todos los postulados de incidencia y también el de las paralelas.

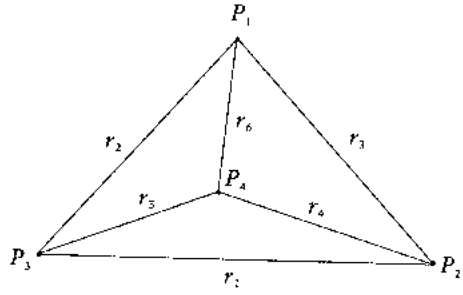

Figura 2.15. *Modelo de geometría que satisface el postulado de las paralelas.*

En efecto, si tomamos, por ejemplo, la recta r_1 y un punto exterior a ella, P_1, existe una única recta, r_6, que pasa por P_1 y es paralela a r_1. Y lo mismo ocurre en los restantes casos.

Ejemplo 2.9. Consideremos ahora la geometría cuyos elementos no definidos son los puntos P_1, P_2, P_3 y las rectas r_1, r_2, r_3 de la Figura 2.16. Dicha geometría verifica los postulados de incidencia pero no el de las paralelas. En efecto, si tomamos la recta r_1 y el único punto exterior a ella, P_1, no existe ninguna recta que pase por P_1 y sea paralela a r_1.

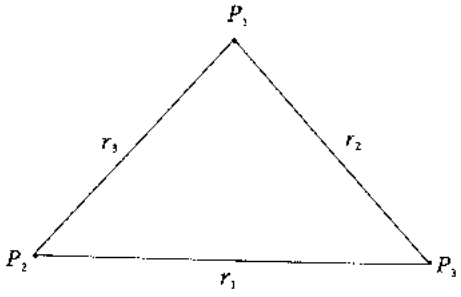

Figura 2.16. *Modelo de geometría donde falla el postulado de las paralelas.*

2.8. Problemas

Problema 2.1. Demuestre las siguientes fórmulas:

a) $1^3 + 2^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$.

b) $1 \cdot 1! + \cdots + n \cdot n! = (n+1)! - 1$.

c) $(1 \cdot 2)^{-1} + (2 \cdot 3)^{-1} + \cdots + [n(n+1)]^{-1} = \dfrac{n}{n+1}$.

d) $n < 2^n$.

e) $a + a^2 + \ldots + a^n = \dfrac{a - a^{n+1}}{1-a}$, siendo $a \neq 1$.

f) $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$.

g) $\dfrac{a^n - b^n}{a-b} = \displaystyle\sum_{i=1}^{n} a^{n-i} \cdot b^{i-1}$, siendo $a \neq b, a, b \in \mathbb{Z}$. (Sugerencia: Demuestre la igualdad $a^n - b^n = (a-b) \displaystyle\sum_{i=1}^{n} a^{n-i} \cdot b^{i-1}$ para todo $n \in \mathbb{N}$).

Problema 2.2. ¿Para qué números naturales se cumplen las siguientes desigualdades?:

a) $2n + 1 < 2^n$.
b) $n^2 < 2^n$.
c) $2^n < n!$.

Problema 2.3. Demuestre que $n \neq n + p$ para todo $n, p \in \mathbb{N}$. (Sugerencia: Aplique inducción sobre n.)

Problema 2.4. Demuestre que no existe ningún número natural m tal que

$$n < m < n + 1,$$

para todo $n \in \mathbb{N}$. (Sugerencia: suponga lo contrario y aplique la Proposición 2.6.)

Problema 2.5. Pruebe que $\operatorname{card}(\{p \in \mathbb{N} \mid p \leq n\}) = n$. (Sugerencia: por inducción y aplique el Problema 2.4.)

Problema 2.6. El **segundo principio de inducción** o *principio de inducción completa* establece que, dada una forma proposicional $p(n)$, $n \in \mathbb{N}$, tal que

(i) $p(1)$ es verdadera, y
(ii) para cualquier natural n, es verdadera la proposición

$$(p(k) \text{ para todo natural } k \leq n) \Rightarrow p(n+1),$$

entonces $p(n)$ es verdadera para todo $n \in \mathbb{N}$.

Demuestre este principio a partir del principio de inducción. (Sugerencia: considere la forma proposicional $q(n) \equiv (p(k)$ para todo natural $k \leq n)$.)

Problema 2.7. Explique cuál es el error, si lo hubiera, en las siguientes «demostraciones» por inducción:

a) $2^1 > 1$. Si $2^n > n$ entonces $2^{n+1} = 2^n \times 2 > n \times 2 = n + n \geq n + 1$. Luego, por inducción, $2^n > n$ para todo $n \in \mathbb{N}$. Por lo tanto, se concluye que $2^{\aleph_0} > \aleph_0$.

b) $(a+b)^1 = a + b$. Supongamos que $(a+b)^k = a + b$ para todo $k \leq n$, $k \in \mathbb{N}$ y consideremos

$$(a+b)^{n+1} = (a+b)^n (a+b) = (a+b)(a+b) = (a+b)^2 = a + b.$$

Por inducción completa se concluye que $(a+b)^n = a + b$, para todo $n \in \mathbb{N}$.

Problema 2.8. ¿Es cierto que para todo $n \in \mathbb{N}$ el número $n^2 + n + 41$ es primo? (Sugerencia: Compruébelo para algunos números naturales menores que 40 elegidos al azar y también para $n = 40$.)

Problema 2.9. Demuestre que, para $n \geq 2$, se verifica la siguiente propiedad:

$$A \cup (B_1 \cap \ldots \cap B_n) = (A \cup B_1) \cap \ldots \cap (A \cup B_n).$$

Problema 2.10. Demuestre, por inducción, que los ángulos interiores de un polígono convexo con n vértices suman $(n-2)\pi$. (Sugerencia: Partiendo del polígono de $n+1$ vértices, construya, como en la Figura 2.17, otro polígono de n vértices.)

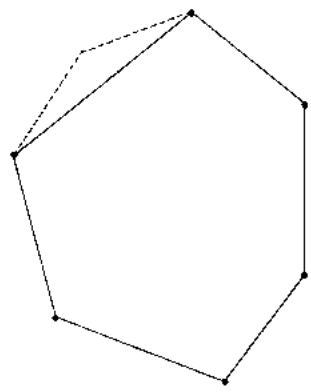

Figura 2.17. *Descomposición de un polígono de $n+1$ vértices en un polígono de n vértices y un triángulo.*

Problema 2.11. Un tablero de ajedrez está formado por 64 casillas cuadradas, de igual tamaño, blancas y negras, de modo que cualquier par de casillas contiguas son de diferente color. Se suprimen las casillas extremas de una de

las diagonales del tablero. ¿Pueden cubrirse las 62 casillas restantes mediante piezas de dominó formadas por dos cuadrados del mismo tamaño que las casillas? ¿Y si el tablero consta de n^2 casillas cuadradas, con $n \in \mathbb{N}$?

Problema 2.12. Considere la familia

$$\mathcal{C} = \{A_n \mid n \in \mathbb{N}\}$$

definida recursivamente por $A_1 = \mathbb{N} - \{1\}$, $A_{n+1} = A_n - \{n+1\}$ para todo $n \in \mathbb{N}$. Pruebe que no hay elemento minimal en el conjunto ordenado $(\mathcal{C}, \subset)$.

Problema 2.13. Demuestre que si tiramos dos dados doce veces, al menos en dos de esas tiradas obtendremos la misma suma de puntuaciones.

Problema 2.14. Pruebe la siguiente versión infinita del principio del palomar: Si se distribuyen los elementos de un conjunto infinito en un número finito de cajas, entonces hay una que contiene una cantidad infinita de elementos.

Problema 2.15.* Demuestre que la aplicación $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ definida como

$$f(m,n) = \frac{1}{2}(m+n-1)(m+n-2) + m$$

proporciona una enumeración de $\mathbb{N}^2$. (Sugerencia: Demuestre que f es suprayectiva considerando la forma proposicional

$$p(N) \equiv (\text{existe } (m,n) \in \mathbb{N}^2 \text{ tal que } f(m,n) = N)$$

y aplicando el principio de inducción sobre N. Para demostrar la inyectividad de f, considérese $f(m,n) = f(p,q)$ y distínganse los casos $m+n = p+q$ y $m+n \neq p+q$.)

Problema 2.16.* Halle el cardinal del conjunto de los naturales primos. (Sugerencia: si dicho conjunto fuese finito, se podrían multiplicar sus elementos y sumarle la unidad a dicho producto.)

Problema 2.17. Demuestre que una buena ordenación no es una enumeración. (Sugerencia: Véase el Problema 1.25.)

Problema 2.18.* Se dice que un conjunto A es *finito según Tarski* si cada familia no vacía $\mathcal{C} \subset \mathcal{P}(A)$, ordenada por la inclusión de conjuntos, tiene elemento minimal en $\mathcal{C}$.

Demuestre que A es finito si, y sólo si, A es finito según Tarski.

Ayuda: use que si A es finito, entonces $\mathcal{P}(A)$ también lo es; si A es infinito, considere un subconjunto numerable $A' \subset A$ con una enumeración $A' = \{a_n \mid n \in \mathbb{N}\}$ y véase el Problema 2.12.

Problema 2.19. Halle el cardinal de $\mathbb{R}^3$, $\mathbb{R}^4$ y, en general, de $\mathbb{R}^n$, con $n \in \mathbb{N}$.

Problema 2.20. Halle el cardinal de las siguientes familias de conjuntos en el plano:

a) Todos los segmentos cerrados por los extremos;
b) los triángulos cuyos vértices tienen coordenadas racionales;
c) los cuadriláteros;
d) las circunferencias.

Problema 2.21. Halle el cardinal de las siguientes familias de subconjuntos del espacio tridimensional:

a) Todos los segmentos abiertos por los extremos;
b) los triángulos;
c) las esferas;
d) las pirámides de base cuadrangular.

Problema 2.22. Halle el cardinal del conjunto de los números reales que son irracionales recurriendo a la hipótesis del continuo.

Problema 2.23.* Un número real se dice que es **algebraico** sobre $\mathbb{Q}$ si es raíz de un polinomio $p(x)$ con coeficientes en $\mathbb{Q}$. Los números algebraicos se utilizan cada vez más en ciencias de la computación al permitir cálculos exactos (métodos numéricos robustos). Así, por ejemplo, $1/2$ y $\sqrt{2}$ son algebraicos porque son raíces de las ecuaciones $2x - 1 = 0$ y $x^2 - 2 = 0$, respectivamente. Los números reales que no son algebraicos se dice que son **trascendentes**. Se pide:

a) Pruebe que todo número racional es algebraico, así como las raíces de índice arbitrario de los números naturales.
b) Pruebe que el conjunto de los polinomios en $\mathbb{Q}[x]$ de grado fijo $n \in \mathbb{N}$ es numerable.
c) Pruebe que $\mathbb{Q}[x]$ es numerable. (Asúmase el axioma de elección).
d) Pruebe que el conjunto de los números algebraicos es numerable.
e) Pruebe que el conjunto de los números trascendentes es infinito no numerable. ¿Puede afirmarse que su cardinal es c?

Problema 2.24.* Demuestre que cada una de las proposiciones siguientes es equivalente al axioma de elección.

a) Si $\mathcal{C} = \{A_i \mid i \in I\}$ es una familia no vacía de conjuntos no vacíos disjuntos dos a dos, entonces existe un subconjunto $B \subset \bigcup_{i \in I} A_i$ tal que $B \cap A_i$ es singular, para cada $i \in I$.

Ayuda para el recíproco: cualquier familia $\mathcal{C} = \{A_i \mid i \in I\}$ se puede reemplazar por otra familia disjunta $\mathcal{C}' = \{A_i \times \{i\} \mid i \in I\}$.

b) Si A es un conjunto no vacío, entonces existe una aplicación

$$f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$$

tal que $f(X) \in X$ para todo $X \in \mathcal{P}(A) \setminus \{\emptyset\}$.

Ayuda para el recíproco: si $\mathcal{C} = \{A_i \mid i \in I\}$ es una familia no vacía de conjuntos no vacíos a partir de $f : \mathcal{P}\left(\bigcup_{i\in I} A_i\right) \setminus \{\emptyset\} \longrightarrow A$ defina $g : I \longrightarrow \bigcup_{i\in I} A_i$.

Problema 2.25.* Demuestre las siguientes proposiciones:

a) Una aplicación $f : A \longrightarrow B$ es suprayectiva si, y sólo si, tiene (al menos) una aplicación inversa a la derecha ($g : B \longrightarrow A$ tal que $f \circ g = I_B$).

Sugerencia: para la existencia de g use la versión del axioma de elección del Problema 2.24*b*) (véase también la demostración del Teorema 2.8).

b) $0 < \operatorname{card}(B) \leq \operatorname{card}(A)$ si, y sólo si, existe una aplicación suprayectiva $f : A \longrightarrow B$. (Ayuda: Utilice el apartado anterior.)

Problema 2.26. Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow X$ aplicaciones inyectivas.

a) ¿Qué puede decirse acerca de la inyectividad de $g \circ f$?
b) ¿Es $g \circ f$ necesariamente suprayectiva?
c) Si X es finito, ¿qué puede decirse sobre la suprayectividad de $g \circ f$?

Problema 2.27. Sea X un conjunto cualquiera y sea 2^X el conjunto de todas las aplicaciones definidas en X con valores en $\{0, 1\}$, es decir,

$$2^X = \{f : X \to \{0, 1\} \mid f \text{ es aplicación}\}.$$

Calcule el cardinal de 2^X. (Ayuda: Demuestre que 2^X es equipotente a $\mathcal{P}(X)$; véase también la demostración de la Proposición 2.11.)

Problema 2.28. Dados dos conjuntos no vacíos A y B, denotaremos por B^A el conjunto de todas las aplicaciones de A en B. Sean A, A', B y B' conjuntos no vacíos tales que A y B son equipotentes a A' y B', respectivamente. Demuestre que B^A y $B'^{A'}$ son equipotentes.

Problema 2.29. Sobre el conjunto, Ω, formado por todos los conjuntos que se puedan concebir, consideramos la forma proposicional $X \notin X$. Considérese también el conjunto $A = \{X \in \Omega \mid X \notin X\}$. Obtenga una contradicción al discutir la pertenencia, o no, de A a sí mismo (Paradoja de Russell).

Problema 2.30.* Encuentre el error en la siguiente demostración que utiliza el Lema de Zorn.

Afirmación: existe un subconjunto finito de $\mathbb{N}$ que no es subconjunto propio de ningún conjunto finito de $\mathbb{N}$.

Demostración: considere la familia $\mathcal{C}$ de todos los subconjuntos finitos de $\mathbb{N}$ ordenada por la inclusión. Para cada subfamilia totalmente ordenada $\mathcal{C}' \subset \mathcal{C}$ el conjunto $\bigcup \mathcal{C}'$ es una cota superior de $\mathcal{C}'$. Por el Lema de Zorn, existe elemento maximal en $\mathcal{C}$, es decir, existe un conjunto finito que no es subconjunto propio de ningún otro conjunto finito.

Problema 2.31.* Demuestre el Teorema de recursión (Dedekind, 1888) siguiendo el esquema de prueba que sigue.

Afirmación: Dados $a \in A$ y una aplicación $f : A \longrightarrow A$, existe una única sucesión $\{a_n\}$ determinada por $a_1 = a$ y $a_{n+1} = f(a_n)$ para todo $n \in \mathbb{N}$.

Demostración: *a*) Pruebe por inducción que para cada $n \in \mathbb{N}$ existe una única aplicación $\varphi_n : \{1, 2, \ldots, n\} \longrightarrow A$ tal que $\varphi_n(1) = a$ y $\varphi_n(k+1) = f(\varphi_n(k))$ para $k = 1, 2, \ldots, n-1$.

b) Verifique que la aplicación $\varphi : \mathbb{N} \longrightarrow A$ definida por $\varphi(n) = \varphi_n(n)$ es una sucesión que cumple $\varphi(1) = a$ y $\varphi(n+1) = f(\varphi(n))$ para todo $n \in \mathbb{N}$.

c) Si una aplicación cualquiera $\psi : \mathbb{N} \longrightarrow A$ cumple $\psi(1) = a$ y $\psi(n+1) = f(\psi(n))$ para todo $n \in \mathbb{N}$, entonces $\psi = \varphi$ (pruebe por inducción sobre n que $\psi(n) = \varphi(n)$).

Problema 2.32.* Este largo ejercicio, que puede considerarse un pequeño proyecto de investigación, tiene por objeto desarrollar una teoría axiomática, de tipo material, para los números naturales (propuesta por Peano en 1899).

Supondremos que existe un conjunto $\mathbb{N} \neq \emptyset$ que satisface los siguientes axiomas:

(*i*) $1 \in \mathbb{N}$ (se le llama elemento unidad).

(*ii*) Para cada $n \in \mathbb{N}$ existe un elemento único $n^* \in \mathbb{N}$ (llamado sucesor de n).

(*iii*) 1 no es sucesor de ningún elemento de $\mathbb{N}$.

(*iv*) $m^* = n^* \Longrightarrow m = n$.

(*v*) Si un subconjunto S de $\mathbb{N}$ satisface $1 \in S$ y, además, $n \in S \Longrightarrow n^* \in S$ cualquiera que sea n, entonces $S = \mathbb{N}$.

Los axiomas (*ii*), (*iii*) y (*iv*) afirman que la aplicación que asocia a cada número natural su sucesor es inyectiva, pero no suprayectiva; (*v*) es el principio de inducción.

Ahora definiremos la suma y el producto en $\mathbb{N}$ por inducción. Dados n (que se toma como fijo) y m (que se considera variable), se definen

(S1) $n + 1 = n^*$.
(S2) $n + m^* = (n + m)^*$.
(P1) $n1 = n$.
(P2) $nm^* = nm + n$.

Se pide demostrar las siguientes proposiciones, en el orden indicado:

a) la suma de dos elementos de $\mathbb{N}$ es un elemento de $\mathbb{N}$;
b) la suma es asociativa;
c) $n + 1 = 1 + n$ para todo $n \in \mathbb{N}$;
d) la suma es conmutativa;
e) el producto de dos elementos de $\mathbb{N}$ es un elemento de $\mathbb{N}$;
f) el producto se distribuye respecto de la suma;
g) el producto es asociativo;
h) el producto es conmutativo y 1 actúa de elemento neutro;

Ayuda:

a) para n fijo, aplicar (*v*) a $S_n = \{m \in \mathbb{N} \mid n + m \in \mathbb{N}\}$;

b) para n, m fijos, ídem con $S_{mn} = \{p \in \mathbb{N} \mid (n+m)+p = n+(m+p)\}$;
c) ídem con $S = \{n \in N \mid n+1 = 1+n\}$;
d) ídem con $S_n = \{m \in N \mid n+m = m+n\}$;
e) ídem con $S_n = \{m \in N \mid nm \in \mathbb{N}\}$;
f) ídem con $S_{np} = \{m \in N \mid (n+p)m = nm+pm\}$;
g) ídem con $S_{mn} = \{p \in N \mid (nm)p = n(mp)\}$; y
h) se empieza con $m = 1$ y se aplica inducción sobre n. A continuación se efectúa la inducción sobre m recurriendo a *f*).

Ahora se define el orden: $m < n$ cuando existe $p \in \mathbb{N}$ tal que $n + p = m$. Naturalmente, $m \leq n$ si $m < n$ o $m = n$.

La prueba de que $(\mathbb{N}, \leq)$ es un buen orden (y, por lo tanto, un orden total) es la misma que la de la Proposición 2.7.

CAPÍTULO 3

GRUPOS

Durante el Renacimiento italiano se introdujo el término «álgebra», de origen árabe, para identificar aquella parte de las matemáticas que se ocupa de las ecuaciones algebraicas, es decir, de la búsqueda de las raíces de los polinomios (inicialmente con coeficientes enteros). Los números racionales permiten resolver las ecuaciones de primer grado, pero las soluciones reales de las ecuaciones de segundo grado son, generalmente, irracionales. Es más, si se desea que toda ecuación algebraica tenga al menos una solución, no queda más remedio que admitir la existencia de un conjunto de números más amplio que el de los reales. Así, de modo natural, el álgebra pasó a ocuparse de los conjuntos de números y de las operaciones sobre los mismos. Extender los conjuntos numéricos tomó su tiempo. Los enteros negativos no fueron admitidos como números por los griegos, pues no servían para contar, ni para medir ni para pesar. Tomaron carta de naturaleza durante el período helenístico (Diofanto), ya bajo el dominio de Roma, y empezaron a ser representados geométricamente, sobre una recta graduada, por iniciativa de Descartes, en el siglo XVII.

Desde hace dos siglos, el álgebra (al principio adjetivada como moderna o abstracta) es la disciplina que se ocupa de las operaciones realizadas con los elementos de uno o de más conjuntos. En efecto, la aparición, en diferentes campos, de estructuras que comparten las mismas propiedades básicas (los axiomas de la estructura) han hecho aconsejable desarrollar una teoría general que permita ahorrar esfuerzos innecesarios, como sería derivar una y otra vez propiedades análogas para cada caso particular. Las estructuras más simples son aquellas en las que existe un solo conjunto dotado de una operación única. Tal es el caso de los grupos.

Los grupos empezaron a surgir en torno a 1800 en tres campos distintos. En primer lugar, en teoría de números, donde Euler introdujo las clases de congruencia en 1761, teoría desarrollada luego en profundidad por Gauss a partir de 1801. Lagrange, por su parte, se ocupó en 1770 de las ecuaciones algebraicas, tratando de entender las razones por las que no se encontraba un método para resolverlas por radicales cuando su grado era superior a 4. Aunque recurrió a la permutación de las raíces de una ecuación, no efectuó operaciones con ellas, algo que es esencial al concepto de grupo y que fue llevado a cabo por Ruffini, quien publicó muchas pruebas fallidas de la im-

posibilidad de resolver las de grado 5. La primera prueba admitida es de Abel (1824), quien se basó en los grupos de permutaciones, siendo Galois quien completó la teoría de ecuaciones en 1831 (aunque su trabajo pasó desapercibido hasta 1846). El tercer campo es la geometría, donde Möbius (1827) y Steiner (1832) empezaron a referirse de forma implícita a los grupos de transformaciones. Los vectores del plano y del espacio, que se venían utilizando en física desde los tiempos de Galileo, y las matrices, utilizadas por los analistas, eran otros ejemplos de grupos que nadie había sido capaz de relacionar con todos los anteriores, hasta que el inglés Cayley dio, en 1854, la definición abstracta. Cayley fue el primero en representar las operaciones binarias sobre conjuntos finitos mediante tablas (a las que, por esa razón, se les da su nombre).

El presente es el primero de cuatro capítulos a lo largo de los cuales se revisarán los conjuntos numéricos (que el lector conoce, intuitivamente, por los cursos de matemática elemental), al tiempo que se van introduciendo estructuras cada vez más complejas. En este capítulo consideraremos los números enteros, introducidos como una extensión de los números naturales, y se analizarán las propiedades algebraicas de la suma y del producto, tomadas inicialmente por separado.

3.1. Operaciones binarias

Definición 3.1. *Una* ***operación binaria*** $*$ *en un conjunto no vacío G es una aplicación de G^2 en G. Se denota mediante el par $(G,*)$.*

El signo $*$ que utilizaremos en esta sección puede representar cualquier tipo de operación binaria, que asigna a cada par ordenado $(a,b) \in G^2$ un elemento $a * b \in G$ mediante alguna propiedad definida en términos de a y b. En secciones posteriores utilizaremos también notación aditiva $(a + b)$ o notación multiplicativa $(a \cdot b$ o bien $ab)$.

Definición 3.2. *Una operación binaria $*$ en G se dice que es* ***asociativa*** *cuando satisface*

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

cualesquiera que sean a, b y c elementos de G. Se dice que $*$ es ***conmutativa*** *cuando*

$$a * b = b * a$$

cualesquiera que sean $a, b \in G$.

Por ejemplo, la unión y la intersección son operaciones binarias sobre el conjunto de las partes de un conjunto A. Además, ambas operaciones son asociativas y conmutativas (véanse en el Ejercicio 1.2 las propiedades 2.4, 2.5, 2.14 y 2.15).

Definición 3.3. *Dada una operación binaria $(G,*)$, se dice que $e \in G$ es* ***elemento neutro*** *para esa operación cuando $e * a = a * e = a$ para todo $a \in G$.*

Cuando la operación es conmutativa resulta redundante la expresión $e*a = a * e = a$; basta con $a * e = a$.

De existir un elemento neutro, tiene que ser único, ya que si e y e' fuesen elementos neutros para $(G,*)$ se tendría $e' = e' * e = e$. Por eso, podemos hablar de «el» elemento neutro y no de «un» elemento neutro.

Por ejemplo, en el conjunto de las partes de un conjunto A, el conjunto $\emptyset$ es el elemento neutro de $(\mathcal{P}(A), \cup)$, mientras que A es el neutro de $(\mathcal{P}(A), \cap)$.

Cuando se usa notación aditiva, el elemento neutro recibe el nombre de **elemento nulo**; en cambio, se denomina **elemento unidad** si la notación empleada es multiplicativa.

Definición 3.4. *Dados $(G,*)$ y $a \in G$ decimos que $a' \in G$ es* ***elemento simétrico*** *de a si satisface $a' * a = a * a' = e$, donde e es el elemento neutro (con lo que estamos suponiendo implícitamente la existencia, y por lo tanto la unicidad, de elemento neutro e).*

Si $(G,*)$ cumple la propiedad asociativa y a' y a'' son simétricos de a entonces se tiene

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

En consecuencia, bajo la hipótesis de asociatividad de la operación binaria, si a tiene simétrico éste es único. Cuando ocurre tal cosa, a es también simétrico de a', por lo que es suficiente decir que a y a' son simétricos (uno respecto del otro). Cuando se utiliza notación aditiva el elemento simétrico se denomina **opuesto** $(-a)$; y si se emplea notación multiplicativa se denomina **inverso** (a^{-1}).

Si $A \neq \emptyset$, entonces los únicos elementos de $(\mathcal{P}(A), \cup)$ y $(\mathcal{P}(A), \cap)$ que poseen simétrico son los respectivos neutros.

Hay tres formas usuales de definir una nueva operación binaria a partir de una dada $(G,*)$: inducir una operación en un subconjunto de G, proyectar una operación sobre un cociente $G/\sim$ (para cierta RBE sobre G) y, por último, definir una operación en el producto cartesiano $G \times H$, cuando se dispone de un segundo par $(H, \triangle)$.

Definición 3.5. *Dado un par $(G,*)$ y un conjunto no vacío $H \subset G$, la operación binaria es* ***cerrada*** *en H si $x * y \in H$ cualesquiera que sean los elementos $x, y \in H$. En ese caso, la restricción de $*$ al subconjunto H se denomina* ***operación binaria inducida*** *y se denota con el mismo símbolo.*

EJERCICIO 3.1. Sea $(G,*)$ una operación binaria cerrada en $H \subset G$. Pruebe que si $(G,*)$ es asociativa (conmutativa), entonces la operación inducida $(H,*)$ es también asociativa (conmutativa).

Definición 3.6. *Dado un conjunto G dotado de una operación $*$ y de una RBE $\sim$, se dice que $*$ y $\sim$ son* ***compatibles*** *cuando, cualesquiera que sean a_1, a_2, b_1 y b_2 en G, se cumple*

$$((a_1 \sim a_2) \wedge (b_1 \sim b_2)) \Longrightarrow ((a_1 * b_1) \sim (a_2 * b_2)) .$$

La compatibilidad garantiza que la operación $*$ puede ***proyectarse****, de manera natural y sin ambigüedad, a una operación entre clases, operando por medio de sus representantes. Es decir, si $\sim$ es compatible con $*$ puede definirse, sobre el conjunto cociente $G/\sim$, la operación binaria*

$$[a] * [b] = [a * b]$$

(podemos usar la misma notación $*$ para la operación entre clases, debido a la compatibilidad).

EJERCICIO 3.2. Pruebe que si una operación binaria en G es asociativa (conmutativa), la operación binaria proyectada sobre el cociente $G/\sim$ por una RBE compatible es también asociativa (conmutativa). Además, si e es el elemento neutro, entonces $[e]$ es el neutro del cociente y, análogamente, si a' es simétrico de a, entonces $[a']$ es el simétrico de $[a]$.

Definición 3.7. *Dados $(A, *)$ y $(B, \odot)$, se define en $A \times B$ la* ***operación binaria producto*** *$\diamond$ así:*

$$(a_1, b_1) \diamond (a_2, b_2) = (a_1 * a_2, b_1 \odot b_2) .$$

EJERCICIO 3.3. Pruebe que el producto de dos operaciones asociativas (conmutativas) es asimismo asociativa (conmutativa). Además, si cada operación tiene elemento neutro (o si todo elemento tiene simétrico para cada operación), el producto también.

3.2. Semigrupos, monoides y grupos

A lo largo de esta sección se supondrá dada una operación binaria $(G, .)$ con notación multiplicativa. Introduciremos las estructuras algebraicas más simples, que involucran a un solo conjunto dotado de una operación.

Definición 3.8. *$(G, .)$ es* ***semigrupo*** *cuando la operación es asociativa.*
Si existe, además, elemento neutro, entonces se dice que $(G, .)$ es un ***monoide****.*
Un monoide en el cual todo elemento tiene simétrico se denomina ***grupo****.*
Un semigrupo (monoide, grupo) cuya operación es conmutativa se dice que es ***abeliano*** *(o conmutativo).*

Si $(G, .)$ es un monoide, denotaremos por e al elemento neutro, aunque también sería coherente con la notación multiplicativa representarlo por 1. El simétrico de a, si existe, se representará por a^{-1}.

La denominación de monoide para esta sencilla estructura algebraica proviene de esta propiedad de unicidad del elemento simétrico («mono» es una partícula de origen griego que significa «uno»), mientras que el término «abeliano» se emplea en honor del matemático Abel.

Ejemplo 3.1. $(\mathbb{N}, +)$ es solamente semigrupo, mientras que $(\mathbb{N}, \times)$, $(\{\aleph_0\}, \times)$,

$(\{\aleph_0, c\}, \times)$, $(\{\aleph_0\}, +)$, $(\{\aleph_0, c\}, +)$, $(\{0, \aleph_0, c\}, +)$ y $(\{1, \aleph_0, c\}, \times)$ son monoides. También son monoides abelianos $(\mathbb{N} \cup \{0\}, +)$ y $(\mathbb{N} \cup \{0\}, \times)$, puesto que ambas operaciones son cerradas (lo que se probó para $\mathbb{N}$), asociativas y conmutativas (para cualquier conjunto de cardinales). De todos los ejemplos anteriores, los únicos grupos corresponden a los conjuntos singulares $(\{\aleph_0\}, \times)$ y $(\{\aleph_0\}, +)$. Un grupo $(G, .)$ cuyo conjunto G es singular se denomina **grupo trivial**.

Podría pensarse que la estructura de semigrupo es demasiado pobre en propiedades para resultar útil, pero no es así. En los últimos tiempos se habla mucho de los *sistemas dinámicos*, estructuras complejas que permiten modelar sistemas físicos inestables o caóticos (para los cuales el etólogo Lorenz acuñó la metáfora del *efecto mariposa*: «el aleteo de una mariposa en Brasil puede provocar un tornado en Texas»). Un sistema dinámico es una terna (X, G, φ), donde X es un conjunto llamado *espacio de estados*, G es un semigrupo $((\mathbb{N} \cup \{0\}, +)$ o $(\mathbb{Z}, +)$ para los sistemas discretos; $(\mathbb{R}_+, +)$ o $(\mathbb{R}, +)$ para los continuos) y

$$\varphi : G \times X \longrightarrow X$$

es una aplicación que satisface ciertas condiciones.

Ejemplo 3.2. El giro del plano en torno a un punto O (que tomaremos como origen de coordenadas) y de ángulo α es una aplicación del plano en sí mismo que asocia a cada punto P otro punto P' tal que las distancias a O desde P y desde P' son las mismas y, además, el ángulo que forman las semirrectas OP y OP' mide α. Denotemos por g_α dicha transformación biyectiva del plano en sí mismo (véase Figura 3.1).

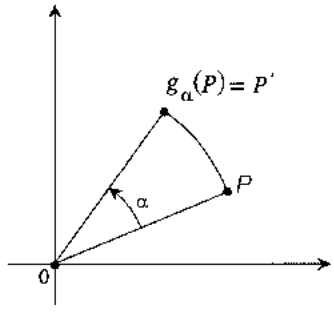

Figura 3.1. *Representación geométrica del giro de ángulo α.*

Es facil ver que $g_\beta \circ g_\alpha = g_{\alpha+\beta}$ (véase Figura 3.2).

Si G denota los giros en el plano, $(G, \circ)$ es un grupo abeliano, siendo g_0 el elemento neutro. La argumentación geométrica se puede sustituir por la meramente algebraica, sin más que definir g_α mediante la fórmula

$$g_\alpha(x, y) = (x \cos\alpha - y \operatorname{sen}\alpha\,,\, x \operatorname{sen}\alpha + y \cos\alpha)\ .$$

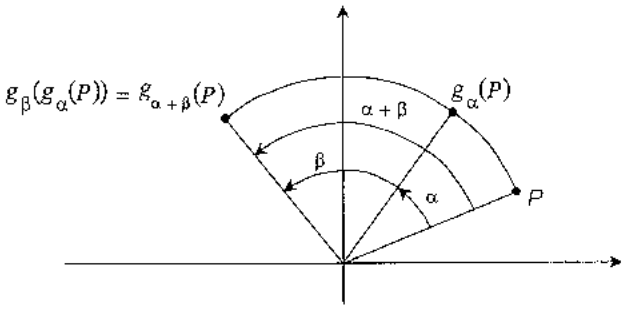

Figura 3.2. *Composición de los giros de ángulos α y β.*

Ejercicio 3.4. Demuestre que el producto cartesiano de semigrupos (monoides, grupos) también lo es con la operación binaria producto. Análogamente, el cociente de un semigrupo (monoide, grupo) por una RBE compatible es asimismo semigrupo (monoide, grupo) con la operación proyectada. Por último, pruebe que en un semigrupo la operación inducida en un subconjunto no vacío, y cerrado para la operación binaria, es también semigrupo (pero no necesariamente será monoide ni grupo, aunque lo sea el semigrupo).

Ejercicio 3.5. En el monoide abeliano $(\{0, \aleph_0, c\}, +)$ se considera la RBE correspondiente a la partición del conjunto en los cardinales finitos e infinitos (las clases de equivalencia son, pues, $\{0\}$ y $\{\aleph_0, c\}$). Compruebe que dicha RBE es compatible con la suma y muestre que el cociente es monoide abeliano, pero no un grupo.

Proposición 3.1. *Si $(G, .)$ es un grupo se cumple, cualesquiera que sean a, b y c en G:*

(*i*) $(a^{-1})^{-1} = a$;
(*ii*) $(ab)^{-1} = b^{-1}a^{-1}$;
(*iii*) si $aa = a$, entonces $a = e$;
(*iv*) si $ab = ac$, entonces $b = c$ (cancelación a la izquierda); y
(*v*) si $ba = ca$, entonces $b = c$ (cancelación a la derecha).

Demostración. Las cinco proposiciones se prueban recurriendo a las definiciones. Por ejemplo, por ser a^{-1} simétrico de a se cumple $a^{-1}a = e = aa^{-1}$. Pero estas igualdades también nos dicen que a es simétrico de a^{-1}, que es lo que afirma (*i*). Las restantes proposiciones se dejan como ejercicio para el lector. □

Teorema 3.1 ***(de caracterización de grupos).*** *Dado un semigrupo $(G, .)$, las siguientes proposiciones son equivalentes:*

(*i*) $(G, .)$ es grupo;
(*ii*) cualesquiera que sean $a, b \in G$, las ecuaciones $ax = b$ y $xa = b$ tienen solución en G.

Demostración. $(i)\Rightarrow(ii)$ Considérese la ecuación

$$b = ax. \tag{3.1}$$

Si existiese un $x \in G$ satisfaciendo la ecuación (3.1), multiplicando ambos miembros por a^{-1} y aplicando propiedades de grupo se tendría

$$a^{-1}b = a^{-1}(ax) = \left(a^{-1}a\right)x = ex = x.$$

Así pues, la única posible solución de (3.1) es $a^{-1}b$. Reemplazando x por $a^{-1}b$ en la ecuación (3.1) y usando la ley asociativa se comprueba que es la solución buscada. El lector probará de igual forma que ba^{-1} es solución (única) de $xa = b$.

$(ii)\Rightarrow(i)$ Probaremos primero que existe elemento neutro en G. Sea $a \in G$ arbitrario. Como suponemos que se cumple (ii), podemos tomar una solución $c \in G$ de la ecuación $xa = a$, por lo que se tendrá $ca = a$. Sea ahora b un elemento cualquiera en G y consideremos la ecuación $ax = b$, que tiene una solución $d \in G$; es decir, $ad = b$. Se tiene entonces

$$cb = c(ad) = (ca)d = ad = b.$$

Hemos probado que, para todo $b \in G$,

$$cb = b. \tag{3.2}$$

Por otra parte, la ecuación $ax = a$ tiene solución $c' \in G$, y se demuestra de igual manera que para todo $b \in G$,

$$bc' = b. \tag{3.3}$$

En particular, tomando $b = c$ en (3.3) y $b = c'$ en (3.2) obtenemos que $c = cc' = c'$, por lo que $c = c' = e$ es el elemento neutro.

Para la existencia del simétrico de un elemento arbitrario $a \in G$ consideremos las ecuaciones $ax = e$ y $xa = e$. Sean b y b' las respectivas soluciones. Entonces,

$$b = eb = \left(b'a\right)b = b'(ab) = b'e = b',$$

por lo que $b = b' = a^{-1}$ es el elemento simétrico. □

Toda operación binaria en un conjunto finito G puede representarse con ayuda de una tabla de doble entrada (**tabla de Cayley**), con una fila y una columna para cada elemento de G, ordenados de una misma manera. En dicha tabla se escribe, en la casilla correspondiente a la fila del elemento x y columna del elemento y, el resultado de la operación xy. Para comprobar, con ayuda de la tabla, las propiedades eventuales de la operación binaria puede procederse como sigue:

(a) La asociatividad requiere comparar la igualdad de los dos productos asociados, $x(yz)$ y $(xy)z$, para todas las ternas ordenadas (x, y, z) que pueden

formarse con los elementos de G. Por desgracia, hay que comparar $[\text{card}\,(G)]^3$ posibles ternas, lo que puede resultar muy tedioso.

(b) La conmutatividad se aprecia a simple vista, pues equivale a la simetría de la tabla respecto de la diagonal de los cuadrados x^2 (casillas correspondientes a fila y columna de un mismo elemento de G).

(c) El elemento neutro, si existe, es aquel que corresponde a la fila y columna que reproduce la ordenación elegida para los elementos de G.

(d) El simétrico del elemento que determina una fila (columna) es el que corresponde a la columna (fila) que se cruza con aquélla en el elemento neutro.

(e) Si $(G, .)$ es asociativo, sabemos que es grupo si y sólo si satisface la condición (ii) del Teorema 3.1. Esta condición es también fácil de apreciar sobre la tabla, pues equivale a afirmar que cada fila y cada columna de la misma es una permutación de los elementos de G.

Ejemplo 3.3. En el conjunto $G = \{0, 1\}$ consideramos las operaciones, $+$ y $\times$, como sigue:

(i)

$+$	0	1
0	0	1
1	1	0

Para la asociatividad basta considerar las 8 ternas que se pueden formar y comprobar la igualdad de los correspondientes productos asociados. Como las filas y columnas son permutaciones de G, se cumple la condición (ii) del Teorema 3.1 y $(G, +)$ es un grupo (abeliano por la simetría).

(ii)

$\times$	0	1
0	0	0
1	0	1

Todas las ternas, excepto $(1, 1, 1)$, proporcionan productos que valen 0, mientras que los dos correspondientes a dicha terna son $(1 \times 1) \times 1 = 1 \times (1 \times 1) = 1$. Se trata de un monoide porque hay una fila (columna), la segunda, que reproduce el encabezamiento de la tabla, pero no de un grupo por cuanto la primera fila (columna) tiene elementos de G repetidos.

Acabaremos esta sección de iniciación a las estructuras más simples (semigrupos, monoides y grupos) introduciendo unos pocos conceptos acerca de las aplicaciones de una estructura en otra que preservan las operaciones, de tal manera que el conjunto imagen tiene «una forma» semejante (la misma estructura algebraica) que el conjunto inicial. De ahí el término *homomorfismo* con el que se denominan tales aplicaciones.

Definición 3.9. *Sean $(G, .)$ y $(H, *)$ dos conjuntos equipados con sus respectivas operaciones binarias. Una aplicación*

$$f : G \longrightarrow H$$

es un ***homomorfismo*** *si*

$$f(xy) = f(x) * f(y)$$

cualesquiera que sean $x, y \in G$. Si, además, f es inyectiva (suprayectiva, biyectiva) se dice que f es un ***monomorfismo (epimorfismo, isomorfismo)****. Un homomorfismo de $(G, .)$ en $(G, .)$ es un* ***endomorfismo****. Si f es a la vez endomorfismo e isomorfismo, entonces es un* ***automorfismo****.*

Desde luego, la identidad de $(G, .)$ en sí mismo es un automorfismo. Sin embargo, la identidad puede no ser homomorfismo (si se consideran dos operaciones binarias diferentes en G). Por ejemplo, para $I_G : (G, +) \longrightarrow (G, \times)$, donde $G = \{0, 1\}$ con las operaciones $+$ y $\times$ definidas en el Ejemplo 3.3, se tiene

$$0 = I_G(0) = I_G(1 + 1) \neq I_G(1) \times I_G(1) = 1 \times 1 = 1.$$

Ejemplo 3.4. En los conjuntos $G = \{0, 1, 2, 3\}$ y $H = \{1, i, -1, -i\}$ consideramos las operaciones $+$ y $\times$ definidas así:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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

Asumiendo que ambas operaciones sean asociativas, no es difícil verificar que $(G, +)$ y $(H, \times)$ son grupos abelianos isomorfos.

EJERCICIO 3.6. Demuestre que, si $(G, .)$ es un semigrupo (monoide, grupo) y $\sim$ es compatible con la operación, entonces la proyección de $(G, .)$ sobre el cociente $(G/\sim, .)$, que asocia a cada elemento $a \in G$ su clase de equivalencia $[a]$, es un epimorfismo, pero no es necesariamente un monomorfismo.

Definición 3.10. *Sea $(G, .)$ un grupo y H un subconjunto no vacío para el cual la operación binaria es cerrada. Si con la operación inducida $(H, .)$ es grupo, entonces se dice que H es un* ***subgrupo*** *de G.*

Desde luego, G y $\{e\}$ son subgrupos de G. En el Ejemplo 3.4, $\{0, 2\}$ es un subgrupo de $(G, +)$. En el Ejemplo 3.2, los giros de centro O y ángulo múltiplo entero de π,

$$\{g_{z\pi}, z \in \mathbb{Z}\},$$

forman un subgrupo de $(G, \circ)$; desde el punto de vista geométrico, dicho subgrupo sólo contiene dos transformaciones: la identidad (z par) y la simetría respecto de O (z impar).

Teorema 3.2. *(de caracterización de subgrupos) Sea $(G,.)$ un grupo y $\emptyset \neq H \subset G$. Entonces H es subgrupo de G si, y sólo si, $ab^{-1} \in H$ cualesquiera que sean $a, b \in H$.*

Demostración. Si $(H,.)$ es grupo, para cualesquiera $a, b \in H$, se tiene que $b^{-1} \in H$, de modo que

$$ab^{-1} \in H. \tag{3.4}$$

Para el recíproco debemos probar que H tiene un elemento neutro, que todo elemento de H tiene simétrico y que la operación es cerrada en H.

Tomando $a = b \in H$ y aplicando (3.4), $aa^{-1} \in H$. Pero $aa^{-1} = e$ en G, por lo que concluimos que existe neutro en H y es el neutro de G.

Aplicaremos ahora (3.4) a los elementos e y a (arbitrario) de H, en ese orden. Se tendrá $a^{-1} = ea^{-1} \in H$, de tal manera que H contiene al simétrico de cada uno de sus elementos.

Por último, para $a, b \in H$, aplicamos (3.4) a los elementos a y b^{-1} en ese orden ($b^{-1} \in H$ por lo anterior), con lo que $ab = a\left(b^{-1}\right)^{-1} \in H$ y con ello hemos completado la prueba. □

Si f es un homomorfismo entre grupos, la imagen inversa del elemento neutro es un subgrupo llamado **núcleo** (en inglés *kernel*) de f, que se denota $\ker f$.

Veremos a continuación que en un grupo abeliano podemos asociar con cada subgrupo una RBE compatible con la operación, lo que permite construir fácilmente grupos cociente.

Proposición 3.2. *Si $(G,.)$ es un grupo abeliano y H es un subgrupo, la siguiente relación binaria sobre G es de equivalencia y compatible con la operación*

$$x \sim y \Longleftrightarrow xy^{-1} \in H. \tag{3.5}$$

Demostración. Veamos qué es una RBE. En efecto, la reflexividad es consecuencia de $e \in H$, la simetría se sigue de la Proposición 3.1 y la transitividad, de la propiedad asociativa de la operación. Obsérvese que en esta parte de la prueba no interviene la conmutatividad. No ocurre lo mismo con la segunda parte.

Terminaremos probando que $\sim$ es compatible con la operación. Tomaremos, con tal fin, cuatro elementos de G (quizás repetidos) tales que $a_1 \sim a_2$ y $b_1 \sim b_2$. De acuerdo con (3.5), $a_1a_2^{-1} \in H$ y $b_1b_2^{-1} \in H$, y, usando la conmutatividad de la operación,

$$(a_1b_1)(a_2b_2)^{-1} = \left(a_1a_2^{-1}\right)\left(b_1b_2^{-1}\right) \in H.$$

Se concluye que $a_1b_1 \sim a_2b_2$. □

El **grupo cociente** $G/\sim$ producido con la RBE asociada a un subgrupo H (recuérdese el Ejercicio 3.2) se denota por G/H. Los elementos de G/H son

clases de elementos $x \in G$. Note que $[x] = xH = \{xh \mid h \in H\}$; en particular, $[e] = H$.

