

# **ALGEBRA ABSTRACTA**

## **PRIMER CURSO**

**John B. Fraleigh**

*Department of Mathematics  
University of Rhode Island*

Versión en español de

**Manuel López Mateos**

*Universidad Nacional Autónoma de México*

Con la colaboración de

**Herminia Ochsenius A.**

*Pontificia Universidad Católica de Chile*



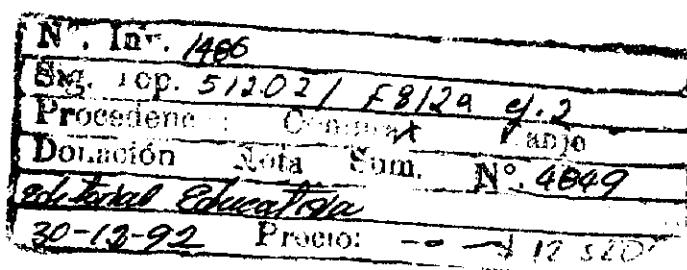
**ADDISON-WESLEY IBEROAMERICANA**

Argentina • Brasil • Chile • Colombia • Ecuador • España  
Estados Unidos • México • Perú • Puerto Rico • Venezuela

Versión en español de la obra titulada *A First Course in Abstract Algebra, third edition*, de John B. Fraleigh, publicada originalmente en inglés por Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, E.U.A. © 1982, 1976, 1967 por Addison-Wesley Publishing Company Inc.

Esta edición en español es la única autorizada.

*A la memoria de mi padre*  
PERCY A. FRAILEIGH



© 1988 por ADDISON-WESLEY IBEROAMERICANA, S. A.  
Wilmington, Delaware, E.U.A.

© 1988 por Sistemas Técnicos de Edición, S. A. de C.V.  
San Marcos, 102. Tlalpan. 14000 México, D.F.

Reservados todos los derechos. Ni todo el libro ni parte de él pueden ser reproducidos, archivados o transmitidos en forma alguna o mediante algún sistema electrónico, mecánico o de fotorreproducción, memoria o cualquier otro, sin permiso por escrito del editor. Miembro de la Cámara Nacional de la Industria Editorial, registro número 1312.

Impreso en México. Printed in Mexico.

ISBN 0-201-64052-X Addison Wesley Iberoamericana  
ISBN 968-858-077-5 Sistemas Técnicos de Edición  
ABCDEFGHIJ-M-898

## Prefacio a la tercera edición

Al igual que en las ediciones anteriores, mi propósito continúa siendo enseñar todo lo posible en un primer curso acerca de grupos, anillos y campos.

Se han eliminado los cuatro capítulos sobre topología algebraica que aparecen marcados con un asterisco en las ediciones anteriores. Me parece que dichas secciones muy pocas veces se cubrían en clase. Se dispone de ejemplares de las ediciones anteriores en bibliotecas y con muchos libreros personales. Cualquier persona que se interese actualmente en leer la breve e intuitiva introducción a la topología algebraica puede localizarlos.

Algunos profesores objetaron la omisión de las demostraciones en las ediciones anteriores donde, en secciones no marcadas con asterisco, simplemente se enunciaron importantes teoremas de la teoría de grupos. Por consiguiente, he añadido secciones marcadas que prueban dichos teoremas. También incluí capítulos sobre la acción de un grupo en un conjunto, seguidos de aplicaciones al conteo de Burnside y a los teoremas de Sylow con demostraciones completas. Se ha incluido un apéndice sobre inducción matemática.

He agregado algunos ejercicios. Tomé en cuenta algunos comentarios y omití las respuestas a los ejercicios pares así como a cualquier ejercicio que requiera demostración. Los ejercicios sobre las demostraciones carecen de sentido cuando éstas se encuentran a sólo treinta segundos de distancia.

Estoy satisfecho de la respuesta que tuvieron la primera y segunda ediciones, no sólo por parte de estudiantes preuniversitarios y de licenciatura, sino además de estudiantes de posgrado que preparan sus exámenes generales. Espero que esta tercera edición continúe siendo útil.

A través de los años he recibido muchas sugerencias y me han corregido diversos errores, lo cual agradezco. Quiero agradecer especialmente a George Bergman, quien me envió doce páginas de comentarios y sugerencias, así como material suplementario, con base en sus experiencias con el libro en el salón de clases. Sus opiniones tuvieron gran influencia en esta revisión.

# Prefacio a la primera edición

El objetivo básico de esta obra es proporcionar un libro de texto a partir del cual el estudiante medio de matemáticas adquiera en un primer curso la mayor exhaustividad y profundidad posibles en el estudio del álgebra abstracta, excluyendo el álgebra lineal. Debido a que el álgebra con frecuencia constituye el primer encuentro del estudiante con una disciplina matemática abstracta, el objetivo secundario es sembrar las semillas a partir de las cuales crecerá una actitud matemática moderna. El dominio de este texto deberá constituir una base firme para un trabajo más especializado en álgebra y será de gran ayuda para cualquier estudio axiomático ulterior de las matemáticas.

De acuerdo con nuestro objetivo secundario, el texto comienza con una sección introductoria acerca del papel de las definiciones en matemáticas, el cual rara vez se menciona. Para poner énfasis en la importancia de las definiciones, cada término, a lo largo del texto, aparece en **negritas** en su definición.

La parte I trata de grupos. El estudio de los grupos y en general de todo el material del texto, toma en cuenta, en la medida de lo posible, la experiencia del estudiante con el álgebra. Con frecuencia resulta difícil, aunque de importancia para el estudiante, comprender el concepto de grupo factor. Por consiguiente, el estudio de grupos factores y homomorfismos se posterga hasta que el estudiante haya tenido tiempo de asimilar el concepto de grupo, para lo cual el análisis es paulatino y detallado.

En las secciones sin asterisco de la parte I, se presentan algunos resultados importantes bien analizados y con abundantes ejemplos, aunque sin demostración. Me parece que en vista de la amplitud del campo de las matemáticas, es importante adiestrar a los estudiantes para entender y hacer uso de resultados aceptados sin sentir que deben corroborar antes cada detalle de las demostraciones. Por supuesto que los matemáticos profesionales lo han hecho durante años. Esta política concuerda con mi objetivo de lograr cierta profundidad en álgebra,

en particular debido a que en muchas escuelas se dedica un solo semestre al estudio de lo que nos ocupa en este libro.

La parte II está dedicada a anillos y campos. No se escatiman esfuerzos para señalar las analogías con el estudio anterior de los grupos. En la parte II se da principal atención al tema de teoría de campos, que nos conduce a la teoría de Galois y la incluye. Los espacios vectoriales se tratan brevemente, sólo con el fin de desarrollar los conceptos de independencia lineal y dimensión, necesarios en teoría de campos. Debido a que los estudiantes suelen encontrar difícil la teoría de campos, he intentado darle un tratamiento paulatino aclarando siempre lo que queremos lograr y cómo lo haremos.

En todo el texto, sin comentarios ni disculpas, se usan propiedades de los racionales que los estudiantes ya conocen aunque nunca hayan visto sus justificaciones rigurosas. Me he dado cuenta que el estudiante medio tiene dificultad para entender la razón de iniciar el estudio formal de resultados que conoce hace años. Despues de haber adquirido una visión global de la naturaleza de las estructuras algebraicas, los estudiantes podrán ver estas propiedades de otra manera. Esta forma de estudio concuerda además con mi objetivo inicial de lograr cierta profundidad en un primer curso.

En vista de que mi deseo es que los estudiantes de álgebra aprendan lo más posible, decidí tratar de manera muy intuitiva el material de teoría de conjuntos, y sólo conforme fuera necesario. Hay dos maneras de adquirir el conocimiento de las aplicaciones de la teoría de conjuntos: estudiarla *per se* o sumergirse en ella y usarla según sea necesario. De acuerdo con mi experiencia, los estudiantes encuentran el estudio de los «prerrequisitos de teoría de conjuntos» al inicio de un curso de álgebra, como la parte más desalentadora. A este respecto, mi enfoque es reflejo de mi disposición a sacrificar a lo largo del libro la elegancia de la presentación matemática y a veces hasta el lenguaje, en aras de la comprensión en este primer curso.

El texto contiene material suficiente para un curso de dos semestres con alumnos medios. Sin embargo, las secciones no marcadas con asterisco se planearon de manera específica con el fin de formar un curso de un semestre. Estas secciones son independientes; en ellas no se emplea el material marcado con asterisco, y representan mi intento de presentar material de cierta profundidad en álgebra, incluso la teoría de Galois, a un grupo medio, en un solo semestre. Desde luego, es posible formar una gran variedad de cursos de un semestre a partir del material disponible. Ciertos capítulos marcados con asterisco son adecuados para su estudio fuera de clase, en particular los capítulos 10, 37, 39 y 48. Si no hay tiempo suficiente para terminar la teoría de campos en el texto, el capítulo 35, que analiza minuciosamente el teorema de Kronecker, o bien el capítulo 39, pueden convertirse en sección final satisfactoria. En mi opinión, no vale la pena comenzar el capítulo 40 si no hay tiempo para terminar el material no marcado con asterisco.

Los ejercicios al final de un capítulo a menudo están divididos en dos grupos por una recta horizontal. Los que se encuentran en la parte superior se recomiendan para un grupo medio y probablemente son los que el autor asignaría a sus alumnos de la Universidad de Rhode Island. Con el objeto de que la transición a

que las matemáticas abstractas sea para los estudiantes tan fácil como sea posible, los ejercicios del primer grupo son sobre todo de cálculos. Los estudiantes medios están completamente perdidos frente a una serie de ejercicios que comienzan con las palabras *probar* o *demostrar*. Claro que el adiestramiento en las demostraciones es importante. Por lo general, el primer grupo de ejercicios contiene alguno marcado con una daga, lo que significa que requiere demostración. Es política del autor reunir estos ejercicios marcados, leerlos y hacer que los estudiantes los reescriban y, si es necesario, capacitarlos para escribir matemáticas y no tontorriadas. Los ejercicios del segundo grupo a menudo incluyen varios que requieren demostración así como algunos adicionales donde se calcula. *El asterisco en un ejercicio no denota dificultad, sino que dicho ejercicio depende de algún material marcado con asterisco en el texto.* Debido a que deseo promover una actitud matemática positiva, algunos ejercicios, en particular al principio del texto, son de naturaleza un tanto matemática. Al final del libro hay respuestas o comentarios acerca de casi todos los ejercicios que no requieren demostraciones. Las demostraciones que se solicitan en los ejercicios no están dadas en las respuestas; no creo que sea pedagógicamente sensato tener tan a la mano dichas demostraciones.

Durante el semestre de primavera de 1966, en la Universidad de Rhode Island, se usó una primera versión mimeografiada de este libro. Quiero expresar aquí mi agradecimiento a George E. Martin quien impartió una de las secciones del curso. Sus comentarios y sugerencias fueron de gran valor al preparar esta versión para su publicación.

J. B. F.

# **Índice general**

## **capítulo 0 Algunas palabras preliminares 1**

- 0.1 El papel de las definiciones 1
- 0.2 Conjuntos 2
- 0.3 Particiones y relaciones de equivalencia 4

## **PARTE I GRUPOS**

### **capítulo 1 Operaciones binarias 10**

- 1.1 Motivación 10
- 1.2 Definición y propiedades 11
- 1.3 Tablas 13
- 1.4 Algunas palabras de advertencia 13

### **capítulo 2 Grupos 18**

- 2.1 Motivación 18
- 2.2 Definición y propiedades elementales 19
- 2.3 Grupos finitos y tablas de grupo 23

### **capítulo 3 Subgrupos 29**

- 3.1 Notación y terminología 29
- 3.2 Subconjuntos y subgrupos 30
- 3.3 Subgrupos cíclicos 33

**capítulo 4 Permutaciones I 37**

- |                               |    |
|-------------------------------|----|
| 4.1 Funciones y permutaciones | 37 |
| 4.2 Grupos de permutaciones   | 40 |
| 4.3 Dos ejemplos importantes  | 42 |

**capítulo 5 Permutaciones II 48**

- |                                   |    |
|-----------------------------------|----|
| 5.1 Ciclos y notación cíclica     | 48 |
| 5.2 Permutaciones pares e impares | 51 |
| 5.3 Grupos alternantes            | 53 |

**capítulo 6 Grupos cíclicos 57**

- |  |    |
|--|----|
| 6.1 Propiedades elementales              | 57 |
| 6.2 Clasificación de grupos cíclicos     | 60 |
| 6.3 Subgrupos de grupos cíclicos finitos | 62 |

**capítulo 7 Isomorfismo 66**

- |  |    |
|--|----|
| 7.1 Definición y propiedades elementales         | 66 |
| 7.2 Cómo mostrar que dos grupos son isomorfos    | 67 |
| 7.3 Cómo mostrar que dos grupos no son isomorfos | 69 |
| 7.4 El teorema de Cayley                         | 71 |

**capítulo 8 Productos directos 78**

- |                                  |    |
|----------------------------------|----|
| 8.1 Productos directos externos  | 78 |
| *8.2 Productos directos internos | 83 |

**capítulo 9 Grupos abelianos finitamente generados 88**

- |                            |    |
|----------------------------|----|
| 9.1 Generadores y torsión  | 88 |
| 9.2 El teorema fundamental | 90 |
| *9.3 Aplicaciones          | 93 |

**\*capítulo 10 Grupos en geometría y análisis 97**

- |                           |     |
|---------------------------|-----|
| *10.1 Grupos en geometría | 97  |
| *10.2 Grupos en análisis  | 102 |

**capítulo 11 Grupos de clases laterales 106**

- 11.1 Introducción 106
- 11.2 Clases laterales 107
- 11.3 Aplicaciones 112

**capítulo 12 Subgrupos normales y grupos factores 116**

- 12.1 Criterios para la existencia de un grupo de clases laterales 116
- 12.2 Automorfismos internos y subgrupos normales 118
- 12.3 Grupos factores 120
- 12.4 Grupos simples 123
- \*12.5 Aplicaciones 124

**capítulo 13 Homomorfismos 130**

- 13.1 Definición y propiedades elementales 130
- 13.2 El teorema fundamental del homomorfismo 133
- 13.3 Aplicaciones 135

**capítulo 14 Series de grupos 139**

- 14.1 Series normales y subnormales 139
- 14.2 El teorema de Jordan-Hölder 141
- \*14.3 El centro y la serie central ascendente 144

**\*capítulo 15 Teoremas del isomorfismo; demostración del teorema de Jordan-Hölder 146**

- \*15.1 Teoremas del isomorfismo 146
- \*15.2 El lema de Zassenhaus (de la mariposa) 149
- \*15.3 Demostración del teorema de Schreier 150

**\*capítulo 16 Acción de un grupo en un conjunto 155**

- \*16.1 El concepto de acción de grupo 155
- \*16.2 Conjuntos fijos y subgrupos de isotropia 157
- \*16.3 Orbitas 158

**\*capítulo 17 Aplicaciones de los  $G$ -conjuntos al conteo 162**

**\*capítulo 18 Teoremas de Sylow 167**

- \*18.1 *p*-grupos 167
- \*18.2 Los teoremas de Sylow 169

**\*capítulo 19 Aplicaciones de la teoría de Sylow 174**

- \*19.1 Aplicaciones a *p*-grupos y la ecuación de clase 174
- \*19.2 Aplicaciones ulteriores 176

**\*capítulo 20 Grupos abelianos libres 181**

- \*20.1 Grupos abelianos libres 181
- \*20.2 Demostración del teorema fundamental 184

**\*capítulo 21 Grupos libres 190**

- \*21.1 Palabras y palabras reducidas 190
- \*21.2 Grupos libres 191
- \*21.3 Homomorfismos de grupos libres 193
- \*21.4 Más sobre grupos abelianos libres 194

**\*capítulo 22 Presentaciones de grupos 197**

- \*22.1 Definición 197
- \*22.2 Presentaciones isomórficas 198
- \*22.3 Aplicaciones 200

**PARTE II ANILLOS Y CAMPOS**

**capítulo 23 Anillos 208**

- 23.1 Definición y propiedades básicas 208
- 23.2 Cuestiones multiplicativas; campos 211

**capítulo 24 Dominios enteros 215**

- 24.1 Divisores de 0 y cancelación 215
- 24.2 Dominios enteros 217
- 24.3 Característica de un anillo 218
- 24.4 Teorema de Fermat 219
- \*24.5 Generalización de Euler 220

**\*capítulo 25 Algunos ejemplos no conmutativos 224**

- \*25.1 Matrices sobre un campo 224**
- \*25.2 Anillos de endomorfismos 227**
- \*25.3 Anillos de grupo y álgebra de grupo 230**
- \*25.4 Cuaterniones 232**

**capítulo 26 El campo de cocientes de un dominio entero 237**

- 26.1 La construcción 237**
- 26.2 Unicidad 242**

**capítulo 27 Nuestro objetivo fundamental 246**

**capítulo 28 Anillos cocientes e ideales 250**

- 28.1 Introducción 250**
- 28.2 Criterios para la existencia de un anillo de clases laterales 251**
- 28.3 Ideales y anillos cocientes 253**

**capítulo 29 Homomorfismos de anillos 257**

- 29.1 Definición y propiedades elementales 257**
- 29.2 Ideales maximales y primos 259**
- 29.3 Campos primos 262**

**capítulo 30 Anillos de polinomios 266**

- 30.1 Polinomios en una indeterminada 266**
- 30.2 Homomorfismos de evaluación 270**
- 30.3 El nuevo enfoque 273**

**capítulo 31 Factorización de polinomios sobre un campo 277**

- 31.1 El algoritmo de la división en  $F[x]$  277**
- 31.2 Polinomios irreducibles 281**
- 31.3 Estructura de ideal en  $F[x]$  285**
- 31.4 Unicidad de la factorización en  $F[x]$  286**

**\*capítulo 32 Dominios de factorización única 291**

- \*32.1 Introducción 291**
- \*32.2 Todo DIP es un DFU 293**
- \*32.3 Si  $D$  es un DFU, entonces  $D[x]$  es un DFU 297**

**\*capítulo 33 Dominios euclidianos 304**

- \*33.1 Introducción y definición 304**
- \*33.2 Aritmética en dominios euclidianos 305**

**\*capítulo 34 Enteros gaussianos y normas 312**

- \*34.1 Enteros gaussianos 312**
- \*34.2 Normas multiplicativas 315**

**capítulo 35 Introducción a los campos de extensión 320**

- 35.1 El objetivo fundamental alcanzado 320**
- 35.2 Elementos algebraicos y trascendentes 322**
- 35.3 El polinomio irreducible de  $\alpha$  sobre  $F$  324**
- 35.4 Extensiones simples 325**

**capítulo 36 Espacios vectoriales 331**

- 36.1 Definición y propiedades elementales 331**
- 36.2 Independencia lineal y bases 333**
- 36.3 Dimensión 335**
- 36.4 Una aplicación a la teoría de campos 338**

**\*capítulo 37 Otras estructuras algebraicas 342**

- \*37.1 Grupos con operadores 342**
- \*37.2 Módulos 344**
- \*37.3 Álgebras 345**

**capítulo 38 Extensiones algebraicas 348**

- 38.1 Extensiones finitas 348**
- 38.2 Campos algebraicamente cerrados y cerraduras algebraicas 352**
- \*38.3 Existencia de una cerradura algebraica 354**

**\*capítulo 39 Construcciones geométricas 360**

- \*39.1 Números construibles 360**
- \*39.2 Imposibilidad de ciertas construcciones 364**

**capítulo 40 Automorfismos de campos 368**

- 40.1 Isomorfismos básicos de la teoría de los campos algebraicos 368
- 40.2 Automorfismos y campos fijos 371
- 40.3 El automorfismo de Frobenius 375

**capítulo 41 El teorema de extensión de isomorfismos 379**

- 41.1 El teorema de extensión 379
- 41.2 Índice de un campo de extensión 381
- \*41.3 Demostración del teorema de extensión 384

**capítulo 42 Campos de descomposición 388**

**capítulo 43 Extensiones separables 394**

- 43.1 Multiplicidad de los ceros de un polinomio 394
- 43.2 Extensiones separables 396
- 43.3 Campos perfectos 398
- \*43.4 Teorema del elemento primitivo 400

**\*capítulo 44 Extensiones totalmente inseparables 404**

- \*44.1 Extensiones totalmente inseparables 404
- \*44.2 Cerraduras separables 406

**capítulo 45 Campos finitos 409**

- 45.1 Estructura de un campo finito 409
- 45.2 La existencia de  $\text{CG}(p^n)$  411

**capítulo 46 Teoría de Galois 415**

- 46.1 Resumen 415
- 46.2 Extensiones normales 416
- 46.3 El teorema principal 417
- 46.4 Grupos de Galois sobre campos finitos 420
- \*46.5 Final de la demostración del teorema principal 421

**\*capítulo 47 Ilustraciones de la teoría de Galois 426**

- \*47.1 Funciones simétricas 426
- \*47.2 Ejemplos 428

## ①

## Algunas palabras preliminares

### 0.1 EL PAPEL DE LAS DEFINICIONES

La mayoría de los estudiantes no comprenden la enorme importancia que tienen las definiciones en matemáticas. Esta importancia surge, en parte, de la necesidad de los matemáticos de comunicarse entre si acerca de su trabajo. Si dos personas que tratan de intercambiar opiniones acerca de un tema tienen ideas diferentes acerca del significado de ciertos términos técnicos, puede haber malos entendidos, fricciones y, quizás, hasta derramamiento de sangre. Imaginen los aprietos en que se encuentra un carnicero frente a un cliente iracundo que trata de comprar lo que todo el mundo llama un costillar pero él insiste en llamar lomo. Desafortunadamente, parece imposible alcanzar el ideal de una terminología generalizada, ni siquiera entre seres tan precisos como los matemáticos. Por ejemplo, cuando se habla de funciones en matemáticas, los matemáticos han dado, al término *rango*, dos significados distintos. Es por ello que, hoy día se tiende a evitar el uso de este término ambiguo y en su lugar, se usa *imagen* o *contradominio*. *En matemáticas debemos luchar para evitar ambigüedades.*

Un ingrediente muy importante de la creatividad matemática es la capacidad de elaborar definiciones útiles que conduzcan a resultados interesantes.

Un estudiante que inicia estudios de posgrado podría pensar que invierte mucho tiempo discutiendo definiciones con sus compañeros. Cuando el autor hacia estudios de posgrado oyó quejarse a un estudiante de física, quien afirmaba que durante la comida los estudiantes de matemáticas siempre se sentaban juntos y discutían, y que el objeto de sus discusiones era siempre una definición. Es común, en los exámenes orales, preguntar definiciones. Si un estudiante no puede explicar el significado de un término, probablemente tampoco pueda dar respuestas sensatas a preguntas que incluyan dicho concepto.

Se entiende que toda definición es una proposición del tipo *si y sólo si* aunque se acostumbre suprimir el *sólo si*. Por tanto, cuando definimos: «un triángulo es isósceles si tiene dos lados de igual longitud», en realidad queremos decir que un triángulo es isósceles si y sólo si tiene dos lados de igual longitud. Ahora bien, no piensen que es necesario memorizar una definición palabra por palabra. Lo importante es *comprender* el concepto para que cada estudiante pueda definir precisamente ese mismo concepto con sus propias palabras. Así, la definición «un triángulo isósceles es aquel que tiene dos lados iguales», es totalmente correcta. También es correcta la definición «un triángulo isósceles es aquel que tiene dos ángulos iguales», pues los triángulos que llamamos isósceles en estas definiciones, son los mismos.

Es importante notar que una vez definido un concepto, para probar algo con respecto a dicho concepto, se *debe* usar la definición como parte de la demostración. *Inmediatamente después de definir un concepto, la definición es la única información disponible acerca del concepto.*

A lo largo del libro, cuando un término aparece en negritas, es porque se está *definiendo*. Los principales conceptos algebraicos se definen de manera explícita; muchos otros se destacan con negritas, sin dar una definición explícita. De esta forma se destacarán ideas en párrafos del libro, teoremas y ejercicios.

## 0.2 CONJUNTOS

La importancia básica de las definiciones en matemáticas es también una debilidad estructural, por la razón de que no todos los conceptos usados pueden definirse. Supongamos, por ejemplo, que definimos el término *conjunto*: «un **conjunto** es una colección bien definida de objetos». Es natural preguntarse de inmediato el significado de *colección*. Quizá definamos entonces: «una colección es un agregado de cosas». ¿Y qué es un *agregado*? Ahora, como nuestro lenguaje es finito, después de algún tiempo se nos acabarán las palabras nuevas y tendremos que repetir algunas de las ya cuestionadas. Entonces, la definición es circular y, obviamente, carece de sentido. Los matemáticos saben que debe haber algunos conceptos sin definición o primitivos. Por el momento, están de acuerdo en que *conjunto* debe ser uno de dichos conceptos primitivos. No definiremos *conjunto*, pero esperamos que al usar expresiones como «el conjunto de todos los números reales» o «el conjunto de todos los miembros del senado de Estados Unidos», las ideas que de su significado tienen distintas personas sean lo bastante similares para permitir la comunicación.

Resumimos brevemente algunas de las cuestiones que se asumirán con respecto a los conjuntos.

- 1 Un conjunto *S* está formado por **elementos**, y si *a* es uno de estos elementos, lo denotaremos por  $a \in S$ .
- 2 Existe sólo un conjunto sin elementos. Es el **conjunto vacío**, que denotamos por  $\emptyset$ .

- 3 Podemos describir un conjunto aludiendo a una propiedad que caracterice a los elementos, como «el conjunto de todos los miembros del senado de Estados Unidos», o listando los elementos. La manera usual de describir un conjunto mediante el listado de sus elementos, consiste en encerrar en llaves las designaciones de los elementos, separados por comas, por ejemplo,  $\{1, 2, 15\}$ . Si se describe un conjunto mediante la propiedad  $P(x)$  que caracteriza a sus elementos  $x$ , también es común usar la notación  $\{x \mid P(x)\}$ , que se lee «el conjunto de todas las  $x$  tales que la proposición  $P(x)$  acerca de  $x$  es verdadera». Así,

$$\begin{aligned}\{2, 4, 6, 8\} &= \{x \mid x \text{ es un número entero positivo par } \leq 8\} \\ &= \{2x \mid x = 1, 2, 3, 4\}.\end{aligned}$$

- 4 Decir que un conjunto está **bien definido**, significa que si  $S$  es un conjunto y  $a$  es un objeto, entonces, o  $a$  está sin lugar a dudas en  $S$ , lo que se denota por  $a \in S$ , o  $a$ , sin lugar a dudas, no está en  $S$ , lo que se denota por  $a \notin S$ . Por tanto, no debemos decir: «considérese el conjunto  $S$  de algunos números positivos», pues no está definido si  $2 \in S$  o  $2 \notin S$ . Por otra parte, si podemos considerar el conjunto  $T$  de todos los enteros positivos primos. Todo entero positivo es definitivamente primo o no lo es. Así,  $5 \in T$  y  $14 \notin T$ . En la práctica puede ser difícil determinar si un objeto está realmente en un conjunto. Por ejemplo, cuando este libro entró a la imprenta no se sabía si  $2^{(2^{17})} + 1$  estaba en  $T$ ; sin embargo,  $2^{(2^{17})} + 1$  con certeza o es primo, o no lo es.

Para el estudiante al cual está dirigido este libro, no será posible basar cada definición en el concepto de conjunto. El autor está consciente de que construye sobre definiciones muy intuitivas, particularmente, al principio del libro. La primera definición del capítulo 1 dice: «una **operación binaria en un conjunto** es una regla ... conjunto». Y ... ¿qué es una regla?

En este libro trabajaremos con varios conjuntos de números ya conocidos. Abordaremos el asunto de la notación de estos conjuntos de una vez y para siempre.

**Z** es el conjunto de todos los enteros (es decir, números enteros: positivos, negativos y cero).

**Z<sup>+</sup>** es el conjunto de todos los enteros positivos. (Se excluye el cero.)

**Q** es el conjunto de todos los números racionales (esto es, números que pueden expresarse como el cociente  $m/n$  de enteros, donde  $n \neq 0$ ).

**Q<sup>+</sup>** es el conjunto de todos los números racionales positivos.

**R** es el conjunto de todos los números reales.

**R<sup>+</sup>** es el conjunto de todos los números reales positivos.

**C** es el conjunto de todos los números complejos.

### 0.3 PARTICIONES Y RELACIONES DE EQUIVALENCIA

Se describió  $\mathbb{Q}$  como el conjunto de todos los números que pueden expresarse como cocientes  $m/n$  de enteros, donde  $n \neq 0$ . Sería incorrecto describir  $\mathbb{Q}$  como el conjunto  $S$  de todas las «expresiones cociente»  $m/n$  para  $m$  y  $n$  en  $\mathbb{Z}$  y  $n \neq 0$ , pues, claramente,  $\frac{2}{3}$  y  $\frac{4}{6}$  son expresiones de cociente distintas pero sabemos que representan el *mismo* número racional. De hecho, cada elemento de  $\mathbb{Q}$  está representado por un número infinito de distintos elementos de  $S$ . En aritmética, *identificamos* como uno solo a los elementos de  $S$  que representan el mismo número racional en  $\mathbb{Q}$ .

La ilustración del párrafo anterior es típica de algunas situaciones en las que consideraremos elementos diferentes de un conjunto como aritmética o algebraicamente equivalentes, de manera que nuestro conjunto se *parte* en celdas, cada una de las cuales podremos considerar como una entidad aritmética o algebraica única. Si  $b$  es un elemento de dicho conjunto,  $b$  representa, por lo general, la celda de todos los elementos identificados con  $b$ . Por ejemplo, en el conjunto anterior  $S$  de cocientes formales, tenemos

$$\begin{aligned}\overline{2/3} &= \left\{ \frac{2}{3}, \frac{-2}{-3}, \frac{4}{6}, \frac{-4}{-6}, \frac{6}{9}, \frac{-6}{-9}, \dots \right\} \\ &= \left\{ \frac{2n}{3n} \mid n \in \mathbb{Z} \text{ y } n \neq 0 \right\}.\end{aligned}$$

Demos una definición precisa de dicha partición.

**Definición** Una *partición de un conjunto* es una descomposición del conjunto en celdas, tales que todo elemento del conjunto está en *exactamente una* de las celdas.

Dos celdas (o conjuntos) que no tengan elementos en común son **ajenas**. Así, las celdas de una partición de un conjunto son ajenas.

¿Cómo sabremos si dos expresiones cocientes  $m/n$  y  $r/s$  de nuestro conjunto  $S$  anterior están en la misma celda, esto es, si representan al mismo número racional? Una manera de decidirlo es reducir ambas fracciones a su expresión más simple. Esto puede ser difícil; por ejemplo,  $1909/4897$  y  $1403/3599$  representan el mismo número racional, pues

$$\frac{1909}{4897} = \frac{23 \cdot 83}{59 \cdot 83} \quad \text{y} \quad \frac{1403}{3599} = \frac{23 \cdot 61}{59 \cdot 61}.$$

Sin embargo, aun con una calculadora manual, puede ser difícil encontrar estas factorizaciones, es una tarea de adivinar y corregir un poco tediosa. Pero como

saben, en aritmética de fracciones sucede que  $m/n = r/s$  si y sólo si  $ms = nr$ . Esto nos da un criterio más eficaz para resolver nuestro problema, a saber,

$$(1909)(3599) = (4897)(1403) = 6\,870\,491.$$

Denotemos por  $a \sim b$  el hecho de que  $a$  está en la misma celda que  $b$  para una partición dada de un conjunto que contenga tanto a  $a$  como a  $b$ . Es claro que siempre se satisfacen las propiedades siguientes:

$a \sim a$ . El elemento  $a$  está en la misma celda que él mismo.

*Si  $a \sim b$  entonces  $b \sim a$ .* Si  $a$  está en la misma celda que  $b$ , entonces  $b$  está en la misma celda que  $a$ .

*Si  $a \sim b$  y  $b \sim c$ , entonces  $a \sim c$ .* Si  $a$  está en la misma celda que  $b$  y  $b$  está en la misma celda que  $c$ , entonces  $a$  está en la misma celda que  $c$ .

El siguiente teorema es fundamental; afirma que una relación  $\sim$  entre elementos de un conjunto que satisface las tres propiedades recién descritas, produce una partición natural del conjunto. Muchas veces, exhibir una relación con estas propiedades, es la forma más concisa de describir una partición de un conjunto, y es por esta razón que analizamos ahora este material.

**Teorema 0.1** *Sea  $S$  un conjunto no vacío y sea  $\sim$  una relación entre elementos de  $S$  que satisface las propiedades siguientes:*

- 1 *(Reflexividad)*  $a \sim a$  para todas las  $a \in S$ .
- 2 *(Simetría)* Si  $a \sim b$ , entonces  $b \sim a$ .
- 3 *(Transitividad)* Si  $a \sim b$  y  $b \sim c$ , entonces  $a \sim c$ .

*Entonces,  $\sim$  produce una partición natural de  $S$ , donde*

$$\bar{a} = \{x \in S \mid x \sim a\}$$

*es la celda que contiene a a para todas las  $a \in S$ . Recíprocamente, cada partición de  $S$  da lugar a una relación natural  $\sim$  que satisface las propiedades reflexiva, simétrica y transitiva si se define  $a \sim b$  como  $a \in \bar{b}$ .*

**Demostración** Ya hemos demostrado la parte «recíproca» del teorema.

Para la afirmación directa, sólo falta demostrar que las celdas definidas por  $\bar{a} = \{x \in S \mid x \sim a\}$  si constituyen, en efecto, una partición de  $S$ , esto es, que todo elemento de  $S$  está en *exactamente una* celda. Sea  $a \in S$ . Entonces  $a \in \bar{a}$ , por la condición 1, de modo que  $a$  está en *al menos una* celda.

Supongamos ahora que  $a$  también estuviera en la celda  $\bar{b}$ . Es necesario mostrar que  $\bar{a} = \bar{b}$  como conjuntos; esto mostraría que  $a$  no puede estar en más de una celda. Para ello mostramos que cada elemento de  $\bar{a}$  está en  $\bar{b}$  y cada elemento de  $\bar{b}$  está en  $\bar{a}$ . Sea  $x \in \bar{a}$ . Entonces,  $x \sim a$ . Pero  $a \in \bar{b}$ , luego  $a \sim b$ ; entonces, por la condición transitiva (3),  $x \sim b$  de modo que  $x \in \bar{b}$ . Así,  $\bar{a}$  es parte de  $\bar{b}$ . Sea ahora  $y \in \bar{b}$ . Entonces  $y \sim b$ . Pero  $a \in \bar{b}$ , de manera que  $a \sim b$  y, por simetría (2),  $b \sim a$ . Entonces, por transitividad,  $y \sim a$ , de modo que  $y \in \bar{a}$ . De aquí

## 6 ALGUNAS PALABRAS PRELIMINARES

que  $\bar{b}$  también es parte de  $\bar{a}$  y, por tanto,  $\bar{b} = \bar{a}$ , con lo cual queda completa nuestra demostración. ■

**Definición** Una relación  $\sim$  en un conjunto  $S$ , que satisface las propiedades reflexiva, simétrica y transitiva descritas en el teorema 0.1, es una *relación de equivalencia en  $S$* . Cada celda  $\bar{a}$  en la partición natural dada por una relación de equivalencia es una *clase de equivalencia*.

Por lo general, reservamos el símbolo  $\sim$  para una relación de equivalencia. Usaremos  $\mathcal{R}$  para una relación entre elementos de un conjunto  $S$  que no es por fuerza una relación de equivalencia en  $S$ .

El término *natural*, que aparece dos veces en el teorema 0.1, tiene el siguiente significado: si se empieza con una relación de equivalencia, luego se forma la partición de clases de equivalencia y se considera después la relación dada por esta partición, se trata de la relación de equivalencia original. En forma análoga, si se comienza con una partición, luego se pasa a la relación de equivalencia y después se construyen las clases de equivalencia, se obtiene la partición original.

**Ejemplo 0.1** Verifíquese directamente que

$$m/n \sim r/s \text{ si y sólo si } ms = nr$$

es una relación de equivalencia en el conjunto  $S$  de expresiones cociente formales que consideramos antes.

*Reflexividad.*  $m/n \sim m/n$ , puesto que  $mn = nm$ .

*Simetría.* Si  $m/n \sim r/s$ , entonces,  $ms = nr$ . De aquí que  $rn = sm$  y, por tanto,  $r/s \sim m/n$ .

*Transitividad.* Si  $m/n \sim r/s$  y  $r/s \sim u/v$ , entonces  $ms = nr$  y  $rv = su$ . Reordenando términos y sustituyendo, obtenemos  $mvs = vms = vnr = nrv = nsu = nus$ . Como  $s \neq 0$ , deducimos que  $mv = nu$ , entonces,  $m/n \sim u/v$ .

Se considera que cada clase de equivalencia de  $S$  es un número racional. ■

El análisis del conjunto  $S$  de expresiones cociente formales que culminó con el ejemplo 0.1 es un caso particular del trabajo que llevaremos a cabo en el capítulo 26.

**Ejemplo 0.2** Definase una relación  $\mathcal{R}$  en el conjunto  $\mathbb{Z}$  mediante  $n \mathcal{R} m$  si y sólo si  $nm \geq 0$  y véase si  $\mathcal{R}$  es una relación de equivalencia.

*Reflexividad.*  $a \mathcal{R} a$ , pues  $a^2 \geq 0$  para toda  $a \in \mathbb{Z}$ .

*Simetría.* Si  $a \mathcal{R} b$ , entonces  $ab \geq 0$ ; por tanto,  $ba \geq 0$  y  $b \mathcal{R} a$ .

*Transitividad.* Si  $a \mathcal{R} b$  y  $b \mathcal{R} c$ , entonces  $ab \geq 0$  y  $bc \geq 0$ . Entonces,  $ab^2c = acb^2 \geq 0$ . Si supiéramos que  $b^2 > 0$ , podríamos deducir que  $ac \geq 0$  y, por tanto, que  $a \mathcal{R} c$ . Debemos examinar por separado el caso en que  $b = 0$ .

Pensándolo bien vemos que  $-3 \not\sim 0$  y  $0 \not\sim 5$ , pero  $-3 \sim 5$ , así que la relación  $\sim$  no es transitiva y, por tanto, no es una relación de equivalencia. ■

Para cada  $n \in \mathbb{Z}^+$  tenemos una relación de equivalencia en  $\mathbb{Z}$  muy importante: la **congruencia módulo  $n$** . Para  $h, k \in \mathbb{Z}$  definimos  $h$  congruente con  $k$  módulo  $n$ , lo cual se escribe  $h \equiv k \pmod{n}$ , si  $h - k$  es divisible entre  $n$ , es decir, que  $h - k = ns$  para alguna  $s \in \mathbb{Z}$ . Por ejemplo,  $17 \equiv 33 \pmod{8}$  puesto que  $17 - 33 = 8(-2)$ . Las clases de equivalencia para la congruencia módulo  $n$  son las **clases residuales módulo  $n$** . Cada una de estas clases residuales contiene un número infinito de elementos. Por ejemplo, pueden convencerse fácilmente de que, para la congruencia módulo 8, la clase residual que contiene el 17 y el 33 es

$$\{\dots, -47, -39, -31, -23, -15, -7, 1, 9, 17, 25, 33, 41, 49, \dots\}.$$

Esta clase residual contiene cada octavo número, comenzando con 1. De hecho, hay siete clases residuales más en la partición dada por la congruencia módulo 8.

En el ejercicio 0.18 pedimos mostrar que, en efecto, la congruencia módulo  $n$  es una relación de equivalencia y que examinen algunas otras clases residuales.

## Ejercicios

---

*En los ejercicios 1 al 4, describase el conjunto listando sus elementos.*

0.1  $\{x \in \mathbb{R} \mid x^2 = 3\}$

0.2  $\{m \in \mathbb{Z} \mid m^2 = 3\}$

0.3  $\{m \in \mathbb{Z} \mid mn = 60 \text{ para alguna } n \in \mathbb{Z}\}$

0.4  $\{m \in \mathbb{Z} \mid m^2 - m < 115\}$

*En los ejercicios 5 al 10 digase si lo descrito es en efecto un conjunto (si está bien definido). Dese otra descripción para cada conjunto.*

0.5  $\{n \in \mathbb{Z}^+ \mid n \text{ es un número grande}\}$

0.6  $\{n \in \mathbb{Z} \mid n^2 < 0\}$

0.7  $\{n \in \mathbb{Z} \mid 39 < n^3 < 57\}$

0.8  $\{x \in \mathbb{Q} \mid \text{el denominador de } x \text{ es mayor que } 100\}$

0.9  $\{x \in \mathbb{Q} \mid \text{se puede escribir } x \text{ con denominador mayor que } 100\}$

0.10  $\{x \in \mathbb{Q} \mid x \text{ se puede escribir con denominador menor que } 3\}$

*En los ejercicios 11 al 19, determinese si la relación dada es una relación de equivalencia en el conjunto. Describase la partición que surge de cada relación de equivalencia.*

0.11  $n \mathcal{R} m \text{ en } \mathbb{Z} \text{ si } nm > 0$

0.12  $x \mathcal{R} y \text{ en } \mathbb{R} \text{ si } x \geq y$

0.13  $x \mathcal{R} y \text{ en } \mathbb{R} \text{ si } |x| = |y|$

0.14  $x \mathcal{R} y \text{ en } \mathbb{R} \text{ si } |x - y| \leq 3$

0.15  $n \mathcal{R} m \text{ en } \mathbb{Z}^+ \text{ si } n \text{ y } m \text{ tienen el mismo número de dígitos en la notación usual de base diez.}$

0.16  $n \mathcal{R} m \text{ en } \mathbb{Z}^+ \text{ si } n \text{ y } m \text{ tienen el mismo dígito final en la notación usual de base diez.}$

## **8 ALGUNAS PALABRAS PRELIMINARES**

**0.17**  $n \not\sim m$  en  $\mathbb{Z}^+$  si  $n - m$  es divisible entre 2.

**0.18** Sea  $n$  un entero en  $\mathbb{Z}^+$ , muéstrese que la congruencia módulo  $n$  es una relación de equivalencia en  $\mathbb{Z}$ . Describanse las clases residuales para  $n = 1, 2, 3$ .

**0.19** El siguiente es un famoso argumento falso. Encuéntrese el error. «El criterio de reflexividad es redundante en las condiciones para una relación de equivalencia, ya que de  $a \sim b$  y  $b \sim a$  (simetría) deducimos  $a \sim a$  por transitividad.»

*En los ejercicios 20 al 24, encuéntrese el número de relaciones de equivalencia posibles en un conjunto  $S$ , a partir del número de sus elementos. (Usar el teorema 0.1.)*

**0.20** 1 elemento

**0.21** 2 elementos

**0.22** 3 elementos

**0.23** 4 elementos

**0.24** 5 elementos

**PARTE**



# **GRUPOS**

# Operaciones binarias

## 1.1 MOTIVACION

¿Cuál es el ingrediente básico del álgebra? El primer contacto de un niño con el álgebra se da cuando se le enseña a sumar y multiplicar números. Analicemos lo que en realidad sucede.

Supongamos que ustedes visitan una civilización desconocida en un mundo desconocido y observan a una criatura de ese mundo, en un salón de clases, enseñando a sumar a otras criaturas. Supongamos además que ustedes ignoran que el grupo aprende a sumar; ustedes simplemente están colocados en esa habitación como observadores y se pide hacer un informe sobre lo que han visto exactamente. El maestro emite unos ruidos que suenan aproximadamente como *glup, poit*. Los alumnos responden *bimt*. A continuación el maestro dice *ompt, gaft* y los alumnos responden *poit*. ¿Qué están haciendo? Ustedes no pueden informar que están sumando números, pues ni siquiera saben que los sonidos representan números. Naturalmente, ustedes comprenden que existe comunicación. Todo lo que pueden decir con seguridad es que estas criaturas conocen alguna regla, de manera que al designarse ciertos pares de cosas en su lenguaje, una después de otra, como *glup, poit*, ellos pueden ponerse de acuerdo en una respuesta, *bimt*. Este proceso es igual al que ocurre en un aula de primer año al enseñar a sumar; el maestro dice *cuatro, siete* y los alumnos responden *once*.

De este modo, al analizar la suma y la multiplicación de números, vemos que la suma es básicamente una regla que se aprende y que nos permite asociar a cada dos números en un orden dado, un número como respuesta. La multiplicación también es una regla, pero diferente. Por último, nótese que al jugar con los estudiantes, los maestros deben tener algo de cuidado acerca de los pares de cosas que dicen. Si de repente un maestro de primer año dice *diez, cielo*, los pobres

alumnos se confundirán. La regla está definida sólo para pares de elementos del mismo conjunto.

## 1.2 DEFINICION Y PROPIEDADES

Como matemáticos, tratemos de recoger la parte medular de estas ideas básicas en una definición útil. Como ya dijimos en la sección introductoria, no intentamos definir un conjunto.

**Definición** Una *operación binaria \* en un conjunto*, es una regla que asigna a cada par ordenado de elementos de un conjunto, algún elemento del conjunto.

La palabra *ordenado* es muy importante en esta definición, pues da la posibilidad de que el elemento asignado al par  $(a, b)$  pueda ser diferente del elemento asignado al par  $(b, a)$ . También tuvimos cuidado de no decir que a cada par ordenado de elementos se le asigna *otro o un tercer elemento*, pues queremos permitir casos tales como los que ocurren en la suma de números, donde a  $(0, 2)$  se le asigna el número 2.

En las primeras secciones denotaremos por  $a * b$  al elemento asignado al par  $(a, b)$  por  $*$ . Si en un análisis simultáneo hay diferentes operaciones binarias, se usarán subíndices o supraíndices en  $*$  para distinguirlos. El método más importante para describir una operación binaria particular  $*$  en un conjunto dado es el de caracterizar al elemento  $a * b$  asignado a cada par  $(a, b)$  mediante alguna propiedad definida en términos de  $a$  y  $b$ .

**Ejemplo 1.1** Definase en  $\mathbb{Z}^+$  una operación binaria  $*$  por  $a * b$  que es igual al mínimo entre  $a$  y  $b$  o al valor común si  $a = b$ . Así,  $2 * 11 = 2$ ;  $15 * 10 = 10$  y  $3 * 3 = 3$ . ■

**Ejemplo 1.2** Definase en  $\mathbb{Z}^+$  una operación binaria  $*'$  mediante  $a *' b = a$ . Así,  $2 *' 3 = 2$ ;  $25 *' 10 = 25$  y  $5 *' 5 = 5$ . ■

**Ejemplo 1.3** Definase en  $\mathbb{Z}^+$  una operación binaria  $*''$  mediante  $a *'' b = (a * b) + 2$  donde  $*$  está definida en el ejemplo 1.1. Así,  $4 *'' 7 = 6$ ;  $25 *'' 9 = 11$  y  $6 *'' 6 = 8$ . ■

Quizá les parezca que estos ejemplos no son importantes, pero piénsenlo bien. Supongamos que van a una tienda a comprar una deliciosa barra de chocolate. Supongamos que ven dos barras idénticas, la etiqueta de una dice 99¢ y la etiqueta de la otra dice 94¢. Por supuesto, toman la de 94¢. Su capacidad para saber cuál quieren depende del hecho de que alguna vez en su vida aprendieron la operación binaria  $*$  del ejemplo 1.1. Es una operación muy importante. Así mismo,

## 12 OPERACIONES BINARIAS

la operación binaria  $*$ ' del ejemplo 1.2 claramente depende de la habilidad para distinguir orden. A menudo se ilustra la importancia del orden pensando en el lío que resultaría si trataran de ponerse primero los zapatos y después los calcetines. No deben apresurarse a descartar algunas operaciones binarias creyendo que son de poca importancia. Es claro que las operaciones usuales de suma y multiplicación de números tienen una importancia práctica bien conocida por todos.

Escogimos los ejemplos 1.1 y 1.2 para demostrar que una operación binaria puede o no depender del orden del par dado. Así, en el ejemplo 1.1,  $a * b = b * a$  para toda  $a, b \in \mathbb{Z}^+$ , y en el ejemplo 1.2 esto no sucede, pues  $5 *' 7 = 5$  pero  $7 *' 5 = 7$ .

Supongamos ahora que se desea considerar una expresión de la forma  $a * b * c$ . Una operación binaria  $*$  permite combinar sólo dos elementos y aquí hay tres. Las maneras obvias de intentar combinar los tres elementos son  $(a * b) * c$  o  $a * (b * c)$ . Con  $*$  definida como en el ejemplo 1.1,  $(2 * 5) * 9$  se calcula  $2 * 5 = 2$  y después  $2 * 9 = 2$ . Así mismo,  $2 * (5 * 9)$  se calcula  $5 * 9 = 5$  y después  $2 * 5 = 2$ . De aquí que  $(2 * 5) * 9 = 2 * (5 * 9)$  y se observa fácilmente que para esta  $*$

$$(a * b) * c = a * (b * c),$$

de manera que no existe ambigüedad al escribir  $a * b * c$ . Pero para  $*''$  del ejemplo 1.3

$$(2 *'' 5) *'' 9 = 4 *'' 9 = 6,$$

mientras que

$$2 *'' (5 *'' 9) = 2 *'' 7 = 4.$$

Así,  $(a *'' b) *'' c$  no necesariamente es igual a  $a *'' (b *'' c)$  y la expresión  $a *'' b *'' c$  puede ser ambigua.

**Definición** Una operación binaria  $*$  en un conjunto  $S$  es **comutativa** si (y sólo si)  $a * b = b * a$  para toda  $a, b \in S$ . La operación  $*$  es **asociativa** si (y sólo si)  $(a * b) * c = a * (b * c)$  para toda  $a, b, c \in S$ .

Como señalamos en la sección introductoria, es costumbre en matemáticas omitir las palabras *y sólo si* de una definición. Se entiende que las definiciones son siempre afirmaciones del tipo *si y sólo si*. *Los teoremas no siempre son afirmaciones del tipo si y sólo si y dicha convención nunca se usa para teoremas.*

No es difícil mostrar que si  $*$  es asociativa, entonces expresiones más largas como  $a * b * c * d$  no son ambiguas. Para propósitos de cálculo, los paréntesis pueden insertarse de cualquier modo; el resultado final de dichos cálculos será el mismo.

## 1.3 TABLAS

Para un conjunto finito, también se puede definir una operación binaria en el conjunto, mediante una tabla. El ejemplo siguiente muestra cómo lo haremos en este libro.

**Ejemplo 1.4** La tabla 1.1 define la operación binaria  $*$  en  $S = \{a, b, c\}$  mediante la regla

(*i*-ésimo lugar en la izquierda)  $*$  (*j*-ésimo lugar arriba) =  
 $=$  (*lugar en el i*-ésimo renglón y *j*-ésima columna del cuerpo de la tabla).

Así,  $a * b = c$  y  $b * a = a$  de modo que  $*$  no es conmutativa. ■

**Tabla 1.1**

*	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

El estudiante puede observar fácilmente que *una operación binaria definida mediante una tabla es conmutativa si y sólo si la tabla es simétrica con respecto a la diagonal que empieza en la esquina superior izquierda de la tabla y termina en la esquina inferior derecha*. Suponemos siempre que los elementos del conjunto están listados en la parte superior de la tabla en el mismo orden en que están listados a la izquierda.

Con excepción del 1.4, nuestros ejemplos de operaciones binarias se han definido en conjuntos de números. Es importante comprender que las operaciones binarias pueden definirse en cualesquiera conjuntos. En efecto, estudiaremos muchas operaciones binarias importantes en conjuntos cuyos elementos no son números. Algunos de los ejemplos dados más adelante consisten en conjuntos cuyos elementos son *funciones*. Suponemos que los estudiantes están familiarizados con ciertas funciones por sus cursos de cálculo, entre otros. Comprendemos que quizás por el momento no entiendan el concepto de función; y más adelante diremos algo sobre ello. Sin embargo, ya queremos ligar los conceptos recién presentados con las matemáticas que ya saben.

## 1.4 ALCUNAS PALABRAS DE ADVERTENCIA

Partiendo de su propia experiencia, el autor sabe del caos que puede resultar si a un estudiante se le pide definir alguna operación binaria en un conjunto. Obsér-

## 14 OPERACIONES BINARIAS

vese que al definir una operación binaria  $*$  en un conjunto  $S$  debemos estar seguros de que

- 1 se asigne exactamente un elemento a cada par ordenado posible de elementos de  $S$ ,
- 2 para cada par ordenado de elementos de  $S$ , el elemento asignado esté en  $S$ .

Con respecto a la condición 1, los estudiantes suelen dar reglas que asignan un elemento de  $S$  a la «mayoría» de los pares ordenados, pero para algunos pares la regla no determina ningún elemento. En este caso,  $*$  no se ha definido  $*$ . También puede suceder que para algunos pares, la regla asigne cualquiera entre varios elementos de  $S$ , esto es, existe ambigüedad. En caso de ambigüedad,  $*$  no está bien definida. Si se viola la condición 2, entonces  $S$  no es cerrado bajo  $*$ .

Ilustraremos ahora algunos intentos por definir operaciones binarias en conjuntos. Algunos son fallidos, como se señala. Puesto que no se compararán las operaciones, denotaremos todas por  $*$ .

**Ejemplo 1.5** En  $\mathbb{Q}$ , «definase»  $*$  por  $a * b = a/b$ . Aquí,  $*$  no está definida ya que esta regla no asigna un número racional al par  $(2, 0)$ . ■

**Ejemplo 1.6** En  $\mathbb{Q}^+$  definase  $*$  por  $a * b = a/b$ . Aquí se satisfacen las condiciones 1 y 2 y  $*$  es una operación binaria en  $\mathbb{Q}^+$ . ■

**Ejemplo 1.7** En  $\mathbb{Z}^+$  «definase»  $*$  por  $a * b = a/b$ . Aquí se viola la condición 2, pues  $1 * 3$  no está en  $\mathbb{Z}^+$ . Así,  $*$  no es una operación binaria en  $\mathbb{Z}^+$  ya que  $\mathbb{Z}^+$  no es cerrado bajo  $*$ . ■

**Ejemplo 1.8** Sea  $S$  el conjunto de todas las funciones con valores reales definidas para todos los números reales. Definase  $*$  como la suma usual de dos funciones, esto es,  $f * g = h$  donde  $h(x) = f(x) + g(x)$  para  $f, g \in S$  y  $x \in \mathbb{R}$ . Esta definición de  $*$  satisface las condiciones 1 y 2 y nos da una operación binaria en  $S$ . ■

**Ejemplo 1.9** Sea  $S$  como en el ejemplo 1.8, definase  $*$  como el producto usual de dos funciones, esto es,  $f * g = h$  donde  $h(x) = f(x)g(x)$ . De nuevo esta definición es buena y da una operación binaria en  $S$ . ■

**Ejemplo 1.10** Sea  $S$  como en el ejemplo 1.8, «definase»  $*$  como el cociente usual de  $f$  por  $g$ , esto es,  $f * g = h$  donde  $h(x) = f(x)/g(x)$ . Aquí se viola la condición 2, ya que las funciones en  $S$  deben estar definidas para todos los números reales y para alguna  $g \in S$ ,  $g(x)$  será cero para algunos valores de  $x$  en  $\mathbb{R}$  y  $h(x)$  no estaría definida en esos números en  $\mathbb{R}$ . Por ejemplo, si  $f(x) = \cos x$  y  $g(x) = x^2$  entonces  $h(0)$  no está definida, de modo que  $h \notin S$ . ■

**Ejemplo 1.11** Sea  $S$  como en el ejemplo 1.8; «definase»  $*$  por  $f * g = h$  donde  $h$  es una función mayor que  $f$  y  $g$ . Esta «definición» es completamente inútil. En

primer lugar, no se ha definido lo que significa que una función sea mayor que otra. Aún si se hubiera hecho, cualquier definición razonable conduciría a la existencia de muchas funciones mayores que  $f$  y que  $g$  y  $\star$  no estaría bien definida. ■

**Ejemplo 1.12.** Sea  $S$  un conjunto formado por veinte personas, todas ellas con diferente estatura. Definase  $\star$  por  $a \star b = c$  donde  $c$  es la persona más alta de las veinte en  $S$ . Esta es una operación binaria correcta en el conjunto, aunque no sea particularmente interesante. ■

**Ejemplo 1.13.** Sea  $S$  como en el ejemplo 1.12, «definase»  $\star$  por  $a \star b = c$  donde  $c$  es la persona más baja en  $S$  que es más alta que  $a$  y que  $b$ . Esta  $\star$  no está definida pues si  $a$  o  $b$  es la persona más alta del conjunto,  $a \star b$  no está determinada. ■

## Ejercicios

---

1.1 Sea la operación binaria  $\star$  definida en  $S = \{a, b, c, d, e\}$  mediante la tabla 1.2.

- Calcúlese  $b \star d$ ,  $c \star c$  y  $[(a \star c) \star e] \star a$  de la tabla.
- Calcúlese  $(a \star b) \star c$  y  $a \star (b \star c)$  de la tabla. ¿Se puede decir, con base en este cálculo, que  $\star$  es asociativa?
- Calcúlese  $(b \star d) \star c$  y  $b \star (d \star c)$  de la tabla. ¿Se puede decir, con base en este cálculo, que  $\star$  es asociativa?
- ¿Acaso  $\star$  es commutativa? ¿Por qué?

Tabla 1.2

$\star$	$a$	$b$	$c$	$d$	$e$
$a$	$a$	$b$	$c$	$b$	$d$
$b$	$b$	$c$	$a$	$e$	$c$
$c$	$c$	$a$	$b$	$b$	$a$
$d$	$b$	$e$	$b$	$e$	$d$
$e$	$d$	$b$	$a$	$d$	$c$

1.2 Complétense la tabla 1.3 de manera que se defina una operación binaria  $\star$  commutativa en  $S = \{a, b, c, d\}$ .

Tabla 1.3

$\star$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$c$	
$b$	$b$	$d$		$c$
$c$	$c$	$a$	$d$	$b$
$d$	$d$			$a$

## 16 OPERACIONES BINARIAS

1.3 La tabla 1.4 puede completarse para definir una operación binaria  $*$  asociativa en  $S = \{a, b, c, d\}$ . Supóngase que esto es posible y llénense los lugares vacíos.

**Tabla 1.4**

$*$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$c$	$d$
$b$	$b$	$a$	$c$	$d$
$c$	$c$	$d$	$c$	$d$
$d$				

1.4 Determinese si cada una de las definiciones de  $*$  dadas a continuación, da una operación binaria en el conjunto dado. En caso de que  $*$  no sea una operación binaria, diga si las condiciones 1 ó 2 o ambas, de la sección 1.4, se violan.

- a) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = a - b$ .
- b) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = a^b$ .
- c) En  $\mathbb{R}$ , definase  $*$  por  $a * b = a - b$ .
- d) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = c$ , donde  $c$  es el menor entero mayor que  $a$  y que  $b$ .
- e) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = c$ , donde  $c$  es al menos 5 unidades mayor que  $a + b$ .
- f) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = c$ , donde  $c$  es el mayor entero menor que el producto de  $a$  y  $b$ .

1.5 Pruébese que si  $*$  es una operación binaria en un conjunto  $S$ , asociativa y conmutativa, entonces

$$(a * b) * (c * d) = [(d * c) * a] * b$$

para toda  $a, b, c, d \in S$ . Supóngase que la ley asociativa se cumple, como en la definición, sólo para ternas, esto es, supóngase sólo

$$(x * y) * z = x * (y * z)$$

para toda  $x, y, z \in S$ .

1.6 Para toda operación binaria  $*$  definida a continuación, determinese cuál  $*$  es conmutativa y cuál  $*$  es asociativa.

- a) En  $\mathbb{Z}$ , definase  $*$  por  $a * b = a - b$ .
- b) En  $\mathbb{Q}$ , definase  $*$  por  $a * b = ab + 1$ .
- c) En  $\mathbb{Q}$ , definase  $*$  por  $a * b = ab/2$ .
- d) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = 2^{ab}$ .
- e) En  $\mathbb{Z}^+$ , definase  $*$  por  $a * b = a^b$ .

1.7 ¿Falso o verdadero?

- a) Si  $*$  es cualquier operación binaria en cualquier conjunto  $S$ , entonces  $a * a = a$  para toda  $a \in S$ .
- b) Si  $*$  es cualquier operación binaria conmutativa en cualquier conjunto  $S$ , entonces  $a * (b * c) = (b * c) * a$  para toda  $a, b, c \in S$ .

- c) Si  $*$  es cualquier operación binaria asociativa en cualquier conjunto  $S$ , entonces  $a * (b * c) = (b * c) * a$  para toda  $a, b, c \in S$ .
- d) Las únicas operaciones binarias importantes son aquéllas definidas en conjuntos de números.
- e) Una operación binaria  $*$  en un conjunto  $S$  es commutativa si existe  $a, b \in S$  tal que  $a * b = b * a$ .
- f) Toda operación binaria definida en un conjunto de un solo elemento es commutativa y asociativa.
- g) Una operación binaria en un conjunto  $S$  asigna al menos un elemento de  $S$  a todo par ordenado de elementos de  $S$ .
- h) Una operación binaria en un conjunto  $S$  asigna a lo más un elemento de  $S$  a todo par ordenado de elementos de  $S$ .
- i) Una operación binaria en un conjunto  $S$  asigna exactamente un elemento de  $S$  a todo par ordenado de elementos de  $S$ .
- j) Una operación binaria en un conjunto  $S$  puede asignar más de un elemento de  $S$  a algún par ordenado de elementos de  $S$ .

1.8 Dése un conjunto diferente a los descritos en los ejemplos del libro y que no sea un conjunto de números. Defínanse dos operaciones binarias diferentes  $*$  y  $*'$  en este conjunto. Asegúrese que el conjunto esté bien definido.

1.9 Sea  $S$  un conjunto con exactamente un elemento. ¿Cuántas operaciones binarias diferentes pueden definirse en  $S$ ? Respóndase a la pregunta si  $S$  tiene 2 elementos; si tiene 3 elementos; si tiene  $n$  elementos.

1.10 ¿Cuántas operaciones binarias commutativas diferentes pueden definirse en un conjunto de 2 elementos?; ¿en un conjunto de 3 elementos?; ¿en un conjunto de  $n$  elementos?

1.11 Obsérvese que las operaciones binarias  $*$  y  $*'$  en el conjunto  $\{a, b\}$  dadas por las tablas

$*$	$a$	$b$	$*'$	$a$	$b$
$a$	$a$	$a$	$a$	$a$	$b$
$b$	$a$	$b$	$b$	$b$	$b$

proporcionan el mismo tipo de estructura algebraica en  $\{a, b\}$  en el sentido de que si se reescribe la tabla para  $*'$

$*'$	$b$	$a$
$b$	$b$	$b$
$a$	$b$	$a$

es como la de  $*$  sólo que los papeles de  $a$  y  $b$  están intercambiados.

- a) Dése una definición natural del concepto de que dos operaciones binarias  $*$  y  $*'$  en el mismo conjunto dan estructuras algebraicas del mismo tipo, y que generalice esta observación.
- b) ¿Cuántos tipos diferentes de estructuras algebraicas están dados por las 16 operaciones binarias diferentes posibles, en un conjunto de 2 elementos?

# Grupos

## 2.1 MOTIVACION

Continuemos el análisis de nuestra experiencia con el álgebra. Una vez que dominamos los problemas de calcular sumas y multiplicaciones de números estuvimos en condiciones de aplicar estas operaciones binarias a la solución de problemas. A menudo los problemas llevaban a ecuaciones que contenían algún número desconocido  $x$  que era necesario determinar. Las ecuaciones más sencillas son las lineales de las formas  $a + x = b$  para la operación de suma y  $ax = b$  para la multiplicación. La ecuación lineal aditiva siempre tiene solución numérica; también la multiplicativa, siempre que  $a \neq 0$ . En efecto, la necesidad de soluciones de las ecuaciones lineales aditivas como  $5 + x = 2$  es una magnífica motivación para los números negativos. De manera similar, la necesidad de números racionales se muestra mediante ecuaciones como  $2x = 3$ , y la necesidad del número complejo  $i$  se muestra mediante la ecuación  $x^2 = -1$ .

Quisiéramos ser capaces de resolver ecuaciones lineales que contengan operaciones binarias. Sin embargo, esto no es posible para toda operación binaria. Por ejemplo, la ecuación  $a * x = a$  no tiene solución en  $S = \{a, b, c\}$  para la operación  $*$  del ejemplo 1.4. Veámos cuáles son las propiedades de la operación de suma de los enteros  $\mathbb{Z}$  que nos permiten resolver la ecuación  $5 + x = 2$  en  $\mathbb{Z}$ . No debemos recurrir a la resta, pues lo que nos ocupa es la solución en términos de una sola operación binaria, en este caso, la suma. Los pasos para la solución son los siguientes:

$$\begin{array}{ll} 5 + x = 2 & \text{está dado} \\ -5 + (5 + x) = -5 + 2 & \text{sumando } -5 \\ (-5 + 5) + x = -5 + 2 & \text{ley asociativa} \end{array}$$

$$\begin{array}{ll} 0 + x = -5 + 2 & \text{calculando } -5 + 5 \\ x = -5 + 2 & \text{propiedad del } 0 \\ x = -3 & \text{calculando } -5 + 2. \end{array}$$

Estrictamente, no hemos mostrado aquí que  $-3$  es una solución, sino que es la única posibilidad de solución. Para mostrar que  $-3$  es una solución, basta calcular  $5 + (-3)$ . Puede hacerse un análisis similar para la ecuación  $2x = 3$  en los números racionales:

$$\begin{array}{ll} 2x = 3 & \text{está dado} \\ \frac{1}{2}(2x) = \frac{1}{2}(3) & \text{multiplicando por } \frac{1}{2} \\ (\frac{1}{2} \cdot 2)x = \frac{1}{2} \cdot 3 & \text{ley asociativa} \\ 1 \cdot x = \frac{1}{2} \cdot 3 & \text{calculando } \frac{1}{2} \cdot 2 \\ x = \frac{1}{2} \cdot 3 & \text{propiedad del } 1 \\ x = \frac{3}{2} & \text{calculando } \frac{1}{2} \cdot 3 \end{array}$$

Veamos qué propiedades deben tener un conjunto  $S$  y una operación binaria  $*$  en  $S$  para permitir la imitación de este procedimiento en una ecuación  $a * x = b$  para  $a, b \in S$ . Es básica para el procedimiento la existencia de un elemento  $e$  en  $S$  con la propiedad de que  $e * x = x$  para toda  $x \in S$ . En el ejemplo aditivo,  $0$  desempeñó el papel de  $e$ , y el  $1$  en el ejemplo multiplicativo. Después, necesitamos un elemento  $a'$  en  $S$  que tenga la propiedad de que  $a' * a = e$ . En el ejemplo aditivo  $-5$  desempeñó el papel de  $a'$ , y en el ejemplo multiplicativo lo hizo  $\frac{1}{2}$ . Por último, necesitamos la ley asociativa. El resto es cuestión de cálculos. Se puede observar fácilmente que para resolver la ecuación  $x * a = b$  (hay que recordar que  $a * x$  no necesariamente es igual a  $x * a$ ); nos gustaría tener un elemento  $e$  en  $S$  tal que  $x * e = x$  para todas las  $x \in S$  y una  $a'$  en  $S$  tal que  $a * a' = e$ . Con todas estas propiedades de  $*$  en  $S$  estaríamos seguros de poder resolver ecuaciones lineales. Estas son precisamente las propiedades de un grupo.

## 2.2 DEFINICION Y PROPIEDADES ELEMENTALES

**Definición** Un *grupo*  $\langle G, *\rangle$  es un conjunto  $G$ , junto con una operación binaria  $*$  en  $G$ , tal que se satisface los siguientes axiomas:

- $\mathcal{G}_1$**  La operación binaria  $*$  es asociativa.
- $\mathcal{G}_2$**  Existe un elemento  $e$  en  $G$  tal que  $e * x = x * e = x$  para todas las  $x \in G$ . (Este elemento  $e$  es un *elemento identidad* para  $*$  en  $G$ .)
- $\mathcal{G}_3$**  Para cada  $a$  en  $G$  existe un elemento  $a'$  en  $G$  con la propiedad de que  $a * a' = a' * a = e$ . (El elemento  $a'$  es un *inverso de  $a$  respecto a  $*$* .)

<sup>†</sup> Recuérdese que las negritas indican que se está definiendo un término. Véase el último párrafo de la sección 0.1. Por tanto, un *elemento identidad* para una operación binaria  $*$  en un conjunto  $S$  es cualquier elemento  $e$  que satisfaga  $e * x = x * e = x$  para todas las  $x \in S$ .

Muchos libros incluyen otro axioma para un grupo, a saber, que  $G$  sea **cerrado bajo la operación  $*$** , es decir, que  $(a * b) \in G$  para todas las  $a, b \in G$ . Para nosotros, ésta es una consecuencia de la **definición** de operación binaria en  $G$ .

Debemos señalar en este momento, que seremos descuidados con la notación. Obsérvese que un grupo no sólo es un conjunto  $G$ . Más bien, que un grupo  $\langle G, * \rangle$  consta de dos entidades, el conjunto  $G$  y la operación binaria  $*$  en  $G$ . Hay dos ingredientes. Denotar al grupo por el símbolo de conjunto  $G$  es lógicamente incorrecto. Sin embargo, conforme se avanza en la teoría, las extensiones lógicas de la notación  $\langle G, * \rangle$  se vuelven tan voluminosas que dificultan la lectura de la exposición. En algún momento, todos los autores se rinden, descuidan la notación y denotan al grupo sólo por la letra  $G$ . Decidimos reconocerlo y ser descuidados desde el principio. Sin embargo, insistimos en que al hablar de un grupo específico  $G$ , debe aclararse cuál será la operación del grupo en  $G$ , pues un conjunto contiene gran variedad de posibles operaciones binarias definidas, constituyendo grupos diferentes. Algunas veces emplearemos la notación  $\langle G, * \rangle$  por razones de claridad en nuestros análisis.

**Teorema 2.1** Si  $G$  es un grupo con una operación binaria  $*$ , entonces las leyes de cancelación izquierda y derecha se cumplen en  $G$ , es decir,  $a * b = a * c$  implica  $b = c$  y  $b * a = c * a$  implica  $b = c$  para  $a, b, c \in G$ .

**Demostración** Supóngase que  $a * b = a * c$ . Entonces, por  $\mathcal{G}_3$  existe  $a'$  y

$$a' * (a * b) = a' * (a * c).$$

Por la ley asociativa

$$(a' * a) * b = (a' * a) * c.$$

Por la definición de  $a'$  en  $\mathcal{G}_3$ ,  $a' * a = e$ , luego

$$e * b = e * c.$$

Por la definición de  $e$  en  $\mathcal{G}_2$ ,

$$b = c$$

En forma análoga, de  $b * a = c * a$  podemos deducir que  $b = c$  multiplicando por  $a'$  por la derecha y usando los axiomas de grupo. ■

Nótese que fue necesario usar la definición de grupo para probar este teorema.

**Teorema 2.2** Si  $G$  es un grupo con operación binaria  $*$  y si  $a$  y  $b$  son elementos cualesquiera de  $G$ , entonces las ecuaciones lineales  $a * x = b$  y  $y * a = b$  tienen soluciones únicas en  $G$ .

*Demostración* Nótese que

$$\begin{aligned} a * (a' * b) &= (a * a') * b && \text{ley asociativa} \\ &= e * b && \text{definición de } a' \\ &= b && \text{propiedad de } e \end{aligned}$$

Por tanto,  $x = a' * b$  es una solución de  $a * x = b$ . De manera análoga,  $y = b * a'$  es una solución de  $y * a = b$ .

Para mostrar que  $y$  es única, supóngase que  $y * a = b$  y  $y_1 * a = b$ . Entonces,  $y * a = y_1 * a$  y por el teorema 2.1  $y = y_1$ . La unicidad de  $x$  se prueba de manera similar. ■

Claro que para probar la unicidad en el último teorema pudimos haber seguido el mismo procedimiento empleado para motivar la definición de grupo que muestra que si  $a * x = b$  entonces  $x = a' * b$ . Sin embargo, preferimos ilustrar la manera usual de probar que un objeto es único. Supongamos que se tienen dos de dichos objetos, y que es necesario probar que deben ser el mismo. Nótese que las soluciones  $x = a' * b$  y  $y = b * a'$  no son necesariamente iguales a menos que  $*$  sea commutativa.

**Definición** Un grupo  $G$  es *abeliano* si su operación binaria  $*$  es commutativa.

Pongamos algunos ejemplos de conjuntos con operaciones binarias que dan grupos y otros que no dan grupos.

**Ejemplo 2.1** El conjunto  $\mathbb{Z}^+$  con la operación  $+$  *no* es un grupo. No existe un elemento identidad para  $+$  en  $\mathbb{Z}^+$ . ■

**Ejemplo 2.2** El conjunto de todos los enteros no negativos (incluyendo el 0) con la operación  $+$  sigue *no* siendo grupo. Existe un elemento identidad 0, pero no un inverso para 2. ■

**Ejemplo 2.3** El conjunto  $\mathbb{Z}$  con la operación  $+$  *es* un grupo. Se satisfacen todas las condiciones de la definición. El grupo es abeliano. ■

**Ejemplo 2.4** El conjunto  $\mathbb{Z}^+$  con la operación de multiplicación *no* es un grupo. Existe una identidad, el 1, pero no hay inverso para 3. ■

**Ejemplo 2.5** El conjunto  $\mathbb{Q}^+$  con la operación multiplicación *es* un grupo. Se satisfacen todas las condiciones de la definición. El grupo es abeliano. ■

**Ejemplo 2.6** Definase  $*$  en  $\mathbb{Q}^+$  por  $a * b = ab/2$ . Entonces

$$(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4}$$

y también

$$a * (b * c) = \frac{a + \frac{bc}{2}}{2} = \frac{abc}{4}.$$

Por tanto,  $*$  es asociativa. Es claro que

$$2 * a = a * 2 = a$$

para todas las  $a \in Q^+$  de modo que 2 es un elemento identidad para  $*$ . Por último,

$$a * \frac{4}{a} = \frac{4}{a} * a = 2,$$

de manera que  $a' = 4/a$  es un inverso de  $a$ . De aquí que  $Q^+$  con la operación  $*$  es un grupo. ■

Existe otro resultado acerca de grupos que deseamos probar en esta sección.

**Teorema 2.3** *En un grupo G con operación  $*$  hay una sola identidad e tal que*

$$e * x = x * e = x$$

*para todas las  $x \in G$ . De la misma manera, para cada  $a \in G$  existe un solo elemento  $a'$  tal que*

$$a' * a = a * a' = e.$$

*En resumen, la identidad y los inversos son únicos en un grupo.*

**Demostración** Supóngase que  $e * x = x * e = x$  y también que  $e_1 * x = x * e_1 = x$  para todas las  $x \in G$ . Déjense competir a  $e$  y  $e_1$ . Considerando  $e$  como identidad,  $e * e_1 = e_1$ . Pero considerando  $e_1$  como identidad,  $e * e_1 = e$ . Por tanto,

$$e_1 = e * e_1 = e,$$

y la identidad en un grupo es única.

Supóngase ahora que  $a' * a = a * a' = e$  y que  $a'' * a = a * a'' = e$ . Entonces

$$a * a'' = a * a' = e$$

y, por el teorema 2.1,

$$a'' = a',$$

de manera que el inverso de  $a$  en un grupo es único. ■

Para su información, queremos hacer notar que las estructuras algebraicas formadas por conjuntos con operaciones binarias en las cuales no se cumplen todos

los axiomas de grupo, también se estudian ampliamente. De estas estructuras más débiles, es el **semigrupo**, un conjunto con una operación binaria asociativa, la que quizás haya acaparado más atención. Recientemente se han estudiado también las estructuras no asociativas.

Por último, es posible dar axiomas formalmente más débiles para un grupo  $\langle G, * \rangle$  a saber:

- 1 La operación binaria  $*$  en  $G$  es asociativa.
- 2 Existe una **identidad izquierda**  $e$  en  $G$  tal que  $e * x = x$  para todas las  $x \in G$ .
- 3 Para cada  $a \in G$  existe un **inverso izquierdo**  $a'$  en  $G$  tal que  $a' * a = e$ .

A partir de esta definición *de un solo lado* podemos probar que la identidad izquierda también es una identidad derecha y que un inverso izquierdo también es un inverso derecho para el mismo elemento. Por tanto, no deberíamos decir que estos axiomas son más débiles, pues dan lugar a las mismas estructuras llamadas grupos. Es posible que en algunos casos sea más fácil corroborar estos *axiomas izquierdos*, que corroborar los *axiomas válidos para los dos lados*. Desde luego, es fácil deducir por simetría que también hay *axiomas derechos* para un grupo.

## 2.3 GRUPOS FINITOS Y TABLAS DE GRUPO

Hasta ahora nuestros ejemplos han correspondido a grupos infinitos, esto es, de grupos donde el conjunto  $G$  tiene un número infinito de elementos. El estudiante se preguntará si puede existir una estructura de grupo en algún conjunto finito; la respuesta es sí, y ciertamente, dichas estructuras son muy importantes.

Puesto que un grupo debe tener al menos un elemento, a saber, la identidad, el conjunto más pequeño que puede dar lugar a un grupo es un conjunto  $\{e\}$  de un elemento. La única operación binaria  $*$  posible en  $\{e\}$  está definida por  $e * e = e$ . El estudiante puede corroborar de inmediato que se cumplen los tres axiomas de grupo. En cada grupo, el elemento identidad es siempre su propio inverso.

Tratemos de construir una estructura de grupo en un conjunto de dos elementos. Como uno de los elementos debe desempeñar el papel de identidad, digamos que el conjunto es  $\{e, a\}$ . Busquemos una tabla para una operación binaria  $*$  en  $\{e, a\}$  que dé una estructura de grupo. Cuando demos una tabla para una operación de grupo, siempre colocaremos los elementos en la parte superior, hacia la derecha, en el mismo orden en que los colocamos del lado izquierdo, hacia abajo, colocando en primer lugar la identidad, como en la tabla siguiente:

*	e	a
e		
a		

Como  $e$  será la identidad, entonces

$$e * x = x * e = x$$

para todas las  $x \in \{e, a\}$ , y nos vemos obligados a llenar la tabla de la manera indicada más adelante, si es que  $*$  va a dar un grupo.

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	

Además,  $a$  debe tener un inverso  $a'$  tal que

$$a * a' = a' * a = e.$$

En nuestro caso  $a'$  debe ser  $e$  o  $a$ . Puesto que obviamente  $a' = e$  no funciona, debemos tener  $a' = a$  de tal modo que debemos completar la tabla de la siguiente manera:

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

Se satisfacen así todos los axiomas de grupo, excepto, quizás, la ley asociativa. Veremos adelante, en una situación más general, que esta operación  $*$  es asociativa. Ustedes pueden aceptarlo en este momento, o hacer el tedioso trabajo de corroborar todos los casos.

Con base en estos ejemplos, podremos enumerar algunas condiciones que una tabla que define una operación binaria en un conjunto finito debe satisfacer, para dotarlo de una estructura de grupo. Es necesario que algún elemento del conjunto, que siempre denotaremos por  $e$ , actúe como identidad. La condición  $e * x = x$  significa que el renglón de la tabla que contiene  $a$   $e$  en el extremo izquierdo, debe contener exactamente los elementos que aparecen hasta arriba de la tabla, en el mismo orden. En forma análoga, la condición  $x * e = x$  significa que la columna de la tabla bajo  $e$ , debe contener precisamente los elementos que aparecen en el extremo izquierdo, en el mismo orden. El hecho de que cada elemento  $a$  tenga un inverso derecho y un izquierdo, quiere decir que en el renglón frente a  $a$  debe aparecer el elemento  $e$  y que en la columna bajo  $a$  debe aparecer  $e$  en primer lugar. Así,  $e$  debe aparecer en cada renglón y en cada columna. Sin embargo, podemos mejorar esto. Por el teorema 2.2, no sólo tienen soluciones únicas las ecuaciones  $a * x = e$  y  $y * a = e$ , sino también las ecuacio-

nes  $a * x = b$  y  $y * a = b$ . Por un argumento análogo, esto significa que cada elemento  $b$  del grupo debe aparecer una y sólo una vez en cada renglón y en cada columna de la tabla.

De manera recíproca, supongamos que una tabla para una operación binaria en un conjunto finito es tal, que hay un elemento actuando como identidad y que cada elemento del conjunto aparece precisamente una vez en cada renglón y en cada columna. Se puede ver entonces, que la estructura es de grupo si y sólo si se cumple la ley asocialiva. Si una operación binaria  $*$  está dada por una tabla, por lo común es laborioso verificar que se cumple la ley asociativa. Si la operación  $*$  se define mediante alguna propiedad que caracteriza a  $a * b$ , suele ser fácil verificar el cumplimiento de la ley asociativa. Afortunadamente, este segundo caso resulta ser el más frecuente.

Se ha visto que hay esencialmente un solo grupo de dos elementos, en el sentido de que si denotamos los elementos por  $e$  y  $a$  colocando primero a la identidad  $e$ , la tabla debe ser así

*	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

Supongamos que un conjunto tiene tres elementos. Como antes, podemos hacer el conjunto  $\{e, a, b\}$ . Para que  $e$  sea una identidad; en este conjunto, una operación binaria  $*$  debe tener una tabla como se muestra en la tabla 2.1. Quedan cuatro lugares por llenar. El estudiante puede ver de inmediato que la tabla 2.1 debe completarse como se muestra en la tabla 2.2, si cada renglón y cada columna debe contener precisamente una vez cada elemento. De nuevo se pide aceptar, sin demostración, el hecho de que esta operación es asociativa, de modo que  $*$  sí da una estructura de grupo en  $G = \{e, a, b\}$ .

Tabla 2.1

*	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$		
$b$	$b$		

Tabla 2.2

*	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

Supongamos ahora que  $G'$  es cualquier otro grupo de tres elementos e imaginemos una tabla para  $G'$  donde la identidad aparece en primer lugar. Debido a que pudimos llenar la tabla para  $G = \{e, a, b\}$  de una sola manera, vemos que si llamamos  $e$  a la identidad de  $G'$ ,  $a$  al siguiente elemento y  $b$  al último, la tabla de  $G'$  que resulte será la misma que la de  $G$ . En otras palabras, las características *estructurales* son las mismas para ambos grupos; un grupo se verá

exactamente igual a otro con sólo cambiar el nombre a sus elementos. Por tanto, cualesquiera dos grupos de tres elementos son estructuralmente el mismo. Esta es nuestra introducción al concepto de *isomorfismo*. Los grupos  $G$  y  $G'$  son *isomorfos*. Algunas veces este concepto parece algo difícil a los estudiantes. No se tratará aquí, más adelante lo haremos de manera precisa.