EJERCICIO 3.7. En el conjunto de los números reales con la operación usual de suma demuestre que el subconjunto $2\pi\mathbb{Z} = \{2\pi z \in \mathbb{R} \mid z \in \mathbb{Z}\}$ es un subgrupo de $(\mathbb{R}, +)$, por lo que $(\mathbb{R}/2\pi\mathbb{Z}, +)$ es un grupo (véase Ejemplo 1.7).

3.3. Los números enteros

Desde hace siglos se ha venido llevando la contabilidad de las unidades económicas (organismos públicos, empresas y particulares) con ayuda de los enteros no negativos, es decir, del conjunto $\mathbb{N} \cup \{0\}$. En efecto, el estado contable de una unidad económica queda descrito mediante una pareja de números $(a,p) \in (\mathbb{N} \cup \{0\})^2$, donde a representa el volumen de sus activos (valor monetario de todos sus bienes disponibles sumado al saldo acreedor) y p representa el pasivo (deuda contraída por todos los conceptos). Si al cabo de cierto tiempo el estado contable es (a', p') y se verifica que $a + p' = a' + p$, entonces no hubo variación del estado contable, aunque se hayan producido durante ese período ingresos y gastos y se hayan concedido y tomado créditos. Quiere esto decir que puede llevarse la contabilidad con la ayuda de una operación aritmética única: la suma de cardinales finitos. Aquellas civilizaciones que desconocieron los sistemas numéricos de posición (como la egipcia o la romana) tuvieron que recurrir a instrumentos *ad hoc* para sumar números naturales (los ábacos). El sistema de numeración en base 10 apareció en la India en el siglo VI, desempeñando el cero un papel auxiliar (llenar los eventuales huecos: así, 203 significa 2 centenas, 3 unidades y ninguna decena), pero careciendo todavía de interpretación como número independiente. Este sistema de numeración fue introducido por los árabes en Europa durante la Edad Media.

Haremos la construcción de $\mathbb{Z}$ a partir de $\mathbb{N} \cup \{0\}$, considerando pares ordenados de cardinales finitos (en lugar del resultado de sus diferencias) y una relación de equivalencia que ponga en una misma clase a todos los pares ordenados que producen la misma diferencia. Tal RBE es la que surge de la siguiente propiedad de los números enteros, bien conocida de la aritmética elemental (véase Figura 3.3):

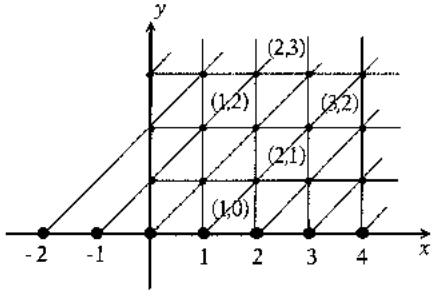

Figura 3.3. *Cada clase de equivalencia está formada por los pares (m,n) pertenecientes a una misma recta oblicua.*

$$m - n = p - q \Longleftrightarrow m + q = n + p.$$

La suma y el producto de pares ordenados están inspirados en las siguientes relaciones, que también deseamos que se cumplan en $\mathbb{Z}$:

$$\begin{aligned}(m-n)+(p-q) &= (m+p)-(n+q)\,,\\ (m-n)(p-q) &= (mp+nq)-(mq+np)\,.\end{aligned}$$

Proposición 3.3. *La relación binaria* $(m,n) \sim (m',n')$ *cuando*

$$m + n' = n + m'$$

es una RBE sobre $(\mathbb{N} \cup \{0\})^2$ *compatible con la suma,*

$$(m,n) + (p,q) = (m+p, n+q)\,,$$

y con el producto,

$$(m,n)(p,q) = (mp+nq, mq+np)\,.$$

Demostración. Es fácil comprobar que $\sim$ satisface las propiedades reflexiva y simétrica, basándose en la conmutatividad de la suma en $\mathbb{N} \cup \{0\}$. Por lo que respecta a la transitividad, suponiendo $(m,n) \sim (m',n')$ y $(m',n') \sim (m'',n'')$, se tiene

$$(m+n') + (m'+n'') = (n+m') + (n'+m'')\,.$$

Aplicando repetidas veces las propiedades asociativa y conmutativa, esta ecuación se puede escribir como

$$(m+n'') + (m'+n') = (n+m'') + (m'+n')\,. \tag{3.6}$$

Cancelando el segundo sumando en ambos miembros de (3.6) se concluye que $(m,n) \sim (m'',n'')$.

Probaremos a continuación la compatibilidad de $\sim$ con la suma y el producto de pares ordenados. Supongamos que $(m,n) \sim (m',n')$ y $(p,q) \sim (p',q')$, es decir, se cumplen las relaciones

$$m + n' = n + m' \tag{3.7}$$

y

$$p + q' = q + p'. \tag{3.8}$$

Sumando miembro a miembro las ecuaciones (3.7) y (3.8), luego de asociar y conmutar, tenemos

$$m + p + n' + q' = n + q + m' + p',$$

que equivale a

$$(m+p, n+q) \sim (m'+p', n'+q').$$

Esto prueba la compatibilidad de la RBE con la suma.

Por lo que respecta a la compatibilidad con el producto, es conveniente recurrir a la transitividad de $\sim$, demostrando que

$$(m,n)(p,q) \sim (m',n')(p,q) \sim (m',n')(p',q'). \tag{3.9}$$

Nos limitaremos a demostrar la primera de las relaciones en (3.9) (la otra es semejante). Debemos probar que

$$(mp+nq, mq+np) \sim (m'p+n'q, m'q+n'p),$$

lo que equivale a demostrar que

$$(m+n')p+(n+m')q = (m+n')q+(n+m')p.$$

Pero esta igualdad se cumple como consecuencia de (3.7). $\square$

Definición 3.11. *El conjunto de los* ***números enteros*** *es el conjunto cociente* $\mathbb{Z} = (\mathbb{N} \cup \{0\})^2 / \sim$.

Como consecuencia de la Proposición 3.3, la suma y producto en $(\mathbb{N} \cup \{0\})^2$, proyectadas sobre el conjunto cociente $\mathbb{Z}$, determinan operaciones binarias bien definidas (por medio de representantes), que seguiremos llamando y denotando de la misma manera que en $\mathbb{N}$.

Proposición 3.4. *$(\mathbb{Z},+)$ es un grupo y $(\mathbb{Z},.)$ es un monoide. Además, ambos son conmutativos.*

Demostración. Es fácil comprobar que $\mathbb{N} \cup \{0\}$ es monoide abeliano para la suma (Ejemplo 3.1), y como la propiedad asociativa, conmutativa y elementos neutros se levantan al producto cartesiano $(\mathbb{N} \cup \{0\})^2$ (Ejercicio 3.3) y se proyectan sobre el cociente $(\mathbb{N} \cup \{0\})^2 / \sim$ (Ejercicio 3.2), tenemos que $(\mathbb{Z},+)$ también es monoide abeliano.

Por otra parte, tampoco es difícil demostrar que $(\mathbb{N} \cup \{0\})^2$ es monoide abeliano para el producto, de tal forma que $(\mathbb{Z},.)$ es, asimismo, monoide abeliano.

Los elementos neutros (nulo y unidad, respectivamente) son:

$$\begin{aligned} [(0,0)] &= \{(0,0),(1,1),(2,2),(3,3),\ldots\} \quad \text{y} \\ [(1,0)] &= \{(1,0),(2,1),(3,2),(4,3),\ldots\}. \end{aligned}$$

Tales números enteros se escriben (por un abuso del lenguaje) como 0 y 1, respectivamente.

Para ver que $(\mathbb{Z},+)$ es un grupo, tan sólo falta probar la existencia de elemento opuesto para cada número entero. En efecto, dado el número entero

$[(m,n)]$, se tiene

$$[(m,n)] + [(n,m)] = [(m+n, m+n)] = [(0,0)] = 0,$$

de tal manera que el entero $[(n,m)]$ es el opuesto del $[(m,n)]$. □

Como la diferencia de números naturales tiene sentido en $\mathbb{Z}$ estamos en condiciones de obtener útiles relaciones entre los cardinales de conjuntos finitos. Dados dos conjuntos finitos A y B, A es la unión de $A \backslash B$ con $A \cap B$, siendo estos conjuntos disjuntos, por lo que

$$\operatorname{card}(A) = \operatorname{card}(A \backslash B) + \operatorname{card}(A \cap B). \tag{3.10}$$

Análogamente, se obtiene

$$\operatorname{card}(B) = \operatorname{card}(B \backslash A) + \operatorname{card}(A \cap B). \tag{3.11}$$

Por otro lado,

$$A \cup B = (A \backslash B) \cup (B \backslash A) \cup (A \cap B),$$

siendo los tres conjuntos del segundo miembro disjuntos dos a dos, de manera que

$$\operatorname{card}(A \cup B) = \operatorname{card}(A \backslash B) + \operatorname{card}(B \backslash A) + \operatorname{card}(A \cap B). \tag{3.12}$$

Combinando (3.10), (3.11) y (3.12) se concluye que

$$\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A \cap B).$$

Obsérvese que la fórmula anterior (de gran utilidad en matemática discreta y en probabilidad) carece de sentido en el caso de cardinales infinitos.

EJERCICIO 3.8. Probar que, dados tres conjuntos finitos A, B y C, se cumple

$$\begin{aligned}\operatorname{card}(A \cup B \cup C) &= \operatorname{card}(A) + \operatorname{card}(B) + \operatorname{card}(C) \\ &\quad - \operatorname{card}(A \cap B) - \operatorname{card}(A \cap C) - \operatorname{card}(B \cap C) \\ &\quad + \operatorname{card}(A \cap B \cap C).\end{aligned}$$

Nos ocuparemos a continuación de ordenar los números enteros. Procuramos definir un orden total que extienda el orden de los números naturales y que sea compatible con las dos operaciones en un sentido que explicitaremos más tarde.

Definiremos el significado de número entero positivo a través de representantes, pero para que la definición sea buena necesitamos el siguiente resultado previo.

Proposición 3.5. *Cada número entero tiene un representante único en* $(\mathbb{N} \cup \{0\})^2$ *con al menos una componente nula (representante canónico).*

Demostración. Dado $z \in \mathbb{Z}$ es posible escribir $z = [(m,n)]$. En el peor caso, m y n son números naturales. Como $(\mathbb{N}, \leq)$ es un orden total, hay tres casos posibles:

(*a*) $m = n$. Entonces $z = [(m,n)] = [(0,0)]$.

(*b*) $m < n$. Entonces existe un $p \in \mathbb{N}$ tal que $m + p = n$ y se tiene

$$z = [(m, m+p)] = [(0,p)]. \tag{3.13}$$

(*c*) $n < m$. Entonces, análogamente, existe un $q \in \mathbb{N}$ tal que $n + q = m$ y tenemos

$$z = [(n+q, n)] = [(q,0)]. \tag{3.14}$$

Así pues, en los tres casos, z tiene una representación con una o dos componentes nulas.

La unicidad se prueba a través de una sencilla discusión que se deja al cuidado del lector. □

Los enteros $[(m,n)]$ que verifican (3.14) se denominan positivos, y los que cumplen (3.13), negativos.

Definición 3.12. *Un número entero es* ***positivo*** *si para algún (todo) representante (m,n) de su clase se cumple que $m > n$. Análogamente, es* ***negativo*** *si se cumple que $m < n$. Denotamos $\mathbb{Z}^+$ y $\mathbb{Z}^-$ a los conjuntos respectivos.*

Proposición 3.6. *$\mathbb{Z}^+$ es cerrado bajo las operaciones de suma y producto inducidas por $\mathbb{Z}$. Además, todo número entero es positivo, negativo o cero (tricotomía).*

Demostración. Sean $a, b \in \mathbb{Z}^+$ y elegimos sus representantes canónicos,

$$a = [(m,0)] \quad \text{y} \quad b = [(n,0)]$$

con $m, n \in \mathbb{N}$. Entonces, es inmediato que

$$a + b = [(m+n, 0)] \in \mathbb{Z}^+,$$

y que

$$ab = [(mn, 0)] \in \mathbb{Z}^+.$$

La tricotomía se sigue de la existencia y unicidad de la representación canónica. □

Es fácil probar que se cumple la regla de los signos. Por ejemplo, si multiplicamos un entero positivo $z = [(q,0)]$ por otro negativo $z' = [(0,p)]$, el producto $zz' = [(0,pq)]$ es negativo.

Definición 3.13. *Dados $a, b \in \mathbb{Z}$, se dice que $a < b$ si*

$$b + (-a) = b - a \in \mathbb{Z}^+.$$

Definimos sobre $\mathbb{Z}$ la relación de orden, $\leq$, así:

$$a \leq b \Longleftrightarrow a = b \vee a < b.$$

Como consecuencia directa de la Proposición 3.6 (tricotomía), la RBO $\leq$ definida sobre $\mathbb{Z}$ es un orden total. Además, los enteros positivos son aquellos $z \in \mathbb{Z}$ tales que $z > 0$.

Que el conjunto de los elementos positivos sea cerrado bajo la suma y el producto determina la compatibilidad del orden respecto de las dos operaciones. Veremos posteriormente que ello implica que se cumplen las dos **leyes de monotonía** básicas:

$$a < b \Longrightarrow a + c < b + c,$$
$$(a < b \wedge c > 0) \Longrightarrow ac < bc.$$

EJERCICIO 3.9. Demuestre que la aplicación $f : \mathbb{N} \longrightarrow \mathbb{Z}$ tal que $f(n) = [(n, 0)]$ es un monomorfismo respecto de la suma y del producto. Además, esta aplicación preserva el orden en el sentido de que $n \leq m \Longrightarrow f(n) \leq f(m)$.

De alguna forma se está afirmando que $\mathbb{Z}^+ = f(\mathbb{N})$ es una copia exacta de $\mathbb{N}$, tanto desde el punto de vista algebraico como del orden. Por eso se dice que el conjunto de los enteros es una extensión del conjunto de los naturales y en este sentido debe interpretarse la afirmación $\mathbb{N} \subset \mathbb{Z}$.

Para terminar esta sección, dedicada a los números enteros, efectuaremos la construcción geométrica de $\mathbb{Z}$ y de $\mathbb{Z}^2$. Siempre que hablemos de construcción geométrica en este texto se sobreentenderá que se dispone de dos instrumentos, una regla (sin graduar) y un compás, y de un segmento unidad. La regla permite construir rectas que pasan por dos puntos y el compás permite construir circunferencias con centro en un punto y cuyo radio se obtiene por traslación de un segmento. Para construir $\mathbb{Z}$ sobre una recta elegimos un punto O de la misma y una dirección arbitraria, que se llamará *positiva*. Trasladando el segmento unidad desde O en esa dirección se construyen $1, 2, \ldots$, y trasladándolo en la dirección opuesta se construyen $-1, -2, \ldots$ (véase Figura 3.4).

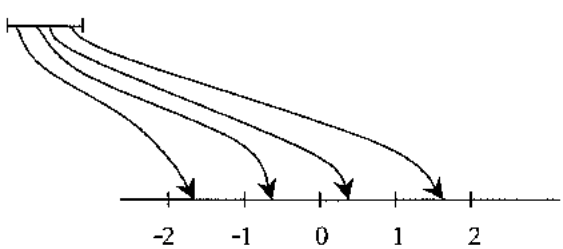

Figura 3.4. *Construcción geométrica de $\mathbb{Z}$.*

La construcción geométrica de $\mathbb{Z}^2$ requiere la previa construcción de una recta perpendicular a la anterior en el punto O (véase Figura 3.5).

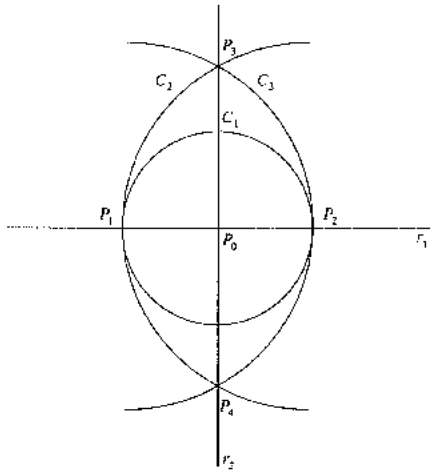

Figura 3.5. *Construcción geométrica de una recta perpendicular a r_1 en $P_0 \in r_1$: se traza una circunferencia con centro en P_0 y radio arbitrario, C_1, cuyas intersecciones con r_1 son P_1 y P_2; se trazan las circunferencias C_2 y C_3 cuyos centros son P_2 y P_1 y cuyo radio es la distancia entre P_1 y P_2; las intersecciones de C_2 y C_3 son P_3 y P_4, que determinan la recta buscada, r_2.*

Acto seguido se construye de nuevo $\mathbb{Z}$ sobre esta recta (como en la Figura 3.4), con lo que hemos construido unos *ejes cartesianos* sobre el plano. Finalmente se trazan rectas perpendiculares a los ejes que pasen por los puntos construidos sobre los mismos (usando el procedimiento indicado en la Figura 3.5). El conjunto de los puntos de intersección de cada par de rectas perpendiculares es $\mathbb{Z}^2$ (véase la Figura 3.6).

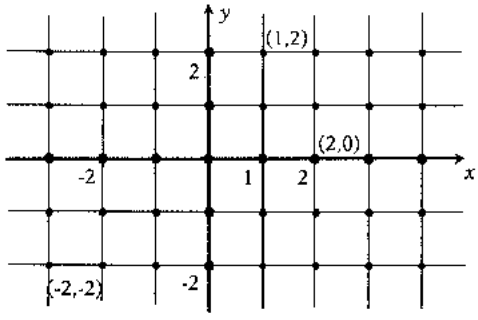

Figura 3.6. *Construcción geométrica de $\mathbb{Z}^2$.*

3.4. Problemas

Problema 3.1. Sobre el conjunto $E = \{0, 1, 2, 3, 4\}$ se define una operación a través de la tabla de abajo. Compruebe que dicha operación satisface todas las propiedades de los grupos, a excepción de una.

$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	4	2	3
2	2	3	0	4	1
3	3	4	1	0	2
4	4	2	3	1	0

Problema 3.2. Analice la estructura algebraica que resulta al dotar al conjunto $\mathbb{N}$ con cada una de las siguientes operaciones:

a) $m \oplus n = \max\{m, n\}$.
b) $m \boxdot n = m$.
c) $m \circledcirc n = \text{m.c.d.}\,(m, n)$.

Problema 3.3. Dado un conjunto $X \neq \emptyset$, demuestre que el conjunto de sus partes, $\mathcal{P}(X)$, es un grupo conmutativo para la diferencia simétrica de conjuntos, que se define así:

$$A \triangle B = (A \cap \overline{B}) \cup (B \cap \overline{A}).$$

Problema 3.4. Sean $(G, \circ)$ y $(H, *)$ grupos y $f : G \longrightarrow H$ un homomorfismo. Demuestre que la imagen por f del elemento neutro de $(G, \circ)$ es el elemento neutro de $(H, *)$ y que la imagen del elemento simétrico de cualquier elemento $a \in G$ es el elemento simétrico de $f(a)$.

Problema 3.5. Considere los grupos abelianos $(G, \circ)$ y $(H, *)$ dados por las siguientes tablas de Cayley:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$*$	s	t	u	v
s	s	t	u	v
t	t	s	v	u
u	u	v	s	t
v	v	u	t	s

a) Determine si $(G, \circ)$ y $(H, *)$ son isomorfos. (Sugerencia: Aplique el Problema 3.4.)
b) Encuentre todos los subgrupos de $(G, \circ)$ y $(H, *)$.

Problema 3.6. En éste y en los próximos problemas se supondrán conocidas las propiedades de los conjuntos numéricos que revisaremos en los próximos

capítulos. Analice la estructura algebraica del conjunto de los números racionales $\mathbb{Q}$ para las siguientes operaciones:

a) $a \oplus b = | a - b |$.

b) $a \boxdot b = \frac{ab}{2}$.

c) $a \circledcirc b = a + b + ab$.

Problema 3.7. Sobre los números reales no negativos se define una operación que asocia a cada par de números la parte entera por defecto de su suma. Clasifique la correspondiente estructura algebraica.

Problema 3.8. Considérese sobre $E = \{(x,y) \in \mathbb{R}^2 \mid x \neq 0\}$ la operación $(a,b) \boxplus (c,d) = (ac, bc + d)$. Pruebe que $(E, \boxplus)$ es un grupo no conmutativo.

Problema 3.9. Considérense las operaciones binarias usuales + y . para números reales. Compruebe que $(]0,+\infty[, .)$ y $(\mathbb{R}, +)$ son grupos abelianos y que $\log x$ define un homomorfismo de $]0,+\infty[$ en $\mathbb{R}$. Clasifique este homomorfismo.

Problema 3.10.* Dado un semigrupo (E, ∇), no siendo E vacío ni singular, se pide:

a) Defina sobre E dos RBE compatibles con ∇, las de mayor y menor grafo, describa sus correspondientes semigrupos cociente y diga si alguno de ellos es grupo.

b) Pruebe que si E es una pareja, cualquier RBE sobre E es compatible con ∇.

c) Dé un ejemplo de RBE sobre un semigrupo (E, ∇) que no sea compatible con la operación.

Problema 3.11. Pruebe que la composición de homomorfismos de cierta clase pertenece a la misma clase y que dos estructuras algebraicas isomorfas (es decir, entre las que existe un isomorfismo) poseen las mismas propiedades algebraicas.

Problema 3.12. Supongamos que $(G, \star)$ y (E, ∇) son grupos y que G' y E' son subgrupos de G y de E, respectivamente. Pruebe que, si f es un homomorfismo de G en E, entonces $f(G')$ y $f^{-1}(E')$ son subgrupos. Deduzca de aquí que el conjunto imagen y $\ker f$ son subgrupos. Demuestre también que f es un monomorfismo si, y sólo si, $\ker f$ es singular.

Problema 3.13.* Sea $G_1, G_2, \ldots$ una sucesión de subgrupos de $(G, \star)$. Demuestre que la intersección de todos ellos es un subgrupo y que la unión también lo es, con tal de que dicha sucesión sea expansiva, es decir, que $G_n \subset G_{n+1}$ para todo $n \in \mathbb{N}$. Pruebe que esta condición (que la sucesión sea expansiva) no es superflua.

Problema 3.14. Sabemos que $G := \mathbb{Q} \setminus \{0\}$ es un grupo conmutativo para el producto. Se define $f : G \longrightarrow G$ tal que $f(x) = x^2$. Demuestre que f es un endomorfismo ni inyectivo ni suprayectivo. Determine también el conjunto cociente $G/\ker(f)$.

Problema 3.15. Dado un grupo G cuya operación denotamos como un producto, se define la aplicación $f : G \longrightarrow G$ tal que $f(x) = x^{-1}$. Pruebe que f es un automorfismo si, y sólo si, G es conmutativo.

Problema 3.16.* Una permutación de $A_n = \{1, \ldots, n\}$ es una aplicación biyectiva de A_n en A_n. Las permutaciones de A_n pueden representarse mediante una matriz $2 \times n$ cuya primera fila son los elementos de A_n y cuya segunda fila está formada por las imágenes de los elementos de la primera. Así, la permutación $f : A_n \longrightarrow A_n$ se representa por

$$\begin{pmatrix} 1 & \ldots\ldots & n \\ f(1) & \ldots\ldots & f(n) \end{pmatrix}.$$

Pruebe que dichas permutaciones forman un grupo con la composición de aplicaciones como operación binaria. Construya la tabla de Cayley para $n = 2, 3$. ¿Para qué valores de n es conmutativo el grupo de las permutaciones?

Problema 3.17.* Sea $E = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b,\ a \in \mathbb{R}\setminus\{0\},\ b \in \mathbb{R}\}$.

a) Demuestre que E es un grupo para la composición de aplicaciones.
b) ¿Es E un grupo abeliano?
c) Sea $H = \{f \in E \mid f(x) = x + b,\ b \in \mathbb{R}\}$. Demuestre que H es un subgrupo de E.
d) Se define en E la relación binaria cuyo grafo es

$$G = \left\{(f,g) \in E^2 \mid g \circ f^{-1} \in H\right\}.$$

Pruebe que G define una relación de equivalencia sobre E.
e) Demuestre que E/G es equipotente a $\mathbb{R}\setminus\{0\}$.

Problema 3.18. Pruebe que si H es un subgrupo de $(\mathbb{Z}, +)$ tal que $1 \in H$, entonces $H = \mathbb{Z}$.

Problema 3.19. Sea $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Se pide:

a) Pruebe que $n\mathbb{Z}$ es subgrupo de $(\mathbb{Z}, +)$, para cada $n \in \mathbb{N}$;
b) Pruebe que $6\mathbb{Z} \cup 10\mathbb{Z}$ no es un subgrupo.
c) ¿Cuál es el mínimo subgrupo de $(\mathbb{Z}, +)$ que contiene a $6\mathbb{Z} \cup 10\mathbb{Z}$?
d) ¿Qué puede decir sobre el mínimo subgrupo de $(\mathbb{Z}, +)$ que contiene a $n\mathbb{Z} \cup m\mathbb{Z}$, para $n, m \in \mathbb{N}$?
e) Determine $6\mathbb{Z} \cap 10\mathbb{Z}$.
f) ¿Qué puede decir sobre $n\mathbb{Z} \cap m\mathbb{Z}$, para $n, m \in \mathbb{N}$?

Problema 3.20. En una clase de 40 alumnos, 30 juegan al fútbol, 22 al tenis y 8 no juegan a ninguno de los dos. ¿Cuántos practican a la vez fútbol y tenis?

Problema 3.21. En un grupo de 200 alumnos hay 70 alumnos que estudian matemáticas, 120 física y 90 química; además, 50 estudian matemáticas y física, 30 matemáticas y química, 40 física y química, y finalmente 20 las tres asignaturas.

a) ¿Es correcta la información si todos estudian alguna de las tres?
b) ¿Cuántos alumnos estudian matemáticas o física?
c) ¿Cuántos alumnos no estudian ninguna asignatura de las dadas?
d) ¿Cuántos alumnos estudian matemáticas o química?
e) ¿Cuántos alumnos estudian al menos alguna de las tres?
f) ¿Cuántos alumnos estudian física o química?

Problema 3.22. En el conjunto formado por todos los números naturales menores de 1.000, ¿cuántos números hay que no son múltiplos ni de 3, ni de 5, ni de 7?

CAPÍTULO 4

ANILLOS Y CUERPOS

Este capítulo se ocupa de estructuras algebraicas ligeramente más complejas que las consideradas en el Capítulo 3, puesto que supondremos que el conjunto considerado está dotado de dos operaciones relacionadas entre sí. En su transcurso analizaremos la relación existente entre la suma y el producto sobre $\mathbb{Z}$, y tomaremos a la tripleta $(\mathbb{Z}, +, .)$ como modelo de una estructura algebraica que surge con mucha frecuencia en matemáticas: el anillo. Al concepto de anillo se llegó al observar la semejanza de comportamientos de los números enteros y de los polinomios desde el punto de vista de la divisibilidad, uno de los problemas matemáticos clásicos. De la divisibilidad en $\mathbb{Z}$ se ocupó Euclides en los libros VII y IX de sus célebres *Elementos*, mientras que la división euclídea de polinomios era introducida por el hispano-portugués Pedro Nuñez (siglo XVI) y desarrollada por Euler (siglo XVIII), quien se ocupó, en particular, de la divisibilidad en el caso de los polinomios con coeficientes enteros. En una monografía sobre teoría de números de Gauss, publicada en 1801 bajo el título de *Disquisitiones Aritmeticae*, se explota la noción de congruencia de números enteros, introducida por Euler, para probar resultados clásicos de Fermat en teoría de números y para obtener nuevos resultados. Veremos que la congruencia es una RBE sobre $\mathbb{Z}$ y que el cociente (de $\mathbb{Z}$ por dicha relación) es un anillo finito. Estos anillos vienen utilizándose desde mediados del siglo XX para generar números seudoaleatorios (que son la herramienta básica en simulación digital). La definición abstracta de anillo es muy tardía (Fraenkel, 1914), aunque ciertos conceptos de la teoría de anillos ya eran conocidos (por ejemplo, el de subconjunto ideal, introducido por Dedekind en su construcción de los números reales a partir de los racionales).

Por lo que respecta al concepto de cuerpo (traducción del alemán «Körper»), también llamado campo (del inglés «field»), se obtuvo por abstracción, como el de grupo, a partir de las estructuras algebraicas que iban surgiendo en el estudio de la resolubilidad por radicales de las ecuaciones algebraicas. Los cuerpos finitos, en particular, son la base para la teoría de la codificación, disciplina en la que se utilizan anillos de polinomios y espacios vectoriales sobre cuerpos finitos.

En este capítulo se obtendrá también el cuerpo de fracciones de un dominio de integridad y, como un caso particular, construiremos un nuevo conjunto numérico, al que también dotaremos de dos operaciones, que extiende al do-

minio de integridad $\mathbb{Z}$ pero que es todavía más rico en propiedades algebraicas: el cuerpo de los números racionales, $(\mathbb{Q}, +, .)$. También veremos cómo la ordenación de los enteros se extiende a un orden de los racionales. La relación existente entre las estructuras algebraica y de orden superpuestas sobre $\mathbb{Q}$ se resume diciendo que $(\mathbb{Q}, +, ., \leq)$ es un cuerpo ordenado arquimediano.

4.1. Anillos: los números enteros y congruencias

Definición 4.1. *Supongamos que sobre un conjunto $A \neq \emptyset$ están definidas dos operaciones binarias, que llamaremos suma y producto (y representaremos con notaciones aditiva y multiplicativa, respectivamente). Se dice que la tripleta $(A, +, .)$ es un* ***anillo*** *si se cumple:*

(*a*) *$(A, +)$ es un grupo conmutativo (cuyo neutro se denota con 0);*
(*b*) *$(A, .)$ es un semigrupo; y*
(*c*) *el producto es distributivo respecto de la suma por ambos lados, es decir,*

$$a(b+c) = ab + ac \text{ y } (b+c)a = ba + ca$$

cualesquiera que sean a, b y c en A.

Si, además, el producto es conmutativo, se dice que $(A, +, .)$ es un ***anillo conmutativo****.*

Si $(A, .)$ es un monoide (conmutativo o no), entonces $(A, +, .)$ es un ***anillo unitario****, denotándose por 1 el neutro del producto. Exigimos, además, que $1 \neq 0$, para evitar considerar al* ***anillo trivial*** *$A = \{0\}$ como anillo unitario.*

Si $(A, +, .)$ es un anillo y $a \in A$, el opuesto de a se denota por $-a$ y su inverso, si es que existe, por a^{-1}. Se definen na y a^n para todo $n \in \mathbb{N}$ por recursión: $1a = a$, $(n+1)a = na + a$, y, $a^1 = a$, $a^{n+1} = a^n a$, respectivamente.

Ejemplo 4.1. Hemos definido en $\mathbb{Z}$ las operaciones suma y producto, y nos preguntamos si el producto es distributivo respecto de la suma. Consideramos tres parejas (m, n), (p, q) y (r, s) de $[\mathbb{N} \cup \{0\}]^2$. Se tiene

$$\begin{aligned}(m,n)\{(p,q)+(r,s)\} &= (m,n)(p+r, q+s)\\ &= (m(p+r)+n(q+s), n(p+r)+m(q+s))\\ &= (m,n)(p,q)+(m,n)(r,s)\end{aligned}$$

Como la RBE que hemos definido sobre $[\mathbb{N} \cup \{0\}]$ es compatible con la suma y con el producto, la relación de arriba se cumplirá también con las clases de equivalencia, es decir,

$$[(m,n)]\{[(p,q)]+[(r,s)]\} = [(m,n)][(p,q)] + [(m,n)][(r,s)],$$

de manera que $(\mathbb{Z}, +, .)$ es un anillo conmutativo y unitario $(1 \neq 0)$.

Definición 4.2. *Un elemento $x \in A$, $x \neq 0$, es* ***divisor de cero*** *por la izquierda (derecha) si existe $y \in A$, $y \neq 0$, tal que $xy = 0$ ($yx = 0$, respectivamente). Un anillo carente de divisores de cero se dice que es* ***íntegro****. Un anillo conmutativo, unitario e íntegro es un* ***dominio de integridad****.*

$(\mathbb{Z}, +, .)$ es un dominio de integridad, ya que si se toman dos enteros no nulos, cada uno de ellos será o positivo o negativo y su producto no podrá ser nulo al cumplirse la regla de los signos.

EJERCICIO 4.1. Compruebe que la tripleta $(G, +, .)$ definida en el Ejemplo 3.3 es un dominio de integridad (finito).

Ejemplo 4.2. Sea $(A, +, .)$ cualquier anillo y consideremos el conjunto de las matrices 2×2

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in A \right\}.$$

Se puede verificar que S con la suma y el producto usuales de matrices es también un anillo. Se denomina **anillo de matrices** de 2×2 sobre A. Si $(A, +, .)$ es unitario, también lo será S, y considerando las matrices

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ y } N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

se observa que $0 = MN \neq NM$, por lo que S no es anillo conmutativo y tiene divisores de cero.

Ejemplo 4.3. Sea $(A, +, .)$ cualquier anillo y $B \neq \emptyset$ un conjunto. Consideremos el conjunto R de todas las aplicaciones $f : B \longrightarrow A$. Para $f, g \in R$ y $x \in B$ definamos $(f + g)(x) = f(x) + g(x)$ y $(f.g)(x) = f(x).g(x)$. Con estas operaciones R es un anillo (conmutativo y unitario si A lo es).

El siguiente resultado reúne algunas propiedades elementales de los anillos.

Proposición 4.1. *Si $(A, +, .)$ es un anillo, $a, b \in A$ y $n \in \mathbb{N}$ se cumple:*

(i) $0a = a0 = 0$;
(ii) $-(ab) = (-a)b = a(-b)$;
(iii) $(-a)(-b) = ab$; y
(iv) $n(ab) = (na)b = a(nb)$

Además, $(A, +, .)$ es íntegro si, y sólo si, se cumplen las dos leyes de cancelación siguientes:

(v) $[(ax = bx) \wedge (x \neq 0)] \Longrightarrow a = b$; y
(vi) $[(xa = xb) \wedge (x \neq 0)] \Longrightarrow a = b$.

Demostración. (*i*) $0a = (0+0)a = 0a+0a$. Sumando el opuesto de $0a$ a ambos miembros, queda $0a = 0$. Lo mismo ocurre por la derecha.

(*ii*) $ab + (-a)b = [a + (-a)]b = 0b = 0$. Por lo tanto $(-a)b$ es el opuesto de ab, es decir, $-(ab) = (-a)b$. La otra igualdad se prueba de la misma forma.

(*iii*) Ambos miembros de la igualdad son opuestos de $-(ab)$, como consecuencia de (*ii*).

(*iv*) Se prueba por inducción.

(*v*) Si $ax = bx$, entonces $(a-b)x = 0$ y, al ser $x \neq 0$, tendrá que ser $a-b = 0$.

(*vi*) La prueba es similar.

Recíprocamente, si $ab = 0$ y $a \neq 0$, aplicando (*v*) a la igualdad $ab = a0$ se obtiene $b = 0$. Análogamente, si $ab = 0$ y $b \neq 0$, aplicando (*vi*) a la igualdad $ab = 0b$ se obtiene $a = 0$. □

Note que si $(A, +, .)$ es un dominio de integridad, cualquier ecuación de la forma $ax = b$ con $a \in A \setminus \{0\}$, $b \in A$ tiene a lo sumo una solución (por la ley de cancelación).

En el capítulo anterior vimos que una forma estándar de obtener un nuevo grupo a partir de otro ya conocido es hacer el cociente por una RBE compatible con la operación. El mismo procedimiento sirve para los anillos, debiendo ser ahora la RBE compatible con las dos operaciones.

Proposición 4.2. *Si $\sim$ es una RBE sobre el anillo $(A, +, .)$ compatible con ambas operaciones, entonces $(A/\sim, +, .)$ es un anillo (llamado* ***anillo cociente****). Además, si $(A, +, .)$ es conmutativo (unitario), $(A/\sim, +, .)$ es asimismo conmutativo (unitario).*

Demostración. Sabemos, de la Sección 3.1, que $(A/\sim, +)$ es grupo conmutativo y que $(A/\sim, .)$ es semigrupo. Por lo que respecta a la propiedad distributiva (por ambos lados) es hereditaria, lo que se prueba exactamente igual que en el Ejemplo 4.1 para $(\mathbb{Z}, +, .)$. La última afirmación es consecuencia del carácter hereditario, a través de cocientes, de la conmutatividad y de la existencia de elemento unidad. □

En el caso de los grupos conmutativos, cualquier subgrupo proporcionaba una RBE compatible. Como un anillo $(A, +, .)$ es un grupo conmutativo si nos restringimos a la adición, una RBE compatible con la suma surgirá de cualquier subgrupo, pero no necesariamente tal RBE será compatible con el producto.

Ejemplo 4.4. El conjunto de las funciones $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, con las operaciones de adición y multiplicación de funciones punto a punto (véase Ejemplo 4.3) es un anillo conmutativo y unitario que denotaremos por $(R, +, \times)$. Consideremos el subconjunto $S \subset R$ de todas las funciones constantes. Es inmediato verificar que $(S, +)$ es un subgrupo de $(R, +)$, por lo que el cociente $(R/S, +)$ es también un grupo.

Supongamos que el producto de clases se definiera por medio de representantes. Tomando, entonces, la función identidad $I_{\mathbb{Z}}$, y denotando por f_1 la función constantemente igual a 1, se tendría que

$$[I_{\mathbb{Z}}] = [I_{\mathbb{Z}} \times f_1] = [I_{\mathbb{Z}}] \times [f_1]. \tag{4.1}$$

Como $[f_1] = 0$ (ya que $f_1 \in S$), se debe cumplir que $[I_{\mathbb{Z}}] \times [f_1] = 0$, por la Proposición 4.1(i). Sin embargo, $[I_{\mathbb{Z}}] \neq 0$, debido a que $I_{\mathbb{Z}} \notin S$, lo que prueba que la ecuación (4.1) es contradictoria. Por lo tanto, se concluye que no es posible en este ejemplo definir el producto de clases por medio de representantes para que resulte un anillo cociente.

Para asegurar que una RBE sea compatible con el producto hay que subir el nivel de exigencia, no bastando que el subgrupo sea subanillo (es decir, un subconjunto que es anillo con las operaciones inducidas), según muestra el Ejemplo 4.4.

Definición 4.3. *Dados dos anillos $(A, +, .)$ y $(B, \oplus, \odot)$, se dice que una aplicación $f : A \to B$ es un* ***homomorfismo de anillos*** *si*

$$f(x+y) = f(x) \oplus f(y) \quad \text{y} \quad f(x.y) = f(x) \odot f(y),$$

cualesquiera que sean $x, y \in A$.

Resulta natural exigir que ambas operaciones sean preservadas por un homomorfismo de anillos. Las definiciones de monomorfismo, epimorfismo, isomorfismo, endomorfismo y automorfismo de anillos son las mismas que se dieron en el capítulo de grupos. Asimismo, las propiedades son semejantes y se enuncian, en forma de problemas, al final del capítulo.

La definición anterior dice que un homomorfismo de anillos f es también un homomorfismo de grupos (abelianos), considerando solamente la primera operación en ambos anillos. De esa forma, podemos concluir, por lo que conocemos de teoría de grupos, que $\ker f = f^{-1}(0)$ es un subgrupo de $(A, +)$. Pero hay algo más. Si $k \in \ker f$ y $a \in A$, entonces

$$f(a.k) = f(a) \odot f(k) = f(a) \odot 0 = 0,$$

de manera que $\ker f$ «absorbe» elementos arbitrarios del anillo con el producto. Esta propiedad adicional del núcleo es lo que se necesita para producir RBE compatibles.

Definición 4.4. *Dado un anillo conmutativo $(A, +, .)$, se dice que un subconjunto $I \neq \emptyset$ es un* ***ideal*** *en dicho anillo si I es un subgrupo aditivo y, además, I es absorbente para los elementos de A, es decir, $ax \in I$ cualesquiera que sean $x \in I$ y $a \in A$.*

Desde luego, si I es un ideal en $(A, +, .)$, también es un subanillo con las operaciones inducidas.

Proposición 4.3. *Si I es un ideal en el anillo conmutativo $(A, +, .)$, entonces la siguiente relación binaria sobre A es una RBE compatible con la suma y el producto:*

$$x \sim y \Longleftrightarrow x - y \in I.$$

Demostración. Sabemos que es una RBE compatible con la suma por ser I un subgrupo de $(A, +)$. Hay que probar la compatibilidad con el producto. Sean, pues, $a_1 \sim a_2$ y $b_1 \sim b_2$ tomados en A. Como $a_1 \in a_2 + I$ y $b_1 \in b_2 + I$, se tendrá

$$a_1 b_1 \in (a_2 + I)(b_2 + I) = a_2 b_2 + a_2 I + b_2 I + II,$$

donde los productos de conjuntos se efectúan elemento a elemento:

$$XY = \{xy \mid (x \in X) \wedge (y \in Y)\}.$$

Por ser I absorbente se tiene que $a_2 I \subset I$, $b_2 I \subset I$ y también $II \subset I$. Así pues, $a_1 b_1 \in a_2 b_2 + I$, es decir, $a_1 b_1 \sim a_2 b_2$. □

La combinación de las Proposiciones 4.2 y 4.3 permite afirmar que A/I es anillo conmutativo, y también unitario si lo es A. Este resultado es la clave para construir los números reales a partir de los números racionales, extensión que llevaremos a cabo en el Capítulo 5. Pero, antes, conviene conocer los anillos de **clases de congruencias** (de Gauss).

EJERCICIO 4.2. Dados tres números enteros, x, y y $m > 1$ (llamado módulo), se dice que x es congruente con y módulo m ($x \equiv_m y$) cuando la diferencia $x - y$ es un múltiplo de m. Se pide:

(i) Pruebe que los múltiplos de m forman un ideal en $\mathbb{Z}$ (que denotaremos $m\mathbb{Z}$).

(ii) Demuestre que la relación $\equiv_m$ sobre $\mathbb{Z}$ es la asociada con el ideal $m\mathbb{Z}$. Por lo tanto, la congruencia define una RBE compatible con ambas operaciones y el anillo cociente $\mathbb{Z}/\equiv_m$ está bien definido. Este anillo de clases de congruencia módulo m se denota por $\mathbb{Z}_m$.

(iii) Pruebe que $\mathbb{Z}_m$ tiene m elementos (pues los restos en la división euclídea por m son $0, 1, \ldots, m-1$). Representaremos por $\overline{x}$ (en lugar de $[x]$) las clases de equivalencia. Verifique que $\overline{0} = m\mathbb{Z}$ y que $\overline{1} = 1 + m\mathbb{Z}$.

(iv) Construya las tablas de Cayley de $(\mathbb{Z}_m, +, .)$, para $m = 2, 3, 4$. ¿Cuándo es íntegro el anillo $(\mathbb{Z}_m, +, .)$?

Definición 4.5. *Un anillo unitario $(K, +, .)$ se dice que es un* ***anillo con división*** *si cada $a \in K$, $a \neq 0$, tiene inverso $a^{-1} \in K$ (es decir, $(K \setminus \{0\}, .)$ es un grupo). Si, además, el producto es conmutativo, decimos entonces que $(K, +, .)$ es un* ***cuerpo*** *o un* ***campo****.*

El siguiente resultado aclara la relación entre dominios de integridad y cuerpos.

Corolario 4.1. (*i*) *Todo cuerpo es dominio de integridad.*
(*ii*) *Todo dominio de integridad finito es cuerpo.*

Demostración. (*i*) Un cuerpo es un anillo conmutativo unitario. Además, si $a \neq 0$ y $b \neq 0$ son elementos del cuerpo, entonces existe a^{-1} y, si fuese $ab = 0$, multiplicando por a^{-1} y aplicando la propiedad asociativa se tendría que $b = 0$.

(*ii*) Sea $(A, +, .)$ dominio de integridad finito y sea $a \neq 0$ un elemento de A. La clave de la prueba es que la aplicación

$$\begin{aligned} f: \quad A &\longrightarrow A \\ x &\longmapsto ax \end{aligned}$$

es inyectiva, ya que, si $ax = ay$ entonces $a(x - y) = 0$, y como $a \neq 0$ y A es dominio de integridad, se tiene $x = y$. Siendo A finito, f tiene que ser biyectiva, por lo que existe un único elemento $x \in A$ tal que $f(x) = 1$, es decir, $ax = 1$. Tal elemento x es el inverso de a y concluimos que $(A, +, .)$ es cuerpo. □

Como consecuencia del Corolario 4.1, $\mathbb{Z}_p$ es un cuerpo si p es un número primo. En caso contrario, $\mathbb{Z}_p$ es un anillo conmutativo y unitario, pero no íntegro (ni, por lo tanto, cuerpo). $\mathbb{Z}$ es dominio de integridad pero no cuerpo, de manera que la finitud es esencial para la validez de (*ii*) en el Corolario 4.1.

Una **ecuación lineal** en un cuerpo $(K, +, .)$ es una expresión del tipo

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

donde $a_i \in K$, $i = 1, 2, \ldots, n$, se llaman **coeficientes** y $b \in K$ es el **término independiente** de la ecuación. Cuando $b = 0$, la ecuación lineal se denomina **homogénea**. Evidentemente, una ecuación puede interpretarse como una forma proposicional sobre el conjunto K^n; las variables $x_1, x_2, \ldots, x_n$ son las **incógnitas** de la ecuación y su conjunto de soluciones es

$$\{(x_1, x_2, \ldots, x_n) \in K^n \mid a_1x_1 + a_2x_2 + \cdots + a_nx_n = b\},$$

es decir, el conjunto de n-plas de elementos de K que hacen verdadera la forma proposicional. El conjunto de soluciones, S, de un sistema de m ecuaciones lineales con coeficientes en K

$$\left.\begin{array}{c} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{array}\right\},$$

es la intersección de los correspondientes a sus m ecuaciones. El sistema es **incompatible** cuando $S = \emptyset$ y **compatible** si $S \neq \emptyset$. En este caso, el sistema es **determinado** si S es un conjunto singular e **indeterminado** cuando tiene más de una solución.

El conocido *método de eliminación* (o de Gauss) está basado en sucesivas transformaciones del sistema inicial utilizando las tres *operaciones elementales* siguientes:

(*i*) intercambiar dos ecuaciones;

(*ii*) multiplicar todos los coeficientes de una ecuación por un elemento de $A\backslash\{0\}$; y

(*iii*) sumarle a una ecuación el producto de un elemento de A por otra ecuación.

El último sistema obtenido es equivalente al primero (tiene el mismo conjunto de soluciones) y debe ser de resolución inmediata, por ejemplo, tener una estructura escalonada con ceros por debajo, y un 1 en cada esquina. Sin importar cuál sea el cuerpo K, siempre se puede obtener un sistema escalonado equivalente por el método de eliminación.

Un sistema homogéneo siempre es compatible (tiene al menos la denominada solución trivial, $(0, \ldots, 0)$). Un sistema homogéneo con más incógnitas que ecuaciones es indeterminado y, cuando el cuerpo K es infinito, tiene infinitas soluciones (véase Problema 4.13).

4.2. Anillos de polinomios

Definición 4.6. *Sea F un cuerpo. El* ***anillo de polinomios*** *en una indeterminada x sobre F, que se expresará como $F[x]$, es el conjunto de todas las expresiones formales $p(x) = a_0 + a_1x + \ldots + a_nx^n$, donde los a_i, llamados los* ***coeficientes*** *del polinomio $p(x)$, están en F. Si $q(x) = b_0 + b_1x + \ldots + b_mx^m$ es también un polinomio en $F[x]$, se definen la igualdad, la suma y el producto de $p(x)$ y $q(x)$ como sigue:*

$$p(x) = q(x) \Longleftrightarrow a_i = b_i \text{ para todo } i \geq 0,$$

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_s + b_s)x^s,$$

donde $s = \max\{n, m\}$; y

$$p(x)q(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + a_nb_mx^{n+m}.$$

Ejemplo 4.5. Sean $p(x) = 1 + 3x^2$ y $q(x) = 4 - 5x + 7x^2 - x^3$. Entonces $p(x) \neq q(x)$, pues $a_3 = 0 \neq -1 = b_3$,

$$p(x) + q(x) = 5 - 5x + 10x^2 - x^3$$

y

$$p(x)q(x) = 4 - 5x + 19x^2 - 16x^3 + 21x^4 - 3x^5.$$

A lo largo de esta sección los polinomios serán considerados, exclusivamente, como expresiones formales que contienen elementos del cuerpo F (coeficientes) y una letra adicional x (indeterminada), con dos operaciones binarias. Veremos que en muchos aspectos $\mathbb{Z}$ y $F[x]$ son muy similares. Una diferencia importante es el concepto de raíz de un polinomio, carente de sentido en los números enteros. El estudio de la naturaleza de tales raíces se abordará

en los capítulos 6 y 7. La prueba del próximo resultado se deja como ejercicio para el lector.

Lema 4.1. *$(F[x], +, .)$ es un anillo conmutativo con unidad.*

Definición 4.7. *Si $p(x) = a_0 + a_1x + \ldots + a_nx^n$ y $a_n \neq 0$ entonces el* ***grado*** *de $p(x)$ es n (denotamos $\deg p(x) = n$).*

Así pues, el grado de un polinomio es la potencia más alta de x, con coeficiente no nulo, presente en la expresión de $p(x)$. Al polinomio $p(x) = 0$ no se le asigna grado. Los polinomios de grado 0 son las constantes no nulas; así, puede interpretarse F como un subanillo de $F[x]$.

Lema 4.2. *Si $p(x) = a_0 + a_1x + \ldots + a_nx^n$ y $q(x) = b_0 + b_1x + \ldots + b_mx^m$ son elementos no nulos en $F[x]$, entonces*

$$\deg(p(x) + q(x)) \leq \max\{\deg p(x), \deg q(x)\};$$

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x).$$

Demostración. Sean $n = \deg p(x)$ y $m = \deg q(x)$, es decir, $a_n \neq 0$ y $b_m \neq 0$. La primera fórmula es inmediata. Para la segunda, la potencia más alta de x que aparece en $p(x)q(x)$ es x^{m+n} (por la definición de producto) y su coeficiente es $a_nb_m \neq 0$, por ser F un cuerpo. □

Proposición 4.4. *$(F[x], +, .)$ es un dominio de integridad.*

Demostración. Se sigue inmediatamente de los Lemas 4.1 y 4.2. □

Una de las cosas que aprendimos a hacer con los polinomios en la enseñanza media es la división de polinomios, con un procedimiento muy similar al de la división entera. Lo recordamos en el siguiente ejemplo, que ilustra lo que se hará en el caso general.

Ejemplo 4.6. Se desea dividir $x^4 - 7x + 1$ entre $2x^2 + 1$. Se divide x^4 entre $2x^2$ para obtener $\frac{1}{2}x^2$. Luego $\frac{1}{2}x^2\left(2x^2 + 1\right) = x^4 + \frac{1}{2}x^2$ se sustrae de $x^4 - 7x + 1$ para obtener el primer resto, $-\frac{1}{2}x^2 - 7x + 1$. Como el grado del resto no es menor que el del divisor, se repite el proceso; se divide ahora $-\frac{1}{2}x^2$ entre $2x^2$ para obtener $-\frac{1}{4}$. Luego, $-\frac{1}{4}\left(2x^2 + 1\right) = -\frac{1}{2}x^2 - \frac{1}{4}$ se sustrae del primer resto para obtener el segundo resto, $-7x + \frac{5}{4}$. Como el grado de este resto es menor que el del divisor, la división ha concluido y expresamos el resultado de todo el proceso como

$$x^4 - 7x + 1 = \left(2x^2 + 1\right)\left(\frac{1}{2}x^2 - \frac{1}{4}\right) - 7x + \frac{5}{4}.$$

Este «repetir el proceso» sugiere inducción y es así como se llevará a cabo la demostración. Lo que se hace es muy semejante al algoritmo de Euclides para números enteros, que para polinomios se denomina *algoritmo de la división*.

Teorema 4.1. ***(Algoritmo de la división).*** *Dados los polinomios $p(x)$ (dividendo) y $q(x)$ (divisor) en $F[x]$, con $q(x) \neq 0$, se cumple que*

$$p(x) = q(x)\,c(x) + r(x),$$

donde $c(x), r(x) \in F[x]$ y $\deg r(x) < \deg q(x)$ o bien $r(x) = 0$. Además, los polinomios ***cociente*** *$c(x)$ y* ***resto*** *$r(x)$ están unívocamente determinados.*

Demostración. Probaremos la existencia de $c(x)$ y $r(x)$ por inducción completa sobre $\deg p(x)$ (véase el segundo principio de inducción en Problema 2.6). Si $p(x) = 0$, o bien, si $\deg p(x) < \deg q(x)$, entonces

$$p(x) = q(x)\,0 + p(x),$$

lo cual satisface la conclusión del teorema.

Supongamos, entonces, que $\deg p(x) \geq \deg q(x)$, de manera que

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \text{y} \quad q(x) = b_0 + b_1 x + \ldots + b_m x^m$$

donde $a_n \neq 0$, $b_m \neq 0$ y $n \geq m$. Consideremos el polinomio

$$\begin{aligned} \frac{a_n}{b_m} x^{n-m} q(x) &= \frac{a_n}{b_m} x^{n-m} (b_0 + b_1 x + \ldots + b_m x^m) \\ &= \frac{a_n b_0}{b_m} x^{n-m} + \ldots + a_n x^n, \end{aligned}$$

que tiene el mismo grado e igual coeficiente que la mayor potencia que $p(x)$, por lo que la diferencia

$$h(x) = p(x) - \frac{a_n}{b_m} x^{n-m} q(x) \tag{4.2}$$

verifica que $\deg h(x) < \deg p(x)$ o bien $h(x) = 0$ (en cuyo caso no hace falta seguir). Por hipótesis de inducción, la conclusión del teorema se cumple para $h(x)$ en virtud de que $\deg h(x) < \deg p(x)$, es decir, podemos escribir

$$h(x) = q(x)\,c_1(x) + r(x), \tag{4.3}$$

donde $c_1(x), r(x) \in F[x]$ y $\deg r(x) < \deg q(x)$ o bien $r(x) = 0$. Combinando (4.2) y (4.3),

$$p(x) - \frac{a_n}{b_m} x^{n-m} q(x) = q(x)\,c_1(x) + r(x),$$

por lo que

$$p(x) = q(x)\left(\frac{a_n}{b_m} x^{n-m} + c_1(x)\right) + r(x) = q(x)\,c(x) + r(x),$$

que es la representación deseada de $p(x)$.

Para probar la unicidad, considérense dos representaciones

$$p(x) = q(x)c_1(x) + r_1(x) = q(x)c_2(x) + r_2(x),$$

lo cual implica

$$q(x)[c_1(x) - c_2(x)] = r_2(x) - r_1(x).$$

Si $r_1(x) \neq r_2(x)$, entonces $c_1(x) \neq c_2(x)$ y, como consecuencia del Lema 4.2, tenemos

$$\begin{aligned} \deg q(x) &\leq \deg q(x) + \deg[c_1(x) - c_2(x)] = \deg[r_2(x) - r_1(x)] \\ &\leq \max\{\deg r_1(x), \deg r_2(x)\}, \end{aligned}$$

por lo que $\deg q(x) \leq \deg r_1(x)$ o bien $\deg q(x) \leq \deg r_2(x)$. En consecuencia, uno de los dos restos no satisfaría la condición de grado requerida.

Alternativamente, si $r_1(x) = r_2(x)$, entonces $c_1(x) = c_2(x)$ (al ser $F[x]$ dominio de integridad). Esto completa la prueba. □

Definición 4.8. *Si $p(x)$ y $q(x) \neq 0$ son polinomios en $F[x]$, entonces se dice que $q(x)$* ***divide*** *a $p(x)$ (y se denota como $q(x) \mid p(x)$) si*

$$p(x) = q(x)c(x)$$

para algún $c(x) \in F[x]$. También se dice que $p(x)$ es ***múltiplo*** *de $q(x)$.*

Un polinomio $p(x) \in F[x]$ de grado positivo se dice ***irreducible*** *en $F[x]$ si, cada vez que se descompone en factores*

$$p(x) = a(x)b(x),$$

con $a(x), b(x) \in F[x]$, entonces $\deg a(x) = 0$ o bien $\deg b(x) = 0$.

Se dice que dos polinomios no simultáneamente nulos $p(x), q(x) \in F[x]$ son ***primos entre sí*** *si los únicos polinomios $d(x) \in F[x]$ que verifican que $d(x) \mid p(x)$ y también $d(x) \mid q(x)$ son los polinomios de grado 0 (constantes no nulas).*

Es importante notar la analogía entre polinomios irreducibles y números primos. Esto no es mera casualidad sino el resultado de que tanto $\mathbb{Z}$ como $F[x]$ son dominios de integridad con algoritmo de la división. El siguiente resultado es de gran utilidad para divisibilidad.

Teorema 4.2 ***(débil de Bezout).*** *Los polinomios no nulos $p(x)$ y $q(x)$ en $F[x]$ son primos entre sí, si, y sólo si, existen $a(x), b(x) \in F[x]$ tales que*

$$1 = a(x)p(x) + b(x)q(x). \tag{4.4}$$

Demostración. Para la prueba directa consideremos el siguiente subconjunto de polinomios

$$I = \{a(x)p(x) + b(x)q(x) \mid a(x), b(x) \in F[x]\}.$$

Es fácil verificar que I es un subgrupo (por ser cerrado bajo diferencias) y absorbente ($F[x]I \subset I$), es decir, I es un ideal. Además, $I \neq \{0\}$, ya que $0 \neq q(x) \in I$. Elegimos un polinomio de grado mínimo $d(x) \in I$. Si $\deg d(x) = 0$, entonces $d(x) = d$ es una constante no nula en el cuerpo F y, por lo tanto, existe $d^{-1} \in F \subset F[x]$. Usando que I es absorbente, $d^{-1}d = 1 \in I$ y obtenemos (4.4).

Si $\deg d(x) > 0$, dado cualquier polinomio $f(x) \in I$ podemos aplicar el algoritmo de la división para representar

$$f(x) = d(x)c(x) + r(x),$$

o, en forma equivalente,

$$r(x) = f(x) - d(x)c(x),$$

con $\deg r(x) < \deg d(x)$. Usando las propiedades del ideal se concluye que $r(x) \in I$, por lo que la única posibilidad, no contradictoria con la elección de $d(x)$ con grado mínimo, es $r(x) = 0$. Concluimos, entonces, que $d(x) \mid f(x)$ para todo $f(x) \in I$. En particular, $d(x) \mid p(x)$ y también $d(x) \mid q(x)$. Como $p(x)$ y $q(x)$ son primos entre sí obtenemos la contradicción $\deg d(x) = 0$.

Para el recíproco, si $1 = a(x)p(x) + b(x)q(x)$, y $d(x)$ es cualquier polinomio tal que $d(x) \mid p(x)$ y $d(x) \mid q(x)$, entonces se tiene que

$$d(x) \mid a(x)p(x) + b(x)q(x),$$

por lo que $d(x) \mid 1$ y $\deg d(x) = 0$. □

La misma propiedad del teorema anterior, pero aplicada a los números enteros, nos dice, por ejemplo, que 8 y 5 son primos entre sí, debido a que $1 = 2 \times 8 - 3 \times 5$; o también, que dos números naturales consecutivos siempre son primos entre sí, puesto que $1 = 1 \times (n+1) - 1 \times n$.

Corolario 4.2. *Si $p(x), f(x) \in F[x]$ son primos entre sí, y, además,*

$$p(x) \mid f(x)g(x),$$

entonces $p(x) \mid g(x)$. En particular, si $p(x)$ es irreducible y si $p(x) \mid f(x)g(x)$, entonces $p(x) \mid f(x)$ o bien $p(x) \mid g(x)$.

Demostración. Como $1 = a(x)p(x) + b(x)f(x)$, multiplicando por $g(x)$ obtenemos

$$g(x) = a(x)p(x)g(x) + b(x)f(x)g(x).$$

Como $p(x)$ divide a los dos sumandos, divide también a la suma, $p(x) \mid g(x)$, que es la primera conclusión deseada.

Si $p(x)$ es irreducible y $p(x)$ no divide a $f(x)$, entonces $p(x)$ y $f(x)$ son primos entre sí y aplicamos lo anterior para obtener que $p(x) \mid g(x)$. □

De gran interés, por sus aplicaciones a la teoría de codificación, son los anillos de polinomios $F[x]$ cuando el cuerpo F tiene dos elementos, $\mathbb{Z}_2[x]$, así como los casos en los que card (F) es 4, 8 y 16.

Para toda la teoría de la divisibilidad, que hemos iniciado en esta sección, es indispensable explicitar el anillo sobre el cual se trabaja. Por ejemplo, el polinomio $x^2 - 2$ es irreducible en $\mathbb{Q}[x]$, pero se descompone en factores en $\mathbb{R}[x]$, en la forma $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$. De igual manera, $x^2 + 1$ es irreducible en $\mathbb{R}[x]$, pero no en $\mathbb{C}[x]$, ya que $x^2 + 1 = (x - i)(x + i)$.

También, en $\mathbb{Z}_2[x]$ se tiene que $x^2+1 = (x+1)(x+1)$ debido a que $1+1 = 0$ en $\mathbb{Z}_2$.

4.3. Cuerpos de fracciones: los racionales

Supongamos que $(A, +, .)$ es un dominio de integridad (como, por ejemplo, $\mathbb{Z}$ o $F[x]$).

Definimos sobre $A \times (A \setminus \{0\})$ la siguiente RBE:

$$(a,b) \sim (c,d) \Longleftrightarrow ad = bc. \tag{4.5}$$

Es evidente que $\sim$ es reflexiva y simétrica. Probaremos que es transitiva. Para ello, supongamos que $(a,b) \sim (c,d)$ y que $(c,d) \sim (e,f)$. Usando (4.5),

$$ad = bc \tag{4.6}$$

y

$$cf = de. \tag{4.7}$$

Si multiplicamos (4.6) por f y (4.7) por b, e igualando, obtenemos $adf = bde$ y, dado que $d \neq 0$ y A es dominio de integridad, $af = be$, o, lo que es lo mismo, $(a,b) \sim (e,f)$.

Ahora, definimos dos operaciones en $A \times (A \setminus \{0\})$, una suma y un producto, que están motivados por las operaciones con fracciones de la matemática elemental, sin más que interpretar la pareja (a,b) como la **fracción** $\frac{a}{b}$:

$$\begin{aligned} (a,b) + (c,d) &= (ad + bc, bd)\ ; \\ (a,b).(c,d) &= (ac, bd)\ . \end{aligned}$$

Es muy fácil probar que estas operaciones son cerradas en $A \times (A \setminus \{0\})$. Bastante más dificultad entraña verificar que ambas operaciones son compatibles con la RBE.

Para ello, supongamos que tenemos cuatro pares satisfaciendo

$$(a,b) \sim (a',b') \quad \text{y} \quad (c,d) \sim (c',d'),$$

o, lo que es equivalente, por (4.5),

$$ab' = ba' \tag{4.8}$$

y

$$cd' = dc'. \tag{4.9}$$

Multiplicando miembro a miembro las igualdades (4.8) y (4.9), tenemos que $ab'cd' = ba'dc'$, es decir, $(ac, bd) \sim (a'c', b'd')$, lo cual prueba la compatibilidad del producto respecto a la RBE.

Para probar la compatibilidad de la suma respecto a $\sim$ utilizaremos la propiedad transitiva de las relaciones de equivalencia. Más concretamente, debemos ver que si

$$(a,b) \sim (a',b') \quad \text{y} \quad (c,d) \sim (c',d'), \tag{4.10}$$

entonces

$$(a,b) + (c,d) \sim (a',b') + (c,d) \sim (a',b') + (c',d'). \tag{4.11}$$

Probaremos la primera relación en (4.11) (la segunda se demuestra de igual forma), es decir, debemos verificar que

$$(ad + bc)\, b'd = bd\,(a'd + b'c)$$

o, lo que es lo mismo,

$$ad^2b' = bd^2a'.$$

Pues bien, dado que $d^2 \neq 0$, esto equivale a $ab' = ba'$, igualdad que se cumple por la hipótesis (4.10).

Estamos en condiciones de probar que las operaciones que acabamos de definir sobre el conjunto cociente de $A \times (A \setminus \{0\})$ por la RBE $\sim$ proporcionan un cuerpo. Cada elemento del cuerpo es una clase de equivalencia $[(a,b)]$, que se denotará simplemente como una fracción $\dfrac{a}{b}$ de alguno de sus representantes (omitiendo el símbolo de clase). Por lo tanto, $\dfrac{a}{b} = \dfrac{c}{d}$ significa que $[(a,b)] = [(c,d)]$, lo cual es equivalente a $ad = bc$.

Teorema 4.3. *$([A \times A \setminus \{0\}] / \sim, +, .)$ es un cuerpo (llamado **cuerpo de fracciones** del dominio de integridad $(A, +, .)$).*

Demostración. Llamaremos K al cociente $[A \times A \setminus \{0\}] / \sim$. Empezaremos por demostrar que $(K, +, .)$ es un anillo conmutativo unitario.

Las propiedades asociativa, conmutativa y existencia de elemento neutro para la suma en $A \times A \setminus \{0\}$ son heredadas por el cociente. También son heredadas las propiedades asociativa, conmutativa y existencia de elemento neutro para el producto, así como la distributividad del producto respec-

to de la suma. Sin embargo, hay elementos en $A \times A \setminus \{0\}$ que carecen de opuesto (por ejemplo, si $A = \mathbb{Z}$, el elemento $(0, 2)$ no tiene opuesto, pues $(0, 2) + (x, y) = (2x, 2y) \neq (0, 1)$ cualquiera que sea el par (x, y)).

Para probar que $(K, +, .)$ es anillo unitario bastará comprobar la existencia de opuestos. En efecto, dado $\frac{a}{b} \in K$ arbitrario, se tiene

$$\frac{a}{b} + \frac{(-a)}{b} = [(a, b) + (-a, b)] = [\left(0, b^2\right)] = [(0, 1)] = 0.$$

Para terminar, veremos que para $\frac{a}{b} \neq 0$, existe $\frac{x}{y} \in K$ tal que $\frac{a}{b} \cdot \frac{x}{y} = 1$ (nótese que si $\frac{a}{b} \neq 0$, entonces $a \neq 0$). La ecuación

$$\frac{a}{b} \cdot \frac{x}{y} = 1$$

es equivalente a

$$\frac{ax}{by} = \frac{1}{1},$$

que es, a su vez, equivalente a

$$ax = by. \tag{4.12}$$

La condición (4.12) significa que $\frac{x}{y} = \frac{b}{a}$ es el elemento inverso de $\frac{a}{b}$. □

En particular, el cuerpo de fracciones de $(\mathbb{Z}, +, .)$ es, por definición, el **cuerpo de los números racionales** $(\mathbb{Q}, +, .)$, cuyos elementos son clases de equivalencia de fracciones (véase Figura 4.1).

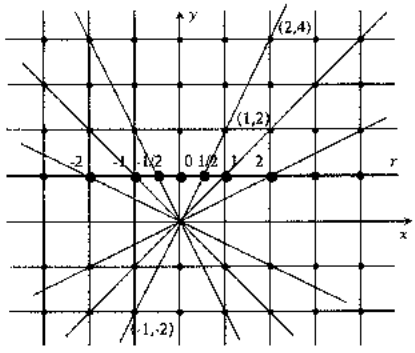

Figura 4.1. *Cada clase de equivalencia en $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ está formada por aquellos pares que pertenecen a una misma recta por el origen. Cada una de dichas rectas (que no pueden ser horizontales), intersectan a la recta r, paralela al eje OX trazada por $(0, 1)$, en un solo punto, que representa al número racional correspondiente.*

La prueba anterior permite observar que el opuesto de $\frac{a}{b}$ es $\frac{(-a)}{b}$ mientras que el inverso de $\frac{a}{b} \neq 0$ es $\frac{b}{a}$. Existe un monomorfismo de anillos natural $E : \mathbb{Z} \longrightarrow \mathbb{Q}$ definido por $E(x) = \frac{x}{1}$. En este sentido debe entenderse la afirmación $\mathbb{Z} \subset \mathbb{Q}$.

De forma análoga, el cuerpo de fracciones del anillo $\mathbb{Q}[x]$ de los polinomios con coeficientes racionales es el **cuerpo de las fracciones algebraicas** (o polinómicas), que denotaremos por $\mathbb{Q}(x)$. Sus representantes son fracciones $\frac{p(x)}{q(x)}$, con $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$, $q(x)$ no nulo. También son de interés los cuerpos de fracciones polinómicas con coeficientes en un cuerpo finito, como por ejemplo, $\mathbb{Z}_p(x)$ para $p \in \mathbb{N}$ y p primo.

4.4. Cuerpos ordenados

Al ampliar sucesivamente los conjuntos numéricos, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$, nos hemos centrado en las operaciones suma y producto, que son cada vez más ricas en propiedades. Por ejemplo, tienen solución en $\mathbb{Z}$ las ecuaciones de la forma $a + x = b$ mientras que también tienen solución en $\mathbb{Q}$ las de la forma $ax + b = c$. En otras palabras, en cada extensión del sistema numérico ganamos propiedades algebraicas.

Pero tan importantes como las propiedades algebraicas son las propiedades del orden. El orden total de $(\mathbb{N}, \leq)$ se extendió al dominio de integridad $\mathbb{Z}$ de manera compatible con la suma y el producto. La compatibilidad (leyes de monotonía) resultó como consecuencia de determinar el conjunto de números enteros positivos, cerrado bajo suma y producto, y con tricotomía. En general, si en un dominio de integridad se establece un conjunto que sea cerrado bajo suma y producto y que cumpla con la tricotomía, entonces queda determinado un orden total compatible con las operaciones.

Definición 4.9. *Sea $(A, +, .)$ un dominio de integridad. Un subconjunto de A, A^+, se dice que es un conjunto de* ***elementos positivos*** *si es cerrado bajo ambas operaciones y, además, para cada $a \in A$ se cumple una, y sólo una, de las siguientes afirmaciones: $a \in A^+$, $-a \in A^+$, o bien $a = 0$.*

Teorema 4.4. *Sea $(A, +, .)$ un dominio de integridad y $A^+ \subset A$ un conjunto de elementos positivos. Para $a, b \in A$, la relación $\leq$ definida por*

$$a \leq b \Longleftrightarrow b - a \in A^+ \cup \{0\},$$

es un orden total (si $b - a$ es positivo escribimos $a < b$). Con el orden así definido se verifica que

$$A^+ = \{a \in A \mid a > 0\}.$$

Este orden es compatible con las operaciones, es decir, se cumplen

$$a < b \Longrightarrow a + c < b + c$$

y

$$(a < b \wedge c \in A^+) \Longrightarrow ac < bc,$$

cualesquiera sean $a, b, c \in A$. *Resumimos todo lo anterior diciendo que* $(A, +, ., \leq)$ *es un* ***dominio ordenado***.

Demostración. Debemos verificar las propiedades de la relación de orden y las de compatibilidad.

La propiedad reflexiva se cumple trivialmente.

Para demostrar que $\leq$ es transitiva, supongamos que $a \leq b$ y que $b \leq c$. Si $a = b$ o $b = c$, se tiene $a \leq c$. Podemos, pues, suponer que $b - a$ y $c - b$ son positivos. Entonces, $c - a = (c - b) + (b - a)$ es positivo, por ser A^+ cerrado bajo suma, lo que implica que $a \leq c$.

Supongamos ahora que $a \neq b$ y que se verifica $a \leq b$ y $b \leq a$. Razonando como antes, sabemos que $b - a \in A^+$ y que $a - b \in A^+$, lo cual es imposible por tricotomía. Se cumple, por lo tanto, la propiedad antisimétrica.

Finalmente, $b - a$ es positivo, o cero, o bien $a - b$ es positivo, por lo que se cumple una, y sólo una de las siguientes proposiciones: $a < b$, $a = b$ o bien $b < a$ (tricotomía del orden sobre A). Por lo tanto, $(A, \leq)$ es un orden total. Además, $a = a - 0 \in A^+$ si, y sólo si, $a > 0$.

Por otra parte, $(b + c) - (a + c) = b - a$ es positivo si, y sólo si, lo es $b - a$. Por lo tanto,

$$a < b \Longleftrightarrow a + c < b + c,$$

verificándose la compatibilidad con la suma. Con respecto al producto, si $a < b$ y $c \in A^+$, como $b - a \in A^+$ y A^+ es cerrado bajo producto, se obtiene $bc - ac = (b - a)c \in A^+$, lo que equivale a afirmar que $ac < bc$. □

Del teorema se deducen algunas propiedades familiares de la aritmética, que son válidas en cualquier dominio ordenado A:

(*i*) Si $a \leq b$ y $c \leq d$, entonces $a + c \leq b + d$.
La demostración es inmediata.

(*ii*) Si $a < b$ y $c \leq d$, entonces $a + c < b + d$.
En efecto, por compatibilidad con la suma se puede escribir

$$a + c < b + c \leq b + d.$$

(*iii*) $ab > 0$ si, y sólo si, $a > 0$ y $b > 0$ o bien $a < 0$ y $b < 0$.

En efecto, si suponemos $ab > 0$, es imposible que $a = 0$ o $b = 0$ (dominio de integridad). Tampoco pueden tener signos diferentes, ya qué si, por ejemplo, $a > 0$ y $b < 0$, se tiene $ab < a0 = 0$, lo cual es inconsistente con $ab > 0$. De igual forma se prueba el recíproco.

(*iv*) $a^2 \geq 0$ cualquiera sea $a \in A$.
Inmediato, por (*iii*).

(*v*) $1 > 0$.
Consecuencia de que $1^2 = 1$, usando (*iv*) y el hecho de que $1 \neq 0$ en un dominio de integridad.

(*vi*) Si $a \leq b$ y $c > 0$, entonces $ac \leq bc$.

(*vii*) Si $a \leq b$ y $c < 0$, entonces $ac \geq bc$.

Nos ocupamos a continuación de la ordenación del cuerpo (dominio de integridad) de los números racionales. Sabemos que todo número racional es de la forma $\frac{a}{b}$, con a y b números enteros, $b \neq 0$.

Definición 4.10. *Un número racional* $\frac{a}{b}$ *es* ***positivo*** *si* $ab > 0$ *(como números enteros).*

Debemos ver que esta definición es independiente de representantes. En efecto, sea $\frac{a}{b} = \frac{c}{d}$, es decir, $ad = bc$, $b \neq 0 \neq d$, y supongamos que $ab > 0$. Entonces ambos números son positivos o negativos. Podemos asegurar que $c \neq 0$ (de lo contrario $a = 0$). Además, si c y d fuesen, positivo uno y negativo el otro, igual ocurriría con ad y bc, siendo esto imposible porque $ad = bc$. Por lo tanto, c y d son positivos o negativos simultáneamente y, en ambos casos, $cd > 0$.

De hecho, si $\frac{a}{b}$ es positivo, puede suponerse que a y b son enteros positivos (si los dos son negativos, se toman sus opuestos). Que la suma y el producto de dos racionales positivos es también positivo se obtiene como consecuencia de que Z^+ es cerrado bajo suma y producto. La tricotomía es consecuencia de que para cualquier racional $\frac{a}{b}$, el entero ab cumple una, y sólo una, de las siguientes proposiciones: $ab > 0$, $ab = 0$, o bien $ab < 0$. El opuesto de un racional positivo es negativo.

Por el Teorema 4.4, la relación de orden en $\mathbb{Q}$ está bien definida a partir del conjunto de los racionales positivos, $\mathbb{Q}^+ : x \leq y$ cuando $y - x \in \mathbb{Q}^+ \cup \{0\}$.

Corolario 4.3. $(\mathbb{Q}, +, ., \leq)$ *es un* ***cuerpo ordenado****, es decir,* $(\mathbb{Q}, +, .)$ *es un cuerpo y* $\leq$ *es un orden total compatible con la suma y el producto. Además, la aplicación que asocia a cada número entero* a *el número racional* $\frac{a}{1}$ *es un monomorfismo de anillos unitarios de* $\mathbb{Z}$ *en* $\mathbb{Q}$ *que preserva el orden.*

Una propiedad que caracteriza a $\mathbb{Q}$ es que es el mínimo cuerpo ordenado, en un sentido que precisaremos a continuación.

Dado un cuerpo ordenado cualquiera, $(K, +, ., \leq)$, denotando por 0_K y 1_K los neutros aditivo y multiplicativo de K ($1_K \neq 0_K$), existe un monomorfismo natural $E : \mathbb{Q} \longrightarrow K$ que se define por etapas (los detalles se dejan a cargo del lector):

$$E(0) = 0_K;$$

$$E(1) = 1_K;$$

$$E(n+1) = E(n) + 1_K, \quad \text{si } n \in \mathbb{N};$$

$$E(-n) = -E(n), \quad \text{si } n \in \mathbb{N};$$

$$E\left(\frac{m}{n}\right) = \frac{E(m)}{E(n)}, \quad \text{si } \frac{m}{n} \in \mathbb{Q}.$$

Este monomorfismo de $\mathbb{Q}$ en K preserva suma, producto y orden, por lo que $E(\mathbb{Q}) \subset K$ es una copia exacta del cuerpo ordenado $\mathbb{Q}$. Se suele denotar también con $\frac{m}{n}$ un **elemento racional de** K cuando, en realidad, es el elemento $E\left(\frac{m}{n}\right)$. En este sentido, todo cuerpo ordenado contiene al cuerpo de los racionales y, por lo tanto, $\mathbb{Q}$ es el mínimo cuerpo ordenado.

Por otro lado, en cada cuerpo ordenado $(K, +, ., \leq)$ existe una aplicación de K en K que puede ser usada para definir una distancia entre los elementos de K.

Definición 4.11. *Si $a \in K$, el **valor absoluto** de a es*

$$|a| = \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases}$$

Las propiedades del valor absoluto de los números racionales (que define, obviamente, una aplicación de $\mathbb{Q}$ en el conjunto de los racionales no negativos $\mathbb{Q}_+$) son conocidas de la matemática elemental. El lector probará sin dificultad que las mismas son válidas en cualquier cuerpo ordenado K (a y b representan elementos arbitrarios del cuerpo):

(*i*) $|a| \geq 0$ y $|a| = 0$ si, y sólo si, $a = 0$.

(*ii*) $|-a| = |a|$.

(*iii*) $a \leq |a|$ y $-a \leq |a|$.

(*iv*) $|a + b| \leq |a| + |b|$ (**propiedad triangular**).

(*v*) $|a| - |b| \leq |a - b|$, que mide la **distancia** entre a y b (usar (*iv*)).

(*vi*) $|ab| = |a|\,|b|$.

(*vii*) $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$, si $b \neq 0$.

(*viii*) Si b es positivo, entonces $|a| < b$ si, y sólo si, $-b < a < b$.

Desde el punto de vista algebraico, la extensión de $\mathbb{Z}$ a $\mathbb{Q}$ comporta una ganancia: toda ecuación de la forma $ax = b$, con $a \neq 0, b \in \mathbb{Q}$, tiene solución única en $\mathbb{Q}$ (por ser cuerpo). El orden extendido $\leq$ sigue siendo un orden total. Sin embargo, una diferencia importante respecto de $\mathbb{Z}$ surge de la combinación

de ambas cosas, ser cuerpo y ser ordenado: entre dos números racionales existe otro racional (y por lo tanto infinitos). Por ejemplo, si $a, b \in \mathbb{Q}$ y $a < b$, entonces $(a+b)/2 \in \mathbb{Q}$ (por propiedades de cuerpo) y se tiene que $a < (a+b)/2 < b$ (usando propiedades del orden).

Otra importante propiedad del orden en $\mathbb{Q}$ (que no se cumple en cualquier cuerpo ordenado) es que $\mathbb{Z}$ abarca la totalidad de $\mathbb{Q}$ en el sentido de que todo racional está entre dos enteros consecutivos. Es decir, si $a \in \mathbb{Q}$, entonces existe $a_0 \in \mathbb{Z}$ tal que

$$a_0 \leq a < a_0 + 1 \tag{4.13}$$

(no hay racionales fuera del alcance de los números enteros). Ésta es conocida como la propiedad arquimediana y admite varias formulaciones equivalentes. Tomaremos como definición una forma con inversos que será particularmente útil para convergencia de sucesiones.

Definición 4.12. *Un cuerpo ordenado K es* ***arquimediano*** *si, y sólo si, para cada $e \in K^+$ existe algún $n \in \mathbb{N}$ tal que $\frac{1}{n} < e$.*

Obsérvese que puede sustituirse «<» por «$\leq$» en esta definición. La propiedad arquimediana también suele usarse en la forma de negación: «no existe un elemento positivo menor que $\frac{1}{n}$ para todo $n \in \mathbb{N}$».

Veremos ahora que se cumple la equivalencia afirmada en (4.13). En efecto, suponiendo que K es un cuerpo ordenado arquimediano, y dado un elemento $a \in K$ arbitrario, el elemento $a_0 \in \mathbb{Z}$ definido (gracias al buen orden de $\mathbb{N}$) como

$$a_0 = \begin{cases} \min\{n \in \mathbb{N} \mid a < n\} - 1, & \text{si } a \in K^+ \\ 0, & \text{si } a = 0 \\ -\min\{n \in \mathbb{N} \mid -a \leq n\}, & \text{si } a \in K^- \end{cases},$$

satisface (4.13). Recíprocamente, dado $e > 0$, si existe $a_0 \in \mathbb{Z}$ tal que $a_0 \leq e^{-1} < a_0 + 1$, entonces $n := a_0 + 1 \in \mathbb{N}$ y satisface $\frac{1}{n} < e$.

Proposición 4.5. *$(\mathbb{Q}, +, \cdot, \leq)$ es arquimediano.*

Demostración. Si $e \in \mathbb{Q}^+$ existe $a \in \mathbb{Q}$ tal que $0 < a < e$. Pero todo racional positivo admite una representación $a = \frac{m}{n}$ con $m, n \in \mathbb{Z}^+$. Entonces, $\frac{1}{n} \leq \frac{m}{n} = a < e$. □

Definición 4.13. *Supongamos que $\{a_n\}$ es una sucesión contenida en un cuerpo ordenado K. Decimos que $\{a_n\}$* ***converge*** *(en K) a un elemento $a \in K$ cuando, para todo $\varepsilon \in K^+$, $|a_n - a| < \varepsilon$ para todo n posterior a un cierto $n_0 \in \mathbb{N}$ (diremos, para abreviar, que $|a_n - a| < \varepsilon$ finalmente). Se escribe entonces $\lim_{n\to\infty} a_n = a$.*

En particular, $\left\{\frac{1}{n}\right\}$ es una sucesión contenida en $\mathbb{Q}$ y, por la Proposición 4.5, dado $e \in \mathbb{Q}^+$ existe $n_0 \in \mathbb{N}$ tal que $\frac{1}{n_0} < e$. Entonces, si $n \geq n_0$, se tiene también $\frac{1}{n} < e$, por lo que $\lim_{n\to\infty} \frac{1}{n} = 0$ en $\mathbb{Q}$. Tal proposición se despacha en los libros de matemática elemental afirmando que «es evidente, al ser $\frac{1}{n}$ arbitrariamente pequeño», cuando, en realidad, es equivalente a la propiedad arquimediana de $(\mathbb{Q}, +, \cdot, \leq)$ (siendo falsa, por ejemplo, para el cuerpo no arquimediano del Problema 5.10). Una vez más, lo que se presenta como evidente en matemática elemental oculta una complejidad que debe ser desvelada.

Terminamos esta sección con algunas consideraciones sobre la representación geométrica de $\mathbb{Q}$.

La clave de la construcción con regla y compás de $\mathbb{Q}$ a partir de $\mathbb{Z}^2$ es el trazado de una recta paralela a una dada y que pasa por un punto dado (véanse las Figuras 4.2 y 4.3).

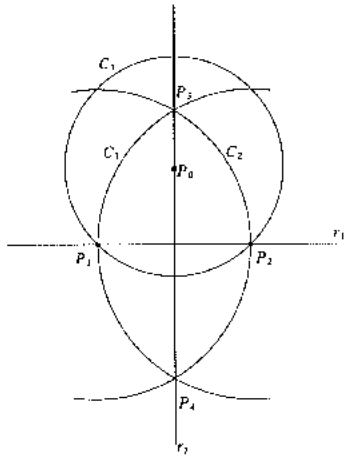

Figura 4.2. *Construcción de una recta perpendicular a r_1 y que pasa por P_0 no perteneciente a r_1: Se traza una circunferencia con centro en P_0 y radio suficientemente grande, C_1, cuyas intersecciones con r_1 son P_1 y P_2; se trazan las circunferencias C_2 y C_3 cuyos centros son P_1 y P_2 y cuyo radio es la distancia entre P_1 y P_2; las intersecciones de C_2 y C_3 son P_3 y P_4, que determinan la recta buscada, r_2.*

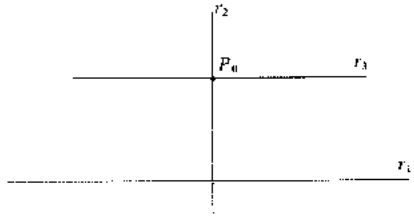

Figura 4.3. *Construcción de una recta paralela a r_1 y que pasa por P_0 no perteneciente a r_1: se traza la recta perpendicular a r_1 y que pasa por P_0, r_2; la recta r_3, perpendicular a r_2 en $P_0 \in r_2$ es la recta buscada.*

Para la construcción del racional $\frac{p}{q}$, $(p,q) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, que se ejemplifica en la Figura 4.4, construimos la recta por $(0,p)$ paralela a la que determinan $(1, 0)$ y $(0,q)$. Su intersección con el eje de abscisas es $\left(\frac{p}{q}, 0\right)$ por semejanza de los triángulos rectángulos que forman dichas rectas con los ejes coordenados.

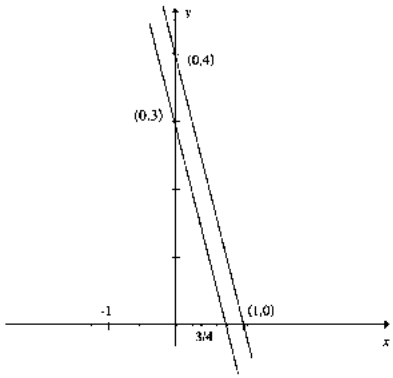

Figura 4.4. *Construcción geométrica de 3/4: la recta por (0, 3) paralela a la determinada por (0, 4) y (1, 0) determina un punto, x, del eje OX. Por semejanza de triángulos,* $\frac{x}{3} = \frac{1}{4}$, *es decir* $x = \frac{3}{4}$.

Luego se construye de nuevo $\mathbb{Q}$ sobre el otro eje, trazándose finalmente rectas perpendiculares a los ejes en los puntos construidos sobre los mismos (recuérdese la Figura 3.6). El conjunto de puntos de las intersecciones es $\mathbb{Q}^2$.

Representando todos los números racionales sobre la recta graduada, ¿la cubrimos enteramente? Veremos que la respuesta a esta pregunta es negativa.

La diagonal de un cuadrado de lado 1 mide $\sqrt{2}$ y puede trasladarse dicha longitud (usando el compás) a un punto de la recta graduada, ubicado entre los números 1 y 2. Probaremos a continuación que $\sqrt{2}$ no es un número racional.

En efecto, si fuera $\sqrt{2} = \frac{a}{b}$, con a y b números naturales primos entre sí, elevando al cuadrado se tendría

$$2b^2 = a^2. \tag{4.14}$$

Esta última igualdad permite afirmar que $2 \mid a^2$ y, teniendo en cuenta que 2 es un número primo, $2 \mid a$, es decir, $a = 2p$ para cierto $p \in \mathbb{N}$. Sustituyendo en la igualdad (4.14) queda

$$b^2 = 2p^2,$$

por lo que también $2 \mid b$. Pero esto es absurdo, porque hemos supuesto que a y b son primos entre sí.

Los racionales dejan «agujeros» en la recta. En el próximo capítulo completaremos la recta introduciendo los números reales.

4.5. Problemas

Problema 4.1. Sobre el conjunto E de los números enteros pares se considera la suma ordinaria y se define un producto $a \star b = \dfrac{ab}{2}$. Analice la estructura $(E, +, \star)$.

Problema 4.2. Estudie las propiedades de la estructura algebraica $(\mathbb{N}, \ominus, \triangle)$, donde $m \oplus n = 3m + 2$ y $m \triangle n = 4mn$.

Problema 4.3. Si $(G, +)$ es un grupo conmutativo con elemento neutro 0, y se define una segunda operación $x \triangle y = 0$ cualesquiera que sean x e y en G, ¿qué estructura tiene $(G, +, \triangle)$?

Problema 4.4. Se pide lo mismo cuando la segunda operación sobre G es $x \boxdot y = y$.

Problema 4.5. Dados dos anillos A y B, cuyas operaciones suma y producto denotamos de la forma habitual, consideramos sobre su producto cartesiano $A \times B$ la suma y el producto por componentes. Analice esta estructura algebraica.

Problema 4.6. Considérense las matrices 2×2 cuyos elementos son números enteros, dotadas de la suma y del producto de matrices ya conocidos de la matemática elemental. Analice las propiedades algebraicas de esa tripleta, clasificándola.

Problema 4.7. En el conjunto de las partes de un conjunto no vacío se consideran la intersección y la diferencia simétrica (véase Problema 1.8). Pruebe que es un anillo conmutativo (llamado ***anillo de Boole***).

Problema 4.8. En $\mathbb{Z}$ se definen las siguientes operaciones:

$$a \oplus b = a + b - 6$$

$$a \otimes b = ab + \mu(a + b) + 42$$

donde μ es un número entero fijo.

a) Demuestre que $(\mathbb{Z}, \oplus)$ es un grupo abeliano.
b) ¿Qué valores de μ hacen que $(\mathbb{Z}, \oplus, \otimes)$ sea un anillo?
c) ¿Es dicho anillo un dominio de integridad?

Problema 4.9. Resuelva el siguiente sistema en el cuerpo de las clases de congruencia módulo 7:

$$\left.\begin{array}{rcrcl} \overline{5}x & + & \overline{2}y & = & \overline{3} \\ \overline{4}x & + & \overline{1}y & = & \overline{6} \end{array}\right\}.$$

Problema 4.10. Resuelva en $\mathbb{Z}_{13}$ y en $\mathbb{Q}$ el siguiente sistema de ecuaciones:

$$\left.\begin{array}{rcrcrcl} \overline{3}x & + & & + & z & = & \overline{0} \\ x & + & \overline{4}y & - & z & = & \overline{0} \end{array}\right\}.$$

Problema 4.11. Resuelva en $\mathbb{Z}_5$ y en $\mathbb{Z}_7$ el siguiente sistema de ecuaciones:

$$\left.\begin{array}{rcrcrcl} \overline{3}x & + & y & + & \overline{2}z & = & \overline{1} \\ x & + & \overline{2}y & + & \overline{3}z & = & \overline{1} \\ \overline{4}x & + & \overline{3}y & + & \overline{2}z & = & \overline{1} \end{array}\right\}.$$

Problema 4.12. Resuelva en $\mathbb{Z}$, $\mathbb{Z}_9$ (sólo anillos), $\mathbb{Z}_{11}$ y $\mathbb{Q}$ (cuerpos) el siguiente sistema de ecuaciones:

$$\left.\begin{array}{rcrcrcrcl} x_1 & + & \overline{3}x_2 & - & x_3 & + & x_4 & = & \overline{1} \\ -\overline{2}x_1 & + & x_2 & + & \overline{2}x_3 & & & = & \overline{7} \\ & & x_2 & & & - & x_4 & = & \overline{0} \end{array}\right\}.$$

Problema 4.13. Demuestre que un sistema homogéneo de ecuaciones lineales con coeficientes en un cuerpo, que tiene más incógnitas que ecuaciones, es indeterminado.