## Ejercicios

---

2.1 Para cada operación binaria  $*$  definida en el conjunto señalado dígase cuándo  $*$  dota al conjunto de una estructura de grupo. De no resultar grupo, dése el primer axioma en el orden  $\mathcal{G}_1; \mathcal{G}_2; \mathcal{G}_3$ ; de la sección 2.2 que no se cumpla.

- Definase  $*$  en  $\mathbb{Z}$  por  $a * b = ab$
- Definase  $*$  en  $\mathbb{Z}$  por  $a * b = a - b$
- Definase  $*$  en  $\mathbb{R}^+$  por  $a * b = ab$
- Definase  $*$  en  $\mathbb{Q}$  por  $a * b = ab$
- Definase  $*$  en el conjunto de todos los números reales distintos de cero por  $a * b = ab$
- Definase  $*$  en  $\mathbb{C}$  por  $a * b = a + b$

2.2 Considérense nuestros axiomas  $\mathcal{G}_1; \mathcal{G}_2$  y  $\mathcal{G}_3$ , para un grupo. Están dados en el orden  $\mathcal{G}_1\mathcal{G}_2\mathcal{G}_3$ . Otros posibles órdenes para enunciarlos son  $\mathcal{G}_1\mathcal{G}_3\mathcal{G}_2; \mathcal{G}_2\mathcal{G}_1\mathcal{G}_3; \mathcal{G}_2\mathcal{G}_3\mathcal{G}_1; \mathcal{G}_3\mathcal{G}_1\mathcal{G}_2$  y  $\mathcal{G}_3\mathcal{G}_2\mathcal{G}_1$ . De estos seis órdenes posibles, precisamente tres son aceptables para una definición. ¿Qué órdenes no son aceptables y por qué? (Recuérdese que la mayoría de los profesores pregunta la definición de grupo cuando menos en un examen.)

2.3 Muéstrese mediante cálculos y por el teorema 2.3 que si  $G$  es un grupo con operación binaria  $*$ , entonces, para todas las  $a, b \in G$ , tenemos que  $(a * b)' = b' * a'$ . ¿Cuál sería una expresión análoga para  $(a * b' * c)'$ ?

2.4 Procédase de la siguiente manera para mostrar que hay dos tipos diferentes posibles de estructura de grupo en un conjunto de cuatro elementos. Sea el conjunto  $\{e, a, b, c\}$  con la identidad  $e$  para la operación del grupo. Entonces la tabla de grupo debe comenzar como se muestra en la tabla 2.3

**Tabla 2.3**

*	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	?		
$b$	$b$			
$c$	$c$			

El cuadro marcado con la interrogación no puede llenarse con  $a$ . Debe llenarse ya sea con la identidad  $e$  o con un elemento diferente de  $e$  y de  $a$ . En el último caso no se pierde generalidad al suponer que este elemento es  $b$ . Si este cuadro se llena con  $e$ , la tabla puede completarse entonces de dos maneras, para dar un grupo. Encuéntrense estas dos tablas. (No es necesario corroborar la ley asociativa.) Si se llena el cuadro con  $b$ , entonces se puede completar la tabla de un solo modo para dar un grupo. Encuéntrese esta tabla.

(Tampoco aquí es necesario corroborar la ley asociativa.) De las tres tablas obtenidas, dos dan el mismo tipo de estructura de grupo. Determinese cuáles son y muéstrese de qué manera debería cambiar el nombre de los elementos de una tabla para que ambas sean la misma. ¿Son comunitativos todos los grupos de 4 elementos?

**2.5** Muéstrese que si  $G$  es un grupo finito con identidad  $e$  y con un número par de elementos, entonces existe  $a \neq e$ , en  $G$ , tal que  $a * a = e$ .

**2.6** ¿Falso o verdadero?

- a) Un grupo puede tener más de un elemento identidad.
  - b) Cualesquiera dos grupos de tres elementos son isomorfos.
  - c) En un grupo, cada ecuación lineal tiene solución.
  - d) La actitud correcta frente a una definición es memorizarla de manera que pueda luego repetirla palabra por palabra como viene en el texto.
  - e) Cualquier definición de grupo dada por alguna persona es correcta siempre que lo que sea grupo según su definición, sea grupo también según la definición del libro.
  - f) Cualquier definición de grupo dada por alguna persona es correcta siempre que esa persona muestre que todo lo que satisface su definición también satisface la del libro y viceversa.
  - g) Todo grupo finito de tres elementos como máximo es abeliano.
  - h) Una ecuación de la forma  $a * x * b = c$  siempre tiene solución única en un grupo.
  - i) El conjunto vacío puede considerarse como grupo.
  - j) Hasta ahora, en el libro no se han presentado ejemplos de grupos no abelianos.
- 

**2.7** Dese una tabla para una operación binaria en el conjunto  $\{e, a, b\}$  de tres elementos que cumpla los axiomas  $\mathcal{G}_2$  y  $\mathcal{G}_3$  de grupo, pero no el axioma  $\mathcal{G}_1$ .

**2.8** De acuerdo con el ejercicio 1.9, hay 16 operaciones binarias posibles en un conjunto de 2 elementos. ¿Cuántas dotan al conjunto de estructura de grupo? ¿Cuántas de las 19,683 operaciones binarias posibles en un conjunto de 3 elementos dotan al conjunto de una estructura de grupo?

**2.9** Sea  $S$  el conjunto de todos los números reales excepto  $-1$ . Definase  $*$  en  $S$  por

$$a * b = a + b + ab.$$

- a) Muéstrese que  $*$  da una operación binaria en  $S$ .
- b) Muéstrese que  $\langle S, *\rangle$  es un grupo.
- c) Encuéntrese la solución de la ecuación  $2 * x * 3 = 7$  en  $S$ .

**2.10** Sea  $R^*$  el conjunto de todos los números reales excepto el 0. Definase  $*$  en  $R^*$  por  $a * b = |ab|$ .

- a) Muéstrese que  $*$  da una operación binaria asociativa en  $R^*$ .
- b) Muéstrese que existe una identidad izquierda para  $*$  y un inverso derecho para cada elemento en  $R^*$ .
- c) Con esta operación binaria, ¿es  $R^*$  un grupo?
- d) Explíquese la importancia de este ejercicio.

**2.11** Si  $*$  es una operación binaria en un conjunto  $S$ , un elemento  $x$  de  $S$  es idempotente para  $*$  si  $x * x = x$ . Pruébese que un grupo tiene exactamente un elemento idempotente. (Pueden usarse los teoremas que ya se han demostrado en el texto.)

2.12 Muéstrese que todo grupo  $G$  con identidad  $e$  tal que  $x * x = e$  para todas las  $x \in G$ , es abeliano. [Sugerencia: considérese  $(ab)^2$ .]

2.13 Pruébese que un conjunto  $G$ , junto con una operación binaria  $*$  en  $G$  que satisface los axiomas izquierdos 1, 2 y 3, dados al final de la sección 2.2, es un grupo.

2.14 Pruébese que un conjunto no vacío  $G$  junto con una operación binaria  $*$  en  $G$  tal que las ecuaciones

$$a * x = b \text{ y } y * a = b \text{ tienen soluciones en } G \text{ para todas las } a, b \in G,$$

es un grupo. [Sugerencia: úsese el ejercicio 2.13.]

2.15 Las siguientes «definiciones» de grupo, que deberán criticarse, se han reproducido literalmente, incluyendo ortografía y puntuación, de los exámenes de algunos alumnos.

a) Un grupo  $G$  es un conjunto de elementos junto con una operación binaria  $*$  tal que se satisfacen las siguientes condiciones

- \* es asociativa
- Existe  $e \in G$  tal que

$$e * x = x * e = x = \text{identidad.}$$

Para toda  $a \in G$  existe un  $a'$  (inverso) tal que

$$a \cdot a' = a' \cdot a = e$$

b) Un grupo es un conjunto  $G$  tal que

- La operación en  $G$  es asociativa.
- existe un elemento identidad ( $e$ ) en  $G$ .
- para toda  $a \in G$ , existe un  $a'$  (inverso para cada elemento)

c) Un grupo es un conjunto con una operación binaria tal que

- está definida la operación binaria
- existe un inverso
- existe un elemento identidad

d) Un conjunto  $G$  se llama un grupo sobre la operación binaria  $*$  tal que para todas las  $a, b \in G$

- Operación binaria  $*$  es asociativa bajo la suma
- existe un elemento  $\{e\}$  tal que

$$a * e = e * a = e$$

Para todo elemento  $a$  existe un elemento  $a'$  tal que

$$a * a' = a' * a = e$$

## 3

## Subgrupos

### 3.1 NOTACION Y TERMINOLOGIA

Es el momento de explicar algo de terminología y notaciones convencionales usadas en la teoría de grupos. Por regla general, los algebristas no usan un símbolo especial  $\bullet$  para denotar una operación binaria diferente de la suma y multiplicación usuales. Se aferran a la notación convencional de la suma y la multiplicación e incluso llaman la operación *suma* o *multiplicación*, dependiendo del símbolo usado. Es obvio que el símbolo para la suma es  $+$  y la multiplicación se denota con la yuxtaposición de los factores sin un punto, si es que no hay confusión. Así, en lugar de la notación  $a \bullet b$  usaremos ya sea  $a + b$  que se lee «la *suma* de  $a$  y  $b$ » o  $ab$  que se lee «el *producto* de  $a$  y  $b$ ». Hay una especie de acuerdo entre caballeros en cuanto a que el símbolo  $+$  se use sólo para designar operaciones conmutativas. Los algebristas se sienten muy incómodos cuando ven  $a + b \neq b + a$ . Por esta razón, al desarrollar nuestra teoría de grupos, en una situación general donde la operación pueda ser o no conmutativa, usaremos siempre la notación multiplicativa.

Los matemáticos usan con frecuencia el símbolo  $0$  para denotar una identidad aditiva y el símbolo  $1$  para denotar una identidad multiplicativa, aunque en realidad no se denoten los enteros  $0$  y  $1$ . Claro que si alguien habla al mismo tiempo de números, podría haber confusión, y se prefiere el uso de símbolos como  $e$  o  $u$  como elementos identidad. Por tanto, una tabla para un grupo de tres elementos se vería como la tabla 3.1 o bien, como dicho grupo es conmutativo, se vería como la tabla 3.2. En situaciones generales seguiremos usando  $e$  para denotar el elemento identidad de un grupo.

Tabla 3.1

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Tabla 3.2

+	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

Se acostumbra denotar el inverso de un elemento  $a$  en un grupo, con  $a^{-1}$  en notación multiplicativa, y con  $-a$  en notación aditiva. En adelante usaremos estas notaciones en lugar del símbolo  $a'$ .

Expliquemos un término más, que se usa tanto, que amerita una definición aparte.

**Definición** Si  $G$  es un grupo finito, entonces el **orden**  $|G|$  de  $G$  es el número de elementos en  $G$ . En general, para cualquier conjunto finito  $S$ ,  $|S|$  es el número de elementos en  $S$ .

Por último, en lugar de la frase *con la operación binaria de* usaremos la palabra *bajo*, así que «el grupo  $R$  con la operación binaria de suma» se convierte en «el grupo  $R$  bajo la suma».

## 3.2 SUBCONJUNTOS Y SUBGRUPOS

Habrán notado que hemos tenido a veces grupos contenidos en grupos mayores. Por ejemplo, el grupo  $\mathbf{Z}$  bajo la suma está contenido en el grupo  $\mathbf{Q}$  bajo la suma, el cual a su vez está contenido en el grupo  $\mathbf{R}$  bajo la suma. Cuando vemos al grupo  $\langle \mathbf{Z}, + \rangle$  como contenido en el grupo  $\langle \mathbf{R}, + \rangle$  es importante notar que la operación  $+$  en los enteros  $n$  y  $m$  como elementos de  $\langle \mathbf{Z}, + \rangle$  produce el mismo elemento  $n + m$  que resultaría si se pensara en  $n$  y  $m$  como elementos de  $\langle \mathbf{R}, + \rangle$ . Por tanto, no debemos considerar al grupo  $\langle \mathbf{Q}^+, \cdot \rangle$  como contenido en  $\langle \mathbf{R}, + \rangle$  aunque  $\mathbf{Q}^+$  está contenido en  $\mathbf{R}$  como conjunto. En este ejemplo,  $2 \cdot 3 = 6$  en  $\langle \mathbf{Q}^+, \cdot \rangle$ , mientras que  $2 + 3 = 5$  en  $\langle \mathbf{R}, + \rangle$ . No sólo se requiere que el conjunto de un grupo esté contenido en el conjunto del otro, sino también que la operación de grupo en el conjunto menor asigne el mismo elemento a cada par ordenado de este conjunto menor que el asignado por la operación de grupo del conjunto mayor. Daremos una serie de definiciones para precisar estas ideas.

**Definición** Un conjunto  $B$  es un **subconjunto de un conjunto A** denotado por  $B \subseteq A$  o  $A \supseteq B$  si cada elemento de  $B$  está en  $A$ . Las notaciones  $B \subset A$  o  $A \supset B$  se usarán para  $B \subseteq A$ , pero  $B \neq A$ .

Nótese que de acuerdo con esta definición, para cualquier conjunto  $A$ ,  $A$  misma y  $\emptyset$  son subconjuntos de  $A$ .

**Definición** Si  $A$  es cualquier conjunto, entonces  $A$  es el *subconjunto imprópicio de  $A$* . Cualquier otro subconjunto de  $A$  es un *subconjunto propio de  $A$* .

**Definición** Sea  $G$  un grupo y sea  $S$  un subconjunto de  $G$ . Si para cada  $a, b \in S$  es cierto que el producto  $ab$  calculado en  $G$  también está en  $S$ , entonces  $S$  es *cerrado bajo la operación de grupo de  $G$* . La operación binaria en  $S$ , así definida, es la *operación inducida en  $S$  desde  $G$* .

Podemos ahora precisar el concepto de grupo contenido en otro.

**Definición** Si  $H$  es un subconjunto de un grupo  $G$  cerrado bajo la operación de grupo de  $G$  y si  $H$  es él mismo un grupo bajo esta operación inducida, entonces  $H$  es un *subgrupo de  $G$* . Denotaremos por  $H \leq G$  o  $G \geq H$  el hecho de que  $H$  es un subgrupo de  $G$ , y  $H \langle G \text{ o } G \rangle H$  significará que  $H \leq G$ , pero  $H \neq G$ .

Así,  $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ , pero  $\langle \mathbb{Q}^+, \cdot \rangle$  no es un subgrupo de  $\langle \mathbb{R}, + \rangle$  aunque, como conjuntos,  $\mathbb{Q}^+ \subset \mathbb{R}$ . Cada grupo  $G$  tiene como subgrupos a  $G$  mismo y  $\{e\}$ , donde  $e$  es el elemento identidad de  $G$ .

**Definición** Si  $G$  es un grupo, entonces  $G$  es el *subgrupo imprópicio de  $G$* . Todos los otros subgrupos son *subgrupos propios*. Además,  $\{e\}$  es el *subgrupo trivial de  $G$* . Todos los otros subgrupos son *no triviales*.

Daremos algunos ejemplos.

**Ejemplo 3.1**  $\mathbb{Q}^+$  bajo multiplicación es un subgrupo propio de  $\mathbb{R}^+$  bajo multiplicación. ■

**Ejemplo 3.2** Hay dos tipos diferentes de estructuras de grupo de orden 4 (véase el ejercicio 2.4). Se describieron por sus tablas de grupo (tablas 3.3 y 3.4). El grupo  $V$  es el **4-grupo de Klein**; la notación  $V$  proviene de la palabra alemana *viergruppe*.

Tabla 3.3

$\mathbb{Z}_4$ :	+	0	1	2	3
	+	0	1	2	3
0	0	1	2	3	
1	1	2	3	0	
2	2	3	0	1	
3	3	0	1	2	

Tabla 3.4

$V$ :	$e$	$a$	$b$	$c$
	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

El único subgrupo propio no trivial de  $\mathbb{Z}_4$  es  $\{0, 2\}$ . Nótese que  $\{0, 3\}$  no es un subgrupo de  $\mathbb{Z}_4$  pues  $\{0, 3\}$  no es cerrado bajo  $+$ . Por ejemplo,  $3 + 3 = 2$  y  $2 \notin \{0, 3\}$ ; sin embargo, el grupo  $V$  tiene tres subgrupos propios no triviales,

$\{e, a\}$ ;  $\{e, b\}$  y  $\{e, c\}$ . Aquí,  $\{e, a, b\}$  no es un subgrupo puesto que  $\{e, a, b\}$  no es cerrado bajo la operación de  $V$ . Por ejemplo,  $ab = c$  y  $c \notin \{e, a, b\}$ . ■

A menudo es conveniente dibujar un *diagrama reticular* de los subgrupos de un grupo. En dicho diagrama una recta que baja de un grupo  $G$  a un grupo  $H$  significa que  $H$  es un subgrupo de  $G$ . Por tanto, el grupo más grande está más arriba en el diagrama. La figura 3.1 contiene los diagramas reticulares para los grupos  $\mathbb{Z}_4$  y  $V$  del ejemplo 3.2.

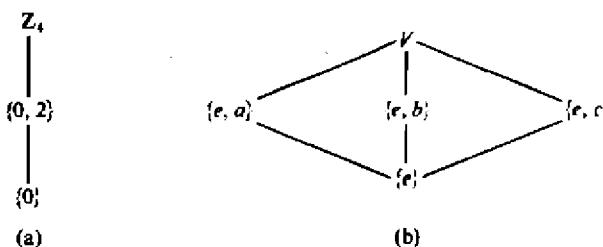


Fig. 3.1 (a) Diagrama reticular para  $\mathbb{Z}_4$ . (b) Diagrama reticular para  $V$ .

Nótese que si  $H \leq G$  y  $a \in H$  entonces, por el teorema 2.2, la ecuación  $ax = a$  debe tener solución única, a saber, el elemento identidad de  $H$ . Pero esta ecuación también puede verse como una ecuación en  $G$  y vemos que esta solución única debe ser también la identidad  $e$  de  $G$ . Un argumento análogo aplicado a la ecuación  $ax = e$  considerada tanto en  $H$  como en  $G$ , muestra que el inverso  $a^{-1}$  de  $a$  en  $G$  es también el inverso de  $a$  en el subgrupo  $H$ .

Conviene tener un criterio de rutina para determinar si un subconjunto de un grupo  $G$  es un subgrupo de  $G$ . El siguiente teorema proporciona dicho criterio. Aunque hay criterios más compactos que involucran una sola condición, preferimos éste, por ser más transparente, para un primer curso.

**Teorema 3.1** *Un subconjunto  $H$  de un grupo  $G$  es un subgrupo de  $G$  si y sólo si*

- 1  *$H$  es cerrado bajo la operación binaria de  $G$ ;*
- 2 *la identidad  $e$  de  $G$  está en  $H$ ;*
- 3 *para todos los  $a \in H$  es cierto que  $a^{-1} \in H$  también.*

**Demostración** El hecho de que si  $H \leq G$  entonces deben cumplirse las condiciones 1, 2 y 3, se desprende de inmediato de la definición de subgrupo y de las observaciones que preceden al enunciado del teorema.

De manera recíproca, supóngase que  $H$  es un subconjunto de un grupo  $G$  tal que se cumplen las condiciones 1, 2 y 3. Por 2 tenemos de inmediato que  $\mathcal{G}_2$  se satisface. También  $\mathcal{G}_3$  se satisface por 3. Falta corroborar el axioma asociativo  $\mathcal{G}_1$ . Pero, con seguridad, para toda  $a, b, c \in H$  es cierto que  $(ab)c = a(bc)$  en  $H$  ya que en realidad podemos considerarla una ecuación en  $G$ , donde se cumple la ley asociativa. De aquí que  $H \leq G$ . ■

### 3.3 SUBGRUPOS CICLICOS

En el ejemplo 3.2 observamos que  $\{0, 3\}$  no es un subgrupo de  $\mathbb{Z}_4$ . Veamos qué tan grande tendría que ser un subgrupo  $H$  de  $\mathbb{Z}_4$  que contenga el 3. Tendría que contener la identidad 0 y el inverso de 3 que es 1. También  $H$  debería contener a  $3 + 3$  que es 2. Así, el único subgrupo de  $\mathbb{Z}_4$  que contiene el 3 es  $\mathbb{Z}_4$  mismo.

Se imitará ahora este razonamiento en una situación general. Como ya se dijo, para un argumento general se usa siempre la notación multiplicativa. Sea  $G$  un grupo y sea  $a \in G$ . Un subgrupo de  $G$  que contenga  $a$  debe, por el teorema 3.1, contener  $aa$ , lo que denotaremos por  $a^2$ . Entonces, debe contener  $a^2a$  lo que denotamos por  $a^3$ . En general, debe contener  $a^n$ , que es el resultado del cálculo de productos de  $a$  por sí mismo,  $n$  factores para cada entero positivo  $n$ . (En notación aditiva denotaríamos esto por  $na$ .) Estas potencias enteras positivas de  $a$  conforman un conjunto cerrado bajo multiplicación. Sin embargo, es posible que el inverso de  $a$  no esté en este conjunto. Desde luego, un subgrupo que contenga  $a$  debe contener también  $a^{-1}$  y, por tanto,  $a^{-1}a^{-1}$ , lo que denotamos por  $a^{-2}$  y en general, debe contener  $a^{-m}$  para toda  $m \in \mathbb{Z}^+$ . Debe contener la identidad  $e = aa^{-1}$ . Por razones simbólicas obvias, estamos de acuerdo en que  $a^0$  sea  $e$ . En resumen, se ha mostrado que *un subgrupo de  $G$  que contenga  $a$ , debe contener todos los elementos  $a^n$  (o  $na$  para grupos aditivos) para toda  $n \in \mathbb{Z}$* . Es decir, un subgrupo que contenga  $a$  debe contener  $\{a^n | n \in \mathbb{Z}\}$ . Obsérvese que estas potencias  $a^n$  de  $a$  no son por fuerza distintas. Por ejemplo, en el grupo  $V$  del ejemplo 3.2

$$a^2 = e, \quad a^3 = a, \quad a^4 = e, \quad a^{-1} = a, \quad \text{y así sucesivamente.}$$

Es fácil ver que se cumple la ley usual de los exponentes  $a^m a^n = a^{m+n}$  para  $m, n \in \mathbb{Z}$ . Es claro para  $m, n \in \mathbb{Z}^+$ . Podemos ilustrar otro tipo de caso con un ejemplo:

$$\begin{aligned} a^{-2}a^5 &= a^{-1}a^{-1}aaaaa = a^{-1}(a^{-1}a)aaaa = a^{-1}aaaaa = a^{-1}(ea)aaa \\ &= a^{-1}aaaa = (a^{-1}a)aaa = eaaa = (ea)aa = aaa = a^3. \end{aligned}$$

Dejamos los detalles de la demostración del caso general a los estudiantes que no teman aburrirse. Casi se ha demostrado el siguiente teorema.

**Teorema 3.2.** *Sea  $G$  un grupo y sea  $a \in G$ . Entonces*

$$H = \{a^n | n \in \mathbb{Z}\}$$

*es un subgrupo de  $G$  y es el menor subgrupo de  $G$  que contiene  $a$ , esto es, cada subgrupo que contiene  $a$  contiene  $H$ .*

<sup>†</sup> Se podrá distinguir entre los términos *minimal* y *menor* cuando se apliquen a subconjuntos de un conjunto  $S$  que tengan alguna propiedad. Un subconjunto  $H$  de  $S$  es *minimal* con respecto a la propiedad si  $H$  tiene la propiedad y ningún subconjunto  $K \subset H$ ,  $K \neq H$  tiene la propiedad. Si  $H$  tiene la propiedad y  $H \subseteq K$  para todo subconjunto  $K$  con la propiedad, entonces  $H$  es el subconjunto menor con la propiedad. Puede haber muchos subconjuntos minimales, pero sólo un subconjunto menor. Para ilustrar,  $\{e, a\}$ ,  $\{e, b\}$  y  $\{e, c\}$  son todos los subgrupos no triviales minimales del grupo  $V$ . (Véase la figura 3.1.) Sin embargo,  $V$  no contiene un subgrupo no trivial menor.

**Demostración** Verifíquese si se cumplen las tres condiciones dadas en el teorema 3.1, para que un subconjunto de un grupo dé un subgrupo. Puesto que  $a^r a^s = a^{r+s}$  para  $r, s \in \mathbb{Z}$ , el producto en  $G$  de dos elementos de  $H$  está en  $H$ . Así,  $H$  es cerrado bajo la operación de grupo de  $G$ . Además,  $a^0 = e$  de modo que  $e \in H$  y para  $a \in H$ ,  $a^{-r} \in H$  y  $a^{-r} a^r = e$ . Todas las condiciones se satisfacen y, por tanto,  $H \leq G$ .

Los argumentos previos al enunciado del teorema muestran que cualquier subgrupo de  $G$  que contenga  $a$ , debe contener  $H$  así,  $H$  es el subgrupo menor de  $G$  que contiene  $a$ . ■

**Definición** El grupo  $H$  del teorema 3.2 es el *subgrupo cíclico de  $G$  generado por  $a$*  y se denotará por  $\langle a \rangle$ .

**Definición** Un elemento  $a$  de un grupo  $G$  genera  $G$  y es un *generador de  $G$*  si  $\langle a \rangle = G$ . Un grupo  $G$  es *cíclico* si existe algún elemento  $a$  en  $G$  que genere  $G$ .

**Ejemplo 3.3** Sean  $\mathbb{Z}_4$  y  $V$  los grupos del ejemplo 3.2. Entonces  $\mathbb{Z}_4$  es cíclico y tanto 1 como 3 son generadores, esto es,

$$\langle 1 \rangle = \langle 3 \rangle = \mathbf{Z}_4.$$

Sin embargo,  $V$  no es cíclico pues  $\langle a \rangle$ ,  $\langle b \rangle$  y  $\langle c \rangle$  son subgrupos propios de 2 elementos. Es claro que  $\langle e \rangle$  es el subgrupo trivial de un elemento. ■

**Ejemplo 3.4** El grupo  $\mathbb{Z}$  bajo la suma es un grupo cíclico. Tanto 1 como  $-1$  son generadores del grupo. ■

**Ejemplo 3.5** Considérese el grupo  $\mathbb{Z}$  bajo la suma y búsquese  $\langle 3 \rangle$ . Aquí, la notación es aditiva y  $\langle 3 \rangle$  debe contener

$$3 \quad 3 + 3 = 6 \quad 3 + 3 + 3 = 9 \quad \text{y así sucesivamente,}$$

$$0 \quad -3 \quad -3 + -3 = -6 \quad -3 + -3 + -3 = -9 \quad \text{y así sucesivamente.}$$

En otras palabras, el subgrupo cíclico generado por 3 consta de todos los múltiplos de 3, positivos, negativos y el cero. Denotamos este subgrupo por  $3\mathbb{Z}$ , así como por  $\langle 3 \rangle$ . De manera similar,  $n\mathbb{Z}$  será el subgrupo cíclico  $\langle n \rangle$  de  $\mathbb{Z}$ . Nótese que  $6\mathbb{Z} \subset 3\mathbb{Z}$ . ■

## Ejercicios

3.1 Determina cuáles de los siguientes subconjuntos de los números complejos son subgrupos bajo la suma del grupo C de los números complejos bajo la suma.

- a)  $\mathbb{R}$       b)  $\mathbb{Q}^+$       c)  $7\mathbb{Z}$   
d) El conjunto  $i\mathbb{R}$  de los números imaginarios puros incluyendo 0  
e) El conjunto  $\pi\mathbb{Q}$  de los múltiplos racionales de  $\pi$   
f) El conjunto  $\{\pi^n \mid n \in \mathbb{Z}\}$

**3.2** A continuación se dan varios grupos. Proporcione una lista completa de todas las relaciones de un grupo cuando es subgrupo de algún otro grupo listado.

$$G_1 = \mathbb{Z} \text{ bajo la suma}$$

$$G_2 = 12\mathbb{Z} \text{ bajo la suma}$$

$$G_3 = \mathbb{Q}^+ \text{ bajo la multiplicación}$$

$$G_4 = \mathbb{R} \text{ bajo la suma}$$

$$G_5 = \mathbb{R}^+ \text{ bajo la multiplicación}$$

$$G_6 = \{\pi^n \mid n \in \mathbb{Z}\} \text{ bajo la multiplicación}$$

$$G_7 = 3\mathbb{Z} \text{ bajo la suma}$$

$$G_8 = \text{el conjunto de todos los múltiplos enteros de } 6 \text{ bajo la suma}$$

$$G_9 = \{6^n \mid n \in \mathbb{Z}\} \text{ bajo la multiplicación.}$$

**3.3** Escribanse al menos 5 elementos de cada uno de los siguientes grupos cíclicos.

a)  $25\mathbb{Z}$  bajo la suma

b)  $\{(\frac{n}{d})^n \mid n \in \mathbb{Z}\}$  bajo la multiplicación

c)  $\{x^n \mid n \in \mathbb{Z}\}$  bajo la multiplicación

**3.4** ¿Cuáles de los siguientes grupos son cíclicos? Para cada grupo cíclico obténganse todos los generadores del grupo.

$$G_1 = \langle \mathbb{Z}, + \rangle \quad G_2 = \langle \mathbb{Q}, + \rangle \quad G_3 = \langle \mathbb{Q}^+, \cdot \rangle \quad G_4 = \langle 6\mathbb{Z}, + \rangle$$

$$G_5 = \{6^n \mid n \in \mathbb{Z}\} \text{ bajo la multiplicación}$$

$$G_6 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ bajo la suma}$$

**3.5** Estúdiense la estructura de la tabla del grupo  $\mathbb{Z}_4$  del ejemplo 3.2.

a) Por analogía, complétense la tabla 3.5 para obtener el grupo cíclico  $\mathbb{Z}_6$  de 6 elementos.  
(No es necesario probar la ley asociativa.)

**Tabla 3.5**

$\mathbb{Z}_6:$	$+$	0	1	2	3	4	5
0	0	1	2	3	4	5	
1	1	2	3	4	5	0	
2	2						
3	3						
4	4						
5	5						

b) Calcúlense los subgrupos  $\langle 1 \rangle$ ,  $\langle 2 \rangle$ ,  $\langle 3 \rangle$ ,  $\langle 4 \rangle$  y  $\langle 5 \rangle$  del grupo  $\mathbb{Z}_6$  dado en la parte a).  
c) ¿Qué elementos son generadores para el grupo  $\mathbb{Z}_6$  de la parte a)?

**3.6** Muestrese que si  $H$  y  $K$  son subgrupos de un grupo abeliano  $G$ , entonces  $\{hk \mid h \in H \text{ y } k \in K\}$  es un subgrupo de  $G$ .

**3.7** ¿Falso o verdadero?

- a) La ley asociativa se cumple en todo grupo.
- b) Puede haber un grupo donde falle la ley de la cancelación.
- c) Todo grupo es un subgrupo de si mismo.

## 36 SUBGRUPOS

- d) Todo grupo tiene precisamente dos subgrupos impropios.
  - e) En todo grupo cíclico, todo elemento es un generador.
  - f) Hasta ahora, no se ha dado en el libro un ejemplo de grupo que no sea abeliano.
  - g) Todo conjunto de números que es grupo bajo la suma, también es grupo bajo la multiplicación.
  - h) Se puede definir un subgrupo como subconjunto de un grupo.
  - i)  $\mathbb{Z}_4$  es un grupo cíclico.
  - j) Todo subconjunto de todo grupo es un subgrupo bajo la operación inducida.
- 

3.8 Encuéntrese el error en el siguiente argumento: «La condición 2 del teorema 3.1 es redundante, ya que puede derivarse de 1 y 3, para ello sea  $a \in H$ . Entonces,  $a^{-1} \in H$  por 3 y, por 1,  $aa^{-1} = e$  es un elemento de  $H$ , lo cual prueba 2.»

3.9 Muéstrese que un subconjunto no vacío  $H$  de un grupo  $G$  es un subgrupo de  $G$  si y sólo si  $ab^{-1} \in H$  para toda  $a, b \in H$ . (Este es uno de los criterios más compactos mencionados antes del teorema 3.1.)

3.10 Pruébese que un grupo cíclico con un solo generador puede tener a lo más 2 elementos.

3.11 Pruébese que si  $G$  es un grupo abeliano con identidad  $e$ , entonces todos los elementos  $x$  de  $G$  que satisfacen la ecuación  $x^2 = e$  forman un subgrupo  $H$  de  $G$ .

3.12 Repítase el ejercicio 3.11 para la situación general del conjunto  $H$  de todas las soluciones  $x$  de la ecuación  $x^n = e$ , para un entero fijo  $n \geq 1$ , en un grupo abeliano  $G$  con identidad  $e$ .

3.13 Muéstrese que si  $a \in G$ , donde  $G$  es un grupo finito con identidad  $e$ , entonces existe  $n \in \mathbb{Z}^+$  tal que  $a^n = e$ .

3.14 Sea la operación binaria de un grupo  $G$  cerrada en un subconjunto finito no vacío  $H$  de  $G$ . Muéstrese que  $H$  es un subgrupo de  $G$ .

3.15 Sea  $G$  un grupo y  $a$  un elemento fijo de  $G$ , muéstrese que

$$H_a = \{x \in G \mid xa = ax\}$$

es un subgrupo de  $G$ .

3.16 Generalizando el ejercicio 3.15, sea  $S$  cualquier subconjunto de un grupo  $G$ .

- a) Muéstrese que  $H_S = \{x \in G \mid xs = sx \text{ para toda } s \in S\}$  es un subgrupo de  $G$ .
- b) Con referencia a la parte a), el subgrupo  $H_G$  es el centro de  $G$ . Muéstrese que  $H_G$  es un grupo abeliano.

3.17 Sea  $H$  un subgrupo de un grupo  $G$ . Para  $a, b \in G$  sea  $a \sim b$  si y sólo si  $ab^{-1} \in H$ . Muéstrese que  $\sim$  es una relación de equivalencia en  $G$ .

3.18 Para los conjuntos  $H$  y  $K$  definase la intersección  $H \cap K$  por

$$H \cap K = \{x \mid x \in H \text{ y } x \in K\}.$$

Muéstrese que si  $H \leq G$  y  $K \leq G$ , entonces  $H \cap K \leq G$ .

3.19 Muéstrese, mediante un ejemplo, la posibilidad de que la ecuación cuadrática  $x^2 = e$  tenga más de dos soluciones en algún grupo  $G$  con identidad  $e$ .

## 4

# Permutaciones I

## 4.1 FUNCIONES Y PERMUTACIONES

En este capítulo y en el siguiente trabajaremos con grupos cuyos elementos son entes llamados *permutaciones*. Estos grupos nos proporcionarán los primeros ejemplos de grupos que no son abelianos. Mostraremos, en un capítulo posterior, que cualquier grupo es estructuralmente el mismo que algún grupo de permutaciones. Por desgracia, este resultado, que parece muy importante, no resulta útil en particular.

Quizás estén familiarizados con la idea de permutación de un conjunto como un rearrreglo de elementos del conjunto. Así, para el conjunto  $\{1, 2, 3, 4, 5\}$  se podría dar, esquemáticamente, un rearrreglo de los elementos, como en la figura 4.1, y obtener el nuevo arreglo  $\{4, 2, 5, 3, 1\}$ . Pensemos en este diagrama esquemático de la figura 4.1 como una traslación o una *transformación* de cada elemento de la columna de la izquierda, en un único elemento (no necesariamente distinto) del mismo conjunto listado a la derecha. De este modo, el 1 va a dar al 4, el 2 se transforma en el 2, y así sucesivamente. Más aún para ser permutación del conjunto, esta transformación debe ser tal que cada elemento aparezca una y sólo una vez en la columna de la derecha. Por ejemplo, el diagrama en la figura

$$1 \rightarrow 4$$

$$2 \rightarrow 2$$

$$3 \rightarrow 5$$

$$4 \rightarrow 3$$

$$5 \rightarrow 1$$

$$1 \rightarrow 3$$

$$2 \rightarrow 2$$

$$3 \rightarrow 4$$

$$4 \rightarrow 5$$

$$5 \rightarrow 3$$

Figura 4.1

Figura 4.2

4.2 no da una permutación, pues en la columna derecha, el 3 aparece dos veces mientras que el 1 no aparece. Definiremos una permutación como dicho tipo de transformación. Sin embargo, la idea general de asignar a cada elemento de algún conjunto un elemento del mismo o quizás de un conjunto diferente, se presentará tan a menudo en nuestro trabajo que daremos primero una definición aparte de este concepto. El concepto es el de *función*, término que ya han encontrado.

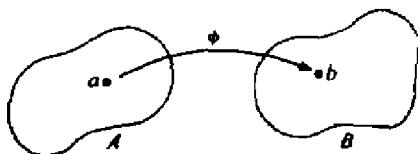


Figura 4.3

**Definición** Una función o transformación  $\phi$  de un conjunto  $A$  en un conjunto  $B$  es una regla que asigna a cada elemento  $a$  de  $A$  exactamente un elemento  $b$  de  $B$ . Se dice que  $\phi$  transforma  $a$  en  $b$  (o que  $\phi$  lleva  $a$  en  $b$ ) y que  $\phi$  transforma o lleva  $A$  en  $B$ .

La notación clásica para denotar que  $\phi$  lleva  $a$  en  $b$  es

$$\phi(a) = b$$

Sin embargo, con frecuencia usaremos la notación

$$a\phi = b$$

También se encuentra en la literatura la notación  $a^\phi = b$ . El elemento  $b$  es la imagen de  $a$  bajo  $\phi$ . El hecho de que  $\phi$  lleva  $A$  en  $B$  se representará simbólicamente por

$$\phi : A \rightarrow B$$

Será útil para el estudiante considerar una función en términos de la figura 4.3. De las tres notaciones posibles dadas después de la definición que expresan que  $\phi$  lleva  $a$  en  $b$ , el estudiante conoce la notación  $\phi(a) = b$  por cursos anteriores.

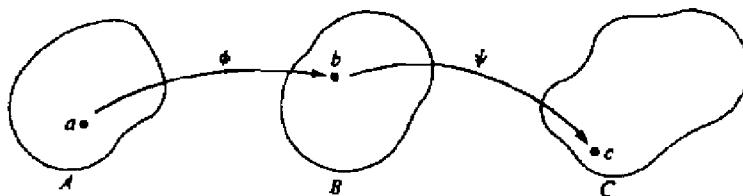


Figura 4.4

Muchos algebristas prefieren las notaciones  $a\phi = b$  y  $a^{\phi} = b$  por la siguiente razón: si  $\phi$  y  $\psi$  son funciones con  $\phi : A \rightarrow B$  y  $\psi : B \rightarrow C$ , entonces existe una función natural que lleva  $A$  en  $C$  como se ilustra en la figura 4.4. Esto es, se puede ir de  $A$  a  $C$  vía  $B$ , usando las funciones  $\phi$  y  $\psi$ . Esta función que lleva  $A$  en  $C$  es la función compuesta constituida por  $\phi$  seguida de  $\psi$ . En la notación clásica  $\phi(a) = b$  y  $\psi(b) = c$  luego,

$$\psi(\phi(a)) = c$$

y se denota la función compuesta por  $\psi\phi$ . El símbolo  $\psi\phi$  para  $\phi$  seguida de  $\psi$  se tiene, entonces, que leer de derecha a izquierda. En las notaciones más recientes tenemos  $a\phi = b$  y  $b\psi = c$  con

$$a(\phi\psi) = (a\phi)\psi = c$$

o  $a^{\phi} = b$  y  $b^{\psi} = c$  con

$$a^{(\phi\psi)} = (a^{\phi})^{\psi} = c$$

Por tanto, la función compuesta en estas notaciones es  $\phi\psi$  y puede leerse de izquierda a derecha. Sugerimos al estudiante leer las notaciones  $a\phi = b$  y  $a^{\phi} = b$  como «la imagen de  $a$  bajo  $\phi$  es  $b$ ». Comprenderán que toda esta discusión no es acerca del concepto, sino sobre notación. Sin embargo, una mala selección de notación puede entorpecer mucho el desarrollo de una teoría matemática.

Volviendo a las permutaciones, de acuerdo con nuestra definición, vemos que la asignación de la figura 4.2 es una función de  $\{1, 2, 3, 4, 5\}$  en si misma. Pero no queremos llamar a esto una permutación. Es necesario escoger aquellas funciones  $\phi$  tal que *todo* elemento del conjunto es imagen de *exactamente un* solo elemento. De nuevo, existe una terminología para una situación más general.

**Definición** Una función de un conjunto  $A$  en un conjunto  $B$  es *uno a uno* si cada elemento de  $B$  es imagen de *al más* un elemento de  $A$  y es *sobre B* si cada elemento de  $B$  es imagen de *al menos* un elemento de  $A$ .

En términos de la figura 4.3, una función  $\phi : A \rightarrow B$  es uno a uno si cada  $b \in B$  tiene *al más una* flecha dirigida hacia si. Decir que  $\phi$  es sobre  $B$ , es decir que *toda*  $b \in B$  tiene *al menos una* flecha dirigida hacia si. Puesto que a menudo estaremos probando qué ciertas funciones son uno a uno, o sobre, o ambas cosas, vale la pena mencionar la técnica a utilizar.

- 1 Para mostrar que  $\phi$  es uno a uno, se muestra que  $a_1\phi = a_2\phi$  implica  $a_1 = a_2$
- 2 Para mostrar que  $\phi$  es sobre  $B$ , se muestra que para todo  $b \in B$  existe  $a \in A$  tal que  $a\phi = b$

Por último, señalemos que para  $\phi : A \rightarrow B$ , el conjunto  $A$  es el **dominio de  $\phi$** ; el conjunto  $B$  es el **codominio de  $\phi$**  y el conjunto  $A\phi = \{a\phi \mid a \in A\}$  es la **imagen de  $A$  bajo  $\phi$** .

Para una permutación del conjunto  $A$  queremos que cada elemento de  $A$  sea imagen de uno y sólo un elemento de  $A$ , de aquí la siguiente definición.

**Definición** Una **permutación de un conjunto  $A$**  es una función de  $A$  en  $A$  que es tanto uno a uno como sobre. En otras palabras, una permutación de  $A$  es una función uno a uno de  $A$  sobre  $A$ .

También escribimos

$$\phi : A \xrightarrow{\text{1-1 sobre}} B$$

para representar una función  $\phi$  uno a uno de  $A$  sobre  $B$ .

Es necesario emplear algo de tiempo en estudiar y tratar de entender estas ideas; esto facilitará el curso. La terminología es todavía la usual, aunque hay otra terminología que está más y más en boga, propagada por los discípulos de N. Bourbaki. No usaremos aquí esa terminología, pero la daremos para que ustedes comprendan su significado en caso de encontrarla. En la nueva terminología, una transformación uno a uno es una **inyección**; una transformación sobre es una **suprayección** y una transformación que es uno a uno y sobre es una **biyección**.

## 4.2 GRUPOS DE PERMUTACIONES

En las permutaciones de un conjunto se define una operación binaria natural, la **multiplicación de permutaciones**. Sea  $A$  un conjunto y sean  $\sigma$  y  $\tau$  permutaciones de  $A$  de modo que  $\sigma$  y  $\tau$  son funciones uno a uno y llevan  $A$  sobre  $A$ . La función compuesta  $\sigma\tau$ , como se ilustra en la figura 4.4, con  $B = C = A$ ;  $\phi = \sigma$  y  $\psi = \tau$ , nos da una transformación de  $A$  en  $A$ . Ahora bien,  $\sigma\tau$  será una permutación si es uno a uno y sobre  $A$ . Usamos la notación de escribir las funciones a la derecha, de manera que  $\sigma\tau$  puede leerse de izquierda a derecha. Mostremos que  $\sigma\tau$  es uno a uno. Si

$$a_1(\sigma\tau) = a_2(\sigma\tau),$$

entonces

$$(a_1\sigma)\tau = (a_2\sigma)\tau,$$

y como está dado que  $\tau$  es uno a uno, sabemos que  $a_1\sigma = a_2\sigma$ . Pero entonces, como  $\sigma$  es uno a uno, esto da  $a_1 = a_2$ . De aquí que  $\sigma\tau$  es uno a uno. Para

mostrar que  $\sigma\tau$  es sobre  $A$ , sea  $a \in A$ . Como  $\tau$  es sobre  $A$ , existe  $a' \in A$  tal que  $a'\tau = a$ . Como  $\sigma$  es sobre  $A$ , existe  $a'' \in A$  tal que  $a' = a''\sigma$ . Entonces,

$$a = a'\tau = (a''\sigma)\tau = a''(\sigma\tau),$$

de modo que  $\sigma\tau$  es sobre  $A$ .

Para ilustrar esto, supóngase que

$$A = \{1, 2, 3, 4, 5\}$$

y que  $\sigma$  es la permutación dada por la figura 4.1. Escribimos  $\sigma$  en una notación más común como

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix},$$

así,  $1\sigma = 4$ ;  $2\sigma = 2$ , y así sucesivamente. Sea

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix},$$

entonces,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}.$$

Por ejemplo,

$$1(\sigma\tau) = (1\sigma)\tau = 4\tau = 2.$$

Mostremos ahora que la colección de todas las permutaciones de un conjunto  $A$  no vacío forma un grupo bajo esta multiplicación de permutaciones.

**Teorema 4.1** *Sea  $A$  un conjunto no vacío y sea  $S_A$  la familia de todas las permutaciones de  $A$ . Entonces  $S_A$  es un grupo bajo la multiplicación de permutaciones.*

**Demostración** Debemos verificar tres axiomas. Como las permutaciones son funciones, para mostrar que para las permutaciones  $\sigma$ ,  $\tau$  y  $\mu$  se cumple que

$$(\sigma\tau)\mu = \sigma(\tau\mu),$$

tenemos que mostrar que cada función compuesta lleva a toda  $a \in A$  en la misma imagen en  $A$ . Esto es, debemos mostrar que

$$a[(\sigma\tau)\mu] = a[\sigma(\tau\mu)]$$

para toda  $a \in A$ . Tenemos

$$a[(\sigma\tau)\mu] = [a(\sigma\tau)]\mu = [(a\sigma)\tau]\mu = (a\sigma)(\tau\mu) = a[\sigma(\tau\mu)].$$

Por consiguiente,  $(\sigma\tau)\mu$  y  $\sigma(\tau\mu)$  llevan toda  $a \in A$  al mismo elemento  $[(a\sigma)\tau]\mu$  y son, por tanto, la misma permutación. Como no empleamos el hecho de que  $\sigma$ ,  $\tau$  y  $\mu$  son uno a uno y sobre, en realidad probamos que la *composición de funciones es asociativa*. Entonces, se satisface  $\mathcal{G}_1$ .

La permutación  $i$  tal que  $ai = a$  para todas las  $a \in A$ , obviamente actúa como identidad. Por tanto, se satisface  $\mathcal{G}_2$ .

Para una permutación  $\sigma$  definimos  $\sigma^{-1}$  como la permutación que invierte la dirección de la transformación  $\sigma$ , esto es,  $a\sigma^{-1}$  será el elemento  $a'$  de  $A$  tal que  $a = a'\sigma$ . La existencia de exactamente un elemento  $a'$  con esa característica se debe a que, como función,  $\sigma$  es uno a uno y sobre. (Véase el ejercicio 4.18.) Es claro que

$$ai = a = a'\sigma = (a\sigma^{-1})\sigma = a(\sigma^{-1}\sigma)$$

y también que

$$a'i = a' = a\sigma^{-1} = (a'\sigma)\sigma^{-1} = a'(\sigma\sigma^{-1}),$$

de manera que  $\sigma^{-1}\sigma$  y  $\sigma\sigma^{-1}$  son, ambas, la permutación  $i$ . Así, se satisface  $\mathcal{G}_3$ .

Al definir permutación, no fue necesario que  $A$  fuera un conjunto finito. Sin embargo, casi todos nuestros ejemplos de grupos de permutaciones tratarán con permutaciones de conjuntos finitos. Es claro que si tanto  $A$  como  $B$  tienen el mismo número de elementos, entonces el grupo de todas las permutaciones de  $A$  tiene la misma estructura que el grupo de todas las permutaciones de  $B$ . Se puede obtener un grupo a partir del otro simplemente cambiando el nombre a los elementos. Este es, de nuevo, el concepto de *grupos isomorfos* mencionado en el capítulo 2 y acerca del cual hablaremos más adelante.

**Definición** Si  $A$  es el conjunto finito  $\{1, 2, \dots, n\}$ , entonces el grupo de todas las permutaciones de  $A$  es el *grupo simétrico de n letras* y se denota por  $S_n$ .

Nótese que  $S_n$  tiene  $n!$  elementos, donde

$$n! = n(n - 1)(n - 2) \dots (3)(2)(1).$$

### 4.3 DOS EJEMPLOS IMPORTANTES

**Ejemplo 4.1** Un ejemplo interesante es el grupo  $S_3$  de  $3! = 6$  elementos. Sea el conjunto  $A = \{1, 2, 3\}$ . Listense las permutaciones de  $A$  y a cada una asígnese

una letra griega con subíndice. Más adelante se aclararán las razones para asignar los nombres y para sombrear la tabla. Sea

$$\begin{aligned}\rho_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \mu_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \rho_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \mu_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \\ \rho_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & \mu_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\end{aligned}$$

Puede verificarse que la tabla de multiplicación dada en la tabla 4.1 es correcta. Nótese que este grupo no es abeliano. Este es el primer ejemplo que tenemos de ello. Hemos visto que cualquier grupo de a lo más 4 elementos es abeliano. Más adelante veremos que un grupo de 5 elementos también es abeliano. Así,  $S_3$  tiene el orden menor entre los grupos no abelianos. ■

**Tabla 4.1**

	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_0$	$\mu_2$	$\mu_3$	$\mu_1$
$\rho_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\mu_3$	$\mu_1$	$\mu_2$
$\mu_1$	$\mu_1$	$\mu_3$	$\mu_2$	$\rho_0$	$\rho_2$	$\rho_1$
$\mu_2$	$\mu_2$	$\mu_1$	$\mu_3$	$\rho_1$	$\rho_0$	$\rho_2$
$\mu_3$	$\mu_3$	$\mu_2$	$\mu_1$	$\rho_2$	$\rho_1$	$\rho_0$

Hay una correspondencia natural entre los elementos de  $S_3$  en el ejemplo 4.1 y las maneras en que pueden colocarse, una sobre otra, dos copias de un triángulo equilátero con vértices 1,2 y 3 (véase la figura 4.5). Por esta razón,  $S_3$  es además el grupo  $D_3$ , de simetrías de un triángulo equilátero. Usamos  $\rho_i$  para las rotaciones y  $\mu_i$  para las imágenes reflejadas en bisectrices de los ángulos. La notación  $D_3$

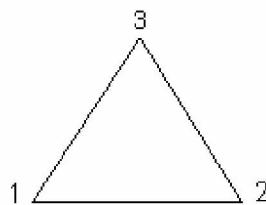


Figura 4.5

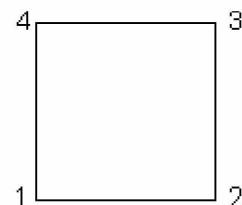


Figura 4.6

representa al tercer grupo diédrico. El **n-ésimo grupo diédrico**  $D_n$ . es el grupo de simetrías del n-ágono regular.

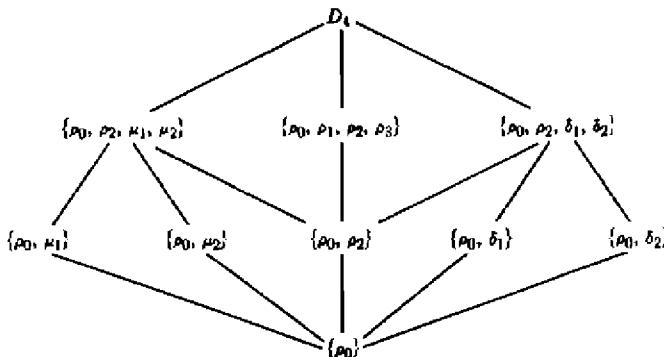
**Ejemplo 4.2** Fórmese el grupo diédrico  $D_4$  de permutaciones, correspondientes a los nodos en que puedan superponerse dos copias de un cuadrado con vértices 1, 2, 3 y 4 (véase la Figura 4.6).  $D_4$  será el **grupo de simetrías del cuadrado**. También se le llama grupo octal. De nuevo, úsese una notación y sombreo en la tabla que parece arbitraria, pero que se explicará más adelante. Intuitivamente usemos  $\rho_i$  para *rotaciones*,  $\mu_i$  para *imágenes reflejadas* en bisectrices perpendiculares a los lados y  $\delta_i$  para los reflejos en las *diagonales*. En este caso hay ocho permutaciones. Sea

$$\begin{aligned}\rho_0 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, & \mu_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\ \rho_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, & \mu_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \\ \rho_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, & \mu_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\ \rho_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, & \mu_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.\end{aligned}$$

Puede verificarse que la tabla para  $D_4$ , dada en la tabla 4.2 es correcta. Nótese que  $D_4$ , tampoco es abeliano. Este grupo es sencillamente una belleza. Nos proporcionará magníficos ejemplos para casi todos los conceptos que presentaremos en teoría de grupos. ¡Qué bellas simetrías hay en la tabla!

**Tabla 4.1**

	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\mu_1$	$\mu_2$	$\delta_1$	$\delta_2$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\mu_1$	$\mu_2$	$\delta_1$	$\delta_2$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_3$	$\rho_0$	$\delta_2$	$\delta_1$	$\mu_1$	$\mu_2$
$\rho_2$	$\rho_2$	$\rho_3$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_1$	$\delta_2$	$\delta_1$
$\rho_3$	$\rho_3$	$\rho_0$	$\rho_1$	$\rho_2$	$\delta_1$	$\delta_2$	$\mu_2$	$\mu_1$
$\mu_1$	$\mu_1$	$\delta_1$	$\mu_2$	$\delta_2$	$\rho_0$	$\rho_2$	$\rho_1$	$\rho_3$
$\mu_2$	$\mu_2$	$\delta_2$	$\mu_1$	$\delta_1$	$\rho_2$	$\rho_0$	$\rho_3$	$\rho_1$
$\delta_1$	$\delta_1$	$\mu_2$	$\delta_2$	$\mu_1$	$\rho_3$	$\rho_1$	$\rho_0$	$\rho_2$
$\delta_2$	$\delta_2$	$\mu_1$	$\delta_1$	$\mu_2$	$\rho_1$	$\rho_3$	$\rho_2$	$\rho_0$



**Fig. 4.7** Diagrama reticular para \$D\_4\$.

Por último, en la figura 4.7 se muestra el diagrama reticular para los subgrupos de \$D\_4\$. Verifíquese si es correcto. ■

## Ejercicios

---

**4.1** Considérense las tres permutaciones en \$S\_6\$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix},$$

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix},$$

Calcúlese

a) \$\sigma\tau\$,      b) \$\sigma\tau^2\$,      c) \$\sigma^2\mu\$,      d) \$\tau\sigma^{-2}\$,      e) \$\sigma\tau\sigma^{-1}\$.

**4.2** ¿Cuáles de las siguientes funciones de \$\mathbb{R}\$ en \$\mathbb{R}\$ son permutaciones de \$\mathbb{R}\$?

- a) \$f\_1: \mathbb{R} \rightarrow \mathbb{R}\$ definida por \$f\_1(x) = x + 1\$
- b) \$f\_2: \mathbb{R} \rightarrow \mathbb{R}\$ definida por \$f\_2(x) = x^2\$
- c) \$f\_3: \mathbb{R} \rightarrow \mathbb{R}\$ definida por \$f\_3(x) = -x^3\$
- d) \$f\_4: \mathbb{R} \rightarrow \mathbb{R}\$ definida por \$f\_4(x) = e^x\$
- e) \$f\_5: \mathbb{R} \rightarrow \mathbb{R}\$ definida por \$f\_5(x) = x^3 - x^2 - 2x\$

**4.3** Considérese el grupo \$S\_3\$ del ejemplo 4.1.

- a) Encuéntrense los subgrupos cíclicos \$\langle \rho\_1 \rangle\$, \$\langle \rho\_2 \rangle\$ y \$\langle \mu\_1 \rangle\$ de \$S\_3\$
- b) Encuéntrense todos los subgrupos, propios e impropios, de \$S\_3\$ y elabórese el diagrama reticular correspondiente.

4.4 Obténgase la tabla de multiplicación para el subgrupo cíclico de  $S_5$  generado por

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}.$$

Habrá 6 elementos. Sean  $\rho, \rho^2, \rho^3, \rho^4, \rho^5$  y  $\rho^0 = \rho^6$ . ¿Acaso este grupo es isomorfo a  $S_3$ ?

4.5 Sea  $A$  un conjunto y  $a$  un elemento de  $A$ . Sea  $T_a$  el conjunto de todas las permutaciones de  $A$  que tengan la propiedad de que  $a\sigma = a$ . Muéstrese que  $T_a$  es un subgrupo del grupo  $S_A$  de todas las permutaciones de  $A$  dado en el teorema 4.1.

4.6 ¿Falso o verdadero?

- a) Toda permutación es una función uno a uno.
  - b) Toda función es una permutación si y sólo si es uno a uno.
  - c) Toda función de un conjunto finito sobre sí mismo debe ser uno a uno.
  - d) Hasta ahora no se ha dado en el libro un ejemplo de un grupo que no sea abeliano.
  - e) Todo subgrupo de un grupo abeliano es abeliano.
  - f) Todo elemento de un grupo genera un subgrupo cíclico del grupo.
  - g) El grupo simétrico  $S_{10}$  tiene 10 elementos.
  - h) El grupo simétrico  $S_3$  es cíclico.
  - i)  $S_n$  no es cíclico para cualquier  $n$ .
  - j) Todo grupo es isomorfo a algún grupo de permutaciones.
- 

4.7 Muéstrese, mediante un ejemplo, que todo subgrupo propio de un grupo no abeliano puede ser abeliano.

4.8 Para las permutaciones  $\sigma, \tau$  y  $\mu$  del ejercicio 4.1, encuéntrese

a)  $|\langle \sigma \rangle|$       b)  $|\langle \tau^2 \rangle|$       c)  $\sigma^{100}$       d)  $\mu^{100}$

4.9 En forma análoga a los ejemplos 4.1 y 4.2, considérese un  $n$ -ágono plano regular para  $n \geq 3$ . Cada una de las maneras en que puedan superponerse dos copias de dicho  $n$ -ágono, corresponde a cierta permutación de los vértices. El conjunto de estas permutaciones es un grupo, el  $n$ -ésimo grupo diédrico  $D_n$ , bajo la multiplicación de permutaciones. Encuéntrese el orden de este grupo  $D_n$ . Proporciónense argumentos geométricos para probar que este grupo tiene un subgrupo con justo la mitad de elementos que tiene el grupo.

4.10 Considérese un cubo que quepa exactamente en una caja cúbica. Como en el caso de los ejemplos 4.1 y 4.2, las maneras en que se puede colocar el cubo dentro de la caja, corresponden a cierto grupo de permutaciones de los vértices del cubo. Este grupo es el grupo de movimientos rígidos del cubo. (No debe confundirse con el grupo de simetrías del cubo que se analizará en los ejercicios del capítulo 10.) ¿Cuántos elementos tiene este grupo? Proporciónense argumentos geométricos para probar que este grupo tiene al menos tres subgrupos diferentes de orden 4 y al menos cuatro subgrupos diferentes de orden 3.

4.11 Muéstrese que  $S_n$  es un grupo no abeliano para  $n \geq 3$ .

4.12 Para complementar el ejercicio 4.11, muéstrese que si  $n \geq 3$ , el único elemento  $\sigma$  de  $S_n$  que satisface  $\sigma y = y\sigma$  para toda  $y \in S_n$  es  $\sigma = i$ , la permutación identidad.

4.13 Sean  $A$  un conjunto,  $B$  un subconjunto de  $A$ , y  $b$  un elemento fijo de  $B$ . ¿Cuál de los siguientes es un subgrupo de  $S_A$ ?

- a)  $\{\sigma \in S_A \mid b\sigma = b\}$
- b)  $\{\sigma \in S_A \mid b\sigma \in B\}$
- c)  $\{\sigma \in S_A \mid B\sigma \subseteq B\}$
- d)  $\{\sigma \in S_A \mid B\sigma = B\}$

4.14 Sea  $A$  un conjunto y  $\sigma \in S_A$ . Para un  $a \in A$  fijo, el conjunto

$$\mathcal{O}_{a,\sigma} = \{a\sigma^n \mid n \in \mathbb{Z}\}$$

es la órbita de  $a$  bajo  $\sigma$ . Encuéntrense las órbitas de 1 bajo cada una de las permutaciones del ejercicio 4.1.

4.15 Respecto al concepto definido en el ejercicio 4.14 muéstrese que si para  $a, b \in A$ ,  $\mathcal{O}_{a,\sigma}$  y  $\mathcal{O}_{b,\sigma}$  tienen algún elemento en común, entonces  $\mathcal{O}_{a,\sigma} = \mathcal{O}_{b,\sigma}$ .

4.16 Si  $A$  es un conjunto, entonces un subgrupo  $H$  de  $S_A$  es transitivo en  $A$  si para toda  $a, b \in A$  existe  $\sigma \in H$  tal que  $a\sigma = b$ . Muéstrese que si  $A$  es un conjunto no vacío finito, entonces existe un subgrupo cíclico finito  $H$  de  $S_A$  con  $|H| = |A|$  que es transitivo en  $A$ .

4.17 Con respecto a los ejercicios 4.14 y 4.16, muéstrese que para  $\sigma \in S_A$ ,  $\langle \sigma \rangle$  es transitivo en  $A$  si y sólo si  $\mathcal{O}_{a,\sigma} = A$  para alguna  $a \in A$ .

*El siguiente ejercicio es de teoría de conjuntos. Se pide probar algo que en el texto usamos de manera intuitiva.*

4.18 Sea  $\phi: A \rightarrow B$ . La transformación  $\phi^{-1}: B \rightarrow A$  es una inversa de  $\phi$  si  $(x\phi)\phi^{-1} = x$  para toda  $x \in A$  y  $(y\phi^{-1})\phi = y$  para toda  $y \in B$ .

- a) Muéstrese que  $\phi$  es una biyección si y sólo si tiene inversa.
- b) Muéstrese que la inversa de una biyección  $\phi$  es única.

## Permutaciones II

### 5.1 CICLOS Y NOTACION CICLICA

Existe otra notación para permutaciones. Supongamos que se distribuyen equitativamente los cinco números 2, 4, 3, 6, 8 en una circunferencia, como se muestra en la figura 5.1. Supóngase que el círculo se rota  $2\pi/5$  radianes en sentido contrario al que giran las manecillas del reloj, de manera que el 2 queda en la posición que antes ocupaba el 4, el 4 a la que ocupaba el 3 y así sucesivamente. Sea  $\sigma$  la permutación en  $S_8$  que deja fijos al 1, 5 y 7 y actúa sobre los elementos restantes mediante la rotación del círculo descrita. Entonces,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 6 & 3 & 5 & 8 & 7 & 2 \end{pmatrix}.$$

Esta permutación  $\sigma$  es un *ciclo de longitud 5*; para ello se introduce una notación nueva, más compacta

$$\sigma = (2, 4, 3, 6, 8).$$

La nueva notación es la *notación cíclica*. Cada elemento que aparece en  $(2, 4, 3, 6, 8)$  se lleva al elemento siguiente excepto el último, que va a dar al primero. Se considera que los elementos que no aparecen en la notación quedan fijos bajo la permutación.

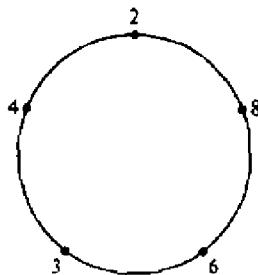


Figura 5.1

**Definición** Una permutación  $\sigma$  de un conjunto  $A$  es un *ciclo de longitud n* si existen  $a_1, a_2, \dots, a_n \in A$  tales que

$$a_1\sigma = a_2, \quad a_2\sigma = a_3, \quad \dots, \quad a_{n-1}\sigma = a_n, \quad a_n\sigma = a_1$$

y  $x\sigma = x$  para toda  $x \in A$  tal que  $x \notin \{a_1, a_2, \dots, a_n\}$ . Escribimos  $\sigma = (a_1, a_2, \dots, a_n)$ .

Al usar la notación cíclica, el conjunto  $A$  debe estar claramente ubicado en el contexto.

**Ejemplo 5.1** Si  $A = \{1, 2, 3, 4, 5\}$ , entonces

$$(1, 3, 5, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

Obsérvese que

$$(1, 3, 5, 4) = (3, 5, 4, 1) = (5, 4, 1, 3) = (4, 1, 3, 5). \blacksquare$$

Puesto que los ciclos son tipos particulares de permutaciones, pueden multiplicarse como cualesquiera dos permutaciones. Sin embargo, el producto de dos ciclos no necesariamente es un ciclo.

**Ejemplo 5.2** Sean  $(1, 4, 5, 6)$  y  $(2, 1, 5)$  ciclos en el grupo  $S_6$  de todas las permutaciones de  $\{1, 2, 3, 4, 5, 6\}$ . Entonces,

$$(1, 4, 5, 6)(2, 1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$$

y

$$(2, 1, 5)(1, 4, 5, 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}.$$

Ninguna de estas dos permutaciones es un ciclo. ■

En una colección de ciclos éstos son ajenos cuando ningún elemento de  $A$  aparece en las notaciones de dos ciclos diferentes de la colección; esto es, si dos ciclos diferentes de la colección no mueven a ningún elemento de  $A$ . En términos de transformaciones, los ciclos serán ajenos si para todos los ciclos de la colección, excepto a lo más un ciclo, todo elemento de  $A$  va a dar a él mismo.

Hay que convenir en que cualquier ciclo de longitud 1 representa la permutación identidad.

Se demostrará que cualquier permutación de un conjunto finito es producto de ciclos ajenos. La demostración será constructiva, es decir, los pasos de la demostración pueden emplearse, dada una permutación, para encontrar su representación como producto de ciclos ajenos. Nos parece que se aprende más de esta demostración que de un argumento inductivo elegante y formal. Ilustraremos la técnica con un ejemplo.

**Ejemplo 5.3** Considerérese la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}.$$

Escribáse como producto de ciclos ajenos. En primer lugar, el 1 se mueve al 6 y el 6 al 1, produciendo el ciclo  $(1, 6)$ . A continuación el 2 se mueve al 5, que a su vez se mueve al 3, el cual se mueve al 2, o  $(2, 5, 3)$ . Esto abarca todos los elementos excepto el 4, que permanece fijo. Así,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3).$$

Es claro que la multiplicación de ciclos *ajenos* es commutativa, así que no es importante el orden de los factores  $(1, 6)$  y  $(2, 5, 3)$ . ■

**Teorema 5.1** *Cada permutación  $\sigma$  de un conjunto finito  $A$  es producto de ciclos ajenos.*

**Demostración** No se pierde generalidad al suponer que  $A = \{1, 2, 3, \dots, n\}$ . Consideréense los elementos

$$1, 1\sigma, 1\sigma^2, 1\sigma^3, \dots$$

Como  $A$  es finito, no pueden ser distintos todos estos elementos. Sea  $1\sigma^r$  el primer término en la sucesión que se repita. Entonces,  $1\sigma^r = 1$  porque si  $1\sigma^r = 1\sigma^s$  con  $0 < s < r$ , tendríamos  $1\sigma^{r-s} = 1$  con  $r - s < r$  contradiciendo la selección de  $r$ . Sea

$$\tau_1 = (1, 1\sigma, 1\sigma^2, \dots, 1\sigma^{r-1}).$$

Vemos que  $\tau_1$ , tiene el mismo efecto que  $\sigma$  en todos los elementos de  $A$  que aparecen en esta notación cíclica para  $\tau_1$ .

Sea  $i$  el primer elemento de  $A$  que no aparece en esta notación cíclica para  $\tau_1$ . Se repite el argumento anterior con la sucesión

$$i, i\sigma, i\sigma^2, \dots,$$

y obtenemos un ciclo  $\tau_2$ . Ahora bien,  $\tau_2$  y  $\tau_1$  son ajenos ya que si tuvieran en común algún elemento  $j$  de  $A$ , serían idénticos, pues cada ciclo podría construirse mediante aplicaciones repetidas de la permutación  $\sigma$  comenzando en  $j$ .

Para continuar, se elegirá ahora el primer elemento de  $A$  que no aparece en las notaciones cíclicas de  $\tau_1$  ni de  $\tau_2$ , y se construirá  $\tau_3$ , y así sucesivamente. Como  $A$  es finito, este proceso debe terminar en alguna  $\tau_m$ . Es claro que el producto

$$\tau_1 \tau_2 \cdots \tau_m$$

tiene el mismo efecto en cada elemento de  $A$  que  $\sigma$ ; así,

$$\sigma = \tau_1 \tau_2 \cdots \tau_m. \blacksquare$$

Será posible convencirse fácilmente de que la representación de una permutación como producto de ciclos ajenos, ninguno de los cuales es la permutación identidad, es única, salvo el orden de los factores.

## 5.2 PERMUTACIONES PARES E IMPARES

**Definición** Un ciclo de longitud 2 es una *transposición*.

De este modo, una transposición deja fijos todos los elementos excepto dos y lleva a cada uno de éstos en el otro. Un cálculo muestra que

$$(a_1, a_2, \dots, a_n) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_n).$$

Por tanto, cualquier ciclo es producto de transposiciones. Tenemos, entonces, el siguiente corolario al teorema 5.1.

**Corolario** Cualquier permutación de un conjunto finito de al menos dos elementos es un producto de transposiciones.

De manera intuitiva, este corolario afirma que cualquier rearrreglo de  $n$  objetos se puede lograr intercambiando sucesivamente pares de ellos.

**Ejemplo 5.4** Al continuar las observaciones previas al corolario, vemos que  $(1, 6)(2, 5, 3)$  es el producto  $(1, 6)(2, 5)(2, 3)$  de transposiciones. ■

Hemos visto que toda permutación de un conjunto finito que tenga al menos 2 elementos, es producto de transposiciones. Las transposiciones pueden no ser ajenas y no es única esta representación de la permutación. Por ejemplo, siempre es posible insertar al principio la transposición  $(a, b)$  dos veces, pues  $(a, b)(a, b)$  es la permutación identidad. Lo cierto es que el número de transposiciones que se usan para representar una permutación dada debe ser siempre par o siempre impar. Este es un hecho importante y la demostración usual, que puede encontrarse en la primera edición de este libro, implica una construcción bastante artificial. En 1971, William I. Miller publicó una demostración que nos parece mejor y que damos aquí<sup>1</sup>.

**Teorema 5.2** *Ninguna permutación de un conjunto finito puede expresarse como un producto de un número par de transposiciones y como un producto de un número impar de transposiciones.*

**Demonstración** No se pierde generalidad al considerar el conjunto  $A = \{1, 2, \dots, n\}$  y suponer que  $n \geq 2$ , de manera que existan las transposiciones.

Estudiemos primero el caso especial de la permutación identidad  $\iota$ . Desde luego,  $\iota$  puede expresarse como un producto de un número par de transposiciones, digamos  $\iota = (1, 2)(1, 2)$ . Debemos mostrar que si

$$\iota = \tau_1 \tau_2 \cdots \tau_k \quad [5.1]$$

donde cada  $\tau_i$  es una transposición, entonces  $k$  debe ser par. Sea  $m$  cualquier entero que aparezca en alguna de las transposiciones en la ecuación [5.1] y sea  $\tau_j$  la primera transposición, contando de izquierda a derecha, en la cual aparece  $m$ . No podemos tener  $j = k$  pues, de ser así,  $\iota$  no hubiera dejado fijo a  $m$ . Ahora bien,  $\tau_j \tau_{j+1}$  debe tener la forma de alguno de los lados izquierdos de las siguientes identidades fáciles de verificar

$$\begin{aligned} (m, x)(m, x) &= \iota \\ (m, x)(m, y) &= (x, y)(m, x) \\ (m, x)(y, z) &= (y, z)(m, x) \\ (m, x)(x, y) &= (x, y)(m, y) \end{aligned} \quad [5.2]$$

Si sustituimos la identidad correcta en la ecuación [5.2], en lugar de  $\tau_j \tau_{j+1}$  en la ecuación [5.1], sucede que reducimos en 2 el número  $k$  de transposiciones o trasladamos la primera aparición de  $m$  un lugar a la derecha. Repetimos este procedimiento hasta eliminar  $m$  de la expresión de la ecuación [5.1]; hay que recordar que  $m$  no puede aparecer por primera vez en la transposición final, así que en algún momento debe aparecer la situación de la primera identidad en la ecuación [5.2] para eliminar a  $m$  por completo. A continuación elegimos otro

<sup>1</sup> William I. Miller, «Even and Odd Permutations», *Mathematics Associations of Two-Year Colleges Journal* 5(1971):32.

entero en  $A$  que aparece en la ecuación [5.1] reducida y lo eliminamos de la ecuación [5.1] mediante un proceso similar y continuamos hasta que el lado derecho de la ecuación [5.1] se reduzca a la sucesión  $n \cdots i$ . Como al sustituir una identidad de la ecuación [5.2] el número  $k$  permanece igual o se reduce en 2, vemos que  $k$  debe haber sido par.

Es fácil probar el teorema partiendo del caso especial para  $i$ . Supóngase que

$$\sigma = \tau_1 \tau_2 \cdots \tau_r = \tau'_1 \tau'_2 \cdots \tau'_s$$

Como cada transposición es su propia inversa, obtenemos

$$i = \sigma \sigma^{-1} = \tau_1 \tau_2 \cdots \tau_r (\tau'_1 \tau'_2 \cdots \tau'_s)^{-1} = \tau_1 \tau_2 \cdots \tau_r \tau'_s \cdots \tau'_2 \tau'_1.$$

Mostramos, en este caso particular, que  $r + s$  es un número par, de modo que  $r$  y  $s$  son ambos números pares o ambos son números impares. ■

**Definición** Una permutación de un conjunto finito es *par* o *impar* de acuerdo con que pueda expresarse como el producto de un número par de transposiciones o como el producto de un número impar de transposiciones, respectivamente.

### 5.3 GRUPOS ALTERNANTES

Afirmamos que para  $n \geq 2$ , el número de permutaciones pares en  $S_n$  es igual al número de permutaciones impares; es decir,  $S_n$  se descompone equitativamente y ambos números son  $(n!)/2$ . Para mostrarlo, sea  $A_n$  el conjunto de permutaciones pares en  $S_n$  y sea  $B_n$  el conjunto de permutaciones impares para  $n \geq 2$ . A continuación definiremos una función uno a uno de  $A_n$  sobre  $B_n$ . Esto es precisamente lo que se necesita para mostrar que  $A_n$  y  $B_n$  tienen el mismo número de elementos.

Sea  $\tau$  cualquier transposición fija en  $S_n$  que existe porque  $n \geq 2$ . Podemos suponer que  $\tau = (1, 2)$ . Definimos la función

$$\lambda_\tau: A_n \rightarrow B_n$$

mediante

$$\sigma \lambda_\tau = \tau \sigma,$$

esto es,  $\sigma \in A_n$  va a dar a  $(1, 2)\sigma$  bajo  $\lambda_\tau$ . Obsérvese que como  $\sigma$  es par, la permutación  $(1, 2)\sigma$  aparece como el producto de  $(1 + \text{número par})$  o sea un número impar de transposiciones, así que, en efecto,  $(1, 2)\sigma$  está en  $B_n$ . Si para  $\sigma$  y  $\mu \in A_n$  sucede que  $\sigma \lambda_\tau = \mu \lambda_\tau$ , entonces

$$(1, 2)\sigma = (1, 2)\mu,$$

y como  $S_n$  es grupo, tenemos  $\sigma = \mu$ . Así,  $\lambda_i$  es una función uno a uno. Por último,

$$\tau = (1, 2) = \tau^{-1},$$

así que si  $\rho \in B_n$ , entonces

$$\tau^{-1}\rho \in A_{\mathfrak{p}}$$

v

$$(\tau^{-1}\rho)\lambda_\tau = \tau(\tau^{-1}\rho) = \rho.$$

Por consiguiente,  $\lambda_i$  es sobre  $B_n$ . De aquí que el número de elementos en  $A_n$  es el mismo que el número de elementos en  $B_n$ , puesto que existe una correspondencia biunívoca entre los elementos de ambos conjuntos.

Nótese que el producto de dos permutaciones pares es par. También, como  $n \geq 2$ ,  $A$  tiene dos elementos  $a$  y  $b$ , y  $\iota = (a, b)(a, b)$  es una permutación par. Por último, nótese que si expresamos  $\sigma$  como producto de transposiciones, el producto de las mismas transposiciones tomadas en el orden opuesto es  $\sigma^{-1}$ . Por tanto, si  $\sigma$  es una permutación par,  $\sigma^{-1}$  también debe ser par. Haciendo referencia al teorema 3.1, se ve que hemos probado:

**Teorema 5.3** Si  $n \geq 2$ , la colección de todas las permutaciones pares de  $\{1, 2, 3, \dots, n\}$  forma un subgrupo de orden  $n!/2$  del grupo simétrico  $S_n$ .

**Definición** El subgrupo de  $S_n$  que consta de las permutaciones pares de  $n$  letras es el grupo alternante  $A_n$  de  $n$  letras.

Tanto  $S_n$  como  $A_n$  son grupos muy importantes. Ya mencionamos, sin demostración, que cada grupo finito es estructuralmente idéntico a algún subgrupo de  $S_n$  para alguna  $n$ . La importancia de  $A_n$  aparecerá más adelante.

## Ejercicios

5.1 Los ciclos siguientes son permutaciones de  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ . Calcúlense los productos que se indican.

- a)  $(1, 4, 5)(7, 8)(2, 5, 7)$       b)  $(1, 3, 2, 7)(4, 8, 6)$   
 c)  $(1, 2)(4, 7, 8)(2, 1)(7, 2, 8, 1, 5)$

5.2 Expréñese cada una de las siguientes permutaciones de  $\{1, 2, 3, 4, 5, 6, 7, 8\}$  como producto de ciclos ajenos y después como producto de transposiciones.

- $$\text{a) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix} \quad \text{b) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$$

$$\text{c) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$$

15.3 Pruébese lo siguiente acerca de  $S_n$  si  $n \geq 2$ .

- Toda permutación en  $S_n$  puede escribirse como producto de a lo más  $n - 1$  transposiciones.
- Toda permutación en  $S_n$  que no es un ciclo puede escribirse como producto de a lo más  $n - 2$  transposiciones.
- Toda permutación impar en  $S_n$  puede escribirse como producto de  $2n + 3$  transposiciones y toda permutación par como producto de  $2n + 8$  transposiciones.

5.4 ¿Cuáles de las permutaciones en  $S_3$  del ejemplo 4.1 son permutaciones pares? Obténgase la tabla para el grupo alternante  $A_3$ .

5.5 Un elemento  $a$  de un grupo  $G$  con identidad  $e$  tiene orden  $r > 0$  si  $a^r = e$  y ninguna potencia positiva menor de  $a$  es la identidad. Considérese el grupo  $S_8$  del ejercicio 5.1.

- ¿Cuál es el orden del ciclo  $(1, 4, 5, 7)$ ?
- Enúnciese un teorema sugerido por la parte a).
- ¿Cuál es el orden de  $\sigma = (4, 5)(2, 3, 7)$  y cuál el de  $\tau = (1, 4)(3, 5, 7, 8)$ ?
- Encuéntrese el orden de cada una de las permutaciones dadas en el ejercicio 5.2 tomando en cuenta su descomposición en producto de ciclos ajenos.
- Enúnciese un teorema sugerido por las partes c) y d). [Sugerencia: las palabras importantes que buscan son *mínimo común múltiplo*.]

5.6 ¿Falso o verdadero?

- a) Toda permutación es un ciclo.
- b) Todo ciclo es una permutación.
- c) Se pudieron haber dado las definiciones de permutaciones pares e impares antes del teorema 5.2.
- d) Cualquier subgrupo no trivial de  $S_9$  que contenga algunas permutaciones impares, contiene una transposición.
- e)  $A_5$  tiene 120 elementos.
- f)  $S_n$  no es cíclico para ninguna  $n \geq 1$ .
- g)  $A_3$  es un grupo commutativo.
- h)  $S_7$  es isomorfo al subgrupo de todos los elementos de  $S_8$  que dejan fijo al número 8.
- i)  $S_7$  es isomorfo al subgrupo de todos los elementos de  $S_8$  que dejan fijo al número 5.
- j) Las permutaciones impares de  $S_8$  forman un subgrupo de  $S_8$ .

5.7 Muéstrese que para todo subgrupo  $H$  de  $S_n$  para  $n \geq 2$ , todas las permutaciones en  $H$  son pares o exactamente la mitad son pares.

5.8 Sea  $\sigma$  una permutación de un conjunto  $A$ . Diremos que « $\sigma$  mueve  $a \in A$ » si  $a\sigma \neq a$ . Si  $A$  es un conjunto finito, ¿cuántos elementos mueve un ciclo  $\sigma \in S_A$  de longitud  $n$ ?

5.9 Sea  $A$  un conjunto infinito. Sea  $H$  el conjunto de todas las  $\sigma \in S_A$  que mueven sólo un número finito de elementos de  $A$  (véase ejercicio 5.8). Muéstrese que  $H$  es un subgrupo de  $S_A$ .

5.10 Sea  $A$  un conjunto infinito. Sea  $K$  el conjunto de todas las  $\sigma \in S_A$  que mueven a lo más 50 elementos de  $A$  (véase ejercicio 5.8). ¿Es  $K$  un subgrupo de  $S_A$ ? ¿Por qué?