Problema 4.14.* Considérese el anillo de polinomios con coeficientes enteros $\mathbb{Z}[x]$ (sustituya F por $\mathbb{Z}$ en la Definición 4.6). Se pide:

a) Pruebe que $(\mathbb{Z}[x], +, .)$ es un dominio de integridad.
b) Defina sobre $\mathbb{Z}[x]$ una RBE compatible con la suma y con el producto.
c) Tras comprobar que los elementos de $\mathbb{Z}[x]$ tales que la potencia de mayor grado tiene coeficiente positivo forman un conjunto de elementos positivos en $\mathbb{Z}[x]$, con orden asociado $\leq$, pruebe que $(\mathbb{Z}[x], +, ., \leq)$ es un dominio de integridad ordenado. Ese orden total sobre $\mathbb{Z}[x]$ se llama *lexicográfico* porque recuerda a la ordenación de las palabras en el diccionario.

Problema 4.15.* Sabiendo que $\mathbb{Q}[x]$ es numerable (Problema 2.23 *c*), determine el cardinal de su cuerpo de fracciones $\mathbb{Q}(x)$ suponiendo que se cumple el axioma de elección. (Sugerencia: Utilice la Proposición 2.10 y el Problema 2.25 *b*.)

Problema 4.16. Demuestre que sólo pueden definirse cuatro aplicaciones de $\mathbb{Z}_2$ en $\mathbb{Z}_2$ y que, dada una cualquiera de ellas, f, existe un polinomio $p(x) \in \mathbb{Z}_2[x]$ tal que la imagen de un elemento $\alpha \in \mathbb{Z}_2$, $f(\alpha)$, se obtiene sustituyendo x por α en $p(x)$. ¿Es único dicho polinomio?

Problema 4.17. Sea A un conjunto arbitrario de 53 números naturales. Demuestre que hay al menos dos elementos de A cuya diferencia es un múltiplo de 52. Ayuda: Utilice el principio del palomar (pág. 51).

Problema 4.18. Halle el menor subanillo de $\mathbb{Q}$ (subconjunto que es anillo con las operaciones inducidas) que contiene a $\frac{1}{5}$ y a $\frac{1}{7}$.

Problema 4.19. Pruebe que $\sqrt{n}$ no es un número racional cuando el número natural n no es un cuadrado perfecto.

Problema 4.20. Sobre $\mathbb{Q}^2$ se consideran la suma y el producto por componentes, es decir, $(x,y)+(z,t)=(x+z,y+t)$ y $(x,y)\times(z,t)=(xz,yt)$.

a) Compruebe que se trata de un anillo conmutativo y unitario, pero no un dominio de integridad.

b) Pruebe que $I=\{(x,y)\in\mathbb{Q}^2 \mid x=0\}$ es un ideal en el anillo anterior, y demuestre que $\mathbb{Q}^2/I$ es isomorfo a $\mathbb{Q}$.

Problema 4.21.* Demuestre que no puede definirse un orden sobre el cuerpo de las clases de congruencia módulo 3 de tal forma que la estructura resultante sea un cuerpo ordenado. Demuestre que, de hecho, ningún cuerpo finito puede ser un cuerpo ordenado.

Problema 4.22. Pruebe que la composición de homomorfismos de cierta clase pertenece a la misma clase y que dos estructuras algebraicas, ambas dotadas con dos operaciones, isomorfas (es decir, entre las que existe un isomorfismo) poseen las mismas propiedades algebraicas.

Problema 4.23. Demuestre que, si $\sim$ es una RBE compatible con las operaciones de un anillo $(A,+,.)$, entonces la aplicación que asocia a cada elemento de A su clase de equivalencia es un epimorfismo.

Problema 4.24. Supongamos que $(A,+,.)$ y $(\overline{A},+,.)$ son anillos y que A' y $\overline{A}'$ son subanillos de A y de $\overline{A}$, respectivamente. Pruebe que, si f es un homomorfismo de A en $\overline{A}$, entonces $f(A')$ y $f^{-1}(\overline{A}')$ son subanillos. Deduzca de aquí que $\ker f$ es un ideal en A, suponiendo que $(A,+,.)$ es conmutativo. Demuestre también que f es un monomorfismo si, y sólo si, $\ker f$ es singular.

Problema 4.25.* Sea $(K,+,.)$ un cuerpo y sea $a\in K$ tal que no existe un $x\in K$ satisfaciendo $x^2=a$ (en cuyo caso se dice que a carece de raíz cuadrada en K). Consideramos sobre K^2 la suma componente a componente y un producto $\triangle$ tal que

$$(x,y)\triangle(z,w)=(xz+ayw,yz+xw).$$

Demuestre que $(K^2,+,\triangle)$ es un cuerpo, que existe un monomorfismo que asocia a $a\in K$ el par ordenado $(a,0)\in K^2$, y que $(a,0)$ tiene raíz cuadrada en K^2 (esta misma construcción permite construir el cuerpo de los complejos a partir del cuerpo de los reales, tomando $a=-1$).

Problema 4.26. Demuestre que la intersección de una familia de subcuerpos de un cuerpo es también un subcuerpo.

Problema 4.27. Demuestre que si una sucesión $\{a_n\}$ converge en un cuerpo ordenado K, entonces $\lim\limits_{n\to\infty} a_n$ es único.

Problema 4.28. Demuestre que un cuerpo ordenado K es arquimediano si, y sólo si, para cada elemento $b \in K^+$ existe $n \in \mathbb{N}$ tal que $b < n$.

Problema 4.29. Demuestre que en cualquier cuerpo no arquimediano K la sucesión de los números naturales $\{n\}$ está acotada superiormente.

CAPÍTULO 5

EL CUERPO DE LOS NÚMEROS REALES

Es difícil precisar cuándo, y dónde, aparecen los números reales por vez primera. La teoría de las magnitudes de Eudoxio, expuesta en el libro V de los *Elementos* de Euclides, puede considerarse un texto acerca de los reales no negativos. Para la mayor parte de los matemáticos griegos existían aquellas magnitudes (en particular, longitudes) que podían representarse mediante la regla y el compás, como $\sqrt{r}$, con $r \in \mathbb{Q}^+$ (véase Figura 5.1). Para la escuela pitagórica, ni siquiera eso: sólo admitían aquellas magnitudes que podían ser construidas mediante la regla y el cartabón, es decir, los números racionales. Como puede verse, la aritmética (antecedente del álgebra) y la geometría aparecían indisolublemente unidas en aquella época.

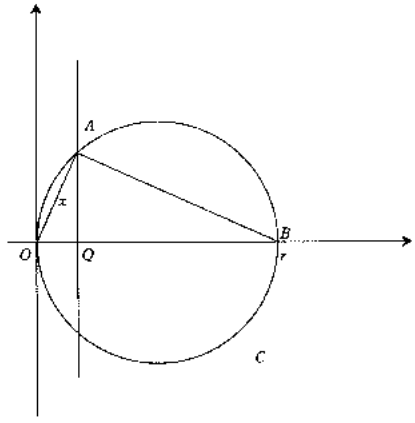

Figura 5.1. *Construcción de $\sqrt{r}$: El punto medio del segmento de extremos O y $B\,(r, 0)$ se toma como centro de una circunferencia, C, que pasa por O y B; el punto A es uno de los puntos de intersección de C con la recta perpendicular al eje de abscisas que pasa por $Q\,(1, 0)$; por ser semejantes los triángulos $\overset{\triangle}{AQO}$ y $\overset{\triangle}{BAO}$ (ángulos iguales) los lados correspondientes son proporcionales, por lo que, llamando x a la longitud del lado AO, se tiene $\frac{x}{1} = \frac{r}{x}$, es decir, $x^2 = r$.*

A mediados del siglo XIX los analistas alemanes experimentaron la necesidad de fundamentar rigurosamente su disciplina, introduciendo el cuerpo de los números reales a partir del cuerpo de los racionales. Hacia 1870 ya se conocían tres caminos que permiten efectuar dicha construcción:

(*a*) Identificar los números reales con los *desarrollos decimales infinitos*, eliminando los terminados en una sucesión de nueves (período 9) para evitar la doble representación de los racionales decimales (período 0). Pueden escribirse en la forma $a_0 + \sum_{n=1}^{\infty} a_n 10^{-n}$ con $a_0 \in \mathbb{Z}$, $a_i \in \{0, 1, \ldots, 8, 9\}$ para $i \in \mathbb{N}$ (idea desarrollada por Weierstrass).

(*b*) Recurrir a las llamadas *cortaduras* en $\mathbb{Q}$, que son particiones de dicho conjunto en dos subconjuntos tales que todos los elementos del primero de ellos son menores que todos los elementos del segundo (camino seguido por Dedekind).

(*c*) Considerar (como hicieron Cantor y Méray) el *anillo cociente* de cierto anillo de sucesiones de números racionales, cuyos elementos se llamarán sucesiones regulares, por un ideal adecuado del mismo, el formado por las sucesiones convergentes a 0, llamadas nulas. Éste es el enfoque que adoptaremos.

Primeramente se demuestra que $\mathbb{R}$ es un cuerpo ordenado y arquimediano, que son propiedades que comparte con $\mathbb{Q}$. A continuación se demuestran las propiedades de completitud que permiten afirmar que la representación de $\mathbb{R}$ sobre una recta graduada la llena por completo, a diferencia de la representación de $\mathbb{Q}$, que es «porosa». Tales propiedades de completitud permiten demostrar un resultado básico del análisis matemático (funciones reales de variable real), el Teorema de Bolzano, que establece que toda curva del plano (gráfica de una función continua) que tiene un extremo en el semiplano superior y el otro en el semiplano inferior corta al eje de abscisas (identificado con $\mathbb{R}$) en al menos un punto, por lo que dicho eje carecería de «agujeros».

5.1. Sucesiones regulares en $\mathbb{Q}$

Si se desea calcular el valor aproximado de $\sqrt{2}$ sin otra herramienta que los números racionales decimales parece razonable proceder como sigue:

1. Se busca, por tanteo, un par consecutivo de números naturales tales que el cuadrado del primero sea menor que 2, y el cuadrado del segundo sea mayor que 2. Tales números son 1 y 2.
2. De entre los elementos del conjunto de racionales decimales $\{1, 1.1, 1.2, \ldots, 1.9, 2\}$ (resultado de dividir el intervalo $[1, 2]$ en 10 partes iguales) se eligen los dos consecutivos cuyos cuadrados sean menor y mayor, respectivamente, que 2. Tales números son 1.4 (cuyo cuadrado vale 1.96) y 1.5 (cuyo cuadrado es 2.25).

Prosiguiendo, se definen por recursión dos sucesiones de racionales (decimales), una creciendo hacia $\sqrt{2}$, la otra decreciendo hacia ese mismo número.

Los primeros términos de tales sucesiones son $1 < 1.4 < 1.41 < 1.414 < 1.4142 < \ldots$ y $2 > 1.5 > 1.42 > 1.415 > 1.4143 > \ldots$

Nos proponemos definir un número real mediante ciertas sucesiones de racionales que lo «aproximan», de tal forma que las sucesiones anteriores serán dos representantes de la clase de un número real, que llamaremos $\sqrt{2}$.

Definición 5.1. *Una sucesión de números racionales $\{a_n\}$ se dice que es* ***acotada en*** $\mathbb{Q}$ *cuando existe $k \in \mathbb{Q}^+$ (cota de $\{a_n\}$) tal que $|a_n| \leq k$ para todo $n \in \mathbb{N}$.*

Se dice que $\{a_n\}$ es ***regular en*** $\mathbb{Q}$ *cuando, para cada $e \in \mathbb{Q}^+$, existe $n_e \in \mathbb{N}$ (dependiente de e) tal que $|a_n - a_m| < e$ cualesquiera que sean $n, m \geq n_e$. También expresaremos este hecho diciendo: $|a_n - a_m| < e$ finalmente.*

Se dice que $\{a_n\}$ es ***nula*** *cuando $\lim_{n\to\infty} a_n = 0$, es decir, para cada $e \in \mathbb{Q}^+$, $|a_n| < e$ finalmente.*

Las dos sucesiones anteriores que aproximan $\sqrt{2}$ son acotadas ($k = 2$ es una cota para ambas). También son regulares porque, si $n \leq m$, entonces $|a_n - a_m| < 10^{1-n}$, siendo 10^{1-n} arbitrariamente pequeño si se toma n suficientemente grande (porque $\mathbb{Q}$ es arquimediano). No son sucesiones nulas, puesto que satisfacen $|a_n| \geq 1$ para todo natural n. Tampoco son convergentes en $\mathbb{Q}$, como se verá en el Ejemplo 5.2 (note que $\sqrt{2} \notin \mathbb{Q}$).

Cualquier **sucesión constante** $\{a\}$ ($a_n = a \in \mathbb{Q}$ para todo $n \in \mathbb{N}$) es acotada, regular y convergente en $\mathbb{Q}$, pero la única sucesión constante que es nula es $\{0\}$.

Las sucesiones $\{1/n\}$, $\{-1/n\}$, $\{(-1)^n/n\}$, $\{2^{-n}\}$, $\{10^{-n}\}$ son ejemplos de sucesiones acotadas. También son nulas debido a que $\mathbb{Q}$ es arquimediano. Veremos a continuación que son regulares.

Proposición 5.1. *Dada una sucesión de racionales $\{a_n\}$, se cumple lo siguiente:*

(i) Si $\{a_n\}$ es convergente en $\mathbb{Q}$, también es regular (en particular, si es nula es regular).

(ii) Si $\{a_n\}$ es regular, también es acotada.

Demostración. (*i*) Supongamos que $\{a_n\}$ es convergente a $a \in \mathbb{Q}$. Tomando $n, m \geq n_{e/2}$, se tiene

$$|a_n - a_m| = |a_n - a + a - a_m| \leq |a_n - a| + |a - a_m| < e/2 + e/2 = e,$$

por lo que $\{a_n\}$ es regular.

(*ii*) Supongamos ahora que $\{a_n\}$ es regular y sea $n_1 \in \mathbb{N}$ tal que

$$|a_n - a_m| < 1$$

para todo par de números naturales $n, m \geq n_1$. Entonces, para cualquier $n \geq n_1$ se tiene que

$$|a_n| - |a_{n_1}| \leq |a_n - a_{n_1}| < 1,$$

de donde,

$$|a_n| < 1 + |a_{n_1}| . \tag{5.1}$$

Llamando

$$k^a = \max \{|a_1|, |a_2|, ..., |a_{n_1-1}|, 1 + |a_{n_1}|\},$$

y, usando (5.1), $|a_n| \leq k^a$ para todo $n \in \mathbb{N}$. Se concluye que $\{a_n\}$ es acotada. □

En lo que sigue de este capítulo denotaremos A al conjunto de todas las sucesiones regulares de números racionales y con I al subconjunto de todas las sucesiones nulas.

Proposición 5.2. *Si se definen la suma y el producto de sucesiones en A, término a término, es decir, $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ y $\{a_n\} \times \{b_n\} = \{a_n b_n\}$, entonces $(A, +, \times)$ es un anillo conmutativo y unitario. Además, $I \subset A$ es un ideal.*

Demostración. Empezaremos probando que la suma y el producto son operaciones cerradas en A. Sean $\{a_n\}$ y $\{b_n\}$ sucesiones regulares y sea e un racional positivo.

En el caso de la suma, sean $n^a_{e/2}$ y $n^b_{e/2}$ números naturales tales que $|a_n - a_m| < e/2$ si $n, m \geq n^a_{e/2}$ y, análogamente, $|b_n - b_m| < e/2$ si $n, m \geq n^b_{e/2}$. Entonces, para $n, m \geq \max \left\{n^a_{e/2}, n^b_{e/2}\right\}$, se tiene

$$\begin{aligned} |(a_n + b_n) - (a_m + b_m)| &\leq |a_n - a_m| + |b_n - b_m| \\ &< e/2 + e/2 = e. \end{aligned}$$

En consecuencia, $\{a_n + b_n\}$ es una sucesión regular.

Para el producto, empezaremos observando que

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_n b_m + a_n b_m - a_m b_m| \\ &\leq |a_n| |b_n - b_m| + |b_m| |a_n - a_m| . \end{aligned}$$

Como $\{a_n\}$ y $\{b_n\}$ son sucesiones acotadas (según Proposición 5.1), existen dos racionales positivos k^a y k^b (cotas para $\{a_n\}$ y $\{b_n\}$, respectivamente) tales que $|a_n| \leq k^a$ y $|b_n| \leq k^b$ para todo $n \in \mathbb{N}$. Si se toman $e_1 = e/(2k^a)$ y $e_2 = e/(2k^b)$, existen números naturales n_{e_1} y n_{e_2} tales que $|b_n - b_m| < e_1$ si $n, m \geq n_{e_1}$, y $|a_n - a_m| < e_2$ si $n, m \geq n_{e_2}$. Tomando $n, m \geq \max \{n_{e_1}, n_{e_2}\}$, se tiene

$$\begin{aligned} |a_n b_n - a_m b_m| &\leq |a_n| |b_n - b_m| + |b_m| |a_n - a_m| \\ &< k^a e_1 + k^b e_2 = e/2 + e/2 = e. \end{aligned}$$

Por lo tanto, $\{a_n b_n\}$ es también una sucesión regular.

Las propiedades algebraicas del anillo de sucesiones se deducen inmediatamente a partir del hecho de que $\mathbb{Q}$ es un cuerpo. Así, por ejemplo, las

sucesiones constantes $\{0\}$ y $\{1\}$ son los elementos neutros para ambas operaciones, y $\{-a_n\} = \{-1\}\{a_n\} \in A$ es la sucesión opuesta de $\{a_n\}$.

Terminaremos probando que I es un ideal en $(A, +, \times)$. Sean $\{a_n\}$ y $\{b_n\}$ dos elementos de I. Como el opuesto de $\{b_n\}$ es $\{-b_n\}$, tomando

$$n \geq \max\left\{n^a_{e/2}, n^b_{e/2}\right\},$$

se tiene

$$\begin{aligned} |a_n + (-b_n)| &\leq |a_n| + |-b_n| = |a_n| + |b_n| \\ &< e/2 + e/2 = e. \end{aligned}$$

Esto prueba que $\{a_n\} - \{b_n\} \in I$, por lo que I es un subgrupo de $(A, +)$.

Falta probar que, si $\{a_n\} \in A$ y $\{b_n\} \in I$, entonces $\{a_n\} \times \{b_n\} \in I$. En efecto, como $\{a_n\}$ es acotada existe un racional positivo k^a tal que $|a_n| \leq k^a$ para todo $n \in \mathbb{N}$. Por otro lado, puesto que $\{b_n\}$ es nula, existe $n^b_{e/k^a} \in \mathbb{N}$ tal que $|b_n| < e/k^a$ cuando $n \geq n^b_{e/k^a}$. Entonces, para $n \geq n^b_{e/k^a}$ tenemos

$$|a_n b_n| = |a_n|\,|b_n| < k^a \frac{e}{k^a} = e.$$

Queda así probado que I es un ideal en A. □

El siguiente ejemplo muestra que $(A, +, \times)$ no es un cuerpo, ya que posee divisores de cero.

Ejemplo 5.1. Considérense las sucesiones regulares $\{a_n\}$ y $\{b_n\}$ tales que

$$a_n = \begin{cases} 0 & \text{si } n \text{ es impar} \\ 1/n, & \text{si } n \text{ es par} \end{cases} \quad \text{y} \quad b_n = \begin{cases} 1/n, & \text{si } n \text{ es impar} \\ 0, & \text{si } n \text{ es par} \end{cases}.$$

Se tiene entonces que $a_n b_n = 0$ para todo $n \in \mathbb{N}$. Puesto que $\{a_n\} \times \{b_n\} = \{0\}$, mientras que $\{a_n\} \neq \{0\} \neq \{b_n\}$, concluimos que $\{a_n\}$ y $\{b_n\}$ son divisores de cero.

Lema 5.1. *Si $\{a_n\}$ es una sucesión regular no nula, entonces existe un racional positivo α tal que $a_n \geq \alpha$ finalmente o, por el contrario, $a_n \leq -\alpha$ finalmente.*

Demostración. Como $\{a_n\}$ no es una sucesión nula, existe un racional positivo e tal que, cualquiera que sea $p \in \mathbb{N}$

$$|a_n| \geq e \text{ para algún natural } n \geq p. \tag{5.2}$$

Como $e/2 > 0$ y $\{a_n\}$ es regular, existe $n_e \in \mathbb{N}$ tal que

$$|a_n - a_m| < e/2 \text{ para todo } m, n \geq n_e. \tag{5.3}$$

Usando (5.2), con $p = n_e$,

$$|a_m| \geq e \text{ para algún natural } m \geq n_e.$$

Como a_m es positivo o negativo, analizamos cada caso. Si $a_m \geq e$, entonces, usando (5.3),

$$a_n = a_m - (a_m - a_n) \geq e - |a_m - a_n| > e/2 \text{ para todo } n \geq n_e.$$

En el otro caso, $-a_m \geq e$, y, nuevamente por (5.3),

$$-a_n = -a_m - (a_n - a_m) \geq e - |a_n - a_m| > e/2 \text{ para todo } n \geq n_e.$$

Se llega a la conclusión deseada tomando $\alpha = e/2$. □

Proposición 5.3. *Si $\{a_n\}$ es una sucesión regular, entonces vale exactamente una de las siguientes afirmaciones:*

(*a*) *$\{a_n\}$ es una sucesión nula.*

(*b*) *Existe $\alpha > 0$ tal que $a_n \geq \alpha$ finalmente.*

(*c*) *Existe $\alpha > 0$ tal que $-a_n \geq \alpha$ finalmente.*

Demostración. Al menos una de la afirmaciones (*a*), (*b*) y (*c*) es cierta, ya que, si (*a*) es falsa, entonces, por el lema anterior, vale (*b*) o (*c*). Es inmediato ver que dos de ellas no pueden ser simultáneamente verdaderas. □

5.2. El cuerpo ordenado de los números reales

A partir del anillo de las sucesiones regulares de números racionales definimos el conjunto de los números reales, $\mathbb{R}$, como el conjunto cociente de dicho anillo por la RBE asociada con el ideal de las sucesiones nulas.

Definición 5.2. *El conjunto de los* ***números reales*** *es $\mathbb{R} = A/I$, es decir, que dos sucesiones regulares $\{a_n\}$ y $\{b_n\}$ representan un mismo número real si, y solamente si, la sucesión $\{a_n - b_n\}$ es nula.*

Cualquier sucesión nula, como la sucesión constante $\{0\}$ o las dos sucesiones $\{a_n\}$ y $\{b_n\}$ del Ejemplo 5.1, representa al mismo número real (llamado «cero» y que se denota por 0). Por otro lado, las dos sucesiones regulares que aproximan $\sqrt{2}$ inferior y superiormente, denotémoslas por $\{a_n\}$ y $\{b_n\}$, son representaciones de un mismo número real (precisamente $\sqrt{2}$) por cuanto, dado un racional positivo e, $|a_n - b_n| = 10^{1-n} < 1/(n-1) < e$, sin más que tomar n suficientemente grande.

Las operaciones suma y producto sobre $\mathbb{R}$ serán las inducidas por dicha RBE y comprobaremos que los números reales constituyen un cuerpo. Es más, es posible extender el orden de $\mathbb{Q}$ a $\mathbb{R}$ de tal manera que obtengamos un cuerpo ordenado (recuérdese el Corolario 4.3).

Lema 5.2. *Si $\{a_n\}$ y $\{b_n\}$ son equivalentes y existe un racional positivo α tal que $a_n \geq \alpha$ finalmente, entonces también existe un racional positivo β tal que $b_n \geq \beta$ finalmente.*

Demostración. Por ser $\{a_n\}$ y $\{b_n\}$ equivalentes, existe $p \in \mathbb{N}$ tal que $|a_n - b_n| < \alpha/2$ para todo $n \geq p$. Por otro lado, como $a_n \geq \alpha$ finalmente, existe $q \in \mathbb{N}$ tal que $a_n \geq \alpha$ para todo $n \geq q$. Por lo tanto, si $n \geq \max\{p, q\}$, se tendrá

$$b_n > a_n - \alpha/2 \geq \alpha - \alpha/2 = \alpha/2.$$

Basta, pues, con tomar $\beta = \alpha/2$. □

Definición 5.3. *Si $\{a_n\}$ es un representante de $a \in \mathbb{R}$ decimos que a es* ***positivo*** *si existe un racional positivo α tal que $a_n \geq \alpha$ finalmente.*

La definición de elemento positivo es independiente del representante elegido. En efecto, sea $a = [\{a_n\}] = [\{a'_n\}]$ y supongamos que existe un racional positivo α tal que $a_n \geq \alpha$ finalmente. En virtud del Lema 5.2 también existe entonces un racional positivo β tal que $a'_n \geq \beta$ finalmente. Por lo tanto, a será clasificado como positivo con ayuda de una cualquiera de sus representaciones. Veremos que el conjunto de los reales positivos, $\mathbb{R}^+$, satisface las condiciones especificadas en la Definición 4.9, escribiendo $a \leq b$ cuando $b - a \in \mathbb{R}^+ \cup \{0\}$.

Proposición 5.4. *$(\mathbb{R}, +, \times, \leq)$ es un cuerpo ordenado. Además, la aplicación de $\mathbb{Q}$ en $\mathbb{R}$ que asocia a cada número racional r la clase de equivalencia de la sucesión constante $\{r\}$ (que denotaremos, abusando del lenguaje, por r) es un monomorfismo de cuerpos que preserva el orden.*

Demostración. Por ser $(\mathbb{R}, +, \times)$ el anillo cociente de un anillo conmutativo y unitario por un ideal es, a su vez, un anillo conmutativo y unitario, donde $1 = [\{1\}]$ es el elemento unidad del anillo (véase el comentario que sigue a la Proposición 4.3). Para ver que es un cuerpo sólo falta probar la existencia de inversos, es decir, que la ecuación $ax = 1$ con $0 \neq a \in \mathbb{R}$, tiene solución en $\mathbb{R}$.

Sea $\{a_n\}$ un representante de a. Como $a \neq 0$, $\{a_n\}$ no es una sucesión nula y, en virtud de la Proposición 5.3, podemos suponer que existe un racional positivo α tal que $a_n \geq \alpha$ para $n \geq p$ (el argumento es similar si $a_n \leq -\alpha$ finalmente). Definimos entonces la sucesión de racionales

$$b_n = \begin{cases} 0, & \text{si } n < p \\ 1/a_n, & \text{si } n \geq p \end{cases}.$$

Veremos que $\{b_n\}$ es regular. En efecto, dado $e \in \mathbb{Q}^+$, existe $n^a_{\alpha^2 e} \in \mathbb{N}$ tal que $|a_n - a_m| < \alpha^2 e$ para todo $n, m \geq n^a_{\alpha^2 e}$. Entonces, para $n \geq \max\{p, n^a_{\alpha^2 e}\}$, se tiene

$$|b_n - b_m| = \frac{|a_m - a_n|}{|a_n|\,|a_m|} \leq \alpha^{-2}\,|a_n - a_m| < \alpha^{-2}\left(\alpha^2 e\right) = e.$$

Por otro lado, es evidente que

$$a_n b_n - 1 = \begin{cases} -1, & \text{si } n < p \\ 0, & \text{si } n \geq p \end{cases},$$

de manera que $\{a_n b_n - 1\}$ es una sucesión nula. Por lo tanto, si $b = [\{b_n\}]$, se tiene

$$ab - 1 = [\{a_n b_n - 1\}] = 0$$

y $x = b$ resulta ser la solución buscada para la ecuacion $ax = 1$.

Ya hemos demostrado que $(\mathbb{R}, +, \times)$ es un cuerpo, por lo que debemos ocuparnos ahora del orden. Usando el Teorema 4.4, $(\mathbb{R}, +, \times, \leq)$ será un cuerpo ordenado si la suma y el producto son operaciones cerradas en $\mathbb{R}^+$, puesto que $\mathbb{R} = \mathbb{R}^+ \cup (-\mathbb{R}^+) \cup \{0\}$ como consecuencia inmediata de la Proposición 5.3.

Probaremos que la suma y el producto de dos reales positivos, a y b, es asimismo positivo. Sean $\{a_n\}$ y $\{b_n\}$ representantes de a y de b, respectivamente. Considerando dos racionales positivos α y β, y dos naturales p y q, tales que $a_n \geq \alpha$ para $n \geq p$ y $b_n \geq \beta$ para $n \geq q$, tenemos, para $n \geq \max\{p, q\}$, que

$$\begin{aligned} a_n + b_n &\geq \alpha + \beta > 0, \\ a_n b_n &\geq \alpha\beta > 0. \end{aligned}$$

De aquí se sigue que $a + b$ y ab son positivos.

Que la aplicación de $\mathbb{Q}$ en $\mathbb{R}$ dada por $r \longmapsto [\{r\}]$ es un monomorfismo de cuerpos que preserva el orden, se deja al cuidado del lector. □

5.3. La propiedad arquimediana

Proposición 5.5 ***(Propiedad arquimediana).*** *Dado un número real positivo cualquiera ε, existe un número natural n tal que $1/n \leq \varepsilon$.*

Demostración. Sea $\{e_n\}$ una sucesión regular de racionales tal que $\varepsilon = [\{e_n\}]$. Por ser $\varepsilon > 0$ existe un racional positivo α tal que $e_n \geq \alpha$ finalmente. Podemos escribir $\alpha^{-1} = \dfrac{p}{q}$, con $p, q \in \mathbb{N}$, de modo que $\alpha^{-1} \leq p$. Entonces,

$$\frac{1}{p} \leq \alpha \leq e_n \text{ finalmente.} \tag{5.4}$$

Como $\{e_n\}$ y $\left\{\dfrac{1}{p}\right\}$ son sucesiones regulares, también lo es $\left\{e_n - \dfrac{1}{p}\right\}$, que define el número real $\varepsilon - \dfrac{1}{p} = \left[\left\{e_n - \dfrac{1}{p}\right\}\right]$. Ahora bien, si $\varepsilon - \dfrac{1}{p}$ fuera negativo, usando la Definición 5.3 se tendría que $\dfrac{1}{p} - e_n > 0$ finalmente, contradiciendo

(5.4). Por lo tanto, $\varepsilon - \dfrac{1}{p} \geq 0$ (debido al orden total de $\mathbb{R}$), lo que implica que existe $p \in \mathbb{N}$ tal que $\dfrac{1}{p} \leq \varepsilon$. □

Informalmente hablando, la propiedad arquimediana dice que para medir la distancia entre dos puntos con la precisión que se quiera, alcanzan los números racionales positivos. Una escala de números reales no es más fina.

En el análisis no estándar de Robinson, introducido durante los años 60, se amplía $\mathbb{R}$ de tal forma que existen elementos positivos que son menores que cualquier racional de la forma $1/n$, con $n \in \mathbb{N}$. En dicho campo numérico falla, por lo tanto, la propiedad arquimediana. Esos escalares positivos, tan pequeños, se pretende que son una interpretación precisa de las «mónadas» a las que se refirió Leibniz en sus escritos pioneros acerca del cálculo diferencial. Hay que advertir que este tipo de análisis no goza de general aceptación entre los matemáticos, aunque nadie puede descartar que puedan encontrarse, algún día, aplicaciones importantes de esta teoría (tampoco fueron bien recibidas las geometrías no euclídeas a principios del siglo XIX y luego resultarían ser apropiadas para la astrofísica). En el Problema 5.10 puede verse un cuerpo no arquimediano muy simple.

Para el siguiente resultado conviene recordar que cualquier cuerpo ordenado K contiene una copia exacta del cuerpo $\mathbb{Q}$ (véase en la Sección 4.4 los comentarios posteriores al Corolario 4.3). Si algún lector prefiere pensar que el cuerpo K es $\mathbb{R}$ en vez de un cuerpo cualquiera, puede hacerlo sin pérdida, pues la demostración no varía. Sin embargo, al final del capítulo usaremos esta versión general para justificar que $\mathbb{R}$ es el *único* cuerpo ordenado arquimediano y completo que existe.

Teorema 5.1. *En un cuerpo ordenado K son equivalentes las siguientes afirmaciones.*

(i) K es arquimediano.

(ii) Todo elemento de K es el límite (en K) de una sucesión de elementos racionales de K.

(iii) Entre dos elementos diferentes de K existe al menos un elemento racional de K.

Demostración. *(i)*⇒*(ii)* Por la propiedad arquimediana, dado $a \in K$ existe un entero a_0 que verifica (4.13), es decir,

$$a_0 \leq a < a_0 + 1.$$

Como $0 \leq a - a_0 < 1$, también $0 \leq 10\,(a - a_0) < 10$. Por lo tanto, existe un dígito $a_1 \in \{0, ..., 9\}$ tal que

$$a_1 \leq 10\,(a - a_0) < a_1 + 1,$$

y también

$$0 \leq a - a_0 - a_1 10^{-1} < 10^{-1}.$$

Nuevamente, en virtud de la hipótesis, existe un dígito a_2 tal que

$$a_2 \leq 10^2 (a - x_1) < a_2 + 1,$$

donde $x_1 = a_0 + a_1 10^{-1}$, es decir,

$$0 \leq a - a_0 - a_1 10^{-1} - a_2 10^{-2} < 10^{-2}.$$

Prosiguiendo con este procedimiento podemos definir una sucesión recursiva de elementos racionales $\{x_n\} \subset K$ tomando

$$x_1 = a_0 + a_1 10^{-1} \text{ y } x_{n+1} = x_n + a_{n+1} 10^{-(n+1)},\ n = 1,2,\ldots$$

Claramente

$$|a - x_n| = a - x_n < 10^{-n} < 1/n,$$

por lo que, usando nuevamente que K es arquimediano, se tiene que $\lim_{n\to\infty} x_n = a$, lo que se expresa escribiendo

$$a = a_0 + 0{,}a_1 a_2 a_3 \ldots,$$

que es el llamado **desarrollo decimal** de a.

$(ii) \Rightarrow (iii)$ Dados dos elementos $a, b \in K$ tales que $a < b$, se tiene que $(a+b)/2 \in K$ y que

$$a < \frac{a+b}{2} < b.$$

Por hipótesis, existe una sucesión racional $\{x_n\}$ que converge a $(a+b)/2$. Tomando

$$\varepsilon = \min\left\{\frac{a+b}{2} - a\,,\, b - \frac{a+b}{2}\right\},$$

existe $n_\varepsilon \in \mathbb{N}$ tal que $\left|x_n - \frac{a+b}{2}\right| < \varepsilon$ para todo $n \geq n_\varepsilon$. En particular, para $n = n_\varepsilon$ se obtiene

$$a - \frac{a+b}{2} \leq -\varepsilon < x_{n_\varepsilon} - \frac{a+b}{2} < \varepsilon \leq b - \frac{a+b}{2}\ ,$$

por lo que $a < x_{n_\varepsilon} < b$ y x_{n_ε} es el elemento racional buscado.

$(iii) \Rightarrow (i)$ Si $\varepsilon \in K^+$, existe $a \in \mathbb{Q}$ tal que $0 < a < \varepsilon$. Pero todo racional positivo admite una representación $a = \frac{m}{n}$ con $m, n \in \mathbb{N}$. Entonces, $\frac{1}{n} \leq \frac{m}{n} = a < \varepsilon$. □

Corolario 5.1. ***(Densidad de $\mathbb{Q}$ en $\mathbb{R}$)*** *Todo intervalo propio de números reales (es decir, que contiene más de un punto) contiene al menos un número racional. Además, todo número real es el límite de una sucesión de números racionales.*

De la prueba del Teorema 5.1 se sigue también que todo número real tiene un desarrollo decimal.

Para concluir esta sección formalizamos una conocida propiedad de los **números decimales**. Un número decimal es un racional que puede representarse mediante una fracción cuyo denominador es una potencia de 10. Por ejemplo, $\frac{7}{50} = \frac{14}{100} = 0{,}14 = 0{,}13\widehat{9}$ es un número decimal, mientras que $\frac{527}{990} = 0{,}5\widehat{32}$ no lo es.

Proposición 5.6. *Los únicos números reales que tienen dos desarrollos decimales son los números decimales.*

Demostración. Supongamos que un número real x admite dos desarrollos decimales distintos:

$$x = a_0 + 0{,}a_1a_2a_3\ldots = b_0 + 0{,}b_1b_2b_3\ldots$$

con $a_0, b_0 \in \mathbb{Z}$ y $a_n, b_n \in \{0, 1, \ldots, 9\}$ para todo $n \in \mathbb{N}$, es decir

$$\begin{aligned} x_n &= a_0 + \sum_{k=1}^{n} a_k 10^{-k} \quad \text{y} \quad \lim_{n\to\infty} x_n = x, \\ y_n &= b_0 + \sum_{k=1}^{n} b_k 10^{-k} \quad \text{y} \quad \lim_{n\to\infty} y_n = x. \end{aligned}$$

Consideremos el menor entero $p \geq 0$ tal que $a_p \neq b_p$. Sin pérdida de generalidad, supongamos que $a_p < b_p$. La sucesión $\{y_n - x_n\}$ verifica en $\mathbb{R}$ que $\lim_{n\to\infty} (y_n - x_n) = 0$, donde

$$y_n - x_n = \begin{cases} 0 & \text{si } n < p \\ \sum_{k=p}^{n} (b_k - a_k)\, 10^{-k} & \text{si } n \geq p\,. \end{cases}$$

Sin embargo, para $n \geq p$ se tiene

$$\begin{aligned} y_n - x_n &= (b_p - a_p)\, 10^{-p} + \sum_{k=p+1}^{n} (b_k - a_k)\, 10^{-k} \\ &\geq (b_p - a_p)\, 10^{-p} - \sum_{k=p+1}^{n} |b_k - a_k|\, 10^{-k} \end{aligned} \tag{5.5}$$

$$\begin{aligned} &\geq (b_p - a_p)\,10^{-p} - \sum_{k=p+1}^{n} 9 \times 10^{-k} \\ &> (b_p - a_p)\,10^{-p} - 9 \times \frac{10^{-(p+1)}}{1 - 10^{-1}} \\ &= (b_p - a_p - 1)\,10^{-p}\,. \end{aligned}$$

Como $y_n - x_n$ debe ser arbitrariamente pequeño, la única posibilidad es que $b_p = a_p + 1$. Pero, entonces, debe ser $a_k - b_k = 9$ para todo $k > p$, pues, en caso contrario, usando (5.5), obtenemos

$$\begin{aligned} y_n - x_n &\geq 10^{-p} - \sum_{k=p+1}^{n} |b_k - a_k|\,10^{-k} \\ &\geq 10^{-p} - \sum_{k=p+1}^{n} 9 \times 10^{-k} + 10^{-q} \\ &\geq 10^{-q} \end{aligned}$$

para algún $q \geq p$.

Por lo tanto, $a_k = 9$ y $b_k = 0$ para todo $k > p$, y el número real x es necesariamente un decimal:

$$\begin{aligned} x &= a_0 + 0{,}a_1a_2\ldots a_p\widehat{9} \\ &= a_0 + 0{,}a_1a_2\ldots(a_p + 1)\,. \quad \square \end{aligned}$$

Resumiendo lo hecho hasta el momento, en lo que concierne a los conjuntos numéricos, hemos empezado definiendo $\mathbb{N}$ como el conjunto de los cardinales de los conjuntos finitos. Sobre este conjunto se han definido dos operaciones, la suma y el producto, con pobres propiedades (al no existir simétricos), así como una RBO que es un buen orden. En la primera ampliación se construyó $\mathbb{Z}$, dominio de integridad (ganando la existencia de opuestos), al que se dotó de una RBO total compatible con la suma y con el producto (perdiendo el buen orden), existiendo un monomorfismo de $\mathbb{N}$ en $\mathbb{Z}$ que preserva el orden. Luego, a partir de $\mathbb{Z}$, se construyó el cuerpo de fracciones $\mathbb{Q}$ (ganando los inversos), que resultó ser un cuerpo ordenado (ganando la propiedad arquimediana), para un cierto orden total que extiende el de $\mathbb{Z}$ (en el sentido de que existe un monomorfismo de $\mathbb{Z}$ en $\mathbb{Q}$ que preserva el orden). En la siguiente extensión, de $\mathbb{Q}$ a $\mathbb{R}$, no hubo ganancia aparente, pues seguimos teniendo un cuerpo ordenado arquimediano. Sin embargo, el nuevo cuerpo tiene propiedades muy útiles desde el punto de vista del análisis matemático, según se verá a continuación. Todo esto está implícito en la relación múltiple

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R},$$

que tan alegremente escribimos.

5.4. Completitud de los reales

Las propiedades que enunciaremos en esta sección como teoremas son específicas de $\mathbb{R}$ (en el Ejemplo 5.2 se muestra que el cuerpo $\mathbb{Q}$ no las comparte). Habíamos visto que en $\mathbb{Q}$ toda sucesión convergente es regular, mientras que el recíproco no es necesariamente cierto. En el cuerpo $\mathbb{R}$ queda resuelta esta carencia de límites.

Teorema 5.2. *Toda sucesión regular $\{r_n\}$ de números racionales es convergente en $\mathbb{R}$. Más en concreto, si $r = [\{r_n\}] \in \mathbb{R}$ entonces $\lim_{n\to\infty} r_n = r$.*

Demostración. Queremos probar que, para cualquier $\varepsilon \in \mathbb{R}^+$, existe un número natural n_0 tal que $| r_n - r |< \varepsilon$ si $n \geq n_0$. Por ser $\mathbb{Q}$ denso en $\mathbb{R}$ existe un número racional α verificando $0 < \alpha < \varepsilon$. Como $\{r_n\}$ es regular, existe un natural n_α tal que $| r_m - r_n |< \alpha$ si $m, n \geq n_\alpha$. Fijando $n \geq n_\alpha$ se tiene, para todo $m \geq n_\alpha$,

$$r_n - \alpha < r_m < r_n + \alpha,$$

de donde

$$0 < r_m - r_n + \alpha,$$

y

$$0 < r_n - r_m + \alpha.$$

Por lo tanto, $\{r_m - r_n + \alpha\}_{m=1}^{\infty}$ y $\{r_n - r_m + \alpha\}_{m=1}^{\infty}$ son sucesiones regulares no negativas finalmente, que representan a los números reales no negativos $r - r_n + \alpha$ y $r_n - r + \alpha$, respectivamente. De aquí se obtiene $-\alpha \leq r - r_n \leq \alpha$, lo cual implica que $|r - r_n| \leq \alpha < \varepsilon$ cuando $n \geq n_\alpha$. □

Nótese que en la demostración del siguiente teorema se usan únicamente las propiedades de $\mathbb{R}$ como cuerpo ordenado arquimediano y el teorema anterior.

Teorema 5.3. ***(Principio de encaje de intervalos)*** *Sea una sucesión $[a_n, b_n]$, $n = 1, 2, \ldots$, de intervalos en $\mathbb{R}$ que satisfacen las condiciones siguientes:*

(i) $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ para todo $n \in \mathbb{N}$; y
(ii) $\lim_{n\to\infty} (b_n - a_n) = 0$.

Entonces la intersección de dicha familia de intervalos encajados, $\cap_{n=1}^{\infty} [a_n, b_n]$, es un conjunto singular.

Demostración. Bastará probar que hay al menos un punto en dicha intersección. En efecto, si hubiese dos, $x \neq y$, entonces

$$0 <| x - y |\leq b_n - a_n$$

para todo $n \in \mathbb{N}$ y fallaría (ii). Demostraremos que dicho punto no es otro que el número real $r = [\{r_n\}]$, donde $r_n \in \mathbb{Q}$ ha sido elegido de manera que $a_n < r_n < b_n$ para cada $n \in \mathbb{N}$ (tales r_n existen porque $\mathbb{R}$ es arquimediano).

En primer lugar, una sucesión $\{r_n\}$ así construida es regular. En efecto, usando (ii), dado $e > 0$, $e \in \mathbb{Q}$, existe $n_0 \in \mathbb{N}$ tal que

$$b_{n_0} - a_{n_0} < e.$$

Por otro lado, como consecuencia de (i), si $k \geq n_0$, entonces

$$r_k \in [a_k, b_k] \subset [a_{n_0}, b_{n_0}].$$

Luego, para cualesquiera $n, m \geq n_0$ se tiene que $r_n, r_m \in [a_{n_0}, b_{n_0}]$, de donde

$$| r_n - r_m | \leq b_{n_0} - a_{n_0} < e.$$

Por lo tanto, la sucesión de racionales $\{r_n\}$ es regular y $r = [\{r_n\}]$ es un número real.

Ya sólo falta probar que $r \in \cap_{n=1}^{\infty} [a_n, b_n]$ y lo haremos por reducción al absurdo, suponiendo que $r \notin [a_p, b_p]$ para algún $p \in \mathbb{N}$. Supongamos que $r < a_p$ (el argumento para $b_p < r$ es análogo). Como $r_n \in [a_n, b_n] \subset [a_p, b_p]$ para todo $n \geq p$, se tiene que $r_n - r \geq a_p - r > 0$. Tomando $\varepsilon = a_p - r$ obtenemos que $|r_n - r| \geq \varepsilon$ para todo $n \geq p$, lo cual contradice la afirmación del Teorema 5.2: $\lim_{n \to \infty} r_n = r$. □

Si seguimos llamando $\{a_n\}$ y $\{b_n\}$ a las sucesiones que aproximan inferior y superiormente $\sqrt{2}$, $\{[a_n, b_n]\}$ es una sucesión de intervalos cerrados encajados cuyas longitudes tienden a cero (véase Figura 5.2).

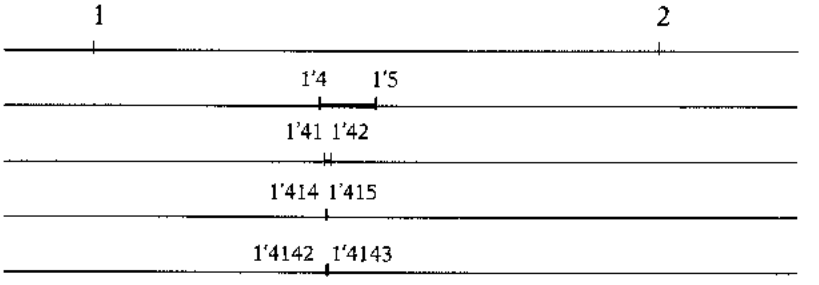

Figura 5.2. *Cinco primeros términos de una sucesión de intervalos encajados cuya intersección es* $\left\{\sqrt{2}\right\}$.

Definición 5.4. *Si los conjuntos no vacíos A y B forman una partición de un conjunto totalmente ordenado X y se cumple $a < b$ cualesquiera que sean $a \in A$ y $b \in B$, entonces se dice que el par (A, B) es una* ***cortadura*** *en X.*

Un ejemplo de cortadura en $\mathbb{R}$ es el par de conjuntos (A, B) donde

$$B = \{x \in \mathbb{R} \mid x^2 > 2, x > 0\}$$

mientras que $A = \mathbb{R} \backslash B$. Es fácil ver que, en este ejemplo, $\max A = \sqrt{2}$ (véase Figura 5.3).

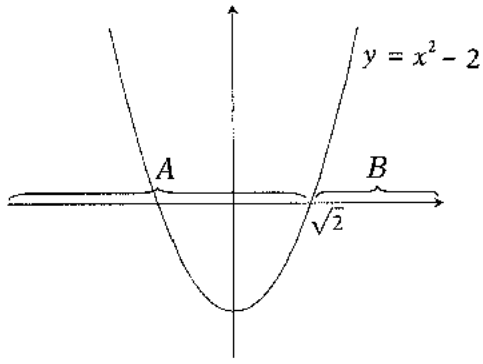

Figura 5.3. *Representación de la cortadura (A, B).*

Nótese que en la demostración del siguiente teorema se usan únicamente propiedades de $\mathbb{R}$ como cuerpo ordenado arquimediano y el principio de encaje de intervalos.

Teorema 5.4. *(**Postulado de continuidad**) Si (A, B) es una cortadura en $\mathbb{R}$ entonces existe máximo de A o bien existe mínimo de B. El número real c que cumple esta condición se denomina **elemento de separación** de la cortadura.*

Demostración. Como A y B son no vacíos, existen números reales $a_0 \in A$ y $b_0 \in B$. Desde luego, $a_0 < b_0$. Denotamos $\alpha = b_0 - a_0 > 0$ la longitud del intervalo inicial $[a_0, b_0]$.

Definimos recursivamente una sucesión de intervalos cerrados encajados $\{[a_n, b_n]\}_{n=1}^{\infty}$, donde el extremo izquierdo de cada intervalo es un elemento de A y el extremo derecho es elemento de B, así:

$$[a_1, b_1] = \begin{cases} [a_0\,,\ a_0 + \alpha/2]\,, & \text{si } a_0 + \alpha/2 \in B \\ [a_0 + \alpha/2\,,\ b_0]\,, & \text{si } a_0 + \alpha/2 \in A\,, \end{cases}$$

y

$$[a_{n+1}, b_{n+1}] = \begin{cases} \left[a_n\,,\ a_n + \alpha/2^{n+1}\right], & \text{si } a_n + \alpha/2^{n+1} \in B \\ \left[a_n + \alpha/2^{n+1},\ b_n\right], & \text{si } a_n + \alpha/2^{n+1} \in A. \end{cases}$$

Por la costrucción, para todo $n \in \mathbb{N}$ se cumple

$$[a_{n+1}, b_{n+1}] \subset [a_n, b_n]\,;$$

con $a_n \in A$ y $b_n \in B$, siendo la longitud de cada intervalo la mitad del anterior,

$$b_n - a_n = \frac{\alpha}{2^n}. \tag{5.6}$$

Recordando que $2^n > n$ para todo $n \in \mathbb{N}$ (Problema 2.1) se tiene

$$\frac{\alpha}{2^n} < \frac{\alpha}{n}. \tag{5.7}$$

Para poder aplicar el principio de encaje de intervalos a la sucesión $\{[a_n, b_n]\}$ bastará probar que $\lim_{n\to\infty}(b_n - a_n) = 0$. En efecto, dado un real positivo ε arbitrario, por la propiedad arquimediana, existe $p \in \mathbb{N}$ tal que $1/p < \varepsilon/\alpha$. Entonces, para todo $n \geq p$, usando (5.6) y (5.7), se tiene que

$$|b_n - a_n| = \frac{\alpha}{2^n} < \frac{\alpha}{n} \leq \frac{\alpha}{p} < \varepsilon.$$

Sea pues $\cap_{n=1}^{\infty}[a_n, b_n] = \{c\}$, con $c \in \mathbb{R}$. Como (A, B) es una cortadura en $\mathbb{R}$, $c \in A$ o bien $c \in B$. Terminaremos probando que $c = \max A$ en el primer caso y que $c = \min B$ en el segundo.

Supongamos que $c \in A$. En este caso, si $a \in A$ es un elemento cualquiera tal que $c \leq a$, como (A, B) es una cortadura, $a < b_n$, pues $b_n \in B$. Entonces, $a_n \leq c \leq a < b_n$ para todo natural n, por lo que $a = c$. Como $c \in A$ es cota superior de A, $c = \max A$.

Análogamente se prueba que si $c \in B$, entonces $c = \min B$. □

Definición 5.5. *Sea $A \neq \emptyset$ un subconjunto de un conjunto totalmente ordenado X. Un elemento $b \in X$ se dice que es* ***supremo*** *de A cuando*

(i) b es una cota superior de A, y
(ii) si b' es una cota superior de A entonces $b \leq b'$.

Cuando existe supremo de A, éste es único, se denotará por $\sup A$ y es la mínima de las cotas superiores de A (en inglés, least upper bound o, abreviadamente, l.u.b.). Si existe $\max A$, entonces $\sup A = \max A$, pero puede suceder que exista $\sup A$ pero no $\max A$. Por ejemplo, para

$$A = \{x \in \mathbb{R} \mid x < 1\}$$

no existe $\max A$, mientras que $\sup A = 1$.

De manera análoga se define el **ínfimo** de un conjunto A, como la máxima de las cotas inferiores de A y se denota por $\inf A$ (en inglés, *greatest lower bound* o, abreviadamente, g.l.b.).

Nótese que en la demostración del siguiente teorema se usan únicamente propiedades de $\mathbb{R}$ como cuerpo ordenado y el postulado de continuidad (no la propiedad arquimediana).

Teorema 5.5 ***(Propiedad del supremo).*** *Todo conjunto no vacío de números reales acotado superiormente tiene supremo.*

Demostración. Sea X un conjunto no vacío de números reales con cota superior b_1. Tomando arbitrariamente un punto $x \in X$, el número real $a_1 = x - 1$ no es una cota superior de X. Consideramos el conjunto no vacío B formado por todas las cotas superiores de X y el complemento $A = \mathbb{R} \backslash B \neq \emptyset$. Obviamente, $b_1 \in B$ y $a_1 \in A$ (véase Figura 5.4).

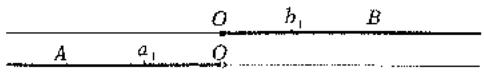

Figura 5.4. *Representación gráfica de los conjuntos A y B de la prueba cuando* $X = \left\{-\frac{1}{n}\right\}$ *o* $X =]-\infty, 0[$.

Es fácil ver que $a < b$ para todo $a \in A$ y $b \in B$, por lo que (A, B) es una cortadura en $\mathbb{R}$. Aplicando el postulado de continuidad existe el elemento de separación $c \in \mathbb{R}$, tal que $c = \max A$ o bien $c = \min B$. En este último caso, $c = \sup X$ por ser la cota superior mínima.

Veamos que el otro caso es imposible. Supongamos que fuera $c = \max A$. Entonces, $c \in A$ y, por lo tanto, $c \notin B$, es decir, c no sería cota superior de X, por lo que existiría $x \in X$ tal que $c < x$. De allí obtendríamos que el número real $a_2 = (c + x)/2 < x$ no sería cota superior de X, por lo que $a_2 \in A$, además de $a_2 > c$, por lo que c no podría ser el máximo de A, en contradicción con el supuesto inicial. □

El resultado anterior es equivalente a afirmar que todo conjunto no vacío acotado inferiormente tiene ínfimo. Basta cambiar el signo a todos los elementos del conjunto y aplicar la proposición anterior, y viceversa.

En ciertos textos de análisis matemático se dice que $\mathbb{R}$ es completo por satisfacer la propiedad del supremo.

Utilizando los conceptos de supremo e ínfimo en el postulado de continuidad, el elemento de separación c de una cortadura (A, B) cumple $c = \sup A = \inf B$. En efecto, si, por ejemplo, $c = \max A$ obviamente $c = \sup A$, pero, también, $c \in A$, por lo que c es cota inferior de B. Además, es la máxima cota inferior de B debido a que ningún $b \in B$ puede ser cota inferior de B $(c < (c + b)/2 < b)$.

El conjunto $B = \{x \in \mathbb{R} \mid x^2 > 2, x > 0\}$ está acotado inferiormente (por 0, por ejemplo), mientras que $A = \mathbb{R} \backslash B$ está acotado superiormente por 2. Pues bien, es fácil ver que $\max A = \sqrt{2}$ y, por lo tanto, $\inf B = \sqrt{2}$ (véase Figura 5.3).

Nótese que en la demostración del siguiente teorema se usan únicamente propiedades de $\mathbb{R}$ como cuerpo ordenado y la propiedad del supremo.

Teorema 5.6 ***(Convergencia de sucesiones monótonas).*** *Toda sucesión de números reales no decreciente y acotada superiormente tiene límite en* $\mathbb{R}$.

Demostración. Sea $\{a_n\}$ una sucesión en $\mathbb{R}$ acotada superiormente, tal que $a_n \leq a_{n+1}$ para todo n natural. Como el conjunto no vacío $A = \{a_n \in \mathbb{R} \mid n \in \mathbb{N}\}$ está acotado superiormente, por la propiedad del supremo, existe $\sup A = a \in \mathbb{R}$. Usando ahora que a es la cota superior mínima de A se tiene que, para

cualquier $\varepsilon > 0$, $\varepsilon \in \mathbb{R}$, existe algún $p \in \mathbb{N}$ tal que

$$a - \varepsilon < a_p \leq a_{p+1} \leq a_{p+2} \leq \cdots \leq a\,.$$

Luego, para todo $n \geq p$,

$$|a - a_n| = a - a_n < \varepsilon\,,$$

lo que equivale a afirmar que $\lim_{n\to\infty} a_n = a$. □

El resultado anterior es equivalente a afirmar que toda sucesión no creciente acotada inferiormente tiene límite.

Sabemos que cada número real tiene un desarrollo decimal. Ahora probaremos que cualquier expresión decimal (finita o infinita, periódica o no) representa un número real. Ésta es la forma de presentación de los números reales en la enseñanza media. Nótese que en la demostración se usarán únicamente propiedades de $\mathbb{R}$ como cuerpo ordenado y el Teorema 5.6.

Teorema 5.7 ***(Representación en $\mathbb{R}$ de las expresiones decimales).*** *Toda expresión decimal de la forma $a_0 + 0,a_1a_2a_3\ldots$, con $a_0 \in \mathbb{Z}$ y $a_n \in \{0,\ldots,9\}$ para todo $n \in \mathbb{N}$, es el desarrollo decimal de un número real. En otras palabras, la sucesión de decimales*

$$\left\{a_0 + \sum_{k=1}^{n} a_k 10^{-k}\right\}_{n=1}^{\infty}$$

tiene límite en $\mathbb{R}$

Demostración. La sucesión

$$x_n = a_0 + \textstyle\sum_{k=1}^{n} a_k 10^{-k}, \quad n = 1,2,\ldots,$$

es no decreciente, ya que $x_{n+1} - x_n = a_{n+1}10^{-n-1} \geq 0$. Veamos que también es acotada superiormente. En efecto,

$$x_n = a_0 + \textstyle\sum_{k=1}^{n} a_k 10^{-k} \leq a_0 + \sum_{k=1}^{n} 9 \times 10^{-k} =$$

$$= a_0 + 9\textstyle\sum_{k=1}^{n} 10^{-k} \leq a_0 + 1\,.$$

La conclusión se sigue del Teorema 5.6. □

Ejemplo 5.2. Veremos que el cuerpo arquimediano $\mathbb{Q}$ incumple todos los teoremas de esta sección. Comenzaremos con el último.

Por el Corolario 5.1 sabemos que $\sqrt{2} \in \mathbb{R}$ es el límite de una sucesión de números racionales $\{x_n\}$, por ejemplo, la que corresponde a su desarrollo decimal, $\sqrt{2} = a_0 + 0,a_1a_2\ldots$, es decir,

$$x_n = a_0 + \sum_{k=1}^{n} a_k 10^{-k}.$$

Se probó que la sucesión $\{x_n\}$ es acotada, no decreciente y $\lim_{n\to\infty} x_n = \sqrt{2}$. Supongamos que $\{x_n\}$ fuera convergente en $\mathbb{Q}$, es decir, supongamos que existe $x \in \mathbb{Q}$ tal que $\lim_{n\to\infty} x_n = x$ en $\mathbb{Q}$. Llegaremos a una contradicción.

En efecto, para todo $e \in \mathbb{Q}^+$ existe $n_e \in \mathbb{N}$ tal que

$$|x - x_n| < e \quad \text{para todo } n \geq n_e\,. \tag{5.8}$$

Por otro lado, para todo $\varepsilon \in \mathbb{R}^+$ existe $m_\varepsilon \in \mathbb{N}$ tal que

$$\left|\sqrt{2} - x_n\right| < \varepsilon \quad \text{para todo } n \geq m_\varepsilon\,.$$

Como es $\mathbb{Q}$ es denso en $\mathbb{R}$ existe $r \in \mathbb{Q}$ tal que $0 < r < \varepsilon/2$. Tomando $e = r$ en la expresión (5.8) y $n \geq \max\left\{n_r, m_{\varepsilon/2}\right\}$,

$$\begin{aligned}
\left|\sqrt{2} - x\right| &= \left|\sqrt{2} - x_n + x_n - x\right| \\
&\leq \left|\sqrt{2} - x_n\right| + |x_n - x| \\
&< \varepsilon/2 + r < \varepsilon\,.
\end{aligned}$$

Entonces $x = \sqrt{2}$, pero esto no es posible, ya que $x \in \mathbb{Q}$ y $\sqrt{2} \notin \mathbb{Q}$. Por lo tanto, $\mathbb{Q}$ no cumple lo que afirma el Teorema 5.7 para $\mathbb{R}$.

Como en la demostración del Teorema 5.7 sólo se usaron propiedades de $\mathbb{R}$ como cuerpo ordenado ($\mathbb{Q}$ también lo es) y el Teorema 5.6, se concluye que $\mathbb{Q}$ tampoco cumple lo que afirma el Teorema 5.6 para $\mathbb{R}$. Por la misma razón, $\mathbb{Q}$ no tiene la propiedad de supremo ni verifica el postulado de continuidad. Además, recordando que $\mathbb{Q}$ es arquimediano, $\mathbb{Q}$ viola el principio de encaje de intervalos. En consecuencia, tampoco cumple lo que afirma el Teorema 5.2 para $\mathbb{R}$.

5.5. Epílogo

Acabaremos este capítulo con algunos comentarios ilustrativos, de lectura opcional, de las conexiones existentes entre los resultados de la Sección 5.4 y teoremas básicos del análisis matemático. Veremos, asimismo, que $\mathbb{R}$ es el único cuerpo arquimediano que completa a los racionales.

Comenzaremos introduciendo algunos conceptos para cuerpos ordenados cualesquiera.

Definición 5.6. *Una sucesión $\{a_n\}$ en un cuerpo ordenado K es de* ***Cauchy*** *si cualquiera que sea $\varepsilon \in K^+$, $|a_n - a_m| < \varepsilon$ finalmente.*

K se dice que es ***completo*** *(en el sentido de Cauchy) cuando toda sucesión de Cauchy converge en K.*

Una sucesión en $\mathbb{Q}$ es regular si, y sólo si, es de Cauchy.

Es fácil probar que toda sucesión convergente en K es de Cauchy. En $\mathbb{R}$ vale también el recíproco, es decir, $\mathbb{R}$ es completo (Cauchy), pero $\mathbb{Q}$ no lo es.

Definición 5.7. *Un cuerpo ordenado K se dice que es* ***relativamente compacto*** *cuando toda sucesión en K acotada contiene una subsucesión convergente en K.*

Se conoce que en un cuerpo ordenado las siguientes siete proposiciones son equivalentes entre sí:

K es arquimediano y cumple el principio de encaje de intervalos.
En K se verifica el postulado de continuidad.
K tiene la propiedad del supremo.
K tiene la propiedad de convergencia de sucesiones monótonas.
Las expresiones decimales se representan en K.
K es relativamente compacto.
K es arquimediano y completo (Cauchy).

En algunos textos de Análisis Matemático se dice que el cuerpo ordenado $\mathbb{R}$ es **completo** por tener la propiedad del supremo. Éste es un sentido de completitud más fuerte, que implica que el cuerpo es arquimediano y completo (Cauchy).

De todo lo visto en este capítulo, algunas nociones son exportables a un conjunto A que no esté totalmente ordenado (en cuyo caso la propiedad arquimediana ni siquiera puede ser formulada en A) pero donde esté definida una *distancia* (como módulo en $\mathbb{C}$ o la norma de vectores en $\mathbb{R}^n$). Por ejemplo, los conceptos de convergencia de sucesiones, acotación, completitud (Cauchy) y relativamente compacto son de este tipo. Al igual que para cuerpos ordenados, completo (Cauchy) es más débil que relativamente compacto.

Volviendo al cuerpo $\mathbb{R}$ y a las funciones de variable real con valores reales, la siguiente proposición, conocida como el teorema de Bolzano, es, también, equivalente a la afirmación: «$\mathbb{R}$ es un cuerpo ordenado, arquimediano y completo»:

Si $a, b \in \mathbb{R}$, $a < b$ y $f : [a,b] \longrightarrow \mathbb{R}$ es una función continua tal que $f(a)f(b) < 0$, entonces existe $\alpha \in [a,b]$ tal que $f(\alpha) = 0$.

Obsérvese que la gráfica de una función continua sobre un intervalo cerrado y acotado puede cortar al eje de abscisas en infinitos puntos, como ocurre con $y = f(x)$ (véase Figura 5.5), donde

$$f(x) = \begin{cases} x \operatorname{sen} \dfrac{1}{x}, & x \neq 0 \\ 0 \quad , & x = 0. \end{cases}$$

En el próximo capítulo veremos que si $f(x)$ es una función polinómica de grado n, el número de sus intersecciones con el eje de abscisas es a lo más n.

Algunos comentarios, para terminar, con respecto a la posible existencia de otro cuerpo ordenado, arquimediano y completo: Cualquier cuerpo ordenado $(K, +, \times, \leq)$ contiene una copia de $\mathbb{Q}$. Si, además, K es arquimediano (véase el Teorema 5.1), $\mathbb{Q}$ es denso en K, o, de manera equivalente, todo elemento

de K es límite de una sucesión (regular) de racionales. Ahora bien, el cuerpo $\mathbb{R}$ fue construido agregándole a $\mathbb{Q}$ *todos* los límites de sucesiones regulares de números racionales, por lo que cada elemento de K está en el cuerpo $\mathbb{R}$. En resumen, todo cuerpo ordenado arquimediano K verifica que

$$\mathbb{Q} \subset K \subset \mathbb{R}\,.$$

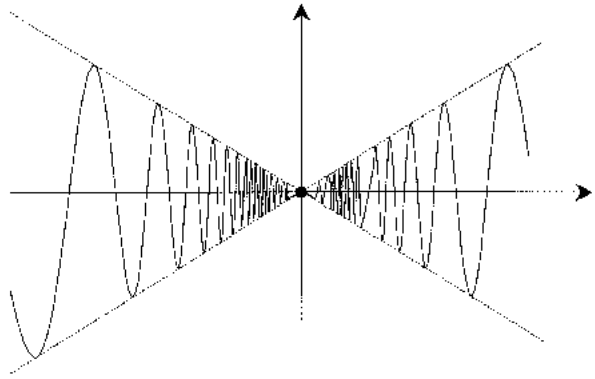

Figura 5.5. *Una ecuación $f(x) = 0$, con f continua en $[a, b]$, $a < b$, puede tener infinitas raíces.*

Ahora bien, si $K \neq \mathbb{R}$, entonces no puede ser completo, ya que si $a \in \mathbb{R}\backslash K$, por el Teorema 5.1, existe una sucesión de racionales $\{a_n\}$ tal que $\lim_{n\to\infty} a_n = a$ (y por lo tanto $\{a_n\}$ es regular), pero esa misma sucesión (pensada dentro de K) carece de límite en K (debido a que una sucesión no puede tener dos límites diferentes en $\mathbb{R}$). La conclusión es que, de todos los cuerpos ordenados y arquimedianos, el único completo es $\mathbb{R}$. Dejaremos asentado como un teorema la conclusión a la que hemos llegado. Obviamente, el razonamiento anterior es tan sólo un esquema de la demostración, pero una prueba completa puede seguir este esquema. Es usual que los matemáticos profesionales antepongan a la secuencia de demostraciones técnicas esquemas de ideas como el descrito anteriormente, que comunican lo esencial de la prueba.

Teorema 5.8. *Todo cuerpo ordenado, arquimediano y completo (Cauchy) es isomorfo al cuerpo $\mathbb{R}$ de los números reales.*

Constituye una parte importante en la formación matemática seguir en detalle una construcción de los números reales, como la que hemos realizado en este capítulo, pero de ahora en adelante no será necesario referirse a esta construcción particular. Es absolutamente irrelevante que un número real sea una clase de equivalencia de sucesiones regulares de números racionales, y este hecho no se volverá a usar en la demostración de ningún teorema acerca de los números reales. Las demostraciones sensatas utilizarán únicamente las propiedades de $\mathbb{R}$ como cuerpo ordenado arquimediano y completo, o alguna de sus equivalencias, ya que estas propiedades lo caracterizan salvo isomorfismo.

En relación con esto, conviene recordar las «teorías axiomáticas de tipo material» a las que nos referíamos en la sección 2.7 (véase también el Problema 2.32). Los textos no elementales de análisis real suelen adoptar un enfoque axiomático, declarando la existencia de un conjunto cuyos elementos verifican una lista de axiomas, que no son otros que las exigencias de cuerpo (Definición 4.5) con un orden compatible (Definición 4.9) y, por ejemplo, la propiedad del supremo (Teorema 5.5). Este tipo de enfoques es consistente con lo afirmado en el párrafo anterior.

Finalmente, para el lector que se sienta agobiado por la noticia de que acabamos de llegar al punto de partida del análisis real, sepa que la matemática que hemos venido haciendo tiene valor y utilidad en sí misma, independientemente del uso que le hemos dado en esta fundamentación.

5.6. **Problemas**

Problema 5.1. Si denotamos A el conjunto de todas las sucesiones de números racionales convergentes en $\mathbb{Q}$ y por I el conjunto de las sucesiones nulas, pruebe que:

a) A es un anillo conmutativo y unitario e I es un ideal,
b) el anillo cociente A/I es un cuerpo isomorfo a $\mathbb{Q}$.

(Sugerencia: *a*) adapte la demostración de la Proposición 5.2; *b*) pruebe que la aplicación $f : A/I \to \mathbb{Q}$ está bien definida por $[\{a_n\}] \longmapsto \lim_{n\to\infty} a_n$ y que es un isomorfismo.)

Problema 5.2. Clasifique la estructura que determina, sobre

$$E = \left\{a + b\sqrt{3} \mid a \in \mathbb{Z}, b \in \mathbb{Z}\right\},$$

la suma y el producto de números reales.

Problema 5.3. Para el conjunto E del Problema 5.2 se considera la correspondencia que asocia al número $a+b\sqrt{3}$ el $a-b\sqrt{3}$. Clasifique esta correspondencia.

Problema 5.4. Sea α la raíz cuadrada de un número natural que no es un cuadrado perfecto, y sean

$$E = \{a + b\alpha \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$$

y

$$F = \{a + b\alpha \mid a \in \mathbb{Q}, b \in \mathbb{Q}\}.$$

Analice la estructura algebraica de $(E, +, .)$ y de $(F, +, .)$.

Problema 5.5. Demuestre que los números reales de la forma $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, donde a, b y c representan números racionales, forman un dominio de integridad. ¿Qué dificultad surge cuando se trata de probar que se trata, en realidad, de un cuerpo?

Problema 5.6.* Demuestre el Teorema de Bolzano usando el principio de encaje de intervalos en $\mathbb{R}$. (Ayuda: Si $a < b$ y $f(a) < 0 < f(b)$, el primer intervalo es $[a, b]$; el segundo es $\left[a, \frac{a+b}{2}\right]$ si $0 < f\left(\frac{a+b}{2}\right)$, etc.)

Problema 5.7. Desde el punto de vista algebraico, la ventaja de $\mathbb{R}$ sobre $\mathbb{Q}$ estriba en la existencia de solución para las ecuaciones de la forma $x^n - a = 0$ para a (real) positivo. Demuestre la existencia de la raíz n-ésima de $a > 0$ recurriendo al Teorema de Bolzano.

Problema 5.8. Pruebe que si $r \neq 0$ es un número racional y $x \neq 0$ es irracional, entonces rx y $r + x$ son irracionales.

Problema 5.9. Demuestre que entre dos números reales diferentes existen infinitos números racionales y también infinitos irracionales.

Problema 5.10.* Considere el dominio de integridad ordenado, $(\mathbb{Z}[x], +, ., \leq)$, de los polinomios con coeficientes enteros dotados del orden lexicográfico (véase Problema 4.14). Denotamos por $(K, +, .)$ el cuerpo de fracciones de $(\mathbb{Z}[x], +, .)$ y decimos que una fracción $\frac{p(x)}{q(x)}$ es positiva cuando $p(x)q(x)$ es positivo en el orden lexicográfico.

a) Pruebe que la definición de fracción positiva es buena (independiente del representante elegido).

b) Se define en K la siguiente RBO $\leq$: dadas dos fracciones r y s, $r \leq s$ cuando $s = r$ o bien $s - r$ es una fracción positiva. Pruebe que $(K, +, ., \leq)$ es un cuerpo ordenado.

c) Pruebe que $(K, +, ., \leq)$ no es arquimediano.

(Ayuda: compruebe que $0 < \frac{1}{x} < \frac{1}{n}$ para todo $n \in \mathbb{N}$).

d) Halle una cota superior para el conjunto de los números naturales.

Problema 5.11.* (Dedekind) Pruebe que el siguiente par de conjuntos de racionales es una cortadura en $\mathbb{Q}$:

$$B = \{x \in \mathbb{Q} \mid x^2 > 2, x > 0\} \text{ y } A = \mathbb{Q} \backslash B.$$

Si se asocia a cada $x \in \mathbb{Q}$ el racional (bien definido)

$$y = \frac{x(x^2+6)}{3x^2+2},$$

verifique que

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

Utilizando las relaciones anteriores, demuestre que no existe elemento de separación para la cortadura (A, B) de $\mathbb{Q}$.

La conclusión es que fallan, en $\mathbb{Q}$, el postulado de continuidad, la propiedad del supremo y el principio de encaje. Por esa razón falla el Teorema de Bolzano para la recta (eje de abscisas) racional.

Problema 5.12. Analice con cuidado las pruebas de los Teoremas 5.3, 5.4, 5.5, 5.6 y 5.7, comprobando que sólo se utilizan las propiedades de los cuerpos ordenados y el teorema que les precede.

Problema 5.13. En un cuerpo ordenado K se definen los conjuntos

$$\begin{aligned} A &= \left\{x \in K \mid x < \frac{1}{n}\text{, para todo } n \in \mathbb{N}\right\}, \\ B &= \left\{x \in K \mid \text{existe } n \in \mathbb{N} : \frac{1}{n} < x\right\}. \end{aligned}$$

Demuestre que (A, B) es una cortadura en K y que no existe elemento de separación cuando K no es arquimediano. (Ayuda: pruebe que si $s \in A$ y $s > 0$ entonces $2s \in A$.)

Problema 5.14. Demuestre que si un cuerpo ordenado K tiene la propiedad del supremo, entonces también se verifica el postulado de continuidad. (Ayuda: para una cortadura (A, B) en K pruebe que $\sup A$ es el elemento de separación.)

Problema 5.15. Pruebe que la sucesión $\{n\}$ de los números naturales no es convergente en ningún cuerpo ordenado K. (Ayuda: Suponga que $\lim\limits_{n\to\infty} n = x \in K$ y pruebe que entonces $\lim\limits_{n\to\infty} n = x - 1$, contradiciendo la unicidad del límite.)

Problema 5.16. Pruebe que si la sucesión $\left\{\frac{1}{n}\right\}$ es convergente en un cuerpo ordenado K, entonces $\lim\limits_{n\to\infty} \frac{1}{n} = 0$. (Ayuda: suponga lo contrario y aplique el problema anterior.)

Problema 5.17.* Una **subsucesión** de una sucesión $\{a_n\}_{n=1}^{\infty}$ es una sucesión de la forma $\{a_{n_k}\}_{k=1}^{\infty}$, donde $n_k \in \mathbb{N}$ y $n_k < n_{k+1}$ para todo $k \in \mathbb{N}$.

a) Pruebe que toda subsucesión de una sucesión convergente en K es también convergente al mismo límite.

b) Pruebe que si una sucesión $\{a_n\}$ es de Cauchy en K y contiene una subsucesión convergente, entonces $\{a_n\}$ también es convergente (al mismo límite).

c) Pruebe que si una sucesión $\{a_n\}$ en K es monótona y contiene una subsucesión convergente, entonces $\{a_n\}$ también es convergente (al mismo límite).

d) Pruebe que en un cuerpo ordenado K toda sucesión contiene una subsucesión que es, o bien no decreciente, o bien no creciente. (Ayuda: véase Spivak, M. (1970), p. 560.)

Problema 5.18. En un cuerpo ordenado K pruebe que $\left\{\dfrac{1}{n}\right\}$ es convergente si, y sólo si, $\{10^{-n}\}$ lo es. (Ayuda: use el Problema 5.17 *a*) y *b*).)

Problema 5.19. Suponga que en un cuerpo ordenado K vale lo afirmado para $\mathbb{R}$ en el Teorema 5.7. Pruebe que, entonces, K es arquimediano. (Ayuda: para $x_n = \sum_{k=1}^{n} 9\,10^{-k}$, analice la convergencia de $\{10^{-n}\} = \{1 - x_n\}$ y aplique el problema anterior.)

Problema 5.20.* Demuestre que si un cuerpo K tiene la propiedad de convergencia de sucesiones monótonas (véase Teorema 5.6), entonces K es arquimediano y completo (Cauchy). (Ayuda: K será arquimediano porque $\left\{\dfrac{1}{n}\right\}$ es monótona no creciente; para la completitud use el Problema 5.17 *d*), luego, que toda sucesión de Cauchy es acotada y, por último, el Problema 5.17 *b*).)

Problema 5.21. Demuestre que el intervalo $A = [0, 1] \subset \mathbb{R}$ es no numerable siguiendo el siguiente esquema de la prueba.

Suponga lo contrario y sea $A = \{x_i \mid i \in \mathbb{N}\}$ una enumeración. Usando la expresión decimal infinita (para los números decimales se elige la representación con período 9) elabore la «lista» de los números reales:

$$\begin{aligned} x_1 &= 0,a_{11}a_{12}\ldots a_{1n}\ldots \\ x_2 &= 0,a_{21}a_{22}\ldots a_{2n}\ldots \\ &\ldots \\ x_n &= 0,a_{n1}a_{n2}\ldots a_{nn}\ldots \\ &\ldots \end{aligned}$$

la expresión decimal $y = 0,b_1b_2\ldots b_n\ldots$ construida así: $b_k = 5$ si $a_{kk} \neq 5$ o de lo contrario $b_k = 6$, para cada $k \in \mathbb{N}$, representa un número real $y \neq x_n$ para todo $n \in \mathbb{N}$.

CAPÍTULO 6

EL CUERPO DE LOS NÚMEROS COMPLEJOS

Entre las operaciones que pueden realizarse con números complejos destaca la radicación, que permite resolver algunas clases de ecuaciones algebraicas. Los babilonios supieron resolver ecuaciones de segundo grado por el método de completar los cuadrados. Las creencias filosóficas y las dificultades notacionales de los griegos les impulsaron a crear un álgebra geométrica que reducía la resolución de ecuaciones a la intersección de curvas planas adecuadamente construidas. En 1202, el italiano Leonardo de Pisa tradujo el «álgebra» del árabe Al-Khwarizmi (de cuyo nombre proviene el término «algoritmo»), que contemplaba la radicación como una operación aritmética más (en los *Elementos* de Euclides tan sólo se consideraban las raíces cuadradas y sus propiedades). La mejora de la notación algebraica por los algebristas italianos del siglo XVI propició nuevos avances. La resolución de ecuaciones cúbicas fue obra de Del Ferro e, independientemente, de Tartaglia y Cardano. En 1545, Ferrari, discípulo de Cardano, logró resolver por radicales las ecuaciones de cuarto grado, lo que hizo pensar en la posibilidad de resolver por radicales cualquier ecuación algebraica.

Los números complejos fueron introducidos por los algebristas italianos del siglo XVI como un artificio que permitiera el cálculo de las raíces reales de las ecuaciones cúbicas mediante radicales. De hecho, las reglas de cálculo con números complejos en forma binómica fueron enunciadas por Bombelli aun sin creer en su existencia como números, llamándoles, por esa razón, imaginarios.

En torno a 1800, Gauss, Argand y Wessel representaron gráficamente los números complejos como vectores del plano. La noción de vector era novedosa en matemáticas pero estaba siendo utilizada por los físicos desde los tiempos de Galileo. La identificación del cuerpo de los complejos $\mathbb{C}$ con el conjunto de pares ordenados de números reales, $\mathbb{R}^2$, provisto de operaciones adecuadas, la obtuvo Hamilton hacia 1830, con lo que la fundamentación de los números complejos sería consecuencia directa de la correspondiente a los números reales que, como sabemos, aún tuvo que esperar medio siglo. Aunque a partir de ese momento ya no existen razones para atribuir a estos números denominaciones de resonancias esotéricas, como «imaginarios» o «complejos», seguiremos ateniéndonos a la tradición, como ya lo hicimos en capítulos previos, donde se habló de números «racionales», «irracionales» o «reales»

(quizás para recordar que los matemáticos siguen bajo el influjo de Pitágoras).

Pero retomemos el hilo de las ecuaciones algebraicas. Fracasados los intentos de resolver la ecuación de quinto grado por parte de matemáticos tan eminentes como Leibniz o Euler, se planteó un objetivo más modesto: demostrar que las ecuaciones algebraicas tienen siempre solución en el cuerpo de los números complejos. El primer intento serio de prueba de este resultado, que se conoce como «Teorema Fundamental del Álgebra», se debe a D'Alembert, en 1746, siendo Gauss el primero en lograr una prueba correcta, en 1799. Sin embargo, la aparición del nuevo método de integración de funciones racionales por descomposición en fracciones simples, de Leibniz y Jean Bernouilli, hizo resurgir el interés por la resolución de ecuaciones algebraicas mediante radicales. El noruego Abel creyó ser capaz de resolver, en 1824, por radicales, la ecuación general de 5° grado. Sin embargo, tras comprobar su error, pugnó por probar su imposibilidad. En 1826 probó algo más: la imposibilidad de resolver por radicales las ecuaciones generales de grado superior a 4. Su trabajo lo completó el francés Galois al caracterizar la víspera de su muerte en duelo de honor, en 1831, cuando contaba 21 años, aquellas ecuaciones que son resolubles por radicales. Con ser importantes los resultados de Abel y Galois, aún lo era más el método utilizado, pues recurrieron a las nociones de cuerpo y de grupo, aunque no las nombrasen. A partir de entonces, los algebristas desplazaron su objetivo desde las ecuaciones algebraicas hasta el estudio de las operaciones sobre conjuntos. Había nacido el álgebra moderna.

6.1. Los números complejos

Si $(K, +, ., \leq)$ es un cuerpo ordenado, dado un elemento $x \in K$, con $x \neq 0$, pueden pasar dos cosas, puesto que el orden es total:

1. $x > 0$. Entonces, por la compatibilidad del orden con el producto, se tiene $x^2 = xx > 0$.
2. $x < 0$. Como $-x > 0$, de nuevo $x^2 = (-x)(-x) > 0$.

En consecuencia, cualquiera que sea $x \in K$, se tiene $x^2 \geq 0$ (así como $x^{2n} \geq 0$ para todo $n \in \mathbb{N}$). De aquí se sigue que $x^2 + 1 = 0$ no tiene solución en ningún cuerpo ordenado.

La extensión del campo de los números reales al campo de los complejos se realiza con la pretensión de que la ecuación $x^2 + 1 = 0$ tenga solución. Por lo tanto, podemos aspirar a que los complejos formen un cuerpo, pero –a cambio de ello– habrá que renunciar a que sea, además, cuerpo ordenado. Se rompe así la cadena de las sucesivas extensiones de los conjuntos numéricos con ganancia de propiedades algebraicas ($\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$) o de orden ($\mathbb{Q} \subset \mathbb{R}$). Como compensación, lo que se consigue en la extensión $\mathbb{R} \subset \mathbb{C}$ es que cualquier ecuación algebraica (y no solamente $x^2 + 1 = 0$) tenga solución, resultado (Teorema Fundamental del Álgebra) de suma importancia que, curiosamente, no puede ser demostrado con herramientas puramente algebraicas.

Supongamos que existe un cuerpo $(K, +, .)$ que contiene a $\mathbb{R}$ como subcuerpo y tal que $x^2 + 1 = 0$ tiene solución en K. Sea $i \in K$ tal que $i^2 + 1 = 0$, es decir, $i^2 = -1$. Desde luego, si a y b son dos números reales, también son

elementos de K y $a + bi \in K$. Es muy fácil operar con los elementos de K de esta forma. En efecto,

$$(a + bi) + (c + di) = (a + c) + (b + d)\, i \tag{6.1}$$

y

$$(a + bi)\,(c + di) = (ac - bd) + (ad + bc)\, i. \tag{6.2}$$

Es más, si $a + bi \neq 0$, su elemento inverso debería ser

$$(a + bi)^{-1} = \frac{a - bi}{(a + bi)\,(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

Veremos a continuación que existe tal cuerpo K.

Definición 6.1. *Llamamos* ***números complejos*** *a los vectores del plano cartesiano* $\mathbb{R}^2 = \mathbb{C}$, *y sobre este conjunto se definen dos operaciones binarias, llamadas suma y producto, que están inspiradas en* (6.1) y (6.2):

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

y

$$(a, b)\,(c, d) = (ac - bd, ad + bc)\,.$$

Proposición 6.1. $(\mathbb{C}, +, .)$ *es un cuerpo en el que la ecuación* $x^2 + 1 = 0$ *tiene solución. Además, la aplicación de* $\mathbb{R}$ *en* $\mathbb{C}$ *que asocia a cada número real* x *el número complejo* $(x, 0)$ *es un monomorfismo de cuerpos.*

Demostración. La prueba es un mero ejercicio. Los neutros son $(0, 0)$ y $(1, 0)$, mientras que el opuesto de (a, b) es $(-a, -b)$ y su inverso es

$$\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right),$$

siempre que $(a, b) \neq (0, 0)$. Se comprueba, por último, que $(0, 1)$ es solución de $x^2 + 1 = 0$ y que la aplicación $f(x) = (x, 0)$ preserva la suma y el producto. □

Como de costumbre, $\mathbb{R}$ se identifica con su imagen por el monomorfismo f, es decir, con el conjunto $\{(x, 0)\,,\, x \in \mathbb{R}\}$, llamado **eje real**. Por analogía, el conjunto $\{(0, y)\,,\, y \in \mathbb{R}\}$ recibe el nombre de **eje imaginario**. Es costumbre escribir $(x, 0)$ o x indistintamente. También es costumbre representar el par $(0, 1) \in \mathbb{C}$ por i (**unidad imaginaria**), por lo que $i^2 = -1$. De esa forma encontramos la **forma binómica** de un número complejo,

$$(a, b) = (a, 0) + (b, 0)\,(0, 1) = a + bi,$$

denominándose a $a = \text{Re}\,(z)$ la **parte real** y a $b = \text{Im}\,(z)$ la **parte imaginaria** de ese número complejo z. El punto (a, b) del plano cartesiano se llama **afijo** del número complejo $a + bi$. Los complejos cuyo afijo se encuentra sobre el eje imaginario se llaman **imaginarios puros**. En otras palabras, los imaginarios puros son los complejos cuya parte real es nula.

La interpretación de la suma de complejos es obvia: se trata de la suma de vectores en el plano (véase Figura 6.1). Si los vectores están alineados, entonces el paralelogramo degenera (y la suma también está alineada).

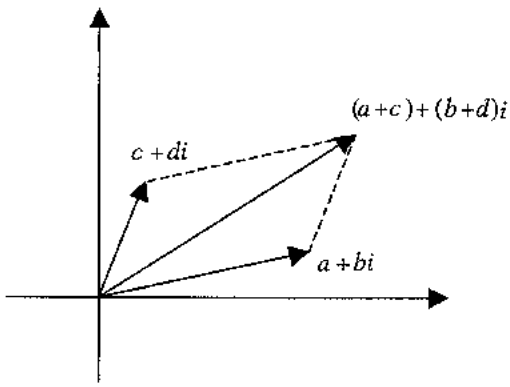

Figura 6.1. *Los afijos de los sumandos forman un paralelogramo con el origen y el afijo de la suma.*

La interpretación geométrica del producto de números complejos no es tan evidente (no tiene nada que ver con el producto escalar de vectores del plano). De hecho, debemos introducir algunos conceptos previamente.

Definición 6.2. *El **módulo** del número complejo $a + bi$ es la distancia entre el origen de coordenadas y el afijo del número o, si se prefiere, la longitud del vector (a, b). En otras palabras, como consecuencia del Teorema de Pitágoras, el módulo de $a + bi$ es el número real*

$$|a + bi| = \sqrt{a^2 + b^2}\,.$$

*El **conjugado** del número complejo $z = a + bi$ es $\bar{z} = a - bi$.*

Es fácil observar que $z + \bar{z} = 2\,\text{Re}\,(z)$ y que $z - \bar{z} = 2\,\text{Im}\,(z)$.

El lector comprobará fácilmente las siguientes propiedades de un número complejo z:

1. $0 \leq |z| \leq |\text{Re}\,(z)| + |\text{Im}\,(z)|$.
2. $|z| = 0$ si, y sólo si, $z = 0$.
3. $|-z| = |z|$.
4. $|\bar{z}| = |z|$.
5. $z\bar{z} = |z|^2$ (real no negativo).

Además, dados dos números complejos z_1 y z_2, se cumplen las siguientes propiedades:

6. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
7. $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.
8. $|z_1 + z_2| \leq |z_1| + |z_2|$ (propiedad triangular).

En efecto, para la propiedad triangular, si $z_1 = a + bi$ y $z_2 = c + di$, entonces $|z_1|$ y $|z_2|$ son las longitudes de dos lados no paralelos del paralelogramo de la Figura 6.1, mientras que $|z_1 + z_2|$ es la longitud de su diagonal. Puede aplicarse entonces la propiedad de los triángulos que afirma que la longitud de un lado es siempre menor que la suma de las correspondientes a los otros dos lados.

El módulo que hemos definido en $\mathbb{C}$ desempeña un papel semejante al del valor absoluto en los cuerpos ordenados, definiéndose la distancia entre z_1 y z_2 como $|z_1 - z_2|$ (véase Figura 6.2).

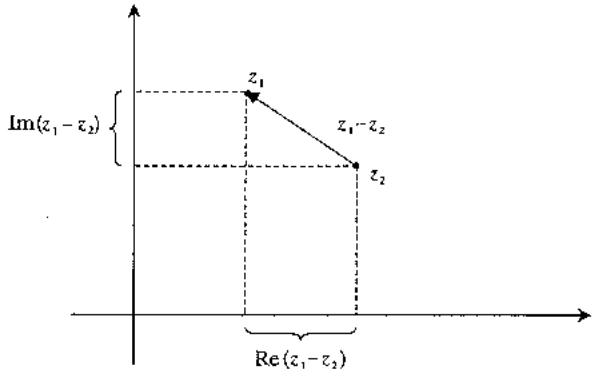

Figura 6.2. *Distancia entre (los afijos de) los complejos z_1 y z_2.*

Esto nos posibilita trabajar con sucesiones de la misma forma que en $\mathbb{Q}$ o en $\mathbb{R}$, a pesar de que $\mathbb{C}$ no es un cuerpo ordenado. Así, diremos que una sucesión de números complejos $\{z_n\}$ es de **Cauchy** cuando para cada $\varepsilon \in \mathbb{R}^+$, $|z_n - z_m| < \varepsilon$ finalmente. Análogamente, diremos que $\{z_n\}$ es **convergente** en $\mathbb{C}$ si existe algún $z \in \mathbb{C}$ tal que para todo $\varepsilon \in \mathbb{R}^+$, $|z_n - z| < \varepsilon$ finalmente.