## 56 PERMUTACIONES II

- 5.11 Demuéstrese de manera más elegante el teorema 5.1; empleese un argumento por inducción sobre el número de elementos movidos por  $\sigma$  (véase ejercicio 5.8).
- 5.12 Considérese  $S_n$  para una  $n \geq 2$  fija y sea  $\sigma$  una permutación impar fija. Muéstrese que toda permutación impar en  $S_n$  es producto de  $\sigma$  y alguna permutación en  $A_n$ .
- 5.13 Demuéstrese que si  $\sigma$  es un ciclo, entonces  $\sigma^2$  es un ciclo, siempre que la longitud de  $\sigma$  sea un entero impar.
- 5.14 Siguiendo la línea de pensamiento iniciada en el ejercicio 5.13, complétense lo siguiente con una condición que incluya  $n$  y  $r$  de tal manera que el enunciado resultante sea un teorema
- Si  $\sigma$  es un ciclo de longitud  $n$ , entonces  $\sigma^r$  también es un ciclo si y sólo si ...
- 5.15 Sea  $G$  un grupo y sea  $a$  un elemento fijo de  $G$ , muéstrese que la transformación  $\lambda_a : G \rightarrow G$  dada por  $g\lambda_a = ag$  para  $g \in G$ , es una permutación del conjunto  $G$ .
- 5.16 Con referencia al ejercicio 5.15, muéstrese que  $H = \{\lambda_a | a \in G\}$  es un subgrupo de  $S_G$ ; el grupo de todas las permutaciones de  $G$ .
- 5.17 Con referencia al ejercicio 4.16, muéstrese que  $H$  del ejercicio 5.16 es transitivo en el conjunto  $G$ . [Sugerencia: esto es un corolario inmediato de uno de los teoremas del capítulo 2.]

## 6

# Grupos cíclicos

## 6.1 PROPIEDADES ELEMENTALES

Recuérdese lo siguiente del capítulo 3:

Si  $G$  es un grupo y  $a \in G$ , entonces

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

es un subgrupo de  $G$  (Teorema 3.2). Este grupo es el **subgrupo cíclico de  $G$  generado por  $a$** . Además, dado un grupo  $G$  y un elemento  $a \in G$ , si

$$G = \{a^n \mid n \in \mathbb{Z}\},$$

entonces  $a$  es un **generador de  $G$**  y el grupo  $G = \langle a \rangle$  es **cíclico**.

El propósito de esta sección es clasificar todos los grupos cíclicos y todos los subgrupos de los grupos cíclicos.

**Teorema 6.1** *Todo grupo cíclico es abeliano.*

**Demostración** Sea  $G$  un grupo cíclico y sea  $a$  un generador de  $G$  tal que

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Si  $g_1$  y  $g_2$  son dos elementos cualesquiera de  $G$ , existen enteros  $r$  y  $s$  tales que  $g_1 = a^r$  y  $g_2 = a^s$ . Entonces,

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1,$$

de modo que  $G$  es abeliano. ■

Seguiremos usando la notación multiplicativa para nuestro trabajo general acerca de grupos cíclicos, a pesar de saber que son abelianos.

Existe un recíproco débil, pero muy importante, del teorema 6.1 que discutiremos con detalle más adelante. A saber, es posible mostrar que todo grupo abeliano «suficientemente pequeño» puede construirse a partir de grupos cíclicos, de una cierta manera. Por tanto, los grupos cíclicos son fundamentales en el estudio de los grupos abelianos. Los grupos cíclicos son una especie de tipos elementales de grupos abelianos. Podría esperarse que una parte de un tipo elemental sea de nuevo un tipo elemental. El siguiente teorema muestra que, en efecto, así sucede. En primer lugar daremos un lema aparentemente trivial, pero muy importante, de la teoría de los números.

**Lema 6.1 (Algoritmo de la división para  $\mathbb{Z}$ )** Si  $m$  es un entero positivo y  $n$  es cualquier entero, entonces existen enteros únicos  $q$  y  $r$  tales que

$$n = mq + r \quad y \quad 0 \leq r < m.$$

**Demostración** Daremos una explicación diagramática intuitiva con base en la figura 6.1. Sobre el eje  $x$  real usado en geometría analítica, se marcan los múltiplos de  $m$  y la posición de  $n$ . Ahora bien,  $n$  caerá en un múltiplo  $qm$  de  $m$  y se puede tomar  $r$  igual a 0, o  $n$  caerá entre dos múltiplos de  $m$ . Si éste es el caso, sea  $qm$  el primer múltiplo de  $m$  a la izquierda de  $n$ . Entonces,  $r$  es como se muestra en la figura 6.1. Nótese que  $0 \leq r < m$ . Después de pensarla un poco, se verá que la unicidad de  $q$  y de  $r$  es clara a partir de los diagramas. ■

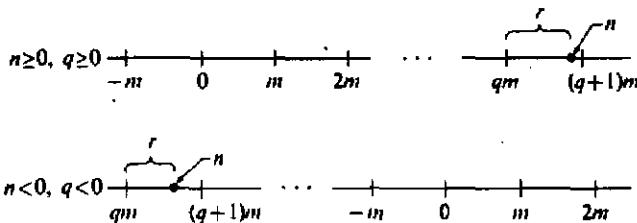


Figura 6.1

**Teorema 6.2** Un subgrupo de un grupo cíclico es cíclico.

**Demostración** Sea  $G$  un grupo cíclico generado por  $a$  y sea  $H$  un subgrupo de  $G$ . Si  $H = \{e\}$ , entonces  $H = \langle e \rangle$  es cíclico. Si  $H \neq \{e\}$ , entonces  $a^n \in H$  para alguna  $n \in \mathbb{Z}^+$ . Sea  $m \in \mathbb{Z}^+$  minimal, tal que  $a^m \in H$ .

Afirmamos que  $c = a^m$  genera  $H$ , esto es,

$$H = \langle a^m \rangle = \langle c \rangle.$$

Debemos mostrar que toda  $b \in H$  es una potencia de  $c$ . Como  $b \in H$  y  $H \leq G$ ,  $b = a^n$  para alguna  $n$ . Encuéntrense  $q$  y  $r$  tales que

$$n = mq + r \quad \text{para } 0 \leq r < m$$

mediante el lema 6.1. Entonces,

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

y

$$a^r = (a^m)^{-q} a^r.$$

Ahora, como  $a^r \in H$ ,  $a^m \in H$  y  $H$  es un grupo, tanto  $(a^m)^{-q}$  como  $a^r$  están en  $H$ . Así,

$$(a^m)^{-q} a^r \in H, \quad \text{esto es } a^r \in H.$$

Ya que  $m$  fue el menor entero positivo tal que  $a^m \in H$  y  $0 \leq r < m$ , debemos tener  $r = 0$ . Por tanto,  $n = qm$  y

$$b = a^n = (a^m)^q = c^q,$$

de modo que  $b$  es una potencia de  $c$ . ■

Por alguna razón, suele pedirse a los estudiantes en un examen de este curso, en el examen oral para la maestría, o en otros exámenes, que demuestren el teorema 6.2. Esto es algo fácil de hacer, pero sirve para averiguar si el estudiante es capaz de entender y construir demostraciones. En primer lugar, nótese que el teorema trata de grupos cíclicos, acerca de los cuales no hemos probado, hasta ahora, prácticamente nada, por tanto, *debe usarse la definición* de grupo cíclico. Es decir, hay que mostrar que un subgrupo  $H$  de un grupo cíclico  $G$  es cíclico. *Debe* tenerse en cuenta que  $G$  cíclico significa que existe  $a \in G$  tal que todo elemento de  $G$  es de forma  $a^n$  para  $n \in \mathbb{Z}$  y que, del aire, hay que sacar un elemento  $c$  de  $H$  que haga lo mismo en  $H$ . *Todo esto proviene sólo de la definición de grupo cíclico.* Lo ingenioso consiste en definir  $c$ . Sin embargo, se trata de una selección natural, ya que es el único elemento de  $H$  que podemos expresar en términos de  $a$ . Después hay que mostrar que  $c$  sirve, esto es, que  $c$  genera  $H$ .

Como se observó en los ejemplos 3.4 y 3.5,  $\mathbb{Z}$  bajo la suma es cíclico y para un entero positivo  $n$ , el conjunto  $n\mathbb{Z}$  de todos los múltiplos de  $n$  es un subgrupo de  $\mathbb{Z}$  bajo la suma; es el subgrupo cíclico generado por  $n$ . El teorema 6.2 muestra que estos subgrupos cíclicos son los únicos subgrupos de  $\mathbb{Z}$  bajo la suma. Se enuncia esto como corolario.

**Corolario** *Los subgrupos de  $\mathbb{Z}$  bajo la suma, son precisamente los grupos  $n\mathbb{Z}$  bajo la suma para  $n \in \mathbb{Z}$ .*

## 6.2 CLASIFICACION DE GRUPOS CICLICOS

Sea  $G$  un grupo ciclico con generador  $a$ . Consideremos dos casos.

**CASO I**  $G$  tiene un número infinito de elementos, esto es, el orden de  $G$  es infinito. En este caso afirmamos que dos exponentes distintos  $h$  y  $k$  no pueden dar elementos iguales  $a^h$  y  $a^k$  de  $G$ . Supóngase que  $a^h = a^k$  y que, digamos,  $h > k$ . Entonces,

$$a^h a^{-k} = a^{h-k} = e,$$

la identidad y  $h - k > 0$ . Sea  $m$  el menor entero positivo tal que  $a^m = e$  (nótese la analogía con la construcción en la demostración del teorema 6.2). Afirmamos que  $G$  tendría entonces únicamente los distintos elementos  $e, a, a^2, \dots, a^{m-1}$ . Sea  $a^r \in G$ ; encuéntrense  $q$  y  $r$  tales que

$$n = mq + r \quad \text{para } 0 \leq r < m$$

por el lema 6.1. Entonces,

$$a^n = a^{mq+r} = (a^m)^q a^r = e^q a^r = a^r$$

para  $0 \leq r < m$ . Esto significaría que  $G$  es finito, contradiciendo la hipótesis del caso I. *Por tanto, todas las potencias de  $a$  son distintas.*

Supóngase que  $G'$  es otro grupo ciclico infinito con generador  $b$ . Es claro que si se cambia el nombre de  $b'$  por el de  $a'$  puede parecer que  $G'$  es exactamente igual a  $G$ , es decir, los grupos son isomorfos. Lo anterior se hará de nuevo, con sumo cuidado, en el siguiente capítulo. *Por consiguiente, todos los grupos cíclicos infinitos son iguales excepto, quizás, por los nombres de los elementos y las operaciones.* Tomaremos  $\mathbb{Z}$  con la operación de suma como el prototipo de cualquier grupo ciclico infinito. De ahora en adelante, en la parte I, «el grupo  $\mathbb{Z}$ » será siempre «el grupo  $\mathbb{Z}$  bajo la suma».

**Ejemplo 6.1** Podrá parecer extraño que  $\mathbb{Z}$  y  $3\mathbb{Z}$ , ambos grupos cíclicos infinitos bajo la suma, sean estructuralmente idénticos a pesar de que  $3\mathbb{Z} < \mathbb{Z}$ . Podría decirse que  $1 \in \mathbb{Z}$  pero  $1 \notin 3\mathbb{Z}$ , así que ¿cómo pueden ser estructuralmente iguales? Los nombres no importan, y si al 1 lo nombramos 3, al 2 lo nombramos 6 y en general al  $n$  lo nombramos  $3n$ , habremos convertido  $\mathbb{Z}$  en  $3\mathbb{Z}$  como grupo aditivo. ■

**CASO II**  $G$  tiene orden finito. En este caso, no todas las potencias positivas de un generador  $a$  de  $G$  son distintas, así que para alguna  $h$  y  $k$  tendremos  $a^h = a^k$ . Siguiendo la argumentación del caso I, existe un entero  $m$  tal que  $a^m = e$  y ninguna potencia positiva menor de  $a$  es  $e$ . Entonces, el grupo  $G$  consta de los distintos elementos  $e, a, a^2, \dots, a^{m-1}$ .

Como suele usarse  $n$  para el orden de un grupo ciclico finito en general, cambiaremos la notación para lo siguiente, estableciendo  $m = n$ .

**Ejemplo 6.2** Es agradable imaginar los elementos  $e = a^0, a^1, a^2, \dots, a^{n-1}$  de un grupo cíclico de orden  $n$ , distribuidos equitativamente sobre una circunferencia (véase la figura 6.2). El elemento  $e = a^0$  está localizado en la parte inferior y el elemento  $a^k$  está localizado a  $k$  de estas unidades iguales, medidas en sentido contrario al que giran las manecillas del reloj, desde  $e = a^0$ . Para multiplicar  $a^k$  y  $a^t$  mediante este diagrama, se comienza desde  $a^k$  y se avanza, en el sentido contrario al que giran las manecillas del reloj,  $t$  unidades más. Para ver en términos aritméticos dónde se termina, encuéntrense  $q$  y  $r$  tales que

$$h + k = nq + r \quad \text{para } 0 \leq r < n.$$

El término  $nq$  nos lleva  $q$  veces alrededor del círculo hasta llegar a  $a^t$ . ■

**Definición** Sea  $n$  un entero positivo fijo y sean  $h$  y  $k$  enteros cualesquiera. El número  $r$  tal que

$$h + k = nq + r \quad \text{para } 0 \leq r < n$$

es la *suma de  $h$  y  $k$  módulo  $n$* .

**Teorema 6.3** El conjunto  $\{0, 1, 2, \dots, n - 1\}$  es un grupo cíclico  $Z_n$  de elementos bajo la suma módulo  $n$ .

En el capítulo 0 se analizó la congruencia módulo  $n$ ; vemos que si  $h + k = r$  en  $Z_n$ , entonces, para la suma en  $Z$ , tenemos  $h + k \equiv r \pmod{n}$ .

La demostración del teorema 6.3 es fácil y servirá para practicar el algoritmo de la división. (Véase el ejercicio 6.8.) Verifiquense mentalmente  $G_1$ ,  $G_2$  y  $G_3$ . Recuérdese el diagrama de la figura 6.3 como se explicó en el ejemplo 6.2. Esto permitirá renombrar el elemento  $a^k$  del ejemplo 6.2 con  $h$ .

Por tanto, hay un grupo cíclico de orden  $n$  para cada entero positivo  $n$ . En la parte I,  $Z_n$  será el grupo dado por el teorema 6.3. Al igual que en el caso infinito, es claro que si  $G$  y  $G'$  son dos grupos cíclicos de  $n$  elementos cada uno, con generadores  $a$  y  $b$ , respectivamente, entonces, al cambiar el nombre de  $b'$  por  $a'$ ,  $G'$  se verá exactamente como  $G$ . Esto es, *cualesquiera dos grupos cíclicos del mismo orden finito son isomorfos*.

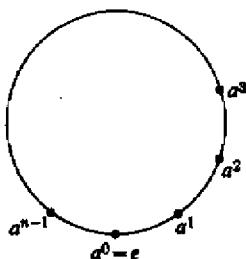


Figura 6.2

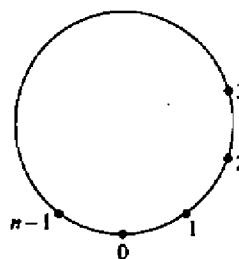


Figura 6.3

### 6.3 SUBGRUPOS DE GRUPOS CICLICOS FINITOS

Hemos terminado la clasificación de grupos cíclicos y nos dedicaremos ahora a los subgrupos. El corolario del teorema 6.2 proporciona información completa acerca de los subgrupos de los grupos cíclicos infinitos. A continuación daremos el teorema básico con respecto a los generadores de subgrupos para los grupos cíclicos finitos.

**Teorema 6.4** *Sea  $G$  un grupo cíclico con  $n$  elementos generado por  $a$ . Sea  $b \in G$  y sea  $b = a^d$ . Entonces,  $b$  genera un subgrupo cíclico  $H$  de  $G$  con  $n/d$  elementos donde  $d$  es el máximo común divisor (abreviado mcd) de  $n$  y  $s$ .*

**Demostración** Se sabe, a partir del teorema 3.2, que  $b$  genera un subgrupo cíclico  $H$  de  $G$ . Sólo falta mostrar que  $H$  tiene  $n/d$  elementos. Siguiendo la discusión en el caso I anterior, podemos observar que  $H$  tiene tantos elementos como la menor potencia de  $b$  que dé la identidad. Ahora bien,  $b = a^d$  y  $b^m = e$  si y sólo si  $(a^d)^m = a^{dm} = e$  o si y sólo si  $n$  divide a  $ms$ . ¿Cuál es el menor valor de  $m$  tal que  $n$  divide a  $ms$ ? Si  $d$  es el mayor número que divide  $n$  y  $s$ , entonces, en la expresión  $n = d(n/d)$ , el factor  $d$  de  $n$  dividirá al factor  $s$  de  $ms$ . No se absorben en  $s$  factores primos de  $n/d$  además del factor  $d$ , ya que escogimos  $d$  como el mayor entero que divide tanto  $n$  como  $s$ . Así,  $n/d$  se absorbe en  $m$  y la menor de dichas  $m$  es  $m = (n/d)$ . ■

**Ejemplo 6.3** Considérese  $\mathbb{Z}_{12}$ , con generador  $a = 1$ . Como el máximo común divisor (mcd) de 3 y 12 es 3,  $3 = 3 \cdot 1$  genera un subgrupo de  $\frac{12}{3} = 4$  elementos, a saber

$$\langle 3 \rangle = \{0, 3, 6, 9\}.$$

Como el mod de 8 y 12 es 4, 8 genera un subgrupo de  $\frac{12}{4} = 3$  elementos, a saber

$$\langle 8 \rangle = \{0, 4, 8\}.$$

Puesto que el mod de 12 y 5 es 1, 5 genera un subgrupo de  $\frac{12}{1} = 12$  elementos, esto es, 5 es un generador de todo el grupo  $\mathbb{Z}_{12}$ . ■

El siguiente corolario es resultado inmediato del teorema.

**Corolario** *Si  $a$  es un generador de un grupo cíclico finito  $G$  de orden  $n$ , entonces, los otros generadores de  $G$  son los elementos de la forma  $a^r$ , donde  $r$  y  $n$  son primos relativos, esto es, donde el máximo común divisor de  $r$  y  $n$  es 1.*

**Ejemplo 6.4** Encuéntrense todos los subgrupos de  $\mathbb{Z}_{18}$  y elabórese el correspondiente diagrama reticular. Todos los subgrupos son cíclicos. Por el corolario del teorema 6.4, los elementos 1, 5, 7, 11, 13 y 17 son todos generadores de  $\mathbb{Z}_{18}$ . Comenzando con 2,

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$$

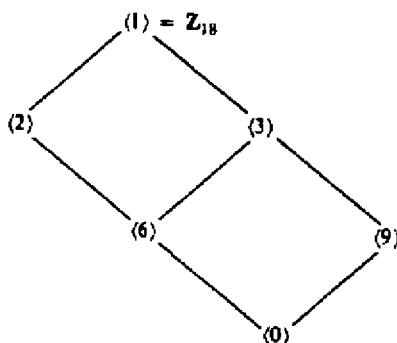


Fig. 6.4 Diagrama reticular para  $\mathbb{Z}_{18}$ .

es de orden 9 y tiene como generadores a los elementos de la forma  $2h$ , donde  $h$  es primo relativo con 9, a saber,  $h = 1, 2, 4, 5, 7$  y  $8$ , así que  $2h = 2, 4, 8, 10, 14$  y  $16$ . El elemento 6 de  $\langle 2 \rangle$  genera  $\{0, 6, 12\}$  y 12 es también generador de este subgrupo.

Hasta ahora hemos encontrado todos los subgrupos generados por  $0, 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14$  y  $16$ . Nos faltan por considerar  $3, 9$  y  $15$ .

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\},$$

el 15 también genera este grupo de orden 6 pues  $15 = 5 \cdot 3$  y el mcd de 5 y 6 es 1. Por último,

$$\langle 9 \rangle = \{0, 9\}.$$

El diagrama reticular de estos subgrupos de  $\mathbb{Z}_{18}$  se da en la figura 6.4.

Este ejemplo es muy fácil; quizás al escribirlo con tan horrible minuciosidad haya parecido difícil. Los ejercicios ayudarán a desarrollar esta habilidad. ■

## Ejercicios

---

- 6.1 Encuéntrese el número de generadores de los grupos cíclicos de órdenes 6, 8, 12 y 60.
- 6.2 Muéstrese que un grupo que tenga sólo un número finito de subgrupos debe ser un grupo finito.
- 6.3 Encuéntrese el número de elementos en cada uno de los grupos cíclicos indicados.
- El subgrupo cíclico de  $\mathbb{Z}_{30}$  generado por el 25.
  - El subgrupo cíclico de  $\mathbb{Z}_{42}$  generado por 30.
  - El subgrupo cíclico  $\langle i \rangle$  del grupo  $C^*$  de números complejos distintos de cero, bajo la multiplicación.
  - El subgrupo cíclico del grupo  $C^*$  de la parte c) generado por  $(1 + i)/\sqrt{2}$ .
  - El subgrupo cíclico del grupo  $C^*$  de la parte c) generado por  $1 + i$ .

**6.4** Para cada uno de los siguientes grupos, encuéntrense todos los subgrupos y eláborese el diagrama reticular correspondiente

a)  $\mathbb{Z}_{12}$

b)  $\mathbb{Z}_{36}$

c)  $\mathbb{Z}_8$

**6.5** Encuéntrense todos los órdenes de los subgrupos de  $\mathbb{Z}_6$ ,  $\mathbb{Z}_8$ ,  $\mathbb{Z}_{12}$ ,  $\mathbb{Z}_{60}$  y  $\mathbb{Z}_{17}$ .

**6.6** ¿Falso o verdadero?

- a) Todo grupo cíclico es abeliano.
- b) Todo grupo abeliano es cíclico.
- c) Q bajo la suma es grupo cíclico.
- d) Todo elemento de todo grupo cíclico genera al grupo.
- e) Existe al menos un grupo no abeliano para cada orden finito  $> 0$ .
- f) Todo grupo de orden  $\leq 4$  es cíclico.
- g) Todos los generadores de  $\mathbb{Z}_{20}$  son números primos.
- h)  $S_3$  es un grupo cíclico.
- i)  $A_3$  es un grupo cíclico.
- j) Todo grupo cíclico de orden  $> 2$  tiene al menos dos generadores distintos.

---

**6.7** Muéstrese, mediante un contraejemplo, que el siguiente «recíproco» del teorema 6.2 no es un teorema: «Si un grupo  $G$  es tal que todo subgrupo propio es cíclico, entonces  $G$  es cíclico».

**6.8** Sea  $+_n$  la suma módulo  $n$  en  $\mathbb{Z}_n = \{1, 2, 3, \dots, n\}$ . Pruébese que  $(\mathbb{Z}_n, +_n)$  es un grupo. [Sugerencia: la asociatividad es el único axioma no trivial. Empléese el algoritmo de la división y muéstrese que tanto  $r +_n (s +_n t)$  como  $(r +_n s) +_n t$ , son el residuo de  $r + s + t$  al dividirlo entre  $n$ .]

**6.9** Sea  $G$  un grupo, supóngase que  $a \in G$  genera un subgrupo cíclico de orden 2 y además es el único elemento con esa propiedad. Muéstrese que  $ax = xa$  para todas las  $x \in G$ . (Comentario: Quizá se haya observado que puede ser difícil encontrar una demostración en álgebra, aun cuando existan demostraciones fáciles. Por lo general, no se pueden dibujar «figuras» que ayuden a visualizar la demostración. A menudo se tiene que inventar el «truco» adecuado. Para encontrar los trucos adecuados hace falta experiencia, intuición y a veces sólo suerte. Uno de los principales algebraistas de este siglo observó alguna vez que la manera de hacer investigación en álgebra es pensar en algún truco y después encontrar un problema que se pueda resolver con ese truco, en lugar de tratar de encontrar el modo de resolver un problema específico. Bien, inténtese resolver este ejercicio; si se presentan dificultades, consultese el «truco» que está en la sección de respuestas.)

**6.10** Sea  $G = \langle a \rangle$  un grupo cíclico finito de orden  $n$ .

- a) Muéstrese que todo subgrupo  $H \leq G$  tiene la forma  $\langle a^m \rangle$ , donde  $m > 0$  es algún divisor de  $n$  y muéstrese que, para enteros positivos  $m$  y  $m'$  que dividan a  $n$ , tenemos  $\langle a^m \rangle = \langle a^{m'} \rangle$  si y sólo si  $m = m'$ .
- b) Sea  $D(n)$  el conjunto de los enteros positivos divisores de  $n$  y sea  $S(G)$  el conjunto de los subgrupos de  $G$ . Tradúzcase el resultado de la parte a) como un enunciado acerca de que cierta transformación de  $D(n)$  a  $S(G)$  es uno a uno y sobre.
- c) Muéstrese que si dos subgrupos del grupo cíclico finito  $G$  tienen el mismo orden, entonces son iguales. ¿Qué enteros son órdenes de los subgrupos de  $G$ ?
- d) Proporciónense un ejemplo para mostrar que para grupos finitos *no cíclicos*  $G$ , la conclusión de la parte c) no es necesariamente cierta.

- 6.11 Sean  $p$  y  $q$  números primos. Encuéntrese el número de generadores del grupo cíclico  $\mathbb{Z}_{pq}$ .
- 6.12 Sea  $p$  un número primo. Encuéntrese el número de generadores del grupo cíclico  $\mathbb{Z}_p$ , donde  $r$  es un entero  $\geq 1$ .
- 6.13 Muéstrese que en un grupo cíclico finito  $G$  de orden  $n$ , la ecuación  $x^m = e$  tiene exactamente  $m$  soluciones  $x$  en  $G$  para cada entero positivo  $m$  que divide a  $n$ .
- 6.14 Con respecto al ejercicio 6.13, ¿cuál es la situación si  $1 < m < n$  y  $m$  no divide a  $n$ ?
- 6.15 Muéstrese que  $\mathbb{Z}_p$  no tiene subgrupos propios si  $p$  es un número primo.
- 6.16 Sea  $G$  un grupo abeliano y sean  $H$  y  $K$  subgrupos cíclicos finitos con  $|H| = r$  y  $|K| = s$ .
- Muéstrese que si  $r$  y  $s$  son primos relativos, entonces  $G$  contiene un subgrupo cíclico de orden  $rs$ .
  - Generalizando la parte a), muéstrese que  $G$  contiene un subgrupo cíclico cuyo orden es el mínimo común múltiplo de  $r$  y  $s$ .

# Isomorfismo

## 7.1 DEFINICIÓN Y PROPIEDADES ELEMENTALES

Nos ocuparemos ahora de precisar, en términos matemáticos, la idea de que dos grupos  $G$  y  $G'$  son estructuralmente iguales o *isomorfos*. Hemos tratado de dar la idea de que los grupos  $G$  y  $G'$  son isomorfos, si son idénticos salvo por el nombre de los elementos y las operaciones. De este modo, podemos obtener  $G'$  a partir de  $G$  cambiando el nombre de un elemento  $x$  en  $G$  por el nombre de cierto elemento  $x'$  en  $G'$ . Esto es, a cada  $x \in G$  se le asigna una contraparte  $x' \in G'$ . En realidad, no es más que una función  $\phi$  con dominio  $G$ . Es claro que dos elementos diferentes  $x$  y  $y$  en  $G$  deben tener contrapartes diferentes  $x' = x\phi$  y  $y' = y\phi$  en  $G'$ , es decir, la función  $\phi$  debe ser uno a uno. Además, cada elemento de  $G'$  debe ser la contraparte de algún elemento de  $G$ , o sea que la función  $\phi$  debe ser sobre  $G'$ . Esto cambia el nombre de los elementos. Por último, si los grupos serán estructuralmente el mismo y si, por el momento, denotamos la operación del grupo de  $G$  por  $*$  y la de  $G'$  por  $*'$ , entonces la contraparte de  $x * y$  debería ser  $x' *' y'$ , o  $(x * y)\phi$  debería ser  $(x\phi) *' (y\phi)$ . Por lo común, se omiten las notaciones  $*$  y  $*'$  para las operaciones y se usa la notación multiplicativa, esto es,

$$(xy)\phi = (x\phi)(y\phi).$$

Nótese que la multiplicación  $xy$  del lado izquierdo en  $(xy)\phi = (x\phi)(y\phi)$  es la multiplicación en  $G$ , mientras que la multiplicación  $(x\phi)(y\phi)$  del lado derecho es la de  $G'$ . Reunimos estas ideas en una definición.

**Definición** Un *isomorfismo entre un grupo  $G$  y un grupo  $G'$*  es una función  $\phi$  uno a uno, que lleva a  $G$  sobre  $G'$  y tal que para todas las  $x$  y  $y$  en  $G$ ,

$$(xy)\phi = (x\phi)(y\phi).$$

Los grupos  $G$  y  $G'$  son *isomorfos*. La notación usual es  $G \simeq G'$ .

Probemos ahora un teorema que resulta muy obvio, si consideramos que un isomorfismo es un cambio de nombre de un grupo de modo que sea como otro. Desde luego, lo probaremos a partir de nuestra definición de isomorfismo.

**Teorema 7.1** Si  $\phi: G \rightarrow G'$  es un isomorfismo entre  $G$  y  $G'$  y  $e$  es la identidad de  $G$ , entonces  $e\phi$  es la identidad en  $G'$ . Además,

$$a^{-1}\phi = (a\phi)^{-1} \quad \text{para todas las } a \in G.$$

Para abreviar, un isomorfismo lleva la identidad a la identidad y los inversos a los inversos.

**Demuestra**ción Sea  $x' \in G'$ . Como  $\phi$  es sobre, existe  $x \in G$  tal que  $x\phi = x'$ . Entonces

$$x' = x\phi = (ex)\phi = (e\phi)(x\phi) = (e\phi)x'.$$

De manera análoga,

$$x' = x\phi = (xe)\phi = (x\phi)(e\phi) = x'(e\phi).$$

Así, para cada  $x' \in G'$  tenemos

$$(e\phi)x' = x' = x'(e\phi),$$

de modo que  $e\phi$  es la identidad de  $G'$ .

Tenemos además que para  $a \in G$

$$e\phi = (a^{-1}a)\phi = (a^{-1}\phi)(a\phi).$$

De manera análoga,

$$e\phi = (aa^{-1})\phi = (a\phi)(a^{-1}\phi).$$

Así,  $a^{-1}\phi = (a\phi)^{-1}$ . ■

## 7.2 COMO MOSTRAR QUE DOS GRUPOS SON ISOMORFOS

En el pasado, algunos alumnos del autor han tenido dificultades para comprender y emplear el concepto de isomorfismo; se utilizó ya en varias secciones antes de precisarlo, con la esperanza de que se comprendieran su importancia y su significado. En cuanto a su uso, daremos ahora un esbozo del procedimiento que

## 68 ISOMORFISMO

seguiría un matemático para mostrar, a partir de la definición, que dos grupos,  $G$  y  $G'$ , son isomorfos.

**PASO 1** Definir la función  $\phi$  que da el isomorfismo de  $G$  con  $G'$ . Esto significa describir, de alguna manera, cuál sería  $x\phi$  en  $G'$  para toda  $x \in G$ .

**PASO 2** Mostrar que  $\phi$  es una función uno a uno.

**PASO 3** Mostrar que  $\phi$  es sobre  $G'$ .

**PASO 4** Mostrar que  $(xy)\phi = (x\phi)(y\phi)$  para todas las  $x, y \in G$ . Esto es sólo cuestión de cálculos. Se calculan ambos lados de la ecuación y se ve si son iguales.

Ilustraremos esta técnica con un ejemplo.

**Ejemplo 7.1** Mostremos que  $\mathbb{R}$  bajo la suma es isomorfo a  $\mathbb{R}^+$  bajo la multiplicación.

**PASO 1** Para  $x \in \mathbb{R}$ , definase  $x\phi = e^x$ . Esto da una transformación  $\phi: \mathbb{R} \rightarrow \mathbb{R}^+$ .

**PASO 2** Si  $x\phi = y\phi$ , entonces  $e^x = e^y$ , de aquí que  $x = y$ . Así,  $\phi$  es uno a uno.

**PASO 3** Si  $r \in \mathbb{R}^+$ , entonces

$$(\ln r)\phi = e^{\ln r} = r,$$

donde  $(\ln r) \in \mathbb{R}$ . Así,  $\phi$  es sobre  $\mathbb{R}^+$ .

**PASO 4** Para  $x, y \in \mathbb{R}$  tenemos

$$(x + y)\phi = e^{x+y} = e^x e^y = (x\phi)(y\phi). \blacksquare$$

Ilustraremos de nuevo esta técnica en un teorema.

**Teorema 7.2** Cualquier grupo cíclico infinito  $G$  es isomorfo al grupo  $\mathbb{Z}$  de los enteros bajo la suma.

*Demostración* Supóngase que  $G$  tiene un generador  $a$  y úsese la notación multiplicativa para la operación en  $G$ . Así,

$$G = \{a^n \mid n \in \mathbb{Z}\}.$$

La discusión en el caso 1 de la sección 6.2 para grupos cíclicos infinitos mostró que los elementos  $a^n$  de  $G$  son todos distintos, esto es,  $a^n \neq a^m$  si  $n \neq m$ .

**PASO 1** Definir  $\phi: G \rightarrow \mathbb{Z}$  por  $a^n\phi = n$  para toda  $a^n \in G$ .

**PASO 2** Si  $a^n\phi = a^m\phi$ , entonces  $n = m$  y  $a^n = a^m$ . Así,  $\phi$  es uno a uno.

**PASO 3** Para cada  $n \in \mathbb{Z}$ , el elemento  $a^n \in G$  va a dar a  $n$  bajo  $\phi$ . Así,  $\phi$  es sobre  $\mathbb{Z}$ .

**PASO 4** Ahora,  $(a^n a^m)\phi = a^{n+m}\phi = n + m$ . ( Nótese que la operación binaria estaba en el grupo  $G$ .) Falta calcular  $(a^n\phi) + (a^m\phi)$ , se usa  $+$  porque la operación en  $\mathbf{Z}$  es la suma. Pero  $(a^n\phi) + (a^m\phi)$  también es  $n + m$ . Por tanto,  $(a^n a^m)\phi = (a^n\phi) + (a^m\phi)$ . ■

La demostración anterior fue muy fácil, hay que asegurarse de haber entendido los pasos.

Es inmediato que cada grupo  $G$  es isomorfo a sí mismo; la función identidad  $i$  definida por  $gi = g$  para todas las  $g \in G$  lo muestra. Si  $G$  es isomorfo a  $G'$ , entonces  $G'$  es isomorfo a  $G$ ; la función  $\phi^{-1}: G' \rightarrow G$  para un isomorfismo  $\phi: G \rightarrow G'$  lo muestra (véase el ejercicio 7.6). Por último, si  $G$  es isomorfo a  $G'$  y  $G'$  es isomorfo a  $G''$ , entonces  $G$  es isomorfo a  $G''$ ; si  $\phi: G \rightarrow G'$  y  $\psi: G' \rightarrow G''$  son isomorfismos, entonces la función compuesta  $\phi\psi$  lo muestra (véase el ejercicio 7.7). Debe reconocerse que hemos demostrado que la propiedad de isomorfismo es una relación de equivalencia en una colección de grupos. Por el teorema 0.1, esto significa que *dada una colección no vacía de grupos, siempre se puede partir la colección en celdas (clases de equivalencia) tales que cualesquiera dos grupos en la misma celda son isomorfos y no hay grupos en celdas distintas que sean isomorfos*.

Hemos visto que cualesquiera dos grupos de orden 3 son isomorfos. *Lo expresamos diciendo que sólo hay un grupo de orden 3, salvo isomorfismo.*

**Ejemplo 7.2** Hay un solo grupo de orden 1, uno de orden 2 y uno de orden 3, salvo isomorfismo. En el ejemplo 3.2 vimos que de orden 4, hay exactamente dos grupos diferentes, salvo isomorfismo: el grupo  $\mathbf{Z}_4$  y el 4-grupo  $V$  de Klein. Hay al menos dos grupos diferentes de orden 6, salvo isomorfismo, a saber,  $\mathbf{Z}_6$  y  $S_3$ . ■

### 7.3 COMO MOSTRAR QUE DOS GRUPOS NO SON ISOMORFOS

Trataremos ahora un tema que se estudia en pocos textos de álgebra:

*¿Cómo se demuestra que dos grupos  $G$  y  $G'$  no son isomorfos, de ser ese el caso?*

Ello significará que no existe función uno a uno  $\phi$  de  $G$  sobre  $G'$  con la propiedad  $(xy)\phi = (x\phi)(y\phi)$ . En general, es claro que no es factible someter a prueba cada función uno a uno y detectar si tiene la propiedad anterior, a menos que no existan funciones uno a uno. Esto sucede si, por ejemplo,  $G$  y  $G'$  son de orden finito y tienen distinto número de elementos.

**Ejemplo 7.3**  $\mathbf{Z}_4$  y  $S_6$  no son isomorfos. No existe función uno a uno de  $\mathbf{Z}_4$  sobre  $S_6$ . ■

En el caso infinito, no siempre está claro si existen o no funciones uno a uno y sobre. Por ejemplo, algún estudiante podría pensar que  $\mathbf{Q}$  tiene «más» elementos

que  $Z$ , pero su profesor puede mostrarle en cinco minutos (¡pidan que lo haga!) que *hay multitud de funciones uno a uno de  $Z$  sobre  $Q$ .* Sin embargo, si es cierto que  $R$  tiene demasiados elementos para ponerlo en una correspondencia uno a uno con  $Z$ . El profesor tardará otros cinco minutos en mostrar esto.

**Ejemplo 7.4**  $Z$  bajo la suma no es isomorfo a  $R$  bajo la suma, porque no existe función uno a uno de  $Z$  sobre  $R$ . ■

*En caso de que existan transformaciones uno a uno de  $G$  sobre  $G'$ , para demostrar que los grupos no son isomorfos (si tal es el caso) se suele exhibir alguna propiedad estructural que un grupo posee y el otro no.* Una propiedad estructural de un grupo es la que debe compartir cualquier grupo isomorfo. No depende de los nombres o de cualquier otra característica no estructural de los elementos. Los siguientes son ejemplos de algunas propiedades estructurales y de otras no estructurales de los grupos.

#### *Propiedades estructurales posibles*

1 El grupo es cíclico.

2 El grupo es abeliano.

3 El grupo tiene orden 8.

4 El grupo es finito.

5 El grupo tiene exactamente dos elementos de orden 6.

6 La ecuación  $x^2 = a$  tiene una solución para cada elemento  $a$  en el grupo.

#### *Propiedades no estructurales posibles*

1' El grupo contiene al 5.

2' Todos los elementos del grupo son números.

3' La operación del grupo se llama «composición».

4' Los elementos del grupo son permutaciones.

5' La operación del grupo se denota por yuxtaposición.

6' El grupo es un subgrupo de  $\langle R, + \rangle$ .

Claro que podríamos listar muchas otras propiedades estructurales posibles. El hecho de que cada una de las propiedades del 1 al 6 son, en efecto, estructurales, conforma un pequeño teorema acerca de grupos isomorfos. En los ejercicios se pedirá demostrar algunos de dichos teoremas. (Véanse los ejercicios 7.8 y 7.9.) En el texto, se considerarán obviamente estructurales.

**Ejemplo 7.5** No puede decirse que  $\mathbb{Z}$  y  $3\mathbb{Z}$  bajo la suma no son isomorfos porque  $17 \in \mathbb{Z}$  y  $17 \notin 3\mathbb{Z}$ . Estas *no* son propiedades estructurales, sino que están relacionadas con los nombres de los elementos. En realidad  $\mathbb{Z}$  y  $3\mathbb{Z}$  son isomorfos bajo la transformación  $\phi: \mathbb{Z} \rightarrow 3\mathbb{Z}$ , donde  $n\phi = 3n$ . ■

**Ejemplo 7.6** No puede decirse que  $\mathbb{Z}$  y  $\mathbb{Q}$ , ambos bajo la suma, no son isomorfos porque  $\frac{1}{2} \in \mathbb{Q}$  y  $\frac{1}{2} \notin \mathbb{Z}$ . Pero sí puede decirse que no son isomorfos porque  $\mathbb{Z}$  es cíclico y  $\mathbb{Q}$  no lo es. ■

**Ejemplo 7.7** El grupo  $\mathbb{Q}^*$  de elementos de  $\mathbb{Q}$  distintos de cero bajo la multiplicación, no es isomorfo al grupo  $\mathbb{R}^*$  de elementos de  $\mathbb{R}$  distintos de cero, bajo la multiplicación. Un argumento es que no existe entre ellos ninguna correspondencia uno a uno; otro es que cada elemento en  $\mathbb{R}^*$  es el cubo de algún elemento de  $\mathbb{R}^*$ , esto es, para  $a \in \mathbb{R}^*$  la ecuación  $x^3 = a$  tiene solución en  $\mathbb{R}^*$ . Esto no es cierto para  $\mathbb{Q}^*$ ; por ejemplo, la ecuación  $x^3 = 2$  no tiene solución en  $\mathbb{Q}^*$ . ■

**Ejemplo 7.8** El grupo  $\mathbb{R}^*$  de números reales distintos de cero bajo la multiplicación, no es isomorfo al grupo  $\mathbb{C}^*$  de los números complejos distintos de cero, bajo la multiplicación. Todo elemento de  $\mathbb{R}^*$  genera un subgrupo cíclico infinito, excepto 1 y  $-1$  que generan subgrupos de orden 1 y 2 respectivamente. Sin embargo, en  $\mathbb{C}^*$ ,  $i$  genera el subgrupo cíclico  $\{i, -1, -i, 1\}$  de orden 4. Usando otro argumento, la ecuación  $x^2 = a$  tiene solución  $x$  en  $\mathbb{C}^*$  para toda  $a \in \mathbb{C}^*$ , pero  $x^2 = -1$  no tiene solución en  $\mathbb{R}^*$ . ■

**Ejemplo 7.9** El grupo  $\mathbb{R}^*$  de números reales distintos de cero bajo la multiplicación no es isomorfo al grupo  $\mathbb{R}$  de números reales bajo la suma. La ecuación  $x + x = a$  siempre tiene solución en  $\langle \mathbb{R}, + \rangle$  para toda  $a \in \mathbb{R}$ , pero la ecuación correspondiente  $x \cdot x = a$  no siempre tiene solución en  $\langle \mathbb{R}^*, \cdot \rangle$ , por ejemplo, si  $a = -1$ . ■

## 7.4 EL TEOREMA DE CAYLEY

Obsérvese cualquier tabla de grupo en el libro. Nótese que cada renglón de la tabla da una permutación del conjunto de elementos del grupo, según están listados en la parte superior de la tabla. De manera análoga, cada columna de la tabla da una permutación del conjunto del grupo, según están listados a la izquierda de la tabla. En vista de estas observaciones, no debe sorprender que al menos todo grupo finito  $G$  sea isomorfo a algún subgrupo del grupo  $S_G$  de todas las permutaciones de  $G$ . Lo mismo sucede con los grupos infinitos: el teorema de Cayley propone que *todo* grupo es isomorfo a algún grupo formado por permutaciones, bajo la multiplicación de permutaciones. Este resultado es al mismo tiempo bello y complicado, aunque no tiene un uso importante. Sin embargo, se trata de un teorema clásico en la teoría de grupos y aparece en casi todos los

libros de álgebra. Más aún, es el primer teorema que vemos con cierta complejidad y reúne diversas ideas y técnicas expuestas por separado. Todo estudiante debe saber lo que propone el teorema de Cayley. Marcamos la demostración con un asterisco para indicar que no consideramos que este resultado sea básico para el libro.

Para facilitar la comprensión de la demostración, se ha dividido en pasos. Comenzando con cualquier grupo dado  $G$ , se procede como sigue:

PASO 1 Encontrar un conjunto  $G'$  de permutaciones que sea candidato a formar un grupo, bajo la multiplicación de permutaciones, isomorfo a  $G$ .

PASO 2 Probar que  $G'$  es un grupo bajo la multiplicación de permutaciones.

PASO 3 Definir una transformación  $\phi: G \rightarrow G'$  y mostrar que  $\phi$  es un isomorfismo entre  $G$  y  $G'$ .

**Teorema 7.3 (de Cayley)** *Todo grupo es isomorfo a un grupo de permutaciones.*

\* **Demostración** Sea  $G$  un grupo dado.

PASO 1 Nuestra primera tarea es encontrar un conjunto  $G'$  de permutaciones que sea candidato a formar un grupo isomorfo a  $G$ . Piénsese en  $G$  simplemente como conjunto y sea  $S_G$  el grupo de todas las permutaciones de  $G$  dado por el teorema 4.1. ( Nótese que en el caso finito si  $G$  tiene  $n$  elementos,  $S_G$  tiene  $n!$  elementos. Así, en general, es claro que  $S_G$  es demasiado grande para ser isomorfo a  $G$ .) Definimos cierto subconjunto de  $S_G$ . Para  $a \in G$  sea  $\rho_a$  la transformación de  $G$  en  $G$  dada por

$$x\rho_a = xa$$

para  $x \in G$ . (Podemos pensar en  $\rho_a$  como *multiplicación derecha por  $a$* .) Si  $x\rho_a = y\rho_a$  entonces  $xa = ya$  y por el teorema 2.1,  $x = y$ . Así,  $\rho_a$  es una función uno a uno. Además, si  $y \in G$ , entonces

$$(ya^{-1})\rho_a = (ya^{-1})a = y,$$

así,  $\rho_a$  lleva a  $G$  sobre  $G$ . Entonces como  $\rho_a: G \rightarrow G$  es uno a uno y sobre  $G$ ,  $\rho_a$  es una permutación de  $G$ , esto es,  $\rho_a \in S_G$ . Sea

$$G' = \{\rho_a \mid a \in G\}.$$

PASO 2 Afirmamos que  $G'$  es un subgrupo de  $S_G$ . Debemos mostrar que  $G'$  es cerrado bajo la multiplicación de permutaciones, que contiene a la permutación identidad y que contiene el inverso de cada uno de sus elementos. En primer lugar afirmamos que

$$\rho_a \rho_b = \rho_{ab}.$$

ra mostrar que estas funciones son iguales, debemos mostrar que actúan igual sobre toda  $x \in G$ . Ahora

$$x(\rho_a \rho_b) = (x\rho_a)\rho_b = (xa)\rho_b = (xa)b = x(ab) = x\rho_{ab}.$$

,  $\rho_a \rho_b = \rho_{ab}$  y por tanto,  $G'$  es cerrado bajo la multiplicación. Es claro que para toda  $x \in G$ ,

$$x\rho_e = xe = x,$$

onde  $e$  es el elemento identidad de  $G$ , de modo que  $\rho_e$  es la permutación identidad de  $S_G$  y está en  $G'$ . Como  $\rho_a \rho_b = \rho_{ab}$  tenemos

$$\rho_a \rho_{a^{-1}} = \rho_{aa^{-1}} = \rho_e$$

demás

$$\rho_{a^{-1}} \rho_a = \rho_e$$

aquí que

$$(\rho_a)^{-1} = \rho_{a^{-1}},$$

modo que  $(\rho_a)^{-1} \in G'$ . Entonces,  $G'$  es un subgrupo de  $S_G$ .

SO 3 Falta probar que  $G$  es isomorfo al grupo  $G'$  descrito. Definase  $G \rightarrow G'$  por

$$a\phi = \rho_a$$

ra  $a \in G$ . Si  $a\phi = b\phi$  entonces  $\rho_a$  y  $\rho_b$  deben ser la misma permutación de  $G$ . particular,

$$e\rho_a = e\rho_b,$$

que  $ea = eb$  y  $a = b$ . Por tanto,  $\phi$  es uno a uno. Es inmediato que  $\phi$  es sobre por la definición de  $G'$ . Finalmente,  $(ab)\phi = \rho_{ab}$  mientras que

$$(a\phi)(b\phi) = \rho_a \rho_b.$$

ro ya se dijo que  $\rho_{ab}$  y  $\rho_a \rho_b$  son la misma permutación de  $G$ . Así,

$$(ab)\phi = (a\phi)(b\phi). \blacksquare$$

ra la demostración del teorema, igualmente pudimos haber usado las permutaciones  $\lambda_x$  de  $G$  definidas por

$$x\lambda_a = ax$$

para  $x \in G$ . (Podemos pensar en  $\lambda_a$  como *multiplicación izquierda por  $a$* .) Estas permutaciones formarían un subgrupo  $G'$  de  $S_G$ , de nuevo isomorfo a  $G$ , pero ahora bajo la transformación  $\psi: G \rightarrow G'$  definida por

$$a\psi = \lambda_{a^{-1}}.$$

**Definición** El grupo  $G'$  en la demostración del teorema 7.3 es la *representación regular derecha de  $G$*  y el grupo  $G''$  del comentario anterior es la *representación regular izquierda de  $G$* .

**Tabla 7.1**

	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

**Tabla 7.2**

	$\rho_e$	$\rho_a$	$\rho_b$
$\rho_e$	$\rho_e$	$\rho_a$	$\rho_b$
$\rho_a$	$\rho_a$	$\rho_b$	$\rho_e$
$\rho_b$	$\rho_b$	$\rho_e$	$\rho_a$

**Ejemplo 7.10** Calculemos la representación regular derecha del grupo dado por la tabla 7.1. Por «calcular» queremos decir dar los elementos de la representación regular derecha y la tabla del grupo. Los elementos son

$$\rho_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}, \quad \rho_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix} \quad \text{y} \quad \rho_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}.$$

La tabla para esta representación es como la tabla original cambiando el nombre de  $x$  por el de  $\rho_x$ , como puede verse en la tabla 7.2. *Este «cambiar de nombre» es la idea básica del isomorfismo*. Por ejemplo,

$$\rho_a \rho_b = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix} \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix} = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix} = \rho_e. \blacksquare$$

Para un grupo finito dado por una tabla del grupo,  $\rho_a$  es la permutación de los elementos con el orden correspondiente a la columna bajo  $a$  y la permutación  $\lambda_a$  corresponde al orden de los elementos en el renglón a la derecha de  $a$ . Se escogieron las notaciones  $\rho_a$  y  $\lambda_a$  para sugerir la multiplicación derecha (*right*) y la multiplicación izquierda (*left*) por  $a$ , respectivamente.

## Ejercicios

7.1 Proporciónense dos argumentos que muestren que  $Z_4$  no es isomorfo al 4-grupo  $V$  de Klein del ejemplo 3.2.

7.2 Divídase la siguiente colección de grupos en subcolecciones de grupos isomorfos, como se analizó después del teorema 7.2. El asterisco (\*) significa todos los elementos del conjunto que sean distintos de cero.

$\mathbb{Z}$ bajo la suma	$S_2$
$\mathbb{Z}_6$	$\mathbb{R}^*$ bajo la multiplicación
$\mathbb{Z}_2$	$\mathbb{R}^+$ bajo la multiplicación
$S_6$	$\mathbb{Q}^*$ bajo la multiplicación
$17\mathbb{Z}$ bajo la suma	$\mathbb{C}^*$ bajo la multiplicación
$\mathbb{Q}$ bajo la suma	El subgrupo $\langle \pi \rangle$ de $\mathbb{R}^*$ bajo la multiplicación
$3\mathbb{Z}$ bajo la suma	El subgrupo $G$ de $S_8$ generado por $(1, 3, 4)(2, 6)$
$\mathbb{R}$ bajo la suma	

7.3 Proporcionese una demostración formal (por ejemplo, la dada para el teorema 7.1) del enunciado: si  $\phi$  es un isomorfismo entre un grupo  $G$  y un grupo  $G'$ , y  $H$  es un subgrupo de  $G$ , entonces

$$H\phi = \{h\phi \mid h \in H\}$$

es un subgrupo de  $G'$ . (Esto es obvio a partir de la motivación de la definición de isomorfismo, pero sería provechoso tratar de escribir una demostración formal basada sólo en la *definición* de isomorfismo.)

7.4 Sea  $G$  un grupo cíclico con generador  $a$ , y sea  $G'$  un grupo isomorfo a  $G$ . Si  $\phi: G \rightarrow G'$  es un isomorfismo, muéstrese que para toda  $x \in G$ ,  $x\phi$  está completamente determinado por el valor  $a\phi$ .

7.5 ¿Falso o verdadero?

- a) Cualesquiera dos grupos de orden 3 son isomorfos.
- b) Salvo isomorfismo, hay un solo grupo cíclico de un orden finito dado.
- c) Cualesquiera dos grupos finitos con el mismo número de elementos son isomorfos.
- d) Todo isomorfismo es una función uno a uno.
- e) Toda función uno a uno entre grupos es un isomorfismo.
- f) La propiedad de ser cíclico (o de no ser cíclico, según el caso) es una propiedad estructural de un grupo.
- g) Una propiedad estructural de un grupo debe ser compartida por todo grupo isomorfo.
- h) Un grupo abeliano no puede ser isomorfo a un grupo no abeliano.
- i) Un grupo aditivo no puede ser isomorfo a un grupo multiplicativo.
- j)  $\mathbb{R}$  bajo la suma es isomorfo a un grupo de permutaciones.

7.6 Sea  $\phi: G \rightarrow G'$  un isomorfismo entre un grupo  $G$  y un grupo  $G'$ . Muéstrese que la transformación  $\phi^{-1}: G' \rightarrow G$ , definida para  $x'\phi^{-1} = x$  por  $x\phi = x'$  donde  $x' \in G'$ , es una función bien definida y es un isomorfismo entre  $G'$  y  $G$ .

7.7 Sea  $\phi: G \rightarrow G'$  un isomorfismo de un grupo  $G$  con un grupo  $G'$  y  $\psi: G' \rightarrow G''$  un isomorfismo de  $G'$  con un grupo  $G''$ . Muéstrese que  $\phi\psi: G \rightarrow G''$  es un isomorfismo entre  $G$  y  $G''$ .

7.8 Sea  $G$  un grupo abeliano. Pruébese que ser abeliano es una propiedad estructural de  $G$  mostrando que si  $G'$  es isomorfo a  $G$ , entonces  $G'$  también es abeliano.

7.9 Sea  $G$  un grupo cíclico. Pruébese que la propiedad de ser cíclico es una propiedad estructural de  $G$ . (Véase el ejercicio 7.8.)

7.10 Un isomorfismo de un grupo con él mismo es un **automorfismo del grupo**. ¿Cuántos automorfismos hay de  $\mathbf{Z}_2$  de  $\mathbf{Z}_6$  de  $\mathbf{Z}_8$  de  $\mathbf{Z}$  y de  $\mathbf{Z}_{17}$ ? [Sugerencia: empleese el ejercicio 7.4.]

7.11 Sea  $\langle G, \cdot \rangle$  un grupo. Considérese la operación binaria  $*$  en el conjunto  $G$ , definida por

$$a * b = b \cdot a$$

para  $a, b \in G$ . Muéstrese que  $\langle G, *\rangle$  es un grupo y que  $\langle G, *\rangle$  es isomorfo a  $\langle G, \cdot \rangle$ . [Sugerencia: considérese la transformación  $\phi$  con  $a\phi = a^{-1}$  para  $a \in G$ .]

*Comentario:* Este es un ejemplo donde las notaciones  $\langle G, \cdot \rangle$  y  $\langle G, *\rangle$  son *muy útiles*. Véase la discusión que sigue a la definición de grupo. Nótese que si  $G$  es finito, entonces se obtiene la tabla del grupo para  $\langle G, *\rangle$  a partir de la tabla del grupo para  $\langle G, \cdot \rangle$ , leyendo de arriba hacia abajo en lugar de hacerlo de izquierda a derecha.

7.12 De manera similar a como se hizo en el teorema 7.2, pruébese que todo grupo cíclico finito de orden  $n$  es isomorfo a  $\mathbf{Z}_n$ .

7.13 Sea  $G$  un grupo y sea  $g$  un elemento fijo de  $G$ . Muéstrese que la transformación  $i_g$  tal que  $x_{i_g} = gxg^{-1}$  para  $x \in G$ , es un isomorfismo de  $G$  consigo, es decir, es un automorfismo de  $G$  (véase el ejercicio 7.10).

\*7.14 Calcúlese la representación regular izquierda de  $\mathbf{Z}_4$ . Calcúlese la representación regular derecha de  $S_3$  usando la notación del ejemplo 4.1.

7.15 Sea  $\langle S, *\rangle$  el grupo de todos los números reales excepto el  $-1$ , bajo la operación  $*$  definida por  $a * b = a + b + ab$  (véase el ejercicio 2.9). Muéstrese que  $\langle S, *\rangle$  es isomorfo al grupo  $\mathbf{R}^*$  de todos los números reales distintos de cero, bajo la multiplicación. Definase un isomorfismo  $\psi : \mathbf{R}^* \rightarrow S$ .

7.16 Sea  $\phi$  un isomorfismo de un grupo  $G$  con un grupo  $G'$ . Si para  $x \in G$  pensamos en  $x\phi$  como un nuevo nombre para  $x$ , o consideramos  $x\phi$  como  $x$  con el nombre cambiado, entonces la condición  $(xy)\phi = (x\phi)(y\phi)$  corresponde a la afirmación de que el diagrama en la figura 7.1 es comunitativo. La frase «el diagrama es comunitativo» significa que si comenzamos en la esquina superior izquierda y seguimos la trayectoria hasta la esquina inferior derecha dada por (flecha vertical) (flecha horizontal), da lo mismo que si seguimos la trayectoria (flecha horizontal) (flecha vertical). Ilustrando con el isomorfismo  $\psi$  de la respuesta al ejercicio 7.15, si consideramos  $x\psi$  como  $x$  cambiada de nombre, para  $x \in \mathbf{R}^*$ , obtenemos el diagrama de la figura 7.2 para  $x = 2$  y  $y = 5$ .

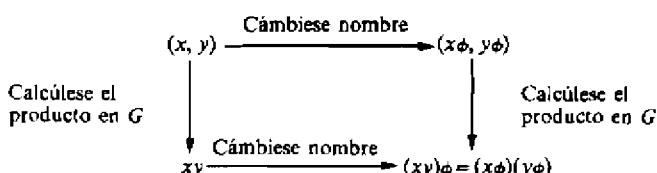


Figura 7.1

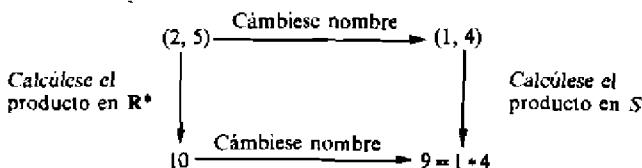


Figura 7.2

- Comenzando con el grupo  $R^*$  bajo la multiplicación, supóngase que  $x$  cambia de nombre a  $x - 4$  para  $x \in R^*$ . Sea  $S_1$  el conjunto de todos los números reales excepto  $-4$ . Definase  $*_1$  en  $S_1$  tal que  $\langle S_1, *_1 \rangle$  sea isomorfo a  $R^*$  bajo la multiplicación mediante este cambio de nombre.
- Repítase la parte a) si  $x \in R^*$  cambia de nombre a  $x - t$  para  $t \in \mathbb{R}$ , fija. Determinese primero el conjunto requerido  $S_2$ .
- Repítase la parte a) si  $x \in R^*$  cambia de nombre a  $x^3 + t$ . Determinese primero el conjunto requerido  $S_3$ .

## Productos directos

### 8.1 PRODUCTOS DIRECTOS EXTERNOS

Veamos cuál es, hasta ahora, nuestro acervo de grupos. Comenzando con los grupos finitos, tenemos el grupo cíclico  $Z_n$ , el grupo simétrico  $S_n$  y el grupo alternante  $A_n$  para cada entero positivo  $n$ . Tenemos también el grupo octal  $D_4$  del ejemplo 4.2 y el 4-grupo  $V$  de Klein. Por supuesto, sabemos que existen subgrupos de estos grupos y que el teorema de Cayley, aplicado a grupos finitos, muestra que cada grupo finito es isomorfo a un subgrupo de algún  $S_n$ . Pero no hay un camino fácil para calcular todos los subgrupos de un grupo dado. Respecto a grupos infinitos, tenemos grupos que constan de conjuntos de números bajo la suma o la multiplicación usual, por ejemplo  $Z$  y  $R$  bajo la suma.

Uno de los objetivos de este capítulo es dar a conocer un método constructivo para formar más grupos, mediante el uso de los grupos ya conocidos como partes constitutivas. Recuperaremos el 4-grupo de Klein a partir de grupos cílicos. En el siguiente capítulo, describiremos, mediante este procedimiento con los grupos cílicos, cómo se obtiene una clase amplia de grupos abelianos que incluye todos los grupos abelianos de orden finito. Comencemos con una definición de teoría de conjuntos.

**Definición** El *producto cartesiano de conjuntos*  $S_1, S_2, \dots, S_n$  es el conjunto de todas las  $n$ -adas ordenadas  $(a_1, a_2, \dots, a_n)$ , donde  $a_i \in S_i$ . El producto cartesiano se denota por

$$S_1 \times S_2 \times \cdots \times S_n$$

o por

$$\prod_{i=1}^n S_i$$

También se puede definir el producto cartesiano de un número infinito de conjuntos, pero la definición es considerablemente más sofisticada y no se necesita.

Ahora bien, sean los grupos  $G_1, G_2, \dots, G_n$ ; usaremos la notación multiplicativa para todas las operaciones de grupo. Considerando las  $G_i$  como conjuntos, podemos formar  $\prod_{i=1}^n G_i$ . Mostraremos que puede formarse un grupo de  $\prod_{i=1}^n G_i$  mediante una operación binaria de *multiplicación por componentes*. Queremos señalar nuestro descuido al usar la misma notación para un grupo y para el conjunto de elementos del grupo.

**Teorema 8.1** *Sean los grupos  $G_1, G_2, \dots, G_n$ . Para  $(a_1, a_2, \dots, a_n)$  y  $(b_1, b_2, \dots, b_n)$  en  $\prod_{i=1}^n G_i$ , definase  $(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)$  como  $(a_1b_1, a_2b_2, \dots, a_nb_n)$ . Entonces,  $\prod_{i=1}^n G_i$  es un grupo, el producto directo externo de los grupos  $G_i$ , bajo esta operación binaria.*

**Demonstración** Nótese que como  $a_i \in G_i$ ,  $b_i \in G_i$  y  $G_i$  es un grupo, tenemos que  $a_i b_i \in G_i$ . Entonces tiene sentido la definición de la operación binaria en  $\prod_{i=1}^n G_i$ , dada en el enunciado del teorema, esto es,  $\prod_{i=1}^n G_i$  es cerrado bajo la operación binaria.

La ley asociativa en  $\prod_{i=1}^n G_i$  depende de la ley asociativa en cada componente:

$$\begin{aligned} (a_1, a_2, \dots, a_n) & [(b_1, b_2, \dots, b_n)(c_1, c_2, \dots, c_n)] = \\ & = (a_1, a_2, \dots, a_n)(b_1c_1, b_2c_2, \dots, b_nc_n) \\ & = (a_1(b_1c_1), a_2(b_2c_2), \dots, a_n(b_nc_n)) \\ & = ((a_1b_1)c_1, (a_2b_2)c_2, \dots, (a_nb_n)c_n) \\ & = (a_1b_1, a_2b_2, \dots, a_nb_n)(c_1, c_2, \dots, c_n) \\ & = [(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)](c_1, c_2, \dots, c_n). \end{aligned}$$

Si  $e_i$  es el elemento identidad en  $G_i$ , entonces es claro que, con la multiplicación por componentes,  $(e_1, e_2, \dots, e_n)$  es una identidad en  $\prod_{i=1}^n G_i$ . Un inverso de  $(a_1, a_2, \dots, a_n)$  es  $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ ; basta calcular el producto por componentes. Por tanto,  $\prod_{i=1}^n G_i$  es un grupo. ■

En caso de que la operación en cada  $G_i$  sea conmutativa, usaremos, algunas veces, notación aditiva en  $\prod_{i=1}^n G_i$  y nos referiremos a  $\prod_{i=1}^n G_i$  como la *suma directa externa de los grupos  $G_i$* . En este caso, en ocasiones se usa la notación  $\bigoplus_{i=1}^n G_i$  en lugar de  $\prod_{i=1}^n G_i$ , especialmente con grupos abelianos con operación  $+$ . La suma directa de grupos abelianos  $G_1, G_2, \dots, G_n$  se puede escribir  $G_1 \oplus G_2 \oplus \dots \oplus G_n$ . Dejamos, como ejercicio, la demostración trivial de que el producto directo externo de grupos abelianos es abeliano.

Es fácil observar que si el conjunto  $S_i$  tiene  $r_i$  elementos para  $i = 1, \dots, n$ , entonces  $\prod_{i=1}^n S_i$  tiene  $r_1 r_2 \cdots r_n$  elementos, porque en una  $n$ -ada hay  $r_1$  elecciones posibles para la primera componente de  $S_1$  y para cada una de estas hay  $r_2$  elecciones posibles de  $S_2$  para la segunda componente y así sucesivamente.

**Ejemplo 8.1** Considérese el grupo  $\mathbf{Z}_2 \times \mathbf{Z}_3$ , con  $2 \cdot 3 = 6$  elementos, a saber,  $(0, 0), (0, 1), (0, 2), (1, 0), (1, 1)$  y  $(1, 2)$ . Aseguramos que  $\mathbf{Z}_2 \times \mathbf{Z}_3$  es cíclico. Basta encontrar un generador. Se intentará con  $(1, 1)$ . Las operaciones en  $\mathbf{Z}_2$  y  $\mathbf{Z}_3$  se escriben como aditivas, así que hacemos lo mismo en el producto directo externo  $\mathbf{Z}_2 \times \mathbf{Z}_3$ .

$$\begin{aligned} (1, 1) &= (1, 1) \\ 2(1, 1) &= (1, 1) + (1, 1) = (0, 2) \\ 3(1, 1) &= (1, 1) + (1, 1) + (1, 1) = (1, 0) \\ 4(1, 1) &= 3(1, 1) + (1, 1) = (1, 0) + (1, 1) = (0, 1) \\ 5(1, 1) &= 4(1, 1) + (1, 1) = (0, 1) + (1, 1) = (1, 2) \\ 6(1, 1) &= 5(1, 1) + (1, 1) = (1, 2) + (1, 1) = (0, 0) \end{aligned}$$

Por tanto,  $(1, 1)$  genera todos los  $\mathbf{Z}_2 \times \mathbf{Z}_3$ . Como sólo hay un grupo cíclico de un orden dado, salvo isomorfismo, tenemos  $(\mathbf{Z}_2 \times \mathbf{Z}_3) \cong \mathbf{Z}_6$ . ■

**Ejemplo 8.2** Considérese  $\mathbf{Z}_3 \times \mathbf{Z}_3$ . Este es un grupo de nueve elementos. Aseguramos que  $\mathbf{Z}_3 \times \mathbf{Z}_3$  no es isomorfo a  $\mathbf{Z}_9$ . Basta mostrar que  $\mathbf{Z}_3 \times \mathbf{Z}_3$  no es cíclico; como la suma se efectúa por componentes y como en  $\mathbf{Z}_3$  cada elemento sumado tres veces a él mismo da la identidad, lo mismo sucede en  $\mathbf{Z}_3 \times \mathbf{Z}_3$ . Así, ningún elemento puede generar al grupo, ya que un generador sumado sucesivamente a sí mismo daría la identidad después de nueve sumandos. Hemos encontrado otro grupo de orden 9. Un argumento similar muestra que  $\mathbf{Z}_2 \times \mathbf{Z}_2$  no es cíclico. Así que  $\mathbf{Z}_2 \times \mathbf{Z}_2$  debe ser isomorfo al 4-grupo de Klein. ■

Los ejemplos anteriores ilustran el siguiente teorema:

**Teorema 8.2** *El grupo  $\mathbf{Z}_m \times \mathbf{Z}_n$  es isomorfo a  $\mathbf{Z}_{mn}$  si y sólo si  $m$  y  $n$  son primos relativos, esto es, si el mcd de  $m$  y  $n$  es 1.*

**Demarcación** Considérese el subgrupo cíclico de  $\mathbf{Z}_m \times \mathbf{Z}_n$  generado por  $(1, 1)$  descrito en el teorema 3.2. Se ha mostrado que el orden de este subgrupo cíclico es la menor potencia de  $(1, 1)$  que da la identidad  $(0, 0)$ . Tomar aquí una potencia de  $(1, 1)$ , con la notación aditiva, significa sumar repetidamente  $(1, 1)$  a sí mismo. Bajo la suma por componentes, la primera componente  $1 \in \mathbf{Z}_m$  da 0 a los  $m$  sumandos, a los  $2m$  sumandos, y así sucesivamente, y la segunda componente  $1 \in \mathbf{Z}_n$  da 0 a los  $n$  sumandos,  $2n$  sumandos, y así sucesivamente. Para que den 0 de manera simultánea, el número de sumandos debe ser múltiplo de  $m$  y de  $n$ . El número menor que es múltiplo tanto de  $m$  como de  $n$  será  $mn$  si y sólo si el mcd de  $m$  y  $n$  es 1; en este caso,  $(1, 1)$  genera un subgrupo cíclico de orden  $mn$ , que es el orden de todo el grupo. Esto muestra que  $\mathbf{Z}_m \times \mathbf{Z}_n$  es isomorfo a  $\mathbf{Z}_{mn}$  si  $m$  y  $n$  son primos relativos.

Si el mcd de  $m$  y  $n$  es  $d > 1$ , entonces  $mn/d$  es divisible entre  $m$  y entre  $n$ . Por consiguiente, para cada  $(r, s)$  en  $\mathbf{Z}_m \times \mathbf{Z}_n$  tenemos

$$\underbrace{(r, s) + (r, s) + \cdots + (r, s)}_{mn/d \text{ sumandos}} = (0, 0).$$

De aquí que ningún elemento  $(r, s)$  en  $\mathbf{Z}_m \times \mathbf{Z}_n$  pueda generar todo el grupo, así que  $\mathbf{Z}_m \times \mathbf{Z}_n$  no es cíclico y, por tanto, no es isomorfo a  $\mathbf{Z}_{mn}$ . ■

Es claro que se puede extender este teorema, mediante un argumento induutivo, al producto de más de dos factores. Se enunciará como corolario sin entrar en los detalles de la demostración.

**Corolario** *El grupo  $\prod_{i=1}^n \mathbf{Z}_{m_i}$  es cíclico e isomorfo a  $\mathbf{Z}_{m_1 m_2 \cdots m_n}$  si y sólo si los números  $m_i$  para  $i = 1, \dots, n$  son tales que el mcd de cualesquiera dos de ellos es 1.*

**Ejemplo 8.3** El corolario anterior muestra que si  $n$  se escribe como producto de potencias de números primos distintos, como en

$$n = (p_1)^{e_1}(p_2)^{e_2} \cdots (p_r)^{e_r},$$

entonces  $\mathbf{Z}_n$  es isomorfo a

$$\mathbf{Z}_{(p_1)^{e_1}} \times \mathbf{Z}_{(p_2)^{e_2}} \times \cdots \times \mathbf{Z}_{(p_r)^{e_r}}.$$

En particular,  $\mathbf{Z}_{72}$  es isomorfo a  $\mathbf{Z}_8 \times \mathbf{Z}_9$ . ■

Ya se usó en varias ocasiones el concepto de la menor potencia positiva de un elemento de un grupo que da la identidad. Se introducirá ahora la terminología usual.

**Definición** Sea  $G$  un grupo y  $a \in G$ . Si existe algún entero positivo  $n$  tal que  $a^n = e$ , el menor de dichos enteros positivos  $n$ , es el *orden de  $a$* . Si no existe dicha  $n$ , entonces  $a$  es de *orden infinito*.

De esto se desprende que si  $a$  es un elemento de un grupo  $G$ , el orden de  $a$  es igual al orden del subgrupo cíclico generado por  $a$ . Este es un hecho muy útil que debe recordarse.

**Teorema 8.3** Sea  $(a_1, a_2, \dots, a_n) \in \prod_{i=1}^n G_i$ . Si  $a_i$  es de orden finito  $r_i$  en  $G_i$ , entonces el orden de  $(a_1, a_2, \dots, a_n)$  en  $\prod_{i=1}^n G_i$  es igual al mínimo común múltiplo de todas las  $r_i$ .

**Demostración** Este es el resultado de repetir el argumento usado en la demostración del teorema 8.2. Para que una potencia de  $(a_1, a_2, \dots, a_n)$  sea igual a

$(e_1, e_2, \dots, e_n)$ , la potencia debe ser de manera simultánea múltiplo de  $r_1$ , para que esta potencia de la primera componente  $a_1$  dé  $e_1$ ; un múltiplo de  $r_2$  para que esta potencia de la segunda componente  $a_2$  dé  $e_2$ , y así sucesivamente. ■

Es obvio que si  $\prod_{i=1}^n G_i$  es un producto directo externo de grupos  $G_i$ , el subconjunto

$$G_i = \{(e_1, e_2, \dots, e_{i-1}, a_i, e_{i+1}, \dots, e_n) \mid a_i \in G_i\},$$

esto es, el conjunto de todas las  $n$ -adas con los elementos identidad en todos los lugares excepto el  $i$ -ésimo, es un subgrupo de  $\prod_{i=1}^n G_i$ . También es claro que este subgrupo  $G_i$  es naturalmente isomorfo a  $G_i$  bajo la correspondencia dada por la proyección que transforma  $\pi_i$ , donde

$$(e_1, e_2, \dots, e_{i-1}, a_i, e_{i+1}, \dots, e_n)\pi_i = a_i.$$

El grupo  $G_i$  se refleja en la  $i$ -ésima componente de los elementos de  $G_i$ , y las  $e_j$  en las otras componentes simplemente van de acompañantes. Consideremos  $\prod_{i=1}^n G_i$  como el *producto directo interno* de estos subgrupos  $G_i$ . Los términos *interno* y *externo*, aplicados a los productos directos de grupos, sólo reflejan si se consideran o no (respectivamente), a los grupos componentes como subgrupos del grupo producto. Después de esta sección, por lo común, omitiremos las palabras *externo* e *interno* y diremos sólo *producto directo*. El significado correcto quedará claro de acuerdo con el contexto. Para quienes lo deseen, en la sección 8.2 (con asterisco) se tratará con cuidado el producto directo interno. Se necesitará una definición básica de teoría de conjuntos y un teorema también básico de la teoría de grupos. Se presentan aquí, pues más adelante les daremos otro uso.

**Definición** Sea  $\{S_i \mid i \in I\}$  una colección de conjuntos. Aquí  $I$  puede ser cualquier conjunto de índices. La *intersección*  $\bigcap_{i \in I} S_i$  de los conjuntos  $S_i$  es el conjunto de todos los elementos que están en todos los conjuntos  $S_i$ , esto es,

$$\bigcap_{i \in I} S_i = \{x \mid x \in S_i \text{ para toda } i \in I\}.$$

Si  $I$  es finito,  $I = \{1, 2, \dots, n\}$  podemos denotar  $\bigcap_{i \in I} S_i$  por

$$S_1 \cap S_2 \cap \dots \cap S_n$$

**Teorema 8.4** La intersección de subgrupos  $H_i$  de un grupo  $G$  para  $i \in I$  es un subgrupo de  $G$ .

**Demostración** Mostremos la cerradura. Sea  $a \in \bigcap_{i \in I} H_i$  y  $b \in \bigcap_{i \in I} H_i$  de modo que  $a \in H_i$  para todas las  $i \in I$  y  $b \in H_i$  para todas las  $i \in I$ . Entonces  $ab \in H_i$  para todas las  $i \in I$  ya que  $H_i$  es un grupo. Así,  $ab \in \bigcap_{i \in I} H_i$ .

Como  $H_i$  es un subgrupo para todas las  $i \in I$ , tenemos que  $e \in H_i$  para todas las  $i \in I$  y de aquí  $e \in \bigcap_{i \in I} H_i$ .

Para concluir, si  $a \in \bigcap_{i \in I} H_i$ , se tiene que  $a \in H_i$  para todas las  $i \in I$ , luego  $a^{-1} \in H_i$  para todas las  $i \in I$ , lo cual implica que  $a^{-1} \in \bigcap_{i \in I} H_i$ . ■

## \*8.2 PRODUCTOS DIRECTOS INTERNOS

**Definición** Sea un grupo  $G$  con subgrupos  $H_i$  para  $i = 1, \dots, n$ .  $G$  es el *producto directo interno de los subgrupos  $H_i$*  si la transformación  $\phi: \prod_{i=1}^n H_i \rightarrow G$  dada por

$$(h_1, h_2, \dots, h_n)\phi = h_1 h_2 \cdots h_n$$

es un isomorfismo.

Nótese que bajo este isomorfismo  $\phi$ , el subgrupo  $\tilde{H}_i$  de  $\prod_{i=1}^n H_i$  va a dar de manera natural sobre  $H_i$ . En vista del isomorfismo que aparece en esta definición, todo lo que observemos para un producto directo externo o para un producto directo interno tiene una interpretación inmediata para el otro.

**Teorema 8.5** Si  $G$  es el producto directo interno de los subgrupos  $H_1, H_2, \dots, H_n$ , entonces cada  $g \in G$  puede escribirse de manera única como  $g = h_1 h_2 \cdots h_n$  donde  $h_i \in H_i$ .

**Demostración** Usando el isomorfismo de la definición, basta mostrar que el enunciado correspondiente es cierto para el producto directo externo  $\prod_{i=1}^n H_i$  con respecto a sus subgrupos  $\tilde{H}_i$ , los cuales son naturalmente isomorfos a  $H_i$ . Debemos mostrar que todo elemento  $(h_1, h_2, \dots, h_n)$  de  $\prod_{i=1}^n H_i$  se puede escribir de manera única como producto

$$(a_1, e_2, \dots, e_n)(e_1, a_2, \dots, e_n) \cdots (e_1, e_2, \dots, a_n),$$

donde  $a_i \in H_i$ . Esto es obvio. Debemos tener  $a_i = h_i$ . ■

La definición y el teorema anteriores sugieren que sería interesante examinar productos de elementos de varios subgrupos de un grupo. En el resto de esta sección trabajaremos con sólo dos subgrupos de un grupo; aunque las definiciones y teoremas pueden generalizarse a más de dos subgrupos.

Sean  $H$  y  $K$  subgrupos de un grupo  $G$ . Nos interesa examinar  $\{hk \mid h \in H, k \in K\}$ , que denotaremos por  $HK$ . Por desgracia, este conjunto  $HK$  no es necesariamente un subgrupo de  $G$ , pues  $h_1k_1h_2k_2$  no por fuerza es de la forma  $hk$ . Claro que si  $G$  es abeliano, o aun si cada elemento  $h$  de  $H$  commuta con cada elemento  $k$  de  $K$ , esto es,  $hk = kh$ , entonces

$$h_1k_1h_2k_2 = h_1h_2k_1k_2 = h_3k_3,$$

## 84 PRODUCTOS DIRECTOS

donde  $h_3 = h_1h_2$  y  $k_3 = k_1k_2$  son elementos de  $H$  y  $K$  respectivamente. Es fácil corroborar que en este caso tenemos un subgrupo, para  $ee = e$  y  $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1}$ .

Tratemos de obtener algún subgrupo en el caso no commutativo. Nótese que siempre hay al menos un subgrupo de  $G$  que contiene  $HK$ , a saber,  $G$  mismo.

**Definición** Sean  $H$  y  $K$  subgrupos de un grupo  $G$ . El *ensamble*  $H \vee K$  de  $H$  y  $K$  es la intersección de todos los subgrupos de  $G$  que contienen  $HK = \{hk \mid h \in H, k \in K\}$ .

Es claro que esta intersección es el subgrupo más pequeño posible de  $G$  que contiene  $HK$ , y si los elementos en  $H$  y en  $K$  commutan, en particular, si  $G$  es abeliano, tenemos  $H \vee K = HK$ . Nótese que como  $h = he$  y  $k = ek$ ,  $H \subseteq HK$  y  $K \subseteq HK$ , por tanto,  $H \leq H \vee K$  y  $K \leq H \vee K$ . Pero es claro que  $H \vee K$  estará contenido en cualquier subgrupo que contenga tanto a  $H$  como a  $K$ . Vemos así que  $H \vee K$  es el menor subgrupo de  $G$  que contiene a  $H$  y a  $K$ .

Concluiremos con un teorema que se utilizará en secciones posteriores marcadas con asterisco.

**Teorema 8.6** Un grupo  $G$  es el producto directo interno de subgrupos  $H$  y  $K$  si y sólo si

- 1  $G = H \vee K$
- 2  $hk = kh$  para todas las  $h \in H$  y todas las  $k \in K$ ,
- 3  $H \cap K = \{e\}$ .

**Demostración** Sea  $G$  el producto interno directo de  $H$  y  $K$ . Afirmando que las condiciones 1, 2 y 3 son obvias si se considera  $G$  como isomorfo al producto directo externo de  $H$  y  $K$  bajo la transformación  $\phi$ , definida por  $(h, k)\phi = hk$ . Bajo esta transformación,

$$H = \{(h, e) \mid h \in H\}$$

corresponde a  $H$  y

$$K = \{(e, k) \mid k \in K\}$$

corresponde a  $K$ . Entonces, las condiciones 1, 2 y 3 siguen inmediatamente de las afirmaciones correspondientes acerca de  $H$  y  $K$  en  $H \times K$ , las cuales son obvias.

En forma recíproca, supóngase que se cumplen las condiciones 1, 2 y 3. Debemos mostrar que la transformación  $\phi$  del producto directo externo  $H \times K$  en  $G$  dada por  $(h, k)\phi = hk$  es un isomorfismo. Ya se definió la transformación  $\phi$ .

Supóngase que

$$(h_1, k_1)\phi = (h_2, k_2)\phi.$$

Entonces,  $h_1k_1 = h_2k_2$ ; de aquí  $h_2^{-1}h_1 = k_2k_1^{-1}$ . Pero  $h_2^{-1}h_1 \in H$  y  $k_2k_1^{-1} \in K$ , y son el mismo elemento, por tanto, están en  $H \cap K = \{e\}$  por la condición 3. En consecuencia,  $h_2^{-1}h_1 = e$  y  $h_1 = h_2$ . De manera análoga,  $k_1 = k_2$ , así que  $(h_1, k_1) = (h_2, k_2)$ . Esto muestra que  $\phi$  es uno a uno.

El hecho de que por la condición 2  $hk = kh$  para todas las  $h \in H$  y todas las  $k \in K$  significa que

$$HK = \{hk \mid h \in H, k \in K\}$$

es un grupo, pues ya vimos que así sucede si los elementos de  $H$  comutaban con los elementos de  $K$ . De modo que, por la condición 1,  $HK = H \vee K = G$  luego  $\phi$  es sobre  $G$ .

Por último,

$$[(h_1, k_1)(h_2, k_2)]\phi = (h_1h_2, k_1k_2)\phi = h_1h_2k_1k_2,$$

mientras que

$$[(h_1, k_1)\phi][(h_2, k_2)\phi] = h_1k_1h_2k_2.$$

Pero por la condición 2, tenemos que  $k_1h_2 = h_2k_1$ . Así,

$$[(h_1, k_1)(h_2, k_2)]\phi = [(h_1, k_1)\phi][(h_2, k_2)\phi]. \blacksquare$$

## Ejercicios

---

8.1 Listense los ocho elementos de  $\mathbb{Z}_2 \times \mathbb{Z}_4$ . Encuéntrese el orden de cada uno de los elementos. ¿Es cíclico este grupo?

8.2 ¿Cuál de los subgrupos cíclicos de  $\mathbb{Z}_6 \times \mathbb{Z}_8$  tiene el orden mayor y cuál de  $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ ?

8.3 Pruébese que el producto directo externo de grupos abelianos es abeliano.

8.4 Encuéntrense todos los subgrupos propios no triviales de  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

8.5 Sin tomar en cuenta el orden de los factores, escribanse productos directos de dos o más grupos de la forma  $\mathbb{Z}_n$  de manera que el producto resultante sea isomorfo a  $\mathbb{Z}_{60}$  de todas las maneras posibles.

8.6 Complétense los enunciados.

- El subgrupo cíclico de  $\mathbb{Z}_{24}$  generado por 18 tiene orden \_\_\_\_
- $\mathbb{Z}_3 \times \mathbb{Z}_4$  es de orden \_\_\_\_
- El elemento (4, 2) de  $\mathbb{Z}_{12} \times \mathbb{Z}_8$  tiene orden \_\_\_\_
- El 4-grupo de Klein es isomorfo a  $\mathbb{Z}_\square \times \mathbb{Z}_\square$
- $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}_4$  tiene \_\_\_\_ elementos de orden finito.

## 8.7 ¿Falso o verdadero?

- a) Si  $G_1$  y  $G_2$  son grupos cualesquiera, entonces  $G_1 \times G_2$  siempre es isomorfo a  $G_2 \times G_1$ .
  - b) Es fácil calcular en un producto directo externo de grupos, si se sabe cómo calcular en cada grupo componente.
  - c) Se debe usar grupos de orden finito al formar un producto directo externo.
  - d) Un grupo de orden primo no puede ser producto directo interno de dos subgrupos propios no triviales.
  - e)  $\mathbb{Z}_2 \times \mathbb{Z}_4$  es isomorfo a  $\mathbb{Z}_8$ .
  - f)  $\mathbb{Z}_2 \times \mathbb{Z}_4$  es isomorfo a  $S_6$ .
  - g)  $\mathbb{Z}_3 \times \mathbb{Z}_8$  es isomorfo a  $S_4$ .
  - h) Todo elemento en  $\mathbb{Z}_4 \times \mathbb{Z}_8$  tiene orden 8.
  - i) El orden de  $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$  es 60.
  - j)  $\mathbb{Z}_m \times \mathbb{Z}_n$  tiene  $mn$  elementos ya sea que  $m$  y  $n$  sean o no primos relativos.
- 

8.8 Encuéntrense todos los subgrupos propios no triviales de  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ .

8.9 Encuéntrense todos los subgrupos de  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$  que sean isomorfos al 4-grupo de Klein.

8.10 Proporcione un ejemplo para ilustrar que no todo grupo abeliano es el producto directo interno de dos subgrupos propios no triviales. (Véase el ejercicio 8.16 para el ejemplo correspondiente en grupos no abelianos.)

8.11 Sea  $G$  un grupo abeliano. Sea  $H$  el subconjunto de  $G$  que consta de la identidad  $e$  junto con todos los elementos de  $G$  de orden 2. Muéstrese que  $H$  es un subgrupo de  $G$ .

8.12 Siguiendo la idea del ejercicio 8.11, determíñese si  $H$  será siempre un subgrupo del grupo abeliano  $G$ , si  $H$  consta de la identidad  $e$  junto con todos los elementos de  $G$  de orden 3, y de orden 4. ¿Para qué enteros positivos  $n$ , será siempre  $H$  un subgrupo para todo grupo abeliano  $G$ , si  $H$  consta de la identidad  $e$  y todos los elementos de  $G$  de orden  $n$ ? Compárese con el ejercicio 3.12.

8.13 Encuéntrese un contraejemplo para el ejercicio 8.11 omitiendo la hipótesis de que  $G$  es abeliano.

8.14 En ocasiones se oye decir que «la intersección de grupos es un grupo». ¿Por qué esto es incorrecto?

\*8.15 Enúnciese un teorema similar al teorema del ejercicio 8.3, pero para el caso de un grupo que es producto interno directo de subgrupos.

\*8.16 Muéstrese que  $S_3$  del ejemplo 4.1 no es el producto interno directo de los subgrupos

$$H = \{\rho_0, \rho_1, \rho_2\} \quad y \quad K = \{\rho_0, \mu_1\}.$$

\*8.17 Sea  $n = rs$ , donde  $r$  y  $s$  son enteros primos relativos, esto es, el mod de  $r$  y  $s$  es 1. Muéstrese que  $\mathbb{Z}_n$  es el producto directo interno de sus subgrupos cíclicos  $\langle r \rangle$  y  $\langle s \rangle$ .

\*8.18 Considérense los subgrupos  $H = \langle 2 \rangle$  y  $K = \langle 6 \rangle$  de  $\mathbb{Z}_{12}$ . Determinense  $HK$  y  $H \vee K$ .

\*8.19 Considérense los subgrupos

$$H = \{\rho_0, \mu_1\} \quad \text{y} \quad K = \{\rho_0, \mu_2\}$$

de  $S_3$  del ejemplo 4.1. Determinense  $HK$  y  $H \vee K$ .

\*8.20 Considérense los subgrupos

$$H = \{\rho_0, \delta_1\} \quad \text{y} \quad K = \{\rho_0, \delta_2\}$$

del grupo  $D_4$  de las simetrías del cuadrado en el ejemplo 4.2. Determinense  $HK$  y  $H \vee K$ .

\*8.21 Sea  $G$  un grupo. Sean  $h$  y  $k$  elementos de  $G$  que comutan y cuyos órdenes  $r$  y  $s$  son primos relativos. Aplíquese el teorema 8.6 a los subgrupos  $\langle h \rangle$  y  $\langle k \rangle$  de  $\langle h \rangle \vee \langle k \rangle$  para mostrar que  $hk$  es de orden  $rs$ .

## Grupos abelianos finitamente generados

Algunos teoremas de álgebra abstracta son fáciles de entender y emplear aunque sus demostraciones sean muy técnicas y de presentación extensa. Esta es la primera de varias secciones del libro donde explicaremos el significado e importancia de algunos teoremas y pediremos que se usen sin demostrarlos. Por lo general, las demostraciones se presentan en secciones posteriores marcadas con asterisco. Hoy día es tan grande el volumen de la literatura matemática, que aquellos matemáticos que insistan en corroborar hasta el último detalle la demostración de cada resultado que usen, no podrán alcanzar límites importantes del tema tratado. Los teoremas que presentamos sin demostración en las secciones no marcadas, están dentro de lo que ya conocemos y consideramos que deben ser familiares para el lector. Sería imposible cubrir en un curso de un semestre en nivel de licenciatura todos estos aspectos fascinantes si insistiéramos en realizar todas sus demostraciones.

### 9.1 GENERADORES Y TORSION

El primer concepto que se definirá tiene gran importancia. A diferencia de nuestro procedimiento anterior, daremos primero una definición elegante y después se explicará a nivel intuitivo en un teorema. Recuérdese, por el teorema 8.4, que la intersección de subgrupos de un grupo es un grupo. Sea  $G$  un grupo y  $a_i$  elementos de  $G$  para  $i \in I$ , donde  $I$  es un conjunto de índices. Existe al menos un subgrupo de  $G$  que contiene todas las  $a_i$ , a saber,  $G$  mismo. Es obvio que la intersección de todos los subgrupos de  $G$  que contienen todas las  $a_i$  es el menor subgrupo de  $G$  que contiene todas las  $a_i$  para  $i \in I$ .

**Definición** Sea  $G$  un grupo y  $a_i \in G$  para  $i \in I$ . El menor subgrupo de  $G$  que contiene  $\{a_i \mid i \in I\}$  es el *subgrupo generado por  $\{a_i \mid i \in I\}$* . Si este subgrupo es todo  $G$ , entonces  $\{a_i \mid i \in I\}$  genere  $G$  y las  $a_i$  son *generadores de  $G$* . Si existe un conjunto finito  $\{a_i \mid i \in I\}$  que genere  $G$ , entonces  $G$  es *finitamente generado*.

Nótese que esta definición es consistente con nuestra definición anterior de generador de un grupo cíclico. Nótese, además, que el siguiente teorema se enuncia y demuestra para cualquier grupo  $G$ , no sólo para grupos abelianos.

**Teorema 9.1** .Si  $G$  es un grupo y  $a_i \in G$  para  $i \in I$ , entonces el subgrupo  $H$  de  $G$  generado por  $\{a_i \mid i \in I\}$  consta de precisamente aquellos elementos de  $G$  que son productos finitos de potencias de exponente entero de  $a_i$ , donde, en ese producto, pueden presentarse varias veces potencias de alguna  $a_i$  dada.

**Demostración** La razón por la cual tenemos que en el producto hay varias potencias para una  $a_i$  dada, es que no se supone que  $G$  es abeliano. Si  $G$  es abeliano, entonces  $(a_1)^{-3}(a_2)^3(a_1)^7$  podría simplificarse como  $(a_1)^4(a_2)^5$ , pero esto puede no ser cierto en el caso no abeliano.

$K$  denotará el conjunto de todos los productos finitos de potencias de exponente entero de  $a_i$ . Es claro que  $K \subseteq H$ . Obsérvese que  $K$  es un subgrupo y entonces, como  $H$  es el menor subgrupo que contiene  $a_i$  para  $i \in I$ , habremos terminado. Es obvio que un producto de elementos en  $K$  está en  $K$ . Como  $(a_1)^0 = e$  tenemos  $e \in K$ . Si para toda  $k$  en  $K$ , se forma, a partir del producto que da  $k$ , un nuevo producto, invirtiendo el orden de las  $a_i$  y poniendo el signo opuesto a todos los exponentes, se tendrá  $k^{-1}$ , que está en  $K$ . Por ejemplo

$$[(a_1)^3(a_2)^4(a_1)^{-7}]^{-1} = (a_1)^7(a_2)^{-2}(a_1)^{-3},$$

lo cual está en  $K$ . ■

**Ejemplo 9.1**  $\mathbb{Z} \times \mathbb{Z}_2$  está generado por  $\{(1, 0), (0, 1)\}$ . ■

Los alumnos que estudiaron la sección \*8.2 notarán que si  $A$  y  $B$  son subgrupos de  $G$ , entonces el subgrupo ensamble  $A \vee B$  es precisamente el subgrupo generado por  $A \cup B$ .

Aunque en esta sección tratamos principalmente con grupos abelianos, usaremos la notación multiplicativa en los análisis generales. Nuestra experiencia indica que los estudiantes comprenden más rápido la notación  $a^n$  que  $na$ . En esta última notación, el estudiante tiende a cometer el error de pensar  $n$  como un elemento del grupo.

**Definición** Un grupo  $G$  es un *grupo de torsión* si todo elemento de  $G$  es de orden finito.  $G$  es *libre de torsión* si ningún otro elemento aparte de la identidad es de orden finito.

**Teorema 9.2** En un grupo abeliano  $G$ , el conjunto  $T$  de todos los elementos de  $G$  de orden finito es un subgrupo de  $G$ , el subgrupo de torsión de  $G$ .

**Demostración** Usamos notación multiplicativa. Sean  $a$  y  $b$  elementos de  $T$ . Entonces, existen enteros positivos  $m$  y  $n$  tales que  $a^m = b^n = e$ . Como  $G$  es abeliano,

$$(ab)^{mn} = a^{mn}b^{mn},$$

entonces,

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^ne^m = e.$$

Por tanto,  $ab$  es de orden finito, luego está en  $T$ . Esto muestra que  $T$  es cerrado bajo la multiplicación del grupo.

Es claro que  $e$  es de orden finito y por tanto está en  $T$ .

Por último, si  $a \in T$  y  $a^m = e$ , entonces

$$e = e^m = (aa^{-1})^m = a^m(a^{-1})^m = e(a^{-1})^m = (a^{-1})^m,$$

así que  $a^{-1}$  es de orden finito y, por tanto, está en  $T$ . ■

**Ejemplo 9.2** Todo grupo finito es un grupo de torsión, mientras que  $\mathbb{Z}$  bajo la suma es libre de torsión. Si consideramos  $\mathbb{Z} \times \mathbb{Z}_2$ , el elemento  $(1, 0)$  no es de orden finito, pero el elemento  $(0, 1)$  es de orden 2. Es claro que  $T = \{(0, 0), (0, 1)\}$  es el subgrupo de torsión de  $\mathbb{Z} \times \mathbb{Z}_2$ . ■

## 9.2 EL TEOREMA FUNDAMENTAL

Se enunciarán ahora algunos lemas que nos conducirán al teorema principal de la sección: el teorema 9.3. Los lemas no se demuestran. El teorema 9.3 se demuestra en el capítulo 20 (marcado). La demostración que ahí se presenta no se construye mediante la sucesión de los lemas dados aquí; seleccionamos estos lemas introductorios para llegar en forma gradual a la comprensión de la estructura de grupo descrita en el teorema.

**Lema 9.1** Si  $G$  es un grupo abeliano finitamente generado con un subgrupo de torsión  $T$ , entonces  $G$  es un producto directo (interno)  $T \times F$  para algún subgrupo  $F$  de  $G$  que sea libre de torsión.

**Demostración** La demostración resultará del teorema 9.3, el cual se demuestra en el capítulo 20 (marcado). ■

**Lema 9.2** Un grupo abeliano  $F$  finitamente generado, libre de torsión, es isomorfo a  $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$  para algún número  $m$  de factores. El número  $m$ , el número de betti de  $F$ , es único.

**Demostración** La demostración resultará del teorema 9.3, el cual se demuestra en el capítulo 20 (marcado). ■

**Lema 9.3** Un grupo abeliano finito  $T$  es isomorfo a dos tipos diferentes de productos directos de grupos cíclicos, como sigue:

1  $T$  es isomorfo a un producto

$$\mathbb{Z}_{p_1, r_1} \times \mathbb{Z}_{p_2, r_2} \times \cdots \times \mathbb{Z}_{p_n, r_n}$$

donde los  $p_i$  son primos no necesariamente distintos. Este producto directo de grupos cíclicos de orden la potencia de un primo isomorfo a  $T$ , es único excepto por un rearrreglo de los factores.

2  $T$  es isomorfo a un producto directo

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$$

donde  $m_i$  divide a  $m_{i+1}$ . Los números  $m_i$ , los coeficientes de torsión de  $T$  son únicos.

**Demostración** La demostración resultará del teorema 9.3, el cual se demuestra en el capítulo 20 (marcado). ■

Los términos *números de betti* y *coeficientes de torsión* provienen de la topología algebraica, donde desempeñan un papel importante.

No es posible exigir que los primos  $p_i$  que aparecen en la forma 1 del lema 3 sean diferentes. Hemos visto, por ejemplo, que  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$  no es isomorfo a  $\mathbb{Z}_{27} \times \mathbb{Z}_3$ , ya que el primero tiene elementos a lo sumo de orden 45, mientras que el segundo es cíclico de orden 225.

Piénsese por un momento en la importancia y el enorme poder del lema 9.3. Proporciona una descripción, salvo isomorfismo, de todos los grupos abelianos finitos.

Se describirá un método para encontrar un grupo, expresado en la forma 2 del lema 9.3, que sea isomorfo a un producto directo dado de grupos cíclicos de orden la potencia de un primo. Para cada primo que aparezca en el orden del grupo, escribanse los subíndices en el producto directo donde aparece ese primo, en orden de magnitud creciente. Manténganse alineados los extremos derechos de las renglones. Así, comenzando con  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$  formamos el ordenamiento

2	4
3	3
	5

## 92 GRUPOS ABELIANOS FINITAMENTE GENERADOS

A continuación se toma el producto de los números en cada columna obteniendo, en este caso, 6 y 60. Entonces,  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$  es isomorfo a  $\mathbb{Z}_6 \times \mathbb{Z}_{60}$ . Así mismo,  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$  da lugar al arreglo

$$\begin{array}{r} 2 & 2 & 2 \\ 3 & 3 & \\ & 5 & \\ \hline 2 & 6 & 30 \end{array}$$

y, por tanto, es isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$ . No se hará una demostración formal de la validez de este algoritmo. Es fácil ver por qué funciona, a partir de la teoría desarrollada en el capítulo 8, en particular del teorema 8.2.

**Ejemplo 9.3** Encuéntrense todos los grupos abelianos (salvo isomorfismo) de orden 360. Primero, se expresa 360 como producto de potencias de primos  $2^3 3^2 5$ . Entonces, al usar la forma 1 del lema 9.3, se obtienen las posibilidades

- 1  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- 2  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- 3  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- 4  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- 5  $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- 6  $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Hay, entonces, seis grupos abelianos diferentes (salvo isomorfismo) de orden 360. En la parte inferior escribimos los seis casos en la forma 2 del lema 9.3, manteniendo los grupos (salvo isomorfismo) en el mismo orden. Esto es, el primer grupo listado en la parte superior es isomorfo al primero de los listados a continuación y así sucesivamente. Esto es fácil de verificar a partir de las observaciones anteriores al ejemplo.

- |   |  |
|---|--|
| 1 $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$ | 2 $\mathbb{Z}_6 \times \mathbb{Z}_{60}$  |
| 3 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90}$ | 4 $\mathbb{Z}_2 \times \mathbb{Z}_{180}$ |
| 5 $\mathbb{Z}_3 \times \mathbb{Z}_{120}$                    | 6 $\mathbb{Z}_{360}$ ■                   |

El teorema principal es resultado inmediato de los lemas anteriores, excepto por el hecho de que un subgrupo de un grupo abeliano finitamente generado es, a su vez, finitamente generado, lo cual se demuestra en el capítulo 20.

**Teorema 9.3 (Teorema fundamental de los grupos abelianos finitamente generados)** Todo grupo abeliano finitamente generado  $G$  es isomorfo al producto directo de los grupos cíclicos de la forma

$$|\quad \mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

donde las  $p_i$  son primos, no necesariamente distintos, y también es isomorfo a un producto de la forma

$$2 \quad \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

donde  $m_i$  divide a  $m_{i+1}$ .

En ambos casos el producto directo es único, excepto por posibles rearreglos de los factores, esto es, el número de factores (número de betti de  $G$ ) de  $\mathbb{Z}$  es único, los coeficientes de torsión  $m_i$  de  $G$  son únicos y las potencias de primos  $(p_i)^r$  son únicas.

*Demostración* En el capítulo 20 (marcado), se encuentra una demostración completa. ■

¿Resulta comprensible la importancia de estos resultados? Entre otras cosas, nos dan información completa acerca de todos los grupos abelianos finitos.

## \*9.3 APLICACIONES

Concluiremos esta sección con una muestra de los muchos teoremas sobre grupos abelianos que podemos demostrar ahora. Algunos son resultado del trabajo desarrollado en el capítulo 8 y para otros se requiere el poderoso teorema 9.3.

**Definición** Un grupo  $G$  tiene *descomposición* si es isomorfo al producto directo de dos subgrupos propios no triviales. De no ser así, decimos que  $G$  es *sin descomposición*.

**Teorema 9.4** Los grupos abelianos finitos sin descomposición son precisamente los grupos cíclicos cuyo orden es potencia de un primo.

*Demostración* Sea  $G$  un grupo abeliano finito, sin descomposición. Por el teorema 9.3 (o por el lema 9.3),  $G$  es isomorfo a un producto directo de grupos cíclicos cuyos órdenes son potencias de primos. Como  $G$  es sin descomposición, este producto directo debe constar de sólo un grupo cíclico de orden una potencia de un primo.

Recíprocamente, sea  $p$  un primo. El material del capítulo 8 muestra que  $\mathbb{Z}_p$  es sin descomposición, pues si  $\mathbb{Z}_p$  fuera isomorfo a  $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$ , donde  $i + j = r$ , entonces todo elemento tendría a lo sumo orden  $p^{\max(i,j)} < p^r$ . ■

**Teorema 9.5** Si  $m$  divide al orden de un grupo abeliano finito  $G$ , entonces  $G$  tiene un subgrupo de orden  $m$ .

*Demostración* Por el teorema 9.3 (o por el lema 9.3) podemos considerar a  $G$  como

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_s)^{r_s}}$$

donde no todos los primos  $p_i$  son necesariamente distintos. Como  $(p_1)^{r_1}(p_2)^{r_2} \cdots (p_n)^{r_n}$  es el orden de  $G$ , entonces  $m$  debe ser de la forma  $(p_1)^{s_1}(p_2)^{s_2} \cdots (p_n)^{s_n}$ , donde  $0 \leq s_i \leq r_i$ . Por el teorema 6.4,  $(p_i)^{r_i-s_i}$  genera un subgrupo cíclico de  $\mathbb{Z}_{(p_i)^{r_i}}$  de orden igual al cociente de  $(p_i)^{r_i}$  sobre el mcd de  $(p_i)^{r_i}$  y  $(p_i)^{r_i-s_i}$ . Pero el mcd de  $(p_i)^{r_i}$  y  $(p_i)^{r_i-s_i}$  es  $(p_i)^{r_i-s_i}$ . Así,  $(p_i)^{r_i-s_i}$  genera un subgrupo cíclico  $\mathbb{Z}_{(p_i)^{r_i}}$  de orden

$$[(p_i)^{r_i}] / [(p_i)^{r_i-s_i}] = (p_i)^{s_i}.$$

Si se recuerda que  $\langle a \rangle$  denota el subgrupo cíclico generado por  $a$ , vemos que

$$\langle (p_1)^{r_1-s_1} \rangle \times \langle (p_2)^{r_2-s_2} \rangle \times \cdots \times \langle (p_n)^{r_n-s_n} \rangle$$

es el subgrupo de orden  $m$  requerido. ■

**Teorema 9.6** *Si  $m$  es un entero libre de cuadrado, es decir, si  $m$  no es divisible por el cuadrado de algún primo, entonces todo grupo abeliano de orden  $m$  es cíclico.*

*Demostración* Sea  $G$  un grupo abeliano de orden  $m$  libre de cuadrado. Entonces, por el teorema 9.3 (o por el lema 9.3),  $G$  es isomorfo a

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$$

donde  $m = (p_1)^{r_1}(p_2)^{r_2} \cdots (p_n)^{r_n}$ . Como  $m$  es libre de cuadrado, debemos tener que todos los  $r_i = 1$  y que todos los  $p_i$  son primos distintos. El corolario del teorema 8.2 muestra, entonces, que  $G$  es isomorfo a  $\mathbb{Z}_{p_1 p_2 \cdots p_n}$ , de manera que  $G$  es cíclico. ■

## Ejercicios

---

9.1 Encuéntrense todos los grupos abelianos (salvo isomorfismo) de orden 720; de orden 1089. Exprésense en las formas 1 y 2 del lema 9.3 y apárelense los grupos isomorfos de la forma 1 y 2.

9.2 Encuéntrense los coeficientes de torsión y el número de betti del grupo

$$\mathbb{Z} \times \mathbb{Z}_6 \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}.$$

9.3 Encuéntrese el subgrupo de  $\mathbb{Z}_{12}$  generado por  $\{2, 3\}$ ; generado por  $\{4, 6\}$  y generado por  $\{8, 6, 10\}$ .

9.4 Encuéntrese el orden del subgrupo de torsión de  $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$ ; y de  $\mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12}$ .

9.5 Muéstrese que un grupo abeliano finito no es cíclico si y sólo si contiene algún subgrupo isomorfo a  $\mathbb{Z}_p \times \mathbb{Z}_p$  para algún primo  $p$ .

## 9.6 ¿Falso o verdadero?

- a) Todo grupo abeliano cuyo orden es un primo es cíclico.
  - b) Todo grupo abeliano cuyo orden es una potencia de un primo es cíclico.
  - c)  $\mathbb{Z}_8$  es generado por  $\{4, 6\}$ .
  - d)  $\mathbb{Z}_8$  es generado por  $\{4, 5, 6\}$ .
  - e) El lema 9.3 clasifica todos los grupos abelianos finitos (salvo isomorfismo).
  - f) Cualesquiera dos grupos abelianos finitamente generados con el mismo número de betti son isomorfos.
  - g) Todo grupo abeliano de orden divisible entre 5 contiene algún subgrupo cíclico de orden 5.
  - h) Todo grupo abeliano de orden divisible entre 4 contiene algún subgrupo cíclico de orden 4.
  - i) Todo grupo abeliano de orden divisible entre 6 contiene algún subgrupo cíclico de orden 6.
  - j) Todo grupo abeliano finito tiene número de betti 0.
- 

## 9.7 ¿Cuántos grupos abelianos de orden 24 (salvo isomorfismo) hay?; ¿y de orden 25?; ¿y de orden (24)(25)?

9.8 Siguiendo la idea sugerida en el ejercicio 9.7, sean  $m$  y  $n$  enteros positivos primos relativos. Muéstrese que existen  $r$  grupos abelianos (salvo isomorfismo) de orden  $m$  y  $s$  de orden  $n$ , entonces, hay (salvo isomorfismo)  $rs$  grupos abelianos de orden  $mn$ .

9.9 Empléese el ejercicio 9.8 para determinar el número de grupos abelianos (salvo isomorfismo) de orden (10)<sup>3</sup>.

9.10 Sea  $G$  un grupo abeliano de orden 72.

- a) ¿Cuántos subgrupos de orden 8 tiene  $G$ ? ¿Por qué?
- b) ¿Cuántos subgrupos de orden 4 tiene  $G$ ? ¿Por qué?

9.11 Pruébese que si un grupo finito abeliano tiene como orden la potencia de un primo  $p$ , entonces, el orden de todo elemento del grupo es una potencia de  $p$ .

9.12 ¿Para cuáles enteros positivos  $n$  es cierto que los únicos grupos abelianos de orden  $n$  son cílicos?

9.13 Sean  $p$  y  $q$  números primos distintos. ¿Cómo se puede comparar el número (salvo isomorfismo) de grupos abelianos de orden  $p^r$  con el número (salvo isomorfismo) de grupos abelianos de orden  $q^s$ ?

9.14 (Para estudiantes que sepan algo de números complejos, especialmente el teorema de De Moivre.) Encuéntrese el subgrupo de torsión  $T$  del grupo multiplicativo  $\mathbb{C}^*$  de números complejos distintos de cero.

9.15 Muéstrese que  $S_3$  está generado por  $\{(1, 2), (1, 2, 3, \dots, n)\}$ . [Sugerencia: muéstrese que conforme  $r$  varía,  $(1, 2, 3, \dots, n)^{r-1}(1, 2)(1, 2, 3, \dots, n)^r$  da todas las transposiciones  $(1, 2), (2, 3), (3, 4), \dots, (n-1, n), (n, 1)$ . Después, muéstrese que cualquier transposición es un producto de algunas de estas transposiciones y empléese el corolario del teorema 5.1.]

9.16 ¿Cuál es el número menor de elementos que puede emplearse para generar  $S_3$  del ejemplo 4.1?; ¿y para el grupo  $D_4$  de simetrías del cuadrado en el ejemplo 4.2?; ¿y para el grupo  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ?

## 96 GRUPOS ABELIANOS FINITAMENTE GENERADOS

9.17 ¿Dónde está el error en el argumento siguiente?

«Por el ejercicio 9.15,  $S_n$  puede ser generado por dos elementos. Por el teorema de Cayley, todo grupo finito es isomorfo a algún subgrupo de algún  $S_n$ . Por tanto, todo grupo finito puede ser generado por dos elementos.»

Nótese que la tercera parte del ejercicio 9.16 muestra que esta conclusión es falsa.

9.18 Sean  $G$ ,  $H$  y  $K$  grupos abelianos finitamente generados. Muéstrese que si  $G \times K \cong H \times K$  entonces  $G \cong H$ .

9.19 Sea, en  $\mathbb{Z} \times \mathbb{Z}$ ,  $G = \{(a, b) \mid a \equiv b \pmod{10}\}$ .

- Pruébese que  $G$  es un subgrupo de  $\mathbb{Z} \times \mathbb{Z}$  y es libre de torsión.
- Muéstrese que  $G$  es finitamente generado.
- Encuéntrese un isomorfismo  $\phi: G \rightarrow \mathbb{Z} \times \cdots \times \mathbb{Z}$  para algún número de factores.

\* 10

## Grupos en geometría y análisis

Interrumpimos nuestro estudio puramente algebraico para señalar, de manera un poco vaga, la importancia del concepto de grupo en geometría y en análisis. Puesto que no tratamos de profundizar en dichas materias, nuestro análisis no será muy preciso.

### \* 10.1 GRUPOS EN GEOMETRÍA

**Definición** Para un geómetra una *transformación de un conjunto A* es una permutación del conjunto, esto es, una función uno a uno de  $A$  sobre sí mismo.

Según el teorema 4.1, las transformaciones de un conjunto forman un grupo bajo la multiplicación de transformaciones (permutación). Hay que recordar que esta multiplicación no es más que la composición de funciones. Esto es, si  $\phi$  y  $\psi$  son transformaciones de  $A$ , entonces el producto  $\mu = \phi\psi$  se define por  $a\mu = (\phi\psi)a$  para  $a \in A$ .

Félix Klein (1849-1925) dio una famosa definición de una *geometría* en su discurso de aceptación de una cátedra en la Universidad de Erlangen (el *Erlanger Programm*), enero 1872. Desde la perspectiva del geómetra actual, la definición de Klein no es lo bastante inclusiva, pero servirá para nuestro propósito.

**Definición (Klein)** Una *geometría* es el estudio de aquellas propiedades de un espacio (conjunto) que permanecen invariantes bajo algún subgrupo fijo de todo el grupo de transformaciones.

Ilustraremos esta definición conforme se aplica a la geometría euclíadiana clásica de la recta, el plano, el espacio tridimensional euclidianos, y demás. Tenemos,

aquí, conjuntos en donde se define el concepto de *distanza entre elementos*. Si consideramos  $d(x, y)$  como la distancia entre los dos elementos  $x$  y  $y$ , entonces, podemos hablar acerca de transformaciones que conservan la distancia.

**Definición** Si  $A$  es un conjunto donde se ha definido el concepto de distancia, una transformación  $\phi$  de  $A$  es una *isometría* si  $d(x, y) = d(x\phi, y\phi)$ , esto es, si  $\phi$  preserva la distancia.

Es claro que el subconjunto de todo el grupo de transformaciones, formado por todas las isometrías del conjunto, es un subgrupo. La *geometría euclíadiana* de la recta, el plano, el espacio tridimensional y demás, es precisamente el estudio de aquellas propiedades que permanecen invariantes bajo el grupo de las isometrías. Así, en la geometría euclíadiana podemos hablar de los conceptos de longitud de un segmento de recta, del tamaño de un ángulo y del número de lados de un polígono, pues todas ellas son invariantes bajo isometría.

Describamos algunas de las isometrías del plano euclidiano. Una *traslación* del plano es una transformación que mueve cada punto una distancia fija en una dirección fija. En términos de coordenadas, una traslación  $\tau_{(a,b)}$  mueve el punto  $(x, y)$  hacia  $(x + a, y + b)$ . Es claro que

$$\tau_{(a,b)} \tau_{(c,d)} = \tau_{(a+c, b+d)}.$$

Se observa de inmediato que las traslaciones forman un subgrupo del grupo de las isometrías isomorfo a  $\mathbb{R} \times \mathbb{R}$  bajo la suma. Una *rotación*  $\rho_{(P,\theta)}$  es una transformación que rota el plano alrededor del punto  $P$  en sentido contrario al que giran las manecillas del reloj, en un ángulo  $\theta$ , donde  $0 \leq \theta < 2\pi$ . Las rotaciones no forman un subgrupo de las isometrías, pues  $\rho_{(P,\theta_1)} \rho_{(Q,\theta_2)}$  no es una rotación si  $P \neq Q$  y  $\theta_1 + \theta_2 = 2\pi$ . Pero es claro que

$$\rho_{(P,\theta_1)} \rho_{(P,\theta_2)} = \rho_{(P,\theta_1 + \theta_2 \bmod 2\pi)},$$

donde

$$(\theta_1 + \theta_2 \bmod 2\pi) = \begin{cases} \theta_1 + \theta_2 & \text{si } (\theta_1 + \theta_2) < 2\pi, \\ \theta_1 + \theta_2 - 2\pi & \text{si } (\theta_1 + \theta_2) \geq 2\pi. \end{cases}$$

Las rotaciones alrededor de un punto fijo  $P$  si forman un subgrupo de las isometrías. Este grupo no es isomorfo a  $\mathbb{R}$  bajo la suma, ya que tiene subgrupos cíclicos de orden finito. Por ejemplo,  $\rho_{(P,\pi/2)}$  genera un subgrupo cíclico de orden 4. Todas las rotaciones alrededor de un punto fijo forman, en realidad, un grupo isomorfo al grupo multiplicativo de números complejos con valor absoluto 1. Por último, una *reflexión* en el plano es una función  $\mu$  que transforma cada punto de una determinada recta  $l$  en sí mismo y a todo punto fuera de la recta a la imagen reflejada en el espejo  $l$  que queda a la misma distancia entre el punto y  $l$ , como se indica en la figura 10.1. Puede demostrarse que las traslaciones, rotaciones y reflexiones generan (en el sentido del capítulo 9) todo el grupo de las isometrías

del plano. En realidad, este conjunto de generadores es mayor de lo necesario. Se puede mostrar que bastan las reflexiones para generar el grupo de las isometrías, toda isometría en el plano se puede expresar como un producto de a lo más tres reflexiones. Es fácil convencerse de que, por ejemplo, una traslación puede escribirse como el producto de dos reflexiones en rectas perpendiculares a la dirección de la traslación, distantes la mitad de la longitud de la traslación. Remitimos al lector interesado a Coxeter [44].

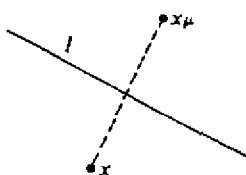


Figura 10.1

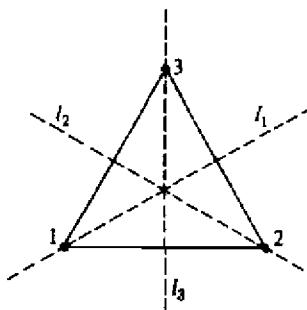


Figura 10.2

El grupo  $S_3$  dado en el ejemplo 4.1 tiene una bella interpretación geométrica. Considerérese un triángulo equilátero como el de la figura 10.2. Sea

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

donde  $\rho$  denota una rotación; podemos considerarla una rotación en sentido contrario al que giran las manecillas del reloj, en  $2\pi/3$  radianes. De manera análoga,

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

es una rotación en sentido contrario al que giran las manecillas del reloj, en  $4\pi/3$  radianes, y

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

es una rotación en 0 radianes. También,

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

donde  $\mu$  denota la imagen en el espejo, corresponde a una reflexión del triángulo en la recta  $I_1$  y, en general, cada  $\mu_i$  del ejemplo 4.1 es una reflexión en la recta  $I_i$ . Una reflexión  $\mu_i$  corresponde a girar el triángulo alrededor del eje  $I_i$ . Resulta clara la elección de la notación en el ejemplo 4.1. Véase de nuevo la tabla 4.1 del ejemplo 4.1. Nótese que se divide en cuatro sectores que señalamos sombreándolos. Este arreglo por sectores se muestra de nuevo en la tabla 10.1. En términos algebraicos, la tabla 10.1 presenta un grupo de orden 2. En términos geométricos, la tabla indica que el producto de dos rotaciones es una rotación; que el producto de una rotación y una reflexión es una reflexión y que el producto de dos reflexiones es una rotación. Esta descomposición del grupo en sectores que forman a su vez un grupo, será el siguiente tema de nuestro estudio algebraico.

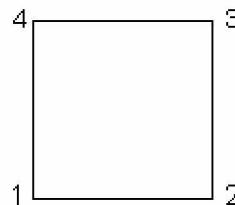
**Tabla 10.1**

	$\rho$ _términos	$\mu$ _términos
$\rho$ _términos	$\rho$ _términos	$\mu$ _términos
$\mu$ _términos	$\mu$ _términos	$\rho$ _términos

Una primera impresión podría ser que las simetrías de un cuadrado formarían  $S_4$ , pero hay que tener cuidado. La permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

no es una isometría del cuadrado de la figura 10.3, pues la distancia del vértice 1 al vértice 2 sería mayor que la distancia entre los vértices 1 y 3. El grupo de simetrías del cuadrado o grupo octal se calculó en el ejemplo 4.2. El cálculo del grupo diédrico de simetrías del  $n$ -ágono regular en el plano para  $n \geq 3$  aparecerá como ejercicio al final de esta sección. Nótese que el grupo de simetrías del  $n$ -ágono regular para  $n \geq 3$  es  $S_n$  sólo en el caso  $n = 3$ .

**Figura 10.3**

En términos geométricos, podemos recuperar  $S_4$ , como el grupo de simetrías del tetraedro regular; cada cara es un triángulo equilátero, como se muestra en la figura 10.4. Podría decirse que no es posible realizar la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

mediante un movimiento rígido, pero así como se tiene que salir del plano para voltear el triángulo equilátero y obtener todo  $S_3$ , también se debe salir del espacio tridimensional al espacio de cuatro dimensiones para «voltear» el tetraedro y obtener todo  $S_4$ . Esta permutación equivale a una reflexión en el plano que contiene a la recta que pasa por los vértices 1 y 4, perpendicular a la recta que pasa por los vértices 2 y 3.

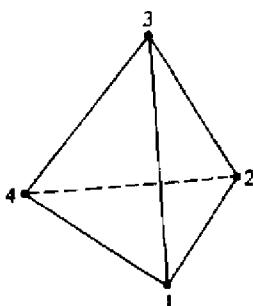


Figura 10.4

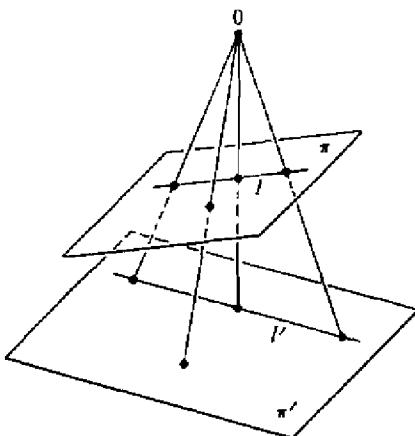
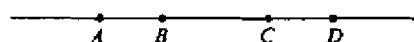


Figura 10.5

Daremos dos ilustraciones más de la definición de Klein. Si aumentamos el plano usual  $\mathbb{R} \times \mathbb{R}$  añadiendo una *recta al infinito* que contenga un punto para cada dirección en  $\mathbb{R} \times \mathbb{R}$ , obtenemos el **plano proyectivo**. En el plano proyectivo no existen objetos tales como rectas paralelas, ya que dos rectas paralelas en  $\mathbb{R} \times \mathbb{R}$ , en el plano proyectivo, se definen como rectas que se intersecan en el punto sobre la recta al infinito que corresponde a su dirección común. Ahora, sean  $\pi$  y  $\pi'$  dos planos proyectivos con sus partes correspondientes a  $\mathbb{R} \times \mathbb{R}$  vistas como parte del espacio tridimensional y como planos no necesariamente paralelos de este espacio. Una **proyección de  $\pi$  sobre  $\pi'$**  es una transformación de  $\pi$  sobre  $\pi'$  mediante la proyección de un punto fuera de ambos planos, o la proyección mediante rayos paralelos. En la figura 10.5 se ilustra la proyección desde un punto. Mediante dos proyecciones es posible proyectar  $\pi$  sobre  $\pi'$  y después devolver  $\pi'$  sobre  $\pi$ , la composición da una transformación de  $\pi$  sobre sí mismo. El **grupo de las transformaciones proyectivas de  $\pi$**  es el subgrupo de todas las transformaciones de  $\pi$  generadas por el tipo de transformaciones de  $\pi$  sobre sí mismo, recién descritas. Es claro que las rectas van a dar a rectas y los cuadriláteros a cuadriláteros, es decir, estos son conceptos de la *geometría proyectiva*. Sin embargo, no se preserva la distancia, de manera que la distancia no es un concepto de la geometría proyectiva. Es posible, en cambio, mostrar que la llamada *razón cruzada*

$$\frac{(CA/CB)}{(DA/DB)}$$

de cuatro puntos sobre una recta, como en la figura 10.6, es una invariante del grupo proyectivo. Esta razón cruzada es casi la única cantidad numérica de la cual se puede echar mano y, por tanto, desempeña un papel muy importante en geometría proyectiva.



**Figura 10.6**

Para concluir, si para un espacio dado podemos definir cuándo los puntos están cerca uno de otro, de manera que podamos hablar de *transformaciones continuas* (este conjunto es un espacio topológico), entonces es posible definir **topología** como el estudio de las propiedades de dichos espacios que son invariantes bajo el grupo de todas las transformaciones que son continuas y cuyas inversas también son continuas. La recta, el plano, el espacio tridimensional euclidianos y demás, son espacios topológicos. Dicho vagamente, una transformación continua con inversa continua es la que se logra doblando, estirando y torciendo el espacio sin rasgarlo ni cortarlo. Para los espacios euclidianos, estas transformaciones incluyen todas las isometrías y, para los planos proyectivos, incluyen todas las transformaciones proyectivas. Topológicamente no se puede diferenciar entre un balón de fútbol y uno de baloncesto, pues uno de ellos se puede deformar, sin romperse, hasta verse como el otro. De manera análoga, un cuadrado y un círculo son topológicamente iguales. Sin embargo, es imposible hacer que un disco sólido de chocolate con menta se vea como un dulce «salvavidas», sin agujerearlo. Entonces, son topológicamente distintos. La topología es, con mucho, el campo más activo hoy día entre todas las geometrías.

## \*10.2 GRUPOS EN ANÁLISIS

Pasando al tema del análisis, describiremos con brevedad algunas situaciones donde surgen los grupos de manera natural. De entrada, en análisis se trabaja, sobre todo, con subgrupos de números complejos, así que los grupos aparecen de manera obvia. Además, considérese la función  $f$  de una variable real dada por  $f(x) = \operatorname{sen} x$ . Tiene una gráfica bien conocida que se muestra en la figura 10.7. También,

$$\operatorname{sen} x = \operatorname{sen}(x + 2\pi n)$$

para todo entero  $n$ , esto es, la función *seno* de una variable real es invariante bajo una transformación de su dominio mediante un elemento del subgrupo cíclico infinito  $\langle 2\pi \rangle$  del grupo de traslaciones de  $\mathbb{R}$ . Una función de una variable real que sea invariante bajo una transformación de su dominio mediante un elemento de un grupo cíclico infinito es una función *periódica*.

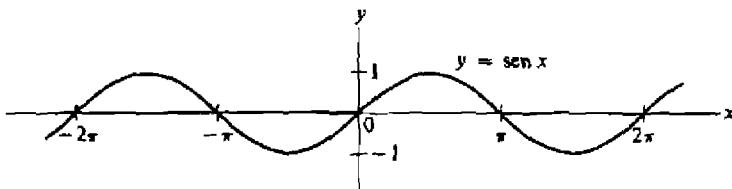


Figura 10.7

Recuérdese que los números complejos se pueden ver como llenando el plano euclíadiano. Una función doblemente periódica es una función en el plano, invariante bajo un elemento de un grupo de transformaciones generado por dos traslaciones en direcciones diferentes (pero no opuestas) (véase la figura 10.8). Aquí, el grupo es isomorfo a  $\mathbb{Z} \times \mathbb{Z}$ . Una función elíptica se define como una función de una variable compleja, meromorfa y doblemente periódica. El término *función meromorfa* se explica en un primer curso en nivel de licenciatura sobre la variable compleja. Así, una función elíptica se conoce donde sea si se conoce en una región fundamental, esto es, una de las regiones con forma de rombo de la figura 10.8. Tanto las funciones trigonométricas como las elípticas son casos particulares de *funciones automorfas*, que son las funciones invariantes bajo un grupo discreto de transformaciones. El término *discreto* significa, a grandes rasgos, que ningún par de elementos del grupo están cerca uno del otro.

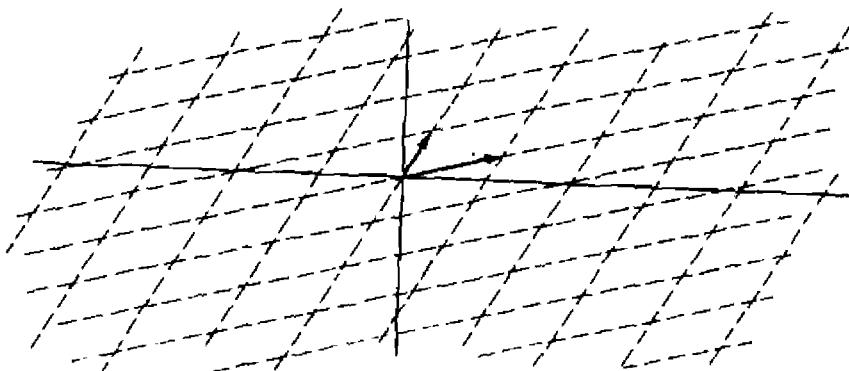


Figura 10.8

Por último, en *teoría de la medida* se asigna un tamaño numérico a ciertos subconjuntos «de buena conducta» de un conjunto. Si el conjunto tiene estructura de grupo  $\langle G, \cdot \rangle$  y si  $a$  es un elemento del grupo, en ocasiones conviene tener una medida tal que el tamaño del subconjunto  $S$  de  $G$  sea el mismo que el tamaño del subconjunto

$$aS = \{a \cdot s \mid s \in S\}.$$

Por analogía con  $R$  y la operación de suma, algunas veces llamamos a  $aS$  la **traslación izquierda de  $S$  mediante  $a$** , de manera similar,  $Sa$  es una **traslación derecha de  $S$  mediante  $a$** . Una **medida invariante izquierda** es una medida tal que el tamaño de  $aS$  es el mismo que el tamaño de  $S$  para toda  $a \in G$  y todo conjunto de buena conducta  $S$ . Se define de manera análoga una **medida invariante derecha**. Así, para  $R$  bajo la suma, nuestra idea común de tamaño (longitud) para conjuntos de buena conducta (intervalos) es una medida invariante izquierda y también derecha. De manera similar, nuestra idea usual de área en el plano  $C$  ( $\text{o } R \times R$ ) bajo la suma es una medida invariante izquierda y también derecha. Sin embargo, nuestra idea de área en  $C^*$ , el grupo de los números complejos distintos de cero bajo la multiplicación, esto es, el plano menos el origen, no es una medida invariante, ni izquierda, ni derecha. Por ejemplo, si  $S$  es el interior de un círculo de radio 1 alrededor del origen, sin el origen, tiene área  $\pi$ , mientras que  $2S$ , que tiene radio 2, tiene área  $4\pi$ . Sin embargo, Haar demostró que existe una medida invariante izquierda (y también una medida invariante derecha): la **medida de Haar en todo grupo topológico localmente compacto**<sup>1</sup>. La clasificación de **grupo topológico localmente compacto** cubre muchos grupos naturales compuestos de números complejos, incluyendo a  $C^*$ .

## Ejercicios

- \*10.1 Revisese el ejercicio 4.9, o hágase ahora si no se hizo antes.
- \*10.2 Muéstrese que el  $n$ -ésimo grupo diédrico  $D_n$  del ejercicio 4.9 puede generarse por dos elementos. Argúmense en términos geométricos.
- \*10.3 Revisese el ejercicio 4.10 o hágase ahora si no se hizo antes.
- \*10.4 Muéstrese que el grupo de movimientos rígidos del cubo dado en el ejercicio 4.10 puede generarse por dos elementos. Argúmense en términos geométricos.
- \*10.5 Considérese el grupo de *todas* las simetrías (isometrías) del cubo. Este grupo incluye todos los movimientos rígidos y también todas las reflexiones del cubo. ¿Cuál es el orden del grupo? Muéstrese que este grupo se puede generar por tres elementos.
- \*10.6 Considérese la *geometría afín finita* de cuatro puntos  $A, B, C, D$  y seis rectas  $AB, AC, AD, BC, BD, CD$  como se indica esquemáticamente en la figura 10.9. Aquí, cada recta contiene precisamente dos puntos. Una **colineación de una geometría afín** es una transformación uno a uno del conjunto de puntos sobre sí mismo que lleva rectas a rectas. (Para hacer este ejercicio, no es necesario saber lo que es en realidad un punto o una recta. Se basa en la idea intuitiva de que una recta se compone de puntos, etc.)
- a) Muéstrese que *toda* transformación uno a uno del conjunto de puntos de esta geometría afín de cuatro puntos, sobre sí misma, es una colineación.
- b) Muéstrese que para cualquier geometría afín, las colineaciones forman un grupo, el **grupo afín** bajo la composición de funciones.
- c) ¿A qué grupo visto anteriormente es isomorfo el grupo afín de la geometría de la figura 10.9?

<sup>1</sup> A. Haar, «Der Massbegriff in der Theorie der kontinuierlichen Gruppen», *Ann. of Math.* (2), 34, 147-169 (1933).

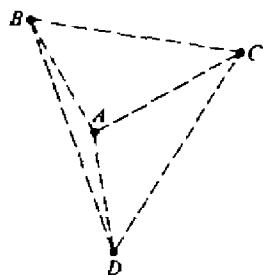


Figura 10.9

\*10.7 Siguiendo la idea del ejercicio 10.6, considérese la geometría afín de nueve puntos y doce rectas, cada una con tres puntos y cuyo esquema se presenta en la figura 10.10.

- Muéstrese que no toda transformación del conjunto de puntos sobre sí mismo, es una colineación para esta geometría de nueve puntos.
- Muéstrese que una colineación en esta geometría de nueve puntos está completamente determinada por sus valores en cualesquier tres puntos que no estén en la misma recta.
- ¿Cuál es el orden del grupo afín, esto es, del grupo de todas las colineaciones, para esta geometría de nueve puntos?
- Considérese el subgrupo  $H$  del grupo afín de la parte c) formado de aquellas colineaciones que dejan fijo cada punto de la recta  $ABC$ . ¿Cuál es el orden de este subgrupo? ¿A qué grupo definido anteriormente es isomorfo este subgrupo?

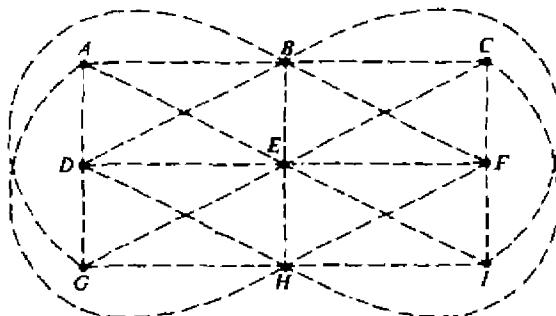


Figura 10.10

# Grupos de clases laterales

## 11.1 INTRODUCCIÓN

Quizás el lector ya haya observado que los 36 lugares de la tabla de  $S_3$  en el ejemplo 4.1 se dividieron, de manera natural en cuatro sectores, cada uno formado sólo por términos  $\rho_i$  o sólo por términos  $\mu_i$ . En la tabla 4.1 se sombrearon los sectores para distinguirlos. Así, el grupo  $S_3$  se partió en celdas  $B_\rho$  y  $B_\mu$  de igual tamaño y el conjunto  $\{B_\rho, B_\mu\}$  forma un grupo cuya tabla se obtiene de la tabla 4.1 y se muestra en la tabla 11.1. Esta partición de un grupo en celdas, tal que el conjunto de celdas forma a su vez un grupo, es un concepto de importancia básica en álgebra. Llamemos a cada elemento de una celda, un **representante de la celda**. La ecuación

$$B_\rho B_\mu = B_\mu$$

significa que *cualquier* representante de  $B_\rho$  multiplicado por *cualquier* representante de  $B_\mu$  da algún representante de  $B_\mu$ .

**Tabla 11.1**

	$B_\rho$	$B_\mu$
$B_\rho$	$B_\rho$	$B_\mu$
$B_\mu$	$B_\mu$	$B_\rho$

Pasando al caso general, nos gustaría determinar condiciones precisas bajo las cuales se puede partir un grupo  $G$  en celdas  $B_i$  tal que *cualquier* representante

de una celda fija  $B_s$ , multiplicado por cualquier representante de otra celda fija  $B_t$ , produzca siempre un representante de una y la misma celda  $B_t$ , la cual será entonces considerada como el producto  $B_s B_t$ . El producto de las celdas  $B_s B_t$  se define como la celda  $B_r$  obtenida al multiplicar representantes de  $B_s$  y  $B_t$ , y, para tener bien definida la operación binaria de multiplicación de celdas en  $\{B_i\}$ , como se explicó en el capítulo 1, la celda final  $B_r$  que contiene el producto de los representantes, debe ser la misma, sin importar los representantes escogidos de  $B_s$  y de  $B_t$ . Esta operación binaria de multiplicación de celdas en el conjunto  $\{B_i\}$  es la operación inducida en  $\{B_i\}$  por la operación de  $G$ . Sólo si esta operación está bien definida, tiene sentido preguntar si el conjunto  $\{B_i\}$  es un grupo bajo la operación.

**Teorema 11.1** Si un grupo  $G$  se puede partir en celdas donde la operación inducida descrita anteriormente está bien definida, y si las celdas forman un grupo bajo esta operación inducida, entonces, la celda que contiene la identidad e de  $G$  debe ser un subgrupo de  $G$ .

**Demostración** Supóngase que  $G$  está partido en celdas con la operación inducida bien definida y formando grupo, y sea  $B_e$  la celda que contiene la identidad. Al calcular  $B_e B_r$ , podemos tomar cualesquiera representantes de  $B_e$  y de  $B_r$ , y calcular su producto en  $G$ . Escojamos  $e \in B_e$  y, digamos,  $r \in B_r$ . Entonces,  $er = r$  y  $r \in B_r$ , así que  $B_e B_r = B_r$ . De manera análoga,  $B_r B_e = B_r$ . Así,  $B_e$  debe actuar como la celda identidad en el grupo de celdas. Por tanto,

$$B_e B_e = B_e.$$

lo cual muestra que, si elegimos todos los representantes posibles,  $B_e$  es cerrado bajo la multiplicación del grupo  $G$ .

Por definición,  $B_e$  contiene a  $e$ .

Sea  $a \in B_r$ . Ahora,  $a^{-1}$  está en alguna celda  $B_k$ . Como  $B_e$  es la celda identidad sabemos que  $B_e B_k = B_k$ . Al escoger representantes  $a \in B_r$  y  $a^{-1} \in B_k$  y usarlos para calcular  $B_e B_k$  se observa que necesariamente  $B_e B_k = B_r$ . Así,  $B_k = B_r$  y  $a^{-1} \in B_r$ .

Por tanto,  $B_e$  es un subgrupo de  $G$ . ■

## 11.2 CLASES LATERALES

Supóngase que se puede partir un grupo  $G$  en celdas, de modo que la operación inducida esté bien definida y forme un grupo. Sea  $B_e$  la celda que contiene a la identidad. El teorema anterior mostró que  $B_e$  es un subgrupo de  $G$ . Sea  $B_a$  la celda que contiene a  $a \in G$ . La ecuación  $B_a B_e = B_a$  muestra, si escogemos al representante  $a \in B_a$  y todos los representantes de  $B_e$ , que el conjunto

$$aB_e = \{ax \mid x \in B_e\}$$

debe estar contenido en  $B_a$ . Esto sugiere que estas *traslaciones* o *clases laterales*  $aH$  de un subgrupo  $H$  pueden ser importantes.

**Definición** Sea  $H$  un subgrupo de un grupo  $G$  y sea  $a \in G$ . La *clase lateral izquierda*  $aH$  de  $H$  es el conjunto  $\{ah \mid h \in H\}$ . La *clase lateral derecha*  $Ha$  se define de manera similar.

Hemos visto que si  $G$  se puede partir en celdas de modo que la operación inducida esté bien definida y forme un grupo, entonces

$$aB_\epsilon \subseteq B_a.$$

Sea  $a^{-1} \in B_k$ . Entonces,  $B_k B_a = B_\epsilon$ , de manera que al escoger representantes  $a^{-1} \in B_k$  y cualquier  $x \in B_a$ , tenemos  $a^{-1}x \in B_\epsilon$ . Así,  $a^{-1}x = b$  y  $x = ab$  donde  $b \in B_\epsilon$ . Esto muestra que

$$B_a \subseteq aB_\epsilon,$$

así que

$$B_a = aB_\epsilon$$

Claro que por un argumento similar también tenemos que  $B_a = B_\epsilon a$ . Estos resultados se resumen en un teorema.

**Teorema 11.2** Si un grupo  $G$  se puede partir en celdas de modo que la operación inducida esté bien definida y forme un grupo, entonces las celdas son precisamente las clases laterales izquierdas (y también las derechas) de un subgrupo de  $G$ . En particular, cada clase lateral izquierda debe ser una clase lateral derecha.

**Ejemplo 11.1** Determinemos cómo se ven las clases laterales izquierdas de  $3\mathbb{Z}$  como subgrupo de  $\mathbb{Z}$  bajo la suma. La notación es aditiva. Desde luego,  $3\mathbb{Z} = 0 + 3\mathbb{Z}$  es él mismo una clase lateral izquierda. Otra clase lateral izquierda es  $1 + 3\mathbb{Z}$ . Después de un momento de reflexión es claro que  $1 + 3\mathbb{Z}$  está formado por todos los enteros que dejan residuo 1 al dividirlos entre 3 en el sentido del lema 6.1. De igual manera, la clase lateral izquierda  $2 + 3\mathbb{Z}$  consta de todos los enteros que dejan residuo 2 al dividirlos entre 3. Puesto que el lema 6.1 muestra que el residuo de cualquier entero dividido entre 3 es un entero  $r$ , donde  $0 \leq r < 3$ , las únicas posibilidades son 0, 1 y 2. Así que éstas son todas las clases laterales izquierdas. ■

Podríamos preguntar en qué caso, dado un subgrupo  $H$  de un grupo  $G$ , las clases laterales izquierdas (o derechas) de  $H$  dan siempre una partición de  $G$  en celdas distintas. Claro está que por el teorema 0.1, cualquiera de dichas particiones corresponde a una relación de equivalencia en  $G$ . Nótese que  $b \in aH$  si y sólo si

$b = ah$  para algún  $h \in H$ , o si y sólo si  $a^{-1}b \in H$ . Esto sugiere examinar la relación  $a \sim b$  si y sólo si  $a^{-1}b \in H$ , para verificar si es una relación de equivalencia. Como se indica en el enunciado del teorema que sigue, esta relación tiene una notación especial.

**Teorema 11.3** *Sea  $H$  un subgrupo de un grupo  $G$ . Las relaciones*

$$a \equiv_{\ell} b \pmod{H} \quad \text{si y sólo si } a^{-1}b \in H$$

y

$$a \equiv_r b \pmod{H} \quad \text{si y sólo si } ab^{-1} \in H$$

*son relaciones de equivalencia en  $G$ , la congruencia izquierda módulo  $H$  y la congruencia derecha módulo  $H$ , respectivamente. Las clases de equivalencia de la congruencia izquierda (derecha) módulo  $H$  son las clases laterales izquierdas (derechas) de  $H$ . Todas las clases laterales de  $H$  tienen el mismo número de elementos.*

**Demostración** Probaremos el enunciado para la congruencia izquierda y las clases laterales izquierdas. Las demostraciones para la congruencia derecha y las clases laterales derechas son similares. Mostremos primero que la congruencia izquierda módulo  $H$  es una relación de equivalencia.

**Reflexividad.**  $a \equiv_{\ell} a \pmod{H}$  porque  $a^{-1}a = e$  está en  $H$ .

**Simetría.** Si  $a \equiv_{\ell} b \pmod{H}$ , entonces  $a^{-1}b \in H$  y  $H$  es un subgrupo, de modo que  $(a^{-1}b)^{-1} = b^{-1}a$  también está en  $H$ ; en consecuencia,  $b \equiv_{\ell} a \pmod{H}$ .

**Transitiva.** Si  $a \equiv_{\ell} b \pmod{H}$  y  $b \equiv_{\ell} c \pmod{H}$ , entonces  $a^{-1}b \in H$  y  $b^{-1}c \in H$ . Como  $H$  es un subgrupo,  $(a^{-1}b)(b^{-1}c) = a^{-1}c$  está en  $H$ , de modo que  $a \equiv_{\ell} c \pmod{H}$ .

Así, la congruencia izquierda módulo  $H$  es una relación de equivalencia.

La clase de equivalencia  $\bar{a}$  que contiene a  $a$  se calcula fácilmente como

$$\begin{aligned}\bar{a} &= \{x \in G \mid x \equiv_{\ell} a \pmod{H}\} = \{x \in G \mid a^{-1}x \in H\} \\ &= \{x \in G \mid a^{-1}x = h \in H\} = \{x \in G \mid x = ah \text{ para alguna } h \in H\} \\ &= aH.\end{aligned}$$

De este modo, las clases de equivalencia de la congruencia izquierda módulo  $H$  son precisamente las clases laterales izquierdas de  $H$ .

Para mostrar que cualesquiera dos clases laterales izquierdas tienen el mismo número de elementos, considérese la transformación  $\lambda_a: H \rightarrow aH$  dada por

$h\lambda_a = ah$ . Es claro que esta transformación  $\lambda_a$  es sobre  $aH$ . Si  $h_1$  y  $h_2$  están en  $H$  y  $ah_1 = ah_2$ , entonces  $h_1 = h_2$  debido a la ley de cancelación del grupo. Así,  $\lambda_a$  lleva a  $H$  de manera uno a uno y sobre  $aH$ . De aquí que toda clase lateral izquierda tiene el mismo número de elementos que  $H$  y, por tanto, todas ellas tienen el mismo número de elementos. ■

Ahora sabemos bastante bien cómo se ve la partición de un grupo en celdas ajenas, si la operación inducida está bien definida y forma grupo. Las celdas son siempre clases laterales (en este caso, por el teorema 11.2, las clases laterales izquierdas y derechas son las mismas) de algún subgrupo. A partir de ahora ya no usaremos el término *celda*; en su lugar usaremos siempre el término *clase lateral*.

Desafortunadamente, las clases laterales izquierdas de un subgrupo de un grupo no siempre forman grupo bajo la operación inducida. La dificultad radica en el hecho de que la operación inducida puede no estar bien definida. Daremos un ejemplo.

**Ejemplo 11.2** Considérese el grupo  $S_3$  del ejemplo 4.1 y el subgrupo  $H = \{\rho_0, \mu_1\}$ . Para encontrar las clases laterales izquierdas de un subgrupo  $H$  de un grupo finito  $G$ , se busca un elemento  $a$  de  $G$  que no esté en  $H$  y se encuentra la clase lateral izquierda  $aH$ . Después, se busca un  $b \in G$  tal que  $b$  no esté en  $H$  ni en  $aH$ , así encontramos una nueva clase lateral izquierda  $bH$ . Continuando este proceso, se hallan todas las clases laterales izquierdas de  $H$  en  $G$ . En el ejemplo es fácil observar que las clases laterales izquierdas de  $H = \{\rho_0, \mu_1\}$  en  $S_3$  son

$$\begin{aligned} H &= \{\rho_0, \mu_1\}, \\ \rho_1 H &= \{\rho_1, \mu_2\}, \\ \rho_2 H &= \{\rho_2, \mu_3\}. \end{aligned}$$

Escribamos de nuevo la tabla del grupo para  $S_3$ , pero con los elementos en el orden

$$\rho_0, \mu_1 | \rho_1, \mu_2 | \rho_2, \mu_3.$$

En la tabla 11.2 sombreados ligeralemente los cuadrados que contienen elementos de la clase lateral  $\{\rho_1, \mu_2\}$ , y oscurecemos más los que contienen elementos de  $\{\rho_2, \mu_3\}$ . Una mirada a la tabla bastará para ver si la operación inducida está bien definida y si estas clases laterales izquierdas forman un grupo. Vemos que no sucede así. El producto de dos celdas no siempre produce elementos de un solo tipo de sombreado, esto es, elementos en una sola clase lateral. Al multiplicar elementos en la clase lateral izquierda  $\{\rho_0, \mu_1\}$  por elementos en la clase lateral izquierda  $\{\rho_1, \mu_2\}$ , podemos obtener todos los elementos en  $\{\rho_1, \rho_2, \mu_2, \mu_3\}$  que no es una clase lateral izquierda. La operación inducida no está bien definida en estas clases laterales izquierdas. ■

Tabla 11.2

	$\rho_0$	$\mu_1$	$\rho_1$	$\mu_2$	$\rho_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\mu_1$	$\rho_1$	$\mu_2$	$\rho_2$	$\mu_3$
$\mu_1$	$\mu_1$	$\rho_0$	$\mu_3$	$\rho_2$	$\mu_2$	$\rho_1$
$\rho_1$	$\rho_1$	$\mu_2$	$\rho_3$	$\mu_3$	$\rho_0$	$\mu_1$
$\mu_2$	$\mu_2$	$\rho_1$	$\mu_1$	$\rho_0$	$\mu_3$	$\rho_2$
$\rho_3$	$\rho_3$	$\mu_3$	$\rho_0$	$\mu_1$	$\rho_1$	$\mu_2$
$\mu_3$	$\mu_3$	$\rho_2$	$\mu_2$	$\rho_1$	$\mu_1$	$\rho_0$

Tabla 11.3

	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

**Ejemplo 11.3** Veamos si el grupo  $Z_6$  se puede partir en un grupo de clases laterales izquierdas del subgrupo  $H = \{0, 3\}$ . Usando notación aditiva, las clases laterales izquierdas son

$$H = \{0, 3\},$$

$$1 + H = \{1, 4\},$$

$$2 + H = \{2, 5\}.$$

La tabla para  $Z_6$ , con los elementos en el orden

$$0, 3 | 1, 4 | 2, 5,$$

sombreado de nuevo los cuadrados según la clase lateral a que pertenece el elemento, se da en la tabla 11.3. ¡Funciona! ¿No es bello? Tan delicioso despliegue de simetría debería producir estremecimientos de felicidad subiendo y bajando por la columna vertebral de cualquiera que tenga algo de sensibilidad matemática. ■

Un grupo de clases laterales izquierdas formado a partir de un grupo  $G$  da alguna información acerca de  $G$ . Si sólo se conoce el grupo de las clases laterales izquierdas, no se puede saber cuál será el producto de cualesquiera dos elementos de  $G$ , pero sí se sabe el *tipo* de elemento resultante del producto de dos *tipos* de elementos. Esta es la importancia del concepto. Lo hemos ilustrado con  $S_3$ , donde los elementos son de dos tipos, del tipo  $\rho$  (rotaciones) y del tipo  $\mu$  (reflexiones). Otro análisis sería que los del tipo  $\rho$  son permutaciones pares y los del tipo  $\mu$  son permutaciones impares. El grupo dado por las dos clases laterales izquierdas de  $A_3$  en  $S_3$  tiene entonces una interpretación sencilla en términos de clasificación de productos de permutaciones en *pares* o *impares*, como se muestra en la tabla 11.4. No es sorprendente que los subgrupos cuyas clases laterales izquierdas forman grupo desempeñen un papel fundamental en la teoría de grupos.

Tabla 11.4

	Par	Impar
Par	Par	Impar
Impar	Impar	Par

Para terminar este análisis, haría falta caracterizar precisamente los tipos de subgrupos de un grupo  $G$  cuyas clases laterales si forman grupo bajo la operación inducida. Dejaremos esto para la siguiente sección, sobre todo porque éste es un material muy importante y queremos que haya tiempo suficiente para asimilarlo.

### 11.3 APLICACIONES

En vez de dar ahora los toques finales a esta teoría, probaremos algunos bellísimos resultados acerca de grupos finitos que resultan con mucha facilidad del trabajo desarrollado hasta aquí.

**Teorema 11.4 (Lagrange)** *Sea  $G$  un grupo de orden finito  $n$  y  $H$  un subgrupo de  $G$ . El orden de  $H$  divide al orden de  $G$ .*

**Demostración** Supóngase que  $H$  tiene  $m$  elementos. Considérese la colección de las clases laterales izquierdas de  $H$ . Por el teorema 11.3, estas clases laterales izquierdas son ajenas, tienen el mismo número  $m$  de elementos que  $H$  y todo elemento de  $G$  está en alguna clase lateral izquierda. Entonces, si hay  $r$  clases laterales izquierdas, debemos tener  $n = rm$  de modo que  $m$  divide a  $n$ . ■

Nótese que este elegante e importante teorema proviene del sencillo conteo hecho en el teorema 11.3 donde se demostró que todas las clases laterales tienen el mismo número de elementos. Nunca se debe subestimar un teorema que cuente algo.

El teorema 9.3 muestra que cualquier grupo *abeliano* de orden primo es cíclico. Pero como corolario del teorema 11.4 tenemos

**Corolario** *Todo grupo de orden primo es cíclico.*

**Demostración** Sea  $G$  de orden primo  $p$  y sea  $a$  un elemento de  $G$  diferente de la identidad. Entonces, el subgrupo cíclico  $\langle a \rangle$  de  $G$  generado por  $a$  tiene al menos dos elementos,  $a$  y  $e$ . Pero, por el teorema 11.4, el orden  $m \geq 2$  de  $\langle a \rangle$  debe dividir al primo  $p$ . Así, debemos tener que  $m = p$  y  $\langle a \rangle = G$ , de modo que  $G$  es cíclico. ■

*Por consiguiente, hay un solo grupo (salvo isomorfismo) de orden un primo dado.* Ahora bien, ¿no se obtuvo fácilmente este resultado elegante a partir del teorema

de Lagrange, un teorema que cuenta? Nunca se debe subestimar un teorema que cuenta algo. El corolario anterior es una pregunta típica de examen.

**Teorema 11.5** *El orden de un elemento de un grupo finito divide al orden del grupo.*

**Demostración** Si se recuerda que el orden de un elemento es igual al orden del subgrupo ciclico generado por el elemento, vemos que este teorema resulta directamente del teorema 11.4. ■

**Definición** Sea  $H$  un subgrupo de un grupo  $G$ . El número de clases laterales izquierdas de  $H$  en  $G$  es el *índice*  $(G : H)$  de  $H$  en  $G$ .

El índice  $(G : H)$  recién definido, puede ser finito o infinito. Si  $G$  es finito, es obvio que  $(G : H)$  es finito y  $(G : H) = |G|/|H|$ , ya que cada clase lateral de  $H$  tiene  $|H|$  elementos. El ejercicio 11.5 muestra que también se puede definir el índice  $(G : H)$  como el número de clases laterales derechas de  $H$  en  $G$ . Enunciaremos un teorema básico acerca de índices de subgrupos y dejaremos la demostración como ejercicio (véase el ejercicio 11.9).

**Teorema 11.6** *Supóngase que  $H$  y  $K$  son subgrupos de un grupo  $G$  tal que  $K \leq H \leq G$  y supóngase que  $(H : K)$  y  $(G : H)$  son ambos finitos. Entonces  $(G : K)$  es finito y  $(G : K) = (G : H)(H : K)$ .*

El teorema 11.4 muestra que si existe algún subgrupo  $H$  de un grupo finito  $G$ , entonces el orden de  $H$  divide al orden de  $G$ . Podríamos preguntarnos si el recíproco es cierto; esto es, si  $G$  es un grupo de orden  $n$ , y  $m$  divide a  $n$ , ¿existe siempre un subgrupo de orden  $m$ ? La respuesta es no, aunque del teorema 9.3 resulta que el recíproco sí es cierto para grupos abelianos (véase el teorema 9.5). Sin embargo, se puede mostrar que  $A_4$  no tiene subgrupo de orden 6, lo cual nos proporciona un contraejemplo para grupos no abelianos.

## Ejercicios

---

**11.1** Encuéntrese el número de clases laterales izquierdas de cada uno de los subgrupos siguientes:

- El subgrupo  $\langle 18 \rangle$  de  $\mathbb{Z}_{36}$
- El subgrupo  $\langle 1 \rangle \times \langle 0 \rangle \times \langle 0 \rangle$  de  $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4$
- El subgrupo  $\langle 0 \rangle \times \langle 1 \rangle \times \langle 2 \rangle$  de  $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4$

**11.2**  $H_1 = \{\rho_0, \rho_2\}$ ,  $H_2 = \{\rho_0, \mu_1\}$  y  $H_3 = \{\rho_0, \rho_1, \rho_2, \rho_3\}$  son tres subgrupos del grupo de simetrías del cuadrado del ejemplo 4.2: Para cada uno de estos subgrupos escribáse la tabla del grupo de simetrías del cuadrado de manera de exhibir las clases laterales izquierdas, como se hizo en los ejemplos 11.2 y 11.3, y determine en qué caso la operación inducida está bien definida y en qué caso las clases laterales izquierdas forman grupo. Si se usan colores diferentes para cada clase lateral, las tablas serán más llamativas.

11.3 Escribanse las clases laterales izquierdas del subgrupo cíclico  $\langle(1, 2)\rangle$  de  $Z_2 \times Z_4$  y determinese si la operación inducida está bien definida y si las clases laterales izquierdas forman grupo. Véase el ejercicio 11.2 respecto al uso de los colores.

11.4 ¿Cuántos grupos hay de orden 17 (salvo isomorfismo)?

11.5 Muéstrese que hay el mismo número de clases laterales izquierdas que derechas, de un subgrupo  $H$  de un grupo  $G$ , esto es, exhibir una transformación uno a uno de la colección de las clases laterales izquierdas sobre la colección de las clases laterales derechas. ( Nótese que este resultado es obvio para grupos finitos, basta contar. La demostración debe valer para cualquier grupo.)

11.6 ¿Falso o verdadero?

- a) Todo subgrupo de todo grupo tiene clases laterales izquierdas.
- b) El número de clases laterales izquierdas de un subgrupo de un grupo finito divide al orden del grupo.
- c) Todo grupo de orden primo es abeliano.
- d) No se pueden tener clases laterales izquierdas de un subgrupo finito de un grupo infinito.
- e) Un subgrupo de un grupo es una clase lateral izquierda de sí mismo.
- f) Sólo subgrupos de grupos finitos pueden tener clases laterales izquierdas.
- g)  $A_n$  es de índice 2 en  $S_n$  para  $n > 1$ .
- h) El teorema de Lagrange es un bello resultado.
- i) Todo grupo finito contiene algún elemento de todo orden que divide al orden del grupo.
- j) Todo grupo cíclico finito contiene algún elemento de todo orden que divide al orden del grupo.

11.7 En el ejercicio 2.5 se mostró que todo grupo finito de orden par  $2n$  contiene algún elemento de orden 2. Usando el teorema de Lagrange, pero no el teorema 9.3, muéstrese que si  $n$  es impar, un grupo abeliano de orden  $2n$  contiene precisamente un elemento de orden 2.

11.8 Muéstrese que un grupo con al menos dos elementos, pero sin subgrupos propios no triviales, debe ser finito y de orden primo.

11.9 Pruébese el teorema 11.6. [Sugerencia: sea  $\{a_iH | i = 1, \dots, r\}$  la familia de las distintas clases laterales izquierdas de  $H$  en  $G$  y  $\{b_jK | j = 1, \dots, s\}$  la colección de las distintas clases laterales izquierdas de  $K$  en  $H$ . Muéstrese que

$$\{(a_i b_j)K | i = 1, \dots, r; j = 1, \dots, s\}$$

es la colección de las distintas clases laterales izquierdas de  $K$  en  $G$ .]

11.10 Muéstrese que si  $H$  es un subgrupo de un grupo abeliano  $G$ , entonces, toda clase lateral izquierda de  $H$  es también una clase lateral derecha de  $H$ .

11.11 Muéstrese que si  $H$  es un subgrupo de índice 2 en un grupo finito  $G$ , entonces toda clase lateral izquierda de  $H$  es también una clase lateral derecha de  $H$ .

11.12 Empleando la notación para  $S_3$  del ejemplo 4.1 trátese de decidir, sin escribir la tabla, si la operación inducida está bien definida en las clases laterales izquierdas del subgrupo

$$\{(\rho_0, 0), (\rho_0, 3), (\rho_1, 0), (\rho_1, 3), (\rho_2, 0), (\rho_2, 3)\}$$

de  $S_3 \times \mathbb{Z}_6$  y si forman grupo. ¿Qué sucede con las clases laterales izquierdas de

$$\{(\rho_0, 0), (\rho_0, 3), (\mu_1, 0), (\mu_1, 3)\}?$$

**11.13** Muéstrese que las clases laterales izquierdas del subgrupo  $\{0\} \times \mathbb{Z}_2$  de  $\mathbb{Z} \times \mathbb{Z}_2$  forman un grupo isomorfo a  $\mathbb{Z}$ , bajo la operación inducida en las clases laterales izquierdas.

**11.14** Muéstrese que si un grupo  $G$  con identidad  $e$  tiene orden finito  $n$ , entonces  $a^n = e$  para todas las  $a \in G$ .

**11.15** Muéstrese que toda clase lateral izquierda del subgrupo  $\mathbb{Z}$  del grupo aditivo de los números reales, contiene exactamente un representante  $x$  en  $\mathbb{R}$  tal que  $0 \leq x < 1$ .

**11.16** Muéstrese que la función *seno* asigna el mismo valor a cada representante de cualquier clase lateral izquierda fija, del subgrupo  $\langle 2\pi \rangle$  del grupo aditivo  $\mathbb{R}$  de los números reales. (Así, el *seno* induce una función bien definida en el conjunto de las clases laterales; el valor de la función en una clase lateral se obtiene cuando escogemos un representante  $x$  de la clase lateral y calculamos  $\sin x$ .)

**11.17** Muéstrese que un grupo cíclico finito de orden  $n$  tiene exactamente un subgrupo de cada orden  $d$  que divide a  $n$  y que éstos son todos los subgrupos que tiene.

**11.18** La función *fi* de Euler se define para enteros positivos  $n$  mediante  $\phi(n) = s$  donde  $s$  es el número de enteros positivos menores o iguales a  $n$  que son primos relativos con  $n$ . Usese el ejercicio 11.17 para mostrar que

$$n = \sum_{d|n} \phi(d),$$

donde la suma se toma sobre todos los enteros positivos  $d$  que dividen a  $n$ . [Sugerencia: nótese que, por el corolario del teorema 6.4, el número de generadores de  $\mathbb{Z}_d$  es  $\phi(d)$ .]

**11.19** Sea  $G$  un grupo finito. Muéstrese que si para cada entero positivo  $m$  el número de soluciones  $x$  de la ecuación  $x^m = e$  en  $G$  es a lo más  $m$ , entonces,  $G$  es cíclico. [Sugerencia: úsese el teorema 11.5 y el ejercicio 11.18 para mostrar que  $G$  debe contener un elemento de orden  $n = |G|$ .]

# Subgrupos normales y grupos factores

## 12.1 CRITERIOS PARA LA EXISTENCIA DE UN GRUPO DE CLASES LATERALES

Regresemos ahora al problema de decidir para cuáles subgrupos  $H$  de un grupo  $G$  las clases laterales izquierdas (derechas) forman grupo bajo la operación inducida. La cuestión crucial es ver si la operación inducida está bien definida.

*Lema 12.1 Si  $H$  es un subgrupo de  $G$  y si la operación inducida de multiplicación de clases laterales en las clases laterales izquierdas (derechas) de  $H$  está bien definida, entonces la colección de clases laterales izquierdas (derechas) de  $H$  forman grupo bajo esta multiplicación de clases laterales inducida.*

*Demostración* Recuérdese que el producto  $(aH)(bH)$  de clases laterales izquierdas se definió como la clase lateral que contiene al producto de cualesquiera dos representantes, uno de  $aH$  y el otro de  $bH$ . Suponemos que este producto de clases laterales está bien definido, esto es, que es independiente de la selección de los representantes de  $aH$  y  $bH$ . Así, para propósitos de cálculo, podemos tomar a  $x$  como representante de la clase lateral  $xH$ .

La verificación de que se cumplen los axiomas de grupo para la colección de las clases laterales depende de que  $G$  satisfaga los axiomas de grupo, ya que la multiplicación de clases laterales está definida en términos de la multiplicación de los elementos de  $G$ . Para probar la ley asociativa debemos mostrar que

$$aH[(bH)(cH)] = [(aH)(bH)]cH.$$

Calculando, tenemos que

$$aH[(bH)(cH)] = (aH)(bcH) = a(bc)H.$$

Y también que

$$[(aH)(bH)](cH) = (abH)(cH) = (ab)cH.$$

Pero, por la ley asociativa en  $G$  sabemos que

$$a(bc) = (ab)c,$$

de modo que la multiplicación de clases laterales también es asociativa. Así mismo,  $eH$  actúa como identidad, pues el representante  $e$  actúa como identidad en  $G$  y el inverso de  $aH$  es  $a^{-1}H$ . ■

**Teorema 12.1** Si  $H$  es un subgrupo de un grupo  $G$ , entonces, la operación inducida de multiplicación está bien definida en las clases laterales izquierdas (derechas) de  $H$  si y sólo si toda clase lateral izquierda es una clase lateral derecha.

**Demostración** Supóngase que la operación inducida está bien definida. Entonces, por el lema 12.1 las clases laterales izquierdas (derechas) forman grupo, y por el teorema 11.2 las clases laterales izquierdas son las mismas que las clases laterales derechas.