Es fácil probar que toda sucesión convergente en $\mathbb{C}$ es de Cauchy (la demostración es idéntica a la de la Proposición 5.1). En el cuerpo $\mathbb{C}$, al igual que en $\mathbb{R}$, vale también el recíproco:

Teorema 6.1. *Toda sucesión de Cauchy de números complejos es convergente en $\mathbb{C}$.*

Demostración. Sea $\{z_n\}$ una sucesión de números complejos y consideremos las dos sucesiones de números reales $\{\mathrm{Re}\,(z_n)\}$ y $\{\mathrm{Im}\,(z_n)\}$. Como $\{z_n\}$ es de Cauchy, para $\varepsilon \in \mathbb{R}^+$ existe $n_\varepsilon \in \mathbb{N}$ tal que $|z_n - z_m| < \varepsilon$ cualesquiera que sean $n, m \geq n_\varepsilon$. Teniendo en cuenta que

$$\begin{aligned} |z_n - z_m| &= \sqrt{(\mathrm{Re}\,(z_n - z_m))^2 + (\mathrm{Im}\,(z_n - z_m))^2} \\ &= \sqrt{(\mathrm{Re}\,(z_n) - \mathrm{Re}\,(z_m))^2 + (\mathrm{Im}\,(z_n) - \mathrm{Im}\,(z_m))^2}, \end{aligned}$$

se tiene que

$$|\mathrm{Re}\,(z_n) - \mathrm{Re}\,(z_m)| = \sqrt{(\mathrm{Re}\,(z_n) - \mathrm{Re}\,(z_m))^2} \leq |z_n - z_m| < \varepsilon\,,$$

y

$$|\mathrm{Im}\,(z_n) - \mathrm{Im}\,(z_m)| = \sqrt{(\mathrm{Im}\,(z_n) - \mathrm{Im}\,(z_m))^2} \leq |z_n - z_m| < \varepsilon\,,$$

cualesquiera que sean $n, m \geq n_\varepsilon$. Así pues, ambas sucesiones de números reales son sucesiones de Cauchy en $\mathbb{R}$ y, por lo tanto, convergentes en $\mathbb{R}$. Si $\lim\limits_{n\to\infty} \mathrm{Re}\,(z_n) = a \in \mathbb{R}$ y $\lim\limits_{n\to\infty} \mathrm{Im}\,(z_n) = b \in \mathbb{R}$, probaremos que

$$\lim_{n\to\infty} z_n = a + ib \in \mathbb{C}.$$

En efecto

$$\begin{aligned} |z_n - (a+ib)| &= |(\mathrm{Re}\,(z_n) - a) + i\,(\mathrm{Im}\,(z_n) - b)| \\ &\leq |\mathrm{Re}\,(z_n) - a| + |\mathrm{Im}\,(z_n) - b| \end{aligned}$$

y cada sumando es tan pequeño como uno quiera con tal de que n sea suficientemente grande. □

Si bien el cuerpo $\mathbb{C}$ no es ordenado, es completo en el sentido de Cauchy.

6.2. Formas polar y exponencial

La Figura 6.3 muestra que los afijos de z y de su opuesto, $-z$, son simétricos respecto del origen, mientras que el afijo de z y el de su conjugado, $\bar{z}$, son simétricos respecto del eje real.

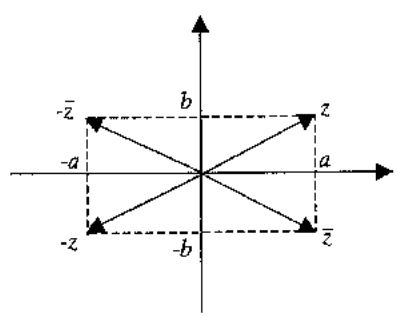

Figura 6.3. *Los afijos de un complejo, de su conjugado y de sus respectivos opuestos forman siempre un rectángulo.*

Si $z \in \mathbb{C}$, $z \neq 0$, entonces $\left|\frac{z}{|z|}\right| = 1$, por lo que el afijo de $\frac{z}{|z|}$ pertenece a la circunferencia unidad. Por lo tanto, $\frac{z}{|z|}$ se puede escribir en la forma $(\cos\varphi, \operatorname{sen}\varphi)$, siendo φ el ángulo entre el semieje positivo horizontal y el vector z (véase Figura 6.4).

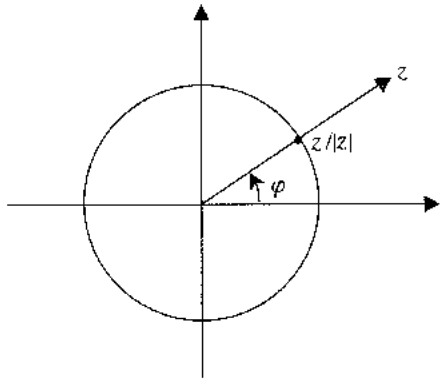

Figura 6.4. *Determinación gráfica del argumento de z.*

Se dice entonces que φ es un **argumento** de z, y se escribe $\varphi = \arg(z)$. A decir verdad, esta notación (que cuenta con una tradición de siglos) es abusiva, por cuanto podemos reemplazar φ por cualquier número real de la forma $\varphi + 2k\pi$, con $k \in \mathbb{Z}$. Por lo tanto, arg no es una aplicación de $\mathbb{C}\setminus\{0\}$ en $\mathbb{R}$, sino en el grupo cociente $(\mathbb{R}/2\pi\mathbb{Z}, +)$ (véase Ejercicio 3.7 de la Sección 3.2). Por eso, sería más coherente escribir $\varphi \in \arg(z)$ que $\varphi = \arg(z)$.

Pues bien, si $\varphi = \arg(z)$, entonces

$$z = |z|(\cos\varphi + i\operatorname{sen}\varphi)$$

es la **forma polar o trigonométrica** de z.

La forma polar permite interpretar geométricamente el producto y el cociente de los números complejos.

Proposición 6.2. *(i) El módulo del producto de dos números complejos es el producto de sus módulos, y el argumento del producto es la suma de sus argumentos.*

(ii) El módulo del cociente de un número complejo por otro no nulo es el cociente de sus módulos, y el argumento del cociente es la diferencia de sus argumentos.

Demostración. Consideremos los números complejos

$$z_1 = |z_1|(\cos\varphi_1 + i\operatorname{sen}\varphi_1) \quad \text{y} \quad z_2 = |z_2|(\cos\varphi_2 + i\operatorname{sen}\varphi_2).$$

(i) Efectuando el producto, tenemos

$$z_1 z_2 = |z_1|\,|z_2|\,(\cos\varphi_1 + i\,\mathrm{sen}\,\varphi_1)\,(\cos\varphi_2 + i\,\mathrm{sen}\,\varphi_2)$$

$$= |z_1|\,|z_2|\,[(\cos\varphi_1\cos\varphi_2 - \mathrm{sen}\,\varphi_1\,\mathrm{sen}\,\varphi_2) + (\mathrm{sen}\,\varphi_1\cos\varphi_2 + \cos\varphi_1\,\mathrm{sen}\,\varphi_2)\,i]$$

$$= |z_1|\,|z_2|\,[\cos\,(\varphi_1 + \varphi_2) + i\,\mathrm{sen}\,(\varphi_1 + \varphi_2)]\,.$$

(ii) De forma semejente, si $z_2 \neq 0$, tenemos

$$\begin{aligned}\frac{z_1}{z_2} &= \frac{|z_1|\,(\cos\varphi_1 + i\,\mathrm{sen}\,\varphi_1)}{|z_2|\,(\cos\varphi_2 + i\,\mathrm{sen}\,\varphi_2)}\\ &= \frac{|z_1|}{|z_2|}\,(\cos\varphi_1 + i\,\mathrm{sen}\,\varphi_1)\,(\cos\varphi_2 - i\,\mathrm{sen}\,\varphi_2)\\ &= \frac{|z_1|}{|z_2|}\,[\cos\,(\varphi_1 - \varphi_2) + i\,\mathrm{sen}\,(\varphi_1 - \varphi_2)]\,.\end{aligned}$$

La conclusión es inmediata. □

Junto con las formas vectorial, binómica y polar de un número complejo conviene considerar una cuarta forma que resulta útil para calcular potencias y raíces de números complejos. La motivación hay que buscarla en los desarrollos en serie de ciertas funciones bien conocidas. En análisis matemático se demuestra (a partir de la fórmula de Taylor en el origen, también llamada fórmula de McLaurin) que

$$\begin{aligned}e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots,\\ \cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots \quad \text{y}\\ \mathrm{sen}\,x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots \quad ,\end{aligned}$$

cualquiera que sea $x \in \mathbb{R}$. Si sustituimos formalmente x por el imaginario puro $i\varphi$ se obtiene, mediante manipulaciones no menos formales, la llamada **Fórmula de Euler**:

$$\begin{aligned}e^{i\varphi} &= 1 + i\varphi + \frac{(i\varphi)^2}{2!} + \frac{(i\varphi)^3}{3!} + \frac{(i\varphi)^4}{4!} + \frac{(i\varphi)^5}{5!} + \cdots\\ &= 1 + i\varphi - \frac{\varphi^2}{2!} - \frac{i\varphi^3}{3!} + \frac{\varphi^4}{4!} + \frac{i\varphi^5}{5!} - \frac{\varphi^6}{6!} - \cdots\\ &= \cos\varphi + i\,\mathrm{sen}\,\varphi.\end{aligned}$$

Este argumento no es, desde luego, una prueba. Sin embargo, con esa motivación definimos

$$e^{i\varphi} := \cos\varphi + i \operatorname{sen}\varphi,$$

para $\varphi \in \mathbb{R}$, de tal forma que podemos escribir, para todo complejo $z = |z|(\cos\varphi + i \operatorname{sen}\varphi)$,

$$z = |z| e^{i\varphi},$$

que es la **forma exponencial** de un número complejo. De la fórmula de Euler se sigue que

$$e^{\pi i} + 1 = 0,$$

curiosa identidad que relaciona los cinco números más importantes en matemáticas: 0, 1, i, π y e.

Como en el caso de los números reales, $s \in \mathbb{C}$ es una **raíz n-ésima** de $z \in \mathbb{C}$ si $s^n = z$. Veremos que todo número complejo no nulo tiene exactamente n raíces distintas, por lo que evitaremos escribir $\sqrt[n]{z}$ (salvo que z sea un número real no negativo). El siguiente resultado proporciona, además, la deseada interpretación geométrica de potencias y raíces de números complejos.

Proposición 6.3. *Sea $z = |z| e^{i\varphi}$ un complejo dado y $n \in \mathbb{N}$. Se cumple:*

(i) $z^n = |z|^n e^{in\varphi}$.
(ii) Si $z \neq 0$, entonces z tiene exactamente n raíces n-ésimas, que son

$$\sqrt[n]{|z|} e^{i\left(\frac{\varphi+2k\pi}{n}\right)}, \quad k = 0, 1, \ldots, n-1.$$

Demostración. (*i*) Por la Proposición 6.2 (*i*),

$$z^2 = |z|^2 (\cos 2\varphi + i \operatorname{sen} 2\varphi) = |z|^2 e^{i2\varphi}.$$

La prueba se completa por inducción sobre n.

(*ii*) Empezaremos viendo que tales números complejos son raíces n-ésimas de z. En efecto, de acuerdo con (*i*) se tiene

$$\left[\sqrt[n]{|z|} e^{i\left(\frac{\varphi+2k\pi}{n}\right)}\right]^n = \left[\sqrt[n]{|z|}\right]^n e^{in\left(\frac{\varphi+2k\pi}{n}\right)} = |z| e^{i(\varphi+2k\pi)} = |z| e^{i\varphi} = z.$$

Para ver que esas n raíces de z son distintas dos a dos efectuaremos su cociente de acuerdo con la Proposición 6.2 (*ii*). Dados $0 \leq k_1 < k_2 \leq n-1$,

$$\frac{\sqrt[n]{|z|} e^{i\left(\frac{\varphi+2k_1\pi}{n}\right)}}{\sqrt[n]{|z|} e^{i\left(\frac{\varphi+2k_2\pi}{n}\right)}} = \cos\left(\frac{2(k_1-k_2)\pi}{n}\right) + i \operatorname{sen}\left(\frac{2(k_1-k_2)\pi}{n}\right) \neq 1$$

puesto que $(k_1 - k_2)/n \notin \mathbb{Z}$.

Terminaremos probando que cualquier otra raíz n-ésima de z pertenece al conjunto considerado en (ii). En efecto, si $s = |s|\, e^{i\alpha}$ es raíz n-ésima de z, se deberá cumplir $s^n = z$, es decir, $|s|^n = |z|$ y $e^{in\alpha} = e^{i\varphi}$. Entonces,

$$\cos n\alpha = \cos\varphi \quad \text{y} \quad \operatorname{sen} n\alpha = \operatorname{sen}\varphi,$$

lo que implica $(n\alpha - \varphi)/2\pi \in \mathbb{Z}$. Supongamos que $(n\alpha - \varphi)/2\pi$ es congruente con k (módulo n) para cierto $k \in \{0, 1, \ldots, n-1\}$ (recuérdese el Ejercicio 4.2 de la Sección 4.1). En ese caso, podemos escribir

$$(n\alpha - \varphi)/2\pi = k + pn,$$

con $p \in \mathbb{Z}$, es decir,

$$\alpha = \frac{\varphi + 2k\pi}{n} + 2p\pi.$$

Entonces,

$$s = |s|\, e^{i\alpha} = \sqrt[n]{|z|}\, e^{i\left(\frac{\varphi + 2k\pi}{n}\right)},$$

que es uno de los n números complejos enumerados en (ii). □

Los afijos de las potencias sucesivas de $z = |z|\, e^{i\varphi}$ están situados sobre la curva del plano formada por los afijos de los números complejos $\left\{ |z|^t e^{it\varphi} \mid t \geq 1 \right\}$ (espiral de Arquímedes). Si $|z| > 1$ dicha curva se aleja del origen (véase Figura 6.5) y si $|z| < 1$ la curva se aproxima al origen sin alcanzarlo (véase Figura 6.6).

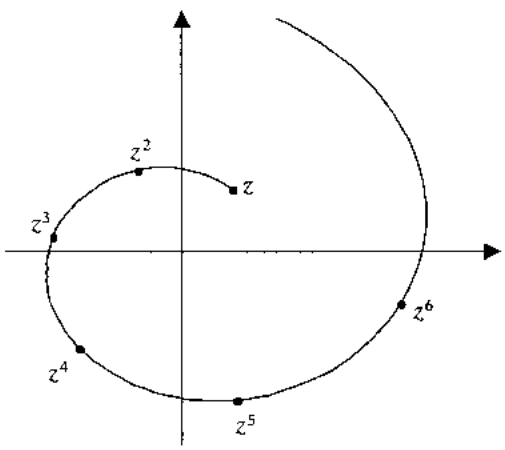

Figura 6.5. *Las espiras de la concha del ammonites aumentan su anchura de acuerdo con un factor constante, según observó Leonardo da Vinci. Este factor vale* $|z|^{2\pi} > 1$ *cuando* $|z| > 1$.

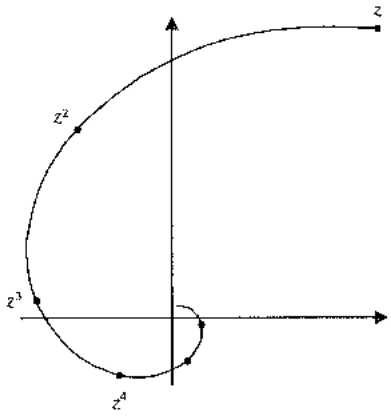

Figura 6.6. *Cuando* $|z| < 1$, *la espiral de Arquímedes se contrae con factor* $|z|^{2\pi} < 1$.

Como consecuencia de la Proposición 6.3, aunque el cuerpo $\mathbb{C}$ ha sido definido como una extensión de $\mathbb{R}$ en la cual -1 tiene raíces cuadradas, ahora sabemos que cualquier otro elemento de $\mathbb{C}$ tiene raíces n-ésimas en el propio $\mathbb{C}$ (¿cuáles son las raíces n-ésimas de 0?).

Ejemplo 6.1. La unidad tiene n raíces n-ésimas, cuyos afijos son los vértices del polígono regular de n lados inscrito en la circunferencia unidad. La posición de dicho polígono queda determinada por el hecho de que el propio 1 es una de esas raíces. Las Figuras 6.7 y 6.8 muestran las raíces cúbicas y las raíces cuartas de la unidad, respectivamente.

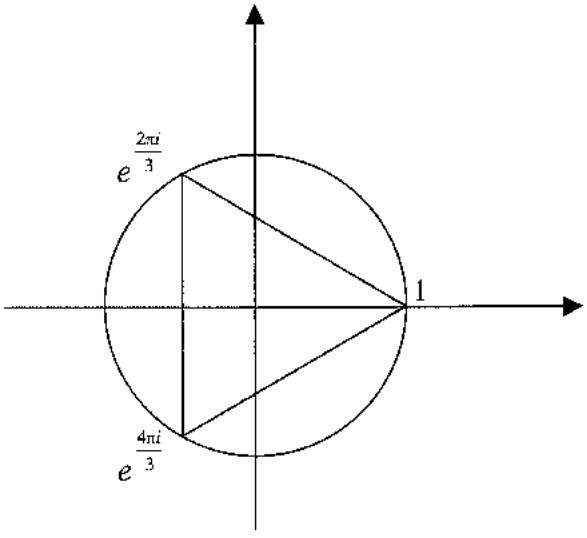

Figura 6.7. *Raíces cúbicas de* 1.

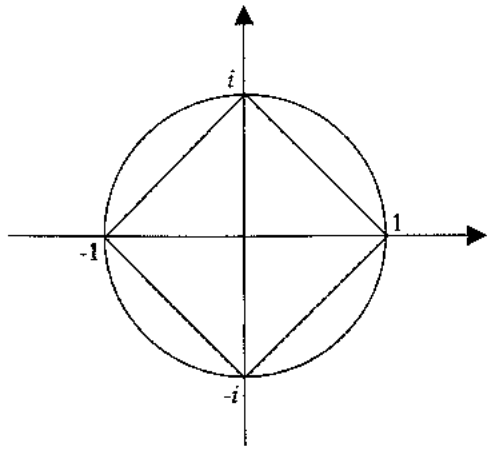

Figura 6.8. *Raíces cuartas de* 1.

6.3. Ecuaciones algebraicas con coeficientes complejos

Supongamos que $p(x)$ es un polinomio con coeficientes complejos, es decir, $p(x) \in \mathbb{C}[x]$. Decimos que $z \in \mathbb{C}$ es una **raíz** (o un **cero**) de $p(x)$ cuando z es una solución de la ecuación algebraica $p(x) = 0$, es decir, al evaluar el polinomio $p(x)$ en $x = z$ se obtiene el número complejo $p(z) = 0$. Esto es equivalente a afirmar que $p(x)$ es un múltiplo de $x - z$, según muestra el siguiente resultado.

Teorema 6.2. ***(del resto)*** *Sean $p(x)$ un polinomio y $z \in \mathbb{C}$. Entonces, z es raíz de $p(x)$ si, y sólo si, $(x - z)$ divide a $p(x)$.*

Demostración. Empezaremos suponiendo que z es una raíz de $p(x)$. Usando el algoritmo de la división (Teorema 4.1) existen polinomios (únicos) cociente y resto, $q(x)$ y $r(x)$, tales que

$$p(x) = (x - z)\, q(x) + r(x),$$

donde $\deg r(x) < \deg(x - z) = 1$ o bien $r(x)$ es el polinomio 0, lo que implica que el polinomio $r(x)$ es una constante, $r(x) = r \in \mathbb{C}$. En la ecuación anterior, evaluando para $x = z$, obtenemos

$$p(z) = (z - z)\, q(z) + r,$$

es decir, $r = 0$. Por lo tanto $p(x) = (x - z)\, q(x)$, como se quería.

El recíproco es inmediato. Si $p(x) = (x - z)\, q(x)$, entonces

$$p(z) = (z - z)\, q(z) = 0$$

y z es una raíz de $p(x)$. □

Observemos que se ha probado, incidentalmente, que

$$\deg q(x) = \deg p(x) - 1.$$

Si $p(x) = a_n x^n + \cdots + a_1 x + a_0$, los coeficientes del polinomio

$$q(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

pueden calcularse mediante la identificación de coeficientes o, lo que es lo mismo, utilizando el esquema conocido como **Regla de Ruffini**:

$$\begin{array}{c|cccccc}
 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\
z & - & zb_{n-1} & zb_{n-2} & \dots & zb_1 & zb_0 \\
\hline
 & b_{n-1} = a_n & b_{n-2} & b_{n-3} & \dots & b_0 & 0
\end{array}$$

Nótese que si los coeficientes de $p(x)$ son reales y z también lo es, el cociente de $p(x)$ por $x - z$ es un polinomio con coeficientes asimismo reales.

Enunciaremos ahora el **Teorema Fundamental del Álgebra**. Se conocen muchas demostraciones de este célebre teorema. En todas ellas se usan conceptos no algebraicos cuyo conocimiento está más allá del alcance de este texto.

Teorema 6.3. *(**de D'Alembert**) Todo polinomio de grado positivo con coeficientes complejos tiene al menos una raíz compleja.*

Como consecuencia del teorema anterior, y usando el Teorema del resto, obtendremos la descomposición de cualquier polinomio de grado positivo $p(x) \in \mathbb{C}[x]$ en factores **lineales** (de grado 1). En efecto, si $z_1 \in \mathbb{C}$ es una raíz de $p(x)$ podremos escribir $p(x) = (x - z_1)q_1(x)$. Si $\deg p(x) = n > 1$, $q_1(x)$ tendrá grado positivo y por ende una raíz compleja z_2. Procediendo así encontraremos n factores lineales de $p(x)$,

$$p(x) = (x - z_1)(x - z_2)\dots(x - z_n)q \tag{6.3}$$

con $q \in \mathbb{C}\setminus\{0\}$. Esto nos dice, entre otras cosas, que los únicos polinomios irreducibles en $\mathbb{C}[x]$ son los lineales. Obviamente, cada z_i $(i = 1, 2, \dots, n)$ es raíz de $p(x)$ pero pueden no ser diferentes entre sí.

Si un cuerpo K cumple lo afirmado para $\mathbb{C}$ en el Teorema de D'Alembert, es decir, si cualquier polinomio con coeficientes en K tiene al menos una raíz en K, se dice entonces que K es un **cuerpo algebraicamente cerrado**. Por lo que hemos visto, $\mathbb{C}$ es algebraicamente cerrado mientras que $\mathbb{R}$ no lo es.

Definición 6.3. *El número $z \in \mathbb{C}$ es una raíz de $p(x)$ de orden de **multiplicidad** $r \in \mathbb{N}$ si, y sólo si, existe un polinomio $q(x)$ tal que $p(x) = (x - z)^r q(x)$, con $q(z) \neq 0$.*

Se dice que z es **raíz simple** de $p(x)$ si su orden de multiplicidad es 1, es **raíz doble** si su orden de multiplicidad es 2, etc.

Corolario 6.1. *Todo polinomio de grado $n \geq 1$ con coeficientes complejos tiene exactamente n raíces complejas, contando cada una de ellas tantas veces como indique su multiplicidad. Con más precisión, si las raíces de un polinomio $p(x)$ son $z_1, \ldots, z_k$, con multiplicidades $r_1, \ldots, r_k$, respectivamente, entonces*

$$p(x) = a_n (x - z_1)^{r_1} \cdots (x - z_k)^{r_k},$$

siendo $r_1 + \cdots + r_k = n$ y a_n el coeficiente de x^n en $p(x)$. En particular, si $p(x) \in \mathbb{C}[x] \setminus \{0\}$, entonces $p(x)$ tiene finitas raíces complejas.

Demostración. Si en la descomposición en factores lineales (6.3) agrupamos los factores repetidos, y reordenando los índices, si fuera necesario, podremos escribir

$$p(x) = (x - z_1)^{r_1} (x - z_2)^{r_2} \ldots (x - z_k)^{r_k} q,$$

donde $q \in \mathbb{C} \setminus \{0\}$, $r_1 + r_2 + \ldots + r_k = n = \deg p(x)$ y todos los z_i $(i = 1, 2, \ldots, k)$ son diferentes entre sí. No es difícil ver que r_i es la multiplicidad de z_i. En efecto, para $i = 1$ por ejemplo,

$$\begin{aligned} p(x) &= (x - z_1)^{r_1} \left[(x - z_2)^{r_2} \ldots (x - z_k)^{r_k} q\right] \\ &= (x - z_1)^{r_1} q(x), \end{aligned}$$

y evaluando $q(x)$ en $x = z_1$,

$$q(z_1) = \left[(z_1 - z_2)^{r_2} \ldots (z_1 - z_k)^{r_k} q\right] \neq 0,$$

ya que $\mathbb{C}$ es íntegro.

Para terminar, comparando el coeficiente de x^n en ambos miembros de (6.3) se concluye que la constante q es precisamente a_n. Se obtiene entonces

$$p(x) = a_n (x - z_1)^{r_1} \cdots (x - z_k)^{r_k},$$

que es la conclusión deseada. □

El Teorema Fundamental del Álgebra afirma la existencia de solución compleja para toda ecuación algebraica. Saber calcularla es otra cosa. Si la ecuación es lineal la solución es inmediata (por ser $\mathbb{C}$ un cuerpo). Si la ecuación es **cuadrática** (o de segundo grado), basta recurrir al conocido método de la **completación de cuadrados**. En efecto, sea $p(x) = ax^2 + bx + c$, con $a \neq 0$, b y c complejos. Se tiene

$$\begin{aligned} ax^2 + bx + c &= a\left[x^2 + \frac{b}{a}x + \frac{c}{a}\right] \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right]; \end{aligned}$$

donde el número complejo $\Delta = b^2 - 4ac$ es el **discriminante** de la ecuación. Entonces x es solución de la ecuación si, y sólo si, $x+b/2a$ es una raíz cuadrada del número complejo $\Delta/4a^2$. Como todo número complejo no nulo tiene exactamente dos raíces cuadradas, lo mismo ocurre con las ecuaciones de 2º grado con coeficientes complejos siempre que $\Delta \neq 0$. Si $\Delta = 0$, entonces $x = -b/2a$ es raíz doble de la ecuación.

Dada una ecuación cúbica, podemos suponer sin merma de generalidad que el coeficiente de x^3 es 1. Sea pues

$$x^3 + bx^2 + cx + d = 0$$

la ecuación dada. Haciendo un primer cambio de variables, $x = y - b/3$, la nueva ecuación (en la variable y) carece de término de 2º grado (la fórmula del binomio de Newton es válida para cualquier anillo conmutativo). Supongamos por lo tanto que la nueva ecuación tiene la forma

$$y^3 + \beta y + \gamma = 0.$$

Un segundo cambio de variables, $y = z - \dfrac{\beta}{3z}$, proporciona la ecuación

$$z^3 - \frac{\beta^3}{27z^3} + \gamma = 0.$$

Finalmente, un tercer cambio de variables, $u = z^3$ conduce a la ecuación de segundo grado

$$u^2 + \gamma u - \frac{\beta^3}{27} = 0.$$

Cada valor de u proporciona tres valores para z; cada valor de z proporciona un valor para y; por último, a cada valor de y le corresponde un único valor de x. Así, el método proporcionará 6 posibles raíces de la ecuación, la mitad de las cuales deberán ser descartadas.

Las ecuaciones de cuarto grado se resuelven de forma semejante. Primero se hace desaparecer el término de tercer grado mediante un cambio de variables lineal. La ecuación resultante se escribe como diferencia de cuadrados, expresión en la que aparece un parámetro que se calcula de tal forma que el sustraendo, que es un polinomio de segundo grado, tenga discriminante nulo. Para hallar tal parámetro hay que resolver una ecuación cúbica auxiliar que se llama *resolvente*. Cada una de las tres raíces de la resolvente proporciona, finalmente, una ecuación de 2º grado. El proceso no es especialmente difícil, pero sí tedioso.

6.4. Ecuaciones algebraicas con coeficientes reales

Toda ecuación algebraica con coeficientes en $\mathbb{R}$ puede considerarse también como una ecuación algebraica con coeficientes complejos. Lo que ocu-

rre es que, para tales ecuaciones, suelen interesar tan sólo las soluciones reales. Las ecuaciones lineales tienen, desde luego, solución real única. Las cuadráticas, $ax^2+bx+c=0$, tienen solución real si, y sólo si, el discriminante es no negativo, en cuyo caso las raíces cuadradas de $\Delta/4a^2$ son $\pm\sqrt{\Delta}/2a$. Se obtiene así la expresión, tan conocida, para las raíces de una ecuación de 2º grado con coeficientes reales:

$$x=\frac{-b\pm\sqrt{\Delta}}{2a}.$$

Si $\Delta<0$, entonces es fácil ver que las soluciones complejas vienen dadas por la expresión

$$x=-\frac{b}{2a}\pm\frac{\sqrt{-\Delta}}{2a}i,$$

por lo que ambas raíces resultan ser complejos conjugados. En realidad esta regla es completamente general.

Proposición 6.4. *Si un número complejo es raíz de un polinomio con coeficientes reales, entonces su conjugado también lo es.*

Demostración. La clave de la prueba está en las buenas propiedades de la conjugación respecto de la suma y el producto ($f(z)=\overline{z}$ es un automorfismo del cuerpo $\mathbb{C}$) y en que $f(a)=a$ cuando $a\in\mathbb{R}$. Sea

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

un polinomio con coeficientes reales, y supongamos que $p(z)=0$ para $z\in\mathbb{C}$. Entonces

$$\begin{aligned}p(\overline{z}) &= a_n\overline{z}^n+\cdots+a_1\overline{z}+a_0\\ &= a_nf(z^n)+\cdots+a_1f(z)+a_0\\ &= f(a_nz^n)+\cdots+f(a_1z)+f(a_0)\\ &= f(p(z))=f(0)=\overline{0}=0\end{aligned}$$

Así pues, $p(\overline{z})=0$, por lo que $\overline{z}$ es también raíz de $p(x)$. □

Corolario 6.2. *Todo polinomio con coeficientes reales se puede escribir como producto de factores lineales y de factores cuadráticos, todos ellos con coeficientes reales. En consecuencia, cada raíz de tales polinomios tiene el mismo orden de multiplicidad que la de su conjugado.*

Demostración. Sean $z_1,\ldots,z_n$ las raíces complejas (posiblemente repetidas) del polinomio

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{R}[x].$$

Podemos reordenarlas dejando las raíces reales al final, de tal forma que $\{z_1, \ldots, z_m\}$ no sean reales mientras que las raíces reales son $\{z_{m+1}, \ldots, z_n\}$. Como consecuencia de la Proposición 6.4 podemos igualmente suponer (reordenando nuevamente si es menester) que $\overline{z_1} = z_2$, $\overline{z_3} = z_4, \ldots \overline{z_{m-1}} = z_m$. De acuerdo con el Corolario 6.1, podemos escribir

$$p(x) = a_n (x - z_1)(x - z_2) \ldots (x - z_{m-1})(x - z_m)(x - z_{m+1}) \ldots (x - z_n).$$

Tomando cualquier par de factores consecutivos $(x - z_{k-1})(x - z_k)$ con k par, $k \leq m$ se tiene que

$$\begin{aligned}(x - z_{k-1})(x - z_k) &= (x - z_k)(x - \overline{z_k}) \\ &= x^2 - (z_k + \overline{z_k})x + z_k\overline{z_k} \\ &= x^2 - 2\operatorname{Re}(z_k)x + |z_k|^2,\end{aligned}$$

que es un polinomio de 2º grado con coeficientes reales. Obtenemos así la descomposición del enunciado para $p(x)$:

$$a_n \left(x^2 - 2\operatorname{Re}(z_2)x + |z_2|^2\right) \ldots \left(x^2 - 2\operatorname{Re}(z_m)x + |z_m|^2\right)(x - z_{m+1}) \ldots (x - z_n).$$

Además, cada factor cuadrático tiene dos raíces que son complejos conjugados entre sí, por lo que el orden de multiplicidad es el mismo para cualquier raíz de $p(x)$ y su correspondiente conjugado. □

Los resultados que anteceden ayudan poco a calcular las raíces reales de una ecuación algebraica con coeficientes reales. Como en muchas aplicaciones las ecuaciones tienen coeficientes racionales (o enteros, al multiplicar por un múltiplo común de los denominadores de los coeficientes) conviene dar reglas que permitan hallar algebraicamente soluciones enteras y racionales. De no ser así, las raíces deberán ser aproximadas mediante métodos numéricos (como el método iterativo de Newton).

Proposición 6.5. *Sea $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ un polinomio con coeficientes enteros y sea α una raíz. Entonces,*

(i) si α es entero, α divide a a_0; y

(ii) si $\alpha = \dfrac{p}{q}$, con $p \in \mathbb{Z}$ y $q \in \mathbb{N}$, números primos entre sí, entonces p divide a a_0 y q divide a a_n.

Demostración. (i) Como $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, se tiene

$$\alpha\left(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1\right) = -a_0.$$

La conclusión es inmediata.

(*ii*) Ahora tenemos

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0,$$

y, multiplicando por q^n,

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0.$$

De aquí se sigue que

$$p\left(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1}\right) = -a_0 q^n, \tag{6.4}$$

así como

$$q\left(a_{n-1}p^{n-1} + \cdots + a_1 pq^{n-2} + a_0 q^{n-1}\right) = -a_n p^n. \tag{6.5}$$

De (6.4) se deduce que p divide a a_0 (pues ninguno de sus factores primos puede estar en q^n al haber supuesto p y q primos entre sí). De forma semejante, (6.5) prueba que q divide a a_n. □

6.5. Problemas

Problema 6.1. Calcule $\dfrac{(1+i)^n}{(1-i)^{n-2}}$, expresando el resultado de todas las formas posibles.

Problema 6.2. Demuestre que $\left(\dfrac{1+i\tan\alpha}{1-i\tan\alpha}\right)^n = \dfrac{1+i\tan n\alpha}{1-i\tan n\alpha}$.

Problema 6.3. Calcule:

a) Las raíces cúbicas de i.
b) Las raíces cúbicas de $2+2i$.
c) Las raíces cuartas de -4.
d) Las raíces sextas de -27.

Problema 6.4. Analice la estructura algebraica del conjunto de las raíces n-ésimas de la unidad para la suma y el producto de números complejos.

Problema 6.5. Para $n = 3$, 4 y 6 se pide:

a) Halle las raíces n-ésimas de la unidad en forma polar.
b) Descomponga $x^n - 1$ en producto de factores de primer y segundo grado con coeficientes reales.

Problema 6.6. Resuelva la ecuación $(2+i)x^2 - (5-i)x + (2-2i) = 0$.

Problema 6.7. Resuelva el sistema de ecuaciones lineales

$$\left\{ \begin{array}{lcl} (2+i)x & + & (2-i)y & = & 6 \\ (3+2i)x & + & (3-2i)y & = & 8 \end{array} \right\}.$$

Problema 6.8. Resuelva la ecuación

$$2x^5 - 20x^4 + 70x^3 - 140x^2 + 248x - 240 = 0.$$

Problema 6.9. Resuelva las siguientes ecuaciones cúbicas mediante cambios de variables:

a) $x^3 - 6x + 9 = 0$.
b) $x^3 - 9x^2 + 36x - 80 = 0$.

Problema 6.10. Considérese la ecuación cuártica $x^4 + 2x^3 - 3x^2 + 2x + 1 = 0$. Se pide:

a) Pruebe que dicha ecuación carece de soluciones racionales.

*b)** Resuélvala utilizando el cambio de variables $y = x + \dfrac{1}{x}$. (Ayuda: Divida la ecuación inicial por x^2.)

Problema 6.11. Analice la forma de resolver las siguientes *ecuaciones simétricas*:

a) $ax^3 + bx^2 + bx + a = 0$.
b) $ax^4 + bx^3 + cx^2 + bx + a = 0$.
c) $ax^5 + bx^4 + cx^3 + cx^2 + bx + a = 0$.

Problema 6.12. Halle las raíces racionales de $15x^4 + x^3 + 13x^2 + x - 2 = 0$.

Problema 6.13. Resuelva la ecuación trigonométrica $\cos^3 x + \tan^2 x = \dfrac{25}{8}$.

Problema 6.14.* Sean $z_1, \ldots, z_n$ los ceros, posiblemente repetidos, del polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Pruebe las siguientes identidades (de Cardano-Viète):

a) $\displaystyle\sum_{1 \le i \le n} z_i = -\frac{a_{n-1}}{a_n}$;

b) $\displaystyle\sum_{1 \le i < j \le n} z_i z_j = \frac{a_{n-2}}{a_n}$;

c) $z_1 \ldots z_n = (-1)^n \dfrac{a_0}{a_n}$.

Problema 6.15. En el anillo de los polinomios con coeficientes reales, $\mathbb{R}[x]$, se considera el conjunto I de los múltiplos de $x^2 + 1$, es decir,

$$I = \left\{ \left(x^2 + 1\right) p(x) \mid p(x) \in \mathbb{R}[x] \right\}.$$

Se pide:

a) Pruebe que I es un ideal en $\mathbb{R}[x]$.

b) Halle un representante del polinomio $x^3 + 3x - 1$ cuyo grado sea menor que 2 para la RBE que I define sobre $\mathbb{R}[x]$.

c) Identifique los elementos del conjunto cociente $\mathbb{R}[x]/I$ y defina la suma y el producto en dicho conjunto con ayuda de los representantes de grado menor que 2.

d) Pruebe que existe un isomorfismo de cuerpo entre $\mathbb{C}$ y $\mathbb{R}[x]/I$ (para las operaciones habituales).

Problema 6.16.* Dado un cuerpo K y $p(x) \in K[x]$, se define la aplicación $\Phi(p) : K \longrightarrow K$ tal que $[\Phi(p)](\alpha)$ es $p(\alpha) \in K$, es decir, el resultado de sustituir x por α en $p(x)$. Pruebe que Φ es inyectiva cuando se toma $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, pero no lo es para $K = \mathbb{Z}_2$. (Ayuda: Recuérdese el Problema 4.16.)

Problema 6.17. Proponga ejemplos que muestren que la proposición: «Si $p \in K[x] \setminus \{0\}$, existe entonces un $\alpha \in K$ tal que $p(\alpha) \neq 0$» es válida o no según cual sea el cuerpo K considerado.

CAPÍTULO 7

EXTENSIONES DE CUERPOS Y SUS APLICACIONES

Los matemáticos griegos fueron grandes expertos en la resolución de problemas geométricos con la ayuda de la regla y el compás, según se refleja en los *Elementos* de Euclides. Hubo, sin embargo, tres problemas muy antiguos, de los que ya se tenía noticia en el siglo V a. de C., que se han resistido a ser resueltos –negativamente– hasta hace relativamente poco tiempo.

Cuenta la leyenda que los atenienses, deseosos de obtener la ayuda de los dioses para frenar una terrible plaga, enviaron una delegación a Delfos, donde se entrevistaron con el oráculo de Apolo. Como contrapartida, la delegación fue invitada a duplicar el volumen del altar cúbico de Apolo. Tomando como unidad de longitud la arista del altar, hubieran debido construir los atenienses un cubo de arista $\sqrt[3]{2}$ pero, en lugar de ello, cometieron el terrible error de duplicar la longitud de las aristas, desatando así la ira divina. Construir con regla y compás un segmento de longitud $\sqrt[3]{2}$ es el problema de la *duplicación del cubo*, también llamado *de Delfos*.

Es muy fácil bisecar un ángulo dado (véase Figura 7.1). También sabemos trisecar un ángulo de 180° o de 90°, pues sabemos cómo construir un ángulo que mide la tercera parte (60° o 30°), pero ¿podemos hacer lo mismo con un ángulo cualquiera? Este segundo problema es el de la *trisección del ángulo*.

En 1837 probó Wantzel la imposibilidad de resolver ambos problemas con la sola ayuda de la regla y el compás.

El tercer problema, la *cuadratura del círculo*, es tan famoso que se ha incorporado al lenguaje coloquial para referirse a algo imposible de conseguir. Se trata de construir un cuadrado de área igual al de un círculo dado. Tomando como unidad de longitud el radio del círculo debería construirse –con regla y compás– un segmento de longitud $\sqrt{\pi}$. Fue Lindemann quien cerró –también negativamente– este problema en 1877, inspirándose en el método utilizado por Hermite para probar, en 1873, la trascendencia del número e (que no es raíz de ningún polinomio con coeficientes enteros, al contrario de lo que ocurre con 0,1, i o $\sqrt[3]{2}$). La existencia de tales elementos había sido demostrada por Liouville en 1844, pero la clasificación de e y de π como trascendentes tuvo que esperar tres décadas más.

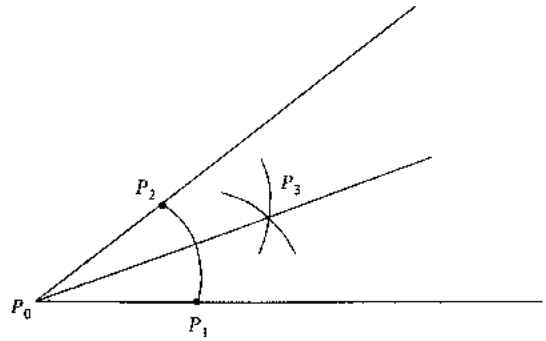

Figura 7.1. *Bisección del ángulo: Con centro en el origen común de las semirrectas, P_0, se traza una circunferencia de radio arbitrario que intersecta a las semirrectas en P_1 y P_2; con centro en P_1 y P_2 se trazan dos circunferencias de radio arbitrario que se cortan en $P_3 \neq P_0$; la recta determinada por P_0 y P_3 es la bisectriz buscada.*

Soluciones aproximadas de estos tres problemas, utilizando herramientas auxiliares, se han dado muchas a lo largo de la historia. Hoy, aunque se sabe con toda certeza que son irresolubles, siguen recibiéndose «soluciones» provenientes de matemáticos aficionados que se niegan a aceptar que las construcciones que proponen son necesariamente erróneas.

Los elementos matemáticos que se necesitan para demostrar la irresolubilidad de los dos primeros problemas son puramente algebraicos. El tercero, en cambio, requiere, además, el concurso del análisis matemático. La primera sección establece los mencionados preliminares algebraicos. Algunos de ellos corresponden a conceptos básicos acerca de espacios vectoriales (de los que el lector conoce al menos los espacios $\mathbb{R}^n$, con la suma definida por componentes y el producto de números reales por vectores que se obtiene al multiplicar por dicho número cada una de sus componentes). Será suficiente, sin embargo, considerar una clase especial de espacios vectoriales: las extensiones de cuerpos intercalados entre $\mathbb{Q}$ y $\mathbb{C}$. El hilo conductor del capítulo son las bases en dichos espacios vectoriales.

7.1. Extensiones de cuerpos

Hemos visto en capítulos anteriores que $\mathbb{Q}$ es un cuerpo para las operaciones suma y producto inducidas por la suma y el producto sobre el cuerpo $\mathbb{C}$. Decimos entonces que $\mathbb{Q}$ es un subcuerpo de $\mathbb{C}$ o que $\mathbb{C}$ es una **extensión** de $\mathbb{Q}$. Análogamente, el conjunto $F = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}$ es una extensión de $\mathbb{Q}$ (siempre para las operaciones inducidas por $\mathbb{C}$), mientras que $\mathbb{C}$, o bien $\mathbb{R}$, es asimismo una extensión de F (véase el Problema 5.2).

Definición 7.1. *Supongamos que $\mathbb{Q} \subset E \subset F \subset \mathbb{C}$, siendo F extensión de E (con lo que se sobreentiende que E y F son cuerpos para las operaciones inducidas por $\mathbb{C}$). Los elementos de E se llamarán* ***escalares*** *y los elementos de F* ***vectores****. Se definen los siguientes conceptos:*

Dado un conjunto finito de vectores $\{v_1, \ldots, v_n\}$ y otro de igual número de escalares $\{\alpha_1, \ldots, \alpha_n\}$, la expresión $\alpha_1 v_1 + \cdots + \alpha_n v_n$ define un único vector que es la ***combinación lineal*** *de $v_1, \ldots, v_n$ con coeficientes $\alpha_1, \ldots, \alpha_n$.*

Un conjunto finito de vectores $\{v_1, \ldots, v_n\}$ es ***linealmente dependiente*** *si existen escalares $\alpha_1, \ldots, \alpha_n$, no todos nulos, tales que $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$. Cuando no ocurre tal cosa se dice que $\{v_1, \ldots, v_n\}$ es* ***linealmente independiente****. Un conjunto infinito de vectores es linealmente independiente cuando lo son todos sus subconjuntos finitos.*

Un conjunto de vectores es un ***sistema generador*** *cuando todo elemento de F es combinación lineal de uno de sus subconjuntos finitos.*

Un conjunto de vectores es ***base*** *(de Hamel) de F si es un sistema generador linealmente independiente.*

Cuando se considera $\mathbb{Q}\left(\sqrt{3}\right) = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}$ como extensión de $\mathbb{Q}$, el conjunto de vectores $\left\{1, \sqrt{3}\right\}$ es base. Podría pensarse que cualquier extensión tiene al menos una base finita, pero no siempre ocurre tal cosa. En efecto, si $\{v_1, \ldots, v_n\}$ fuese una base para $\mathbb{R}$ como extensión de $\mathbb{Q}$, entonces

$$\mathbb{R} = \{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid (\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}^n\}.$$

Como card $(\mathbb{Q}^n) = \aleph_0$, $\mathbb{R}$ sería entonces a lo sumo numerable (cosa que no ocurre).

Supongamos ahora que el conjunto $X = \{v_i, i \in I\}$, donde el conjunto de índices I es posiblemente infinito, es una base de F, como extensión de E. Sea $v \in F$ un vector arbitrario no nulo. Veremos que hay una única forma de expresar v como combinación lineal de elementos de X.