En forma recíproca, supóngase que toda clase lateral izquierda  $aH$  es también una clase lateral derecha. Como  $g \in gH$  y la clase lateral derecha que contiene a  $g$  es  $Hg$ , donde  $g \in G$ , suponemos que como conjuntos  $gH = Hg$  para todas las  $g \in G$ . Queremos mostrar que al definir  $(aH)(bH)$  multiplicando representantes, la clase lateral izquierda donde se halla el producto de los representantes es la misma para todas las elecciones posibles de estos representantes. Para ello, supóngase que  $a_1$  y  $a_2$  son representantes de  $aH$ , y  $b_1$  y  $b_2$  son representantes de  $bH$ . Es necesario mostrar que  $a_1b_1$  y  $a_2b_2$  están en la misma clase lateral izquierda de  $H$ . Como  $aH = a_1H = a_2H$  y  $bH = b_1H = b_2H$ , podemos escribir  $a_1 = a_2h_1$  y  $b_1 = b_2h_2$  para algún  $h_1$  y  $h_2$  en  $H$ . Entonces,

$$a_1b_1 = a_2h_1b_2h_2.$$

Ahora, como por hipótesis  $b_2H = Hb_2$ , tenemos  $h_1b_2 = b_2h_3$  para algún  $h_3 \in H$ . Así,

$$a_1b_1 = a_2b_2h_3h_2, \quad \text{de modo que } a_1b_1 \in a_2b_2H,$$

esto es,  $a_1b_1$  y  $a_2b_2$  están en la misma clase lateral izquierda. Esto muestra que la operación inducida está bien definida. ■

## 12.2 AUTOMORFISMOS INTERNOS Y SUBGRUPOS NORMALES

Sabemos ahora que las clases laterales de un subgrupo  $H$  de un grupo  $G$  forman grupo bajo la operación inducida de multiplicación de clases laterales si y sólo si  $gH = Hg$  para toda  $g \in G$ . Puede reescribirse  $gH = Hg$  como  $H = g^{-1}Hg$  para todas las  $g \in G$ , donde, por supuesto,

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}.$$

Para comprender mejor el significado de  $g^{-1}Hg$  estudiaremos, para cada  $g \in G$ , la transformación  $i_g: G \rightarrow G$  dada por

$$xi_g = g^{-1}xg.$$

**Definición** Un isomorfismo de un grupo  $G$  en sí mismo es un *automorfismo del grupo  $G$* .

**Teorema 12.2** Para cada  $g \in G$ , la transformación  $i_g: G \rightarrow G$  dada por  $xi_g = g^{-1}xg$  es un automorfismo de  $G$ , el *automorfismo interno de  $G$  bajo la conjugación por  $g$* .

**Demostración** Debemos mostrar que  $i_g$  es un isomorfismo de  $G$  en sí mismo. La transformación está definida, así que mostremos que es uno a uno, sobre y que

$$(xy)i_g = (xi_g)(yi_g).$$

Primero, uno a uno, si  $xi_g = yi_g$ , entonces,  $g^{-1}xg = g^{-1}yg$  de modo que  $x = y$  por la ley de cancelación del grupo. Ahora, sobre, si  $x \in G$  entonces

$$(gxg^{-1})i_g = g^{-1}(gxg^{-1})g = x.$$

Por último,

$$(xy)i_g = g^{-1}xyg,$$

y también,

$$(xi_g)(yi_g) = (g^{-1}xg)(g^{-1}yg) = g^{-1}xyg. \blacksquare$$

Como un automorfismo de  $G$  es un isomorfismo de  $G$  en sí mismo, sólo intercambia los nombres de los elementos de  $G$ , preservando todas las características de la estructura algebraica. Esto es,  $i_g$  transformará un subgrupo de  $G$  uno a uno

sobre un subgrupo (posiblemente distinto) de  $G$ ; un elemento de orden  $n$  de  $G$  sobre un elemento de orden  $n$  (posiblemente distinto) en  $G$ , y así sucesivamente. Ahora, decir que  $gH = Hg$  es lo mismo que decir que

$$H = g^{-1}Hg = \{g^{-1}hg \mid h \in H\}.$$

Esto significa que  $i_g$  lleva a  $H$  sobre sí mismo. Ello no significa que por fuerza  $hi_g = h$  para todas las  $h \in H$ , sino que  $hi_g \in H$  para todas las  $h \in H$ . Esto es,  $g^{-1}Hg = H$  significa que  $i_g$  induce una permutación de  $H$ .

**Definición** Un subgrupo  $H$  de un grupo  $G$  es un *subgrupo normal* (o *invariante*) de  $G$  si  $g^{-1}Hg = H$  para todas las  $g \in G$ , esto es, si  $H$  permanece invariante bajo todo automorfismo interno de  $G$ .

Así, los subgrupos normales son precisamente aquellos subgrupos importantes de un grupo, con la propiedad de que para las clases laterales (izquierdas y derechas son las mismas), la operación inducida está bien definida y las clases laterales forman grupo.

Vale la pena notar que si  $H$  es un subgrupo de  $G$  tal que  $g^{-1}Hg \subseteq H$  para todas las  $g \in G$ , entonces,  $g^{-1}Hg = H$  para todas las  $g \in G$ , esto es,  $H$  es entonces un subgrupo normal de  $G$ . Para ello, supóngase que  $g^{-1}Hg \subseteq H$  para todas las  $g \in G$ . Deseamos mostrar que  $H \subseteq g^{-1}Hg$ . Sea  $h \in H$ . Entonces,  $(g^{-1})^{-1}Hg^{-1} \subseteq H$  y, por tanto,  $(g^{-1})^{-1}hg^{-1} = h_1$  y  $h_1 \in H$ . Luego,  $ghg^{-1} = h_1$  de manera que  $h = g^{-1}h_1g$  y  $h \in g^{-1}Hg$ . Por tanto, para mostrar que un subgrupo  $H$  de un grupo  $G$  es un subgrupo normal, se suele mostrar que  $g^{-1}hg \in H$  para todas las  $h \in H$  y todas las  $g \in G$ .

**Teorema 12.3** Todo subgrupo de un grupo abeliano es un subgrupo normal.

**Demostración** Es fácil, porque si  $H$  es un subgrupo de un grupo abeliano  $G$ , entonces para todas las  $g \in G$  y  $h \in H$  tenemos

$$g^{-1}hg = g^{-1}gh = gh = h. \blacksquare$$

**Ejemplo 12.1** El ejemplo 11.2 muestra que  $\{\rho_0, \mu_1\}$  no es un subgrupo normal de  $S_3$  del ejemplo 4.1. En efecto,

$$(\rho_1)^{-1}\mu_1\rho_1 = \rho_2\mu_1\rho_1 = \mu_2 \notin \{\rho_0, \mu_1\}.$$

Aquí  $i_{\rho_1}$  transforma  $\{\rho_0, \mu_1\}$  en el subgrupo  $\{\rho_0, \mu_2\}$ . ■

**Definición** Dos subgrupos  $H$  y  $K$  de un grupo  $G$  son *conjugados* si  $H = a^{-1}Ka$  para alguna  $a \in G$ , esto es, si uno se transforma en el otro mediante algún automorfismo interno de  $G$ .

Así, el ejemplo 12.1 muestra que  $\{\rho_0, \mu_1\}$  y  $\{\rho_0, \mu_2\}$  son subgrupos conjugados de  $S_3$  del ejemplo 4.1.

## 12.3 GRUPOS FACTORES

**Definición** Si  $N$  es un subgrupo normal de un grupo  $G$ , el grupo de las clases laterales de  $N$  bajo la operación inducida es el *grupo factor de  $G$  módulo  $N$*  y se denota por  $G/N$ . Las clases laterales son las *clases residuales de  $G$  módulo  $N$* .

**Ejemplo 12.2** Con referencia al ejemplo 11.1, vemos que como  $\mathbf{Z}$  es abeliano,  $3\mathbf{Z}$  es un subgrupo normal y así  $\mathbf{Z}/3\mathbf{Z}$  es el grupo factor de las tres clases residuales

$$0 + 3\mathbf{Z}, \quad 1 + 3\mathbf{Z}, \quad 2 + 3\mathbf{Z}.$$

Este es un grupo de orden 3 y, por tanto, es cíclico e isomorfo a  $\mathbf{Z}_3$ . ■

**Ejemplo 12.3** El subgrupo  $n\mathbf{Z}$  es normal en  $\mathbf{Z}$  para todas las  $n \in \mathbf{Z}^+$ . Hay  $n$  clases residuales:

$$0 + n\mathbf{Z}, \quad 1 + n\mathbf{Z}, \quad \dots, \quad (n - 1) + n\mathbf{Z}.$$

Como efectuamos la suma de clases residuales seleccionando representantes, es inmediato que la transformación  $\phi_n: \mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{Z}_n$  dada por

$$(m + n\mathbf{Z})\phi_n = m \quad \text{para } 0 \leq m < n$$

es un isomorfismo. ■

Por un abuso de notación, a veces escribimos  $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$  y pensamos a  $\mathbf{Z}_n$  como el grupo aditivo de clases residuales de  $\mathbf{Z}$  módulo  $\langle n \rangle$ , o de nuevo, por abuso de notación, como el grupo de clases residuales de  $\mathbf{Z}$  módulo  $n$ . Recuérdese del capítulo 0, que dos enteros  $a$  y  $b$  son congruentes módulo  $n$  y se denota  $a \equiv b \pmod{n}$ , si y sólo si  $n$  es divisor de  $a - b$ . Este es precisamente el criterio para que  $a$  y  $b$  estén en la misma clase lateral de  $\mathbf{Z}/n\mathbf{Z}$ .

Queremos señalar aquí que la construcción de  $\mathbf{Z}/n\mathbf{Z}$  es el enfoque *elegante* de la demostración de la existencia de un grupo cíclico de orden  $n$ , en oposición al enfoque intuitivo del teorema 6.3.

**Ejemplo 12.4** Calculemos el grupo factor  $(\mathbf{Z}_4 \times \mathbf{Z}_6)/\langle(0, 1)\rangle$ . Aquí,  $\langle(0, 1)\rangle$  es el subgrupo cíclico  $H$  de  $\mathbf{Z}_4 \times \mathbf{Z}_6$  generado por  $(0, 1)$ . Así,

$$H = \{(0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (0, 5)\}.$$

Como  $\mathbf{Z}_4 \times \mathbf{Z}_6$  tiene veinticuatro elementos y  $H$  tiene seis elementos, todas las clases laterales de  $H$  deben tener seis elementos y  $(\mathbf{Z}_4 \times \mathbf{Z}_6)/H$  debe tener orden 4. Como  $\mathbf{Z}_4 \times \mathbf{Z}_6$  es abeliano, también lo es  $(\mathbf{Z}_4 \times \mathbf{Z}_6)/H$  (recuérdese que se

calcula en un grupo factor mediante representantes del grupo original). «Calcular»  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$  significa determinar este grupo abeliano finito de acuerdo con la clasificación del teorema fundamental de los grupos abelianos finitamente generados (teorema 9.3). En notación aditiva, las clases laterales son

$$H = (0, 0) + H, \quad (1, 0) + H, \quad (2, 0) + H, \quad (3, 0) + H.$$

Como podemos calcular escogiendo los representantes  $(0, 0)$ ,  $(1, 0)$ ,  $(2, 0)$  y  $(3, 0)$ , es claro que  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$  es isomorfo a  $\mathbb{Z}_4$ . Nótese que esto era de esperarse, pues en un grupo factor módulo  $H$ , todo en  $H$  se convierte en la identidad, esto es, hacemos todo en  $H$  igual a cero. Así, todo el segundo factor  $\mathbb{Z}_6$  de  $\mathbb{Z}_4 \times \mathbb{Z}_6$  colapsa, dejando precisamente el primer factor  $\mathbb{Z}_4$ . Este es un ejemplo de la situación general dada en el teorema 12.7. ■

**Ejemplo 12.5** Calculemos el grupo factor  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 2)\rangle$ . Ahora bien, aquí  $(0, 2)$  genera el subgrupo

$$H = \{(0, 0), (0, 2), (0, 4)\}$$

de  $\mathbb{Z}_4 \times \mathbb{Z}_6$  de orden 3. Aquí no se altera el primer factor  $\mathbb{Z}_4$  de  $\mathbb{Z}_4 \times \mathbb{Z}_6$ . Por otro lado, el factor  $\mathbb{Z}_6$  esencialmente se colapsa por un subgrupo de orden 3, dando un grupo factor en el segundo factor de orden 2, que debe ser isomorfo a  $\mathbb{Z}_2$ . Por tanto,  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 2)\rangle$  es isomorfo a  $\mathbb{Z}_4 \times \mathbb{Z}_2$ . ■

**Ejemplo 12.6** Calculemos el grupo factor  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2, 3)\rangle$ . ¡Cuidado! Existe la tentación de decir que el 2 de  $\mathbb{Z}_4$  y el 3 de  $\mathbb{Z}_6$  se hacen ambos iguales a cero, de manera que  $\mathbb{Z}_4$  se colapsa a un grupo factor isomorfo a  $\mathbb{Z}_2$  y  $\mathbb{Z}_6$  a uno isomorfo a  $\mathbb{Z}_3$  dando un grupo factor total isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_3$ . ¡Esto es erróneo! Nótese que

$$H = \langle(2, 3)\rangle = \{(0, 0), (2, 3)\}$$

es de orden 2, de modo que  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2, 3)\rangle$  tiene orden 12, no 6. Hacer  $(2, 3)$  igual a cero no hace cero individualmente a  $(2, 0)$  y a  $(0, 3)$ , así que los factores no se colapsan por separado.

Los grupos abelianos posibles de orden 12 son  $\mathbb{Z}_4 \times \mathbb{Z}_3$  y  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$  y debemos decidir a cuál es isomorfo nuestro grupo factor. Estos dos grupos se distinguen de manera muy fácil porque  $\mathbb{Z}_4 \times \mathbb{Z}_3$  tiene un elemento de orden 4 y  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$  no lo tiene. Afirmamos que la clase lateral  $(1, 0) + H$  es de orden 4 en el grupo factor  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$ . Para encontrar la menor potencia de una clase lateral que dé la identidad en un grupo factor módulo  $H$ , debemos, escogiendo representantes, encontrar la menor potencia de un representante que esté en el subgrupo  $H$ . Es claro que,

$$4(1, 0) = (1, 0) + (1, 0) + (1, 0) + (1, 0) = (0, 0)$$

es la primera vez en que  $(1, 0)$ , sumado a sí mismo, da un elemento de  $H$ . Así,  $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2, 3)\rangle$  tiene un elemento de orden 4 y es isomorfo a  $\mathbb{Z}_4 \times \mathbb{Z}_3$ , o  $\mathbb{Z}_{12}$ . ■

**Ejemplo 12.7** Calculemos (esto es, clasifiquemos según el teorema 9.3) el grupo  $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 1)\rangle$ . Podemos visualizar  $\mathbb{Z} \times \mathbb{Z}$  como los puntos del plano con ambas coordenadas enteras, como se indican, con puntos, en la figura 12.1. El subgrupo  $\langle(1, 1)\rangle$  consta de aquellos puntos que están en la recta a  $45^\circ$  que pasa por el origen, indicada en la figura. La clase lateral  $(1, 0) + \langle(1, 1)\rangle$  consta de aquellos puntos sobre la recta a  $45^\circ$  que pasa por el punto  $(1, 0)$ , también mostrado en la figura. Para continuar, vemos con facilidad que cada clase lateral consta de aquellos puntos que están sobre una de las rectas a  $45^\circ$  de la figura. Podemos escoger los representantes

$$\dots, (-3, 0), (-2, 0), (-1, 0), (0, 0), (1, 0), (2, 0), (3, 0), \dots$$

de las clases laterales, para calcular en el grupo factor. Como estos representantes corresponden precisamente a los puntos de  $\mathbb{Z}$  sobre el eje  $x$ , se ve de inmediato, que el grupo factor  $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 1)\rangle$  es isomorfo a  $\mathbb{Z}$ . ■

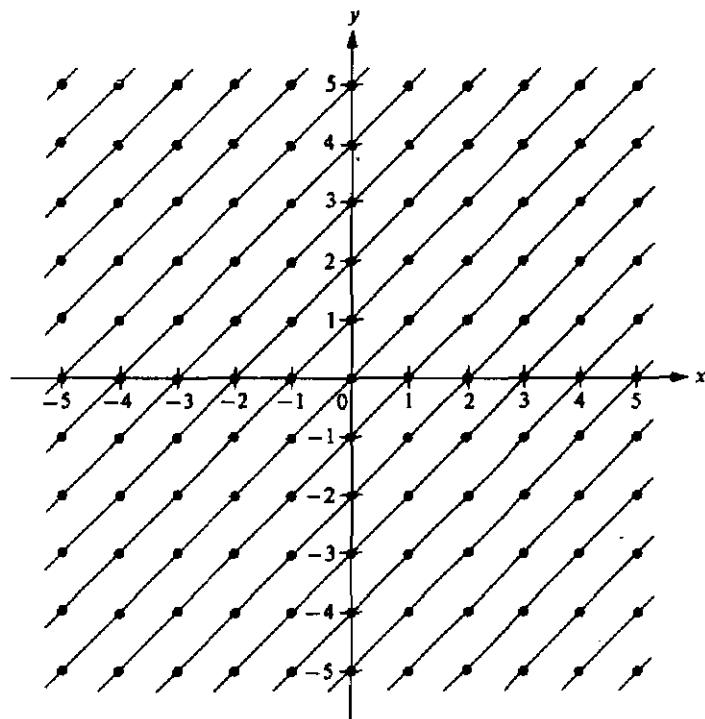


Figura 12.1

## 12.4 GRUPOS SIMPLES

Como se mencionó en la sección anterior, una característica de un grupo factor es que da información superficial acerca de la estructura de todo el grupo. Claro que en ocasiones no hay subgrupos normales propios no triviales. Por ejemplo, el teorema 11.4 muestra que un grupo de orden primo puede no tener subgrupos propios no triviales de ningún tipo.

**Ejemplo 12.8** Es claro que tanto el subgrupo impropio  $G$ , como el subgrupo trivial  $\{e\}$  de un grupo  $G$  son subgrupos normales. Es obvio que,  $G/G$  es el grupo trivial de un elemento mientras que  $G/\{e\}$  es isomorfo a  $G$  bajo la transformación natural que lleva a  $g\{e\}$  en  $g$  para cada  $g \in G$ . Estos grupos factores no son útiles para dar mayor información acerca de la estructura de  $G$ . ■

**Definición** Un grupo es *simple* si no tiene subgrupos normales propios no triviales.

**Teorema 12.4** El grupo alternante  $A_n$  es simple para  $n \geq 5$ .

**Demostración** Véase el ejercicio 22. ■

En el último capítulo del libro daremos un uso importante al teorema 12.4. Hay muchos otros grupos simples además de los dados con anterioridad. Por ejemplo,  $A_5$  es de orden 60 y  $A_6$  es de orden 360 y hay un grupo simple de orden no primo, a saber, 168, entre estos órdenes.

Recientemente se terminó la determinación y clasificación completa de todos los grupos simples finitos. Cientos de matemáticos han trabajado en esta tarea durante las últimas tres décadas. En el capítulo 14, al hablar de series de grupos, se indicará que un grupo finito tiene una especie de factorización en grupos simples, donde los factores son únicos salvo el orden. La situación es análoga a la factorización en primos de los enteros positivos. El nuevo conocimiento de todos los grupos simples finitos se puede usar ya para resolver algunos problemas de la teoría de grupos finitos.

Hemos visto en este libro que un grupo abeliano simple finito, es isomorfo a  $\mathbb{Z}_p$  para algún primo  $p$ . En 1964, Thompson y Feit [21] probaron una antigua conjectura de Burnside al mostrar que todo grupo simple no abeliano finito, es de orden par. Más adelante, en la década de los setenta, Aschbacher dio grandes pasos hacia la clasificación completa. A principios de 1980, Griess anunció que había construido un grupo simple «monstruo», ya predicho, de orden

$$808,017,424,794,512,875,886,459,904,961, \\ 710,757,005,754,368,000,000,000.$$

Aschbacher añadió los detalles finales de la clasificación, en agosto de 1980. Los artículos de investigación que contribuyen a la clasificación completa llenan, aproximadamente, cinco mil páginas de revistas especializadas.

## \*12.5 APLICACIONES

Durante el resto de esta sección, trataremos de ilustrar algunos otros aspectos de los grupos factores (probando subgrupos normales, cálculos con grupos factores, su importancia, usos y demás). Para ilustrar lo fácil que es calcular en un grupo factor, si es posible calcular en todo el grupo, probamos el siguiente teorema.

**Teorema 12.5** *Un grupo factor de un grupo cíclico es cíclico.*

**Demostración** Sea  $G$  cíclico, con generador  $a$  y sea  $N$  un subgrupo normal de  $G$ . Afirmando que la clase lateral  $aN$  genera a  $G/N$ . Debemos calcular todas las potencias de  $aN$ . Pero esto significa calcular, en  $G$ , todas las potencias del representante  $a$  y todas estas potencias dan todos los elementos de  $G$ . Por tanto, las potencias de  $aN$  dan todas las clases laterales de  $N$  y  $G/N$  es cíclico. ■

Nótese que al formar el grupo factor de  $G$  módulo un subgrupo  $N$ , esencialmente se están haciendo todos los elementos de  $G$  que están en  $N$ , iguales a  $e$ , así,  $N$  forma la nueva identidad en el grupo factor. Esto indica otro uso de los grupos factores. Supóngase, por ejemplo, que se estudia la estructura de un grupo no abeliano  $G$ . Como el teorema 9.3 da información completa acerca de la estructura de todos los grupos abelianos suficientemente pequeños, puede ser de interés tratar de formar un grupo abeliano lo más parecido a  $G$  que sea posible: una versión abelianizada de  $G$ , partiendo de  $G$  y después requiriendo que  $ab = ba$  para todas las  $a$  y  $b$  en la nueva estructura de grupo. Requerir que  $ab = ba$  es pedir que en el nuevo grupo  $aba^{-1}b^{-1} = e$ . Un elemento  $aba^{-1}b^{-1}$  en un grupo, es un **comutador del grupo**. Así, tratamos de formar una versión abelianizada de  $G$ , reemplazando todo comutador de  $G$  por  $e$ . Debido a la primera observación en este párrafo, deberíamos intentar entonces formar el grupo factor de  $G$  módulo el menor subgrupo normal que hallemos y que contenga a todos los comutadores de  $G$ .

**Teorema 12.6** *El conjunto de todos los comutadores  $aba^{-1}b^{-1}$  de un grupo  $G$  genera un subgrupo normal  $G'$  (el **subgrupo comutador**) de  $G$  y  $G/G'$  es abeliano. Más aún,  $G/N$  es abeliano si y sólo si  $G' \leq N$ .*

**Demostración** Sin duda, los comutadores generan un subgrupo  $G'$ ; debemos mostrar que es normal en  $G$ . Nótese que el inverso  $(aba^{-1}b^{-1})^{-1}$  de un comutador es otra vez un comutador, a saber,  $bab^{-1}a^{-1}$ . Además,  $e = eee^{-1}e^{-1}$  es un comutador. El teorema 9.1 muestra, entonces, que  $G'$  consta precisamente de todos los productos finitos de comutadores. Para  $x \in G'$  debemos mostrar que  $g^{-1}xg \in G'$ , para todas las  $g \in G$ , o que si  $x$  es un producto de comutadores también lo es  $g^{-1}xg$  para todas las  $g \in G$ . Insertando  $e = gg^{-1}$  entre cada

producto de conmutadores que se presente en  $x$  vemos que es suficiente mostrar para cada conmutador  $cdc^{-1}d^{-1}$ , que  $g^{-1}(cdc^{-1}d^{-1})g$  está en  $G'$ . Pero,

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}cdc^{-1})(e)(d^{-1}g) \\ &= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g], \end{aligned}$$

lo cual está en  $G'$ . Así,  $G'$  es normal en  $G$ .

El resto del teorema es obvio si ya se adquirió la sensibilidad adecuada acerca de grupos factores. Pero no se visualiza así, sino que la conclusión de que  $G/G'$  es abeliano, resulta de

$$\begin{aligned} (aG')(bG') &= abG' = ab(b^{-1}a^{-1}ba)G' \\ &= (abb^{-1}a^{-1})baG' = baG' = (bG')(aG'). \end{aligned}$$

Más aún, si  $G/N$  es abeliano, entonces  $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$ , esto es,  $aba^{-1}b^{-1}N = N$ , de modo que  $aba^{-1}b^{-1} \in N$  y  $G' \leq N$ . Por último, si  $G' \leq N$ , entonces

$$\begin{aligned} (aN)(bN) &= abN = ab(b^{-1}a^{-1}ba)N \\ &= (abb^{-1}a^{-1})baN = baN = (bN)(aN). \blacksquare \end{aligned}$$

**Teorema 12.7** Si  $G$  es el producto interno directo de los subgrupos  $H$  y  $K$ , entonces  $H$  y  $K$  son subgrupos normales de  $G$ . Además,  $G/H$  es isomorfo a  $K$  de manera natural.

*Demostración* Podemos considerar a  $G$  como isomorfo al producto directo externo  $H \times K$ . Necesitamos demostrar que  $\bar{H} = \{(h, e) | h \in H\}$  es normal en  $H \times K$  y que  $(H \times K)/\bar{H}$  es isomorfo a  $\bar{K} = \{(e, k) | k \in K\}$ .

Para la normalidad, es necesario mostrar que

$$(h, k)^{-1}\bar{H}(h, k) = \bar{H}$$

para todas las  $(h, k) \in H \times K$ . Pero,

$$\begin{aligned} (h, k)^{-1}(h_1, e)(h, k) &= (h^{-1}, k^{-1})(h_1, e)(h, k) \\ &= (h^{-1}h_1h, k^{-1}ek) = (h^{-1}h_1h, e), \end{aligned}$$

y  $(h^{-1}h_1h, e) \in \bar{H}$ . Así,  $\bar{H}$  es normal en  $H \times K$ . Es claro que todas las clases laterales de  $\bar{H}$  son de la forma  $(e, k)\bar{H}$  para  $k \in K$ . Es obvio que la transformación

$$\phi: \bar{K} \rightarrow (H \times K)/\bar{H} \quad \text{dada por} \quad (e, k)\phi = (e, k)\bar{H}$$

es un isomorfismo. ■

**Ejercicios**

A menudo, los estudiantes escriben tonterías cuando tienen que probar por primera vez teoremas acerca de grupos factores. Los primeros dos ejercicios están diseñados para llamar la atención acerca de un tipo elemental de error.

**12.1** Se pide a un estudiante mostrar que si  $H$  es un subgrupo normal de un grupo abeliano  $G$ , entonces  $G/H$  es abeliano. La demostración del estudiante comienza así:

Debemos mostrar que  $G/H$  es abeliano. Sean  $a$  y  $b$  dos elementos de  $G/H$ .

- Por qué, al leer esta demostración, el profesor espera encontrar tonterías a partir de ese momento en el trabajo del estudiante?
- ¿Qué debería haber escrito el estudiante?
- Complétense la demostración.

**12.2** Se pide a un estudiante probar que si  $G$  es un grupo de torsión, entonces  $G/H$  también lo es, para todo subgrupo normal  $H$  de  $G$ . El estudiante escribe:

Debemos demostrar que cada elemento de  $G/H$  es de orden finito. Sea  $x \in G/H$ .

Reséndanse las mismas preguntas del ejercicio 12.1.

**12.3** Complétense los enunciados.

- El grupo factor  $\mathbb{Z}_6/\langle 3 \rangle$  es de orden \_\_\_\_.
- El grupo factor  $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle (2) \times (2) \rangle$  es de orden \_\_\_\_.
- El grupo factor  $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle (2, 2) \rangle$  es de orden \_\_\_\_.
- La clase lateral  $5 + \langle 4 \rangle$  es de orden \_\_\_\_ en el grupo factor  $\mathbb{Z}_{12}/\langle 4 \rangle$ .
- La clase lateral  $26 + \langle 12 \rangle$  es de orden \_\_\_\_ en el grupo factor  $\mathbb{Z}_{60}/\langle 12 \rangle$ .

**12.4** Muéstrese que  $A_n$  es un subgrupo normal de  $S_n$  y calcúlese  $S_n/A_n$ , esto es, encontrar un grupo conocido al cual sea isomorfo  $S_n/A_n$ .

**12.5** Calcúlese (es decir, clasifíquese según el teorema 9.3) lo siguiente:

- $(\mathbb{Z} \times \mathbb{Z})/\langle (0, 1) \rangle$ .
- $(\mathbb{Z} \times \mathbb{Z})/\langle (1, 2) \rangle$ .
- $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle (1, 1, 1) \rangle$ .

**12.6** Este ejercicio ilustra el hecho de que si  $G$  contiene dos subgrupos normales isomorfos  $H$  y  $K$ , entonces  $G/H$  no necesariamente es isomorfo a  $G/K$ . Depende de la forma en que  $H$  y  $K$  están inmersos en  $G$ .

- Calcúlese  $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (1, 0) \rangle$ . Nótese que  $\langle (1, 0) \rangle$  es cíclico de orden 2. «Calcular» significa descubrir a cuál de los dos grupos (salvo isomorfismo) de orden 4 es isomorfo este grupo factor.
- Repítase la parte a) con  $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (0, 2) \rangle$ .
- Repítase la parte a) con  $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (1, 2) \rangle$ .

**12.7** Encuéntrense todos los subgrupos de  $S_3$  del ejemplo 4.1 que sean conjugados a  $\{\rho_0, \mu_1\}$ .

**12.8** Pruébese que el subgrupo de torsión  $T$  de un grupo abeliano  $G$  es un subgrupo normal de  $G$  y que  $G/T$  es libre de torsión. (Nótese que no se puede usar el lema 9.1, pues  $G$  puede no ser finitamente generado. Procédase directamente a partir de las definiciones)

de un grupo de torsión y de un subgrupo normal. No hay que cometer los errores que cometieron los estudiantes en los ejercicios 12.1 y 12.2.)

**12.9** ¿Falso o verdadero?

- a) Tiene sentido hablar del grupo factor  $G/N$  si y sólo si  $N$  es un subgrupo normal del grupo  $G$ .
  - b) Todo subgrupo de un grupo abeliano  $G$  es un subgrupo normal de  $G$ .
  - c) Un automorfismo interno de un grupo abeliano debe ser precisamente la transformación identidad.
  - d) Todo grupo factor de un grupo finito es de orden finito.
  - e) Todo grupo factor de un grupo de torsión es un grupo de torsión.
  - f) Todo grupo factor de un grupo libre de torsión es libre de torsión.
  - g) Todo grupo factor de un grupo abeliano es abeliano.
  - h) Todo grupo factor de un grupo no abeliano es no abeliano.
  - i)  $\mathbb{Z}/n\mathbb{Z}$  es cíclico de orden  $n$ .
  - j)  $\mathbb{R}/n\mathbb{R}$  es cíclico de orden  $n$ , donde  $n\mathbb{R} = \{nr \mid r \in \mathbb{R}\}$  y se considera  $\mathbb{R}$  bajo la suma.
- 

**12.10** Describanse todos los subgrupos de orden  $\leq 4$  de  $\mathbb{Z}_4 \times \mathbb{Z}_4$  y en cada caso clasifíquese el grupo factor de  $\mathbb{Z}_4 \times \mathbb{Z}_4$  módulo el subgrupo según el teorema 9.3 parte 1. Esto es, describase el subgrupo y digase que el grupo factor de  $\mathbb{Z}_4 \times \mathbb{Z}_4$  módulo el subgrupo es isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_4$ , o a lo que sea el caso. [Sugerencia:  $\mathbb{Z}_4 \times \mathbb{Z}_4$  tiene seis subgrupos cíclicos diferentes de orden 4. Describanse, dando un generador, como el subgrupo  $\langle(1, 0)\rangle$ . Hay un subgrupo de orden 4 isomorfo al 4-grupo de Klein. Hay tres subgrupos de orden 2.]

**12.11** Sea  $H$  un subgrupo normal de un grupo finito  $G$  y sea  $m = (G : H)$ . Muéstrese que  $a^m \in H$  para toda  $a \in G$ .

**12.12** Muéstrese que una intersección de subgrupos normales de un grupo  $G$  es, de nuevo, un subgrupo normal de  $G$ .

**12.13** Muéstrese que tiene sentido hablar del menor subgrupo normal de un grupo  $G$ , que contiene un subconjunto dado  $S$  de  $G$ . [Sugerencia: úsese el ejercicio 12.12.]

**12.14** Muéstrese que si un grupo finito  $G$  tiene exactamente un subgrupo  $H$  de un orden dado, entonces  $H$  es un subgrupo normal de  $G$ .

**12.15** Muéstrese que si un grupo finito  $G$  contiene un subgrupo propio de índice 2 en  $G$ , entonces  $G$  no es simple.

**12.16** Muéstrese que si  $H$  y  $N$  son subgrupos de un grupo  $G$ , y  $N$  es normal en  $G$ , entonces  $H \cap N$  es normal en  $H$ . Muéstrese, con un ejemplo, que  $H \cap N$  no necesariamente es normal en  $G$ .

**12.17** Sea  $G$  un grupo que contiene al menos un subgrupo de orden finito  $s$ . Muéstrese que la intersección de todos los subgrupos de  $G$  de orden  $s$  es un subgrupo normal de  $G$ . [Sugerencia: tómese en cuenta el hecho de que si  $H$  tiene orden  $s$  entonces también lo tiene  $x^{-1}Hx$  para todas las  $x \in G$ .]

**12.18** a) Muéstrese que todos los automorfismos de un grupo  $G$  forman un grupo bajo la composición de funciones.

b) Muéstrese que los automorfismos internos de un grupo  $G$  forman un subgrupo normal del grupo de todos los automorfismos de  $G$  bajo la composición de funciones.

## 128 SUBGRUPOS NORMALES Y GRUPOS FACTORES

[Advertencia: asegúrese de demostrar que los automorfismos internos forman un subgrupo.]

**12.19** Muéstrese que el conjunto de todas las  $g \in G$  tales que  $i_g: G \rightarrow G$  es el automorfismo interno identidad  $j_e$  es un subgrupo normal del grupo  $G$ .

**12.20** Sea  $G$  un grupo. Muéstrese que la relación  $a \sim b$  si y sólo si  $a = g^{-1}bg$  para alguna  $g \in G$  es una relación de equivalencia en  $G$ . Algunas clases de equivalencia contienen sólo un elemento  $c$ . Caracterízense dichos elementos  $c$ .

**12.21** Sea  $G$  un grupo. Muéstrese que la relación  $A \sim B$  si y sólo si  $A$  y  $B$  son subgrupos conjugados de  $G$ , de manera que  $A = g^{-1}Bg$  para alguna  $g \in G$ , es una relación de equivalencia en la colección de todos los subgrupos de  $G$ . Algunas clases de equivalencia pueden contener un solo subgrupo  $K$ . Caracterízense dichos subgrupos  $K$ .

**12.22** Pruébese que  $A_n$  es simple para  $n \geq 5$ . Sigáse los pasos y las sugerencias siguientes.

- Muéstrese que  $A_n$  contiene a todo 3-ciclo si  $n \geq 3$ .
- Muéstrese que  $A_n$  está generado por los 3-ciclos para  $n \geq 3$ . [Sugerencia: nótese que  $(a, b)(c, d) = (a, c, d)(a, c, b)$  y que  $(a, b)(a, c) = (a, b, c)$ .]
- Sean  $r$  y  $s$  elementos fijos de  $\{1, 2, \dots, n\}$  para  $n \geq 3$ . Muéstrese que  $A_n$  está generado por los  $n$  ciclos «especiales» de orden 3 de la forma  $(r, s, i)$  para  $1 \leq i \leq n$ . [Sugerencia: muéstrese que todo 3-ciclo es producto de 3-ciclos «especiales», calculando]

$$(r, s, i)^2, \quad (r, s, i)^2(r, s, j), \quad (r, s, i)(r, s, j)^2,$$

y

$$(r, s, i)(r, s, j)^2(r, s, k)(r, s, l)^2.$$

Obsérvese que estos productos dan todos los tipos posibles de 3-ciclos.]

- Sea  $N$  un subgrupo normal de  $A_n$  para  $n \geq 3$ . Muéstrese que si  $N$  contiene algún 3-ciclo entonces  $N = A_n$ . [Sugerencia: muéstrese que  $(r, s, i) \in N$  implica que  $(r, s, j) \in N$  para  $j = 1, 2, \dots, n$ , calculando  $((i, j)(r, s))^{-1}(r, s, i)^2((i, j)(r, s))$ .]
- Sea  $N$  un subgrupo normal de  $A_n$  para  $n \geq 5$ . Muéstrese que debe ser cierto alguno de los casos siguientes y conclúyase en cada caso que  $N = A_n$ .

Caso 1  $N$  contiene un 3-ciclo.

Caso 2  $N$  contiene un producto de ciclos ajenos y al menos uno de ellos tiene longitud mayor que 3. [Sugerencia: supóngase que  $N$  contiene el producto ajeno  $\sigma = (a_1, a_2, \dots, a_r)\mu$ . Muéstrese que  $(a_1, a_2, a_3)^{-1}\sigma(a_1, a_2, a_3)\sigma^{-1}$  está en  $N$  y calcúlese.]

Caso 3  $N$  contiene un producto ajeno de la forma  $\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)\mu$ . [Sugerencia: muéstrese que  $(a_1, a_2, a_3)^{-1}\sigma(a_1, a_2, a_3)\sigma^{-1}$  está en  $N$  y calcúlese.]

Caso 4  $N$  contiene un producto ajeno de la forma  $\sigma = (a_1, a_2, a_3)\mu$  donde  $\mu$  es un producto de 2-ciclos ajenos. [Sugerencia: muéstrese que  $\sigma^2 \in N$  y calcúlese.]

Caso 5  $N$  contiene un producto ajeno  $\sigma$  de la forma  $\sigma = (a_1, a_2)(a_3, a_4)\mu$  donde  $\mu$  es un producto de un número par de 2-ciclos ajenos. [Sugerencia: muéstrese que  $(a_1, a_2, a_3)^{-1}\sigma(a_1, a_2, a_3)\sigma^{-1}$  está en  $N$  y calcúlese para deducir que  $\alpha = (a_1, a_2)(a_3, a_4)$  está en  $N$ . Usando por primera vez que  $n \geq 5$ , encuéntrese  $i \in \{1, 2, \dots, n\}$  tal que  $i \neq a_1, a_2, a_3, a_4$ . Sea  $\beta = (a_1, a_3, i)$ . Muéstrese que  $\beta^{-1}\alpha\beta \in N$  y calcúlese.]

- \***12.23** Encuéntrese el subgrupo comutador  $G'$  del grupo  $D_4$  de simetrías del cuadrado del ejemplo 4.2.

- \*12.24 a) Muéstrese que si  $N$  es un subgrupo normal de  $G$  y  $H$  es cualquier subgrupo de  $G$ , entonces  $HN = NH = N \vee H$ .
- b) Muéstrese que si  $N$  y  $M$  son subgrupos normales de  $G$ , entonces  $NM$  también es un subgrupo normal de  $G$ .
- \*12.25 Muéstrese que si  $H$  y  $K$  son subgrupos normales de un grupo  $G$  tal que  $H \cap K = \{e\}$ , entonces  $hk = kh$  para todas las  $h \in H$  y  $k \in K$ . [Sugerencia: considérese el comutador  $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$ .]

## Homomorfismos

### 13.1 DEFINICIÓN Y PROPIEDADES ELEMENTALES

Un isomorfismo entre un grupo  $G$  y un grupo  $G'$  se definió como una transformación  $\phi$  uno a uno de  $G$  sobre  $G'$  tal que para todas las  $a$  y  $b$  en  $G$ ,  $(ab)\phi = (a\phi)(b\phi)$ . Si se anula la condición de que  $\phi$  sea uno a uno y sobre y nos quedamos con  $(ab)\phi = (a\phi)(b\phi)$ , entonces, la transformación  $\phi$  es un *homomorfismo*. Como veremos, los homomorfismos están intimamente relacionados con los grupos factores.

**Definición** Una transformación  $\phi$  de un grupo  $G$  en un grupo  $G'$  es un *homomorfismo* si

$$(ab)\phi = (a\phi)(b\phi)$$

para todos los elementos  $a$  y  $b$  en  $G$ .

Examinemos la idea que hay detrás de la condición  $(ab)\phi = (a\phi)(b\phi)$  para que  $\phi: G \rightarrow G'$  sea homomorfismo. Esta condición es lo único que distingue a un homomorfismo de una simple transformación de  $G$  en  $G'$ . Asegura que  $\phi$  es una transformación que relaciona estructuras. La estructura algebraica de  $G$  está por completo determinada por la operación binaria en  $G$ , y la de  $G'$  está por completo determinada por la operación binaria en  $G'$ . En la condición  $(ab)\phi = (a\phi)(b\phi)$ , la operación  $ab$  en el lado izquierdo ocurre en  $G$ , mientras que la operación  $(a\phi)(b\phi)$  del lado derecho, ocurre en  $G'$ . Así, la condición para ser homomorfismo relaciona la estructura de  $G$  con la de  $G'$ .

**Ejemplo 13.1** La transformación natural  $\gamma$  de  $\mathbf{Z}$  en  $\mathbf{Z}_n$  dada por  $my = r$  donde  $r$  es el residuo (en el sentido del lema 6.1) de  $m$  al dividirlo entre  $n$ , es un homomorfismo. Es necesario observar que

$$(s + t)\gamma = s\gamma + t\gamma.$$

Si

$$(1) \quad s = q_1 n + r_1 \quad y \quad (2) \quad t = q_2 n + r_2$$

para  $0 \leq r_i < n$ , entonces  $s\gamma = r_1$  y  $t\gamma = r_2$ . Así,

$$s\gamma + t\gamma = (r_1 + r_2) \text{ módulo } n.$$

Esto es, si  $r_1 + r_2 = q_3 n + r_3$  para  $0 \leq r_3 < n$ , entonces

$$s\gamma + t\gamma = r_3.$$

Sumando las ecuaciones (1) y (2) obtenemos

$$s + t = (q_1 + q_2)n + r_1 + r_2 = (q_1 + q_2 + q_3)n + r_3$$

y  $0 \leq r_3 < n$ . Así, también tenemos

$$(s + t)\gamma = r_3.$$

Si consideramos  $\mathbf{Z}_n$  como el grupo  $\mathbf{Z}/n\mathbf{Z}$  de clases residuales módulo  $n$ , vemos que  $\gamma$  asigna a cada elemento de  $\mathbf{Z}$  la clase lateral o clase residual módulo  $n$  en la cual aparece. Este es un ejemplo de la situación general descrita en el siguiente teorema. ■

**Teorema 13.1** Si  $N$  es un subgrupo normal de un grupo  $G$ , entonces la transformación canónica (o natural)  $\gamma: G \rightarrow G/N$  dada por  $a\gamma = aN$  para  $a \in G$ , es un homomorfismo.

**Demostración** Esto es una consecuencia inmediata de la definición de multiplicación de clases laterales en términos de multiplicación de representantes, pues

$$(ab)\gamma = abN = (aN)(bN) = (a\gamma)(b\gamma). \blacksquare$$

**Definición** El *kernel* de un homomorfismo  $\phi$  de un grupo  $G$  en un grupo  $G'$  es el conjunto de elementos de  $G$  cuya imagen, bajo  $\phi$ , es el elemento identidad de  $G'$ .

**Ejemplo 13.2** Para la transformación canónica  $\mathbf{Z} \rightarrow \mathbf{Z}_n$  dada en el ejemplo 13.1 el kernel es  $n\mathbf{Z}$ . Nótese que  $n\mathbf{Z}$  es un subgrupo normal de  $\mathbf{Z}$  y que  $\mathbf{Z}/n\mathbf{Z}$  es isomorfo a  $\mathbf{Z}_n$ . ■

El ejemplo anterior ilustra la conexión general entre homomorfismos y grupos factores que enunciaremos y probaremos en el teorema 13.3.

**Definición** Sea  $\phi$  una transformación de un conjunto  $X$  en un conjunto  $Y$  y sea  $A \subseteq X$  y  $B \subseteq Y$ . La *imagen  $A\phi$  de  $A$  en  $Y$  bajo  $\phi$*  es  $\{a\phi \mid a \in A\}$ . La *imagen inversa  $B\phi^{-1}$  de  $B$  en  $X$*  es  $\{x \in X \mid x\phi \in B\}$ .

El siguiente teorema proporciona algunas características estructurales preservadas bajo un homomorfismo.

**Teorema 13.2** Sea  $\phi$  un homomorfismo de un grupo  $G$  en un grupo  $G'$ . Si  $e$  es la identidad en  $G$ , entonces  $e\phi$  es la identidad en  $G'$  y si  $a \in G$ , entonces  $a^{-1}\phi = (a\phi)^{-1}$ . Si  $H$  es un subgrupo de  $G$ , entonces  $H\phi$  es un subgrupo de  $G'$ , y  $H$  normal en  $G$  implica que  $H\phi$  es normal en  $G'\phi$ . Ahora, en la otra dirección, si  $K'$  es un subgrupo de  $G'$ , entonces  $K'\phi^{-1}$  es un subgrupo de  $G$  y  $K'$  normal en  $G\phi$  implica que  $K'\phi^{-1}$  es normal en  $G$ . Dicho brevemente, bajo un homomorfismo, subgrupos corresponden a subgrupos y subgrupos normales a subgrupos normales.

**Demostración** Sea  $\phi$  un homomorfismo de  $G$  en  $G'$ . Entonces,

$$a\phi = (ae)\phi = (a\phi)(e\phi).$$

De aquí que  $e\phi$  debe ser la identidad  $e'$  en  $G'$ . La ecuación

$$e\phi = (aa^{-1})\phi = (a\phi)(a^{-1}\phi)$$

muestra que  $a^{-1}\phi = (a\phi)^{-1}$ .

Sea  $H$  un subgrupo de  $G$  y sean  $a\phi$  y  $b\phi$  dos elementos cualesquiera en  $H\phi$ . Entonces,  $(ab)\phi = (a\phi)(b\phi)$  de modo que  $(a\phi)(b\phi) \in H\phi$ , esto es,  $H\phi$  es cerrado bajo la operación de  $G'$ . El hecho de que  $e' = e\phi$  y  $a^{-1}\phi = (a\phi)^{-1}$  completa la demostración de que  $H\phi$  es un subgrupo de  $G\phi$ . Supóngase que  $H$  es normal en  $G$  y sea  $g\phi \in G\phi$ . Ahora bien,

$$(g\phi)^{-1}(h\phi)(g\phi) = (g^{-1}\phi)(h\phi)(g\phi) = (g^{-1}hg)\phi.$$

Como  $g^{-1}hg \in H$ , tenemos que  $(g^{-1}hg)\phi \in H\phi$ . Así,  $H\phi$  es normal en  $G\phi$ .

Ahora, en la otra dirección, sea  $K'$  un subgrupo de  $G'$ . Supóngase que  $a$  y  $b$  están en  $K'\phi^{-1}$ . Entonces,  $(ab)\phi = (a\phi)(b\phi)$  y  $(a\phi)(b\phi) \in K'$ , de modo que  $ab \in K'\phi^{-1}$ . Además,  $K'$  debe contener a la identidad  $e\phi$ , de modo que  $e \in K'\phi^{-1}$ . Si  $a \in K'\phi^{-1}$ , entonces  $a\phi \in K'$ , de modo que  $(a\phi)^{-1} \in K'$ . Pero  $(a\phi)^{-1} = a^{-1}\phi$ , luego  $a^{-1} \in K'\phi^{-1}$ . Por tanto,  $K'\phi^{-1}$  es un subgrupo de  $G$ . Si  $K'$  es un subgrupo normal de  $G\phi$  entonces para  $b \in K'\phi^{-1}$  y  $g \in G$  tenemos

$$(g^{-1}bg)\phi = (g\phi)^{-1}(b\phi)(g\phi),$$

y  $(g\phi)^{-1}(b\phi)(g\phi)$  está en  $K'$ , de modo que  $g^{-1}bg \in K'\phi^{-1}$ . Por tanto,  $K'\phi^{-1}$  es normal en  $G$ . ■

Quizás el teorema 13.2 parezca complejo, pero es muy sencillo y la demostración es en realidad mecánica. Sería un excelente ejercicio escribir toda la demostración sin usar el libro. Así se verá si de verdad se han entendido las definiciones incluidas.

## 13.2 EL TEOREMA FUNDAMENTAL DEL HOMOMORFISMO

El teorema 13.2 muestra, en particular, que para un homomorfismo  $\phi: G \rightarrow G'$ , el kernel  $K = \{e'\}\phi^{-1}$  es un subgrupo normal de  $G$ . Estamos ahora en condición de probar el teorema principal.

**Teorema 13.3 (Teorema fundamental del homomorfismo)** Sea  $\phi$  un homomorfismo de un grupo  $G$  en un grupo  $G'$ , con kernel  $K$ . Entonces,  $G\phi$  es un grupo y existe un isomorfismo canónico (natural) de  $G\phi$  con  $G/K$ .

**Demostración** En el teorema 13.2 se vio que  $G\phi$  es un grupo, pues  $G$  es un caso particular de un subgrupo de  $G$ . Sea  $aK \in G/K$ , tratemos de definir una transformación  $\psi: G/K \rightarrow G\phi$  mediante

$$(aK)\psi = a\phi.$$

Definimos, así, la transformación  $\psi$  en una clase lateral escogiendo un representante  $a$  de la clase lateral; primero debemos mostrar que  $\psi$  está bien definida, esto es, que es independiente de nuestra selección del representante. Para ello, sea  $b \in aK$ . Es necesario mostrar que  $a\phi = b\phi$ . Pero  $b \in aK$  significa que  $b = ak_1$ , para  $k_1 \in K$ , de modo que  $a^{-1}b = k_1$ . Entonces,

$$e' = k_1\phi = (a^{-1}b)\phi = (a^{-1}\phi)(b\phi) = (a\phi)^{-1}(b\phi).$$

De aquí

$$b\phi = (a\phi)e' = a\phi.$$

Así,  $\psi$  está bien definida.

Para mostrar que  $\psi$  es uno a uno, supóngase que  $(aK)\psi = (bK)\psi$ . Entonces,  $a\phi = b\phi$ , de modo que

$$e' = (a\phi)^{-1}(b\phi) = (a^{-1}\phi)(b\phi) = (a^{-1}b)\phi.$$

Así, por la definición de  $K$ ,  $a^{-1}b \in K$ . Pero,  $a^{-1}b \in K$  implica que  $b \in aK$ , de modo que  $bK = aK$ . Por tanto es uno a uno.

Es obvio que  $\psi$  es sobre  $G\phi$ .

La ecuación

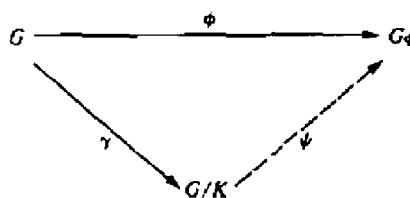
$$[(aK)(bK)]\psi = (abK)\psi = (ab)\phi = (a\phi)(b\phi) = [(aK)\psi][(bK)\psi]$$

completa la demostración de que  $\psi$  es un isomorfismo.

La transformación  $\psi$  es una transformación canónica (o natural) en el sentido de que si  $\gamma$  es el homomorfismo canónico  $\gamma:G \rightarrow G/K$  del teorema 13.1, entonces,

$$\phi = \gamma\psi.$$

Decimos que el diagrama de la figura 13.1 es *commutativo*. ■



**Figura 13.1**

La comprensión del teorema 13.3 a menudo causa problemas a los estudiantes. En realidad afirma que para un homomorfismo  $\phi$  del grupo  $G$ , la imagen es, excepto por los nombres de los elementos, justamente  $G/K$ , donde  $K$  es el kernel, y que el homomorfismo  $\phi$  es esencialmente la transformación canónica  $\gamma:G \rightarrow G/K$ . En otras palabras, en cierto sentido el teorema 13.1 describe todos los homomorfismos.

*Diremos aquí, de una vez y para siempre, que cuando se tenga un homomorfismo, hay dos cosas de principal importancia: la imagen y el kernel.*

Los teoremas 13.1 y 13.3 muestran que los homomorfismos corresponden de manera natural a los grupos factores. A saber, para cada grupo factor  $G/N$  existe un homomorfismo  $\gamma:G \rightarrow G/N$  con kernel  $N$ . De manera reciproca, para cada homomorfismo  $\phi:G \rightarrow G'$  la imagen  $G\phi$  es esencialmente  $G/K$  donde  $K$  es el kernel de  $\phi$ . «Esencialmente» quiere decir salvo un isomorfismo canónico.

**Ejemplo 13.3** Los alumnos que tengan algún conocimiento de teoría de números complejos, verán que la transformación  $\phi:\mathbb{R} \rightarrow \mathbb{C}^*$  dada por

$$x\phi = \cos x + i \sin x$$

es un homomorfismo de  $\mathbb{R}$  bajo la suma  $\mathbb{C}^*$  es el grupo multiplicativo de los números complejos distintos de cero. Nótese que  $\cos x + i \sin x = 1$  si y sólo si

$x = 2\pi n$  para algún entero  $n$ . Así, el kernel del homomorfismo es el subgrupo cíclico  $\langle 2\pi \rangle$  de  $\mathbb{R}$ .

El teorema 13.3 muestra que  $\mathbb{R}/\langle 2\pi \rangle$  es isomorfo a  $\mathbb{R}\phi$ , que es el grupo multiplicativo de los números complejos con valor absoluto 1, esto es, los números complejos sobre el círculo unitario. Este isomorfismo se puede visualizar en sentido geométrico. Toda clase lateral de  $\mathbb{R}/\langle 2\pi \rangle$  tiene precisamente un representante  $\geq 0$  y  $< 2\pi$ . Así,  $\mathbb{R}/\langle 2\pi \rangle$  se puede visualizar como el intervalo  $0 \leq x < 2\pi$  y si lo doblamos de manera que el *extremo abierto* del intervalo en  $2\pi$  se coloque sobre el *extremo cerrado* en 0, formará un círculo. La suma en  $\mathbb{R}/\langle 2\pi \rangle$  visto como círculo, no es más que la suma de longitudes de arco (o de ángulos centrales) y eso es lo que sucede precisamente cuando se multiplican dos números complejos sobre el círculo unitario. ■

### 13.3 APPLICACIONES

**Definición** Un *subgrupo normal maximal de un grupo G* es un subgrupo normal  $M$  que no es igual a  $G$  y tal que ningún subgrupo normal propio  $N$  de  $G$  contiene propiamente a  $M$ .

**Teorema 13.4**  $M$  es un subgrupo normal maximal de  $G$  si y sólo si  $G/M$  es simple.

**Demuestra** Sea  $M$  un subgrupo normal maximal de  $G$ . Considérese el homomorfismo canónico  $\gamma: G \rightarrow G/M$  dado por el teorema 13.1. Ahora bien,  $\gamma^{-1}$  de cualquier subgrupo normal propio de  $G/M$  sería un subgrupo normal propio de  $G$  que contuviera propiamente a  $M$ . Pero  $M$  es maximal, de modo que esto no puede suceder. Por tanto,  $G/M$  debe ser simple.

De manera reciproca, el teorema 13.2 muestra que si  $N$  es un subgrupo normal de  $G$  que contiene propiamente a  $M$ , entonces  $N\gamma$  es normal en  $G/M$ . Si además  $N \neq G$ , entonces

$$N\gamma \neq G/M \quad \text{y} \quad N\gamma \neq \{M\}.$$

Así, si  $G/M$  es simple, de manera que no puede existir dicha  $N\gamma$ ; dicha  $N$  no puede existir y  $M$  es maximal. ■

Nótese que un homomorfismo  $\phi$  da un isomorfismo del dominio de  $\phi$  con la imagen de  $\phi$  si y sólo si  $\phi$  es una transformación uno a uno.

**Teorema 13.5** Un homomorfismo  $\phi$  de un grupo  $G$  es una función uno a uno si y sólo si el kernel de  $\phi$  es  $\{e\}$ .

**Demuestra** Desde luego, si la transformación  $\phi$  es uno a uno, el kernel es sólo  $\{e\}$  pues sabemos que  $e\phi$  es la identidad  $e'$  de la imagen.

En forma recíproca, supóngase que el kernel es  $\{e\}$ . Si  $a\phi = b\phi$ , entonces,

$$e' = e\phi = (a\phi)^{-1}(b\phi) = (a^{-1}\phi)(b\phi) = (a^{-1}b)\phi,$$

de modo que  $a^{-1}b$  está en el kernel. Como el kernel es  $\{e\}$ , debemos tener que  $a^{-1}b = e$ , de modo que  $a = b$ . Así,  $\phi$  es uno a uno. ■

A la luz del teorema 13.5, revisemos la lista de pasos que los matemáticos usan por lo común para exhibir un isomorfismo.

**PASO 1** Definir la transformación.

**PASO 2** Probar que la transformación es un homomorfismo.

**PASO 3** Probar que el kernel de la transformación es  $\{e\}$ . Se sabe entonces que la transformación es un isomorfismo del dominio con la imagen.

Aunque no usaremos esta terminología, como información diremos que un homomorfismo  $\phi:G \rightarrow G'$  que sea una transformación uno a uno, es un monomorfismo y  $\phi$  es un epimorfismo si es sobre  $G'$ .

## Ejercicios

---

**13.1** Determinese cuáles de las transformaciones siguientes son homomorfismos. Un asterisco (\*) denota elementos distintos de cero. Si la transformación es un homomorfismo, describanse la imagen y el kernel.

- a)  $\phi:\mathbb{Z} \rightarrow \mathbb{R}$  bajo la suma, dado por  $n\phi = n$
- b)  $\phi:\mathbb{R} \rightarrow \mathbb{Z}$  bajo la suma, dado por  $x\phi = \text{mayor entero } \leq x$
- c)  $\phi:\mathbb{R}^* \rightarrow \mathbb{R}^*$  bajo la multiplicación, dado por  $x\phi = |x|$
- d)  $\phi:\mathbb{Z}_6 \rightarrow \mathbb{Z}_2$  dado por  $x\phi = \text{residuo de } x \text{ al dividirlo entre } 2$ , como en el lema 6.1
- e)  $\phi:\mathbb{Z}_9 \rightarrow \mathbb{Z}_4$  dado por  $x\phi = \text{residuo de } x \text{ al dividirlo entre } 2$ , en el sentido del lema 6.1

**13.2** Sea  $G$  un grupo generado por  $\{a_i \mid i \in I\}$ , donde  $I$  es algún conjunto de índices y  $a_i \in G$ . Sea  $\phi:G \rightarrow G'$  un homomorfismo de  $G$  en un grupo  $G'$ . Muestrese que el valor de  $\phi$  en cada elemento de  $G$  está por completo determinado por los valores  $a_i\phi$ . Así, por ejemplo, un homomorfismo de un grupo cíclico está por completo determinado por el valor del homomorfismo en un generador del grupo. [Sugerencia: úsese el teorema 9.1 y, por supuesto, la definición de homomorfismo.]

**13.3** ¿Cuántos homomorfismos hay de  $\mathbb{Z}$  sobre  $\mathbb{Z}_2$ ? ¿de  $\mathbb{Z}$  en  $\mathbb{Z}_2$ ? ¿de  $\mathbb{Z}$  sobre  $\mathbb{Z}_3$ ? [Sugerencia: úsese el ejercicio 13.2. Véase también el ejercicio 13.11.]

**13.4** ¿Cuántos homomorfismos hay de  $\mathbb{Z}$  en  $\mathbb{Z}_6$ ? ¿de  $\mathbb{Z}$  sobre  $\mathbb{Z}_6$ ? [Sugerencia: úsese el ejercicio 13.2. Véase también el ejercicio 13.11.]

**13.5** ¿Cuántos homomorfismos hay de  $\mathbb{Z}_{12}$  sobre  $\mathbb{Z}_2$ ? ¿de  $\mathbb{Z}_{12}$  en  $\mathbb{Z}_2$ ? ¿de  $\mathbb{Z}_{12}$  sobre  $\mathbb{Z}_6$ ? ¿de  $\mathbb{Z}_{12}$  en  $\mathbb{Z}_{14}$ ? ¿de  $\mathbb{Z}_{12}$  en  $\mathbb{Z}_{16}$ ? [Sugerencia: úsese el ejercicio 13.2.]

**13.6** ¿Qué podemos decir acerca de los homomorfismos de un grupo simple?

## 13.7 ¿Falso o verdadero?

- a)  $A_n$  es un subgrupo normal de  $S_n$ .
  - b) Todo isomorfismo es también un homomorfismo.
  - c) Todo homomorfismo es un isomorfismo.
  - d) Un homomorfismo es un isomorfismo del dominio con la imagen si y sólo si el kernel consta del grupo con sólo el elemento identidad.
  - e) La imagen, bajo algún homomorfismo de un grupo de seis elementos, puede tener cuatro elementos.
  - f) La imagen, bajo un homomorfismo de un grupo de seis elementos, puede tener doce elementos.
  - g) Existe algún homomorfismo de algún grupo de seis elementos en algún grupo de doce elementos.
  - h) Existe algún homomorfismo de algún grupo de seis elementos en algún grupo de diez elementos.
  - i) Todos los homomorfismos de un grupo de orden primo son, en algún sentido, triviales.
  - j) No es posible tener un homomorfismo de algún grupo infinito en algún grupo finito.
- 

13.8 ¿Cuántos homomorfismos hay de  $Z_2 \times Z_2$  en  $Z_2$ ? ¿de  $Z_2 \times Z_2$  sobre  $Z_2$ ? ¿de  $Z_2 \times Z_2$  en  $Z_6$ ? ¿de  $Z_2 \times Z_2$  en  $Z_2 \times Z_2 \times Z_1$ ? ¿de  $Z_1 \times Z_2$  en  $Z_2 \times Z_1 \times Z_4$ ? [Sugerencia: úsese el ejercicio 13.2.]

13.9 El signo de una permutación par es  $+1$  y el signo de una permutación impar es  $-1$ . Obsérvese que la transformación  $\text{sgn}_n: S_n \rightarrow \{1, -1\}$  definida por

$$\text{sgn}_n(\sigma) = \text{signo de } \sigma$$

es un homomorfismo de  $S_n$  sobre el grupo  $\{1, -1\}$  bajo la multiplicación. ¿Cuál es el kernel?

13.10 Para dos grupos  $G_1$  y  $G_2$  considérese la transformación  $\pi_1: (G_1 \times G_2) \rightarrow G_1$  dada por  $(x, y)\pi_1 = x$ . Muéstrese que  $\pi_1$  es un homomorfismo. ¿Cuál es el kernel? ¿A qué grupo es isomorfo el kernel?

13.11 Sea  $G$  cualquier grupo y sea  $a$  cualquier elemento de  $G$ . Sea  $\phi: \mathbb{Z} \rightarrow G$  definida por  $n\phi = a^n$ . Muéstrese que  $\phi$  es un homomorfismo. Describase la imagen y las posibilidades para el kernel de  $\phi$ . [Comentario: usando este ejercicio y el teorema 13.3 obtenemos la demostración elegante de que todo grupo cíclico es isomorfo a  $\mathbb{Z}/n\mathbb{Z}$  para algún entero no negativo  $n$  y además, la demostración elegante de que todo elemento de un grupo genera un subgrupo cíclico del grupo.]

13.12 Sea  $G$  un grupo.

- a) Si  $\phi: \mathbb{Z} \times \mathbb{Z} \rightarrow G$  es un homomorfismo y  $(1, 0)\phi = h$  mientras que  $(0, 1)\phi = k$ , encuéntrese  $(m, n)\phi$ .
- b) Sean  $h, k \in G$  y sea  $\psi: \mathbb{Z} \times \mathbb{Z} \rightarrow G$  definido por  $(m, n)\psi = h^m k^n$ . Dese una condición necesaria y suficiente, incluyendo a  $h$  y  $k$  para que  $\psi$  sea un homomorfismo. Pruebese la condición.
- c) Encuéntrese una condición necesaria y suficiente en  $G$  tal que la transformación descrita en la parte b) sea un homomorfismo para cualquier selección de  $h, k \in G$ .

13.13 Sea  $G$  un grupo abeliano finito de orden  $n$  y sea  $r$  un entero positivo, primo relativo con  $n$ .

- Muéstrese que la transformación  $\phi_r:G \rightarrow G$  dada por  $a\phi_r = a^r$  es un isomorfismo de  $G$  sobre sí mismo. (Sigase el esbozo que aparece después del teorema 13.5.)
- Dedúzcase que la ecuación  $x^r = a$  siempre tiene una solución única en un grupo abeliano finito  $G$ , si  $r$  es primo relativo con el orden de  $G$ . ¿Qué sucede si  $r$  y el orden de  $G$  no son primos relativos?

13.14 Muéstrese que si  $G$ ,  $G'$  y  $G''$  son grupos y si  $\phi:G \rightarrow G'$  y  $\psi:G' \rightarrow G''$  son homomorfismos, entonces, la función compuesta  $\phi\psi:G \rightarrow G''$  es un homomorfismo.

13.15 Sea  $G$  un grupo y sea  $\mathcal{F}_G$  el grupo de los automorfismos internos de  $G$  dado en el ejercicio 12.18. Muéstrese que la transformación  $\phi:G \rightarrow \mathcal{F}_G$  dada por  $g\phi = i_g$  es un homomorfismo de  $G$  sobre  $\mathcal{F}_G$ . Muéstrese que el kernel (el centro de  $G$ ) es

$$\{a \in G \mid ax = xa \text{ para toda } x \in G\}.$$

Determinese cuándo  $\phi$  es un isomorfismo.

13.16 Sean  $G_1$  y  $G_2$  grupos y sean  $\phi_1:G_1 \rightarrow G_1$  y  $\phi_2:G_2 \rightarrow G_2$  homomorfismos, tales que  $\phi_1\phi_2 = \phi_2\phi_1 = i$ , donde  $i$  es la transformación identidad; esto es,  $\phi_1\phi_2:G_1 \rightarrow G_1$  y  $\phi_2\phi_1:G_2 \rightarrow G_2$  son ambos la transformación identidad. Muéstrese que tanto  $\phi_1$  como  $\phi_2$  son isomorfismos de  $G_1$  con  $G_2$  y que  $\phi_1 = (\phi_2)^{-1}$ .

13.17 Sean  $G$  y  $G'$  grupos y sean  $H$  y  $H'$  subgrupos normales de  $G$  y  $G'$  respectivamente. Sea  $\phi$  un homomorfismo de  $G$  en  $G'$ . Muéstrese que  $\phi$  induce un homomorfismo natural  $\phi_*:G/H \rightarrow G'/H'$  si  $H\phi \subseteq H'$ . (Este hecho se usa con frecuencia en topología algebraica.)

## 14

## Series de grupos

### 14.1 SERIES NORMALES Y SUBNORMALES

Este capítulo trata del concepto de *serie* de un grupo  $G$ , que permite comprender la estructura de  $G$ . Los resultados, presentados sin demostrar, valen tanto para grupos abelianos como para grupos no abelianos. No son muy importantes para grupos abelianos finitamente generados, pues contamos ya con el poderoso teorema 9.3. Sin embargo, para facilitar los cálculos, casi todos los ejemplos se tomarán de grupos abelianos. Los resultados se demuestran en el siguiente capítulo.

**Definición** Una *serie subnormal* (o *subinvariante*) de un grupo  $G$  es una sucesión finita  $H_0, H_1, \dots, H_n$  de subgrupos de  $G$  tal que  $H_i < H_{i+1}$  y  $H_i$  es un subgrupo normal de  $H_{i+1}$ , con  $H_0 = \{e\}$  y  $H_n = G$ . Una *serie normal* (o *invariante*) de  $G$  es una sucesión finita  $H_0, H_1, \dots, H_n$  de subgrupos normales de  $G$  tal que  $H_i < H_{i+1}$ ,  $H_0 = \{e\}$  y  $H_n = G$ .

Nótese que para grupos abelianos, coinciden los conceptos de serie subnormal y serie normal, pues todo subgrupo es normal. Una serie normal siempre es subnormal, pero el recíproco no necesariamente es cierto. Definimos serie subnormal antes que serie normal, pues dicho concepto es más importante para nuestro trabajo.

**Ejemplo 14.1** Dos ejemplos de series normales de  $\mathbb{Z}$  bajo la suma son

$$\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

y

$$\{0\} < 9\mathbb{Z} < \mathbb{Z} \blacksquare$$

**Ejemplo 14.2** Considérese el grupo  $D_4$  de simetrías del cuadrado en el ejemplo 4.2. Puede corroborarse con facilidad que

$$\{ \rho_0 \} < \{ \rho_0, \mu_1 \} < \{ \rho_0, \rho_2, \mu_1, \mu_2 \} < D_4$$

es una serie subnormal. No es una serie normal, puesto que  $\{ \rho_0, \mu_1 \}$  es no normal en  $D_4$ . ■

**Definición** Una serie subnormal (normal)  $\{K_j\}$  es un *refinamiento de una serie subnormal (normal)*  $\{H_i\}$  de un grupo  $G$  si  $\{H_i\} \subseteq \{K_j\}$ , esto es, si cada  $H_i$  es una de las  $K_j$ .

**Ejemplo 14.3** La serie

$$\{0\} < 72\mathbb{Z} < 24\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

es un refinamiento de la serie

$$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}.$$

Se han insertado dos nuevos términos,  $4\mathbb{Z}$  y  $24\mathbb{Z}$ . ■

Los grupos factores  $H_{i+1}/H_i$  son de interés en el estudio de la estructura de  $G$ . Tanto en el caso de las series normales como en los subnormales, están definidos estos grupos factores, ya que en ambos casos,  $H_i$  es normal en  $H_{i+1}$ .

**Definición** Dos series subnormales (normales)  $\{H_i\}$  y  $\{K_j\}$  del mismo grupo  $G$  son *isomorfas* si existe una correspondencia uno a uno entre las colecciones de grupos factores  $\{H_{i+1}/H_i\}$  y  $\{K_{j+1}/K_j\}$  tal que los grupos factores correspondientes son isomorfos.

Es claro que dos series subnormales (normales) isomorfas deben tener el mismo número de grupos.

**Ejemplo 14.4** Las dos series de  $\mathbb{Z}_{15}$ .

$$\{0\} < \langle 5 \rangle < \mathbb{Z}_{15}$$

y

$$\{0\} < \langle 3 \rangle < \mathbb{Z}_{15},$$

son isomorfas. Tanto  $\mathbb{Z}_{15}/\langle 5 \rangle$  como  $\langle 3 \rangle/\{0\}$  son isomorfos a  $\mathbb{Z}_3$ , y  $\mathbb{Z}_{15}/\langle 3 \rangle$  es isomorfo a  $\langle 5 \rangle/\{0\}$  o a  $\mathbb{Z}_3$ . ■

## 14.2 EL TEOREMA DE JORDAN-HÖLDER

El siguiente teorema es muy importante en esta teoría.

**Teorema 14.1 (Schreier)** *Dos series subnormales (normales) de un grupo  $G$  tienen refinamientos isomorfos.*

**Demostración** Véase la demostración de este teorema en el capítulo 15. ■

En realidad, la demostración de teorema 14.1 no es muy difícil. Sin embargo, sabemos por experiencia que muchos estudiantes se pierden en la demostración y sienten que no pueden entender el teorema. No lo demostramos en las secciones sin asterisco, aunque la podrían seguir la mayoría de los estudiantes. Sin embargo, ilustraremos el teorema.

**Ejemplo 14.5** Tratemos de encontrar refinamientos isomorfos de las series

$$\{0\} < 8\mathbf{Z} < 4\mathbf{Z} < \mathbf{Z}$$

y

$$\{0\} < 9\mathbf{Z} < \mathbf{Z}$$

dadas en el ejemplo 14.1. Considérese el refinamiento

$$\{0\} < 72\mathbf{Z} < 8\mathbf{Z} < 4\mathbf{Z} < \mathbf{Z}$$

de  $\{0\} < 8\mathbf{Z} < 4\mathbf{Z} < \mathbf{Z}$  y el refinamiento

$$\{0\} < 72\mathbf{Z} < 18\mathbf{Z} < 9\mathbf{Z} < \mathbf{Z}$$

de  $\{0\} < 9\mathbf{Z} < \mathbf{Z}$ . En ambos casos los refinamientos tienen cuatro grupos factores isomorfos a  $\mathbf{Z}_4$ ,  $\mathbf{Z}_2$ ,  $\mathbf{Z}_9$  y  $72\mathbf{Z}$  o  $\mathbf{Z}$ . El orden en el cual se presentan los grupos factores es, desde luego, diferente. ■

Llegamos ahora al plato fuerte de la teoría.

**Definición** Una serie subnormal  $\{H_i\}$  de un grupo  $G$  es una *serie de composición* si todos los grupos factores  $H_{i+1}/H_i$  son simples. Una serie normal  $\{H_i\}$  de  $G$  es una *serie principal* si todos los grupos factores  $H_{i+1}/H_i$  son simples.

Nótese que, para grupos abelianos, coinciden los conceptos de series principales y de composición. Además, como toda serie normal es subnormal, toda serie principal es una serie de composición para cualquier grupo, sea abeliano o no.

**Ejemplo 14.6** Afirmamos que  $\mathbb{Z}$  no tiene serie de composición (ni principal). Pues si

$$\{0\} = H_0 < H_1 < \cdots < H_{n-1} < H_n = \mathbb{Z}$$

es una serie subnormal,  $H_1$  debe ser de la forma  $r\mathbb{Z}$  para alguna  $r \in \mathbb{Z}^+$ . Pero, entonces,  $H_1/H_0$  es isomorfo a  $r\mathbb{Z}$ , el cual es cíclico infinito con varios subgrupos normales propios no triviales, por ejemplo,  $2r\mathbb{Z}$ . Así,  $\mathbb{Z}$  no tiene series de composición (ni principales). ■

**Ejemplo 14.7** La serie

$$\{e\} < A_n < S_n$$

para  $n \geq 5$  es una serie de composición (y también una serie principal) de  $S_n$ , pues  $A_n/\{e\}$  es isomorfo a  $A_n$ , el cual es simple para  $n \geq 5$ , y  $S_n/A_n$  es isomorfo a  $\mathbb{Z}_2$ , que es simple. Así mismo, las dos series dadas en el ejemplo 14.4 son series de composición (y además series principales) de  $\mathbb{Z}_{15}$ . Son isomorfas, según se mostró en dicho ejemplo. Esto ilustra nuestro teorema principal que se enunciará en breve. ■

Obsérvese que, por el teorema 13.4,  $H_{i+1}/H_i$  es simple si y sólo si  $H_i$  es un subgrupo normal maximal de  $H_{i+1}$ . Así, para una serie de composición, cada  $H_i$  debe ser un subgrupo normal maximal de  $H_{i+1}$ . Para formar una serie de composición de un grupo  $G$ , debemos buscar un subgrupo normal maximal  $H_{n-1}$  de  $G$ , luego un subgrupo normal maximal de  $H_{n-1}$ , y así sucesivamente. Si este proceso termina en un número finito de pasos, tenemos una serie de composición. Nótese que, por el teorema 13.4, una serie de composición no puede tener más refinamiento. Para formar una serie principal, debemos buscar un subgrupo normal maximal  $H_{n-1}$  de  $G$ , después un subgrupo normal maximal de  $H_{n-1}$  que sea, además, normal en  $G$ , y así sucesivamente. El teorema principal es el siguiente:

**Teorema 14.2 (Jordan-Hölder)** Cualesquiera dos series de composición (principales) de un grupo  $G$  son isomorfas.

**Demostración** Sean  $\{H_i\}$  y  $\{K_j\}$  dos series de composición (principales) de  $G$ . Por el teorema 14.1, tienen refinamientos isomorfos. Pero, como los grupos factores son ya simples, el teorema 13.4 muestra que ninguna de esas series tiene más refinamientos. Así,  $\{H_i\}$  y  $\{K_j\}$  ya deben ser isomorfos. ■

Para el caso de un grupo finito, se debería considerar una serie de composición como cierto tipo de factorización del grupo en grupos factores simples, análoga a la factorización de un entero positivo en primos. En ambos casos, la factorización es única, salvo el orden de los factores.

**Teorema 14.3** Si  $G$  tiene una serie de composición (principal) y si  $N$  es un subgrupo normal propio de  $G$ , entonces existe una serie de composición (principal) que contiene a  $N$ .

**Demostración** La serie

$$\{e\} < N < G$$

es una serie subnormal y normal. Como  $G$  tiene una serie de composición  $\{H_i\}$ , entonces, por el teorema 14.1, existe un refinamiento de  $\{e\} < N < G$  a una serie subnormal isomorfa a un refinamiento de  $\{H_i\}$ . Pero en tanto serie de composición,  $\{H_i\}$  no puede tener mayor refinamiento. Así,  $\{e\} < N < G$  puede refinarse a una serie subnormal, cuyos grupos factores son todos ellos simples, esto es, a una serie de composición. Se emplea un argumento similar si comenzamos con una serie principal  $\{K_j\}$  de  $G$ . ■

**Ejemplo 14.8** Una serie de composición (y principal) de  $\mathbb{Z}_4 \times \mathbb{Z}_9$ , que contiene a  $\langle(0, 1)\rangle$  es

$$\{(0, 0)\} < \langle(0, 3)\rangle < \langle(0, 1)\rangle < \langle 2 \rangle \times \langle 1 \rangle < \langle 1 \rangle \times \langle 1 \rangle = \mathbb{Z}_4 \times \mathbb{Z}_9. ■$$

La siguiente definición es básica para el último capítulo del libro, que trata de la solución de ecuaciones polinomiales en términos de radicales.

**Definición** Un grupo  $G$  es *soluble* si tiene una serie de composición  $\{H_i\}$  tal que todos los grupos factores  $H_{i+1}/H_i$  son abelianos.

Por el teorema de Jordan-Hölder, vemos que para los grupos solubles, *toda* serie de composición  $\{H_i\}$  debe tener grupos factores abelianos  $H_{i+1}/H_i$ .

**Ejemplo 14.9** El grupo  $S_3$  es soluble, pues la serie de composición

$$\{e\} < A_3 < S_3$$

tiene grupos factores isomorfos a  $\mathbb{Z}_3$  y  $\mathbb{Z}_2$  que son abelianos. El grupo  $S_3$  no es soluble, pues, como  $A_3$  es simple, la serie

$$\{e\} < A_3 < S_3$$

es una serie de composición y  $A_3/\{e\}$ , que es isomorfo a  $A_3$ , no es abeliano. *Se puede mostrar que este grupo  $A_5$ , de orden 60 es el menor grupo que no es soluble.* Este hecho está intimamente relacionado con el hecho de que una ecuación polinomial de grado 5 no es, en general, soluble por radicales, pero una ecuación polinomial de grado  $\leq 4$  lo es. ■

### \* 14.3 EL CENTRO Y LA SERIE CENTRAL ASCENDENTE

Daremos otro tipo de series de un grupo.

**Definición** El centro de un grupo  $G$  es el conjunto de todas las  $a \in G$  tales que  $ax = xa$  para todas las  $x \in G$ , esto es, el conjunto de elementos de  $G$  que comutan con todo elemento de  $G$ .

**Teorema 14.4** El centro de un grupo es un subgrupo normal del grupo.

**Demuestração** La demostración es tan fácil e instructiva que la dejaremos como ejercicio en este capítulo. ■

Es fácil encontrar el centro de un grupo finito  $G$  si se tiene la tabla del grupo. Es claro que un elemento  $a$  estará en el centro de  $G$  si y sólo si, en la tabla, los elementos del renglón cuyo extremo izquierdo es  $a$  están dados en el mismo orden que los elementos de la columna debajo de  $a$ .

Ahora, sea  $G$  un grupo y sea  $Z(G)$  el centro de  $G$ . Como, por el teorema 14.4,  $Z(G)$  es normal en  $G$ , podemos formar el grupo factor  $G/Z(G)$  y encontrar el centro  $Z(G/Z(G))$  de este grupo factor. Como  $Z(G/Z(G))$  es normal en  $G/Z(G)$ , si  $\gamma: G \rightarrow G/Z(G)$  es la transformación canónica, entonces, por el teorema 13.2,  $[Z(G/Z(G))]_{\gamma}^{-1}$  es un subgrupo normal  $Z_1(G)$  de  $G$ . Entonces, podemos formar el grupo factor  $G/Z_1(G)$  y encontrar su centro, tomar  $(\gamma_1)^{-1}$  del centro para obtener  $Z_2(G)$ , y así sucesivamente.

**Definición** La serie

$$\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

descrita en el análisis anterior, es la serie central ascendente del grupo  $G$ .

**Ejemplo 14.10** El centro de  $S_3$  es precisamente la identidad  $\{\rho_0\}$ . Así, la serie central ascendente de  $S_3$  es

$$\{\rho_0\} \leq \{\rho_0\} \leq \{\rho_0\} \leq \cdots$$

El centro del grupo  $D_4$  de simetrías del cuadrado en el ejemplo 4.2 es  $\{\rho_0, \rho_2\}$ . (Recuerdan que dijimos que este grupo nos daría bellos ejemplos de casi todo lo que discutíramos?) Como  $G/\{\rho_0, \rho_2\}$  es de orden 4 y, por tanto, abeliano, su centro es todo  $G/\{\rho_0, \rho_2\}$ . Así, la serie central ascendente de  $D_4$  es

$$\{\rho_0\} \leq \{\rho_0, \rho_2\} \leq D_4 \leq D_4 \leq D_4 \leq \cdots. ■$$

**Ejercicios**

14.1 Dense refinamientos isomorfos de las dos series normales  $\{0\} < 60\mathbb{Z} < 20\mathbb{Z} < \mathbb{Z}$  y  $\{0\} < 245\mathbb{Z} < 49\mathbb{Z} < \mathbb{Z}$  de  $\mathbb{Z}$  bajo la suma.

14.2 Encuéntrense todas las series de composición de  $\mathbb{Z}_{60}$  y muéstrese que, en efecto, son todas isomorfas.

14.3 Encuéntrense todas las series de composición de  $\mathbb{Z}_3 \times \mathbb{Z}_5$ .

14.4 Encuéntrense todas las series de composición de  $S_3 \times \mathbb{Z}_2$ .

<sup>†</sup>14.5 Muéstrese que si

$$H_0 = \{e\} < H_1 < H_2 < \cdots < H_n = G$$

es una serie subnormal (normal) de un grupo  $G$  y si  $H_{i+1}/H_i$  es de orden finito  $S_{i+1}$ , entonces  $G$  es de orden finito  $S_1 S_2 \cdots S_n$ .

14.6 ¿Falso o verdadero?

- a) Toda serie normal es además subnormal.
- b) Toda serie subnormal es además normal.
- c) Toda serie principal es una serie de composición.
- d) Toda serie de composición es una serie principal.
- e) Todo grupo abeliano tiene exactamente una serie de composición.
- f) Todo grupo finito tiene una serie de composición.
- g) Un grupo es soluble si y sólo si tiene una serie de composición con grupos factores simples.
- h)  $S_3$  es un grupo soluble.
- i) El teorema de Jordan-Hölder tiene cierta analogía con el teorema fundamental de la aritmética, que afirma que cualquier entero positivo mayor que 1 se puede factorizar de manera única, salvo el orden, como producto de primos.
- j) Todo grupo finito de orden primo es soluble.

14.7 Muéstrese que un grupo abeliano infinito no puede tener series de composición. [Sugerencia: úsese el ejercicio 14.5 junto con el hecho de que un grupo abeliano infinito siempre tiene un subgrupo normal propio.]