Puesto que X es un sistema generador, v puede expresarse como combinación lineal de vectores de X. Supongamos que v puede expresarse como combinación lineal de dos subconjuntos finitos de X, que podemos escribir en la forma $\{v_i, i \in J\}$ y $\{v_i, i \in K\}$, donde J y K son subconjuntos finitos no vacíos de I. Sea $v = \sum_{i \in I} \alpha_i v_i$, con todos los $\alpha_i = 0$ salvo cuando $i \in J$, en cuyo caso $\alpha_i \neq 0$. Sea también $v = \sum_{i \in I} \beta_i v_i$, con $\beta_i \neq 0$ si, y sólo si, $i \in K$. Se tiene entonces (véase el diagrama de la Figura 7.2)

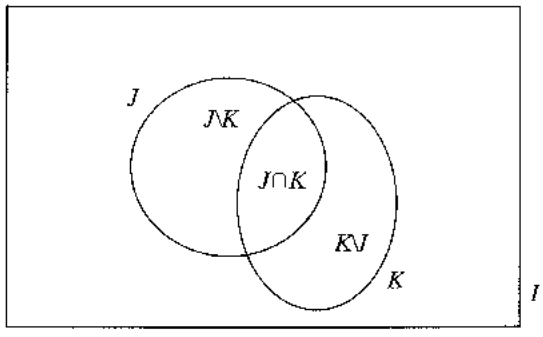

Figura 7.2. *Partición de $J \cup K$ en los subconjuntos $J \backslash K$, $K \backslash J$ y $J \cap K$.*

$$0 = v - v = \sum_{i \in J \setminus K} \alpha_i v_i + \sum_{i \in K \setminus J} (-\beta_i) v_i + \sum_{i \in J \cap K} (\alpha_i - \beta_i) v_i. \tag{7.1}$$

Como hemos supuesto que X es linealmente independiente, deberán ser cero todos los escalares que aparecen en (7.1). Esto solamente es posible si las dos primeras sumas carecen de sumandos, es decir, $J \setminus K = \emptyset$ y $K \setminus J = \emptyset$, y son cero todos los escalares que aparecen en la tercera suma. En otras palabras, deberá ocurrir que $J = K$ y que $\alpha_i = \beta_i$ para todo $i \in J = K$.

Se ha probado, por lo tanto, que cualquier vector no nulo se expresa de forma única como combinación lineal de los elementos de una base. Y esta afirmación es también cierta para el vector 0 como consecuencia de la independencia lineal de X. Estamos en condiciones de definir las componentes de un vector respecto de una base.

Definición 7.2. *Si $\{v_i, i \in I\}$ es una base de F, como extensión de E, y $v \in F$, los escalares únicos $\{\alpha_i, i \in I\}$ tales que $v = \sum_{i \in I} \alpha_i v_i$ (suma en realidad finita, por ser $\alpha_i \neq 0$ a lo sumo en un subconjunto finito de I) se denominan* ***componentes*** *de v respecto de dicha base.*

Lema 7.1. *Si F, como extensión de E, posee una base con n elementos, cualquier otro conjunto de F con más de n vectores es linealmente dependiente.*

Demostración. Sea $\{v_1, \ldots, v_n\}$ una base y sea $\{w_1, \ldots, w_p\} \subset F$, con $p > n$. Para $i = 1, \ldots, p$, denotamos por $\alpha_{i1}, \ldots, \alpha_{in}$ las componentes de w_i respecto de $\{v_1, \ldots, v_n\}$. Debemos probar que la ecuación

$$x_1 w_1 + \cdots + x_p w_p = 0 \tag{7.2}$$

tiene una solución $(x_1, \ldots, x_p) \in E^p$ que no es $(0, \ldots, 0)$.

Para empezar, (7.2) es equivalente a

$$\begin{aligned} 0 &= x_1 (\alpha_{11} v_1 + \cdots + \alpha_{1n} v_n) + \cdots + x_p (\alpha_{p1} v_1 + \cdots + \alpha_{pn} v_n) \\ &= (\alpha_{11} x_1 + \cdots + \alpha_{p1} x_p) v_1 + \cdots + (\alpha_{1n} x_1 + \cdots + \alpha_{pn} x_p) v_n. \end{aligned} \tag{7.3}$$

Además, teniendo en cuenta que $\{v_1, \ldots, v_n\}$ es linealmente independiente, (7.3) equivale al sistema

$$\left\{ \begin{array}{ccccccc} \alpha_{11} x_1 & + & \ldots & + & \alpha_{p1} x_p & = & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{1n} x_1 & + & \ldots & + & \alpha_{pn} x_p & = & 0 \end{array} \right\}. \tag{7.4}$$

Como (7.4) es un sistema homogéneo con más incógnitas que ecuaciones, es seguro que (7.4) posee soluciones no nulas (véase Problema 4.13). En consecuencia, lo mismo ocurrirá con (7.2). Concluimos que $\{w_1, \ldots, w_p\}$ es linealmente dependiente. □

Proposición 7.1. *Si F, como extensión de E, posee una base finita, entonces todas las bases de F tienen exactamente el mismo cardinal.*

Demostración. Sea $\{v_1, \ldots, v_n\} \subset F$ una base. Cualquier base infinita de F contendría un subconjunto de $n+1$ elementos. Como consecuencia del Lema 7.1, dicho subconjunto sería linealmente dependiente, siendo así que todos los subconjuntos finitos de una base son linealmente independientes. Por lo tanto, si una base es finita, también lo son todas las demás bases.

Sea $\{w_1, \ldots, w_p\}$ otra base finita. Por aplicación directa del Lema 7.1 deberá ser $p \leq n$. Intercambiando los papeles de $\{w_1, \ldots, w_p\}$ (tomado ahora como base) y $\{v_1, \ldots, v_n\}$, también deberá ser $n \leq p$. La conclusión es inmediata. □

Por ejemplo, todas las bases de $\mathbb{Q}\left(\sqrt{3}\right) = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}$, como extensión $\mathbb{Q}$, tienen 2 elementos.

Si F es una extensión de E que tiene una base finita, entonces el cardinal de cualquiera de sus bases se llama **dimensión de la extensión** y se denota por $[F : E]$.

Proposición 7.2. *Si G es una extensión de F con base finita y F es una extensión de E con base finita, entonces G es también una extensión de E con base finita y se cumple*

$$[G : E] = [G : F]\,[F : E]\,.$$

Demostración. Consideremos sendas bases de Hamel para F sobre E y para G sobre F. Denotémoslas por $\{a_i, i \in I\}$ y $\{b_j, j \in J\}$, respectivamente. El lector comprobará que $\{a_i b_j, (i,j) \in I \times J\}$ es una base de Hamel de G sobre E. □

Definición 7.3. *Se dice que $\alpha \in \mathbb{C}$ es **algebraico** sobre E, subcuerpo de $\mathbb{C}$, cuando existe un polinomio de $E[x]$ (anillo de los polinomios con coeficientes en E) del cual α es una raíz. En ese caso la **extensión algebraica** de E por α, que denotaremos por $E(\alpha)$, es la intersección de todos los subcuerpos de $\mathbb{C}$ que contienen al conjunto $E \cup \{\alpha\}$.*

*Se define el **grado de** α (algebraico sobre E) como el mínimo de los grados de los polinomios no nulos de $E[x]$ para los que α es una raíz.*

*Los elementos de $\mathbb{C}$ que no son algebraicos sobre E se dice que son **trascendentes** sobre E (cuando no se especifica el cuerpo se sobreentiende que $E = \mathbb{Q}$).*

Es fácil comprobar que $E(\alpha)$ es, efectivamente, una extensión de E. En particular, si $\alpha \in E$ es evidente que $E(\alpha) = E$. Por otro lado, si

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in E[x]$$

es un polinomio de grado mínimo entre aquellos que tienen a α como raíz, entonces $p(x)$ es irreducible y no tiene ninguna otra raíz en E (recuérdese el argumento del Teorema del resto). El polinomio **mónico** (con coeficiente 1 para la potencia de mayor grado)

$$\frac{p(x)}{a_n} = x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots + \frac{a_1}{a_n} x + \frac{a_0}{a_n}$$

se denomina **polinomio minimal** de α. Si hubiese dos polinomios minimales distintos para α la diferencia de ambos tendría grado inferior a n y α sería una raíz del mismo, lo cual es imposible. En consecuencia, el polinomio minimal de un elemento algebraico es único.

Volvamos al ejemplo que venimos arrastrando desde el comienzo de este capítulo: $\sqrt{3}$ es algebraico sobre $\mathbb{Q}$ y su polinomio minimal es $x^2 - 3$, por lo que el grado de $\sqrt{3}$ es 2.

Supongamos que $\alpha_1 \in \mathbb{C}$ es algebraico sobre E y que $\alpha_2 \in \mathbb{C}$ es algebraico sobre $E(\alpha_1)$. Entonces la extensión algebraica de E por α_1 y α_2 es $E(\alpha_1)(\alpha_2)$, que se denota, para simplificar, $E(\alpha_1, \alpha_2)$. Por inducción se define, análogamente, $E(\alpha_1, \ldots, \alpha_p)$, siempre que α_{k+1} sea algebraico sobre $E(\alpha_1, \ldots, \alpha_k)$, $k = 1, \ldots, p-1$.

Proposición 7.3. *Si $\alpha \in \mathbb{C}$ es algebraico sobre E y el grado de α es m, entonces $\{1, \alpha, \ldots, \alpha^{m-1}\}$ es base para $E(\alpha)$. Por lo tanto, $[E(\alpha) : E] = m$.*

Demostración. Desde luego, $\{1, \alpha, \ldots, \alpha^{m-1}\} \subset E(\alpha)$ es un conjunto linealmente independiente. El conjunto de las combinaciones lineales de dichas potencias de α con coeficientes en E constituyen un grupo conmutativo para la suma. Demostraremos que es un cuerpo.

Para ver que el producto de dos de dichas combinaciones lineales es un elemento del conjunto basta probar que toda potencia de α se puede escribir como combinación lineal de $1, \alpha, \ldots, \alpha^{m-1}$.

Si $h(x)$ es el polinomio minimal de α, con

$$h(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + x^m,$$

entonces

$$\alpha^m = -a_0 - a_1 \alpha - \cdots - a_{m-1} \alpha^{m-1}. \tag{7.5}$$

Por lo tanto,

$$\begin{aligned} \alpha^{m+1} &= \alpha\left(-a_0 - a_1\alpha - \cdots - a_{m-1}\alpha^{m-1}\right) \\ &= -a_0\alpha - a_1\alpha^2 - \cdots - a_{m-1}\alpha^m. \end{aligned} \tag{7.6}$$

Sustituyendo (7.5) en (7.6) se concluye que α^{m+1} es también una combinación lineal de $\{1, \alpha, \ldots, \alpha^{m-1}\}$. Por inducción, lo mismo ocurre en general. Así pues, el conjunto de todas las combinaciones lineales de $\{1, \alpha, \ldots, \alpha^{m-1}\}$ es un anillo unitario conmutativo.

Para terminar, bastará probar que, si

$$c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} \neq 0,$$

entonces

$$\frac{1}{c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1}} \tag{7.7}$$

es también un elemento del conjunto, es decir, una combinación lineal de $\{1, \alpha, \ldots, \alpha^{m-1}\}$.

Consideremos el polinomio $g(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1}$. Dado que $g(x)$ y $h(x)$ son primos entre sí (dado que $h(x)$ es irreducible y $\deg g(x) < \deg h(x)$), se puede aplicar el Teorema 4.2 (débil de Bezout) que asegura la existencia de polinomios $p(x)$ y $q(x)$, con coeficientes en E, tales que

$$p(x) g(x) + q(x) h(x) = 1.$$

Tomando $x = \alpha$, queda $p(\alpha) g(\alpha) = 1$, ya que $h(\alpha) = 0$. Por lo tanto, el complejo de (7.7) es $p(\alpha)$, que también es combinación lineal con coeficientes en E de $\{1, \alpha, \ldots, \alpha^{m-1}\}$. □

Corolario 7.1. *Si F es una extensión de E con base finita y $\alpha \in F$ es algebraico sobre E, entonces el grado de α divide a $[F : E]$.*

Demostración. Como el grado de la extensión F de E es finito y $E \subset E(\alpha)$, también es finito el grado de la extensión F de $E(\alpha)$. Aplicando la Proposición 7.2 tenemos

$$[F : E] = [F : E(\alpha)] [E(\alpha) : E],$$

siendo $[E(\alpha) : E]$ el grado de α en virtud de la Proposición 7.3. □

Proposición 7.4. *Si F es una extensión de E con base finita y $\alpha \in F$, entonces α es algebraico sobre E.*

Demostración. Si $m = [F : E]$ es el grado de la extensión F de E, entonces el conjunto $S = \{1, \alpha, \ldots, \alpha^m\} \subset F$ es linealmente dependiente, ya que card $(S) = m + 1$. Por lo tanto, existen $a_i \in E$, $i = 0, 1, \ldots, m$, no todos nulos, tales que

$$\sum_{i=0}^{m} a_i \alpha^i = 0. \tag{7.8}$$

Definimos un polinomio en $E[x]$ con los coeficientes de (7.8) así:

$$p(x) := \sum_{i=0}^{m} a_i x^i.$$

Obviamente, $p(\alpha) = 0$, por lo que α es algebraico sobre E. □

Es interesante discutir la existencia de una base (evidentemente infinita) para $\mathbb{R}$ como extensión de $\mathbb{Q}$. La existencia de una de tales bases está relacionada con la ecuación funcional de Cauchy, que se analiza en la siguiente sección. Suponiendo el Lema de Zorn (véase Sección 2.6) se demostrará la existencia de base de un cuerpo $F \subset \mathbb{C}$ extensión de un cuerpo K.

Teorema 7.1. *Supongamos que vale el lema de Zorn. Sea K un cuerpo y F una extensión de K ($\mathbb{Q} \subset K \subset F \subset \mathbb{C}$). Entonces existe una base de F como espacio vectorial sobre K.*

Demostración. La familia $\mathcal{E}$ formada por todos los conjuntos de vectores linealmente independientes, ordenados por la inclusión de conjuntos, $(\mathcal{E}, \subset)$, es una RBO. Veremos que $(\mathcal{E}, \subset)$ cumple las hipótesis del Lema de Zorn. Para ello, sea $\mathcal{L} \subset \mathcal{E}$ un subconjunto tal que $(\mathcal{L}, \subset)$ es un orden total y definimos

$$\overline{B} := \bigcup_{B \in \mathcal{L}} B .$$

Veremos que $\overline{B} \in \mathcal{E}$, es decir, que $\overline{B}$ es linealmente independiente, y que $\overline{B}$ es una cota superior de $\mathcal{L}$ en $\mathcal{E}$. En efecto, dado un conjunto finito de vectores $\{v_1, \dots, v_n\} \subset \overline{B}$, existen elementos $B_1, \dots, B_n$ en $\mathcal{L}$ tales que $v_k \in B_k$ para $k = 1, \dots, n$. Como $(\mathcal{L}, \subset)$ está totalmente ordenado, y siendo finita la familia $\mathcal{C} = \{B_1, \dots, B_n\} \subset \mathcal{L}$, existe último elemento de $\mathcal{C}$. Luego todos los B_k son subconjuntos de uno de ellos, por lo que $\{v_1, \dots, v_n\}$ está contenido en algún $B_p \in \mathcal{C}$, que es un conjunto linealmente independiente. Entonces $\{v_1, \dots, v_n\} \subset B_p$ es también un conjunto linealmente independiente.

Concluimos que $\overline{B}$ es linealmente independiente y, obviamente, $B \subset \overline{B}$ para todo $B \in \mathcal{L}$. En resumen, $\overline{B} \in \mathcal{E}$ es una cota superior de $\mathcal{L}$. Por el Lema de Zorn existe un elemento maximal M de $(\mathcal{E}, \subset)$.

Veremos, ahora, que M es un sistema generador de F. Si así no fuera, existiría $v \in F$ tal que v no sería combinación lineal de ninguno de los subconjuntos finitos de M. Entonces $M \cup \{v\}$ tendría todos sus subconjuntos finitos linealmente independientes, contradiciendo el carácter maximal de M.

Siendo M un sistema generador linealmente independiente es una base de F. □

7.2. La ecuación funcional de Cauchy

Analizaremos un problema sobre funciones reales de variable real que intrigó grandemente a los matemáticos del siglo XIX.

Definición 7.4. *Una función $f : \mathbb{R} \to \mathbb{R}$ es **aditiva** cuando*

$$f(x+y) = f(x) + f(y) \tag{7.9}$$

para cualquier par de elementos $x, y \in \mathbb{R}$.

(7.9) se denomina **ecuación funcional de Cauchy** (f es la incógnita de dicha ecuación).

Definición 7.5. *Una función $f : \mathbb{R} \to \mathbb{R}$ es **homogénea** cuando*

$$f(\alpha x) = \alpha f(x)$$

cualesquiera que sean $\alpha, x \in \mathbb{R}$.

Obsérvese que, si f es homogénea, se tiene $f(x) = f(x.1) = xf(1)$, de manera que la gráfica de f es la recta que pasa por el origen cuya pendiente es $f(1)$ (véase Figura 7.3).

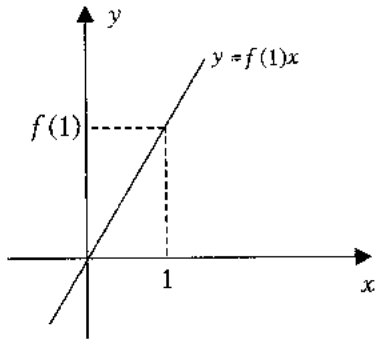

Figura 7.3. *Gráfica de una función homogénea f.*

De hecho, es fácil ver que f es homogénea si, y sólo si, $f(x) = ax$ para cierto $a \in \mathbb{R}$. En tal caso,

$$f(x+y) = a(x+y) = ax + ay = f(x) + f(y),$$

de forma que cualquier función homogénea es aditiva. A raíz de demostrar Cauchy, en 1821, que las funciones aditivas «casi» son homogéneas (en el sentido que especifican las dos próximas proposiciones), los matemáticos se preguntaron acerca de la validez del recíproco: las funciones aditivas, ¿son siempre homogéneas?

Proposición 7.5. *Si $f : \mathbb{R} \to \mathbb{R}$ es aditiva, entonces $f(rx) = rf(x)$ para todo $r \in \mathbb{Q}$ y para todo $x \in \mathbb{R}$.*

Demostración. Por ser f aditiva, $f(0) = f(0+0) = f(0) + f(0)$, de donde se deduce que

$$f(0) = 0. \tag{7.10}$$

Aplicando (7.10) podemos escribir

$$0 = f(x + (-x)) = f(x) + f(-x),$$

obteniéndose

$$f(-x) = -f(x). \tag{7.11}$$

Probaremos por inducción que

$$f(nx) = nf(x), \text{ para todo } n \in \mathbb{N} \text{ y para todo } x \in \mathbb{R}. \tag{7.12}$$

En efecto,

$$f(2x) = f(x+x) = f(x) + f(x) = 2f(x)$$

y, suponiendo cierto $f(nx) = nf(x)$, obtenemos

$$f((n+1)x) = f(nx+x) = f(nx) + f(x) = nf(x) + f(x) = (n+1)f(x).$$

Cualesquiera que sea $n \in \mathbb{N}$ y $x \in \mathbb{R}$, de (7.11) y (7.12) se deduce que

$$f(-nx) = f(n(-x)) = nf(-x) = (-n)f(x). \tag{7.13}$$

Combinando (7.10), (7.12) y (7.13) se concluye que

$$f(zx) = zf(x), \text{ para todo } z \in \mathbb{Z} \text{ y para todo } x \in \mathbb{R}. \tag{7.14}$$

Por otro lado, si $q \in \mathbb{N}$ y $x \in \mathbb{R}$, por (7.12), tenemos

$$f(x) = f\left(q\left(\frac{x}{q}\right)\right) = qf\left(\frac{x}{q}\right),$$

es decir,

$$f\left(\frac{x}{q}\right) = \frac{1}{q}f(x). \tag{7.15}$$

Por último, si $x \in \mathbb{R}$ y $r \in \mathbb{Q}$, escribiendo $r = \dfrac{p}{q}$, con $p \in \mathbb{Z}$ y $q \in \mathbb{N}$, de (7.14) y (7.15) se sigue que

$$f(rx) = f\left(\frac{1}{q}(px)\right) = \frac{1}{q}f(px) = \frac{p}{q}f(x) = rf(x) \quad \square$$

Proposición 7.6. *Si $f : \mathbb{R} \to \mathbb{R}$ es aditiva y es, además, continua en algún punto, entonces f es homogénea.*

Demostración. Empezaremos probando que, bajo la hipótesis, f es continua en $\mathbb{R}$.

Supongamos f continua en $\overline{x} \in \mathbb{R}$ y sea $b \neq \overline{x}$ arbitrario. Se tiene

$$\begin{aligned}
\lim_{x\to b} f(x) &= \lim_{x\to b} [f(x+\overline{x}-b) + f(b-\overline{x})] \\
&= \lim_{y\to \overline{x}} [f(y) + f(b-\overline{x})] \\
&= f(\overline{x}) + f(b) + f(-\overline{x}) = f(b),
\end{aligned}$$

tras efectuar el cambio de variable $y = x + \overline{x} - b$ y utilizar, asimismo, (7.11).

Probaremos ahora que f es homogénea.

Como $\mathbb{Q}$ es denso en $\mathbb{R}$, dado $x \in \mathbb{R}$ se puede escribir $x = \lim_{n\to\infty} r_n$, para cierta sucesión $\{r_n\} \subset \mathbb{Q}$. Se tiene entonces, por la continuidad de f en x y por la Proposición 7.5,

$$f(x) = \lim_{n\to\infty} f(r_n) = \lim_{n\to\infty} r_n f(1) = f(1)\,x.$$

Esto prueba que f es homogénea. □

Bajo las hipótesis de la Proposición 7.6 hemos visto que f es continua sobre $\mathbb{R}$. En ese caso, si $\alpha < \beta$ (números reales arbitrarios), f es una función acotada sobre el intervalo $[\alpha, \beta]$ (Teorema de Weierstrass), siendo evidente que la acotación de una función no garantiza su continuidad (considérese la función de Dirichlet, que vale 1 sobre los números racionales y 0 sobre los irracionales). Por esa razón, el siguiente resultado, probado por Darboux en 1880 (aunque la prueba que damos es obra de Young, 1958), supone una mejora de la condición suficiente de Cauchy (Proposición 7.6).

Proposición 7.7. *Si $f : \mathbb{R} \to \mathbb{R}$ es aditiva y está acotada sobre un intervalo propio (intervalo que contiene más de un punto), entonces f es homogénea.*

Demostración. Supongamos que f está acotada, por $k > 0$, en un intervalo $[\alpha, \beta]$, con $\alpha < \beta$ (todo intervalo propio en $\mathbb{R}$ contiene un intervalo de este tipo).

Veremos que f está acotada en $[0, c]$, para $c = \beta - \alpha > 0$.

En efecto, si $y \in [0, c]$, entonces $y + \alpha \in [\alpha, \beta]$ y se tiene

$$|f(y)| - |f(\alpha)| \leq |f(y) + f(\alpha)| = |f(y + \alpha)|,$$

por lo que

$$|f(y)| \leq k + |f(\alpha)|.$$

Consideramos entonces la función $\varphi(x) := f(x) - ax$, con $a := \dfrac{f(c)}{c}$. Probaremos un par de propiedades de esta función.

(*a*) φ es aditiva: dados x e y en $\mathbb{R}$,

$$\varphi(x + y) = f(x + y) - a(x + y) = f(x) - ax + f(y) - ay = \varphi(x) + \varphi(y).$$

(*b*) φ está acotada en $\mathbb{R}$: como $\varphi(c) = 0$ y φ es aditiva, $\varphi(x + c) = \varphi(x)$, para todo $x \in \mathbb{R}$. Esto significa que φ es periódica, con período c, por lo que φ está acotada en $\mathbb{R}$ si lo está en $[0, c]$, cosa que se cumple al ser suma de dos funciones, $f(x)$ y $-ax$, que son acotadas en $[0, c]$.

Aplicando (7.12) a φ, dado $x \in \mathbb{R}$ y $n \in \mathbb{N}$, se tiene $\varphi(nx) = n\varphi(x)$.

Si fuese $\varphi(x) \neq 0$, entonces $\lim_{n\to\infty} \varphi(nx)$ valdría $+\infty$ o $-\infty$, por lo que φ no podría ser acotada en $\mathbb{R}$. Por lo tanto, $\varphi(x) = 0$, para todo $x \in \mathbb{R}$. En otras palabras, $f(x) = ax$ para todo $x \in \mathbb{R}$, que es lo que se quería demostrar. □

Así pues, a principios del siglo XX se sabía que toda función homogénea es aditiva y que el recíproco es también cierto si se cumple una condición muy poco restrictiva: que la función es acotada en un intervalo propio. En 1905 probó Hamel el siguiente resultado, cuya hipótesis es la existencia de una base infinita (*base de Hamel*).

Proposición 7.8. *Si existe una base de $\mathbb{R}$ como extensión de $\mathbb{Q}$ existen entonces funciones aditivas que no son homogéneas.*

Demostración. Sea $\{x_i,\ i \in I\}$ una base de $\mathbb{R}$ sobre $\mathbb{Q}$. Desde luego, $x_i \neq 0$ para todo $i \in I$.

Sean j y k dos índices cualesquiera de I, con $j \neq k$. Obviamente, $x_j \neq x_k$.

Dado $x \in \mathbb{R}$ existen escalares únicos $\{\alpha_i, i \in I\}$, todos nulos salvo un número finito, tales que $x = \sum_{i \in I} \alpha_i x_i$. Se define entonces

$$f(x) = \sum_{i \in I} \alpha_i f(x_i)\,, \text{ con } f(x_i) = \begin{cases} x_i\,, & i \notin \{j, k\} \\ x_k\,, & i = j \\ x_j\,, & i = k \end{cases}.$$

La definición de $f(x)$ es buena, por la unicidad de las componentes $\{\alpha_i, i \in I\}$, y es inmediato comprobar que f es aditiva.

Si f fuese homogénea se podría escribir $f(x) = ax$, para cierto $a \in \mathbb{R}$. Como

$$f(x_j) = x_k \neq x_j = f(x_k)\,,$$

necesariamente $0 \neq a \neq 1$. Desde luego,

$$x_k = f(x_j) = ax_j \tag{7.16}$$

y

$$x_j = f(x_k) = ax_k. \tag{7.17}$$

De (7.16) y (7.17) se sigue que $x_k = a^2 x_k$, lo que implica $a = -1$. Entonces, (7.16) proporciona $x_k + x_j = 0$, lo que contradice que $\{x_i,\ i \in I\}$ sea una base. En consecuencia, f no puede ser homogénea. □

Desgraciadamente, nadie ha sido capaz de encontrar una base de $\mathbb{R}$ como extensión de $\mathbb{Q}$, aunque su existencia está demostrada si se acepta, como hacen casi todos los matemáticos, el axioma de elección. La existencia de funciones aditivas no homogéneas sigue siendo, por lo tanto, un problema abierto para los más escépticos.

7.3. Números construibles con regla y compás

En la construcción geométrica de $\mathbb{Z}$ (Figura 3.4) se trazaba (con la regla) una recta de forma totalmente arbitraria y se elegía un punto de ella como origen; a partir del origen se trasladaba el segmento tomado como unidad en ambos sentidos (con ayuda del compás). La construcción de la malla que representa a $\mathbb{Z}^2$ requiere el trazado de una recta perpendicular a la primera recta por el origen (Figura 3.5); en esa construcción se traza una circunferencia con centro en el origen y cuyo radio arbitrario lo elegiremos como la distancia entre dos puntos previamente construidos; la elección de este número natural no afecta al resultado de la construcción. Una vez representado $\mathbb{Z}$ sobre ambos ejes se trazan perpendiculares a los mismos por los puntos que representan a los enteros (Figura 3.6), lo que puede hacerse trazando circunferencias de radio natural arbitrario. La construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}^2$ (Figura 4.4) requiere el trazado de rectas que pasan por dos puntos de $\mathbb{Z}^2$ (ya construidos) y de circunferencias cuyos centros y radios ya han sido construidos (véanse las Figuras 4.2 y 4.3). $\mathbb{Q}^2$ se construye como $\mathbb{Z}^2$, trazando rectas perpendiculares a los ejes, pero ahora por los puntos que representan a $\mathbb{Q}$ sobre los mismos.

A partir de $\mathbb{Z}^2$ hubiésemos podido construir elementos que no están en $\mathbb{Q}$, pero que también se pueden construir a partir de $\mathbb{Q}^2$. Dejaremos la construcción de tales números irracionales para la siguiente fase. Así, por ejemplo, los puntos de intersección de la circunferencia con centro $(0, 0)$ y radio la distancia entre $(0, 0)$ y $(1, 1)$, es decir, $\sqrt{2}$, con los ejes son $\left(\pm\sqrt{2}, 0\right)$, $\left(0, \pm\sqrt{2}\right)$.

A partir de la malla que representa a $\mathbb{Q}^2$ iniciaremos la primera fase en la construcción de números irracionales con la regla y el compás ideales. Utilizando la regla se pueden construir rectas que pasan por pares de puntos de coordenadas racionales. Dichas rectas admiten una ecuación de la forma

$$ax + by + c = 0,$$

con a, b y c racionales (véase Problema 7.4). Por otro lado, con el compás se podrán dibujar circunferencias con centro en un punto de $\mathbb{Q}^2$ y cuyo radio se obtenga trasladando un segmento con extremos en $\mathbb{Q}^2$. En consecuencia, las circunferencias que pueden construirse tienen ecuación de la forma

$$(x - a)^2 + (y - b)^2 = r^2,$$

donde $r^2 = s^2 + t^2$, $a, b, s, t \in \mathbb{Q}$. Por lo tanto, admiten una ecuación de la forma

$$x^2 + y^2 + a'x + b'y + c' = 0,$$

con los coeficientes a', b', c' racionales.

Los nuevos puntos que se pueden obtener a partir de $\mathbb{Q}^2$ serán: (a) las intersecciones de dos rectas; (b) las intersecciones de una circunferencia con una recta y (c) las intersecciones de dos circunferencias. Pretendemos identificar esos tres conjuntos de puntos.

(a) Si las rectas de ecuaciones $ax + by + c = 0$ y $a'x + b'y + c' = 0$, con coeficientes racionales, se cortan en un punto, entonces el sistema

$$\left\{ \begin{array}{c} ax+by+c=0 \\ a'x+b'y+c'=0 \end{array} \right\}$$

tiene una solución única $(x,y) \in \mathbb{Q}^2$ (véase Problema 7.6).

(b) Para resolver el sistema con coeficientes racionales

$$\left\{ \begin{array}{c} x^2+y^2+ax+by+c=0 \\ a'x+b'y+c'=0 \end{array} \right\},$$

puede eliminarse una de las incógnitas. Por ejemplo, suponiendo $b' \neq 0$, puede despejarse y en la segunda ecuación y sustituir en la primera, con lo que resulta una ecuación de segundo grado en la variable x con coeficientes racionales. La solución de dicha ecuación será de la forma $x = \delta \pm \sqrt{\gamma}$, siendo δ y γ racionales y $\gamma \geq 0$, puesto que estamos suponiendo que el sistema es compatible.

Obviamente, la forma de y será la misma que la de x, por lo que se obtienen puntos (x,y) tales que

$$x \in \mathbb{Q}(\sqrt{\gamma}) \ ; \ y \in \mathbb{Q}(\sqrt{\gamma}) \ , \gamma \in \mathbb{Q}, \ \gamma \geq 0.$$

(c) Es fácil ver que el sistema

$$\left\{ \begin{array}{c} x^2+y^2+ax+by+c=0 \\ x^2+y^2+a'x+b'y+c'=0 \end{array} \right\}$$

es equivalente a otro del tipo (b), por lo que podemos ahorrarnos la discusión.

En resumen, sólo pueden construirse, en esta fase, puntos del plano cuyas coordenadas pertenecen al cuerpo $\mathbb{Q}(\sqrt{\gamma})$, para algún $\gamma \in \mathbb{Q}$, $\gamma \geq 0$. Desde el punto de vista geométrico, si en la Sección 4.4 se representó $\mathbb{Q}^2$ mediante los nudos de una malla que refinaba la de la Figura 3.6, que proporcionaba $\mathbb{Z}^2$, ahora un punto construido en esta fase se ubica en algún nudo de la malla, todavía más fina, que representa el conjunto $\mathbb{Q}(\sqrt{\gamma})^2$.

Repitiendo la operación, sólo pueden obtenerse en la segunda fase puntos que tienen sus coordenadas en un cuerpo de la forma $\mathbb{Q}(\sqrt{\gamma}, \sqrt{\gamma'})$, siendo γ un número racional y $\gamma' \in \mathbb{Q}(\sqrt{\gamma})$, γ y γ' no negativos. Como esta operación puede repetirse un número finito de veces, concluimos que, mediante la regla y el compás ideales, sólo pueden construirse puntos cuyas coordenadas son elementos de alguna extensión algebraica de la forma

$$\mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}),$$

donde $\alpha_1 \in \mathbb{Q}$, $\alpha_{k+1} \in \mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_k})$, para $1 \leq k \leq n$.

Teniendo en cuenta que la afirmación de la Proposición 7.2 referida al grado de una doble extensión se puede generalizar por inducción se tiene que

$$[\mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}) : \mathbb{Q}] =$$

$$[\mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}) : \mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_{n-1}})] \cdots [\mathbb{Q}(\sqrt{\alpha_1}) : \mathbb{Q}].$$

Como el grado de $\sqrt{\alpha_1}$ (algebraico sobre $\mathbb{Q}$) es 1 o 2, al igual que el de $\sqrt{\alpha_2}$ (algebraico sobre $\mathbb{Q}(\sqrt{\alpha_1})$), etc., se tendrá necesariamente, por la Proposición 7.3, que

$$\left[\mathbb{Q}\left(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}\right) : \mathbb{Q}\right] = 2^p$$

para cierto entero p, $0 \leq p \leq n$.

En otras palabras, todos los puntos del plano construibles con regla y compás partiendo de $\mathbb{Q}^2$ tienen una marca genética hereditaria, a saber, sus coordenadas pertenecen a una extensión de $\mathbb{Q}$ cuyo grado es una potencia de 2. Un punto que no posea dicha característica no puede construirse con regla y compás.

7.4. Imposibilidad de los tres problemas clásicos

Duplicación del cubo

Probaremos que el cubo de arista unidad no puede ser duplicado mediante la regla y el compás, es decir, suponiendo que $\left(\sqrt[3]{2}, 0\right)$ es construible llegaremos a una contradicción.

El polinomio minimal asociado a $\sqrt[3]{2}$ es $x^3 - 2$ (irreducible en $\mathbb{Q}$, ya que ± 1, ± 2 no son raíces y, por la Proposición 6.5, son las únicas posibles raíces racionales). Así pues, el grado de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es 3.

Por lo visto en la Sección 7.3, si $\left(\sqrt[3]{2}, 0\right)$ fuera construible, entonces $\sqrt[3]{2} \in \mathbb{Q}\left(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}\right)$ y el grado de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ sería un divisor de 2^p (por el Corolario 7.1), esto es, 3 dividiría a 2^p para algún entero no negativo p, que es una contradicción.

Trisección del ángulo

Probaremos la imposibilidad de la trisección del ángulo de 60°. Dicho ángulo es construible con regla y compás (basta construir un triángulo equilátero).

Demostraremos por reducción al absurdo la imposibilidad de construir el ángulo de 20° ($\pi/9$ radianes). Tomemos una de las semirrectas que forman el ángulo como eje positivo de abscisas y, como eje de ordenadas, una recta perpendicular por el vértice del ángulo.

La intersección de la otra semirrecta (supuestamente construible) con la circunferencia de centro en el origen y de radio unidad permite construir, con regla y compás, el punto $A(\cos(\pi/9), \operatorname{sen}(\pi/9))$. Como podemos trazar la recta perpendicular al eje de abscisas desde A, concluimos que es posible construir un segmento de longitud $\alpha = \cos(\pi/9)$ (véase la Figura 7.4).

Puesto que $\cos(3\varphi) = 4\cos^3(\varphi) - 3\cos(\varphi)$, y $\cos(\pi/3) = 1/2$, resulta que α es una raíz de la ecuación $4x^3 - 3x = 1/2$, cuyos coeficientes son números racionales.

Es fácil probar que la ecuación $8x^3 - 6x - 1 = 0$ no tiene raíces racionales (Proposición 6.5), por lo que $x^3 - \frac{3}{4}x - \frac{1}{8}$ es el polinomio minimal de α, cuyo

grado resulta ser 3. Tenemos, por lo tanto, la misma contradicción que antes: un número construible que no porta la marca genética (pues su grado no es una potencia de 2).

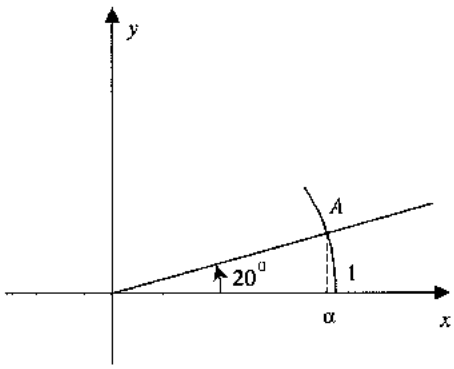

Figura 7.4. *Construcción con regla y compás de* $\alpha = \cos\left(\frac{\pi}{9}\right)$.

Cuadratura del círculo

Tomando como unidad el radio del círculo, se trata de construir un cuadrado de área π, es decir, un segmento (el lado del cuadrado) de longitud $\sqrt{\pi}$. Si $\sqrt{\pi}$ puede construirse con regla y compás, entonces $\sqrt{\pi}$ pertenece a alguna extensión de $\mathbb{Q}$ de grado finito. Por la Proposición 7.4, $\sqrt{\pi}$ debería ser algebraico sobre $\mathbb{Q}$. De este hecho daremos tan sólo un esbozo de la prueba, que se hace por reducción al absurdo.

Hay que empezar con un razonamiento algebraico. Consideremos $\mathbb{Q}$ como subcuerpo de $\mathbb{C}$.

Proposición 7.9. *(i) si* $\sqrt{\pi}$ *es algebraico, entonces* π *es algebraico.*
(ii) Si π *es algebraico, entonces* $i\pi$ *es algebraico.*

Demostración. (*i*) Si $\sqrt{\pi}$ es algebraico, entonces su polinomio minimal $h(x)$ se puede escribir de la forma

$$h(x) = p(x) + q(x),$$

siendo $p(x)$ el polinomio formado por los monomios de grado par, y $q(x)$ el de los monomios de grado impar. Sacando factor común x, en $q(x)$, se tiene

$$h(x) = p(x) + xr(x),$$

siendo todos los monomios de $r(x)$ de grado par.

Fácilmente se comprueba que π es raíz del polinomio que resulta al hacer el cambio de variable $x^2 = y$ en $[p(x)]^2 - x^2[r(x)]^2$, por lo que π es algebraico sobre $\mathbb{Q}$.

(*ii*) Repitiendo el razonamiento anterior se concluye que π^2 es algebraico y, de igual forma, $\pi^4 = (i\pi)^4$ también será algebraico. Ahora bien, si $(i\pi)^4$ es raíz de $g(x)$, entonces $i\pi$ será raíz de $g(x^4)$, por lo que $i\pi$ será, a su vez, algebraico. □

Lindemann probó, en 1877, la trascendencia de $i\pi$, basándose en la misma integral que utilizara Hermite para probar la trascendencia de e, siendo tal la dificultad de la prueba que le dejó, según confesión propia, sin deseos de abordar la trascendencia de π.

7.5. **Problemas**

Problema 7.1. Describa los siguientes cuerpos:

a) $\mathbb{Q}(i)$.

b) $\mathbb{R}(i)$.

c) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

Problema 7.2. Determine las dimensiones de las siguientes extensiones algebraicas:

a) $\mathbb{Q}(i)$ sobre $\mathbb{Q}$.

b) $\mathbb{R}(i)$ sobre $\mathbb{R}$.

c) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ sobre $\mathbb{Q}$.

Problema 7.3. Pruebe que $\sqrt[n]{2}$ es algebraico sobre $\mathbb{Q}$ y determine una base de $\mathbb{Q}\left(\sqrt[n]{2}\right)$ como extensión de $\mathbb{Q}$.

Problema 7.4. Pruebe que si una recta pasa por un par de puntos de coordenadas racionales entonces admite una ecuación de la forma $ax+by+c = 0$, con a, b, y c racionales. Recíprocamente, cualquier recta $ax+by+c = 0$, con a, b y c racionales está determinada por dos puntos de coordenadas racionales.

Problema 7.5. Demuestre que cualquier circunferencia de ecuación

$$x^2 + y^2 + Ax + By + C = 0,$$

con A, B y C racionales tiene como centro un punto del plano de coordenadas racionales y como radio la raíz cuadrada de cierto número racional.

Problema 7.6. Pruebe que un sistema compatible determinado de dos ecuaciones lineales con coeficientes racionales y dos incógnitas tiene como solución un par de números racionales.

Problema 7.7. Pruebe que cualquier elemento de $\mathbb{Q}(\sqrt{\gamma})$, donde γ representa un número racional no negativo puede construirse con regla y compás (el procedimiento de la Figura 5.1 sólo construye $\sqrt{\gamma}$).

Problema 7.8.* El Problema 7.7 constituye el primer paso de la demostración por inducción de que **todo** punto con coordenadas en alguna extensión algebraica de la forma

$$\mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}),$$

donde $\alpha_1 \in \mathbb{Q}$, $\alpha_{k+1} \in \mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_k})$, para $1 \leq k \leq n$, puede construirse con regla y compás.

Problema 7.9. Pruebe que si $\alpha, \beta \in \mathbb{C}$ son algebraicos sobre $\mathbb{Q}$ y del mismo grado, entonces $\mathbb{Q}(\alpha)$ es isomorfo a $\mathbb{Q}(\beta)$. (Ayuda: Defina el isomorfismo utilizando sendas bases de $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\beta)$.)

Problema 7.10.* Pruebe que, si α es trascendente sobre $\mathbb{Q}$, entonces $\mathbb{Q}(\alpha)$ es isomorfo al cuerpo de las fracciones algebraicas $\mathbb{Q}(x)$. (Ayuda: Establezca primero el isomorfismo entre los anillos $\mathbb{Q}[x]$ y $\mathbb{Q}[\alpha]$ que asocia a cada polinomio el resultado de sustituir x por α.)

Problema 7.11. Pruebe que $\mathbb{Q}\left(\sqrt{2}\right)$ no es completo (Cauchy). (Ayuda: Pruebe que $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$.)

Problema 7.12. Pruebe que ningún segmento con extremos en $\mathbb{Q}^2$ tiene longitud $\sqrt{3}$. (Ayuda: Si existe tal segmento, existen tres naturales a, b y c tales que $a^2 + b^2 = 3c^2$. A partir de la terna con menor c se llega a una contradicción al efectuar la división euclídea de los tres números por 3).

Problema 7.13. El problema anterior muestra que el punto $\left(0, \sqrt{3}\right)$ no se puede construir en la primera fase partiendo de $\mathbb{Q}^2$. ¿No es esto contradictorio con lo afirmado en el Problema 7.7?

SOLUCIONES A LOS PROBLEMAS

Capítulo 1

1.9.

$A \cup B = [-2, 5]$ $\quad A \cap B = [-1, 4[$

$A \times B = \{(x,y) \in \mathbb{R}^2 \mid (-2 \leq x < 4) \wedge (-1 \leq y \leq 5)\}$

$A \cup C = [-2, 4[$ $\quad A \cap C = \{-2, -1, 0\}$

$A \times C = \{(x,y) \in \mathbb{R}^2 \mid (-2 \leq x < 4) \wedge ((y = -2) \vee (y = -1) \vee (y = 0))\}$

$B \cup C = [-1, 5] \cup \{-2\}$ $\quad B \cap C = \{-1, 0\}$

$B \times C = \{(x,y) \in \mathbb{R}^2 \mid (-1 \leq x \leq 5) \wedge ((y = -2) \vee (y = -1) \vee (y = 0))\}$

1.10.

a) $G = \{(1, 14), (2,12), (3,10), (4,8), (5,6), (6,4), (7,2)\}$.

b) Conjunto original: $\{1,2,3,4,5,6,7\}$.
Conjunto imagen: $\{2,4,6,8,10,12,14\}$.

1.11.

F no es aplicación, G y $G \circ F$ son aplicaciones suprayectivas y no inyectivas.

1.12.

a) Es aplicación biyectiva.

b) No es ninguna de las tres cosas.

1.13.

Es suprayectiva pero no inyectiva, ya que, por ejemplo, $f(1,1) = f(1,-1)$.

1.14.

Se demuestra que no se cumplen las proposiciones *a*), *b*) y *c*) para aplicaciones en general, considerando, por ejemplo, los conjuntos $A = \{a, b, c\}$, $B = \{\alpha, \beta, \gamma\}$ y $X = \{a, b\}$ y la aplicación de A en B cuyo grafo es

$$f = \{(a,\alpha), (b,\beta), (c,\beta)\}.$$

1.15.

a) Sean los conjuntos $A = \{a,b,c\}$, $B = \{\alpha,\beta\}$, $A_1 = \{a\}$ y $A_2 = \{a,b\}$. Si consideramos la aplicación $f = \{(a,\alpha), (b,\alpha), (c,\beta)\}$, se tiene la igualdad entre las imágenes de A_1 y A_2. Por otra parte, si la aplicación considerada es $g = \{(a,\alpha), (b,\beta), (c,\beta)\}$ se tiene el contenido estricto.

b) Sean los conjuntos $A = \{a,b\}$, $B = \{\alpha,\beta,\gamma\}$, $B_1 = \{\beta\}$ y $B_2 = \{\beta,\gamma\}$ y la aplicación $g = \{(a,\alpha), (b,\beta)\}$. En este ejemplo se da la igualdad entre las imágenes inversas de B_1 y B_2. Por otra parte, si la aplicación considerada es la f del apartado *a*) se tiene el contenido estricto entre las imágenes inversas de $B_1 = \{\alpha\}$ y $B_2 = \{\alpha,\beta\}$.

d) Sean los conjuntos $A = \{a,b,c\}$, $B = \{\alpha,\beta\}$, $A_1 = \{a,b\}$ y $A_2 = \{b,c\}$. Si consideramos la aplicación cuyo grafo es $f = \{(a,\alpha), (b,\beta), (c,\beta)\}$, se tiene la igualdad entre la imagen de $A_1 \cap A_2$ y la intersección de las imágenes de A_1 y A_2. Por otra parte, si la aplicación considerada tiene como grafo $g = \{(a,\alpha), (b,\beta), (c,\alpha)\}$ se tiene el contenido estricto.