14.8 Encuéntrese una serie de composición de  $S_3 \times S_3$ . ¿Es soluble  $S_3 \times S_3$ ?

14.9 Muéstrese que un producto directo finito de grupos solubles es soluble.

14.10 ¿Es soluble el grupo  $D_4$  de simetrías del cuadrado del ejemplo 4.2?

\*14.11 Encuéntrese el centro de  $S_3 \times \mathbb{Z}_4$ .

\*14.12 Pruébese que el centro de un grupo es un subgrupo normal del grupo. [Advertencia: No se olvide la necesidad de probar que es un subgrupo, antes de probar que es normal.]

\*14.13 Encuéntrese la serie central ascendente de  $S_3 \times \mathbb{Z}_4$ .

## \* 15

# Teoremas del isomorfismo; demostración del teorema de Jordan-Hölder

## \*15.1 TEOREMAS DEL ISOMORFISMO

Existen varios teoremas acerca de grupos factores isomorfos y se les conoce como *teoremas del isomorfismo* de la teoría de grupos. El primero de ellos es el teorema 13.3 que reenunciaremos aquí para facilitar su referencia. En la figura 15.1 se ilustra el teorema con un diagrama.

**Teorema 15.1 (Primer teorema del isomorfismo)** *Sea  $\phi: G \rightarrow G'$  un homomorfismo con kernel  $K$  y sea  $\gamma_K: G \rightarrow G/K$  el homomorfismo canónico. Entonces, existe un isomorfismo único  $\psi: G/K \rightarrow G\phi$  tal que  $x\phi = x(\gamma_K\psi)$  para cada  $x \in G$ .*

Recuérdese que si  $H$  y  $N$  son subgrupos de un grupo  $G$ , entonces  $HN = \{hn \mid h \in H, n \in N\}$ . En el capítulo 8, definimos el *ensamble*  $H \vee N$  como el menor subgrupo de  $G$  que contiene a  $HN$ . Es claro que  $H \vee N$  es, además, el menor subgrupo de  $G$  que contiene a  $H$  y a  $N$ , ya que dicho subgrupo debe contener a  $HN$ . En general,  $HN$  no necesariamente es un subgrupo de  $G$ . Sin embargo, tenemos el lema siguiente.

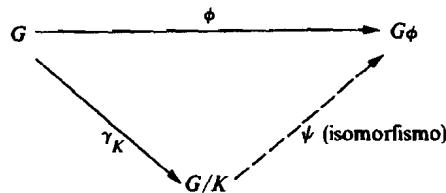


Figura 15.1

**Lema 15.1** Si  $N$  es un subgrupo normal de  $G$  y  $H$  es cualquier subgrupo de  $G$ , entonces  $H \vee N = HN = NH$ . Si, además,  $H$  también es normal en  $G$ , entonces  $HN$  es normal en  $G$ .

**Demostración** Mostremos que  $HN$  es un subgrupo de  $G$ , de donde se sigue inmediatamente que  $H \vee N = HN$ . Sea  $h_1, h_2 \in H$  y  $n_1, n_2 \in N$ . Como  $N$  es un subgrupo normal, tenemos que  $n_1h_2 = h_2n_3$  para alguna  $n_3 \in N$ . Entonces  $(h_1n_1)(h_2n_2) = h_1(n_1h_2)n_2 = h_1(h_2n_3)n_2 = (h_1h_2)(n_3n_2) \in HN$ , de modo que  $HN$  es cerrado bajo la operación inducida en  $G$ . Es claro que  $e = ee$  está en  $HN$ . Para  $h \in H$  y  $n \in N$  tenemos  $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}n_4$  para alguna  $n_4 \in N$ , ya que  $N$  es un subgrupo normal. Así,  $(hn)^{-1} \in HN$ , de modo que  $HN \leq G$ . Un argumento similar muestra que  $NH$  es un subgrupo, así que  $NH = H \vee N = HN$ .

Supóngase ahora que  $H$  también es normal en  $G$  y sea  $h \in H$ ,  $n \in N$  y  $g \in G$ . Entonces,  $g^{-1}hng = (g^{-1}hg)(g^{-1}ng) \in HN$ , de modo que, en efecto,  $HN$  es normal en  $G$ . ■

Estamos preparados ya para el segundo teorema del isomorfismo.

**Teorema 15.2 (Segundo teorema del isomorfismo)** Sea  $H$  un subgrupo de  $G$  y sea  $N$  un subgrupo normal de  $G$ . Entonces,  $(HN)/N \cong H/(H \cap N)$ .

**Demostración** Como  $N$  es normal en  $G$ , vemos de inmediato que  $H \cap N$  es normal en  $H$  (véase el ejercicio 15.1). Sea  $h \in H$  y  $n \in N$ . Intentemos definir  $\phi: HN \rightarrow H/(H \cap N)$  por  $(hn)\phi = h(H \cap N)$ . Es necesario mostrar que  $\phi$  está bien definida. Sea  $h_1 \in H$  y  $n_1 \in N$  y suponiendo que  $h_1n_1 = hn$ . Entonces,  $h^{-1}h_1 = nn_1^{-1}$  así que  $h^{-1}h_1$  está en  $H$  y en  $N$ , y, por ello, está en  $H \cap N$ . Por tanto,  $h(H \cap N) = h_1(H \cap N)$  en  $H/(H \cap N)$ . Así,  $(h_1n_1)\phi = (hn)\phi$  de modo que  $\phi$  está bien definida.

Afirmamos que  $\phi$  es un homomorfismo sobre  $H/(H \cap N)$ . Sea  $n_1, n_2 \in N$  y  $h_1, h_2 \in H$ . Como en el lema anterior, podemos escribir  $n_1h_2 = h_2n_3$  pues  $N$  es normal en  $G$ . Entonces,  $[(h_1n_1)(h_2n_2)]\phi = [(h_1h_2)(n_3n_2)]\phi = h_1h_2(H \cap N) = h_1(H \cap N) \cdot h_2(H \cap N) = (h_1n_1)\phi \cdot (h_2n_2)\phi$ , de modo que  $\phi$  es un homomorfismo. Como  $(he)\phi = h(H \cap N)$  para todas las  $h \in H$ , vemos que  $\phi$  es sobre  $H/(H \cap N)$ .

El kernel de  $\phi$  consta de todas las  $hn \in HN$  tales que  $h \in H \cap N$ ; entonces, este kernel es  $(H \cap N)N$ . Es claro que,  $(H \cap N)N = N$ . Así,  $\phi$  es un homomorfismo sobre  $H/(H \cap N)$  con kernel  $N$ , de modo que, por el teorema 15.1,  $(HN)/N \cong H/(H \cap N)$ . ■

**Ejemplo 15.1** Sea  $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ ,  $H = \mathbb{Z} \times \mathbb{Z} \times \{0\}$ , y  $N = \{0\} \times \mathbb{Z} \times \mathbb{Z}$ . Entonces, es claro que  $HN = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  y  $H \cap N = \{0\} \times \mathbb{Z} \times \{0\}$ . Tenemos  $(HN)/N \cong \mathbb{Z}$  y, además,  $H/(H \cap N) \cong \mathbb{Z}$ . ■

Si  $H$  y  $K$  son dos subgrupos normales de  $G$  y  $K \leq H$ , entonces, claramente  $H/K$  es un subgrupo normal de  $G/K$ . El tercer teorema de isomorfismo habla de estos grupos.

**Teorema 15.3 (Tercer teorema del isomorfismo)** Sean  $H$  y  $K$  subgrupos normales de un grupo  $G$  con  $K \leq H$ . Entonces,  $G/H \simeq (G/K)/(H/K)$ .

**Demostración** Sea  $\phi: G \rightarrow (G/K)/(H/K)$  dada por  $a\phi = (aK)(H/K)$  para  $a \in G$ . Es claro que  $\phi$  es sobre  $(G/K)/(H/K)$ ; y para  $a, b \in G$ ,

$$\begin{aligned} (ab)\phi &= [(ab)K](H/K) = [(aK)(bK)](H/K) = [(aK)(H/K)][(bK)(H/K)] \\ &= (a\phi)(b\phi), \end{aligned}$$

así que  $\phi$  es un homomorfismo. El kernel consta de aquellas  $x \in G$  tales que  $x\phi = H/K$ . Estas  $x$  son precisamente los elementos de  $H$ . Entonces, el teorema 15.1 muestra que  $G/H \simeq (G/K)/(H/K)$ . ■

Una bella manera de visualizar el teorema 15.3 es considerar la transformación canónica  $\gamma_H: G \rightarrow G/H$  como factorizada vía un subgrupo normal  $K$  de  $G$ ,  $K \leq H \leq G$ , para dar

$$\gamma_H = \gamma_K \gamma_{H/K},$$

salvo el isomorfismo natural, como se ilustra en la figura 15.2. Otra forma de verlo es usar el diagrama reticular de la figura 15.3 donde cada grupo es un subgrupo normal de  $G$  y está contenido en el que está arriba de él. Cuanto más grande sea el subgrupo normal, tanto menor es el grupo factor. Se puede pensar entonces que  $G$  está colapsado por  $H$ , esto es,  $G/H$ , como menor que  $G$  colapsado por  $K$ . El teorema 15.3 afirma que se puede colapsar  $G$  hasta  $G/H$  en dos pasos. Primero, colapsar hasta  $G/K$  y después, usando  $H/K$ , colapsarlo hasta  $(G/K)/(H/K)$ . El resultado total es el mismo (salvo isomorfismo) que colapsar  $G$  por  $H$ .

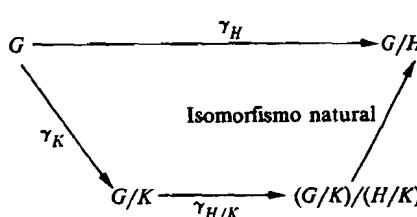


Figura 15.2

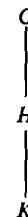


Figura 15.3

**Ejemplo 15.2** Considérese  $K = 6\mathbb{Z} < H = 2\mathbb{Z} < G = \mathbb{Z}$ . Entonces,  $G/H = \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2$ . Ahora bien,  $G/K = \mathbb{Z}/6\mathbb{Z}$  tiene como elementos

$$6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z} \text{ y } 5 + 6\mathbb{Z}.$$

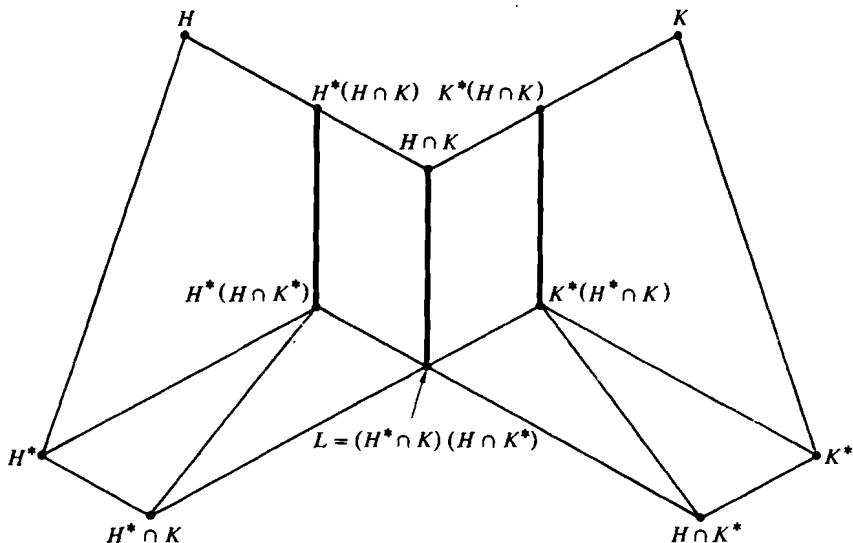
De estas seis clases laterales,  $6\mathbb{Z}$ ,  $2 + 6\mathbb{Z}$  y  $4 + 6\mathbb{Z}$  están en  $2\mathbb{Z}/6\mathbb{Z}$ . Es claro que  $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z})$  tiene dos elementos y además es isomorfo a  $\mathbb{Z}_2$ . De manera

alternativa, obsérvese que  $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}_6$  y  $2\mathbb{Z}/6\mathbb{Z}$  corresponden *bajo este isomorfismo* al subgrupo cíclico  $\langle 2 \rangle$  de  $\mathbb{Z}_6$ . Así,  $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z}) \simeq \mathbb{Z}_6/\langle 2 \rangle \simeq \mathbb{Z}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ . ■

## \*15.2 EL LEMA DE ZASSENHAUS (DE LA MARIPOSA)

La demostración del teorema de Jordan-Hölder se desprende fácilmente de un lema bastante técnico, desarrollado por Zassenhaus, al que también se le conoce como «lema de la mariposa», debido a que la figura 15.4, que acompaña al lema, tiene forma de mariposa.

Sean  $H$  y  $K$  subgrupos de un grupo  $G$  y sean  $H^*$  un subgrupo normal de  $H$  y  $K^*$  un subgrupo normal de  $K$ . Aplicando la primera parte del enunciado del lema 15.1 a  $H^*$  y a  $H \cap K$  como subgrupos de  $H$ , vemos que  $H^*(H \cap K)$  es grupo. Argumentos análogos muestran que  $H^*(H \cap K^*)$ ,  $K^*(H \cap K)$  y  $K^*(H^* \cap K)$  también son grupos. Es muy fácil mostrar que  $H^* \cap K$  es un subgrupo normal de  $H \cap K$  (véase el ejercicio 15.2). El mismo argumento, usando el lema 15.1, aplicado a  $H^* \cap K$  y a  $H \cap K^*$  como subgrupos de  $H \cap K$ , muestra que  $L = (H^* \cap K)(H \cap K^*)$  es un grupo. Tenemos así, el retículo de los subgrupos, que se muestra en la figura 15.4. Pueden verificarse fácilmente las relaciones de inclusión indicadas en el diagrama.



**Figura 15.4**

Como  $H \cap K^*$  y  $H^* \cap K$  son ambos subgrupos normales de  $H \cap K$ , la segunda afirmación del lema 15.1 muestra que  $L = (H^* \cap K)(H \cap K^*)$  es un

subgrupo normal de  $H \cap K$ . Hemos denotado esta particular relación de subgrupos normales mediante una línea gruesa en medio de la figura 15.4. Afirmando que las otras dos líneas gruesas también indican relaciones de subgrupos normales y que los tres grupos factores dados por las tres relaciones de subgrupos normales son isomorfos. Para mostrarlo, definiremos un homomorfismo  $\phi: H^*(H \cap K) \rightarrow (H \cap K)/L$ , y mostraremos que  $\phi$  es sobre  $(H \cap K)/L$  con kernel  $H^*(H \cap K^*)$ . De aquí se sigue que  $H^*(H \cap K^*)$  es normal en  $H^*(H \cap K)$  y que  $H^*(H \cap K)/H^*(H \cap K^*) \cong (H \cap K)/L$ . Por simetría, se deduce un resultado análogo para los grupos que se encuentran en la línea gruesa del lado derecho de la figura 15.4.

Sea  $\phi: H^*(H \cap K) \rightarrow (H \cap K)/L$  definida como sigue. Para  $h \in H^*$  y  $x \in H \cap K$  sea  $(hx)\phi = xL$ . Mostremos que  $\phi$  está bien definida y que es un homomorfismo. Sean  $h_1, h_2 \in H^*$  y  $x_1, x_2 \in H \cap K$ . Si  $h_1x_1 = h_2x_2$ , entonces  $h_2^{-1}h_1 = x_2x_1^{-1} \in H^* \cap (H \cap K) = H^* \cap K \subseteq L$ , de modo que  $x_1L = x_2L$ . Así,  $\phi$  está bien definida. Como  $H^*$  es normal en  $H$ , existe  $h_3$  en  $H^*$  tal que  $x_1h_2 = h_3x_1$ . Entonces,

$$\begin{aligned} [(h_1x_1)(h_2x_2)]\phi &= [(h_1h_3)(x_1x_2)]\phi = (x_1x_2)L \\ &= (x_1L)(x_2L) = (h_1x_1)\phi \cdot (h_2x_2)\phi. \end{aligned}$$

Así,  $\phi$  es un homomorfismo.

Es obvio que  $\phi$  es sobre  $(H \cap K)/L$ . Por último, si  $h \in H^*$  y  $x \in H \cap K$ , entonces  $(hx)\phi = xL = L$  si y sólo si  $x \in L$ , o si y sólo si  $hx \in H^*L = H^*(H^* \cap K)(H \cap K^*) = H^*(H \cap K^*)$ . Así,  $\text{Ker}(\phi) = H^*(H \cap K^*)$ .

Hemos probado el lema siguiente:

**Lema 15.2 (Zassenhaus)** *Sean  $H$  y  $K$  subgrupos de un grupo  $G$  y sean  $H^*$  y  $K^*$  subgrupos normales de  $H$  y  $K$  respectivamente. Entonces,*

- 1  *$H^*(H \cap K^*)$  es un subgrupo normal de  $H^*(H \cap K)$ .*
- 2  *$K^*(H^* \cap K)$  es un subgrupo normal de  $K^*(H \cap K)$ .*
- 3  *$H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K)$   
 $\cong (H \cap K)/[(H^* \cap K)(H \cap K^*)]$ .*

### \*15.3 DEMOSTRACION DEL TEOREMA DE SCHREIER

En el capítulo 14 se mostró que el teorema de Jordan-Hölder se desprendía de inmediato del teorema de Schreier (teorema 14.1). Reenunciaremos aquí el teorema de Schreier para facilitar su referencia y daremos la demostración.

**Teorema 15.4 (Schreier)** *Dos series subnormales (normales) de un grupo  $G$  tienen refinamientos isomorfos.*

*Demostración* Sea  $G$  un grupo y sean

$$\{e\} = H_0 < H_1 < H_2 < \cdots < H_n = G \quad [15.1]$$

y

$$\{e\} = K_0 < K_1 < K_2 < \cdots < K_m = G \quad [15.2]$$

dos series subnormales de  $G$ . Para  $i$ , donde  $0 \leq i \leq n - 1$ , forman la cadena de grupos

$$H_i = H_i(H_{i+1} \cap K_0) \leq H_i(H_{i+1} \cap K_1) \leq \cdots \leq H_i(H_{i+1} \cap K_m) = H_{i+1}.$$

Esto inserta  $m - 1$  grupos, no necesariamente distintos, entre  $H_i$  y  $H_{i+1}$ . Si hacemos esto para cada  $i$  donde  $0 \leq i \leq n - 1$ , y hacemos  $H_{i,j} = H_i(H_{i+1} \cap K_j)$ , entonces se obtiene la cadena de grupos

$$\begin{aligned} \{e\} &= H_{0,0} \leq H_{0,1} \leq H_{0,2} \leq \cdots \leq H_{0,m-1} \leq H_{1,0} \\ &\leq H_{1,1} \leq H_{1,2} \leq \cdots \leq H_{1,m-1} \leq H_{2,0} \\ &\leq H_{2,1} \leq H_{2,2} \leq \cdots \leq H_{2,m-1} \leq H_{3,0} \\ &\leq \cdots \\ &\leq H_{n-1,1} \leq H_{n-1,2} \leq \cdots \leq H_{n-1,m-1} \leq H_{n-1,m} = G. \end{aligned} \quad [15.3]$$

Esta cadena [15.3] contiene  $nm + 1$  grupos no necesariamente distintos y  $H_{i,0} = H_i$  para cada  $i$ . Por el lema de Zassenhaus [15.3], es una cadena subnormal, esto es, cada grupo es normal en el siguiente grupo. Esta cadena refina la serie en [15.1].

De manera simétrica, hacemos  $K_{j,i} = K_j(K_{j+1} \cap H_i)$  para  $0 \leq j \leq m - 1$  y  $0 \leq i \leq n$ . Esto da una cadena subnormal

$$\begin{aligned} \{e\} &= K_{0,0} \leq K_{0,1} \leq K_{0,2} \leq \cdots \leq K_{0,n-1} \leq K_{1,0} \\ &\leq K_{1,1} \leq K_{1,2} \leq \cdots \leq K_{1,n-1} \leq K_{2,0} \\ &\leq K_{2,1} \leq K_{2,2} \leq \cdots \leq K_{2,n-1} \leq K_{3,0} \\ &\leq \cdots \\ &\leq K_{m-1,1} \leq K_{m-1,2} \leq \cdots \leq K_{m-1,n-1} \leq K_{m-1,n} = G. \end{aligned} \quad [15.4]$$

Esta cadena [15.4], contiene  $mn + 1$  grupos, no necesariamente distintos y  $K_{j,0} = K_j$  para cada  $j$ . Esta cadena refina la serie en [15.2].

Por el lema de Zassenhaus, tenemos que

$$H_i(H_{i+1} \cap K_{j+1})/H_i(H_{i+1} \cap K_j) \simeq K_j(K_{j+1} \cap H_{i+1})/K_j(K_{j+1} \cap H_i),$$

o

$$H_{i,j+1}/H_{i,j} \simeq K_{j,i+1}/K_{j,i} \quad [15.5]$$

para  $0 \leq i \leq n - 1$  y  $0 \leq j \leq m - 1$ . Los isomorfismos de la ecuación [15.5] dan una correspondencia uno a uno de los grupos factores isomorfos, entre las cadenas subnormales de la ecuación [15.3] y la ecuación [15.4]. Para verificar esta correspondencia, nótese que  $H_{i,0} = H_i$  y  $H_{i,m} = H_{i+1}$  mientras que  $K_{j,0} = K_j$  y  $K_{j,n} = K_{j+1}$ . Cada cadena en la ecuación [15.3] y en la ecuación [15.4] contiene un arreglo rectangular de  $mn$  símbolos  $\leq$ . Cada  $\leq$  da lugar a un grupo factor. Los grupos factores que surgen del  $r$ -ésimo renglón de los  $\leq$  en la ecuación [15.3] corresponden a los grupos factores que surgen de la  $r$ -ésima columna de los  $\leq$  en la ecuación [15.4]. Suprimiendo los grupos repetidos, de las cadenas en la ecuación [15.3] y en la [15.4], obtenemos series subnormales de grupos distintos que son refinamientos isomorfos de las ecuaciones [15.1] y [15.2]. Esto comprueba el teorema para series subnormales.

Para series normales donde todos los  $H_i$  y  $K_j$  son normales en  $G$ , simplemente observamos que todos los grupos  $H_{i,j}$  y  $K_{j,i}$  formados con anterioridad son, además, normales en  $G$  así que se aplica la misma demostración. Esta normalidad de  $H_{i,j}$  y  $K_{j,i}$  se sigue de manera inmediata de la segunda afirmación del lema 15.1 y del hecho de que las intersecciones de subgrupos normales de un grupo producen subgrupos normales. ■

## Ejercicios

\*15.1 Muéstrese que si  $H$  y  $N$  son subgrupos de  $G$  y si  $N$  es normal en  $G$ , entonces  $H \cap N$  es normal en  $H$ .

\*15.2 Sean  $H^*$ ,  $H$  y  $K$  subgrupos de  $G$  con  $H^*$  normal en  $H$ . Muéstrese que  $H^* \cap K$  es normal en  $H \cap K$ .

\*15.3 Sean  $H$ ,  $K$  y  $L$  subgrupos normales de  $G$  con  $H < K < L$ . Sean  $A = G/H$ ,  $B = K/H$  y  $C = L/H$ .

a) Muéstrese que  $B$  y  $C$  son subgrupos normales de  $A$ , y que  $B < C$ .

b) ¿A qué grupo es isomorfo  $(A/B)/(C/B)$ ?

\*15.4 Sean  $K$  y  $L$  subgrupos normales de  $G$  con  $K \vee L = G$  y  $K \cap L = \{e\}$ . Muéstrese que  $G/K \cong L$  y  $G/L \cong K$ .

*Al usar los tres teoremas de isomorfismo, a menudo es necesario conocer la correspondencia real dada por el isomorfismo y no sólo el hecho de que los grupos son isomorfos. Los siguientes seis ejercicios les servirán de «entrenamiento» para ello.*

\*15.5 Sea  $\phi: \mathbf{Z}_{12} \rightarrow \mathbf{Z}_3$  el homomorfismo tal que  $1\phi = 2$ .

a) Encuéntrese el kernel  $K$  de  $\phi$ .

b) Listense las clases laterales en  $\mathbf{Z}_{12}/K$  mostrando los elementos en cada clase lateral.

c) Dése la correspondencia entre  $\mathbf{Z}_{12}/K$  y  $\mathbf{Z}_3$  dada por la transformación  $\psi$  descrita en el teorema 15.1.

\*15.6 Sea  $\phi: \mathbf{Z}_{18} \rightarrow \mathbf{Z}_{12}$  el homomorfismo donde  $1\phi = 10$ .

a) Encuéntrese el kernel  $K$  de  $\phi$ .

b) Listense las clases laterales en  $\mathbf{Z}_{18}/K$  mostrando los elementos en cada clase lateral.

- c) Encuéntrese el grupo  $Z_{18}\phi$ .  
d) Dése la correspondencia entre  $Z_{18}/K$  y  $Z_{18}\phi$  dada por la transformación  $\psi$  descrita en el teorema 15.1.

\*15.7 En el grupo  $Z_{24}$  sea  $H = \langle 4 \rangle$  y  $N = \langle 6 \rangle$ .

- a) Lístense los elementos en  $HN$  (que podemos escribir  $H + N$  para estos grupos aditivos) y en  $H \cap N$ .  
b) Lístense las clases laterales en  $HN/N$  mostrando los elementos en cada clase lateral.  
c) Lístense las clases laterales en  $H/(H \cap N)$  mostrando los elementos en cada clase lateral.  
d) Dése la correspondencia entre  $HN/N$  y  $H/(H \cap N)$  descrita en la demostración del teorema 15.2.

\*15.8 Repítase el ejercicio 15.7 para el grupo  $Z_{36}$  con  $H = \langle 6 \rangle$  y  $N = \langle 9 \rangle$ .

\*15.9 En el grupo  $G = Z_{24}$ , sea  $H = \langle 4 \rangle$  y  $K = \langle 8 \rangle$ .

- a) Lístense las clases laterales en  $G/H$  exhibiendo los elementos en cada clase lateral.  
b) Lístense las clases laterales en  $G/K$  exhibiendo los elementos en cada clase lateral.  
c) Lístense las clases laterales en  $H/K$  exhibiendo los elementos en cada clase lateral.  
d) Lístense las clases laterales en  $(G/K)/(H/K)$  exhibiendo los elementos en cada clase lateral.  
e) Dése la correspondencia entre  $G/H$  y  $(G/K)/(H/K)$  descrita en la demostración del teorema 15.3.

\*15.10 Repítase el ejercicio 15.9 para el grupo  $G = Z_{36}$  con  $H = \langle 9 \rangle$  y  $K = \langle 18 \rangle$ .

\*15.11 Sea  $G$  igual a  $Z_{36}$ . Hágase referencia a la demostración del teorema 15.4.

Sea

$$\{0\} < \langle 12 \rangle < \langle 3 \rangle < Z_{36}$$

la serie subnormal [15.1], y sea

$$\{0\} < \langle 18 \rangle < Z_{36}$$

la serie subnormal [15.2]. Encuéntrese las cadenas [15.3] y [15.4] y exhiban los grupos factores isomorfos como se describieron en la demostración. Escribanse las cadenas [15.3] y [15.4] en el arreglo rectangular mostrado en el texto.

\*15.12 Repítase el ejercicio 15.11 para el grupo  $Z_{24}$  con la serie subnormal [15.1]

$$\{0\} < \langle 12 \rangle < \langle 4 \rangle < Z_{24}$$

y [15.2]

$$\{0\} < \langle 6 \rangle < \langle 3 \rangle < Z_{24}.$$

\*15.13 Muéstrese que un subgrupo  $K$  de un grupo soluble  $G$  es soluble. [Sugerencia: sea  $H_0 = \{e\} < H_1 < \cdots < H_n = G$  una serie de composición para  $G$ . Muéstrese que los distintos grupos  $K \cap H_i$  para  $i = 0, \dots, n$ , forman una serie de composición para  $K$ . Obsérvese que para el teorema 15.2

$$(K \cap H_i)/(K \cap H_{i-1}) \simeq [H_{i-1}(K \cap H_i)]/[H_{i-1}],$$

con  $H = K \cap H_i$  y  $N = H_{i-1}$ , y que  $H_{i-1}(K \cap H_i) \leq H_i$ .]

\*15.14 Sea  $H_0 = \{e\} < H_1 < \cdots < H_n = G$  una serie de composición del grupo  $G$ . Sea  $N$  un subgrupo normal de  $G$  y supóngase que  $N$  es un grupo simple. Muéstrese que los distintos grupos entre  $H_0, H_iN$  para  $i = 0, \dots, n$  también forman una serie de composición para  $G$ . [Sugerencia: por el lema 15.1,  $H_iN$  es un grupo. Muéstrese que  $H_{i-1}N$  es normal en  $H_iN$ . Por el teorema 15.2,

$$(H_iN)/(H_{i-1}N) \simeq H_i/[H_i \cap (H_{i-1}N)],$$

y, por el teorema 15.3, el último grupo es isomorfo a

$$[H_i/H_{i-1}]/[(H_i \cap (H_{i-1}N))/H_{i-1}].$$

Pero  $H_i/H_{i-1}$  es simple.]

\*15.15 Sea  $G$  un grupo y sea  $H_0 = \{e\} < H_1 < \cdots < H_n = G$  una serie de composición para  $G$ . Sea  $N$  un subgrupo normal de  $G$ , y sea  $\gamma: G \rightarrow G/N$  la transformación canónica. Muéstrese que los distintos grupos entre  $H_i\gamma$  para  $i = 0, \dots, n$  forman una serie de composición para  $G/N$ . [Sugerencia: obsérvese que la transformación

$$\psi: H_iN \rightarrow (H_i\gamma)/(H_{i-1}\gamma)$$

definida por

$$(h_iN)\psi = ((h_iN)\gamma)(H_{i-1}\gamma)$$

es un homomorfismo con kernel  $H_{i-1}N$ . Por el teorema 15.1,

$$(H_i\gamma)/(H_{i-1}\gamma) \simeq (H_iN)/(H_{i-1}N).$$

Procédase vía el teorema 15.2 como se mostró en la sugerencia del ejercicio 15.14.]

\*15.16 Pruébese que la imagen homomorfa de un grupo soluble es soluble. [Sugerencia: aplíquese el ejercicio 15.15 para obtener una serie de composición para la imagen homomorfa. Entonces, las sugerencias de los ejercicios 15.14 y 15.15 muestran cómo se ven, en la imagen, los grupos factores de esta serie de composición.]

## \*16

# Acción de un grupo en un conjunto

## \*16.1 EL CONCEPTO DE ACCIÓN DE GRUPO

Ya son familiares las funciones y los productos cartesianos, así que podemos adoptar un punto de vista más sofisticado del concepto de operación binaria en un conjunto  $S$  que aquél que adoptamos en el capítulo 1. Una **operación binaria** en  $S$  es una función que transforma  $S \times S$  en  $S$ . Si denotamos la función por  $*$ , es más convencional expresar  $(s_1, s_2)* = s_3$  como  $s_1 * s_2 = s_3$ . La función  $*$  da una regla para «multiplicar» cualquier elemento de  $S$  por un elemento de  $S$  para producir un elemento de  $S$ .

En general, para cualesquiera conjuntos  $A$ ,  $B$  y  $C$  podemos considerar la transformación  $*: A \times B \rightarrow C$  como definición de una «multiplicación» donde cada elemento  $a$  de  $A$  por cualquier elemento  $b$  de  $B$  tiene como valor algún elemento  $c$  de  $C$ . Escribimos, por supuesto,  $a * b = c$  o simplemente,  $ab = c$ . En este capítulo hablaremos del caso en que  $X$  es un conjunto,  $G$  un grupo y tenemos una transformación  $*: X \times G \rightarrow X$ . Escribiremos  $(x, g)*$  como  $x * g$  o  $xg$ .

**Definición** Sea  $X$  un conjunto y  $G$  un grupo. Una **acción de  $G$  en  $X$**  es una transformación  $*: X \times G \rightarrow X$  tal que:

- 1  $xe = x$  para todas las  $x \in X$
- 2  $x(g_1g_2) = (xg_1)g_2$  para todas las  $x \in X$  y todas las  $g_1, g_2 \in G$ .

Bajo estas condiciones,  $X$  es un *G*-conjunto.

**Ejemplo 16.1** Sea  $X$  cualquier conjunto y  $S_X$  el grupo de todas las permutaciones de  $X$ . Entonces,  $X$  es un  $S_X$ -conjunto donde para  $x \in X$  y  $\sigma \in S_X$ , la acción  $x\sigma$

de  $\sigma$  en  $x$  es el efecto de la permutación  $\sigma$  en  $x$ . La condición 2 se cumple, como consecuencia de la definición de multiplicación de permutaciones como composición de funciones y la condición 1 es inmediata a partir de la definición de la permutación identidad. En particular,  $\{1, 2, 3, \dots, n\}$  es un  $S_n$ -conjunto. ■

**Ejemplo 16.2** Todo grupo  $G$  en sí mismo es un  $G$ -conjunto, donde la acción de  $g_2 \in G$  sobre  $g_1 \in G$  está dada por la multiplicación derecha. Esto es,  $(g_1, g_2)* = g_1g_2$ . Si  $H$  es un subgrupo de  $G$ , también podemos considerar  $G$  como un  $H$ -conjunto donde  $(g, h)* = gh$ . ■

**Ejemplo 16.3** Sea  $H$  un subgrupo de  $G$ . Entonces  $G$  es un  $H$ -conjunto bajo la conjugación, donde  $(g, h)* = h^{-1}gh$  para  $g \in G$  y  $h \in H$ . La condición 1 es obvia y para la condición 2 nótese que  $(g, h_1h_2)* = (h_1h_2)^{-1}g(h_1h_2) = h_2^{-1}(h_1^{-1}gh_1)h_2 = ((g, h_1)*, h_2)*$ . Siempre escribiremos esta acción de  $H$  en  $G$  mediante la conjugación como  $h^{-1}gh$ . La abreviatura  $gh$  descrita antes de la definición, causaría una terrible confusión con la operación de grupo de  $G$ . Veremos en el capítulo 18 que esta acción de  $H$  en  $G$  es muy importante para analizar la estructura del grupo  $G$ . ■

**Ejemplo 16.4** Sea  $H$  un subgrupo de  $G$  y sea  $R_H$  el conjunto de todas las clases laterales derechas de  $H$ . Entonces,  $R_H$  es un  $G$ -conjunto, donde la acción de  $g \in G$  en la clase lateral derecha  $Hx$  está dada por  $(Hx)g = H(xg)$ . Una serie de ejercicios mostrará que cada  $G$ -conjunto es isomorfo al que puede formarse usando estos  $G$ -conjuntos de clases laterales derechas como bloques constitutivos. (Véanse los ejercicios 16.12 al 16.15.)

**Ejemplo 16.5** Sea  $G$  el grupo  $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$  de las simetrías del cuadrado, descrito en el ejemplo 4.2. En la figura 16.1 mostramos el cuadrado con vértices 1, 2, 3, 4, como en la figura 4.6. Además, denominamos a los lados  $s_1, s_2, s_3, s_4$ , a las diagonales  $d_1$  y  $d_2$ , y a los ejes vertical y horizontal  $m_1$  y  $m_2$ , al centro  $C$  y a los puntos medios de los lados  $s_i$ ,  $P_i$ . Recuérdese que  $\rho_i$  corresponde a rotar el cuadrado en sentido contrario al que giran las manecillas del reloj en  $\pi/2$  radianes,  $\mu_i$  corresponde a voltear el cuadrado alrededor del eje  $m_i$ , y  $\delta_i$  a voltear el cuadrado alrededor de la diagonal  $d_i$ .

Sea

$$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}.$$

Entonces,  $X$  se puede considerar como un  $D_4$ -conjunto de la manera obvia. La tabla 16.1 describe en su totalidad la acción de  $D_4$  en  $X$  y se da para proporcionar ilustraciones geométricas de las ideas que se presentarán. Hay que asegurarse de comprender cómo está formada la tabla. ■

Tabla 16.1

	1	2	3	4	$s_1$	$s_2$	$s_3$	$s_4$	$m_1$	$m_2$	$d_1$	$d_2$	$C$	$P_1$	$P_2$	$P_3$	$P_4$
$\rho_0$	1	2	3	4	$s_1$	$s_2$	$s_3$	$s_4$	$m_1$	$m_2$	$d_1$	$d_2$	$C$	$P_1$	$P_2$	$P_3$	$P_4$
$\rho_1$	2	3	4	1	$s_2$	$s_3$	$s_4$	$s_1$	$m_2$	$m_1$	$d_2$	$d_1$	$C$	$P_2$	$P_3$	$P_4$	$P_1$
$\rho_2$	3	4	1	2	$s_3$	$s_4$	$s_1$	$s_2$	$m_3$	$m_2$	$d_3$	$d_2$	$C$	$P_3$	$P_4$	$P_1$	$P_2$
$\rho_3$	4	1	2	3	$s_4$	$s_1$	$s_2$	$s_3$	$m_2$	$m_1$	$d_2$	$d_1$	$C$	$P_4$	$P_1$	$P_2$	$P_3$
$\mu_1$	2	1	4	3	$s_1$	$s_4$	$s_3$	$s_2$	$m_1$	$m_2$	$d_2$	$d_1$	$C$	$P_1$	$P_4$	$P_3$	$P_2$
$\mu_2$	4	3	2	1	$s_3$	$s_2$	$s_1$	$s_4$	$m_1$	$m_2$	$d_3$	$d_1$	$C$	$P_3$	$P_2$	$P_1$	$P_4$
$\delta_1$	3	2	1	4	$s_2$	$s_1$	$s_4$	$s_3$	$m_2$	$m_1$	$d_1$	$d_2$	$C$	$P_2$	$P_1$	$P_4$	$P_3$
$\delta_2$	1	4	3	2	$s_4$	$s_3$	$s_2$	$s_1$	$m_2$	$m_1$	$d_1$	$d_2$	$C$	$P_4$	$P_3$	$P_2$	$P_1$

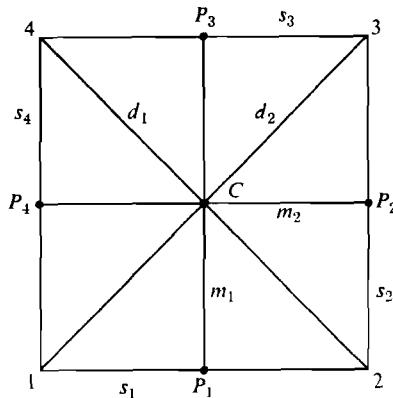


Figura 16.1

## \*16.2 CONJUNTOS FIJOS Y SUBGRUPOS DE ISOTROPIA

Sea  $X$  un  $G$ -conjunto. Sea  $x \in X$  y  $g \in G$ . Será importante saber cuándo  $xg = x$ .  
Sea

$$X_g = \{x \in X \mid xg = x\} \quad \text{y} \quad G_x = \{g \in G \mid xg = x\}.$$

**Ejemplo 16.6** Para el  $D_4$ -conjunto  $X$  del ejemplo 16.5 tenemos

$$X_{\rho_0} = X, \quad X_{\rho_1} = \{C\}, \quad X_{\mu_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}$$

Además, con  $G = D_4$

$$G_1 = \{\rho_0, \delta_2\}, \quad G_{s_3} = \{\rho_0, \mu_1\}, \quad G_{d_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\}.$$

Dejamos el cálculo de los otros  $X_\sigma$  y  $G_x$  para los ejercicios 16.1 y 16.2. ■

Quizás el lector ya haya observado que los subconjuntos  $G_x$  dados en el ejemplo anterior fueron, en cada caso, subgrupos de  $G$ . Esto es cierto en general.

**Teorema 16.1** *Sea  $X$  un  $G$ -conjunto. Entonces,  $G_x$  es un subgrupo de  $G$  para cada  $x \in X$ .*

**Demuestra**ción Sea  $x \in X$  y sea  $g_1, g_2 \in G_x$ . Entonces,  $xg_1 = x$  y  $xg_2 = x$ . Por tanto,  $x(g_1g_2) = (xg_1)g_2 = xg_2 = x$ , de modo que  $g_1g_2 \in G_x$  y  $G_x$  es cerrado bajo la operación inducida de  $G$ . Claro que  $xe = x$ , de modo que  $e \in G_x$ . Si  $g \in G_x$  entonces,  $xg = x$ , de modo que  $x = xe = x(gg^{-1}) = (xg)g^{-1} = xg^{-1}$  y, por tanto,  $g^{-1} \in G_x$ . Así,  $G_x$  es un subgrupo de  $G$ . ■

**Definición** Sea  $X$  un  $G$ -conjunto y sea  $x \in X$ . El subgrupo  $G_x$  es el **subgrupo de isotropia de  $x$** .

## \*16.3 ORBITAS

Para el  $D_4$ -conjunto  $X$  del ejemplo 16.5 con la tabla de acción en la tabla 16.1, los elementos del subconjunto  $\{1, 2, 3, 4\}$  van a dar, bajo la acción de  $D_4$ , a elementos del mismo subconjunto. Más aún, cada uno de los elementos 1, 2, 3 y 4 va a dar a todos los otros elementos del subconjunto, mediante los diversos elementos de  $D_4$ . Procedemos a mostrar que es posible partir todo  $G$ -conjunto  $X$  en subconjuntos de este tipo.

**Teorema 16.2** *Sea  $X$  un  $G$ -conjunto. Para  $x_1, x_2 \in X$ , sea  $x_1 \sim x_2$  si y sólo si existe  $g \in G$  tal que  $x_1g = x_2$ . Entonces  $\sim$  es una relación de equivalencia en  $S$ .*

**Demuestra**ción Para cada  $x \in X$  tenemos  $xe = x$ , de modo que  $x \sim x$  y  $\sim$  es reflexiva.

Supóngase que  $x_1 \sim x_2$ , de modo que  $x_1g = x_2$  para alguna  $g \in G$ . Entonces,  $x_2g^{-1} = (x_1g)g^{-1} = x_1(gg^{-1}) = x_1e = x_1$ , de modo que  $x_2 \sim x_1$  y  $\sim$  es simétrica.

Por último, si  $x_1 \sim x_2$  y  $x_2 \sim x_3$ , entonces  $x_1g_1 = x_2$  y  $x_2g_2 = x_3$  para algunos  $g_1, g_2 \in G$ . Entonces,  $x_1(g_1g_2) = (x_1g_1)g_2 = x_2g_2 = x_3$ , de modo que  $x_1 \sim x_3$  y  $\sim$  es transitiva. ■

**Definición** Sea  $X$  un  $G$ -conjunto. Cada celda en la partición de la relación de equivalencia, descrita en el teorema 16.2, es una **órbita en  $X$  bajo  $G$** . Si  $x \in X$ , la celda que contiene a  $x$  es la **órbita de  $x$** . Denotamos esta celda por  $xG$ .

La relación entre las órbitas de  $X$  y la estructura de grupo de  $G$  es central en las aplicaciones que aparecen en los dos capítulos siguientes. El teorema a

continuación expone esta relación. Recuérdese que para un conjunto  $X$  usamos  $|X|$  para el número de elementos en  $X$  y  $(G:H)$  es el índice de un subgrupo  $H$  en un grupo  $G$ .

**Teorema 16.3** *Sea  $X$  un  $G$ -conjunto y sea  $x \in X$ . Entonces  $|xG| = (G:G_x)$ .*

**Demostración** Definimos una transformación  $\phi$  uno a uno de  $xG$  sobre la colección de clases laterales derechas de  $G_x$  en  $G$ . Sea  $x_1 \in xG$ . Entonces, existe  $g_1 \in G$  tal que  $xg_1 = x_1$ . Definimos  $x_1\phi$  como la clase lateral derecha  $G_{x_1}g_1$  de  $G_{x_1}$ . Debemos mostrar que esta transformación  $\phi$  está bien definida, y es independiente de la selección de  $g_1 \in G$ . Supóngase que también  $xg'_1 = x_1$ . Entonces,  $xg_1 = xg'_1$ , de modo que  $(xg_1)g_1^{-1} = (xg'_1)g_1^{-1}$  de donde deducimos que  $x = x(g_1g_1^{-1})$  por tanto,  $g_1g_1^{-1} \in G_x$ , entonces,  $g_1 \in G_{x_1}g_1$  y  $G_{x_1}g_1 = G_{x_1}g'_1$ . Así, la transformación  $\phi$  está bien definida.

Para mostrar que la transformación  $\phi$  es uno a uno, supóngase que  $x_1, x_2 \in xG$  y que  $x_1\phi = x_2\phi$ . Entonces, existen  $g_1, g_2 \in G$  tales que  $x_1 = xg_1$ ,  $x_2 = xg_2$  y  $g_2 \in G_{x_1}g_1$ . Entonces,  $g_2 = gg_1$  para alguna  $g \in G_x$ , de modo que  $x_2 = xg_2 = x(gg_1) = (xg)g_1 = xg_1 = x_1$ . Así,  $\phi$  es uno a uno.

Para concluir, mostremos que cada clase lateral derecha de  $G_x$  en  $G$  es de la forma  $x_1\phi$  para alguna  $x_1 \in xG$ . Sea  $G_{x_1}g_1$  una clase lateral derecha. Entonces, si  $x_1 = xg_1$ , tenemos  $G_{x_1}g_1 = x_1\phi$ . Así,  $\phi$  lleva a  $xG$  sobre la colección de clases laterales derechas. ■

**Ejemplo 16.7** Sea  $X$  el  $D_4$ -conjunto en el ejemplo 16.5, con la tabla de acción dada en la tabla 16.1. Con  $G = D_4$  tenemos  $1G = \{1, 2, 3, 4\}$  y  $G_1 = \{\rho_0, \delta_2\}$ . Como  $|G| = 8$  tenemos que  $|1G| = (G:G_1) = 4$ . ■

No basta recordar sólo la ecuación de cardinalidad del teorema 16.3, sino además, que los *elementos de  $G$  que llevan  $x$  a  $xg_1$  son precisamente los elementos de la clase lateral derecha  $G_{x_1}g_1$* . Esto es claro a partir de la demostración.

## Ejercicios

---

*En los ejercicios 1 al 3 sea*

$$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}$$

*el  $D_4$ -conjunto del ejemplo 16.5 con tabla de acción dada en la tabla 16.1. Encuéntrese lo siguiente, donde  $G = D_4$ .*

- \*16.1 Los conjuntos fijos  $X_\sigma$  para cada  $\sigma \in D_4$ , esto es,  $X_{\rho_0}, X_{\rho_1}, \dots, X_{\delta_2}$ .
- \*16.2 Los grupos de isotropía  $G_x$  para cada  $x \in X$ , esto es,  $G_1, G_2, \dots, G_{P_3}, G_{P_4}$ .
- \*16.3 Las órbitas en  $X$  bajo  $D_4$ .
- \*16.4 Un  $G$ -conjunto  $X$  no vacío es **transitivo** si para cada  $x_1, x_2 \in X$  existe  $g \in G$  tal que  $x_1g = x_2$ . Caracterícese un  $G$ -conjunto transitivo en términos de sus órbitas.

## 160 ACCIÓN DE UN GRUPO EN UN CONJUNTO

\*16.5 Sea  $X$  un  $G$ -conjunto y sea  $S \subseteq X$ . Si  $sG \subseteq S$  para todas las  $s \in S$ , entonces  $S$  es un **sub- $G$ -conjunto**. Caracterícese un sub- $G$ -conjunto de un  $G$ -conjunto  $X$  en términos de las órbitas en  $X$  bajo  $G$ .

\*16.6 Sean  $X$  y  $Y$   $G$ -conjuntos con el *mismo* grupo  $G$ . Un **isomorfismo** entre los  $G$ -conjuntos  $X$  y  $Y$  es una transformación  $\phi: X \rightarrow Y$  tal que es uno a uno, sobre  $Y$  y satisface  $(x\phi)g = (xg)\phi$  para todas las  $x \in X$  y  $g \in G$ . Dos  $G$ -conjuntos son **isomorfos** si existe tal isomorfismo entre ellos. Sea  $X$  el  $D_4$ -conjunto del ejemplo 16.5.

- Encuéntrense dos órbitas distintas de  $X$  que sean sub- $D_4$ -conjuntos isomorfos.
- Muéstrese que las órbitas  $\{1, 2, 3, 4\}$  y  $\{s_1, s_2, s_3, s_4\}$  no son sub- $D_4$ -conjuntos isomorfos. [Sugerencia: encuéntrese un elemento de  $G$  que actúa de manera esencialmente diferente en las dos órbitas.]
- Las órbitas que se dieron como respuesta a la parte a), ¿son los dos únicos sub- $D_4$ -conjuntos isomorfos, diferentes, de  $X$ ?

16.7 Un grupo  $G$  actúa **fielmente** en un  $G$ -conjunto  $X$  si la identidad es el único elemento de  $G$  que deja fijo a todo elemento de  $X$ . Sea  $X$  el  $D_4$ -conjunto del ejemplo 16.5.

- ¿ $D_4$  actúa fielmente en  $X$ ?
- Encuéntrense todas las órbitas en  $X$  en las cuales  $D_4$  actúa fielmente como sub- $D_4$ -conjunto.

\*16.8 Sea  $X$  un  $G$ -conjunto. Con referencia al ejercicio 16.7, muéstrese que  $G$  actúa fielmente en  $X$  si y sólo si no hay dos elementos distintos de  $G$  que tengan la misma acción en cada elemento de  $X$ .

\*16.9 Sea  $X$  un  $G$ -conjunto y sea  $Y \subseteq X$ . Sea  $G_Y = \{g \in G \mid yg = y \text{ para todas las } y \in Y\}$ . Generalizando el teorema 16.1, muéstrese que  $G_Y$  es un subgrupo de  $G$ .

\*16.10 ¿Falso o verdadero?

- a) Todo  $G$ -conjunto es, además, un grupo.
- b) Cada elemento de un  $G$ -conjunto queda fijo bajo la identidad de  $G$ .
- c) Si todo elemento de un  $G$ -conjunto queda fijo bajo el mismo elemento  $g$  de  $G$ , entonces  $g$  debe ser la identidad  $e$ .
- d) Sea  $X$  un  $G$ -conjunto con  $x_1, x_2 \in X$  y  $g \in G$ . Si  $x_1g = x_2g$  entonces  $x_1 = x_2$ .
- e) Sea  $X$  un  $G$ -conjunto con  $x \in X$  y  $g_1, g_2 \in G$ . Si  $xg_1 = xg_2$ , entonces  $g_1 = g_2$ .
- f) Cada órbita de un  $G$ -conjunto  $X$  es un sub- $G$ -conjunto transitivo.
- g) Sea  $X$  un  $G$ -conjunto y sea  $H \leq G$ . Entonces, se puede considerar  $X$ , de manera natural, como un  $H$ -conjunto.
- h) Con referencia a g), las órbitas de  $X$  bajo  $H$  son las mismas que las órbitas en  $X$  bajo  $G$ .
- i) Si  $X$  es un  $G$ -conjunto, entonces cada elemento de  $G$  actúa como una permutación de  $X$ .
- j) Sea  $X$  un  $G$ -conjunto y sea  $x \in X$ . Si  $G$  es finito, entonces  $|G| = |xG| \cdot |G_x|$ .

\*16.11 Sea  $G$  el grupo aditivo de los números reales. Sea la acción de  $\theta \in G$  sobre el plano real  $\mathbf{R}^2$  dada por la rotación del plano alrededor del origen, en sentido contrario al que giran las manecillas del reloj, en  $\theta$  radianes. Sea  $P$  un punto del plano distinto del origen.

- Muéstrese que  $\mathbf{R}^2$  es un  $G$ -conjunto.
- Describase en términos geométricos la órbita que contiene a  $P$ .
- Encuéntrese el grupo  $G_P$ .

Los ejercicios 12 al 15, muestran cómo pueden formarse todos los  $G$ -conjuntos posibles, salvo isomorfismo, a partir de un grupo  $G$ .

\*16.12 Sea  $\{X_i \mid i \in I\}$  una colección ajena de conjuntos, es decir,  $X_i \cap X_j = \emptyset$  para  $i \neq j$ . Sea cada  $X_i$  un  $G$ -conjunto para el mismo grupo  $G$ .

- Muéstrese que  $\bigcup_{i \in I} X_i$  puede verse, de manera natural, como un  $G$ -conjunto, la **unión** de los  $G$ -conjuntos  $X_i$ .
- Muéstrese que todo  $G$ -conjunto  $X$  es la unión de sus órbitas.

\*16.13 Sea  $X$  un  $G$ -conjunto transitivo y sea  $x_0 \in X$ . Muéstrese que  $X$  es isomorfo al  $G$ -conjunto  $R$  de clases laterales derechas de  $G_{x_0}$  descrito en el ejemplo 16.4. [Sugerencia: para  $x \in X$  supóngase que  $x = x_0g$  y definir  $\phi: X \rightarrow R$  por  $x\phi = G_{x_0}g$ . Asegúrese de mostrar que  $\phi$  está bien definida.]

\*16.14 Sean  $X_i$  para  $i \in I$ ,  $G$ -conjuntos para el mismo grupo  $G$  y supóngase que los conjuntos  $X_i$  no necesariamente son ajenos. Sea  $X'_i = \{(x, i) \mid x \in X_i\}$  para cada  $i \in I$ . Entonces, los conjuntos  $X'_i$  son ajenos y podemos considerarlos, todavía, como  $G$ -conjuntos, de manera obvia. (Los elementos de  $X_i$  se han marcado con  $i$  para distinguirlos de los elementos de  $X_j$  para  $i \neq j$ .) El  $G$ -conjunto  $\bigcup_{i \in I} X'_i$  es la **unión ajena** de los  $G$ -conjuntos  $X_i$ . Usando los ejercicios 16.12 y 16.13, muéstrese que todo  $G$ -conjunto es isomorfo a una unión ajena de los  $G$ -conjuntos de clases laterales derechas, descritas en el ejemplo 16.4.

\*16.15 Los ejercicios anteriores muestran que todo  $G$ -conjunto es isomorfo a una unión ajena de  $G$ -conjuntos de clases laterales derechas. Surge entonces la cuestión de si los  $G$ -conjuntos de clases laterales derechas de subgrupos distintos  $H$  y  $K$  pueden ser isomorfos. Nótese que la transformación definida en la sugerencia del ejercicio 16.13 depende de la selección de  $x_0$  como «punto base». Si  $x_0$  se reemplaza por  $x_0g_0$  y si  $G_{x_0} \neq G_{x_0g_0}$ , entonces las colecciones  $R_H$  de clases laterales derechas de  $H = G_{x_0}$  y  $R_K$  de clases laterales derechas de  $K = G_{x_0g_0}$  forman  $G$ -conjuntos distintos que deben ser isomorfos, pues ambos,  $R_H$  y  $R_K$ , son isomorfos a  $X$ .

- Sea  $X$  un  $G$ -conjunto transitivo y sea  $x_0 \in X$  y  $g_0 \in G$ . Si  $H = G_{x_0}$ , describase  $K = G_{x_0g_0}$  en términos de  $H$  y  $g_0$ .
- Basados en a) averígüense condiciones para los subgrupos  $H$  y  $K$  de  $G$  tales que los  $G$ -conjuntos de clases laterales derechas de  $H$  y de  $K$  sean isomorfos.
- Pruébese la conjectura enunciada para b).

\*16.16 Salvo isomorfismo, ¿cuántos conjuntos  $Z_4$  transitivos  $X$  hay? (Usense los ejercicios anteriores.) Dése un ejemplo de cada tipo de isomorfismo, listando una tabla de acción para cada uno, como en la tabla 16.1. Considerérense elementos del conjunto  $X$  las letras minúsculas  $a, b, c$  y demás.

\*16.17 Repítase el ejercicio 16.16 para el grupo  $Z_6$ .

\*16.18 Repítase el ejercicio 16.16 para el grupo  $S_3$ . Lístense los elementos de  $S_3$  en el orden  $\iota, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)$ .

## **Aplicaciones de los G-conjuntos al conteo**

Esta sección presenta una aplicación al conteo, de nuestro trabajo con G-conjuntos. Supóngase, por ejemplo, que se desea contar de cuántas maneras distintas se pueden marcar las seis caras de un cubo, con uno hasta seis puntos, para formar un dado. El dado usual está marcado de manera que, cuando se coloca sobre una mesa con el 1 hacia abajo y el 2 hacia el frente, el 6 está hacia arriba, el 3 hacia la izquierda, el 4 hacia la derecha y el 5 hacia atrás. Claramente, es posible marcar el cubo de otra manera, para dar un dado distinto.

Distingamos, por el momento, las caras del cubo y llamémosles abajo, arriba, izquierda, derecha, frente y atrás. Entonces, abajo puede tener cualquiera de las seis marcas, de uno a seis puntos; arriba podrá tener cualquiera de las cinco marcas restantes, y así sucesivamente. Hay  $6! = 720$  maneras en total, de marcar las caras del cubo. Algunas maneras de marcar, producen el mismo dado que otras, en el sentido de que una marcación puede llevarse a otra, mediante una rotación del cubo marcado. Por ejemplo, si el dado usual, descrito antes, se rota  $90^\circ$  en sentido contrario al que giran las manecillas del reloj, según se le mira desde arriba, entonces el 3 quedará en la cara de enfrente en lugar del 2, pero es el mismo dado.

Hay 24 posiciones posibles de un cubo sobre una mesa, pues cualquiera de las seis caras puede colocarse hacia abajo y después, cualquiera de cuatro hacia el frente, esto da  $6 \cdot 4 = 24$  posiciones posibles. Cualquier posición se puede alcanzar, a partir de cualquier otra, mediante una rotación del dado. Estas rotaciones forman un grupo  $G$ , el cual es isomorfo a un subgrupo de  $S_8$  (véase el ejercicio 4.10). Sea  $X$  el conjunto de las 720 maneras posibles de marcar un cubo y sea la acción de  $G$  en  $X$  mediante la rotación del cubo. Consideraremos que dos marcaciones dan el mismo dado, si podemos llevar una en la otra bajo la acción de algún elemento de  $G$ , esto es, mediante alguna rotación del cubo. En otras palabras, consideraremos que cada órbita en  $X$  bajo  $G$  corresponde a un solo dado

y que órbitas diferentes dan datos diferentes. La determinación del número de datos distintos nos conduce, entonces, a la cuestión de determinar el número de órbitas bajo  $G$  en un  $G$ -conjunto  $X$ .

El siguiente teorema proporciona una herramienta para determinar el número de órbitas en un  $G$ -conjunto  $X$  bajo  $G$ . Recuérdese que para cada  $g \in G$  tenemos el conjunto  $X_g$  de los elementos de  $X$  que permanecen fijos bajo  $g$ , de modo que  $X_g = \{x \in X \mid xg = x\}$ . Recuérdese también, que para cada  $x \in X$  tenemos  $G_x = \{g \in G \mid xg = x\}$  y que  $xG$  es la órbita de  $x$  bajo  $G$ .

**Teorema 17.1 (Burnside)** *Sea  $G$  un grupo finito y  $X$  un  $G$ -conjunto finito. Si  $r$  es el número de órbitas en  $X$  bajo  $G$ , entonces*

$$r \cdot |G| = \sum_{g \in G} |X_g|. \quad [17.1]$$

*Demostración* Consideremos todos los pares  $(x, g)$  donde  $xg = x$  y sean  $N$  el número de dichos pares. Para cada  $g \in G$  hay  $|X_g|$  pares que tienen a  $g$  como segundo miembro. Así,

$$N = \sum_{g \in G} |X_g|. \quad [17.2]$$

Por otro lado, para cada  $x \in X$  hay  $|G_x|$  pares que tienen a  $x$  como primer elemento. Así, tenemos también que

$$N = \sum_{x \in X} |G_x|.$$

Por el teorema 16.3, tenemos  $|xG| = (G:G_x)$ . Pero sabemos que  $(G:G_x) = |G|/|G_x|$  así, obtenemos  $|G_x| = |G|/|xG|$ . Entonces,

$$N = \sum_{x \in X} \frac{|G|}{|xG|} = |G| \left( \sum_{x \in X} \frac{1}{|xG|} \right).$$

Ahora bien,  $1/|xG|$  tiene el mismo valor para todas las  $x$  en la misma órbita y si  $\mathcal{O}$  es cualquier órbita, entonces

$$\sum_{x \in \mathcal{O}} \frac{1}{|xG|} = 1.$$

Así, obtenemos

$$N = |G| (\text{número de órbitas en } X \text{ bajo } G) = |G| \cdot r. \quad [17.3]$$

La comparación de la ecuación [17.2] con la [17.3] da la ecuación [17.1]. ■

**Corolario** Si  $G$  es un grupo finito y  $X$  es un  $G$ -conjunto finito, entonces

$$(\text{número de órbitas en } X \text{ bajo } G) = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

**Demostración** La demostración de este corolario resulta inmediatamente del teorema anterior. ■

Como primer ejemplo, continuemos con el cálculo del número de dados distintos.

**Ejemplo 17.1** Sea  $X$  el conjunto de las 720 marcaciones distintas de las caras de un cubo, usando de uno hasta seis puntos. Sea  $G$  el grupo de las 24 rotaciones del cubo, como lo analizamos con anterioridad. Vimos que el número de dados distintos es el número de órbitas en  $X$  bajo  $G$ . Ahora bien,  $|G| = 24$ . Para  $g \in G$  donde  $g \neq e$ , tenemos  $|X_g| = 0$  porque cualquier rotación diferente a la identidad cambia cualquiera de las 720 marcas por otra distinta. Sin embargo,  $|X_e| = 720$  pues la identidad deja fijas las 720 marcaciones. Entonces, por el corolario del teorema 17.1,

$$(\text{número de órbitas}) = \frac{1}{24} \cdot 720 = 30$$

así que hay treinta dados distintos. ■

Es claro que se puede contar el número de dados distintos, sin utilizar la maquinaria del corolario anterior, sino usando combinatoria elemental, como a menudo se enseña en los primeros cursos de matemáticas finitas. Al marcar un cubo para hacer un dado, se puede suponer por rotación, si es necesario, que la cara marcada con 1 está abajo. Hay cinco selecciones posibles para la cara de arriba (la opuesta). Al rotar el dado según se ve desde arriba, cualquiera de las cuatro caras restantes se puede colocar en la posición del frente, así que no hay selecciones diferentes en lo que se refiere a la cara frontal. Pero, con respecto al número en la cara frontal, hay  $3 \cdot 2 \cdot 1$  posibilidades para las tres caras laterales restantes. Así pues, hay  $5 \cdot 3 \cdot 2 \cdot 1 = 30$  posibilidades en total.

Los siguientes dos ejemplos aparecen en algunos textos de matemáticas finitas y son fáciles de resolver por medios elementales. Usamos el corolario del teorema 17.1 para tener más práctica en pensar en términos de órbitas.

**Ejemplo 17.2** ¿De cuántas maneras distintas se pueden sentar siete personas en una mesa redonda, donde no hay una «cabecera» de mesa? Claro que hay  $7!$  maneras de asignar personas a sillas diferentes. Sea  $X$  el conjunto de las  $7!$  asignaciones posibles. Una rotación de gente se logra al mover cada persona un lugar hacia la derecha y produce el mismo arreglo. Dicha rotación genera un grupo cíclico  $G$  de orden 7, el cual consideraremos actúa sobre  $X$  de la manera obvia. De nuevo, sólo la identidad  $e$  deja cualquier arreglo fijo y deja fijos los  $7!$  arreglos. Por el corolario del teorema 17.1,

$$(\text{número de órbitas}) = \frac{1}{7} \cdot 7! = 6! = 720. ■$$

**Ejemplo 17.3** ¿Cuántos collares distintos (sin broche) se pueden hacer, usando siete cuentas de diferentes colores y del mismo tamaño? A diferencia de la mesa en el ejemplo 17.2, el collar se puede voltear, además de rotarse. Así, consideremos todo el grupo diédrico  $D_7$  de orden  $2 \cdot 7 = 14$  actuando en el conjunto  $X$  de  $7!$  posibilidades. Entonces, el número de collares distintos es

$$(\text{número de órbitas}) = \frac{1}{14} \cdot 7! = 360. \blacksquare$$

Al usar el corolario del teorema 17.1, debemos calcular  $|G|$  y  $|X_g|$  para cada  $g \in G$ . En los ejemplos y ejercicios,  $|G|$  no será un verdadero problema. Demos un ejemplo donde  $|X_g|$  no sea tan trivial de calcular como en los ejemplos anteriores. Supondremos que el lector sabe combinatoria muy elemental.

**Ejemplo 17.4** Encontremos el número de maneras diferentes en que pueden pintarse las aristas de un triángulo equilátero, si disponemos de cuatro colores distintos, suponiendo que se usa un solo color en cada arista y que puede usarse el mismo color en aristas diferentes.

Claramente, hay  $4^3 = 64$  maneras en total, de pintar las aristas, pues cada una de las tres puede ser de cualquiera de los cuatro colores. Consideremos  $X$  como el conjunto de estos 64 triángulos pintados posibles. El grupo  $G$  actuando en  $X$  es el grupo de simetrías del triángulo que es isomorfo a  $S_3$  y consideramos que es  $S_3$ . Usemos, para los elementos de  $S_3$ , la notación dada en el capítulo 4. Necesitamos calcular  $|X_g|$  para cada uno de los seis elementos  $g$  en  $S_3$ .

$ X_{\rho_0}  = 64$	todo triángulo pintado queda fijo bajo $\rho_0$ .
$ X_{\rho_1}  = 4$	para ser invariante bajo $\rho_1$ , todas las aristas deben ser del mismo color y hay 4 colores posibles.
$ X_{\rho_2}  = 4$	por la misma razón que para $\rho_1$ .
$ X_{\mu_1}  = 16$	las aristas que se intercambian deben ser del mismo color (4 posibilidades) y la otra arista también puede ser de cualquiera de los colores (por 4 posibilidades).
$ X_{\mu_2}  =  X_{\mu_3}  = 16$	por la misma razón que para $\mu_1$ .

Entonces

$$\sum_{g \in S_3} |X_g| = 64 + 4 + 4 + 16 + 16 + 16 = 120.$$

Así,

$$(\text{número de órbitas}) = \frac{1}{6} \cdot 120 = 20,$$

y hay veinte triángulos pintados, distintos. ■

**Ejemplo 17.5** Repitamos el ejemplo 17.4 con la hipótesis de que se usa un color diferente para cada arista. El número de maneras posibles de pintar las aristas es entonces  $4 \cdot 3 \cdot 2 = 24$ ; sea  $X$  el conjunto de los 24 triángulos pintados posibles. De nuevo es posible considerar  $S_3$  como el grupo que actúa en  $X$ . Como todas las aristas son de distinto color, vemos que  $|X_{\rho_0}| = 24$  mientras que  $|X_g| = 0$  para  $g \neq \rho_0$ . Así,

$$(\text{número de órbitas}) = \frac{1}{6} \cdot 24 = 4$$

así que hay 4 triángulos distintos. ■

## Ejercicios

---

*En cada uno de los ejercicios siguientes, empléese el corolario del teorema 17.1 para resolver el problema, aunque la respuesta se pueda obtener por métodos más elementales.*

\*17.1 Encuéntrese el número de órbitas en  $\{1, 2, 3, 4, 5, 6, 7, 8\}$  bajo el subgrupo cíclico  $\langle(1, 3, 5, 6)\rangle$  de  $S_8$ .

\*17.2 Encuéntrese el número de órbitas en  $\{1, 2, 3, 4, 5, 6, 7, 8\}$  bajo el subgrupo de  $S_8$  generado por  $(1, 3)$  y  $(2, 4, 7)$ .

\*17.3 Encuéntrese el número de dados distintos con forma de tetraedro, que se pueden formar colocando uno, dos, tres y cuatro puntos en las caras de un tetraedro regular en lugar de un cubo.

\*17.4 Se desea pintar cubos de madera, cada cara de diferente color, para hacer juguetes. ¿Cuántos cubos distintos se pueden hacer, si se dispone de ocho colores de pintura?

\*17.5 Respóndase el ejercicio 17.4 si los colores se pueden repetir a voluntad en caras distintas. [Sugerencia: las veinticuatro rotaciones de un cubo constan de la identidad, nueve que dejan invariante un par de caras opuestas, ocho que dejan invariante un par de vértices opuestos y seis que dejan invariante un par de aristas opuestas.]

\*17.6 Cada una de las ocho esquinas del cubo se pintará con uno de cuatro colores, cada color se puede usar desde en una, hasta en las ocho esquinas. Encuéntrese el número de marcaciones distintas posibles. (Véase la sugerencia del ejercicio 17.5.)

\*17.7 Encuéntrese el número de maneras distintas en que se pueden pintar las orillas de una tarjeta cuadrada, si se dispone de seis colores de pintura y

- a) ningún color se puede usar más de una vez,
- b) se puede usar el mismo color en cualquier número de orillas.

\*17.8 Considérense seis alambres rectos de igual longitud, con los extremos soldados para formar las aristas de un tetraedro regular. En medio de cada alambre se insertará una resistencia de 50 ohms o de 100 ohms. Supóngase que se dispone de al menos seis de cada tipo de resistencia. ¿Cuántos alambrados, esencialmente distintos, son posibles?

\*17.9 Cada una de las seis caras de un prisma rectangular de 60 cm de largo, con extremos de 30 cm cuadrados, se pintará con uno de seis colores posibles. ¿Cuántos prismas pintados, distintos, son posibles si

- a) ningún color se puede repetir en caras distintas?
- b) cada color se puede usar en cualquier número de caras?

## \* 18

## Teoremas de Sylow

El teorema 9.3 proporciona información completa acerca de todos los grupos abelianos finitos. El estudio de los grupos no abelianos finitos es mucho más complicado. Los teoremas de Sylow dan alguna información importante sobre ellos.

Sabemos que el orden de un subgrupo de un grupo finito  $G$  debe dividir a  $|G|$ . Si  $G$  es abeliano, existen subgrupos de todo orden que divida a  $|G|$ . Al final del capítulo 11, mencionamos que esto no era cierto para grupos no abelianos; se puede mostrar que  $A_4$  no tiene subgrupo de orden 6. Los teoremas de Sylow aseguran que para la potencia de un primo que divide a  $|G|$ , existe un subgrupo cuyo orden es esa potencia de un primo. También dan alguna información acerca del número de dichos subgrupos.

Las demostraciones de los teoremas de Sylow son otra aplicación de la acción de un grupo en un conjunto. En esta ocasión el conjunto se forma a partir del grupo; en algunos casos, el conjunto es el grupo mismo, otras veces, es una colección de clases laterales de un subgrupo y otras más, es una colección de subgrupos.

### \*18.1 $p$ -GRUPOS

En el capítulo anterior dimos aplicaciones de una ecuación que contaba el número de órbitas en un  $G$ -conjunto finito. La mayoría de los resultados en esta sección provienen de una ecuación que cuenta el número de elementos en un  $G$ -conjunto finito.

Sea  $X$  un  $G$ -conjunto finito. Recuérdese que para  $x \in X$ , la órbita de  $x$  en  $X$  bajo  $G$  es  $xG = \{xg \mid g \in G\}$ . Supóngase que hay  $r$  órbitas en  $X$  bajo  $G$  y sea

$\{x_1, x_2, \dots, x_r\}$  un conjunto que contiene un elemento de cada órbita en  $X$ . Como todo elemento de  $X$  está precisamente en una órbita, tenemos que

$$|X| = \sum_{i=1}^r |x_i G|. \quad [18.1]$$

Puede haber órbitas en  $X$  con un solo elemento. Sea  $X_G = \{x \in X \mid xg = x \text{ para todas las } g \in G\}$ .  $X_G$  es, precisamente, la unión de las órbitas en  $X$  con un solo elemento. Supóngase que hay  $s$  órbitas con un solo elemento, donde  $0 \leq s \leq r$ . Entonces,  $|X_G| = s$  y podemos reescribir la ecuación [18.1] como

$$|X| = |X_G| + \sum_{i=s+1}^r |x_i G|. \quad [18.2]$$

Gran parte de los resultados de este capítulo se obtendrán a partir de la ecuación [18.2]. Desarrollaremos la teoría de Sylow como en Hungerford [9], donde se da el crédito a R. J. Nunke por la idea que se sigue en la demostración. Ahí se da crédito por la demostración del teorema 18.2 (Teorema de Cauchy) a J. H. McKay.

El teorema 18.1 no es precisamente un teorema de conteo, pero si tiene una conclusión numérica. Cuenta módulo  $p$ . El teorema parece ser muy poderoso. En el resto del capítulo, si escogemos el conjunto adecuado, la acción de grupo adecuada y aplicamos el teorema 18.1, lo que buscamos parece caernos del cielo. Comparados con las demostraciones antiguas, estos argumentos son extremadamente bellos y elegantes.

En todo el capítulo,  $p$  será siempre un entero primo.

**Teorema 18.1** *Sea  $G$  un grupo de orden  $p^n$  y sea  $X$  un  $G$ -conjunto finito. Entonces,  $|X| \equiv |X_G| \pmod{p}$ .*

**Demostración** Usando la notación de la ecuación [18.2], sabemos, por el teorema 16.3, que  $|x_i G| = (G : G_{x_i})$ . Pero  $(G : G_{x_i})$  divide a  $|G|$  y por tanto,  $p$  divide a  $(G : G_{x_i})$  y así, divide a  $|x_i G|$  para  $s+1 \leq i \leq r$ . La ecuación [18.2] muestra, entonces, que  $|X| - |X_G|$  es divisible entre  $p$ , de modo que  $|X| \equiv |X_G| \pmod{p}$ . ■

**Definición** Un grupo  $G$  es un  $p$ -grupo si todo elemento en  $G$  tiene orden alguna potencia del primo  $p$ . Un subgrupo de un grupo  $G$  es un  $p$ -subgrupo de  $G$ , si el subgrupo es, él mismo, un  $p$ -grupo.

El objetivo de este capítulo es mostrar que un grupo finito  $G$  tiene un subgrupo de todo orden la potencia de un primo, que divide a  $|G|$ . Como primer paso, probamos el teorema de Cauchy, en el cual se afirma que si  $p$  divide a  $|G|$ , entonces  $G$  tiene un subgrupo de orden  $p$ .

**Teorema 18.2 (Cauchy)** *Sea  $G$  un grupo finito y  $p$  divide a  $|G|$ . Entonces  $G$  tiene algún elemento de orden  $p$  y, por tanto, un subgrupo de orden  $p$ .*

*Demostración* Formemos el conjunto  $X$  de todas las  $p$ -adas  $(g_1, g_2, \dots, g_p)$  de elementos de  $G$  que tienen la propiedad de que el producto de las coordenadas en  $G$  es  $e$ . Esto es,

$$X = \{(g_1, g_2, \dots, g_p) \mid g_i \in G \text{ y } g_1g_2 \cdots g_p = e\}.$$

Afirmamos que  $p$  divide a  $|X|$ . Al formar una  $p$ -ada en  $X$ , podemos tomar  $g_1, g_2, \dots, g_{p-1}$  como cualesquiera elementos de  $G$  y entonces  $g_p$  queda determinado de manera única como  $(g_1g_2 \cdots g_{p-1})^{-1}$ . Así,  $|X| = |G|^{p-1}$  y como  $p$  divide a  $|G|$  vemos que  $p$  divide a  $|X|$ .

Sea  $\sigma$  el ciclo  $(1, 2, 3, \dots, p)$  en  $S_p$ . Dejemos que  $\sigma$  actúe en  $X$  mediante

$$(g_1, g_2, \dots, g_p)\sigma = (g_{1\sigma}, g_{2\sigma}, \dots, g_{p\sigma}) = (g_2, g_3, \dots, g_p, g_1).$$

Nótese que  $(g_2, g_3, \dots, g_p, g_1) \in X$ , pues  $g_1(g_2g_3 \cdots g_p) = e$  implica que  $g_1 = (g_2g_3 \cdots g_p)^{-1}$  de modo que, también  $(g_2g_3 \cdots g_p)g_1 = e$ . Así,  $\sigma$  actúa en  $X$ ; consideremos el subgrupo  $\langle\sigma\rangle$  de  $S_p$  actuando en  $X$  por iteración, de la manera obvia.

Ahora bien,  $|\langle\sigma\rangle| = p$ , aplicamos el teorema 18.1 y sabemos que  $|X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$ . Como  $p$  divide a  $|X|$ , debemos tener que  $p$  también divide a  $|X_{\langle\sigma\rangle}|$ . Examinemos  $X_{\langle\sigma\rangle}$ . Ahora bien, el ciclo  $\sigma$  y, por tanto,  $\langle\sigma\rangle$ , dejan fija a  $(g_1, g_2, \dots, g_p)$  si y sólo si  $g_1 = g_2 = \cdots = g_p$ . Conocemos al menos un elemento en  $X_{\langle\sigma\rangle}$ , a saber,  $(e, e, \dots, e)$ . Como  $p$  divide a  $|X_{\langle\sigma\rangle}|$  debe haber al menos  $p$  elementos en  $X_{\langle\sigma\rangle}$ . Entonces, existe algún elemento  $a \in G$ ,  $a \neq e$ , tal que  $(a, a, \dots, a) \in X_{\langle\sigma\rangle}$  y  $a^p = e$ , de modo que  $a$  tiene orden  $p$ . Es claro que  $\langle a \rangle$  es un subgrupo de  $G$  de orden  $p$ . ■

*Corolario* Sea  $G$  un grupo finito. Entonces,  $G$  es un  $p$ -grupo si y sólo si  $|G|$  es una potencia de  $p$ .

*Demostración* Dejamos la demostración de este corolario para el ejercicio 18.5. ■

## \*18.2 LOS TEOREMAS DE SYLOW

Sea  $G$  un grupo y sea  $\mathcal{S}$  la colección de todos los subgrupos de  $G$ . Convertimos  $\mathcal{S}$  en un  $G$ -conjunto, haciendo que  $G$  actúe en  $\mathcal{S}$  por conjugación. Esto es, si  $H \in \mathcal{S}$  de modo que  $H \leq G$ , y  $g \in G$ , entonces la acción de  $g$  en  $H$  produce el subgrupo conjugado  $g^{-1}Hg$ . (Para evitar confusión nunca escribiremos esta acción como  $Hg$ .) Ahora bien, por el teorema 16.1,  $H_G = \{g \in G \mid g^{-1}Hg = H\}$  es un subgrupo de  $G$ . Resulta obvio que  $H$  es un subgrupo normal de  $H_G$ . Como  $H_G$  consta de todos los elementos de  $G$  que dejan invariante a  $H$  bajo la conjugación,  $H_G$  es el mayor subgrupo de  $G$  que tiene a  $H$  como subgrupo normal.

**Definición** El subgrupo  $H_G$ , recién analizado, es el *normalizador de  $H$  en  $G$*  y se denotará desde ahora por  $N[H]$ .

**Lema 18.1** Sea  $H$  un  $p$ -subgrupo del grupo finito  $G$ . Entonces,

$$(N[H]:H) \equiv (G:H) \pmod{p}.$$

**Demostración** Sea  $\mathcal{R}$  el conjunto de clases laterales derechas de  $H$  en  $G$  y sea la acción de  $H$  en  $\mathcal{R}$ , la traslación derecha, de modo que  $(Hx)h = H(xh)$ . Entonces,  $\mathcal{R}$  se convierte en un  $H$ -conjunto. Nótese que  $|\mathcal{R}| = (G:H)$ .

Determinemos  $\mathcal{R}_H$ , esto es, aquellas clases laterales derechas que quedan fijas bajo todos los elementos de  $H$ . Veamos,  $Hx = (Hx)h$  si y sólo si  $H = Hxhx^{-1}$ , o si y sólo si  $xhx^{-1} \in H$ . Así,  $Hx = (Hx)h$  para todas las  $h \in H$  si y sólo si  $xhx^{-1} = (x^{-1})^{-1}hx^{-1} \in H$  para todas las  $h \in H$ , o si y sólo si  $x^{-1} \in N[H]$ , o si y sólo si  $x \in N[H]$ . Así, las clases laterales derechas en  $\mathcal{R}_H$  son aquellas contenidas en  $N[H]$ . El número de dichas clases laterales es  $(N[H]:H)$ , de modo que  $|\mathcal{R}_H| = (N[H]:H)$ .

**Corolario** Sea  $H$  un  $p$ -subgrupo de un grupo finito  $G$ . Si  $p$  divide a  $(G:H)$  entonces  $N[H] \neq H$ .

**Demostración** Se sigue del lema 18.1, que  $p$  divide a  $(N[H]:H)$ , el cual debe ser diferente de 1. Así,  $H \neq N[H]$ . ■

Ahora estamos preparados para el primero de los teoremas de Sylow, que asegura la existencia de subgrupos de  $G$  de orden la potencia de un primo, para cualquier potencia de primo que divida a  $|G|$ .

**Teorema 18.3 (Primer teorema de Sylow)** Sea  $G$  un grupo finito y sea  $|G| = p^n m$  donde  $n \geq 1$ , y donde  $p$  no divide a  $m$ . Entonces,

- 1  $G$  contiene un subgrupo de orden  $p^i$  para cada  $i$  donde  $1 \leq i \leq n$ ,
- 2 todo subgrupo  $H$  de  $G$ , de orden  $p^i$  es un subgrupo normal de algún subgrupo de orden  $p^{i+1}$  para  $1 \leq i < n$ .

**Demostración** 1. Por el teorema de Cauchy (teorema 18.2), sabemos que  $G$  contiene un subgrupo de orden  $p$ . Usemos un argumento de inducción y mostremos que la existencia de un subgrupo de orden  $p^i$  para  $i < n$  implica la existencia de un subgrupo de orden  $p^{i+1}$ . Sea  $H$  un subgrupo de orden  $p^i$ . Como  $i < n$ , vemos que  $p$  divide a  $(G:H)$ . Por el lema 18.1, sabemos, entonces, que  $p$  divide a  $(N[H]:H)$ . Como  $H$  es un subgrupo normal de  $N[H]$ , podemos formar  $N[H]/H$  y vemos que  $p$  divide a  $|N[H]/H|$ . Por el teorema de Cauchy, el grupo factor  $N[H]/H$  tiene un subgrupo  $K$  de orden  $p$ . Si  $\gamma: N[H] \rightarrow N[H]/H$  es el homomorfismo canónico, entonces  $K\gamma^{-1} = \{x \in N[H] \mid xy \in K\}$  es un subgrupo de  $N[H]$  y, por tanto, de  $G$ . Este subgrupo contiene a  $H$  y es de orden  $p^{i+1}$ .

2. Repetimos la construcción de la parte 1 y notamos que  $H < K\gamma^{-1} \leq N[H]$  donde  $|K\gamma^{-1}| = p^{i+1}$ . Como  $H$  es normal en  $N[H]$ , es claro que es normal, en el grupo  $K\gamma^{-1}$  que es posiblemente menor. ■

**Definición** Un *p-subgrupo de Sylow*  $P$  de un grupo  $G$  es un  $p$ -subgrupo maximal de  $G$ , esto es, un  $p$ -subgrupo que no está contenido en un  $p$ -subgrupo mayor.

Sea  $G$  un grupo finito, donde  $|G| = p^n m$ , como en el teorema 18.3. El teorema muestra que los  $p$ -subgrupos de Sylow de  $G$  son precisamente aquellos subgrupos de orden  $p^n$ . Si  $P$  es un  $p$ -subgrupo de Sylow, todo conjugado  $g^{-1}Pg$  de  $P$  también es un  $p$ -subgrupo de Sylow. El segundo teorema de Sylow afirma que todo  $p$ -subgrupo de Sylow se puede obtener a partir de  $P$  en esta forma, esto es, que cualesquiera dos  $p$ -subgrupos de Sylow son conjugados.

**Teorema 18.4 (Segundo teorema de Sylow)** Sean  $P_1$  y  $P_2$   $p$ -subgrupos de Sylow de un grupo finito  $G$ . Entonces,  $P_1$  y  $P_2$  son subgrupos conjugados de  $G$ .

**Demostración** Aquí, la gracia es hacer que uno de los subgrupos actúe en las clases laterales derechas del otro y usar el teorema 18.1. Sea  $\mathcal{R}$  la colección de clases laterales derechas de  $P_1$  y  $P_2$  actúe sobre  $\mathcal{R}$  mediante  $(P_1x)y = P_1(xy)$  para  $y \in P_2$ . Entonces,  $\mathcal{R}$  es un  $P_2$ -conjunto. Por el teorema 18.1,  $|\mathcal{R}_{P_2}| \equiv |\mathcal{R}| \pmod{p}$  y  $|\mathcal{R}| = (G:P_1)$  no es divisible entre  $p$ , de modo que  $|\mathcal{R}_{P_2}| \neq 0$ . Sea  $P_1x \in \mathcal{R}_{P_2}$ . Entonces,  $P_1xy = P_1x$  para todas las  $y \in P_2$ , de modo que  $P_1xyx^{-1} = P_1$  para todas las  $y \in P_2$ . Así,  $xyx^{-1} \in P_1$  para todas las  $y \in P_2$  de modo que  $xP_2x^{-1} \leq P_1$ . Como  $|P_1| = |P_2|$  debemos tener  $P_1 = x^{-1}P_2x$ , de modo que  $P_1$  y  $P_2$  son, en efecto, subgrupos conjugados. ■

El último teorema de Sylow posee información acerca del número de los  $p$ -subgrupos de Sylow. Se dan algunos ejemplos después del teorema y muchos más en el capítulo siguiente.

**Teorema 18.5 (Tercer teorema de Sylow)** Si  $G$  es un grupo finito y  $p$  divide a  $|G|$ , entonces el número de  $p$ -subgrupos de Sylow es congruente con 1 módulo  $p$  y divide a  $|G|$ .

**Demostración** Sea  $P$  un  $p$ -subgrupo de Sylow de  $G$ . Sea  $\mathcal{S}$  el conjunto de todos los  $p$ -subgrupos de Sylow y sea la acción de  $P$  en  $\mathcal{S}$  mediante la conjugación, de manera que  $x \in P$  lleva a  $T \in \mathcal{S}$  en  $x^{-1}Tx$ . Por el teorema 18.1,  $|\mathcal{S}| \equiv |\mathcal{S}_P| \pmod{p}$ . Hallemos  $\mathcal{S}_P$ . Si  $T \in \mathcal{S}_P$ , entonces  $x^{-1}Tx = T$  para todas las  $x \in P$ . Así,  $P \leq N[T]$ . Claro que, además,  $T \leq N[T]$ . Como  $P$  y  $T$  son  $p$ -subgrupos de Sylow de  $G$ , también son  $p$ -subgrupos de Sylow de  $N[T]$ . Pero entonces, por el teorema 18.4, son conjugados en  $N[T]$ . Como  $T$  es un subgrupo normal de  $N[T]$ , es su único conjugado en  $N[T]$ . Así,  $T = P$ . Entonces,  $\mathcal{S}_P = \{P\}$ . Como  $|\mathcal{S}| \equiv |\mathcal{S}_P| = 1 \pmod{p}$ , vemos que el número de  $p$ -subgrupos de Sylow es congruente con 1 módulo  $p$ .

Ahora bien, sea  $G$  actuando en  $\mathcal{S}$  por conjugación. Como todos los  $p$ -subgrupos de Sylow son conjugados, entonces hay sólo una órbita en  $\mathcal{S}$  bajo  $G$ . Si  $P \in \mathcal{S}$ , entonces  $G_P = N[P]$ . Entonces, por el teorema 16.3  $|\mathcal{S}| = |\text{órbita de } P| = (G : G_P)$ . Pero  $(G : G_P)$  es un divisor de  $|G|$ , de modo que el número de  $p$ -subgrupos de Sylow divide a  $|G|$ . ■

**Ejemplo 18.1** Los 2-subgrupos de Sylow de  $S_3$  tienen orden 2. Los subgrupos de orden 2 de  $S_3$  del ejemplo 4.1 son

$$\{\rho_0 \mu_1\}, \quad \{\rho_0 \mu_2\}, \quad \{\rho_0 \mu_3\}.$$

Nótese que hay tres subgrupos y que  $3 \equiv 1 \pmod{2}$ . Además, 3 divide al 6, que es el orden de  $S_3$ . Puede verse fácilmente que

$$\{\rho_0, \mu_1\}i_{\rho_1} = \{\rho_0, \mu_2\} \quad \text{y} \quad \{\rho_0, \mu_1\}i_{\rho_2} = \{\rho_0, \mu_3\}$$

donde  $xi_{\rho_j} = (\rho_j)^{-1}x\rho_j$ , lo cual ilustra que todos ellos son conjugados. ■

**Ejemplo 18.2** Usemos los teoremas de Sylow para mostrar que ningún grupo de orden 15 es simple. Sea  $G$  de orden 15. Aseguramos que  $G$  tiene un subgrupo normal de orden 5. Por el teorema 18.3,  $G$  tiene al menos un subgrupo de orden 5 y por el teorema 18.5, el número de dichos subgrupos es congruente con 1 módulo 5 y divide a 15. Como 1, 6 y 11 son los únicos números positivos menores que 15 que son congruentes con 1 módulo 5 y como entre ellos sólo el número 1 divide al 15, vemos que  $G$  tiene exactamente un subgrupo  $P$  de orden 5. Pero para cada  $g \in G$  el automorfismo interno  $i_g$  de  $G$  con  $xi_g = g^{-1}xg$  transforma a  $P$  sobre un subgrupo  $g^{-1}Pg$ , de nuevo, de orden 5. De aquí que por fuerza  $g^{-1}Pg = P$  para todas las  $g \in G$  de manera que  $P$  es un subgrupo normal de  $G$ . Por tanto,  $G$  no es simple. ■

Confiamos en que el ejemplo 18.2 dé alguna idea del poder del teorema 18.5. Nunca hay que subestimar un teorema que cuente algo, aunque sea módulo  $p$ .

## Ejercicios

---

\*18.1 Completense los enunciados.

- a) Un 3-subgrupo de Sylow de un grupo de orden 12 tiene orden \_\_\_\_.
- b) Un 3-subgrupo de Sylow de un grupo de orden 54 tiene orden \_\_\_\_.
- c) Un grupo de orden 24 debe tener \_\_\_\_ o \_\_\_\_ 2-subgrupos de Sylow. (Usese sólo la información dada en el teorema 18.5.)
- d) Un grupo de orden  $255 = (3)(5)(17)$  debe tener \_\_\_\_ o \_\_\_\_ 3-subgrupos de Sylow y \_\_\_\_ o \_\_\_\_ 5-subgrupos de Sylow. (Usese sólo la información dada en el teorema 18.5.)

\*18.2 Encuéntrense los 3-subgrupos de Sylow de  $S_4$  y demuéstrese que todos ellos son conjugados.

\*18.3 Sea  $G$  un grupo finito y  $p$  que divide a  $|G|$ . Pruébese que si  $G$  tiene un solo  $p$ -subgrupo de Sylow, éste es un subgrupo normal, de modo que  $G$  no es simple.

\*18.4 Muéstrese que todo grupo de orden 45 tiene un subgrupo normal de orden 9.

\*18.5 Pruébese el corolario del teorema 18.2.

\*18.6 Sea  $G$  un grupo finito y  $p$  que divide a  $|G|$ . Sea  $P$  un  $p$ -subgrupo de Sylow de  $G$ . Muéstrese que  $N[N[P]] = N[P]$ . [Sugerencia: pruébese que  $P$  es el único  $p$ -subgrupo de Sylow de  $N[N[P]]$  y úsese el teorema 18.4.]

\*18.7 ¿Falso o verdadero?

- a) Cualesquiera dos  $p$ -subgrupos de Sylow de un grupo finito son conjugados.
- b) El teorema 18.5 muestra que un grupo de orden 15 tiene un solo 5-subgrupo de Sylow.
- c) Todo  $p$ -subgrupo de Sylow de un grupo finito tiene como orden una potencia de  $p$ .
- d) Todo  $p$ -subgrupo de todo grupo finito es un  $p$ -subgrupo de Sylow.
- e) Todo grupo abeliano finito tiene exactamente un  $p$ -subgrupo de Sylow para cada primo  $p$  que divide al orden de  $G$ .
- f) El normalizador en  $G$  de un subgrupo  $H$  de  $G$  es siempre un subgrupo normal de  $G$ .
- g) Si  $H$  es un subgrupo de  $G$ , entonces  $H$  es siempre un subgrupo normal de  $N[H]$ .
- h) Un  $p$ -subgrupo de Sylow de un grupo finito  $G$  es normal en  $G$  si y sólo si es el único  $p$ -subgrupo de Sylow de  $G$ .
- i) Si  $G$  es un grupo abeliano y  $H$  es un subgrupo de  $G$ , entonces  $N[H] = H$ .
- j) Un grupo de orden  $P^n$ , la potencia de un primo, no tiene  $p$ -subgrupos de Sylow.

\*18.8 Sea  $G$  un grupo finito y que  $p$  divide a  $|G|$ . Sea  $P$  un  $p$ -subgrupo de Sylow de  $G$  y sea  $H$  cualquier  $p$ -subgrupo de  $G$ . Muéstrese que existe  $g \in G$  tal que  $g^{-1}Hg \leq P$ .

\*18.9 Encuéntrense dos 2-subgrupos de Sylow de  $S_4$  y muéstrese que son conjugados.

\*18.10 Muéstrese que todo grupo de orden  $(35)^3$  tiene un subgrupo normal de orden 125.

\*18.11 Muéstrese que no hay grupos simples de orden  $255 = (3)(5)(17)$ .

\*18.12 Muéstrese que no hay grupos simples de orden  $p^m m$  donde  $p$  es primo y  $m < p$ .

\*18.13 Sea  $G$  un grupo finito. Considérese  $G$  como un  $G$ -conjunto donde  $G$  actúa sobre sí mismo por conjugación.

- Muéstrese que  $G_G$  es el centro  $Z(G)$  de  $G$ . (Véase la sección 14.3.)
- Usese el teorema 18.1 para mostrar que el centro de un  $p$ -grupo finito no trivial es no trivial.

\*18.14 Muéstrese que un grupo finito de orden  $p^n$  contiene subgrupos *normales*  $H_i$  para  $0 \leq i \leq n$ , tales que  $|H_i| = p^i$  y  $H_i < H_{i+1}$  para  $0 \leq i < n$ . [Sugerencia: véase el ejercicio 18.13 y tómese en cuenta la sección 14.3.]

\*18.15 Muéstrese que un  $p$ -subgrupo normal de un grupo finito está contenido en todo  $p$ -subgrupo de Sylow.

## Aplicaciones de la teoría de Sylow

En este capítulo daremos varias aplicaciones de los teoremas de Sylow. Seguramente les parecerá sorprendente la facilidad con que se pueden deducir ciertos hechos acerca de grupos de orden particular. Hay que comprender, sin embargo, que trabajamos sólo con grupos de orden finito y que, en realidad, apenas empezamos con el problema general de determinar la estructura de todos los grupos finitos. Si el orden de un grupo tiene sólo unos cuantos factores, entonces las técnicas ilustradas en este capítulo pueden ser útiles para determinar la estructura del grupo. Esto se demostrará más adelante, en el capítulo 22, donde veremos cómo, en ocasiones, es posible determinar todos los grupos (salvo isomorfismo) de ciertos órdenes, aun cuando algunos de ellos no sean abelianos. No obstante, si el orden de un grupo finito es altamente compuesto, esto es, si tiene un número grande de factores, en general el problema es más difícil.

### \*19.1 APPLICACIONES A $p$ -GRUPOS Y LA ECUACIÓN DE CLASE

**Teorema 19.1** *Todo grupo cuyo orden es la potencia de un primo (esto es, todo  $p$ -grupo finito) es soluble.*

**Demostración** Si  $G$  tiene orden  $p^r$ , se deduce de inmediato, por el teorema 18.3, que  $G$  tiene subgrupos  $H_i$  de orden  $p^i$ , cada uno normal en un subgrupo de orden  $p^{i+1}$  para  $1 \leq i < r$ . Entonces,

$$\{e\} = H_0 < H_1 < H_2 < \cdots < H_r = G$$

es una serie de composición donde los grupos factores son de orden  $p$  y, por tanto, abelianos y en realidad, cílicos. Así,  $G$  es soluble. ■

Las antiguas demostraciones de los teoremas de Sylow usaban la *ecuación de clase*. Siguiendo el hilo de la demostración, en el capítulo 18 se evitó explícitamente mencionar la ecuación de clase, aunque la ecuación [18.2] es una forma general de ella. Desarrollemos ahora la clásica ecuación de clase para que se conozca.

Sea  $X$  un  $G$ -conjunto finito donde  $G$  es un grupo finito. Entonces, la ecuación [18.2] dice que

$$|X| = |X_G| + \sum_{i=s+1}^r |x_iG| \quad [19.1]$$

donde  $x_i$  es un elemento en la  $i$ -ésima órbita en  $X$ . Considérese ahora un caso particular de la ecuación [19.1], donde  $X = G$  y la acción de  $G$  sobre  $G$  es por conjugación, de modo que  $g \in G$  lleva a  $x \in X = G$  en  $g^{-1}xg$ . Entonces,

$$\begin{aligned} X_G &= \{x \in G \mid g^{-1}xg = x \text{ para todas las } g \in G\} \\ &= \{x \in G \mid xg = gx \text{ para todas las } g \in G\} = Z(G), \end{aligned}$$

el centro de  $G$ . Si hacemos  $c = |Z(G)|$  y  $n_i = |x_iG|$  en la ecuación [19.1], obtenemos

$$|G| = c + n_{c+1} + \cdots + n_r \quad [19.2]$$

donde  $n_i$  es el número de elementos en la  $i$ -ésima órbita de  $G$  bajo la conjugación por sí mismo. Nótese que  $n_i$  divide  $|G|$  para  $c+1 \leq i \leq r$  pues, por la ecuación [19.1], sabemos que  $|x_iG| = (G : G_{x_i})$ , que es un divisor de  $|G|$ .

**Definición** La ecuación [19.2] es la *ecuación de clase de  $G$* . Cada órbita en  $G$  bajo conjugación por  $G$  es una *clase conjugada* en  $G$ .

**Ejemplo 19.1** Es fácil comprobar que para  $S_3$  del ejemplo 4.1, las clases conjugadas son

$$\{\rho_0\}, \quad \{\rho_1, \rho_2\}, \quad \{\mu_1, \mu_2, \mu_3\}.$$

La ecuación de clase de  $S_3$  es

$$6 = 1 + 2 + 3. \blacksquare$$

Para ilustrar el uso de la ecuación de clase, probemos un teorema; el mismo que se probó en el ejercicio 18.13(b).

**Teorema 19.2** El centro de un  $p$ -grupo no trivial  $G$  es no trivial.

**Demostración** En la ecuación [19.2] para  $G$ , cada  $n_i$  divide  $|G|$  para  $c+1 \leq i \leq r$ , así que  $p$  divide cada  $n_i$  y, claramente,  $p$  divide  $|G|$ . Por tanto,  $p$  divide  $c$ . Ahora,  $e \in Z(G)$ , de modo que  $c \geq 1$ . Así,  $c \geq p$  y existe alguna  $a \in Z(G)$  donde  $a \neq e$ . ■

Pasemos ahora a un lema sobre productos directos, que usaremos en algunos de los teoremas posteriores.

**Lema 19.1** *Sea  $G$  un grupo que contiene a los subgrupos normales  $H$  y  $K$  tales que  $H \cap K = \{e\}$  y  $H \vee K = G$ . Entonces,  $G$  es isomorfo a  $H \times K$ .*

**Demostración** Mostremos que se satisfacen las tres condiciones del teorema 8.6. Como  $H \cap K = \{e\}$  y  $H \vee K = G$ , basta mostrar que  $hk = kh$  para  $h \in H$  y  $k \in K$ . Considérese el conmutador  $hkh^{-1}k^{-1}$ . El agrupamiento  $(hkh^{-1})k^{-1}$  muestra que el conmutador está en  $K$ , pues  $K$  es normal y  $hkh^{-1} \in K$ . De manera análoga, el agrupamiento  $h(kh^{-1}k^{-1})$  muestra que el conmutador está en  $H$ . De aquí,  $hkh^{-1}k^{-1} \in (H \cap K)$ , de modo que  $hkh^{-1}k^{-1} = e$ , o  $hk = kh$ . El lema está probado. ■

**Teorema 19.3** *Para un número primo  $p$ , todo grupo  $G$  de orden  $p^2$  es abeliano.*

**Demostración** Si  $G$  no es cíclico, entonces todo elemento, excepto  $e$ , debe ser de orden  $p$ . Sea  $a$  uno de dichos elementos. Entonces, el subgrupo cíclico  $\langle a \rangle$  de orden  $p$  no es todo  $G$ . Sea además  $b \in G$  con  $b \notin \langle a \rangle$ . Entonces,  $\langle a \rangle \cap \langle b \rangle = \{e\}$  pues un elemento  $c$  en  $\langle a \rangle \cap \langle b \rangle$ , con  $c \neq e$  generaría tanto  $\langle a \rangle$  como  $\langle b \rangle$ , resultando  $\langle a \rangle = \langle b \rangle$ , lo cual es contrario a la construcción. Del teorema 18.3,  $\langle a \rangle$  es normal en algún subgrupo de orden  $p^2$  de  $G$ , esto es, normal en todo  $G$ . Así mismo,  $\langle b \rangle$  es normal en  $G$ . Ahora,  $\langle a \rangle \vee \langle b \rangle$  es un subgrupo de  $G$  que contiene propiamente  $\langle a \rangle$  y de orden que divide  $p^2$ . De aquí,  $\langle a \rangle \vee \langle b \rangle$  debe ser todo  $G$ . Así, se satisface la hipótesis del lema 19.1 y  $G$  es isomorfo a  $\langle a \rangle \times \langle b \rangle$  y, por tanto, es abeliano. ■

## \*19.2 APLICACIONES ULTERIORES

Analicemos ahora la existencia de grupos simples de ciertos órdenes. Hemos visto que todo grupo de orden primo es simple. También afirmamos que  $A_n$  es simple para  $n \geq 5$  y que  $A_5$  es el menor grupo simple cuyo orden no es primo. Una famosa conjetura de Burnside afirma que todo grupo simple finito de orden no primo debe ser de orden par. Fue un triunfo cuando lo demostraron, recientemente, Thompson y Feit [21].

**Teorema 19.4** *Si  $p$  y  $q$  son primos distintos con  $p < q$ , entonces, todo grupo  $G$  de orden  $pq$  tiene un solo subgrupo de orden  $q$  y este subgrupo es normal en  $G$ . De aquí,  $G$  no es simple. Si  $q$  no es congruente con 1, módulo  $p$ , entonces  $G$  es abeliano y cíclico.*

*Demostración* Los teoremas 18.3 y 18.5 señalan que  $G$  tiene un  $q$ -subgrupo de Sylow y que el número de dichos subgrupos es congruente con 1 módulo  $q$  y divide a  $pq$  y, por tanto, debe dividir a  $p$ . Como  $p < q$ , la única posibilidad es el número 1. Así, hay sólo un  $q$ -subgrupo de Sylow  $Q$  de  $G$ . Este grupo  $Q$  debe ser normal en  $G$ , pues bajo un automorfismo interno, va a dar a un grupo del mismo orden, es decir, a si mismo. Entonces,  $G$  no es simple.

Así mismo, existe un  $p$ -subgrupo de Sylow  $P$  de  $G$ , y el número de estos divide a  $q$  y es congruente con 1 módulo  $p$ . Este número debe ser 1 o  $q$ . Si  $q$  no es congruente con 1 módulo  $p$ , entonces el número debe ser 1 y  $P$  es normal en  $G$ . Supongamos que  $q \not\equiv 1 \pmod{p}$ . Como todo elemento de  $Q$ , distinto de  $e$ , es de orden  $q$  y todo elemento de  $P$ , distinto de  $e$ , es de orden  $p$ , tenemos  $Q \cap P = \{e\}$ . Además,  $Q \vee P$  debe ser un subgrupo de  $G$  que contiene propiamente  $Q$  y de orden que divide  $pq$ . De aquí,  $Q \vee P = G$  y, por el lema 19.1,  $G$  es isomorfo a  $Q \times P$  o  $\mathbb{Z}_q \times \mathbb{Z}_p$ . Así,  $G$  es abeliano y cíclico. ■

Necesitamos otro lema para disponer de los siguientes argumentos de conteo.

**Lema 19.2** *Si  $H$  y  $K$  son subgrupos finitos de un grupo  $G$ , entonces*

$$|HK| = \frac{(|H|)(|K|)}{|H \cap K|}.$$

*Demostración* Recuérdese que  $HK = \{hk \mid h \in H, k \in K\}$ . Sea  $|H| = r$ ,  $|K| = s$  y  $|H \cap K| = t$ . Es claro que  $HK$  tiene a lo más  $rs$  elementos. Sin embargo, es posible que  $h_1k_1$  sea igual a  $h_2k_2$  para  $h_1, h_2 \in H$  y  $k_1, k_2 \in K$ , esto es, puede haber colapsos. Si  $h_1k_1 = h_2k_2$ , entonces, sea

$$x = (h_2)^{-1}h_1 = k_2(k_1)^{-1}.$$

Ahora,  $x = (h_2)^{-1}h_1$  muestra que  $x \in H$ , y  $x = k_2(k_1)^{-1}$  muestra que  $x \in K$ . De aquí,  $x \in (H \cap K)$  y

$$h_2 = h_1x^{-1} \quad y \quad k_2 = xk_1.$$

Por otro lado, si para  $y \in (H \cap K)$  hacemos  $h_3 = h_1y^{-1}$  y  $k_3 = yk_1$ , entonces, claramente,  $h_3k_3 = h_1k_1$ , con  $h_3 \in H$  y  $k_3 \in K$ . Así, cada elemento  $hk \in HK$  puede representarse en la forma  $h_ik_i$  para  $h_i \in H$  y  $k_i \in K$  tantas veces como elementos haya en  $H \cap K$ , esto es,  $t$  veces. Por tanto, el número de elementos en  $HK$  es  $rs/t$ . ■

El lema anterior es otro resultado que cuenta algo, luego no hay que subestimarlo. Se usará el lema de la siguiente manera: un grupo finito no puede tener subgrupos  $H$  y  $K$  demasiado grandes con intersecciones muy pequeñas, de ser así, el orden de  $HK$  excedería el orden de  $G$ , lo cual es imposible. Por ejemplo, un grupo de orden 24 no puede tener dos subgrupos de orden 12 y 8 con intersección de orden 2.

El resto de este capítulo consta de varios ejemplos que ilustran las técnicas para probar que todos los grupos de ciertos órdenes son abelianos o tienen subgrupos normales propios no triviales, es decir, que no son simples. Se usará un hecho que hemos mencionado sólo en los ejercicios. *Un subgrupo  $H$  de índice 2 en un grupo finito  $G$  siempre es normal* pues, contando, vemos que las clases laterales izquierdas son sólo  $H$  mismo y la clase lateral formada por todos los elementos de  $G$  que no están en  $H$ . Las clases laterales derechas son las mismas. Así, toda clase lateral derecha es una clase lateral izquierda y, por el teorema 12.1 y el análisis que le sigue,  $H$  es normal en  $G$ .

**Ejemplo 19.2** Ningún grupo de orden  $p^r$  para  $r > 1$  es simple, donde  $p$  es primo. Por el teorema 18.3, dicho grupo  $G$  contiene un subgrupo de orden  $p^{r-1}$  normal en un subgrupo de orden  $p^r$ , el cual debe ser todo  $G$ . Así, un grupo de orden 16 no es simple; tiene un subgrupo normal de orden 8. ■

**Ejemplo 19.3** Todo grupo de orden 15 es cíclico (y de aquí, abeliano y no simple, pues 15 no es primo). Esto sucede porque  $15 = (5)(3)$  y 5 no es congruente con 1 módulo 3. Se aplica el teorema 19.4, y hemos terminado. ■

**Ejemplo 19.4** Ningún grupo de orden 20 es simple, pues si  $G$  es uno de dichos grupos,  $G$  contiene un número de 5-subgrupos de Sylow congruente con 1 módulo 5 y divisor de 20, por tanto, sólo 1. Este 5-subgrupo de Sylow es, entonces, normal, pues todos sus conjugados deben ser él mismo. ■

**Ejemplo 19.5** Ningún grupo de orden 30 es simple. Hemos visto que basta demostrar que hay un solo  $p$ -subgrupo de Sylow para algún primo  $p$  que divide 30. Por el teorema 18.5, las posibilidades para el número de 5-subgrupos de Sylow son 1 ó 6, y para 3-subgrupos de Sylow son 1 ó 10. Pero si  $G$  tiene seis 5-subgrupos de Sylow, entonces la intersección de cualquier par de ellos es un subgrupo de cada uno de ellos de orden que divide 5, por tanto, es  $\{e\}$ . Así, cada uno contiene cuatro elementos de orden 5 que no está en ninguno de los otros. De aquí,  $G$  debe contener 24 elementos de orden 5. De manera análoga, si  $G$  tiene diez 3-subgrupos de Sylow, tendrá al menos 20 elementos de orden 3. Los dos tipos de subgrupos de Sylow juntos requerirían un total de al menos 44 elementos de  $G$ . Así, existe algún subgrupo normal, ya sea de orden 5 o de orden 3. ■

**Ejemplo 19.6** Ningún grupo de orden 48 es simple. En efecto, mostraremos que un grupo  $G$  de orden 48 tiene un subgrupo normal de orden 16 o de orden 8. Por el teorema 18.5,  $G$  tiene uno o tres 2-subgrupos de Sylow de orden 16. Si hay un solo subgrupo de orden 16, por el argumento ya conocido, es normal en  $G$ .

Supóngase que hay tres subgrupos de orden 16 y sean  $H$  y  $K$  dos de ellos. Entonces,  $H \cap K$  debe ser de orden 8, pues si  $H \cap K$  fuera de orden  $\leq 4$  entonces, por el lema 19.2,  $HK$  tendría al menos  $(16)(16)/4 = 64$  elementos, contradiciendo el hecho de que  $G$  tiene sólo cuarenta y ocho elementos. Por tanto,  $H \cap K$  es normal tanto en  $H$  como en  $K$  (por ser de índice 2, o por el teorema 18.3). De aquí, el normalizador de  $H \cap K$  contiene  $H$  y  $K$  y debe tener orden un múltiplo  $> 1$  de 16 y divisor de 48, por tanto, 48. Así,  $H \cap K$  debe ser normal en  $G$ . ■

**Ejemplo 19.7** Ningún grupo de orden 36 es simple. Dicho grupo  $G$  tiene uno o cuatro subgrupos de orden 9. Si hay uno solo de dichos subgrupos, es normal en  $G$ . Si hay cuatro de dichos subgrupos, sean  $H$  y  $K$  dos de ellos. Comó en el ejemplo 19.6,  $H \cap K$  debe tener al menos tres elementos, si no,  $HK$  tendría ochenta y un elementos, lo cual es imposible. Así, el normalizador de  $H \cap K$  tiene orden un múltiplo  $> 1$  de 9 y divisor de 36; de aquí que el orden debe ser 18 ó 36. Si el orden es 18, entonces el normalizador es de índice 2 y, por tanto, es normal en  $G$ . Si el orden es 36, entonces  $H \cap K$  es normal en  $G$ . ■

**Ejemplo 19.8** Todo grupo de orden  $255 = (3)(5)(17)$  es abeliano (y por tanto cíclico, por el teorema 9.3, y no simple, pues 255 no es primo). Por el teorema 18.5, dicho grupo  $G$  tiene sólo un subgrupo  $H$  de orden 17. Entonces,  $G/H$  tiene orden 15 y, por el ejemplo 19.3, es abeliano. Por el teorema 12.6, se sabe que el subgrupo conmutador  $G'$  de  $G$  está contenido en  $H$ . Así, como subgrupo de  $H$ ,  $G'$  tiene orden 1 ó 17. El teorema 18.5 muestra, además, que  $G$  tiene 1 ó 85 subgrupos de orden 3, o bien, 1 ó 51 subgrupos de orden 5. Sin embargo, 85 subgrupos de orden 3 requerirían 170 elementos de orden 3 en  $G$ , y 51 subgrupos de orden 5 requerirían 204 elementos de orden 5 en  $G$ ; juntos requerirían, entonces, 375 elementos en  $G$ , lo cual es imposible. De aquí que hay un subgrupo  $K$  que tiene orden 3 u orden 5 y es normal en  $G$ . Entonces,  $G/K$  tiene orden  $(5)(17)$  u orden  $(3)(17)$ , en ambos casos, el teorema 19.4 muestra que  $G/K$  es abeliano. Así,  $G' \leq K$  y tiene orden 3, 5 ó 1. Como  $G' \leq H$  implicó que  $G'$  tuviera orden 17 ó 1, concluimos que  $G'$  tiene orden 1. De aquí,  $G' = \{e\}$  y  $G/G' \simeq G$  es abeliano. Entonces, el teorema 9.3 muestra que  $G$  es cíclico. ■

## Ejercicios

---

\*19.1 Mediante argumentos análogos a los usados en los ejemplos de esta sección, obsérvese que todo grupo de orden no primo menor que 60 contiene un subgrupo normal propio no trivial y, por tanto, no es simple. No es necesario escribir los detalles. (Los casos más difíciles se analizaron en los ejemplos.)

\*19.2 Pruébese que todo grupo de orden  $(5)(7)(47)$  es abeliano y cíclico.

\*19.3 ¿Falso o verdadero?

- a) Todo grupo de orden 159 es cíclico.
- b) Todo grupo de orden 102 tiene un subgrupo normal propio no trivial.
- c) Todo grupo soluble es de orden la potencia de un primo.
- d) Todo grupo de orden la potencia de un primo es soluble.
- e) Resultaría muy tedioso, usando los métodos ilustrados en el texto, mostrar que ningún grupo de orden no primo entre 60 y 168 es simple.
- f) Ningún grupo de orden 21 es simple.
- g) Todo grupo de 125 elementos tiene al menos 5 elementos que conmutan con todo elemento del grupo.
- h) Todo grupo de orden 42 tiene un subgrupo normal de orden 7.
- i) Todo grupo de orden 42 tiene un subgrupo normal de orden 8.
- j) Los únicos grupos simples son los  $\mathbb{Z}_p$  y  $A_n$ , donde  $p$  es primo y  $n \neq 4$ .

- \*19.4 Pruébese que ningún grupo de orden 96 es simple.
- \*19.5 Pruébese que ningún grupo de orden 160 es simple.
- \*19.6 Sea  $D_4$  el grupo de simetrías del cuadrado en el ejemplo 4.2.
- Encuéntrese la descomposición de  $D_4$  en clases conjugadas.
  - Escribáse la ecuación de clase para  $D_4$ .
- \*19.7 Este ejercicio determina las clases conjugadas de  $S_n$  para todo entero  $n \geq 1$ .
- Muéstrese que si  $\sigma = (a_1, a_2, \dots, a_m)$  es un ciclo en  $S_n$  y  $\tau$  es cualquier elemento de  $S_n$ , entonces  $\tau^{-1}\sigma\tau = (a_1\tau, a_2\tau, \dots, a_m\tau)$ .
  - Dedúzcase de a) que cualesquiera dos ciclos en  $S_n$  de la misma longitud son conjugados.
  - Dedúzcase de a) y b) que el producto de  $s$  ciclos ajenos en  $S_n$  de longitudes  $r_i$  para  $i = 1, 2, \dots, s$ , se conjuga con cualquier otro producto de  $s$  ciclos ajenos de longitudes  $r_i$  en  $S_n$ .
  - Muéstrese que el número de clases conjugadas en  $S_n$  es  $p(n)$  donde  $p(n)$  es el número de maneras, ignorando el orden de los sumando, en que se puede expresar  $n$  como suma de enteros positivos. El número  $p(n)$  es el **número de particiones de  $n$** .
  - Calcúlese  $p(n)$  para  $n = 1, 2, 3, 4, 5, 6, 7$ .
- \*19.8 Encuéntrense las clases conjugadas y la ecuación de clase de  $S_4$ . [Sugerencia: úsese el ejercicio 19.7.]
- \*19.9 Encuéntrense las ecuaciones de clase para  $S_5$  y  $S_6$ . [Sugerencia: úsese el ejercicio 19.7.]
- \*19.10 Muéstrese que el número de clases conjugadas en  $S_n$  es, además, el número de grupos abelianos distintos (salvo isomorfismo) de orden  $p^n$ , donde  $p$  es un número primo. [Sugerencia: úsese el ejercicio 19.7.]
- \*19.11 Muéstrese que si  $n > 2$ , el centro de  $S_n$  es el subgrupo que consta sólo de la permutación identidad. [Sugerencia: úsese el ejercicio 19.7.]

## \*20

## Grupos abelianos libres

En este capítulo presentaremos el concepto de grupo abeliano libre y probaremos algunos resultados al respecto. El capítulo concluye con una demostración del teorema fundamental de los grupos abelianos finitamente generados (teorema 9.3).

### \*20.1 GRUPOS ABELIANOS LIBRES

Debería repasarse el material relacionado con el conjunto generador de un grupo  $G$  y con los grupos finitamente generados, presentado al principio del capítulo 9. En el presente capítulo trataremos exclusivamente con grupos abelianos y usaremos la notación aditiva como sigue:

0 para la identidad, + para la operación

$$\begin{aligned} na &= \underbrace{a + a + \cdots + a}_{n \text{ sumandos}} \\ -na &= \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ sumandos}} \end{aligned} \quad \left. \begin{array}{l} \text{para } n \in \mathbb{Z}^+ \text{ y } a \in G. \end{array} \right.$$

$0a = 0$  donde el primer 0 está en  $\mathbb{Z}$  y el segundo en  $G$ .

Seguiremos usando el símbolo  $\times$  para el producto directo de grupos, en lugar de cambiar a la notación de suma directa.

Es claro que  $\{(1, 0), (0, 1)\}$  es un conjunto generador para el grupo  $\mathbb{Z} \times \mathbb{Z}$  puesto que  $(n, m) = n(1, 0) + m(0, 1)$  para cualquier  $(n, m)$  en  $\mathbb{Z} \times \mathbb{Z}$ . Este conjunto generador tiene la propiedad de que cada elemento de  $\mathbb{Z} \times \mathbb{Z}$  se puede expresar de manera única en la forma  $n(1, 0) + m(0, 1)$ . Esto es, los coeficientes  $n$  y  $m$  en  $\mathbb{Z}$  son únicos.

**Teorema 20.1** Sea  $X$  un subconjunto de un grupo abeliano  $G$  distinto de cero. Las condiciones siguientes acerca de  $X$  son equivalentes.

- 1 Cada elemento distinto de cero en  $G$  se puede expresar de manera única en la forma  $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ , para  $n_i \neq 0$  en  $\mathbf{Z}$  y  $x_i$  distintas en  $X$ .
- 2  $X$  genera  $G$  y  $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$  para  $n_i \in \mathbf{Z}$  y  $x_i \in X$  distintas, si y sólo si  $n_1 = n_2 = \cdots = n_r = 0$ .

**Demostración** Supóngase que la condición 1 es cierta. Como  $G \neq \{0\}$ , tenemos que  $X \neq \{0\}$ . Se sigue de 1, que  $0 \in X$ , pues si  $x_i = 0$  y  $x_j \neq 0$ , entonces  $x_j = x_i + x_j$ , lo cual contradice la unicidad de la expresión para  $x_j$ . De 1 se sigue que  $X$  genera  $G$  y también que  $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$  si  $n_1 = n_2 = \cdots = n_r = 0$ . Supóngase que  $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$  con alguna  $n_i \neq 0$ ; al quitar los términos con coeficiente cero y renombrarlos, es posible suponer que todas las  $n_i \neq 0$ . Entonces,

$$\begin{aligned} x_1 &= x_1 + (n_1x_1 + n_2x_2 + \cdots + n_rx_r) \\ &= (n_1 + 1)x_1 + n_2x_2 + \cdots + n_rx_r, \end{aligned}$$

lo cual da dos maneras de escribir  $x_1 \neq 0$  lo que contradice la hipótesis de unicidad de la condición 1. Así, la condición 1 implica la condición 2.

Mostremos ahora que la condición 2 implica la condición 1. Sea  $a \in G$ . Como  $X$  genera  $G$ , podemos escribir  $a$  en la forma  $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ . Supóngase que  $a$  tiene otra expresión del mismo tipo en términos de elementos de  $X$ . Usando algunos coeficientes cero en las dos expresiones, podemos suponer que ambas tienen los mismos elementos de  $X$  y que son de la forma

$$\begin{aligned} a &= n_1x_1 + n_2x_2 + \cdots + n_rx_r \\ a &= m_1x_1 + m_2x_2 + \cdots + m_rx_r. \end{aligned}$$

Al restar, obtenemos

$$0 = (n_1 - m_1)x_1 + (n_2 - m_2)x_2 + \cdots + (n_r - m_r)x_r,$$

de modo que, por la condición 2,  $n_i - m_i = 0$  y  $n_i = m_i$  para  $i = 1, 2, \dots, r$ . Así, los coeficientes son únicos. ■

**Definición** Un grupo abeliano con un conjunto generador no vacío  $X$  que satisface las condiciones descritas en el teorema 20.1 es un **grupo abeliano libre** y  $X$  es una **base** del grupo.

**Ejemplo 20.1** El grupo  $\mathbf{Z} \times \mathbf{Z}$  es un grupo abeliano libre y  $\{(1, 0), (0, 1)\}$  es una base. Es claro que una base para el grupo abeliano libre  $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$  es  $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ , y así sucesivamente. Así, los productos directos finitos del grupo  $\mathbf{Z}$  con él mismo son grupos abelianos libres. ■

**Ejemplo 20.2** El grupo  $\mathbf{Z}_n$  no es abeliano libre, pues  $nx = 0$  para toda  $x \in \mathbf{Z}_n$ , y  $n \neq 0$ , lo cual contradice la condición 2. ■

Supóngase que el grupo abeliano libre  $G$  tiene base finita  $X = \{x_1, x_2, \dots, x_r\}$ . Si  $a \in G$  y  $a \neq 0$ , entonces  $a$  tiene una expresión única de la forma

$$a = n_1 x_1 + n_2 x_2 + \cdots + n_r x_r, \quad \text{para } n_i \in \mathbf{Z}.$$

Definimos

$$\phi: G \rightarrow \underbrace{\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}}_{r \text{ factores}}$$

por  $a\phi = (n_1, n_2, \dots, n_r)$  y  $0\phi = (0, 0, \dots, 0)$ . Es fácil probar que  $\phi$  es un isomorfismo. Dejamos los detalles para los ejercicios (véase el ejercicio 20.1) y enunciamos el resultado como un teorema.

**Teorema 20.2** Si  $G$  es un grupo abeliano libre distinto de cero con una base de  $r$  elementos, entonces  $G$  es isomorfo a  $\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$  con  $r$  factores.

Es un hecho que cualesquiera dos bases de un grupo abeliano libre  $G$  contienen el mismo número de elementos. Probaremos esto sólo para el caso en que  $G$  tenga una base finita, aunque también es cierto si toda base de  $G$  es infinita. La demostración es realmente bella; da una caracterización sencilla del número de elementos en una base en términos del tamaño de un grupo factor.

**Teorema 20.3** Sea  $G \neq \{0\}$  un grupo abeliano libre con una base finita. Entonces, toda base de  $G$  es finita y todas las bases tienen el mismo número de elementos.

*Demostración* Sea  $G$  con base  $\{x_1, x_2, \dots, x_r\}$ . Entonces,  $G$  es isomorfo a  $\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$  con  $r$  factores. Sea  $2G = \{2g \mid g \in G\}$ . Se comprueba fácilmente que  $2G$  es un subgrupo de  $G$ . Como  $G \cong \mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$  para  $r$  factores, tenemos

$$G/2G \cong (\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z})/(2\mathbf{Z} \times 2\mathbf{Z} \times \cdots \times 2\mathbf{Z}) \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2$$

con  $r$  factores. Así,  $|G/2G| = 2^r$  de modo que el número de elementos en cualquier base finita de  $G$  es  $\log_2 |G/2G|$ . Así, cualesquiera dos bases finitas tienen el mismo número de elementos.

Falta demostrar que  $G$  no puede tener, además, una base infinita. Sea  $Y$  cualquier base de  $G$  y sean  $\{y_1, y_2, \dots, y_s\}$  elementos distintos en  $Y$ . Sea  $H$  el subgrupo de  $G$  generado por  $\{y_1, y_2, \dots, y_s\}$  y sea  $K$  el subgrupo de  $G$  generado por los elementos restantes de  $Y$ . Es fácil ver que  $G \cong H \times K$ , de modo que  $G/2G \cong (H/2H) \times (K/2K) \cong (H/2H) \times (K/2K)$ . Como  $|H/2H| = 2^s$ ,

$|G/2G| \geq 2^s$ . Como  $|G/2G| = 2^r$ ,  $s \leq r$ . Entonces,  $Y$  no puede ser un conjunto infinito, ya que, de ser así, podríamos tomar  $s > r$ . ■

**Definición** Si  $G$  es un grupo abeliano libre, el *rango de  $G$*  es el número de elementos en una base de  $G$ . (Todas las bases tienen el mismo número de elementos.)

## \*20.2 DEMOSTRACION DEL TEOREMA FUNDAMENTAL

Probaremos el teorema fundamental (teorema 9.3) mostrando que cualquier grupo abeliano finitamente generado es isomorfo a un grupo factor de la forma

$$(\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z})/(d_1\mathbf{Z} \times d_2\mathbf{Z} \times \cdots \times d_s\mathbf{Z} \times \{0\} \times \cdots \times \{0\}),$$

donde tanto el «numerador» como el «denominador» tienen  $n$  factores y  $d_1$  divide  $d_2$ , que divide  $d_3$ , ..., que divide  $d_s$ . De aquí se seguirá fácilmente la descomposición 2 del teorema 9.3.

Para mostrar que  $G$  es isomorfo a dicho grupo factor, mostraremos que existe algún homomorfismo de  $\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$  sobre  $G$  con kernel de la forma  $d_1\mathbf{Z} \times d_2\mathbf{Z} \times \cdots \times d_s\mathbf{Z} \times \{0\} \times \cdots \times \{0\}$ . Entonces, el resultado se obtendrá por el teorema 13.3. Los teoremas siguientes darán los detalles del análisis. El objetivo de estos párrafos introductorios es hacer notar hacia dónde vamos al leer lo que sigue.

**Teorema 20.4** Sea  $G$  un grupo abeliano finitamente generado, con conjunto generador  $\{a_1, a_2, \dots, a_n\}$ . Sea

$$\phi: \underbrace{\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}}_{n \text{ factores}} \rightarrow G$$

definido por  $(h_1, h_2, \dots, h_n)\phi = h_1a_1 + h_2a_2 + \cdots + h_na_n$ . Entonces  $\phi$  es un homomorfismo sobre  $G$ .

**Demostración** Del significado de  $h_i a_i$  para  $h_i \in \mathbf{Z}$  y  $a_i \in G$  se desprende en seguida que  $[(h_1, \dots, h_n) + (k_1, \dots, k_n)]\phi = (h_1 + k_1, \dots, h_n + k_n)\phi = (h_1 + k_1)a_1 + \cdots + (h_n + k_n)a_n = (h_1a_1 + k_1a_1) + \cdots + (h_na_n + k_na_n) = (h_1a_1 + \cdots + h_na_n) + (k_1a_1 + \cdots + k_na_n) = (h_1, \dots, h_n)\phi + (k_1, \dots, k_n)\phi$ . Como  $\{a_1, \dots, a_n\}$  genera  $G$ , es claro que el homomorfismo  $\phi$  es sobre  $G$ . ■

Probemos ahora una «propiedad de reemplazo» que permite ajustar una base.

**Teorema 20.5** Si  $X = \{x_1, \dots, x_r\}$  es una base de un grupo abeliano libre  $G$  y  $t \in \mathbf{Z}$ , entonces para  $i \neq j$  el conjunto  $Y = \{x_1, \dots, x_{j-1}, x_j + tx_i, x_{j+1}, \dots, x_r\}$ , también es una base de  $G$ .

*Demostración* Como  $x_j = (-t)x_i + (1)(x_j + tx_i)$ , se puede recobrar  $x_j$  de  $Y$ , el cual, entonces, también genera  $G$ . Supóngase que

$$n_1x_1 + \cdots + n_{j-1}x_{j-1} + n_j(x_j + tx_i) + n_{j+1}x_{j+1} + \cdots + n_rx_r = 0.$$

Entonces,

$$n_1x_1 + \cdots + (n_i + n_jt)x_i + \cdots + n_jx_j + \cdots + n_rx_r = 0,$$

y como  $X$  es una base,  $n_1 = \cdots = n_i + n_jt = \cdots = n_j = \cdots = n_r = 0$ . De  $n_j = 0$  y  $n_i + n_jt = 0$  se sigue que también  $n_i = 0$ , de modo que  $n_1 = \cdots = n_i = n_j = \cdots = n_r = 0$  y se satisface la condición 2 del teorema 20.1. Así,  $Y$  es una base. ■

**Ejemplo 20.3** Una base de  $\mathbf{Z} \times \mathbf{Z}$  es  $\{(1, 0), (0, 1)\}$ . Otra base es  $\{(1, 0), (4, 1)\}$ , pues  $(4, 1) = 4(1, 0) + (0, 1)$ . Sin embargo,  $\{(3, 0), (0, 1)\}$  no es base. No es posible expresar, por ejemplo,  $(2, 0)$  en la forma  $n_1(3, 0) + n_2(0, 1)$  para  $n_1, n_2 \in \mathbf{Z}$ . Aquí,  $(3, 0) = (1, 0) + 2(1, 0)$ , se sumó a sí mismo un múltiplo de un elemento de la base, en lugar de sumarlo a un elemento diferente de la base. ■

Un grupo abeliano libre  $G$ , de rango finito, puede tener varias bases. Mostremos que si  $K \leq G$  entonces  $K$  también es abeliano libre, con rango no mayor que el de  $G$ . Además, y esto es importante, existen bases de  $G$  y de  $K$  bellamente relacionadas una con la otra.

**Teorema 20.6** *Sea  $G$  un grupo abeliano libre, distinto de cero, de rango finito  $n$ , y sea  $K$  un subgrupo distinto de cero de  $G$ . Entonces  $K$  es abeliano libre, de rango  $s \leq n$ . Más aún, existe una base  $\{x_1, x_2, \dots, x_n\}$  para  $G$  y enteros positivos  $d_1, d_2, \dots, d_s$  donde  $d_i$  divide a  $d_{i+1}$  para  $i = 1, \dots, s-1$ , tales que  $\{d_1x_1, d_2x_2, \dots, d_sx_s\}$  es una base de  $K$ .*

*Demostración* Mostremos que  $K$  tiene una base de la forma descrita, lo cual mostrará, por supuesto, que es abeliano libre de rango a lo más  $n$ . Supóngase que  $Y = \{y_1, \dots, y_n\}$  es una base para  $G$ . Todos los elementos distintos de cero en  $K$  se pueden expresar en la forma:

$$k_1y_1 + \cdots + k_ny_n,$$

donde algún  $|k_i|$  es distinto de cero. De entre todas las bases  $Y$  de  $G$ , selecciónese una  $Y_1$  que produzca el mínimo de dichos valores distintos de cero  $|k_i|$  al escribir todos los elementos distintos de cero de  $K$ , en términos de elementos de la base en  $Y_1$ . Si es necesario, con una nueva numeración de los elementos de  $Y_1$ , se puede suponer que existe  $w_1 \in K$  tal que

$$w_1 = d_1y_1 + k_2y_2 + \cdots + k_ny_n$$

donde  $d_1 > 0$  y  $d_1$  es el mínimo coeficiente obtenido según se describió. Usando el algoritmo de la división, escribábase  $k_j = d_1 q_j + r_j$ , donde  $0 \leq r_j < d_1$  para  $j = 2, \dots, n$ . Entonces,

$$w_1 = d_1(y_1 + q_2 y_2 + \cdots + q_n y_n) + r_2 y_2 + \cdots + r_n y_n. \quad [20.1]$$

Ahora bien, sea  $x_1 = y_1 + q_2 y_2 + \cdots + q_n y_n$ . Por el teorema 20.5,  $\{x_1, y_2, \dots, y_n\}$  también es una base de  $G$ . De la ecuación [20.1] y la selección de  $Y_1$  para el coeficiente mínimo  $d_1$ , se observa que  $r_2 = \cdots = r_n = 0$ . Así,  $d_1 x_1 \in K$ .

Consideremos ahora bases para  $G$  de la forma  $\{x_1, y_2, \dots, y_n\}$ . Cada elemento de  $K$  puede expresarse en la forma

$$h_1 x_1 + k_2 y_2 + \cdots + k_n y_n.$$

Como  $d_1 x_1 \in K$ , podemos sustraer un múltiplo adecuado de  $d_1 x_1$  y después usar la minimalidad de  $d_1$  para ver que  $h_1$  es un múltiplo de  $d_1$ , se observa que, en realidad,  $k_2 y_2 + \cdots + k_n y_n$  está en  $K$ . Entre todas esas bases  $\{x_1, y_2, \dots, y_n\}$  escogemos  $Y_2$  que produzca algún  $k_i \neq 0$  de magnitud mínima. (Es posible que todos los  $k_i$  sean siempre cero. En este caso,  $K$  está generado por  $d_1 x_1$  y eso es todo.) Podemos suponer, reenumerando los elementos de  $Y_2$ , que existe  $w_2 \in K$  tal que

$$w_2 = d_2 y_2 + \cdots + k_n y_n$$

donde  $d_2 > 0$  y  $d_2$  es minimal en el sentido recién descrito. Precisamente como en el párrafo anterior, podemos modificar la base de  $Y_2 = \{x_1, y_2, \dots, y_n\}$  a una base  $\{x_1, x_2, y_3, \dots, y_n\}$  para  $G$  donde  $d_1 x_1 \in K$  y  $d_2 x_2 \in K$ . Escribiendo  $d_2 = d_1 q + r$  para  $0 \leq r < d_1$ , se ve que  $\{x_1 + q x_2, x_2, y_3, \dots, y_n\}$  es una base para  $G$ , y  $d_1 x_1 + d_2 x_2 = d_1(x_1 + q x_2) + r x_2$  está en  $K$ . Por la selección minimal de  $d_1$ , se ve que  $r = 0$ , de modo que  $d_1$  divide  $d_2$ .

Consideremos todas las bases de la forma  $\{x_1, x_2, y_3, \dots, y_n\}$  para  $G$  y examinemos elementos de  $K$  de la forma  $k_3 y_3 + \cdots + k_n y_n$ . El patrón es claro. El proceso continúa hasta obtener una base  $\{x_1, x_2, \dots, x_s, y_{s+1}, \dots, y_n\}$  donde el único elemento de  $K$  de la forma  $k_{s+1} y_{s+1} + \cdots + k_n y_n$  es cero, esto es, todas las  $k_i$  son cero. Entonces, se hace que  $x_{s+1} = y_{s+1}, \dots, x_n = y_n$  y obtenemos una base de  $G$  de la forma descrita en el enunciado del teorema 20.6. ■

**Teorema 20.7** *Todo grupo abeliano finitamente generado es isomorfo a un grupo de la forma*

$$\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r} \times \mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$$

donde  $m_i$  divide a  $m_{i+1}$  para  $i = 1, \dots, r - 1$ .

**Demostración** Para el propósito de esta demostración, será conveniente usar las notaciones  $\mathbf{Z}/1\mathbf{Z} = \mathbf{Z}/\mathbf{Z} \cong \mathbf{Z}_1 = \{0\}$ . Sea  $G$  finitamente generado por  $n$

elementos. Sea  $F = \mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$  para  $n$  factores. Considérese el homomorfismo  $\phi: F \rightarrow G$  del teorema 20.4 y sea  $K$  el kernel de este homomorfismo. Entonces, existe una base para  $F$  de la forma  $\{x_1, \dots, x_n\}$  donde  $\{d_1 x_1, \dots, d_n x_n\}$  es una base de  $K$  y  $d_i$  divide  $d_{i+1}$ , para  $i = 1, \dots, s - 1$ . Por el teorema 13.3,  $G$  es isomorfo a  $F/K$ . Pero,

$$\begin{aligned} F/K &\simeq (\mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z})/(d_1 \mathbf{Z} \times d_2 \mathbf{Z} \times \cdots \times d_s \mathbf{Z} \times \{0\} \times \cdots \times \{0\}) \\ &\simeq \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z} \times \cdots \times \mathbf{Z}. \end{aligned}$$

Es posible que  $d_1 = 1$ , en cuyo caso  $\mathbf{Z}_{d_1} = \{0\}$  y puede eliminarse (salvo isomorfismo) de este producto. De manera análoga,  $d_2$  puede ser 1, y así sucesivamente. Al hacer que sea  $m_1$  la primera  $d_i > 1$ ,  $m_2$  la siguiente  $d_i$ , y así sucesivamente, se deduce el teorema de inmediato. ■

Hemos demostrado la parte más difícil del teorema 9.3. Es claro que existe una descomposición en potencias de primos, ya que se pueden descomponer los grupos  $\mathbf{Z}_{m_i}$  en factores potencias de primos. La parte restante del teorema 9.3 analiza la unicidad del número de betti, los coeficientes de torsión y las potencias de primos. El número de betti aparece como el rango del grupo abeliano libre  $G/T$ , donde  $T$  es el subgrupo de torsión de  $G$ . Por el teorema 20.3, que muestra la unicidad del número de betti, este rango es invariante. La unicidad de los coeficientes de torsión y de las potencias de primos es un poco más difícil de mostrar. Damos algunos ejercicios que indican su unicidad (véanse los ejercicios 20.12 al 20.20).

## Ejercicios

---

\*20.1 Complétese la demostración del teorema 20.2.

\*20.2 Encuéntrese una base  $\{(a_1, a_2, a_3), (b_1, b_2, b_3), (c_1, c_2, c_3)\}$  para  $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$  con todas las  $a_i \neq 0$ , las  $b_i \neq 0$  y las  $c_i \neq 0$ . (Hay varias respuestas posibles.)

\*20.3 ¿Es  $\{(2, 1), (3, 1)\}$  una base para  $\mathbf{Z} \times \mathbf{Z}$ ? Pruébese la respuesta.

\*20.4 ¿Es  $\{(2, 1), (4, 1)\}$  una base para  $\mathbf{Z} \times \mathbf{Z}$ ? Pruébese la respuesta.

\*20.5 Encuéntrense condiciones sobre  $a, b, c, d \in \mathbf{Z}$  para que  $\{(a, b), (c, d)\}$  sea una base de  $\mathbf{Z} \times \mathbf{Z}$ . [Sugerencia: resuélvase  $x(a, b) + y(c, d) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$  en  $\mathbf{R}$  y véase en qué caso los valores están en  $\mathbf{Z}$ .]

†\*20.6 Muéstrese que un grupo abeliano libre no contiene elementos distintos de cero de orden finito.

\*20.7 ¿Falso o verdadero?

- a) Todo grupo abeliano libre es libre de torsión.
- b) Todo grupo abeliano libre de torsión, finitamente generado, es un grupo abeliano libre.
- c) Existe algún grupo abeliano libre para todo rango entero positivo.

- d) Un grupo abeliano finitamente generado es abeliano libre si su número de betti es igual al número de elementos en algún conjunto generador.
- e) Si  $X$  genera un grupo abeliano libre  $G$  y  $X \subseteq Y \subseteq G$ , entonces  $Y$  genera  $G$ .
- f) Si  $X$  es una base de un grupo abeliano libre  $G$  y  $X \subseteq Y \subseteq G$ , entonces  $Y$  es una base de  $G$ .
- g) Todo grupo abeliano libre distinto de cero tiene un número infinito de bases.
- h) Todo grupo abeliano libre de rango al menos 2 tiene un número infinito de bases.
- i) Si  $K$  es un subgrupo distinto de cero de un grupo abeliano libre finitamente generado, entonces  $K$  es abeliano libre.
- j) Si  $K$  es un subgrupo distinto de cero de un grupo abeliano libre finitamente generado, entonces  $G/K$  es abeliano libre.

\*20.8 Muéstrese, mediante un ejemplo, la posibilidad de que un subgrupo propio de un grupo abeliano libre de rango finito  $r$  también tenga rango  $r$ .

\*20.9 Muéstrese que si  $G$  y  $G'$  son grupos abelianos libres, entonces  $G \times G'$  es abeliano libre.

\*20.10 Muéstrese que los grupos abelianos libres de rango finito son precisamente los grupos abelianos finitamente generados donde ningún elemento distinto de cero es de orden finito.

\*20.11 Muéstrese que  $\mathbb{Q}$  bajo la suma no es un grupo abeliano libre. [Sugerencia: muéstrese que no hay dos números racionales distintos  $n/m$  y  $r/s$  que puedan estar contenidos en un conjunto que satisfaga las condiciones 2 del teorema 20.1.]

*Los ejercicios 12 al 17 se refieren a la demostración de la unicidad de las potencias de primos que aparecen en la descomposición en potencias de primos del subgrupo de torsión  $T$  de un grupo abeliano finitamente generado.*

\*20.12 Sea  $p$  un primo fijo. Muéstrese que los elementos de  $T$  de orden alguna potencia de  $p$ , junto con el cero, forman un subgrupo  $T_p$  de  $T$ .

\*20.13 Muéstrese que en cualquier descomposición en potencias de primos de  $T$ , el subgrupo  $T_p$  del ejercicio anterior es isomorfo al producto directo de aquellos factores cíclicos de orden alguna potencia del primo  $p$ . [Esto reduce el problema a mostrar que el grupo  $T_p$  no puede tener descomposiciones en productos de grupos cíclicos esencialmente diferentes.]

\*20.14 Sea  $G$  cualquier grupo abeliano y sea  $n$  cualquier entero positivo. Muéstrese que  $G[n] = \{x \in G \mid nx = 0\}$  es un subgrupo de  $G$ . (En notación multiplicativa,  $G[n] = \{x \in G \mid x^n = e\}$ .)

\*20.15 Con referencia al ejercicio 20.14, muéstrese que  $\mathbb{Z}_{p^r}[p] \simeq \mathbb{Z}_p$  para cualquier  $r \geq 1$  y cualquier primo  $p$ .

\*20.16 Usando el ejercicio 20.15, muéstrese que

$$(\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_m}})[p] \simeq \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{m \text{ factores}}$$

siempre que cada  $r_i \geq 1$ .

\*20.17 Sea  $G$  un grupo abeliano finitamente generado y  $T_p$  el subgrupo definido en el ejercicio 20.12. Supóngase que  $T_p \cong \mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_m}} \cong \mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_n}}$  donde  $1 \leq r_1 \leq r_2 \leq \cdots \leq r_m$  y  $1 \leq s_1 \leq s_2 \leq \cdots \leq s_n$ . Debemos mostrar que  $m = n$  y  $r_i = s_i$  para  $i = 1, \dots, n$  para completar la demostración de la unicidad de la descomposición en potencias de primos.

- Usese el ejercicio 20.16 para mostrar que  $n = m$ .
- Supóngase que  $r_i = s_j$  para todas las  $i < j$ . Muéstrese que  $r_j = s_j$ , lo cual completará la demostración. [Sugerencia: supóngase que  $r_j < s_j$ . Considerese el subgrupo  $p^{r_j}T_p = \{p^{r_j}x \mid x \in T_p\}$  y muéstrese que este subgrupo tendría, entonces, dos descomposiciones en potencias de primos con números diferentes de factores distintos de cero. A continuación argúmese que esto es imposible por la parte a) de este ejercicio.]

Sea  $T$  el subgrupo de torsión de un grupo abeliano finitamente generado. Supóngase que  $T \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ , donde  $m_i$  divide  $m_{i+1}$  para  $i = 1, \dots, r - 1$  y  $n_j$  divide  $n_{j+1}$  para  $j = 1, \dots, s - 1$  y  $m_1 > 1$  y  $n_1 > 1$ . Deseamos mostrar que  $r = s$  y  $m_k = n_k$  para  $k = 1, \dots, r$  demostrando, así, la unicidad de los coeficientes de torsión. Esto se hace en los ejercicios 18 al 20.

\*20.18 Indíquese cómo se puede obtener una descomposición en potencias de primos a partir de una descomposición en coeficientes de torsión. (Obsérvese que, en el ejercicio anterior, se muestra que las potencias de primos obtenidas son únicas.)

\*20.19 Compruébese, a partir del ejercicio 20.18, que  $m_r$  y  $n_s$  pueden caracterizarse, ambos, de la manera siguiente: sean  $p_1, \dots, p_t$  los primos distintos que dividen a  $|T|$ , y sean  $p_1^{k_1}, \dots, p_t^{k_t}$  las mayores potencias de estos primos, que aparecen en la descomposición (única) de potencias de primos. Entonces,  $m_r = n_s = p_1^{k_1}p_2^{k_2} \cdots p_t^{k_t}$ .

\*20.20 Caracterícese  $m_{r-i}$  y  $n_{s-i}$  mostrando que son iguales y muéstrese que  $m_{r-i} = n_{s-i}$  para  $i = 1, \dots, r - 1$  y que  $r = s$ .

## Grupos libres

En éste y el siguiente capítulo analizaremos una parte de la teoría de grupos que es de gran interés, no sólo en álgebra, sino también en topología. De hecho, en Crowell y Fox [45, capítulos 3 y 4] hay un excelente análisis, bastante accesible, de grupos libres y presentaciones de grupos.

### \* 21.1 PALABRAS Y PALABRAS REDUCIDAS

Sea  $A$  cualquier conjunto (no necesariamente finito) de elementos  $a_i$  para  $i \in I$ . Consideramos  $A$  como un alfabeto y las  $a_i$  como letras del alfabeto. Cualquier símbolo de la forma  $a_i^n$  con  $n \in \mathbb{Z}$  es una sílaba y una cadena finita  $w$  de sílabas, escritas en yuxtaposición, es una palabra. Presentamos también la palabra vacía 1, que no tiene sílabas.

**Ejemplo 21.1** Sea  $A = \{a_1, a_2, a_3\}$ . Entonces, si adoptamos la convención de que  $a_i^1$  es lo mismo que  $a_i$ ,

$$a_1 a_3^{-4} a_2^2 a_3, \quad a_2^3 a_2^{-1} a_3 a_1^2 a_1^{-7} \quad \text{y} \quad a_3^2$$

son palabras. ■

Hay dos tipos naturales de modificaciones de ciertas palabras: las contracciones elementales. El primero consiste en reemplazar  $a_i^n a_i^m$  en una palabra, por  $a_i^{n+m}$ . El segundo tipo consiste en reemplazar  $a_i^0$  en una palabra por 1, esto es, quitarla de la palabra. Mediante un número finito de contracciones elementales, toda palabra se puede cambiar por una palabra reducida, para la cual no es posible

efectuar más contracciones elementales. Nótese que estas contracciones elementales equivalen formalmente a las manipulaciones usuales de exponentes enteros.

**Ejemplo 21.2** La forma reducida de la palabra  $a_2^3a_2^{-1}a_3a_1^2a_1^{-7}$  del ejemplo 21.1 es  $a_2^2a_3a_1^{-5}$ . ■

Es necesario advertir aquí que no se analizarán con profundidad varios puntos que en algunos libros toman páginas en demostrar, usualmente mediante complicados argumentos de inducción, divididos en varios casos. Por ejemplo, supóngase que se da una palabra y se desea encontrar su forma reducida. Puede haber gran variedad de contracciones elementales que pudieran efectuarse primero. ¿Cómo saber que la palabra reducida final es la misma, sin importar en qué orden se efectuaron las contracciones elementales? Probablemente, el estudiante dirá que es obvio. Algunos autores realizan un esfuerzo considerable para probarlo. El autor se inclina a estar de acuerdo con el estudiante en este punto. Le parece tedioso este tipo de demostraciones y no le han hecho sentirse mejor. Sin embargo, el autor es el primero en reconocer que no es un gran matemático. Con deferencia hacia el hecho de que muchos matemáticos piensan que estas cosas sí necesitan de considerable análisis, marcaremos cada ocasión en que simplemente calificaremos tales hechos mediante la frase «Parecería obvio que», conservando las comillas.

## \*21.2 GRUPOS LIBRES

Sea  $F[A]$  el conjunto de todas las palabras reducidas formadas con nuestro alfabeto  $A$ . Sea  $F[A]$  un grupo de manera natural. Para  $w_1$  y  $w_2$  en  $F[A]$  definimos  $w_1 \cdot w_2$  como la forma reducida de la palabra obtenida por la yuxtaposición  $w_1w_2$  de las dos palabras.

**Ejemplo 21.3** Si

$$w_1 = a_2^3a_1^{-5}a_3^2$$

y

$$w_2 = a_3^{-2}a_1^2a_3a_2^{-2},$$

entonces,  $w_1 \cdot w_2 = a_2^3a_1^{-3}a_3a_2^{-2}$ . ■

«Parecería obvio que» esta operación de multiplicación en  $F[A]$  está bien definida y es asociativa. Es obvio que la palabra vacía 1 actúa como elemento identidad. «Parecería obvio que», dada una palabra reducida  $w \in F[A]$ , si se forma la palabra a partir de la primera, escribiendo primero las silabas de  $w$  en el orden opuesto y después reemplazando cada  $a_i^n$  por  $a_i^{-n}$ , entonces, la palabra resultante  $w^{-1}$  es también una palabra reducida y

$$w \cdot w^{-1} = w^{-1} \cdot w = 1.$$

**Definición** El grupo  $F[A]$ , recién descrito, es el *grupo libre generado* por  $A$ .

Regresemos al teorema 9.1 y a la definición anterior a él para ver que este uso del término *generado*, es consistente con el uso anterior. Comenzando con un grupo  $G$  y un conjunto generador  $\{a_i \mid i \in I\}$  podríamos preguntar si  $G$  es *libre en*  $\{a_i\}$ , esto es, si  $G$  es esencialmente el grupo libre generado por  $\{a_i\}$ . Definamos su significado preciso.

**Definición** Si  $G$  es un grupo con un conjunto  $A = \{a_i\}$  de generadores y si  $G$  es isomorfo a  $F[A]$  bajo una transformación  $\phi: G \rightarrow F[A]$  tal que  $a_i\phi = a_i$ , entonces  $G$  es *libre en*  $\{a_i\}$  y las  $a_i$  son los *generadores libres de*  $G$ . Un grupo es *libre* si es libre en algún conjunto  $\{a_i\}$  no vacío.

**Ejemplo 21.4** El único ejemplo de grupo libre que se ha presentado hasta ahora es  $\mathbb{Z}$ , el cual es libre en un generador. Claramente, todo grupo libre es infinito. ■

El lector deberá referirse a la literatura respectiva, para las demostraciones de los siguientes tres teoremas. No se usarán estos resultados. Se enuncian sólo para informar de estos interesantes hechos.

**Teorema 21.1** Si un grupo  $G$  es libre en  $\{a_i\}$  y también en  $\{b_j\}$ , entonces los conjuntos  $\{a_i\}$  y  $\{b_j\}$  tienen el mismo número de elementos, esto es, cualesquiera dos conjuntos de generadores libres de un grupo libre tienen la misma cardinalidad.

**Definición** Si  $G$  es libre en  $\{a_i\}$ , el número de elementos en  $\{a_i\}$  es el *rango del grupo libre*  $G$ .

En realidad, el siguiente teorema es bastante evidente a partir del teorema 21.1.

**Teorema 21.2** Dos grupos libres son isomorfos si y sólo si tienen el mismo rango.

**Teorema 21.3** Un subgrupo propio no trivial de un grupo libre es libre.

**Ejemplo 21.5** Sea  $F[\{x, y\}]$  el grupo libre en  $\{x, y\}$ . Sea

$$y_k = x^k y x^{-k}$$

para  $k \geq 0$ . No habrá dificultad para convencerse de que  $y_k$  para  $k \geq 0$  son generadores libres del subgrupo de  $F[\{x, y\}]$  que generan. Esto ilustra que, aunque un subgrupo de un grupo libre es libre, el rango del subgrupo puede ser mucho mayor que el rango de todo el grupo. ■

## \*21.3 HOMOMORFISMOS DE GRUPOS LIBRES

Nuestro trabajo en esta sección se referirá principalmente a homomorfismos definidos en un grupo libre. Los resultados son sencillos y elegantes.

**Teorema 21.4** *Sea  $G$  generado por  $\{a_i \mid i \in I\}$  y sea  $G'$  un grupo cualquiera. Si  $a'_i$  para  $i \in I$  son elementos cualesquiera en  $G'$ , no necesariamente distintos, entonces existe a lo más un homomorfismo  $\phi: G \rightarrow G'$  tal que  $a_i\phi = a'_i$ . Si  $G$  es libre en  $\{a_i\}$  entonces existe precisamente uno de dichos homomorfismos.*

*Demostración* Sea  $\phi$  un homomorfismo de  $G$  en  $G'$  tal que  $a_i\phi = a'_i$ . Ahora, por el teorema 9.1, para cualquier  $x \in G$  tenemos

$$x = \prod_j a_{ij}^{n_j}$$

para algún producto finito de los generadores  $a_i$ , donde las  $a_{ij}$ , que aparecen en el producto, no necesariamente son distintas. Entonces, como  $\phi$  es un homomorfismo, debemos tener

$$x\phi = \prod_j (a_{ij}^{n_j})\phi = \prod_j (a'_{ij})^{n_j}.$$

Así, un homomorfismo está determinado por completo por sus valores en elementos de un conjunto generador. Esto muestra que hay a lo más un homomorfismo tal que  $a_i\phi = a'_i$ .

Ahora, supóngase que  $G$  es libre en  $\{a_i\}$ , esto es, que  $G = F[\{a_i\}]$ . Para

$$x = \prod_j a_{ij}^{n_j}$$

en  $G$ , definase  $\psi: G \rightarrow G'$  por

$$x\psi = \prod_j (a'_{ij})^{n_j}.$$

Esta transformación está bien definida, pues  $F[\{a_i\}]$  consta precisamente de palabras reducidas; ningún par de productos formales diferentes en  $F[\{a_i\}]$  son iguales. Como las reglas para calcular con exponentes en  $G'$  son formalmente iguales que las usadas para exponentes en  $G$ , es claro que  $(xy)\psi = (x\psi)(y\psi)$  para cualesquiera elementos  $x$  y  $y$  en  $G$ , así que  $\psi$  es, en efecto, un homomorfismo. ■

Quizá debimos haber probado antes la primera parte de este teorema, en lugar de haberla relegado a los ejercicios. Nótese que el teorema afirma que *un homomorfismo de un grupo está completamente determinado si se conoce su valor en cada*

elemento de un conjunto generador. Esto es bastante obvio y podría haberse mencionado inmediatamente después de la definición de homomorfismo. En particular, un homomorfismo de un grupo cíclico está completamente determinado por su valor en uno cualquiera de los generadores del grupo.

**Teorema 21.5** Todo grupo  $G'$  es la imagen homomorfa de algún grupo libre  $G$ .

**Demostración** Sea  $G' = \{a'_i\}$  y sea  $\{a_i\}$  un conjunto con el mismo número de elementos que  $G'$ . Sea  $G = F[\{a_i\}]$ . Entonces, por el teorema 21.4, existe un homomorfismo  $\psi$  que transforma  $G$  en  $G'$  tal que  $a_i\psi = a'_i$ . Claramente, la imagen de  $G$  bajo  $\psi$  es todo  $G'$ . ■

## \*21.4 MAS SOBRE GRUPOS ABELIANOS LIBRES

Es importante no confundir el concepto de grupo libre con el concepto de grupo abeliano libre. Un grupo libre en más de un generador, no es abeliano. En el capítulo anterior definimos un grupo abeliano libre como un grupo abeliano que tiene una base, esto es, un conjunto generador que satisface las propiedades descritas en el teorema 20.1. Hay otro enfoque, vía grupos libres, de los grupos abelianos libres. Describiremos este enfoque.

Sea  $F[A]$  el grupo libre en el conjunto generador  $A$ . Por el momento, escribiremos  $F$  en lugar de  $F[A]$ . Nótese que si  $A$  contiene más de un elemento,  $F$  no es abeliano. Sea  $F'$  el subgrupo conmutador de  $F$ . Entonces,  $F/F'$  es un grupo abeliano y es claro que  $F/F'$  es abeliano libre con base  $\{a + F' | a \in A\}$ . Si cambiamos el nombre de  $a + F'$  por  $a$ , podemos ver  $F/F'$  como un grupo abeliano libre con base  $A$ . Esto indica cómo puede construirse un grupo abeliano libre a partir de un conjunto dado como base. Todo grupo abeliano libre puede construirse de esta manera, salvo isomorfismo. Esto es, si  $G$  es abeliano libre con base  $X$ , se forma el grupo libre  $F[X]$ , y se forma el grupo factor de  $F[X]$  módulo su subgrupo conmutador, se tendrá un grupo isomorfo a  $G$ .

Los teoremas 21.1, 21.2 y 21.3 valen tanto para grupos abelianos libres, como para grupos libres. De hecho, en el teorema 20.6 se probó la versión abeliana del teorema 21.3 para el caso de rango finito. En contraste con el ejemplo 21.5 para grupos libres, es cierto que para un grupo abeliano libre, el rango de un subgrupo es a lo más el rango de todo el grupo. El teorema 20.6 también lo muestra para el caso de rango finito.

### Ejercicios

\*21.1 Encuéntrese la forma reducida y el inverso de la forma reducida de cada una de las siguientes palabras.

a)  $a^2b^{-1}b^3a^3c^{-1}c^4b^{-2}$

b)  $a^2a^{-3}b^3a^4c^4c^2a^{-1}$

**\*21.2** Calcúlense los productos dados en las partes a) y b) del ejercicio 21.1 en el caso de que  $\{a, b, c\}$  sea un conjunto de generadores que conforman una base de un grupo abeliano libre. Encuéntrense los inversos de estos productos.

\*21.3 ¿Cuántos homomorfismos diferentes hay de un grupo libre de rango 2 en

- a)  $\mathbf{Z}_4$ ?      b)  $\mathbf{Z}_6$ ?      c)  $S_3$ ?

\*21.4 ¿Cuántos homomorfismos diferentes hay de un grupo libre de rango 2 sobre



\*21.5 ¿Cuántos homomorfismos diferentes hay de un grupo abeliano libre de rango 2 en

- a)  $Z_4$ ?      b)  $Z_6$ ?      c)  $S_3$ ?

\*21.6 ¿Cuántos homomorfismos diferentes hay de un grupo abeliano libre de rango 2 sobre



<sup>††</sup>21.7 Tómese uno de los ejemplos de esta sección donde se haya usado la frase «Parecía obvio que» y analícese la reacción que se tuvo con respecto a ese ejemplo.

**\*21.8 ¿Falso o verdadero?**

- a) Todo subgrupo propio de un grupo libre es un grupo libre.
  - b) Todo subgrupo propio de todo grupo abeliano libre es un grupo libre.
  - c) Una imagen homomorfa de un grupo libre es un grupo libre.
  - d) Todo grupo abeliano libre tiene base.
  - e) Los grupos abelianos libres de rango finito son precisamente grupos abelianos finitamente generados.
  - f) Ningún grupo libre es abeliano.
  - g) Ningún grupo abeliano libre es libre.
  - h) Ningún grupo abeliano libre de rango  $> 1$  es libre.
  - i) Cualesquiera dos grupos libres son isomorfos.
  - j) Cualesquiera dos grupos abelianos libres del mismo rango son isomorfos.

\*21.9 Sea  $G$  un grupo abeliano finitamente generado con identidad 0. Un conjunto finito  $\{b_1, \dots, b_n\}$  donde  $b_i \in G$  es una **base para  $G$**  si  $\{b_1, \dots, b_n\}$  genera  $G$  y  $\sum_{i=1}^n m_i b_i = 0$  si y sólo si  $m_i b_i = 0$  donde  $m_i \in \mathbb{Z}$ .

- a) Muéstrese que  $\{2, 3\}$  no es una base para  $\mathbb{Z}_4$ . Encuéntrese una base para  $\mathbb{Z}_4$ .
  - b) Muéstrese que tanto  $\{1\}$  como  $\{2, 3\}$  son bases para  $\mathbb{Z}_6$ . (Esto muestra que puede variar el número de elementos en una base, para un grupo abeliano  $G$  finitamente generado con torsión; esto es, no por fuerza es un *invariante del grupo  $G$* .)
  - c) ¿Es una base de un grupo abeliano libre, según se definió en el capítulo 20, una base en el sentido en que se usó en este ejercicio?
  - d) Muéstrese que todo grupo abeliano finito tiene una base  $\{b_1, \dots, b_n\}$ , donde el orden de  $b_i$  divide al orden de  $b_{i+1}$ . Puede usarse cualquier teorema del libro, aunque no se haya demostrado.

Hoy día, en las exposiciones de álgebra, se usa con frecuencia (en particular por los discípulos de N. Bourbaki) la siguiente técnica para introducir un nuevo ente algebraico:

- 1 Describanse las propiedades algebraicas que poseerá ese ente algebraico.

- 2 Pruébense que cualesquiera dos entes algebraicos con estas propiedades son isomorfos, esto es, que estas propiedades caracterizan al ente.  
 3 Muéstrese que existe al menos uno de dichos entes.

*Los tres ejercicios siguientes ilustran esta técnica para tres entes algebraicos, los cuales son conocidos por el estudiante. Para no descubrir sus identidades, usamos nombres ficticios en los dos primeros ejercicios. La última parte de estos dos primeros ejercicios pide dar el nombre común del ente en cuestión.*

\*21.10 Sea  $G$  un grupo cualquiera. Un grupo abeliano  $G^*$  es un **grupo blip** de  $G$  si existe un homomorfismo fijo  $\phi$  de  $G$  sobre  $G^*$  tal que cada homomorfismo  $\psi$  de  $G$  en un grupo abeliano  $G'$  se puede factorizar como  $\psi = \phi\theta$  donde  $\theta$  es un homomorfismo de  $G^*$  en  $G'$  (véase la Fig. 21.1).

- Muéstrese que cualesquiera dos grupos blip de  $G$  son isomorfos. [Sugerencia: sean  $G_1^*$  y  $G_2^*$  dos grupos blip de  $G$ . Entonces, cada uno de los homomorfismos fijos  $\phi_1:G \rightarrow G_1^*$  y  $\phi_2:G \rightarrow G_2^*$  pueden factorizarse vía otro grupo blip, de acuerdo con la definición de un grupo blip; esto es,  $\phi_1 = \phi_2\theta_1$  y  $\phi_2 = \phi_1\theta_2$ . Muéstrese que  $\theta_1$  es un isomorfismo de  $G_2^*$  sobre  $G_1^*$ . Aplíquese el ejercicio 13.16.]
- Muéstrese que para todo grupo  $G$  existe un grupo blip  $G^*$  de  $G$ .
- ¿Cuál de los conceptos presentados antes corresponden a la idea de un grupo blip de  $G$ ?

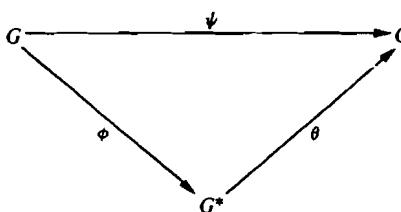


Figura 21.1

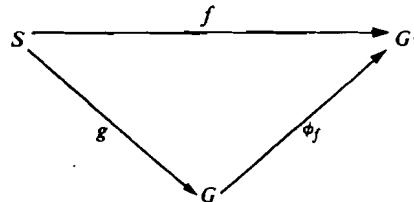


Figura 21.2

\*21.11 Sea  $S$  un conjunto cualquiera. Un grupo  $G$  junto con una función fija  $g:S \rightarrow G$  constituye un **grupo blop** en  $S$  si para cada grupo  $G'$  y transformación  $f:S \rightarrow G'$  existe un homomorfismo único  $\phi_f$  de  $G$  en  $G'$  tal que  $f = g\phi_f$  (véase la Fig. 21.2).

- Sea  $S$  un conjunto fijo. Muéstrese que si  $G_1$ , junto con  $g_1:S \rightarrow G_1$  y  $G_2$ , junto con  $g_2:S \rightarrow G_2$  son grupos blop en  $S$ , entonces  $G_1$  y  $G_2$  son isomorfos. [Sugerencia: muéstrese que  $g_1$  y  $g_2$  son transformaciones uno a uno y que  $Sg_1$  y  $Sg_2$  generan a  $G_1$  y a  $G_2$ , respectivamente. Procédase, después, de manera análoga a la sugerencia del ejercicio 21.10.]
- Sea  $S$  un conjunto. Muéstrese que existe un grupo blop en  $S$ . Puede usarse cualquier teorema del libro.
- ¿Cuál de los conceptos presentados antes corresponde a esta idea de grupo blop en  $S$ ?

\*21.12 Caracterícese, mediante propiedades, un grupo abeliano libre, de manera similar al ejercicio 21.11.

## \* 22

# Presentaciones de grupos

## \*22.1 DEFINICION

En este capítulo, de acuerdo con la mayor parte de la literatura acerca de presentaciones de grupos, hacemos que 1 sea la identidad de un grupo. La idea de *presentación de grupo* es formar un grupo dando un conjunto de generadores para el grupo y ciertas ecuaciones o relaciones que deseamos satisfagan los generadores. Se desea que el grupo sea tan libre como sea posible en los generadores sujetos a estas relaciones.