1.18.

Un ejemplo que demuestra que la suprayectividad no siempre es heredada por la restricción es el siguiente:

Consideramos los conjuntos $A = \{a,b,c\}$, $B = \{\alpha,\beta\}$ y $A' = \{a,b\}$ y la aplicación de A en B cuyo grafo es $f = \{(a,\alpha), (b,\alpha), (c,\beta)\}$. La aplicación f es suprayectiva mientras que su restricción a A' no lo es.

1.19.

Dado $n \in \mathbb{N}$, el conjunto cociente es $\mathbb{Z}/G = \{[0], [1], \ldots, [n-1]\}$ donde $[x] = \{y \in \mathbb{Z} \mid y = pn + x,\ p \in \mathbb{Z}\}$.

1.21.

No es una relación de buen orden, ya que, por ejemplo, el subconjunto $\{1\} \times]0,1[$ de $\mathbb{R}^2$ no tiene primer elemento.

Cualquier $(x,y) \in \mathbb{R}^2$ con $x \leq 0$ es una cota inferior de B y cualquier $(x,y) \in \mathbb{R}^2$ con $x \geq 1$ es una cota superior.

Dado cualquier subconjunto A de $\mathbb{N}^2$, $\min A = (M,N)$ donde $M = \min\{m \in \mathbb{N} \mid (m,n) \in A\}$ y $M = \min\{n \in \mathbb{N} \mid (M,n) \in A\}$.

1.23.

No es correcta la prueba. Dado un $x \in E$, es cierto que $(x,y) \in G \Longrightarrow (x,x) \in G$. Sin embargo, puede haber elementos $x \in E$ para los que no existe ningún $y \in E$ tal que $(x,y) \in G$ y en ese caso no podríamos deducir que $(x,x) \in G$.

1.24.

Relaciones de equivalencia:

$G_1 = \{(1,1), (2,2), (3,3)\}$

$G_2 = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$

$G_3 = \{(1,1),(2,2),(3,3),(1,3),(3,1)\}$
$G_4 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$
$G_5 = \{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$
Relaciones de orden total:
$G_6 = \{(1,1),(2,2),(3,3),(1,2),(1,3),(2,3)\}$
$G_7 = \{(1,1),(2,2),(3,3),(1,2),(1,3),(3,2)\}$
$G_8 = \{(1,1),(2,2),(3,3),(1,2),(3,1),(3,2)\}$
$G_9 = \{(1,1),(2,2),(3,3),(2,1),(1,3),(2,3)\}$
$G_{10} = \{(1,1),(2,2),(3,3),(2,1),(3,1),(2,3)\}$
$G_{11} = \{(1,1),(2,2),(3,3),(2,1),(3,1),(3,2)\}$
Todas las relaciones de orden anteriores son de buen orden.
G_1 es una relación de orden que no es total.

1.25.

a) Es una relación de buen orden y, por tanto, de orden total.

b) Tienen máximo todos los subconjuntos finitos y los infinitos cuya intersección con los números pares es finita y no vacía.

1.26.

a) No es una relación de orden total y, por lo tanto, tampoco de buen orden.

b) No tiene máximo ni mínimo. Los minimales de A son $(2,6)$, $(8,5)$ y $(7,2)$ y los maximales son $(4,1)$, $(8,5)$ y $(7,2)$.

1.27.

Es una relación de equivalencia y el conjunto cociente está formado por todas las rectas del plano con pendiente 1.

1.28.

a) Sí, es una relación de equivalencia.

b) La clase de equivalencia de un punto A de $\mathbb{R}^2$ es la circunferencia de centro O y radio $d(O,A)$. El conjunto cociente está formado por todas las circunferencias concéntricas de centro O.

1.29.

A_1 y B_1 son maximales, B_2 es minimal y mínimo y no tiene máximo.

1.30.

$B = \{(x,y) \in \mathbb{R}^2 \mid y = 1\}$.

1.31.

Si A es finito la afirmación es verdadera, ya que para cualquier $a_2 \in A$, si $a_2 \neq a_1$, entonces a_2 no es maximal y existe $a_3 \in A$ tal que $a_2 \preceq a_3$ y $a_2 \neq a_3$. Si $a_3 \preceq a_1$ no hace falta seguir. En caso contrario se repite el argumento para a_3.

Como sólo hay un número finito de elementos en A el proceso termina.
Para el caso infinito considere el siguiente contraejemplo: $(\mathbb{N}, \preceq)$ con el orden dado por

$$2 \preceq 3 \preceq 4 \preceq \cdots$$
$$2 \preceq 1$$

Capítulo 2

2.2.

a) $n \geq 3$ *b*) $n \geq 5$ *c*) $n \geq 4$.

2.7.

a) La desigualdad se cumple para todo $n \in \mathbb{N}$, pero $\aleph_0 \notin \mathbb{N}$.

b) En el último paso de la demostración se utiliza la igualdad $(a+b)^2 = a+b$, que se supone cierta por la hipótesis de inducción completa. Sin embargo, si $n = 1$, tan sólo podemos suponer cierto $(a+b)^k = a+b$ para todo número natural $k \leq 1$.

2.8.

Para $n = 40$ se tiene $40^2 + 40 + 41 = 1681 = 41^2$, que no es un número primo.

2.11.

En el primer caso no se pueden cubrir todas las casillas del tablero porque sobran dos casillas del mismo color (no contiguas). En el segundo caso, podrán cubrirse todas las casillas sólo si n es par (el mismo número de casillas blancas que de casillas negras).

2.13.

Se aplica el principio del palomar: las once posibles puntuaciones suma, $\{2,3, \ldots, 12\}$, son los nidos y las doce tiradas, las palomas.

2.15.

<u>f sobre</u>: Para $N = 1, f(1,1) = N$. Si $f(m,n) = N$, entonces $N+1 = f(m+1, n-1)$ si $n > 1$ y $N+1 = f(1, m+1)$ si $n = 1$.

<u>f inyectiva</u>: Supongamos $f(m,n) = f(p,q)$. Si $m+n = p+q$, se llega a $(m,n) = (p,q)$. En caso contrario, si $p+q = m+n+h$ con $h \geq 1$, se llega a la siguiente contradicción:

$$f(p,q) = f(m,n) + \frac{1}{2}\left(h\left(h+2n-3\right) + 2m\left(h-1\right) + 2p\right) \neq f(m,n).$$

2.16.

Cardinal $\aleph_0$.

2.19.

card $(\mathbb{R}^n) = c$ para todo $n \in \mathbb{N}$. Se demuestra por inducción.

2.20.

a) Si denotamos por S el conjunto que nos dan, resulta que $S \subset \mathbb{R}^4$ y contiene un subconjunto $T = \{(0,0,x,0) \mid x \in \mathbb{R}\setminus\{0\}\}$ que es equipotente a $\mathbb{R}\setminus\{0\}$, por lo que card $(S) = c$.

b) Cardinal $\aleph_0$.

c) Cardinal c.

d) Cardinal c.

2.21.

a) Cardinal c.

b) Cardinal c.

c) Cardinal c.

d) Cardinal c.

2.22.

Cardinal c. Como $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$, se tiene card $(\mathbb{I}) \leq c$. Se establece que $\mathbb{I}$ es infinito probando, por ejemplo, que $\mathbb{N} \sim \sqrt{2}\mathbb{N} \subset \mathbb{I}$. Luego se aplica la hipótesis del continuo.

2.23.

b) Se prueba que el conjunto en cuestión es equipotente al conjunto $\mathbb{Z}\setminus\{0\} \times \mathbb{Z} \times \overset{(n}{\cdots} \times \mathbb{Z}$.

c) Es una unión numerable de conjuntos numerables.

d) El conjunto de los números algebraicos es unión de los conjuntos formados por las soluciones reales de cada una de las ecuaciones algebraicas, por lo que es unión numerable de conjuntos finitos.

e) Si fuera numerable, $\mathbb{R}$ también lo sería. Se puede afirmar que su cardinal es c si se acepta la hipótesis del continuo.

2.26.

a) La composición de aplicaciones inyectivas es inyectiva.

b) Considérese, por ejemplo, $f = g : \mathbb{N} \longrightarrow \mathbb{N}$ como la función sucesor.

c) $g \circ f$ es inyectiva por *a*). Si $g \circ f : X \longrightarrow X$ no fuera suprayectiva, X sería infinito.

2.27.

Si card $X = \alpha$, entonces card $2^X = 2^\alpha$.

2.30.

Se trabaja en el conjunto ordenado $(C, \subset)$, pero la unión creciente de conjuntos finitos no siempre es finito. Por lo tanto, no se puede asegurar que cada

subfamilia totalmente ordenada $\mathcal{C}' \subset \mathcal{C}$ tenga una cota superior en $\mathcal{C}$ y el lema de Zorn no es aplicable.

Capítulo 3

3.1.

No satisface la propiedad asociativa.

3.2.

a) Monoide abeliano.

b) Semigrupo.

c) Semigrupo abeliano.

3.5.

a) No son isomorfos.

b) Subgrupos de G: $G_1 = \{a\}$, $G_2 = \{a,c\}$ y G. Subgrupos de H: $H_1 = \{s\}$, $H_2 = \{s,t\}$, $H_3 = \{s,u\}$, $H_4 = \{s,v\}$ y H.

3.6.

a) Ni siquiera es semigrupo.

b) Monoide abeliano.

c) Monoide abeliano.

3.7.

Es una operación cerrada conmutativa.

3.9.

Es un isomorfismo.

3.10.

a) $G_1 = \{(x,x) \mid x \in E\}$ y $G_2 = \{(x,y) \mid x,y \in E\}$.

$E/G_1 = E$ y $E/G_2 = \{[x]\}$, x cualquier elemento de E. E/G_2 es grupo abeliano.

b) Si E es una pareja las únicas RBE que se pueden definir sobre E son las del apartado anterior.

c) Consideramos el semigrupo $(\mathbb{N},+)$ y la RBE cuyo grafo es $G = \{(n,n), n \in \mathbb{N}; (1,2),(2,1)\}$.

3.13.

La condición de que la sucesión de subgrupos sea expansiva no es superflua, puesto que, si consideramos el grupo $(\mathbb{R}^2,+)$ y los subgrupos no vacíos $G_1 = \{(x,0) \mid x \in \mathbb{R}\}$ y $G_2 = \{(0,x) \mid x \in \mathbb{R}\}$, la unión de G_1 y G_2 no es un subgrupo. (Véase también el Problema 3.19.)

3.14.

$G/\ker(f) = \mathbb{Q}_+$.

3.16.

La tabla de Cayley del producto en A_2 es

	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

El grupo de las permutaciones sólo es conmutativo para $n = 2$ y $n = 3$.

3.17.

b) No es grupo abeliano.

e) Dado $f \in E$ tal que $f(x) = ax + b$, la clase de equivalencia de f es el conjunto de todas las funciones de E que tienen el coeficiente de x igual a a.

3.19.

c) $2\mathbb{Z}$.

d) El mínimo subgrupo de $(\mathbb{Z}, +)$ que contiene a $n\mathbb{Z} \cup m\mathbb{Z}$ es $q\mathbb{Z}$ donde $q = \operatorname{mcd}(m, n)$.

e) $6\mathbb{Z} \cap 10\mathbb{Z} = 30\mathbb{Z}$

f) $n\mathbb{Z} \cap m\mathbb{Z} = q\mathbb{Z}$, donde $q = \operatorname{mcm}(m, n)$.

3.20.

Hay 20 alumnos que practican a la vez fútbol y tenis.

3.21.

a) No, no es correcta la información.

b) 140 alumnos.

c) 20 alumnos.

d) 130 alumnos.

e) 180 alumnos.

f) 170 alumnos.

3.22.

Hay 457 números.

Capítulo 4

4.1.
Es un dominio de integridad.

4.2.
$(\mathbb{N}, \oplus)$ no es ni tan siquiera un semigrupo. $(\mathbb{N}, \triangle)$ es un semigrupo abeliano.

4.3.
Es un anillo conmutativo.

4.4.
$(G, \boxdot)$ es un semigrupo, pero no se verifica la propiedad distributiva.

4.5.
Es un anillo.

4.6.
Es un anillo unitario.

4.8.
b) $\mu = -6$.
c) Sí, es un dominio de integridad. Puesto que el neutro de la operación $\oplus$ es 6, para demostrar que no tiene divisores de cero hay que probar que $a \otimes b = 6 \Longrightarrow (a = 6) \vee (b = 6)$.

4.9.
La solución es $x = \overline{3}$ e $y = \overline{1}$.

4.10.
El conjunto de soluciones en $\mathbb{Z}_{13}$ es $\{(\overline{4}z, \overline{9}z, z) \mid z \in \mathbb{Z}_{13}\}$ y en $\mathbb{Q}$ es $\{(-y, y, 3y) \mid y \in \mathbb{Q}\}$.

4.11.
En $\mathbb{Z}_5$ el sistema es incompatible. En $\mathbb{Z}_7$ tiene solución única y es $x = \overline{2}$, $y = \overline{6}$ y $z = \overline{5}$.

4.12.
Solución en $\mathbb{Z}$: $S = \{(x_1, 1, x_1 + 3, 1) \mid x_1 \in \mathbb{Z}\}$.
Solución en $\mathbb{Z}_9$: $S = \{(1 + x_3 + 5x_4, x_4, x_3, x_4) \mid x_3, x_4 \in \{0, 1, \ldots, 8\}\}$.
Solución en $\mathbb{Z}_{11}$: $S = \{(8 + x_3, 1, x_3, 1) \mid x_3 \in \{0, 1, \ldots, 10\}\}$.
Solución en $\mathbb{Q}$: $S = \{(x_3 - 3, 1, x_3, 1) \mid x_3 \in \mathbb{Q}\}$.

4.14.
b) Consideramos la RBE definida por el ideal $2\mathbb{Z}[x]$.

4.15.

card $\{\mathbb{Q}[x] \times \mathbb{Q}[x] \setminus \{0\}\} = \aleph_0$ y la aplicación

$$f : \mathbb{Q}[x] \times \mathbb{Q}[x] \setminus \{0\} \longrightarrow \mathbb{Q}(x)$$
$$(p(x), q(x)) \longmapsto \left[\frac{p(x)}{q(x)}\right]$$

es suprayectiva, por lo que card $\mathbb{Q}(x) \leq \aleph_0$.

4.16.

$f_0(x) = 0 = x^2 + x = \ldots \qquad f_1(x) = 1 = x^2 + x + 1 = \ldots$
$f_2(x) = x = x^2 = \ldots \qquad f_3(x) = x + 1 = x^2 + 1 = \ldots$

4.17.

Se distribuyen los números naturales en 52 «nidos», según el resto módulo 52 que tengan:

$$A_i = \{n \in \mathbb{N} \mid n \equiv_{52} (i-1)\},$$

$i = 1, \ldots, 52$. Los 53 elementos de A serán las palomas.

4.18.

El menor subanillo de $\mathbb{Q}$ que contiene a $\frac{1}{5}$ y a $\frac{1}{7}$ es

$$E = \left\{\frac{p}{q} \in \mathbb{Q} \mid \text{mcd}\,(p,q) = 1,\ q = 5^n \cdot 7^m,\ n,m \in \mathbb{N} \cup \{0\}\right\}.$$

4.21.

En cualquier cuerpo ordenado se tiene que $0 < 1$; por lo tanto, $0 + 1 < 1 + 1$ y también $0 + 1 + 1 < 1 + 1 + 1$. La interpretación en $\mathbb{Z}_3$ de las desigualdades anteriores es $[0] < [1] < [2] < [0]$.

Si $(K, +, \cdot, \leq)$ fuese un cuerpo finito ordenado, el conjunto $\{n\mathbf{1} \mid n \in \mathbb{N}\} \subset K$ también es finito, por lo que $n1 = m1$ para ciertos $n, m \in \mathbb{N}$, $n < m$. Aplicando la ley de cancelación obtenemos $0 = m - n$, lo cual es imposible.

Capítulo 5

5.1.

a) En la demostración de la Proposición 5.2 reemplace en todos los sitios la palabra «regular» por «convergente», a_m por $a = \lim_{n\to\infty} a_n$, y también, b_m por $b = \lim_{n\to\infty} b_n$.

b) La aplicación $f : A/I \to \mathbb{Q}$ definida por $[\{a_n\}] \longmapsto \lim_{n\to\infty} a_n$ está bien defini-

da debido a que $\{a_n\}$ es convergente en $\mathbb{Q}$; además, si $\{a_n\} \backsim \{b_n\}$, entonces $\lim_{n\to\infty} (a_n - b_n) = 0$, por lo que $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$. Debe probarse que f es homomorfismo de anillos y que es biyectivo.

5.2.

Dominio de integridad.

5.3.

Automorfismo de anillo.

5.4.

Dominio de integridad y cuerpo, respectivamente.

5.5.

De

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = x + y\sqrt[3]{2} + z\sqrt[3]{4}$$

se sigue que (x, y, z) es solución de un sistema de tres ecuaciones lineales con tres incógnitas, que no es fácil de probar que tiene solución única (en $\mathbb{Q}^3$) siempre que no se tenga $a = b = c = 0$.

5.6.

Sea $f : [a, b] \to \mathbb{R}$ una función continua con $f(a) < 0 < f(b)$. Supongamos que $f(x) \neq 0$ para todo $x \in]a, b[$. Entonces existe una sucesión de intervalos encajados $\{[a_n, b_n]\}$ tal que $[a_1, b_1] = [a, b]$ y $f(a_n) < 0 < f(b_n)$ para todo $n \in \mathbb{N}$. Si $\{c\} = \bigcap_{n=1}^{\infty} [a_n, b_n]$, por la continuidad de f se tiene $f(c) = \lim_{n\to\infty} f(a_n) \leq 0$ y también $f(c) = \lim_{n\to\infty} f(b_n) \geq 0$. Esto contradice la suposición.

5.7.

La función $f(x) := x^n - a$ cambia de signo en un intervalo $[0, c]$, $c > 0$, donde f es continua.

5.14.

Si $\sup A \in B$ y no es el mínimo de B, entonces existe $b \in B$ para el cual $b < \sup A$. Siendo $\sup A$ la cota superior mínima existirá $a \in A$ tal que $b < a < \sup A$, lo que contradice que (A, B) sea cortadura.

5.17.

Consulte algún texto de análisis matemático, por ejemplo, Rudin, W.(1980).

Capítulo 6

6.1.

Sea $z_n = \dfrac{(1+i)^n}{(1-i)^{n-2}}$, $n \in \mathbb{N}$, y sea $(\mathbb{Z}_4, +, \cdot)$ el anillo de las clases de congruencia módulo 4 (recuérdese Ejercicio 4.2).

Si $\overline{n} = \overline{0}$, entonces $z_n = -2i = (0,-2) = 2i \operatorname{sen} \dfrac{3\pi}{2} = 2e^{i\frac{3\pi}{2}}$.

Si $\overline{n} = \overline{1}$, entonces $z_n = 2 = (2,0) = 2\cos 0 = 2e^{i0}$.

Si $\overline{n} = \overline{2}$, entonces $z_n = 2i = (0,2) = 2i \operatorname{sen} \dfrac{\pi}{2} = 2e^{i\frac{\pi}{2}}$.

Si $\overline{n} = \overline{3}$, entonces $z_n = -2 = (-2,0) = 2\cos\pi = 2e^{i\pi}$.

6.2.

Obsérvese que

$$\frac{1 + i\tan\alpha}{1 - i\tan\alpha} = \frac{\cos\alpha + i\operatorname{sen}\alpha}{\cos\alpha - i\operatorname{sen}\alpha} = \frac{e^{i\alpha}}{e^{-i\alpha}} = e^{2i\alpha}.$$

6.3.

a) $-i$; $\dfrac{\sqrt{3}+i}{2}$; $\dfrac{-\sqrt{3}+i}{2}$.

b) $-1+i$; $\sqrt{\dfrac{2+\sqrt{3}}{2}} + \left(\sqrt{\dfrac{2-\sqrt{3}}{2}}\right)i$; $-\sqrt{\dfrac{2-\sqrt{3}}{2}} - \left(\sqrt{\dfrac{2+\sqrt{3}}{2}}\right)i$.

c) $1+i$; $1-i$; $-1+i$; $-1-i$.

d) $i\sqrt{3}$; $-i\sqrt{3}$; $\dfrac{3+i\sqrt{3}}{2}$; $\dfrac{3-i\sqrt{3}}{2}$; $-\dfrac{3+i\sqrt{3}}{2}$; $\dfrac{-3+i\sqrt{3}}{2}$.

6.4.

Es grupo conmutativo para el producto (la suma no es operación binaria).

6.5.

a) Sustituir $n = 3, 4, 6$ en $e^{i\frac{2k\pi}{n}}$, $k = 0, 1, \ldots, n-1$.

$n = 3$: 1; $\dfrac{-1+i\sqrt{3}}{2}$; $\dfrac{-1-i\sqrt{3}}{2}$.

$n = 4$: 1; -1; i; $-i$.

$n = 6$: 1; -1; $\dfrac{1+i\sqrt{3}}{2}$; $\dfrac{-1+i\sqrt{3}}{2}$; $\dfrac{-1-i\sqrt{3}}{2}$; $\dfrac{1-i\sqrt{3}}{2}$.

b) $x^3 - 1 = (x-1)\left(x^2+x+1\right)$.

$x^4 - 1 = (x-1)(x+1)\left(x^2+1\right)$.

$x^6 - 1 = (x-1)(x+1)\left(x^2-x+1\right)\left(x^2+x+1\right)$.

6.6.

$1-i;\ \dfrac{4-2i}{5}.$

6.7.

$x=2+i, y=2-i.$

6.8.

$2, 3, 5, 2i, -2i.$

6.9.

a) $-3,\ \dfrac{3\pm i\sqrt{3}}{2}.$

b) $5, 2\pm 2\sqrt{3}i.$

6.10.

a) Las únicas posibles raíces racionales son 1 y -1.

b) $\dfrac{\sqrt{6}-1\pm\sqrt{3-2\sqrt{6}}}{2}$ y $\dfrac{-\sqrt{6}-1\pm\sqrt{3+2\sqrt{6}}}{2}.$

6.11.

a) -1 y las raíces de $ax^2+(b-a)x+a$.

b) Divida por x^2 y haga la sustitución $y=x+\dfrac{1}{x}$.

c) -1 y las raíces de $ax^4+(b-a)x^3+(c-b+a)x^2+(b-a)x+a=0$, que es simétrica de grado 4 (como la de *b*)).

6.12.

$\dfrac{1}{3}$ y $-\dfrac{2}{5}.$

6.13.

$$x=\begin{cases}\dfrac{\pi}{3}+2k\pi, & k\in\mathbb{Z}\\[2ex] \dfrac{5\pi}{3}+2k\pi, & k\in\mathbb{Z}\end{cases}$$

6.14.

Por el Teorema Fundamental del Álgebra, $p(x)=0$ tiene n raíces complejas (posiblemente repetidas) $z_1,\ldots,z_n$. Entonces

$$p(x)=a_nx^n+\ldots+a_0=a_n(x-z_1)(x-z_n)=$$

$$=a_n\left[x^n-(z_1+\ldots+z_n)x^{n-1}+(z_1z_2+\ldots+z_{n-1}z_n)x^{n-2}+\right.$$

$$\left.+\ldots+(-1)^n z_1\ldots z_n\right].$$

Se termina identificando coeficientes.

6.15.

a) El mismo argumento utilizado para probar que los múltiplos de $p \in \mathbb{Z}$ forman un ideal en $\mathbb{Z}$.

b) $2x - 1$.

c) $\mathbb{R}[x]/I$ puede identificarse con el conjunto de las rectas en la división euclídea por $x^2 + 1$, es decir, los polinomios de grado menor o igual a 1. Por lo tanto,

$$[ax + b] + [cx + d] = [(a + c)x + (b + d)]$$

$$[ax + b] \cdot [cx + d] = [(ad + bc)x + (bd - ac)].$$

d) $\Phi(a, b) = [bx + a]$ define un isomorfismo entre $\mathbb{C}$ y $\mathbb{R}[x]/I$.

6.16.

La inyectividad es consecuencia del Corolario 6.1: Si $p(\alpha) = q(\alpha)$ para todo $\alpha \in \mathbb{Q}$, entonces $p - q \in \mathbb{Q}[x]$ tiene infinitas raíces racionales y sólo puede ser $p - q = 0$.

En el caso de $\mathbb{Z}_2$, $\mathbb{Z}_2[x]$ tiene infinitos elementos, mientras que sólo hay cuatro aplicaciones de $\mathbb{Z}_2$ en $\mathbb{Z}_2$. Por lo tanto, Φ no puede ser inyectiva.

6.17.

Es verdadera para $K = \mathbb{C}$ (o $\mathbb{R}$, o $\mathbb{Q}$) debido al Corolario 6.1, y falsa para $K = \mathbb{Z}_2$ ($p(x) = x^2 + x$ se anula en 0 y en 1, a pesar de no ser el polinomio nulo).

Capítulo 7

7.1.

a) $\mathbb{Q}(i) = \{a + bi \mid a \in \mathbb{Q} \wedge b \in \mathbb{Q}\}$.

b) $\mathbb{R}(i) = \{a + bi \mid a \in \mathbb{R} \wedge b \in \mathbb{R}\}$.

c) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\right\}$.

7.2.

a) 2.

b) 2.

c) 4.

7.3.

$x^n - 2$ es el polinomio minimal de $\sqrt[n]{2}$ y la base pedida es $\left\{1, \sqrt[n]{2}, \ldots, \sqrt[n]{2^{n-1}}\right\}$.

7.4.

Pueden distinguirse tres casos:

a) $a = 0$ y $b \neq 0$: $\left(0, -\frac{c}{b}\right)$ y $\left(1, -\frac{c}{b}\right)$.

b) $a \neq 0$ y $b = 0$: $\left(-\frac{c}{a}, 0\right)$ y $\left(-\frac{c}{a}, 1\right)$.

c) $a \neq 0 \neq b$: $\left(0, -\frac{c}{b}\right)$ y $\left(1, -\frac{c+a}{b}\right)$.

7.5.

El centro es $\left(-\frac{A}{2}, -\frac{B}{2}\right)$ y el radio $\frac{\sqrt{A^2 + B^2 - 4C}}{2}$.

7.6.

La solución de $\left.\begin{array}{r} ax + by = c \\ a'x + b'y = c' \end{array}\right\}$, que suponemos que tiene solución única, es $\left(\frac{cb' - c'b}{ab' - a'b}, \frac{ac' - a'c}{ab' - a'b}\right) \in \mathbb{Q}^2$.

7.7.

Puede suponerse que γ no es el cuadrado de un número racional. Las intersecciones de la circunferencia $(x - a)^2 + y^2 = \gamma b^2$ con la recta $y = 0$ son $(a \pm b\sqrt{\gamma}, 0)$, por lo que pueden construirse los elementos de $\mathbb{Q}(\sqrt{\gamma}) = \{a + b\sqrt{\gamma} \mid a \in \mathbb{Q} \wedge b \in \mathbb{Q}\}$.

BIBLIOGRAFÍA

A continuación se recomiendan una serie de obras en las que el lector puede consultar y, en ocasiones, profundizar y completar los conceptos expuestos en este libro. Algunas citas bibliográficas van acompañadas de un pequeño comentario acerca de cuáles son los aspectos tratados y con qué nivel.

AIGNER, M. y ZIEGLER, G.M. (1999): *Proofs from THE BOOK*, Ed. Springer, Berlín. Contiene una selección de teoremas cuyas pruebas consideran los autores especialmente brillantes e ingeniosas. Algunos de sus capítulos se refieren a cardinalidad (Cap. 1, 16, 20 y 21), irracionalidad de ciertos números reales (Cap. 6) o álgebra básica (Cap. 5). Nivel intermedio (avanzado en ocasiones).

BELNA, J.P. (2000): *Cantor*, Ed. Les Belles Lettres. Lectura recomendada acerca de la vida y obra de este gran matemático.

BIRKHOFF, G. y McLANE, S. (1980): *Álgebra moderna*, Ed. Vicens-Vives, Barcelona. Trata los temas de estructuras algebraicas con un nivel intermedio.

BOURBAKI, N. (1972): *Elementos de historia de la matemáticas*, Ed. Alianza Universidad.

BOYER, C.B. (1986): *Historia de la matemática*, Alianza Universidad Textos.

BURGER, E. (1968): *Fundamentos del análisis*, Universidad Nacional de San Luis. Cardinales, ordinales y la construcción de los conjuntos numéricos desde la teoría intuitiva de conjuntos, con sucesiones regulares. Nivel intermedio.

CASTELLET, M. y LLERENA, I. (1994): *Álgebra lineal y geometría*, Ed. Reverté/Universitat Autónoma de Barcelona, Barcelona. Nivel intermedio para los temas de teoría de grupos y el anillo de los polinomios.

COHEN, L.W. y EHRLICH, G. (1977): *The estructure of the real number system*, Robert E. Krieger Publishing Company, Inc. Trata la construcción de los sistemas numéricos desde una axiomática de conjuntos, con sucesiones regulares. Nivel intermedio.

COURANT, R. y ROBBINS, H. (1971): *¿Qué es la matemática? Una exposición elemental de sus ideas y métodos*, Ed. Aguilar. Partiendo de conceptos elementales alcanza temas avanzados. De lectura y estudio recomendados; en particular, los temas sobre sistemas de números y construcciones geométricas.

DIEUDONNÉ, J. (1998): *Mathematics-The music of reason*, Ed. Springer, Berlín [basada en Dieudonné, J., *Pour l'honneur de l'esprit humain*, Hachette, 1987]. Es un libro de apreciación matemática de lectura muy recomendable para los usuarios de este texto. Los apéndices tienen dificultad intermedia, y algunos de ellos complementan ciertos capítulos del libro.

DUGUNDJI, J. (1989): *Topology*, Wm. C. Brown Publishers, Dubuque, Iowa. En sus capítulos 1 y 2 trata la teoría de conjuntos, ordinales y cardinales con un nivel intermedio.

DELGADO, F., FUERTES, C. y XAMBÓ, S. (1998): *Introducción al álgebra*, Universidad de Valladolid. Trata los temas de ideales, dominios de integridad, anillo de polinomios y extensiones de cuerpos con un nivel intermedio.

DORRONSORO, J. y HERNÁNDEZ, E. (1996): *Números, grupos y anillos*, Ed. Addison-Wesley/Universidad Autónoma de Madrid, Salamanca. Trata, con un nivel básico, algunos aspectos de los Capítulos 1, 2, 3 y 4.

DURBIN, J.R. (2000): *Modern algebra. An introduction*, Ed. John Wiley & Sons, Inc, USA. Adaptado a todos los capítulos, aunque más profundo en la parte algebraica y más superficial en las construcciones numéricas.

FAVA, N.A. (1978): *El número*, Ed. Docencia, Buenos Aires. Nivel básico para los temas de conjuntos numéricos.

FRAENKEL, A. y BAR-HILLEL, Y. (1973): *Foundations of set theory*. North Holland. Nivel avanzado para el Capítulo 2.

FRALEIGH, J.B. (1987): *Álgebra abstracta*, Ed. Addison-Wesley Iberoamericana, Delaware. Nivel intermedio para los Capítulos 1, 3, 4 y 7.

GARCÍA GARCÍA, J. y LÓPEZ PELLICER, M. (1992): *Álgebra lineal y geometría. Curso teórico-práctico*, Ed. Marfil, Alcoy. Trata, con un nivel básico, los Capítulos 1, 3 y 4 y muy superficialmente las construcciones de los números reales y complejos.

GOLDREI, D. (1996): *Classic set theory*, Ed. Chapman & Hall, London. Trata en profundidad el tema de cardinales y las contrucciones numéricas.

HAMILTON, A.G. (1981): *Lógica para matemáticos*, Paraninfo. Nivel avanzado.

HALMOS, P.R. (1967): *Teoría intuitiva de conjuntos*, Ed. Continental. Nivel intermedio para los temas de estructuras algebraicas.

HERSTEIN, I.N. (1980): *Álgebra moderna: grupos, anillos, cuerpos y teoría de Galois*, Ed. Trillas, México. Trata, con un nivel intermedio, los temas de estructuras algebraicas y el Capítulo 7.

HERSTEIN, I.N. (1988): *Álgebra abstracta*, Grupo Editorial Iberoamérica. Trata, con un nivel intermedio, los temas de estructuras algebraicas y el Capítulo 7.

HUNGERFORTH, T.W. (1974): *Álgebra*, Holt, Rinehart and Winston, Inc. Nivel intermedio para el Capítulo 7.

JOHNSON, D.L. (1998): *Elements of logic via numbers and sets*, Ed. Springer-Verlag, London. Nivel básico para los Capítulos 1 y 2.

KLINE, M. (1992): *El pensamiento matemático de la antigüedad a nuestros días*, Ed. Alianza Universidad, Madrid.

KURATOWSKI, K. (1966): *Introducción a la teoría de conjuntos y a la topología*, Ed. Vicens-Vives, Barcelona. Nivel intermedio para el Capítulo 2.

KUROSH, A.G. (1968): *Curso de álgebra superior*, Ed. MIR. Nivel intermedio para los temas de estructuras algebraicas.

LIPSCHUTZ, S. (1982): *Topología general*, Serie Schaum (Capítulos 1, 2, 3 y 4). Compendio de problemas resueltos de nivel inicial sobre temas de los Capítulos 1 y 2.

MOSTERÍN, J. (2000): *Los lógicos*, Ed. Espasa-Calpe. Barcelona, 2000. Libro de naturaleza biográfica centrado en Frege, Cantor, Russell, Von Neumann, Gödel y Turing. De lectura recomendada.

ROBINSON, A. (1966): *Non-standar analysis*, North Holland. Trata los temas de la contrucción de los números reales y de las proposiciones indemostrables con un nivel avanzado.

RUDIN, W. (1980): *Principios de análisis matemático*, 3/e, McGraw-Hill. Al inicio trata los sistemas de números reales y complejos, y sucesiones numéricas. Nivel intermedio.

SCHECHTER, E. (1997): *Handbook of analysis and its foundations*, Ed. Academic Press, USA. Nivel avanzado para los Capítulos 1, 2 y 7, de lectura farragosa.

SCHUMACHER, C. (1997): *Chapter zero. Fundamental notions of abstract mathematics*, Ed. Addison- Wesley, EE.UU. Nivel básico para los Capítulos 1 y 2.

SINGH, S. (1998): *El enigma de Fermat*, Ed. Planeta, Barcelona. Libro muy recomendable para los alumnos que empiezan a tomar contacto con el lenguaje de las matemáticas. De fácil lectura.

SPIVAK, M. (1970): *Calculus*, Ed. Reverté. Trata, con nivel básico, la construcción de los números reales con un enfoque vía cortaduras y la unicidad.

TORRETTI, R. (1998): *El paraíso de Cantor. La tradición conjuntista en la filosofía matemática*, Ed. Universitaria, S.A. y Universidad Nacional Andrés Bello, Santiago de Chile. Nivel intermedio para los Capítulos 1 y 2.

ÍNDICE ALFABÉTICO

Afijo de un número complejo, 158
Algoritmo de la división, 112
Anillo, 104
  íntegro, 105
  cociente, 106
  con división, 108
  conmutativo, 104
  trivial, 104
  unitario, 104
Anillo de, 105
  Boole, 125
  clases de congruencia, 108
  matrices, 105
  polinomios, 110
Aplicación, 22
  biyectiva, 23
  identidad, 23
  inyectiva, 22
  suprayectiva, 23
Argumento de un número complejo, 161
Automorfismo, 89
Axioma de elección, 66

Bases de Hamel, 66, 177
Bernstein, teorema de, 51
Buen orden, 30
Buena ordenación de cardinales, 66

Campo, 108
Cantor
  paradoja de, 55
  teorema de, 54
Cardinal
  del continuo, 60
  numerable, 57
Cayley, tabla de, 87
Clase de equivalencia, 27
  representante de una, 27
Coeficientes de
  una ecuación lineal, 109
  un polinomio, 110
Combinación lineal, 177
Componentes de un vector, 178
Conjugado de un número complejo, 158
Conjunto, 18
  a lo sumo numerable, 57
  cociente, 27
  complementario, 19
  definición
    por comprehensión, 18
    por extensión, 18
  final de una correspondencia, 22
  imagen de otro, 22
  infinito, finito, 43
  inicial de una correspondencia, 22
  numerable, 57
  preimagen de otro, 22
  singular, 21
  universal, 55
  vacío, 18
Conjuntos equipotentes, 39
Contradicción, 17
Convergencia de
  sucesiones, 122
    en C, 159
    monótonas, 145

Correspondencia, 22
codominio de una, 22
composición, 25
dominio de una, 22
inversa, 25
Cortadura, 142
elemento de separación, 143
Cota
inferior, 29
superior, 29
Cuerpo, 108
algebraicamente cerrado, 167
extensión de otro dado, 176
ordenado, 120
arquimediano, 122
completo, 147
relativamente compacto, 148
Cuerpo de
fracciones
algebraicas, 118
de un dominio de integridad, 116
los números complejos, 157
los números racionales, 117

Demostración
por discusión de casos posibles, 17
por reducción al absurdo, 17
Densidad de Q en R, 139
Desarrollo decimal, 62
de un número real, 138
existencia de, 146
Diferencia
de conjuntos, 19
simétrica de conjuntos, 31
Dimensión de una extensión, 179
Distancia, 121
Divisibilidad de un polinomio por otro, 113
Divisor de cero, 105
Dominio
de integridad, 105
ordenado, 119

Ecuación
cuadrática, 168
discriminante, 169
funcional de Cauchy, 182
lineal, 109
homogénea, 109
incógnitas, 109
término independiente, 109
Eje
imaginario, 157
real, 157
Elemento
imagen de otro, 22
inverso, 83
maximal, 29
máximo, 29
minimal, 29
mínimo, 29
neutro, 83
nulo, 83
opuesto, 83
preimagen de otro, 22
racional de un cuerpo ordenado, 121
simétrico, 83
unidad, 83
Elementos
algebraicos, 179
positivos en un dominio de integridad, 118
trascendentes, 179
Endomorfismo, 89
Enumeración, 57
Epimorfismo, 89
Escalares, 176
Espiral de Arquímedes, 164
Extensión algebraica, 179

Familia de conjuntos, 18
Forma
binómica de un número complejo, 157
exponencial de un número complejo, 163
polar de un número complejo, 161
trigonométrica de un número complejo, 161
Forma proposicional, 18
Fórmula de Euler, 162
Fracción, 115
Función, 24
aditiva, 182
gráfica de una, 24
homogénea, 182
real de variable real, 24
sucesor, 45

Grado de
un polinomio, 111
una extensión algebraica, 179
Grafo de
una correspondencia, 22
Grupo, 84
abeliano, 84
cociente, 90
de permutaciones, 100
teorema de caracterización, 86
trivial, 85

Hipótesis
del continuo, 66
del continuo generalizada, 66
Homomorfismo, 89
de anillos, 107
núcleo de un, 90

Ideal, 107
Igualdad de conjuntos, 19
Inclusión de conjuntos, 19
Infimo, 144
Intersección de conjuntos, 19
Isomorfismo, 89

Ley
de cancelación, 49
de tricotomía, 30
Leyes de
De Morgan, 20
monotonía, 96

Método de
la completación de cuadrados, 168
Módulo de un número complejo, 158
Modus
ponendo ponens, 17
tolendo tolens, 17
Monoide, 84
abeliano, 84
Monomorfismo, 89
Múltiplo de un polinomio, 113

Número
cardinal, 39
natural, 43
Números
algebraicos, 77
complejos, 157
decimales, 139
enteros, 93
positivos, negativos, 95
imaginarios puros, 158
racionales positivos, 120
reales, 134
positivos, 135
trascendentes, 77

Operación binaria, 82
asociativa, 82
cerrada, 83
conmutativa, 82
inducida, 83
producto, 84
proyectada, 84
Operadores lógicos, 15
conjunción, 15
disyunción, 15
equivalencia, 15
implicación, 15
negación, 15
Orden
extendido, 29
inducido, 29
lexicográfico, 33
parcial, 30
total, 30

Par ordenado, 21
Pareja, 21
Parte
imaginaria de un número complejo, 158
real de un número complejo, 158
Partes de un conjunto, 21
Partición de un conjunto, 28
Peano
primer teorema de, 45
segundo teorema de, 46
Permutación, 100
Polinomio
cociente, 112
irreducible, 113
minimal, 180
mónico, 179
resto, 112
Polinomios primos entre sí, 113
Postulado de continuidad, 143

Potencia en base 2 de un cardinal, 42
Primer elemento, 29
Principio
de encaje de intervalos, 141
de inducción completa, 74
de inducción matemática, 47
del palomar, 51
tercio excluso, 17
Producto cartesiano
de dos conjuntos, 21
de una familia de conjuntos, 65
Producto de
cardinales, 41
números complejos, 157
números enteros, 93
Propiedad
antisimétrica, 20
arquimediana, 136
asociativa, 20
conmutativa, 20
del supremo, 144
distributiva, 20
reflexiva, 20
transitiva, 20
triangular, 121
Proposición lógica, 15

Raíz
de un polinomio, 166
orden de multiplicidad, 167
doble, 167
n-ésima, 163
simple, 167
Regla de Ruffini, 167
Relación
antirreflexiva, 28
antisimétrica, 26
binaria, 26
circular, 33
de equipotencia, 39
de equivalencia, 26
compatible con una operación, 83
de orden, 28
compatible con una operación, 50
de pertenencia, 18
reflexiva, 26
simétrica, 26
transitiva, 26
Restricción de
una aplicación, 23
una correspondencia, 33
Rusell, paradoja de, 78

Semigrupo, 84
abeliano, 84
Sistema
compatible, 109
de ecuaciones lineales, 109
determinado, 109
incompatible, 109
indeterminado, 109
Sistema generador, 177
Sistemas axiomáticos
formales, 71
materiales, 72
Subgrupo, 89
teorema de caracterización, 90
Subsucesión, 152
Sucesión, 51
acotada, 131
constante, 131
de Cauchy, 147
de números complejos, 159
nula, 131
recursiva, 51
regular, 131
Suma de
cardinales, 40
números complejos, 157
números enteros, 93
Supremo, 144

Tablas de verdad, 15
Tautología, 15
Teorema
débil de Bezout, 113
de D'Alembert, 167
del resto, 166
fundamental del álgebra, 156, 167

Último elemento, 29
Unidad imaginaria, 157
Unión de conjuntos, 19

Valor absoluto, 121
Vectores, 176
linealmente dependientes, 177
linealmente independientes, 177

Zermelo, teorema de, 66
Zorn, lema de, 66

Impreso en el mes de septiembre de 2000
en Talleres LIBERDÚPLEX, S. L.
Constitución, 19
08014 Barcelona

Otros títulos:

Enric Trillas, Claudi Alsina
y Josep-Maria Terricabras
Introducción a la lógica borrosa

Hermenegildo Fernández-Abascal,
Marta María Guijarro,
José Luis Rojo y José Antonio Sanz
Ejercicios de cálculo de probabilidades. Resueltos y comentados

Jaime Llopis
La estadística: una orquesta hecha instrumento

Antonio Lecuona Newman
y José Ignacio Nogueira
Turbomáquinas

J. M. Rodríguez García, Domingo Pestana,
Elena Romero y Venancio Álvarez
Curso práctico de Cálculo y Precálculo

William H. Schlesinger
Biogeoquímica: un análisis del cambio global

Lotar Beyer y Vicente Fernández Herrero
Química Inorgánica

R. Boyd y J. B. Silk
¿Cómo evolucionan los humanos?

L. Cognetti, M. Jarà y G. Magazzu
Biología marina

Este libro pretende, en primer lugar, entrenar a los alumnos de los dos primeros cursos universitarios en el uso del lenguaje matemático y del método deductivo, de tal forma que puedan leer provechosamente otros textos matemáticos y sean capaces de expresar con precisión y rigor sus propios argumentos. De ahí que comience con una introducción a la lógica y a la teoría intuitiva de conjuntos. A continuación, se presentan las estructuras algebraicas y de orden imprescindibles para fundamentar el análisis matemático, siendo la resolución de ecuaciones algebraicas el hilo conductor de los capítulos centrales, donde se empieza introduciendo los números naturales como los cardinales de los conjuntos finitos y se termina construyendo los números complejos a partir de los reales. El capítulo acerca de los cardinales transfinitos permite reflexionar sobre los límites del método deductivo, en relación con las paradojas que surgen en la teoría intuitiva de conjuntos y la imposibilidad de decidir la verdad o la falsedad de la hipótesis del continuo.

El libro está escrito en un lenguaje inteligible, subraya las raíces intuitivas de muchas ideas matemáticas —ilustradas con figuras apropiadas cuando es posible— y utiliza las aplicaciones de las matemáticas y su historia como elementos motivadores. Este es el propósito del último capítulo, dedicado a las extensiones de cuerpos y a sus aplicaciones a la ecuación funcional de Cauchy, a las bases de Hamel y a la imposibilidad de ciertas construcciones geométricas con regla y compás. Todos los capítulos contienen una amplia colección de problemas resueltos.

http://www.ariel.es

938112-4

9 788434 480261 00

Ariel Ciencia