**Ejemplo 22.1** Supóngase que  $G$  tiene generadores  $x$  y  $y$ , y es *libre excepto por la relación*  $xy = yx$ , lo cual se puede expresar como  $xyx^{-1}y^{-1} = 1$ . Es claro que la condición  $xy = yx$  es precisamente la requerida para que  $G$  sea commutativo, aunque  $xyx^{-1}y^{-1}$  sea sólo uno de los muchos comutadores posibles de  $F[\{x, y\}]$ . Así,  $G$  es abeliano libre en dos generadores y es isomorfo a  $F[\{x, y\}]$  módulo su subgrupo commutador. Este subgrupo commutador de  $F[\{x, y\}]$  es el menor subgrupo normal que contiene  $xyx^{-1}y^{-1}$  puesto que cualquier subgrupo normal que contiene  $xyx^{-1}y^{-1}$  da lugar a un grupo factor abeliano, de modo que, por el teorema 12.6, contiene el subgrupo commutador. ■

El ejemplo anterior ilustra la situación general. Sea  $F[A]$  un grupo libre, supóngase que se desea formar un nuevo grupo lo más parecido posible a  $F[A]$ , sujeto a ciertas ecuaciones que se deben satisfacer. Cualquier ecuación se puede escribir de forma tal que el lado derecho sea 1. Así, podemos considerar las ecuaciones como  $r_i = 1$ , donde  $r_i \in F[A]$ . Claramente, si se requiere que  $r_i = 1$ , entonces se deberá tener que

$$x^{-1}(r_i^n)x = 1$$

para cualquier  $x \in F[A]$  y  $n \in \mathbb{Z}$ . Además, cualquier producto de elementos iguales a 1 será de nuevo igual a 1. Así, cualquier producto finito de la forma

$$\prod_j x_j^{-1}(r_{ij}^n)x_j,$$

donde las  $r_{ij}$  no por fuerza son distintas, tendrá que ser igual a 1 en el nuevo grupo. Es muy fácil corroborar que el conjunto de todos estos productos finitos es un subgrupo normal  $R$  de  $F[A]$ . Así, cualquier grupo que se parezca lo más posible a  $F[A]$ , sujeto a las condiciones  $r_i = 1$ , tendrá también  $r = 1$  para toda  $r \in R$ . Pero  $F[A]/R$  se parece a  $F[A]$  (recuérdese que multiplicamos clases laterales, escogiendo representantes) excepto en que  $R$  ha colapsado y formado la identidad 1. Así, el grupo que buscamos es (al menos isomorfo a)  $F[A]/R$ . Podemos ver este grupo como el descrito por el conjunto generador  $A$  y el conjunto  $\{r_i\}$ .

**Definición** Sea  $A$  un conjunto y sea  $\{r_i\} \subseteq F[A]$ . Sea  $R$  el menor de los subgrupos normales de  $F[A]$  que contiene las  $r_i$ . Una *presentación de G* es un isomorfismo  $\phi$  de  $F[A]/R$  sobre el grupo  $G$ . Los conjuntos  $A$  y  $\{r_i\}$  constituyen una *presentación de grupo*. El conjunto  $A$  es el conjunto de *generadores de la presentación* y cada  $r_i$  es un *conector*. Cada  $r \in R$  es una *consecuencia de*  $\{r_i\}$ . Una ecuación  $r_i = 1$  es una *relación*. Una *presentación finita* es aquella en donde  $A$  y  $\{r_i\}$  son, ambos, conjuntos finitos.

Esta definición puede parecer complicada, pero en realidad no lo es. En el ejemplo 22.1,  $\{x, y\}$  es el conjunto de generadores y  $xyx^{-1}y^{-1}$  es el único conector. La ecuación  $xyx^{-1}y^{-1} = 1$  o,  $xy = yx$  es una relación. Este era un ejemplo de una presentación finita.

Si una presentación de grupo tiene generadores  $x_j$  y conectores  $r_i$  usaremos las notaciones

$$(x_j : r_i) \quad \text{o} \quad (x_j : r_i = 1)$$

para denotar la presentación de grupo. Podemos referirnos a  $F[\{x_j\}]/R$  como al *grupo con presentación*  $(x_j : r_i)$ .

## \*22.2 PRESENTACIONES ISOMORFAS

**Ejemplo 22.2** Considérese la presentación de grupo con

$$A = \{a\} \quad \text{y} \quad \{r_i\} = \{a^6\},$$

esto es, la presentación

$$(a : a^6 = 1).$$

Este grupo, definido por un generador  $a$ , con la relación  $a^6 = 1$ , es claramente isomorfo a  $\mathbb{Z}_6$ .

Considérese ahora al grupo definido por dos generadores  $a$  y  $b$  con  $a^2 = 1$ ,  $b^3 = 1$  y  $ab = ba$ , esto es, el grupo con presentación

$$(a, b : a^2, b^3, aba^{-1}b^{-1}).$$

La condición  $a^2 = 1$  da  $a^{-1} = a$ . También,  $b^3 = 1$  da  $b^{-1} = b^2$ . Así, todo elemento en este grupo puede escribirse como un producto de potencias no negativas de  $a$  y  $b$ . La relación  $aba^{-1}b^{-1} = 1$ , esto es,  $ab = ba$ , nos permite escribir primero todos los factores con  $a$  y después los factores con  $b$ . De aquí que todo elemento del grupo es igual a algún  $a^n b^m$ . Pero,  $a^2 = 1$  y  $b^3 = 1$  muestran entonces que hay sólo seis elementos distintos

$$1, b, b^2, a, ab, ab^2.$$

Por tanto, esta presentación también da un grupo de orden 6 que es abeliano y, por el teorema 9.3, también debe ser cíclico e isomorfo a  $\mathbb{Z}_6$ . ■

El ejemplo anterior ilustra que presentaciones diferentes pueden dar grupos isomorfos. Cuando esto sucede tenemos **presentaciones isomórficas**. Puede ser muy difícil determinar si dos presentaciones son isomórficas. Se ha demostrado recientemente (véase Rabin [22]) que un buen número de dichos problemas relacionados con esta teoría no son, en general, solubles, esto es, no existe una *rutina* ni una manera bien definida para descubrir una solución en todos los casos. Estos problemas no solubles incluyen el problema de decidir cuándo dos presentaciones son isomórficas, cuándo un grupo dado por una presentación es finito, libre, abeliano o trivial, y el famoso *problema de la palabra*, que consiste en determinar en qué caso una palabra  $r$  dada es consecuencia de un conjunto dado de palabras  $\{r_i\}$ .

La importancia de este material se indica en el teorema 21.5, el cual garantiza que *todo grupo tiene una presentación*.

**Ejemplo 22.3** Mostremos que

$$(x, y : y^2x = y, yx^2y = x)$$

es una presentación del grupo trivial de un elemento. Sólo necesitamos probar que  $x$  y  $y$  son consecuencias de los conectores  $y^2xy^{-1}$  y  $yx^2yx^{-1}$ , o que  $x = 1$  y  $y = 1$  pueden deducirse de  $y^2x = y$  y  $yx^2y = x$ . Ilustramos ambas técnicas.

Como consecuencia de  $y^2xy^{-1}$  obtenemos  $yx$  después de conjugar por  $y$ . De  $yx$  deducimos  $x^{-1}y^{-1}$ , después  $(x^{-1}y^{-1})(yx^2yx^{-1})$  da  $xyx^{-1}$ . Conjugando  $xyx^{-1}$  por  $x$  obtenemos  $y$ . De  $y$  obtenemos  $y^{-1}$  y  $y^{-1}(yx)$  es  $x$ .

Trabajando con relaciones, en lugar de conectores, de  $y^2x = y$  deducimos  $yx = 1$  después de multiplicar por  $y^{-1}$  por la izquierda. Después, sustituyendo  $yx = 1$  en  $yx^2y = x$ , esto es,  $(yx)(xy) = x$ , obtenemos  $xy = x$ . Entonces,

multiplicando por  $x^{-1}$  por la izquierda, tenemos  $y = 1$ . Al sustituir esto en  $yx = 1$  obtenemos  $x = 1$ .

Ambas técnicas implican igual trabajo pero, de alguna manera, nos parece más natural a muchos de nosotros, trabajar con relaciones. ■

## \*22.3 APLICACIONES

Concluimos este capítulo con dos aplicaciones.

**Ejemplo 22.4** Determinemos todos los grupos de orden 10, salvo isomorfismo. Por el teorema 9.3, sabemos que todo grupo abeliano de orden 10 es isomorfo a  $\mathbb{Z}_{10}$ . Supóngase que  $G$  es no abeliano de orden 10. Por la teoría de Sylow,  $G$  contiene un subgrupo normal  $H$  de orden 5 y  $H$  debe ser cíclico. Sea  $a$  un generador de  $H$ . Entonces,  $G/H$  es de orden 2 y, por tanto, isomorfo a  $\mathbb{Z}_2$ . Si  $b \in G$  y  $b \notin H$  debemos tener que  $b^2 \in H$ . Como todo elemento de  $H$ , excepto el 1, tiene orden 5, entonces, si  $b^2$  no fuera igual a 1, tendría orden 5, de modo que  $b$  tendría orden 10. Esto significaría que  $G$  sería cíclico contradiciendo nuestra hipótesis de que  $G$  no es abeliano. Así,  $b^2 = 1$ . Por último, como  $H$  es un subgrupo normal de  $G$ ,  $bHb^{-1} = H$ , en particular,  $bab^{-1} \in H$ . Como la conjugación por  $b^{-1}$  es un automorfismo de  $H$ ,  $bab^{-1}$  debe ser otro elemento de  $H$  de orden 5, de aquí que  $bab^{-1}$  es igual a  $a$ ,  $a^2$ ,  $a^3$ , o  $a^4$ . Pero si  $bab^{-1} = a$  esto daría  $ba = ab$  y entonces, claramente,  $G$  sería abeliano, puesto que  $a$  y  $b$  generan  $G$ . Así, las posibilidades para presentaciones de  $G$  son:

- 1  $(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$ ,
- 2  $(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$ ,
- 3  $(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$ .

Nótese que las tres presentaciones pueden dar grupos de orden a lo más 10, ya que la última relación  $ba = a^4b$  nos permite expresar todo producto de las  $a$  y las  $b$  en  $G$  en la forma  $a^rb^t$ . Entonces,  $a^5 = 1$  y  $b^2 = 1$  muestran que el conjunto

$$S = \{a^0b^0, a^1b^0, a^2b^0, a^3b^0, a^4b^0, a^0b^1, a^1b^1, a^2b^1, a^3b^1, a^4b^1\}$$

incluye todos los elementos de  $G$ .

Sin embargo, no es claro que todos estos elementos en  $S$  son distintos, de modo que tengamos en los tres casos un grupo de orden 10. Por ejemplo, la presentación de grupo

$$(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$$

nos da un grupo en el cual, usando la ley asociativa, tenemos que

$$\begin{aligned} a &= b^2a = (bb)a = b(ba) = b(a^2b) = (ba)(ab) \\ &= (a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b^2 = a^4. \end{aligned}$$

Así, en este grupo  $a = a^4$ , de modo que  $a^3 = 1$ , lo cual, junto con  $a^5 = 1$ , da  $a^2 = 1$ . Pero  $a^2 = 1$  junto con  $a^3 = 1$  significa que  $a = 1$ . De aquí que todo elemento en el grupo con presentación

$$(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$$

es igual a 1 o a  $b$ , es decir, este grupo es isomorfo a  $\mathbb{Z}_2$ . Un estudio similar de

$$(bb)a = b(ba)$$

para

$$(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$$

muestra de nuevo que  $a = a^4$ , así que también produce un grupo isomorfo a  $\mathbb{Z}_2$ .

Queda solamente

$$(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$$

como candidato para grupo no abeliano de orden 10. En este caso, puede mostrarse que todos los elementos de  $S$  son distintos, así que esta presentación sí da un grupo  $G$  no abeliano de orden 10. ¿Cómo podemos mostrar que todos los elementos en  $S$  representan distintos elementos de  $G$ ? La manera fácil es observar que ya sabemos que hay al menos un grupo no abeliano de orden 10, el grupo diédrico  $D_5$ . Como  $G$  es el candidato que queda, debe cumplirse que  $G \simeq D_5$ . Otra manera es la siguiente: tratemos de convertir  $S$  en un grupo *definiendo*  $(a^x b^y)(a^u b^v)$  como  $a^x b^y$  donde  $x$  es el residuo de  $s + u(4)$  cuando se divide entre 5 y  $y$  es el residuo de  $t + v$  cuando se divide entre 2, en el sentido del lema 6.1. En otras palabras, usamos la relación  $ba = a^4b$  como guía para *definir* el producto  $(a^x b^y)(a^u b^v)$  de dos elementos de  $S$ . Es fácil ver que  $a^0 b^0$  actúa como identidad y que dado  $a^x b^y$  podemos determinar  $t$  y  $s$  sucesivamente haciendo

$$t \equiv -v \pmod{2}$$

y después

$$s \equiv -u(4) \pmod{5},$$

obteniendo  $a^x b^y$  que es un inverso izquierdo para  $a^u b^v$ . Tendremos una estructura de grupo en  $S$  si y sólo si se cumple la ley asociativa. En el ejercicio 22.7 pedimos realizar los cálculos para la ley asociativa y descubrir una condición para que  $S$  sea grupo bajo dicha definición de multiplicación. En este caso, el criterio del ejercicio equivale a la congruencia válida

$$4^2 \equiv 1 \pmod{5}.$$

Así, obtenemos un grupo de orden 10. Nótese que

$$2^2 \not\equiv 1 \pmod{5}$$

y

$$3^2 \not\equiv 1 \pmod{5},$$

de modo que el ejercicio 22.7 muestra además que

$$(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$$

y

$$(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$$

no dan grupos de orden 10. ■

**Ejemplo 22.5** Determinemos todos los grupos de orden 8, salvo isomorfismo. Conocemos los tres abelianos

$$\mathbf{Z}_8, \quad \mathbf{Z}_2 \times \mathbf{Z}_4, \quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Usando generadores y relaciones, daremos presentaciones de los grupos no abelianos.

Sea  $G$  no abeliano de orden 8. Como  $G$  es no abeliano, no tiene elementos de orden 8, así que cada elemento, excepto la identidad, es de orden 2 ó 4. Si todo elemento fuera de orden 2 entonces, para  $a, b \in G$  tendríamos que  $(ab)^2 = 1$ , esto es,  $abab = 1$ . Entonces, como también  $a^2 = 1$  y  $b^2 = 1$ , tendríamos

$$ba = a^2bab^2 = a(ab)^2b = ab,$$

contrario a la hipótesis de que  $G$  no es abeliano. Así,  $G$  tiene al menos un elemento de orden 4.

Sea  $\langle a \rangle$  el subgrupo de  $G$  de orden 4. Si  $b \notin \langle a \rangle$ , las clases laterales  $\langle a \rangle$  y  $b\langle a \rangle$  llenarían todo  $G$ . Por tanto,  $a$  y  $b$  son generadores de  $G$  y  $a^4 = 1$ . Como  $\langle a \rangle$  es normal en  $G$  (por la teoría de Sylow, o porque es de índice 2),  $G/\langle a \rangle$  es isomorfo a  $\mathbf{Z}_2$  y tenemos  $b^2 \in \langle a \rangle$ . Si  $b^2 = a$  o  $b^2 = a^3$ , entonces  $b$  sería de orden 8. Por tanto,  $b^2 = 1$  o  $b^2 = a^2$ . Por último, como  $\langle a \rangle$  es normal, tenemos  $bab^{-1} \in \langle a \rangle$  y como  $b\langle a \rangle b^{-1}$  es un subgrupo conjugado a  $\langle a \rangle$  y, por ende, isomorfo a  $\langle a \rangle$ , vemos que  $bab^{-1}$  debe ser un elemento de orden 4. Así,  $bab^{-1} = a$  o  $bab^{-1} = a^3$ . Si  $bab^{-1}$  fuera igual a  $a$ , entonces  $ba$  sería igual a  $ab$ , lo cual haría a  $G$  abeliano. En consecuencia,  $bab^{-1} = a^3$  de modo que  $ba = a^3b$ . Así, tenemos dos posibilidades para  $G$ , a saber,

$$G_1 : (a, b : a^4 = 1, b^2 = 1, ba = a^3b)$$

y

$$G_2 : (a, b : a^4 = 1, b^2 = a^2, ba = a^3b).$$

Nótese que  $a^{-1} = a^3$  y que  $b^{-1}$  es  $b$  en  $G_1$  y  $b^3$  en  $G_2$ . Estos hechos, junto con la relación  $ba = a^3b$  nos permiten expresar todo elemento en  $G_i$  en la forma

$a^m b^n$ , como en los ejemplos 22.2 y 22.4. Como  $a^4 = 1$  y  $b^2 = 1$  o  $b^2 = a^2$ , los elementos posibles en cada grupo son

$$1, a, a^2, a^3, b, ab, a^2b, a^3b.$$

Así,  $G_1$  y  $G_2$  tienen, cada uno, orden a lo más 8. Que  $G_1$  es un grupo de orden 8 puede verse a partir del ejercicio 22.7. Un argumento análogo al usado en el ejercicio 22.7, muestra que también  $G_2$  es de orden 8.

Como  $ba = a^3b \neq ab$ , vemos que  $G_1$  y  $G_2$  son no abelianos. Que los dos grupos no son isomorfos se sigue del hecho de que, mediante un cálculo, mostramos que  $G_1$  tiene sólo dos elementos de orden 4, a saber,  $a$  y  $a^3$ . Por otro lado, en  $G_2$  todos los elementos excepto el 1 y  $a^2$  son de orden 4. Se pedirá en el ejercicio 22.3 el cálculo de las tablas para estos grupos. Para ilustrar, supongamos que se desea calcular  $(a^2b)(a^3b)$ . Usando en forma repetida  $ba = a^3b$  obtenemos

$$(a^2b)(a^3b) = a^2(ba)a^2b = a^5(ba)ab = a^8(ba)b = a^{11}b^2.$$

Entonces, para  $G_1$  tenemos

$$a^{11}b^2 = a^{11} = a^3,$$

pero si estamos en  $G_2$ , obtenemos

$$a^{11}b^2 = a^{13} = a.$$

El grupo  $G_1$  es el **grupo octal** y no es más que nuestro viejo amigo, el grupo  $D_4$  de simetrías del cuadrado. El grupo  $G_2$  es el **grupo de cuaterniones**; la razón del nombre se explicará en la sección 25.4. ■

## Ejercicios

---

\*22.1 Dése una presentación de  $Z_4$  con un generador; con dos generadores; con tres generadores.

\*22.2 Dése una presentación de  $S_3$  que lleve tres generadores.

\*22.3 Dense las tablas del grupo octal

$$(a, b : a^4 = 1, b^2 = 1, ba = a^3b)$$

y del grupo de cuaterniones

$$(a, b : a^4 = 1, b^2 = a^2, ba = a^3b).$$

En ambos casos, escribanse los elementos en el orden 1,  $a, a^2, a^3, b, ab, a^2b, a^3b$ . ( Nótese que no es necesario calcular *todos* los productos. Ya se sabe que estas presentaciones dan grupos de orden 8 y apenas se calculen suficientes productos, el resto están forzados de manera que en cada renglón y en cada columna de la tabla aparezca cada elemento exactamente una vez.)

**\*22.4** ¿Falso o verdadero?

- a) Todo grupo tiene una presentación.
  - b) Todo grupo tiene varias presentaciones diferentes.
  - c) Todo grupo tiene dos presentaciones que no son isomorfas.
  - d) Todo grupo tiene una presentación finita.
  - e) Todo grupo con una presentación finita es de orden finito.
  - f) Todo grupo cíclico tiene una presentación con un solo generador.
  - g) Todo conjugado de un conector es consecuencia del conector.
  - h) Dos presentaciones con el mismo número de generadores siempre son isomórficas.
  - i) En una presentación de un grupo abeliano, el conjunto de consecuencias de los conectores contiene al subgrupo comutador del grupo libre en los generadores.
  - j) Toda presentación de un grupo libre tiene a 1 como único conector.
- 

**\*22.5** Muéstrese que

$$(a, b : a^3 = 1, b^2 = 1, ba = a^2b)$$

da un grupo de orden 6. Pruébese que no es abeliano.

**\*22.6** Muéstrese que la presentación

$$(a, b : a^3 = 1, b^2 = 1, ba = a^2b)$$

del ejercicio 22.5 da al único (salvo isomorfismo) grupo no abeliano de orden 6 y, por tanto, da un grupo isomorfo a  $S_3$ .

**\*22.7** Sea

$$S = \{a^i b^j \mid 0 \leq i < m, 0 \leq j < n\},$$

esto es,  $S$  consta de todos los productos formales  $a^i b^j$  comenzando con  $a^0 b^0$  y terminando con  $a^{m-1} b^{n-1}$ . Sea  $r$  un entero positivo, definase la multiplicación en  $S$  por

$$(a^i b^j)(a^k b^l) = a^{x} b^y,$$

donde  $x$  es el residuo de  $i + l(r^t)$  al dividirlo entre  $m$ , y  $y$  es el residuo de  $j + k(r^t)$  al dividirlo entre  $n$ , en el sentido del lema 6.1.

- Muéstrese que una condición necesaria y suficiente para que valga la ley asociativa en  $S$  y sea grupo bajo esta multiplicación, es que  $r^t \equiv 1 \pmod{m}$ .
- Dedúzcase de la parte a) que la presentación de grupo

$$(a, b : a^m = 1, b^n = 1, ba = a^r b)$$

da un grupo de orden  $mn$ , si y sólo si  $r^t \equiv 1 \pmod{m}$ .

**\*22.8** Determiníense, salvo isomorfismo, todos los grupos de orden 14. [Sugerencia: sigase el esbozo del ejemplo 22.4 y úsese el ejercicio 22.7, parte b).]

**\*22.9** Determiníense, salvo isomorfismo, todos los grupos de orden 21. [Sugerencia: sigase el esbozo del ejemplo 22.4 y úsese el ejercicio 22.7 parte b). Puede parecer que hay dos presentaciones que dan grupos no abelianos. Muéstrese que son isomórficos.]

\*22.10 Muéstrese que si  $n = pq$  con  $p$  y  $q$  primos,  $q > p$  y  $q \equiv 1 \pmod{p}$ , entonces hay exactamente un (salvo isomorfismo) grupo no abeliano de orden  $n$ . Supóngase (como se probará más adelante) que los  $q - 1$  elementos distintos de cero de  $\mathbb{Z}_q$  forman un grupo cíclico  $\mathbb{Z}_q^*$  bajo la multiplicación módulo  $q$ . [Sugerencia: las soluciones de  $x^p \equiv 1 \pmod{q}$  forman un subgrupo cíclico de  $\mathbb{Z}_q^*$  con elementos  $1, r, r^2, \dots, r^{p-1}$ . En el grupo con presentación  $(a, b : a^q = 1, b^p = 1, ba = a'b)$  tenemos  $bab^{-1} = a'$  de modo que  $b^j ab^{-j} = a^{(r^j)}$ . Así, como  $b^j$  genera  $\langle b \rangle$  para  $j = 1, \dots, p - 1$ , esta presentación es isomorfa a

$$(a, b^j : a^q = 1, (b^j)^p = 1, (b^j)a = a^{(r^j)}(b^j)),$$

de modo que todas las presentaciones  $(a, b : a^q = 1, b^p = 1, ba = a^{(r^j)}b)$  son isomorfas.]

\*22.11 Determínense todos los grupos de orden 12 (salvo isomorfismo).

\*22.12 Determínense todos los grupos de orden 30 (salvo isomorfismo).



**PARTE**

**III**

# **ANILLOS Y CAMPOS**

## Anillos

### 23.1 DEFINICION Y PROPIEDADES BASICAS

Hasta aquí, hemos trabajado con conjuntos en los cuales se ha definido una sola operación binaria. Los ejemplos conocidos de conjuntos de números muestran que debe ser muy importante el estudio de conjuntos, en los que se hayan definido dos operaciones binarias. El sistema más general de este tipo que estudiaremos aquí, es el de anillo.

**Definición** Un **anillo**  $\langle R, +, \cdot \rangle$  es un conjunto  $R$  junto con dos operaciones binarias  $+$  y  $\cdot$ , que llamamos suma y multiplicación, definidas en  $R$  tales que se satisfacen los siguientes axiomas:

- $\mathcal{R}_1$   $\langle R, + \rangle$  es un grupo abeliano.
- $\mathcal{R}_2$  La multiplicación es asociativa.
- $\mathcal{R}_3$  Para todas las  $a, b, c \in R$ , se cumple la **ley distributiva izquierda**  $a(b + c) = (ab) + (ac)$  y la **ley distributiva derecha**  $(a + b)c = (ac) + (bc)$ .

**Ejemplo 23.1** Hay que estar conscientes de que los axiomas  $\mathcal{R}_1$ ,  $\mathcal{R}_2$  y  $\mathcal{R}_3$  para un anillo, se cumplen en cualquier subconjunto de números complejos que sea grupo bajo la suma y sea cerrado bajo la multiplicación. Por ejemplo,  $\langle \mathbb{Z}, +, \cdot \rangle$ ,  $\langle \mathbb{Q}, +, \cdot \rangle$ ,  $\langle \mathbb{R}, +, \cdot \rangle$  y  $\langle \mathbb{C}, +, \cdot \rangle$  son anillos. ■

Respetaremos la convención usual de efectuar la multiplicación antes que la suma, así, la ley distributiva izquierda, por ejemplo, se presenta como

$$a(b + c) = ab + ac,$$

sin paréntesis en el lado derecho de la ecuación. Además, debido a una convención semejante a nuestra notación en teoría de grupos, nos referiremos, de manera algo incorrecta, a *un anillo R*, en lugar de a *un anillo <R, +, ·>* siempre que no haya confusión. En particular, de ahora en adelante,  $\mathbf{Z}$  será  $\langle \mathbf{Z}, +, \cdot \rangle$  y  $\mathbf{Q}, \mathbf{R}$  y  $\mathbf{C}$  serán, también, los anillos obvios. Si es necesario, nos referiremos a  $\langle R, + \rangle$  como el *grupo aditivo del anillo R*.

**Ejemplo 23.2** Considérese el grupo cíclico  $\langle \mathbf{Z}_n, + \rangle$ . Si definimos para  $a, b \in \mathbf{Z}_n$  el producto  $ab$  como el residuo del producto usual de enteros cuando se dividen entre  $n$ , se puede mostrar que  $\langle \mathbf{Z}_n, +, \cdot \rangle$  es un anillo. Usaremos este hecho con toda libertad. Por ejemplo, en  $\mathbf{Z}_{10}$  tenemos  $(3)(7) = 1$ . Esta operación en  $\mathbf{Z}_n$  es la **multiplicación módulo n**. No verificaremos que se cumplen aquí los axiomas de anillo, pues son consecuencia directa de parte de la teoría que de todos modos tenemos que desarrollar. ■

A partir de ahora,  $\mathbf{Z}_n$  será siempre  $\langle \mathbf{Z}_n, +, \cdot \rangle$ . Siguiendo con asuntos de notación, 0 será siempre la identidad aditiva de un anillo. El inverso aditivo de un elemento  $a$  de un anillo es  $-a$ . Con frecuencia nos referiremos a la suma

$$a + a + \cdots + a$$

con  $n$  sumandos. Esta suma será denotada por  $n \cdot a$ . Sin embargo,  $n \cdot a$  no debe interpretarse como multiplicación de  $n$  por  $a$  en el anillo, pues el entero  $n$  puede no estar en el anillo. Si  $n < 0$ , sea

$$n \cdot a = (-a) + (-a) + \cdots + (-a)$$

para  $|n|$  sumandos. Por último, definimos

$$0 \cdot a = 0$$

para  $0 \in \mathbf{Z}$  en el lado izquierdo de la ecuación y  $0 \in R$  en el lado derecho. En realidad, la ecuación  $0a = 0$  vale también para  $0 \in R$  en ambos lados. El teorema siguiente prueba éste y otros hechos fáciles pero importantes. Nótese el uso frecuente de las leyes distributivas en la demostración de este teorema. *Estas leyes distributivas son el único medio disponible para relacionar, en un anillo, los conceptos aditivos con los multiplicativos.*

**Teorema 23.1** *Si R es un anillo con identidad aditiva 0 entonces, para cualquier  $a, b \in R$ , tenemos*

- 1  $0a = a0 = 0$ ,
- 2  $a(-b) = (-a)b = -(ab)$ ,
- 3  $(-a)(-b) = ab$ .

*Demostración* Para la condición 1, nótese que

$$a0 = a(0 + 0) = a0 + a0.$$

Entonces, por la ley de cancelación para el grupo aditivo  $\langle R, + \rangle$  tenemos  $0 = a0$ . Así mismo,

$$0a = (0 + 0)a = 0a + 0a$$

implica que  $0a = 0$ . Esto prueba la condición 1.

Para entender la demostración de la condición 2, hay que recordar que, por definición,  $-(ab)$  es el elemento que, sumado a  $ab$ , da 0. Así, para mostrar que  $a(-b) = -(ab)$ , debe mostrarse precisamente que  $a(-b) + ab = 0$ . Por la ley distributiva izquierda,

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

pues, por la condición 1,  $a0 = 0$ . Así mismo,

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

Para la condición 3, nótese que, por la condición 2,

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

De nuevo, por la condición 2,

$$-(a(-b)) = -(-(ab)),$$

y  $-(-(ab))$  es el elemento que, sumado a  $-(ab)$ , da 0. Este es  $ab$  por definición de  $-(ab)$  y por la unicidad de un inverso en un grupo. Así,  $(-a)(-b) = ab$ . ■

Es importante comprender la demostración anterior. Si no se puede seguir la lógica y uso de las definiciones, más adelante habrá dificultades. (Quizá ya tengan dificultades.) El teorema permite usar las reglas conocidas para los signos.

Esperamos que se empiece a comprender que, en el estudio de cualquier tipo de estructura matemática, una idea de importancia básica es el concepto de que dos sistemas que son estructuralmente idénticos, esto es, que uno sea exactamente como el otro, excepto por los nombres. En álgebra, siempre se llama a este concepto *isomorfismo*. El concepto de que dos anillos sean el mismo, excepto por el nombre de los elementos, nos conduce, como en el caso de los grupos, a la siguiente definición.

**Definición** Un *isomorfismo*  $\phi$  de un anillo  $R$  con un anillo  $R'$  es una función uno a uno que transforma  $R$  sobre  $R'$  tal que para todas las  $a, b \in R$ ,

- 1  $(a + b)\phi = a\phi + b\phi$ ,
- 2  $(ab)\phi = (a\phi)(b\phi)$ .

Entonces, los anillos  $R$  y  $R'$  son *isomorfos*.

**Ejemplo 23.3** Como los grupos abelianos,  $\langle \mathbb{Z}, + \rangle$  y  $\langle 2\mathbb{Z}, + \rangle$  son isomorfos bajo la transformación  $\phi: \mathbb{Z} \rightarrow 2\mathbb{Z}$  con  $x\phi = 2x$  para  $x \in \mathbb{Z}$ . Nótese que  $2\mathbb{Z}$  es cerrado bajo la multiplicación usual y que  $\langle 2\mathbb{Z}, +, \cdot \rangle$  es un anillo. Aquí,  $\phi$  no es un isomorfismo de anillo, pues  $(xy)\phi = 2xy$  mientras que  $(x\phi)(y\phi) = 2x2y = 4xy$ . ■

A partir de ahora,  $n\mathbb{Z}$  será siempre el anillo  $\langle n\mathbb{Z}, +, \cdot \rangle$ .

## 23.2 CUESTIONES MULTIPLICATIVAS; CAMPOS

Todos los anillos que hemos visto hasta ahora tienen una multiplicación que es conmutativa. Muchos de ellos, como  $\mathbb{Z}$ ,  $\mathbb{Q}$  y  $\mathbb{R}$  tienen, además, identidad multiplicativa 1. Sin embargo,  $2\mathbb{Z}$  no tiene elemento identidad para la multiplicación. Hay muchos anillos en los cuales la multiplicación no es conmutativa. El estudiante que conozca un poco de teoría de matrices, verá que las matrices  $n \times n$  cuyos registros son elementos de  $\mathbb{Z}$  (o  $\mathbb{Q}$ ,  $\mathbb{R}$  o  $\mathbb{C}$ ) forman un anillo bajo la suma y multiplicación de matrices, donde la multiplicación no es conmutativa si  $n \geq 2$ . Estos anillos de matrices sí tienen un elemento identidad para la multiplicación. Los trataremos con mayor detalle en el capítulo 25.

Es evidente que  $\{0\}$  con  $0 + 0 = 0$  y  $(0)(0) = 0$  da un anillo. Aquí, 0 actúa como identidad multiplicativa y como identidad aditiva. Por el teorema 23.1, éste es el único caso en que 0 puede actuar como identidad multiplicativa, pues si  $0a = a$  podemos deducir que  $a = 0$ . Cada vez que hablamos de una identidad multiplicativa en un anillo, excluiremos este caso trivial, esto es, cuando hablamos de una identidad multiplicativa, supondremos que es distinta de cero.

**Definición** Un anillo en donde la multiplicación es conmutativa es un **anillo conmutativo**. Un anillo  $R$  con identidad multiplicativa 1 tal que  $1x = x1 = x$  para todas las  $x \in R$  es un **anillo con unitario**. Una identidad multiplicativa en un anillo es un **elemento unitario**.

**Teorema 23.2** Si  $R$  es un anillo con unitario, entonces este elemento unitario 1 es la única identidad multiplicativa.

**Demostración** Procedemos exactamente como lo hicimos para grupos. Sean 1 y  $1'$  identidades multiplicativas en un anillo  $R$  y dejemos que compitan. Considerando el 1 como identidad tenemos

$$(1)(1') = 1'.$$

Considerando el  $1'$  como la identidad tenemos

$$(1)(1') = 1.$$

Así,  $1 = 1'$ . ■

Si  $R_1, R_2, \dots, R_n$  son anillos, podemos formar el conjunto  $R_1 \times R_2 \times \dots \times R_n$  de todas las  $n$ -adas ordenadas  $(r_1, r_2, \dots, r_n)$  donde  $r_i \in R_i$ . Si definimos la suma y la multiplicación de  $n$ -adas por componentes (como para grupos) veremos en seguida, a partir de los axiomas de anillo en cada componente, que el conjunto de todas estas  $n$ -adas forman un anillo bajo la suma y la multiplicación por componentes. El anillo  $R_1 \times R_2 \times \dots \times R_n$  es el **producto directo** de los anillos  $R_i$ . Es claro que dicho producto directo es conmutativo o tiene elemento unitario si y sólo si cada  $R_i$  es conmutativo o tiene elemento unitario, respectivamente.

En un anillo  $R$  con unitario, el conjunto  $R^*$  de elementos distintos de cero será un grupo multiplicativo si es cerrado bajo la multiplicación del anillo y si existen inversos. Un **inverso multiplicativo** de un elemento  $a$  en un anillo  $R$  con unitario 1 es un elemento  $a^{-1} \in R$  tal que  $aa^{-1} = a^{-1}a = 1$ . Así como para grupos, el inverso multiplicativo de un elemento  $a$  en  $R$  es único si es que existe (véase el ejercicio 23.12). El teorema 23.1 muestra que no tendría sentido tener un inverso multiplicativo para el 0, a menos que se deseé considerar el conjunto  $\{0\}$  donde  $0 + 0 = 0$  y  $(0)(0) = 0$  como un anillo, con 0 como identidad aditiva y multiplicativa. Ya acordamos excluir este caso trivial cuando hablemos de anillos con unitario. Así, tenemos que analizar la existencia de inversos multiplicativos para elementos distintos de cero en un anillo con unitario. Quizás estén cansados de tantas definiciones, pero no queda más remedio.

**Definición** Sea  $R$  un anillo con unitario. Un elemento  $u$  en  $R$  es una **unidad de  $R$**  si tiene un inverso multiplicativo en  $R$ . Si todo elemento distinto de cero en  $R$  es una unidad, entonces  $R$  es un **semi campo** o **anillo con división**. Un **campo** es un anillo conmutativo con división.

**Ejemplo 23.4**  $\mathbf{Z}$  no es un campo pues, por ejemplo, el 2 no tiene inverso multiplicativo, de modo que el 2 no es una unidad en  $\mathbf{Z}$ . Las únicas unidades en  $\mathbf{Z}$  son 1 y  $-1$ . Claramente,  $\mathbf{Q}$  y  $\mathbf{R}$  son campos. ■

Existen, de manera natural, los conceptos de subanillo de un anillo y subcampo de un campo. Un **subanillo de un anillo** es un subconjunto del anillo que es anillo bajo las operaciones inducidas de todo el anillo; un **subcampo** se define de modo análogo para un subconjunto de un campo. De hecho, digamos de una vez que, si tenemos un conjunto, junto con cierto tipo específico de estructura algebraica en el conjunto, llamamos **glob** a esta conglomeración (grupo, anillo, campo, dominio entero, espacio vectorial, y demás), entonces cualquier subconjunto de este conjunto, tal que la estructura algebraica inducida de manera natural, que *produce una estructura algebraica del mismo tipo*, es un **subglob**. Si  $K$  y  $L$  son globos, denotaremos por  $K \leq L$  que  $K$  es un subglob de  $L$ , y  $K < L$  denotará que  $K \leq L$  pero que  $K \neq L$ .

Por último, queremos advertir que no debe confundirse el uso de las palabras **unidad** y **unitario**. Unitario es la identidad multiplicativa, mientras que unidad es cualquier elemento que tiene un inverso multiplicativo. Así, la identidad multiplicativa o unitario, es una unidad, pero no toda unidad es unitario. Por ejemplo,  $-1$  es una unidad en  $\mathbf{Z}$  pero  $-1$  no es unitario, esto es,  $-1 \neq 1$ .

**Ejercicios**

**23.1** Digase para cuáles de los siguientes conjuntos las operaciones indicadas de suma y multiplicación están definidas (el conjunto es cerrado) y dan estructura de anillo. Si el anillo no se forma, explíquese por qué.

- $n\mathbb{Z}$  con la suma y multiplicación usuales
- $\mathbb{Z}^+$  con la suma y multiplicación usuales
- $\mathbb{Z} \times \mathbb{Z}$  con la suma y multiplicación por componentes
- $2\mathbb{Z} \times \mathbb{Z}$  con la suma y multiplicación por componentes
- $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$  con la suma y multiplicación usuales
- $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  con la suma y multiplicación usuales
- El conjunto de todos los números complejos imaginarios puros  $ri$  para  $r \in \mathbb{R}$  con la suma y multiplicación usuales

**23.2** En cada parte del ejercicio 23.1 en que se forme un anillo, dígase si el anillo es conmutativo, si tiene unitario y si es un campo.

**23.3** Describanse todas las unidades de cada uno de los siguientes anillos.

- |   |                                   |
|---|-----------------------------------|
| a) $\mathbb{Z}$                                     | b) $\mathbb{Z} \times \mathbb{Z}$ |
| c) $\mathbb{Z}_3$                                   | d) $\mathbb{Q}$                   |
| e) $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ | f) $\mathbb{Z}_4$                 |

**†23.4** Muéstrese que si  $U$  es la colección de todas las unidades en un anillo  $\langle R, +, \cdot \rangle$  con unitario, entonces  $\langle U, \cdot \rangle$  es grupo. [Advertencia: asegúrese que  $U$  es cerrado bajo la multiplicación.]

**23.5** Muéstrese que  $a^2 - b^2 = (a + b)(a - b)$  para todas las  $a$  y  $b$  en un anillo  $R$  si y sólo si  $R$  es conmutativo.

**23.6** ¿Falso o verdadero?

- a) Todo campo también es anillo.
- b) Todo anillo tiene identidad multiplicativa.
- c) Todo anillo con unitario tiene al menos dos unidades.
- d) Todo anillo con unitario tiene a lo más dos unidades.
- e) Es posible que un subconjunto de algún campo sea anillo pero no un subcampo, bajo las operaciones inducidas.
- f) Las leyes distributivas para un anillo no son muy importantes.
- g) En un campo, la multiplicación es conmutativa.
- h) Los elementos distintos de cero de un campo forman grupo bajo la multiplicación del campo.
- i) En todo anillo, la suma es conmutativa.
- j) Todo elemento de un anillo tiene inverso aditivo.

**23.7** Sea  $(R, +)$  un grupo abeliano. Muéstrese que  $(R, +, \cdot)$  es un anillo si definimos  $ab = 0$  para todas las  $a, b \in R$ .

**23.8** Muéstrese que los anillos  $2\mathbb{Z}$  y  $3\mathbb{Z}$  no son isomorfos. Muéstrese que los campos  $\mathbb{R}$  y  $\mathbb{C}$  no son isomorfos.

**23.9** (Exponenciación estudiantil.) Sea  $p$  un primo. Muéstrese que en el anillo  $\mathbb{Z}_p$  se tiene  $(a + b)^p = a^p + b^p$  para todos los  $a, b \in \mathbb{Z}_p$ . [Sugerencia: obsérvese que la expansión binomial usual para  $(a + b)^p$  es válida en un anillo conmutativo.]

**23.10** Dese un ejemplo de un anillo unitario  $1$  que tenga un subanillo unitario  $1' \neq 1$ .

23.11 Muéstrese que el elemento unitario en un subcampo de un campo debe ser el unitario de todo el campo, en contraste con el ejercicio 23.10 para anillos.

23.12 Muéstrese que el inverso multiplicativo de una unidad en un anillo con unitario es única.

23.13 Un elemento  $a$  de un anillo  $R$  es **nilpotente** si  $a^n = 0$  para algún  $n \in \mathbb{Z}^+$ . Muéstrese que si  $a$  y  $b$  son elementos nilpotentes de un anillo *comunitativo*, entonces  $a + b$  también es nilpotente.

23.14 Muéstrese que un anillo  $R$  no tiene elementos nilpotentes distintos de cero si y sólo si 0 es la única solución de  $x^2 = 0$  en  $R$ .

23.15 Muéstrese que un subconjunto  $S$  de un anillo  $R$  da un subanillo de  $R$  si y sólo si es válido lo siguiente:

$$0 \in S;$$

$$(a - b) \in S \text{ para todas las } a, b \in S;$$

$$ab \in S \text{ para todas las } a, b \in S.$$

23.16 a) Muéstrese que una intersección de subanillos de un anillo  $R$  es, de nuevo, un subanillo de  $R$ .

b) Muéstrese que la intersección de subcampos de un campo  $F$  es, de nuevo, un subcampo de  $F$ .

23.17 Sea  $R$  un anillo y sea  $a$  un elemento fijo de  $R$ . Sea  $I_a = \{x \in R \mid ax = 0\}$ . Muéstrese que  $I_a$  es un subanillo de  $R$ .

23.18 Sea  $R$  un anillo y sea  $a$  un elemento fijo de  $R$ . Sea  $R_a$  el subanillo de  $R$  que es la intersección de todos los subanillos de  $R$  que contienen  $a$  (véase el ejercicio 23.16). El anillo  $R_a$  es el **subanillo de  $R$  generado por  $a$** . Muéstrese que el grupo abeliano  $\langle R_a, + \rangle$  está generado (en el sentido del capítulo 9) por  $\{a^n \mid n \in \mathbb{Z}^+\}$ .

23.19 Considérese  $\langle S, +, \cdot \rangle$  donde  $S$  es un conjunto y  $+$  y  $\cdot$  son operaciones binarias en  $S$  tales que

$\langle S, + \rangle$  es un grupo,

$\langle S^*, \cdot \rangle$  es un grupo, donde  $S^*$  está formado por todos los elementos de  $S$  excepto la identidad aditiva,

$$a(b + c) = (ab) + (ac) \text{ y } (a + b)c = (ac) + (bc) \text{ para todas las } a, b, c \in S.$$

Muéstrese que  $\langle S, +, \cdot \rangle$  es un anillo de división. [Sugerencia: aplíquense las leyes distributivas a  $(1 + 1)(a + b)$  para probar la comutatividad de la suma.]

23.20 Un anillo  $R$  es un **anillo booleano** si  $a^2 = a$  para todas las  $a \in R$ . Muéstrese que todo anillo booleano es comunitativo.

23.21 (Para estudiantes que tengan algún conocimiento sobre las leyes de la teoría de conjuntos.) Para un conjunto  $S$  sea  $\mathcal{P}(S)$  la colección de todos los subconjuntos de  $S$ . Defínanse las operaciones binarias  $+$  y  $\cdot$  en  $\mathcal{P}(S)$  por

$$A + B = (A \cup B) - (A \cap B) = \{x \mid x \in A \text{ o } x \in B, \text{ pero } x \notin (A \cap B)\}$$

y

$$A \cdot B = A \cap B$$

para  $A, B \in \mathcal{P}(S)$ .

a) Dense las tablas para  $+$  y  $\cdot$  en  $\mathcal{P}(S)$  donde  $S = \{a, b\}$ . [Sugerencia:  $\mathcal{P}(S)$  tiene cuatro elementos.]

b) Muéstrese que para cualquier conjunto  $S$ ,  $\langle \mathcal{P}(S), +, \cdot \rangle$  es un anillo booleano (véase el ejercicio 23.20).

## 24

# Dominios enteros

En esta sección, para motivar su estudio, usaremos polinomios de manera intuitiva. Será hasta el capítulo 30 cuando se traten con detalle.

## 24.1 DIVISORES DE 0 Y CANCELACION

Una de las propiedades algebraicas más importantes de nuestro sistema numérico usual es que el producto de dos números puede ser 0 sólo si al menos uno de los dos factores es cero. Se suele usar con frecuencia este hecho, incluso de manera inconsciente. Supóngase, por ejemplo, que se pide resolver la ecuación

$$x^2 - 5x + 6 = 0.$$

Lo primero que se hace es factorizar el lado izquierdo:

$$x^2 - 5x + 6 = (x - 2)(x - 3).$$

Después se concluye que los únicos valores posibles para  $x$  son 2 y 3. ¿Por qué? Porque si  $x$  se reemplaza por cualquier número  $a$ , el producto  $(a - 2)(a - 3)$  de los números resultantes es 0, si y sólo si  $a - 2 = 0$  o  $a - 3 = 0$ .

**Ejemplo 24.1** Resolvamos la ecuación  $x^2 - 5x + 6 = 0$  en  $\mathbf{Z}_{12}$ . Ahora,  $x^2 - 5x + 6 = (x - 2)(x - 3)$  sigue siendo válido si consideramos  $x$  como un número en  $\mathbf{Z}_{12}$ . Pero en  $\mathbf{Z}_{12}$  no sólo  $0a = a0 = 0$  para todas las  $a \in \mathbf{Z}_{12}$ , sino además,

$$\begin{aligned} (2)(6) &= (6)(2) = (3)(4) = (4)(3) = (3)(8) = (8)(3) \\ &= (4)(6) = (6)(4) = (4)(9) = (9)(4) = (6)(6) = (6)(8) \\ &= (8)(6) = (6)(10) = (10)(6) = (8)(9) = (9)(8) = 0. \end{aligned}$$

Así, nuestra ecuación no tiene sólo las soluciones 2 y 3, sino también 6 y 11 pues  $(6 - 2)(6 - 3) = (4)(3) = 0$  y  $(11 - 2)(11 - 3) = (9)(8) = 0$  en  $\mathbf{Z}_{12}$ . ■

Estas ideas son tan importantes que las formalizaremos en una definición.

**Definición** Si  $a$  y  $b$  son dos elementos distintos de cero de un anillo  $R$  tal que  $ab = 0$ , entonces  $a$  y  $b$  son *divisores de 0*. En particular,  $a$  es un *divisor izquierdo de 0* y  $b$  es un *divisor derecho de 0*.

En un anillo commutativo, todo divisor izquierdo de 0 es también un divisor derecho de 0 y reciprocamente. Así, no hay distinción entre divisores izquierdo y derecho de cero en un anillo commutativo.

El ejemplo 24.1 muestra que en  $\mathbf{Z}_{12}$  los elementos 2, 3, 4, 6, 8, 9 y 10 son todos divisores de 0. Nótese que estos son precisamente los números en  $\mathbf{Z}_{12}$  que no son primos relativos con 12, esto es, aquéllos cuyo mcd con 12 no es 1. Nuestro siguiente teorema muestra que éste es un ejemplo de una situación general.

**Teorema 24.1** *En el anillo  $\mathbf{Z}_n$  los divisores de 0 son precisamente aquellos elementos que no son primos relativos con  $n$ .*

**Demostración** Sea  $m \in \mathbf{Z}_n$ , donde  $m \neq 0$ , y sea  $d \neq 1$  el mcd de  $m$  y  $n$ . Entonces,

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n.$$

y  $(m/d)n$  da 0 como múltiplo de  $n$ . Así,  $m(n/d) = 0$  en  $\mathbf{Z}_n$ , mientras que ni  $m$  ni  $n/d$  es 0, así que  $m$  es un divisor de 0.

Por otro lado, supóngase que  $m \in \mathbf{Z}_n$  es primo relativo con  $n$ . Si para  $s \in \mathbf{Z}_n$  tenemos  $ms = 0$ , entonces  $n$  divide al producto  $ms$  de  $m$  y  $s$  como elementos del anillo  $\mathbf{Z}$ . Como  $n$  no tiene factores  $> 1$  en común con  $m$ , debe ser que  $n$  divide a  $s$ , de modo que  $s = 0$  en  $\mathbf{Z}_n$ . ■

**Corolario** *Si  $p$  es primo, entonces  $\mathbf{Z}_p$  no tiene divisores de 0.*

**Demostración** La demostración de este corolario resulta de inmediato del teorema 24.1. ■

Otra indicación de la importancia del concepto de divisores de 0 se muestra en el siguiente teorema. Sea  $R$  un anillo y sean  $a, b, c \in R$ . Las leyes de cancelación valen en  $R$  si  $ab = ac$  con  $a \neq 0$ , implica  $b = c$  y  $ba = ca$  con  $a \neq 0$  implica  $b = c$ . Estas son las leyes de cancelación multiplicativas. Es claro que las leyes de cancelación aditiva valen en  $R$ , pues  $\langle R, + \rangle$  es grupo.

**Teorema 24.2** *Las leyes de cancelación valen en  $R$  si y sólo si  $R$  no tiene divisores de 0, izquierdos ni derechos.*

*Demostración* Sea  $R$  un anillo en el cual se cumplen las leyes de cancelación, supóngase que  $ab = 0$  para algunas  $a, b \in R$ . Debemos mostrar que  $a$  es cero o  $b$  es 0. Si  $a \neq 0$ , entonces  $ab = a0$  implica que  $b = 0$ , por las leyes de cancelación. Análogamente,  $b \neq 0$  implica que  $a = 0$ , de modo que no puede haber divisores izquierdos ni derechos de 0, si las leyes de cancelación se cumplen.

Recíprocamente, supóngase que  $R$  no tiene divisores izquierdos ni derechos de 0 y supóngase que  $ab = ac$  con  $a \neq 0$ . Entonces,

$$ab - ac = a(b - c) = 0.$$

Como  $a \neq 0$  y  $R$  no tiene divisores izquierdos de 0, debemos tener  $b - c = 0$ , de modo que  $b = c$ . Un argumento similar muestra que  $ba = ca$ , con  $a \neq 0$ , implica  $b = c$ . ■

Supóngase que  $R$  es un anillo sin divisores de 0. Entonces, la ecuación  $ax = b$  con  $a \neq 0$  en  $R$ , puede tener a lo más una solución  $x$  en  $R$ , pues si  $ax_1 = b$  y  $ax_2 = b$ , entonces  $ax_1 = ax_2$  y, por el teorema 24.2,  $x_1 = x_2$ , pues  $R$  no tiene divisores de 0. Si  $R$  tiene elemento unitario 1 y  $a$  es una unidad en  $R$  con inverso multiplicativo  $a^{-1}$ , entonces, es claro que la solución  $x$  de  $ax = b$  es  $a^{-1}b$ . En el caso de que  $R$  sea comutativo, en particular, si  $R$  es un campo, se acostumbra denotar a  $a^{-1}b$  y  $ba^{-1}$  (por comutatividad son iguales) por el cociente formal  $b/a$ . Esta notación de cociente no debe usarse en el caso de que  $R$  no sea comutativo, pues no se sabría si  $b/a$  denota al elemento  $a^{-1}b$  o al elemento  $ba^{-1}$ . En un campo  $F$  es usual definir un cociente  $b/a$ , donde  $a \neq 0$ , como la solución  $x$  en  $F$  de la ecuación  $ax = b$ . Esta definición es consistente con nuestras observaciones anteriores y usaremos esta notación cociente cuando trabajemos en un campo. En particular, el inverso multiplicativo de un elemento  $a$  distinto de cero, en un campo es  $1/a$ .

## 24.2 DOMINIOS ENTEROS

**Definición** Un *dominio entero*  $D$  es un anillo comutativo unitario que no contiene divisores de 0.

Así, si los coeficientes de un polinomio pertenecen a un dominio entero, podemos resolver una ecuación polinomial en la cual se pueda factorizar el polinomio en factores lineales, haciendo, como es usual, cada factor igual a 0.

Como se mostrará en nuestra jerarquía de estructuras algebraicas, un dominio entero está entre un anillo comutativo con unitario y un campo. El teorema 24.2 muestra que las leyes de cancelación para la multiplicación se cumplen en un dominio entero. Hemos visto que  $\mathbf{Z}$  y  $\mathbf{Z}_p$ , para cualquier primo  $p$  son dominios enteros, pero  $\mathbf{Z}_n$  no es un dominio entero si  $n$  no es primo.

**Teorema 24.3** Todo campo  $F$  es un dominio entero.

*Demostración* Sea  $a, b \in F$ , supóngase que  $a \neq 0$ . Entonces, si  $ab = 0$  tenemos

$$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right)0 = 0.$$

Pero entonces,

$$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right)a\right]b = 1b = b.$$

Hemos mostrado que  $ab = 0$  con  $a \neq 0$  implica que  $b = 0$  en  $F$ , de modo que no existen divisores de 0 en  $F$ . Es claro que  $F$  es un anillo conmutativo con unitario y así, queda probado el teorema. ■

Hasta ahora, los únicos campos que se han visto son  $\mathbf{Q}$ ,  $\mathbf{R}$  y  $\mathbf{C}$ . El corolario del siguiente teorema nos dará algunos campos de orden finito.

**Teorema 24.4** *Todo dominio entero finito es un campo.*

*Demostración* Sean

$$0, 1, a_1, \dots, a_n$$

todos los elementos de un dominio entero finito  $D$ . Es necesario mostrar que para  $a \in D$ , donde  $a \neq 0$ , existe  $b \in D$  tal que  $ab = 1$ . Considérese ahora

$$a1, aa_1, \dots, aa_n$$

Afirmamos que todos estos elementos de  $D$  son distintos, pues  $aa_i = aa_j$  implica que  $a_i = a_j$ , por las leyes de cancelación que valen en un dominio entero. Además, como  $D$  no tiene divisores de 0, ninguno de estos elementos es 0. Contando, tenemos que  $a1, aa_1, \dots, aa_n$  son los elementos  $1, a_1, \dots, a_n$  en algún orden, de manera que  $a1 = 1$ , esto es,  $a = 1$ , o bien  $aa_i = 1$  para alguna  $i$ . Así,  $a$  tiene inverso multiplicativo. ■

**Corolario** *Si  $p$  es primo, entonces  $\mathbf{Z}_p$  es un campo.*

*Demostración* La demostración de este corolario resulta inmediatamente del hecho de que  $\mathbf{Z}_p$  es un dominio entero y del teorema 24.4. ■

## 24.3 CARACTÉRISTICA DE UN ANILLO

Sea  $R$  cualquier anillo. Podemos preguntar si existe algún entero positivo  $n$  tal que  $n \cdot a = 0$  para todas las  $a \in R$ , donde  $n \cdot a$  significa  $a + a + \dots + a$  para  $n$  sumandos, tal como se explicó en la sección 23.1. Por ejemplo, el entero  $m$  tiene esta propiedad para el anillo  $\mathbf{Z}_m$ .

**Definición** Si para un anillo  $R$  existe algún entero positivo  $n$  tal que  $n \cdot a = 0$  para todas las  $a \in R$ , entonces, el menor de dichos enteros positivos es la **característica del anillo  $R$** . Si no existen dichos enteros positivos, entonces  $R$  es de **característica 0**.

Usaremos el concepto de característica principalmente para campos.

**Ejemplo 24.2** El anillo  $\mathbf{Z}_n$  es de característica  $n$  mientras que  $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$  y  $\mathbf{C}$  tienen, todos, característica 0. ■

**Teorema 24.5** Si  $R$  es un anillo con unitario 1, entonces  $R$  tiene característica  $n > 0$  si y sólo si  $n$  es el menor entero positivo tal que  $n \cdot 1 = 0$ .

**Demostración** Por definición, si  $R$  tiene característica  $n > 0$ , entonces,  $n \cdot a = 0$  para todas las  $a \in R$ , así, en particular,  $n \cdot 1 = 0$ .

Recíprocamente, supóngase que  $n$  es un entero positivo tal que  $n \cdot 1 = 0$ . Entonces, para cualquier  $a \in R$  tenemos

$$n \cdot a = a + a + \cdots + a = a(1 + 1 + \cdots + 1) = a(n \cdot 1) = a0 = 0.$$

El teorema se deduce de inmediato. ■

## 24.4 TEOREMA DE FERMAT

Concluimos esta sección con algunas elegantes aplicaciones a la teoría de números. Es fácil ver que *para cualquier campo, los elementos distintos de cero forman grupo bajo la multiplicación de campo*. En particular, para  $\mathbf{Z}_p$  los elementos

$$1, 2, 3, \dots, p - 1$$

forman un grupo de orden  $p - 1$  bajo la multiplicación módulo  $p$ . Como el orden de cualquier elemento en un grupo divide al orden del grupo, vemos que para  $a \neq 0$  y  $a \in \mathbf{Z}_p$ ,  $a^{p-1} = 1$  en  $\mathbf{Z}_p$ . Más adelante veremos en detalle, tanto para la multiplicación como para la suma, que  $a \in \mathbf{Z}_p$  puede considerarse representante de la clase lateral  $a + p\mathbf{Z}$  y que el producto de clases laterales se puede calcular mediante multiplicación módulo  $p$  de representantes, de manera análoga al cálculo de las sumas. La colección  $\mathbf{Z}/p\mathbf{Z}$  de estas clases laterales se convierten en un anillo isomorfo a  $\mathbf{Z}_p$ . Supongámoslo por ahora; esto nos da inmediatamente el llamado pequeño teorema de Fermat.

**Teorema 24.6 (Fermat)** Si  $a \in \mathbf{Z}$  y  $p$  es un primo que no divide  $a$ , entonces  $p$  divide  $a^{p-1} - 1$ , esto es,  $a^{p-1} \equiv 1 \pmod{p}$  para  $a \not\equiv 0 \pmod{p}$ .

**Corolario** Si  $a \in \mathbf{Z}$ , entonces  $a^p \equiv a \pmod{p}$  para cualquier primo  $p$ .

*Demostración* Si  $a \not\equiv 0 \pmod{p}$ , la demostración del corolario resulta del teorema 24.6. Si  $a \equiv 0 \pmod{p}$  entonces, ambos lados se reducen a 0 módulo  $p$ . ■

Este corolario será de gran importancia más adelante cuando se estudien los campos finitos.

**Ejemplo 24.3** Calculemos el residuo de  $8^{10^3}$  al dividirlo entre 13. Usando el teorema de Fermat, tenemos

$$\begin{aligned} 8^{10^3} &\equiv (8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv 8^7 \equiv (-5)^7 \\ &\equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \pmod{13}. \end{aligned}$$

## \* 24.5 GENERALIZACION DE EULER

Euler dio una generalización del teorema de Fermat. Su generalización se deduce inmediatamente del teorema siguiente.

**Teorema 24.7** *El conjunto  $G_n$  de elementos distintos de cero de  $\mathbb{Z}_n$  que no son divisores de 0 forman grupo bajo la multiplicación módulo n.*

*Demostración* Primero, debemos mostrar que  $G_n$  es cerrado bajo la multiplicación módulo  $n$ . Sea  $a, b \in G_n$ . Si  $ab \notin G_n$ , entonces existiría  $c \neq 0$  en  $\mathbb{Z}_n$  tal que  $(ab)c = 0$ . Ahora,  $(ab)c = 0$  implica que  $a(bc) = 0$ . Como  $b \in G_n$  y  $c \neq 0$ , tenemos  $bc \neq 0$ , por definición de  $G_n$ . Pero, entonces,  $a(bc) = 0$  implicaría que  $a \notin G_n$ , contrario a la hipótesis. Nótese que hemos mostrado que, para cualquier anillo, el conjunto de elementos que no son divisores de 0 es cerrado bajo la multiplicación. Ninguna estructura de  $\mathbb{Z}_n$ , además de la estructura de anillo, se ha empleado hasta ahora.

Mostremos ahora que  $G_n$  es un grupo. Es claro que la multiplicación módulo  $n$  es asociativa y  $1 \in G_n$ . Falta mostrar que, para  $a \in G_n$ , existe  $b \in G_n$  tal que  $ab = 1$ . Sean

$$1, a_1, \dots, a_r$$

los elementos de  $G_n$ . Los elementos

$$a1, aa_1, \dots, aa_r$$

son todos diferentes, pues si  $aa_i = aa_j$ , entonces  $a(a_i - a_j) = 0$  y como  $a \in G_n$  y, por tanto, no es un divisor de 0, debemos tener  $a_i - a_j = 0$  o  $a_i = a_j$ . En consecuencia, contando, encontramos que  $a1 = 1$  o alguna  $aa_i$  debe ser 1, de modo que  $a$  tiene inverso multiplicativo. ■

Nótese que la única propiedad de  $\mathbb{Z}_n$  usada en este último teorema, además del hecho de que era un anillo con unitario, fue que era finito. En los teoremas 24.4 y 24.7 hemos empleado (esencialmente en la misma construcción) un argumento de conteo. Los argumentos de conteo son, a menudo, sencillos, pero están entre las herramientas más poderosas de todas las matemáticas.

Definamos  $\varphi(n)$  como el número de enteros positivos menores o iguales a  $n$  y primos relativos con  $n$ . Por ejemplo, si  $n = 12$  los enteros positivos menores o iguales a 12 y primos relativos con 12, son 1, 5, 7 y 11, así,  $\varphi(12) = 4$ . Por el teorema 24.1,  $\varphi(n)$  es el número de elementos de  $\mathbb{Z}_n$  que no son divisores de 0. Esta función  $\varphi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  es la función **f<sub>i</sub>** de Euler. Podemos describir, ahora, la generalización de Euler del teorema de Fermat.

**Teorema 24.8 (Euler)** Si  $a$  es un entero primo relativo con  $n$ , entonces  $a^{\varphi(n)} - 1$  es divisible entre  $n$ , esto es,  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

**Demostración** Si  $a$  es primo relativo con  $n$ , entonces, la clase lateral  $a + n\mathbb{Z}$  de  $n\mathbb{Z}$  que contiene el número  $a$  contiene un entero  $b < n$  y primo relativo con  $n$ . Usando el hecho (que probaremos más adelante) de que la multiplicación de estas clases laterales, mediante la multiplicación módulo  $n$  de representantes, está bien definida, tenemos que

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{n}.$$

Pero, por los teoremas 24.1 y 24.7,  $b$  puede verse como un elemento del grupo multiplicativo  $G_n$  de orden  $\varphi(n)$  formado por los  $\varphi(n)$  elementos de  $\mathbb{Z}_n$  primos relativos con  $n$ . Así,

$$b^{\varphi(n)} \equiv 1 \pmod{n},$$

y se deduce el teorema. ■

## Ejercicios

---

**24.1** Encuéntrense todas las soluciones de la ecuación  $x^3 - 2x^2 - 3x = 0$  en  $\mathbb{Z}_{12}$ .

**24.2** Resuélvase la ecuación  $3x = 2$  en el campo  $\mathbb{Z}_7$  y en el campo  $\mathbb{Z}_{23}$ .

**24.3** Encuéntrese la característica de cada uno de los siguientes anillos:

- |                                       |  |
|---------------------------------------|--|
| a) $2\mathbb{Z}$                      | b) $\mathbb{Z} \times \mathbb{Z}$        |
| c) $\mathbb{Z}_3 \times 3\mathbb{Z}$  | d) $\mathbb{Z}_3 \times \mathbb{Z}_3$    |
| e) $\mathbb{Z}_3 \times \mathbb{Z}_4$ | f) $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ |

**24.4** Usando el teorema de Fermat, encuéntrese el residuo de  $3^{47}$  al dividirlo entre 23.

**24.5** a) Muéstrese que 1 y  $p - 1$  son los únicos elementos del campo  $\mathbb{Z}_p$  que son sus propios inversos multiplicativos. [Sugerencia: considérese la ecuación  $x^2 - 1 = 0$ .]

- b) De la parte a), dedúzcase la mitad del *teorema de Wilson* que afirma que si  $p$  es primo, entonces  $(p - 1)! \equiv -1 \pmod{p}$ . (La otra mitad afirma que si  $(n - 1) \equiv -1 \pmod{n}$ , entonces,  $n$  es primo.)

**24.6** ¿Falso o verdadero?

- a)  $n\mathbb{Z}$  tiene divisores de cero si  $n$  no es primo.
  - b) Todo campo es un dominio entero.
  - c) La característica de  $n\mathbb{Z}$  es  $n$ .
  - d) Como anillo,  $\mathbb{Z}$  es isomorfo a  $n\mathbb{Z}$  para todas las  $n \geq 1$ .
  - e) La ley de la cancelación vale para cualquier anillo que sea isomorfo a un dominio entero.
  - f) Todo dominio entero de característica 0 es infinito.
  - g) El producto directo de dos dominios enteros es, de nuevo, un dominio entero.
  - h) Un divisor de cero en un anillo conmutativo con unitario puede no tener inverso multiplicativo.
  - i)  $n\mathbb{Z}$  es un subdominio de  $\mathbb{Z}$ .
  - j)  $\mathbb{Z}$  es un subcampo de  $\mathbb{Q}$ .
- 

**24.7** Encuéntrense todas las soluciones de la ecuación  $x^2 + 2x + 2 = 0$  en  $\mathbb{Z}_6$ ; de la ecuación  $x^2 + 2x + 4 = 0$  en  $\mathbb{Z}_6$ .

**24.8** Un elemento  $a$  de un anillo  $R$  es **idempotente** si  $a^2 = a$ . Muéstrese que un anillo con división contiene exactamente dos elementos idempotentes.

**24.9** Muéstrese que una intersección de subdominios de un dominio entero  $D$  es, de nuevo, un subdominio de  $D$ .

**24.10** Muéstrese que un anillo finito  $R$  con unitario y sin divisores de 0 es un anillo con división. (En realidad, es un campo, aunque la conmutatividad es difícil de probar. Véase el teorema 25.5.) [Nota: en la demostración, para mostrar que  $a \neq 0$  es una unidad, debe mostrarse que un «inverso multiplicativo izquierdo» de  $a \neq 0$  en  $R$  es, también, un «inverso multiplicativo derecho».]

**24.11** Sea  $R$  un anillo que contiene al menos dos elementos. Supóngase que para cada elemento  $a \in R$  diferente de cero, existe una  $b \in R$  única tal que  $aba = b$ .

- a) Muéstrese que  $R$  no tiene divisores de 0.
- b) Muéstrese que  $bab = b$ .
- c) Muéstrese que  $R$  tiene unitario.
- d) Muéstrese que  $R$  es un anillo de división.

**24.12** Muéstrese que la característica de un subdominio de un dominio entero  $D$  es igual a la característica de  $D$ .

**24.13** Muéstrese que si  $D$  es un dominio entero, entonces,  $\{n \cdot 1 \mid n \in \mathbb{Z}\}$  es un subdominio de  $D$  contenido en todo subdominio de  $D$ .

**24.14** Muéstrese que la característica de un dominio entero  $D$  debe ser 0 o un primo  $p$ . [Sugerencia: si la característica de  $D$  es  $mn$ , considérese  $(m \cdot 1)(n \cdot 1)$  en  $D$ .]

**24.15** Usese el teorema de Fermat para mostrar que para cualquier entero positivo  $n$ ,  $n^{37} - n$  es divisible entre 383 838. [Sugerencia:  $383\,838 = (37)(19)(13)(7)(3)(2)$ .]

**24.16** Este ejercicio muestra que todo anillo  $R$  puede agrandarse (si es necesario) a un anillo  $S$  con unitario, con la misma característica que  $R$ . Sea  $S = R \times \mathbb{Z}$ , si  $R$  tiene característica 0, y  $R \times \mathbb{Z}_n$ , si  $R$  tiene característica  $n$ . Sea la suma en  $S$ , la suma usual por componentes y sea la multiplicación definida por

$$(r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1 n_2)$$

donde  $n \cdot r$  tiene el significado explicado en el capítulo 23.

- a) Muéstrese que  $S$  es un anillo.
- b) Muéstrese que  $S$  tiene unitario.
- c) Muéstrese que  $S$  y  $R$  tienen la misma característica.
- d) Muéstrese que la transformación  $\phi: R \rightarrow S$  dada por  $r\phi = (r, 0)$  para  $r \in R$  es un isomorfismo de  $R$  con un subanillo de  $S$ .

**\*24.17** Dése la tabla de la multiplicación de grupo para el grupo multiplicativo de aquellos elementos de  $\mathbb{Z}_{12}$  primos relativos con 12. ¿A qué grupo de orden 4 es isomorfo?

**\*24.18** Hágase la tabla de los valores de  $\phi(n)$  para  $n \leq 30$ .

**\*24.19** Usese la generalización de Euler del teorema de Fermat, para encontrar el residuo de  $7^{1000}$  al dividirlo entre 24.

## Algunos ejemplos no commutativos

Debido a la amplitud del tema no profundizaremos sobre los anillos no conmutativos y semicampos, así es que como podrán imaginarse, de manera natural, surge gran cantidad de anillos no conmutativos importantes en álgebra; en este capítulo sólo daremos algunos ejemplos de ellos.

### 25.1 MATRICES SOBRE UN CAMPO

Sea  $F$  cualquier campo (digamos  $\mathbf{Q}$ ,  $\mathbf{R}$  o  $\mathbf{C}$ ), considérese el conjunto  $M_2(F)$  de todos los arreglos cuadrados de  $2 \times 2$

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

donde todas las  $a_{ij}$  están en  $F$ . El primer subíndice  $i$  de  $a_{ij}$  indica el *renglón* donde está  $a_{ij}$  en el arreglo cuadrado y el segundo subíndice  $j$  indica la *columna*. Así,  $a_{12}$  es el elemento de  $F$  situado en el primer renglón y segunda columna del arreglo cuadrado. Dicho arreglo cuadrado es una **matriz de  $2 \times 2$  sobre  $F$** . El conjunto  $M_n(F)$  de todas las **matrices de  $n \times n$  sobre  $F$**  se define de manera análoga.

Definimos la suma de matrices en  $M_2(F)$  por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix},$$

esto es, sumando los elementos de lugares correspondientes. Después de pensar un momento, se verá que, debido a que  $F$  satisface los axiomas de campo,  $\langle M_2(F), + \rangle$  es un grupo abeliano con identidad aditiva

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

y con

$$-\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}.$$

La multiplicación de matrices en  $M_2(F)$  está definida por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Esta multiplicación parece difícil, se recuerda mejor por

$$(a_{ij})(b_{ij}) = (c_{ij}),$$

donde

$$c_{rs} = \sum_{i=1}^2 a_{ri}b_{is}.$$

Con la definición análoga para la multiplicación de matrices, en donde la suma va de  $i = 1$  a  $n$  y la definición análoga obvia para la suma de matrices, todo lo que se ha hecho es válido para el conjunto  $M_n(F)$  de todas las matrices de  $n \times n$  sobre  $F$ .

**Ejemplo 25.1** En  $M_2(Q)$

$$\begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 2 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$$

y

$$\begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 2 & -5 \end{pmatrix} = \begin{pmatrix} 0 & -5 \\ 11 & -20 \end{pmatrix}. \blacksquare$$

Para mostrar que  $\langle M_n(F), +, \cdot \rangle$  es un anillo, falta probar las leyes asociativa y distributiva. Lo ilustramos con la ley asociativa para la multiplicación de matrices en  $M_n(F)$ . Usando las propiedades de campo de  $F$  y la definición de multipli-

cación de matrices en  $M_n(F)$ , si  $d_{rs}$  está en el lugar correspondiente a  $(a_{ij})[(b_{ij})(c_{ij})]$ , tenemos

$$d_{rs} = \sum_{k=1}^n a_{rk} \left( \sum_{j=1}^n b_{kj} c_{js} \right) = \sum_{j=1}^n \left( \sum_{k=1}^n a_{rk} b_{kj} \right) c_{js} = e_{rs},$$

donde  $e_{rs}$  está en el  $r$ -ésimo renglón y  $s$ -ésima columna de  $[(a_{ij})(b_{ij})](c_{ij})$ . Las leyes distributivas se prueban de manera análoga. Consideramos demostrado el siguiente teorema.

**Teorema 25.1** *Si  $F$  es un campo, entonces el conjunto  $M_n(F)$  de todas las matrices de  $n \times n$  de elementos de  $F$  forma un anillo bajo la suma y multiplicación de matrices.*

Estos anillos de matrices se usan en álgebra lineal. En este contexto pueden considerarse correspondientes a cierto tipo de funciones y, desde este punto de vista, se puede mostrar que la multiplicación de matrices es precisamente la composición de funciones. Como la composición de funciones siempre es asociativa, da otra demostración, más elegante, de la ley asociativa.

Nótese que  $M_1(F)$  es isomorfo a  $F$  bajo la transformación  $\phi: F \rightarrow M_1(F)$  dada por  $a\phi = (a)$  para  $a \in F$ . Recuérdese que esta sección trata de anillos no conmutativos. Es cierto que  $M_n(F)$  es no conmutativo si  $n \geq 2$ . El ejemplo 25.2 lo ilustra para  $M_2(F)$ .

**Ejemplo 25.2** Como todo campo  $F$  contiene elementos 0 y 1,  $M_2(F)$  siempre tiene entre sus elementos a

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

La definición de multiplicación de matrices muestra que

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

mientras que

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Así,  $M_2(F)$  es no conmutativo. Como

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

es la identidad aditiva, este ejemplo muestra, además, que existen divisores de 0 en  $M_2(F)$ . Lo mismo es cierto sobre  $M_n(F)$ , para  $n \geq 2$ . Dejamos como ejercicio la demostración de que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

es el elemento unitario en  $M_2(F)$  (véase el ejercicio 25.2). ■

## \*25.2 ANILLOS DE ENDOMORFISMOS

Sea  $A$  cualquier grupo abeliano. Un homomorfismo de  $A$  en sí mismo es un **endomorfismo de  $A$** . Sea  $\text{Hom}(A)$  el conjunto de todos los endomorfismos de  $A$ . Como la composición de dos homomorfismos de  $A$  en si mismo es de nuevo uno de dichos homomorfismos, definimos la multiplicación en  $\text{Hom}(A)$  por la composición de funciones, así, la multiplicación es asociativa.

Para definir suma, para  $\phi, \psi \in \text{Hom}(A)$ , tenemos que describir el valor de  $(\phi + \psi)$  en cada  $a \in A$ . Definase

$$a(\phi + \psi) = (a\phi) + (a\psi).$$

Como

$$\begin{aligned} (a+b)(\phi + \psi) &= (a+b)\phi + (a+b)\psi = (a\phi + b\phi) + (a\psi + b\psi) \\ &= (a\phi + a\psi) + (b\phi + b\psi) = a(\phi + \psi) + b(\phi + \psi), \end{aligned}$$

veremos que  $\phi + \psi$  está en  $\text{Hom}(A)$ .

Como  $A$  es conmutativo, tenemos que

$$a(\phi + \psi) = (a\phi) + (a\psi) = (a\psi) + (a\phi) = a(\psi + \phi)$$

para todas las  $a \in A$ , de modo que  $\phi + \psi = \psi + \phi$  y la suma en  $\text{Hom}(A)$  es conmutativa. La asociatividad de la suma se sigue de

$$\begin{aligned} a[\phi + (\psi + \theta)] &= a\phi + a(\psi + \theta) = a\phi + (a\psi + a\theta) \\ &= (a\phi + a\psi) + a\theta = a(\phi + \psi) + a\theta = a[(\phi + \psi) + \theta]. \end{aligned}$$

Si  $e$  es la identidad aditiva de  $A$ , entonces, el homomorfismo 0 definido por

$$a0 = e$$

para  $a \in A$  es claramente una identidad aditiva en  $\text{Hom}(A)$ . Por último, para

$$\phi \in \text{Hom}(A),$$

$-\phi$  definida por

$$a(-\phi) = -(a\phi)$$

está en  $\text{Hom}(A)$ , puesto que

$$\begin{aligned} (a + b)(-\phi) &= -((a + b)\phi) = -(a\phi + b\phi) \\ &= -(a\phi) + (-b\phi) = a(-\phi) + b(-\phi). \end{aligned}$$

Es claro que  $\phi + (-\phi) = 0$ . Así,  $\langle \text{Hom}(A), + \rangle$  es un grupo abeliano.

Nótese que no hemos usado aún el hecho de que nuestras funciones son *homomorfismos* excepto para mostrar que  $\phi + \psi$  y  $-\phi$  son, nuevamente, *homomorfismos*. Así, el conjunto  $A^A$  de *todas las funciones* de  $A$  en  $A$  es un grupo abeliano bajo exactamente la misma definición de suma y es claro que la composición de funciones da, de nuevo, una bella multiplicación asociativa en  $A^A$ . Sin embargo, si necesitamos ahora el hecho de que estas funciones en  $\text{Hom}(A)$  son homomorfismos, para probar la ley distributiva derecha en  $\text{Hom}(A)$ . Excepto por esta ley distributiva derecha  $\langle A^A, +, \cdot \rangle$  satisface todos los axiomas para un anillo. Sean  $\phi, \psi$  y  $\theta$  en  $\text{Hom}(A)$  y sea  $a \in A$ . Entonces,

$$a[(\phi + \psi)\theta] = [a(\phi + \psi)]\theta = (a\phi + a\psi)\theta.$$

Como  $\theta$  es un *homomorfismo*,

$$(a\phi + a\psi)\theta = (a\phi)\theta + (a\psi)\theta = a(\phi\theta) + a(\psi\theta) = a(\phi\theta + \psi\theta).$$

Así,  $(\phi + \psi)\theta = \phi\theta + \psi\theta$ . La ley distributiva izquierda no causa dificultad, aun en  $A^A$  y resulta de

$$a[\phi(\psi + \theta)] = a\phi(\psi + \theta) = (a\phi)\psi + (a\phi)\theta = a(\phi\psi) + a(\phi\theta) = a(\phi\psi + \phi\theta).$$

Así, hemos probado el siguiente teorema.

**Teorema 25.2** *El conjunto  $\text{Hom}(A)$  de todos los endomorfismos de un grupo abeliano  $A$  forma un anillo bajo la suma de homomorfismos y la multiplicación de homomorfismos (composición de funciones).*

De nuevo, para mostrar las aplicaciones que puede tener este capítulo, debemos dar un ejemplo para mostrar que  $\text{Hom}(A)$  no es por fuerza conmutativo. Parece razonable esperarlo, pues la composición de funciones, en general, no es

comutativa. Sin embargo, en algunos casos,  $\text{Hom}(A)$  podría ser conmutativo. De hecho,  $\text{Hom}(\langle \mathbf{Z}, + \rangle)$  es conmutativo. En el ejercicio 25.10, pedimos al estudiante que lo demuestre.

**Ejemplo 25.3** Considérese el grupo abeliano libre  $\langle \mathbf{Z} \times \mathbf{Z}, + \rangle$  analizado en la parte I. Podemos especificar un endomorfismo de este grupo abeliano libre, dando sus valores en los generadores del grupo  $(1, 0)$  y  $(0, 1)$ . Definir

$$\phi \in \text{Hom}(\langle \mathbf{Z} \times \mathbf{Z}, + \rangle)$$

por

$$(1, 0)\phi = (1, 0) \quad \text{y} \quad (0, 1)\phi = (1, 0).$$

Definir  $\psi$  por

$$(1, 0)\psi = (0, 0) \quad \text{y} \quad (0, 1)\psi = (0, 1).$$

Intuitivamente,  $\phi$  transforma todo sobre el primer factor de  $\mathbf{Z} \times \mathbf{Z}$ , y  $\psi$  colapsa el primer factor. Así,

$$(n, m)(\phi\psi) = (n + m, 0)\psi = (0, 0),$$

mientras que

$$(n, m)(\psi\phi) = (0, m)\phi = (m, 0).$$

De aquí que  $\phi\psi \neq \psi\phi$ . ■

**Ejemplo 25.4** Sea  $F$  un campo y sea  $F[x]$  el conjunto de todas las expresiones polinomiales formales con coeficientes en  $F$ . (Analizaremos dichos polinomios en el capítulo 30. Por ahora, nos basaremos en la intuición del lector.) Un elemento típico de  $F[x]$  se puede escribir en la forma

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

donde  $a_0, a_1, a_2, \dots, a_n \in F$ . Con la suma usual de polinomios,  $F[x]$  se vuelve un grupo abeliano, de manera que podemos considerar  $\text{Hom}(F[x])$ . Un elemento de  $\text{Hom}(F[x])$  actúa en cada polinomio en  $F[x]$ , multiplicando por  $x$ . Sea  $X$  este endomorfismo, de modo que

$$(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)X = a_0x + a_1x^2 + a_2x^3 + \cdots + a_nx^{n+1}.$$

Otro elemento de  $\text{Hom}(F[x])$  es la diferenciación formal con respecto a  $x$ . (La conocida fórmula «la derivada de una suma es la suma de las derivadas» garanti-

za que la diferenciación es un endomorfismo de  $F[x]$ .) Sea  $Y$  este endomorfismo de modo que

$$(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)Y = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

En el ejercicio 25.12 pedimos mostrar que  $XY - YX = 1$ , donde  $1$  es el unitario (la transformación idéntica) en  $\text{Hom}(F[x])$ . Así,  $XY \neq YX$ . La multiplicación de polinomios en  $F[x]$  por cualquier elemento de  $F$  también da un elemento de  $\text{Hom}(F[x])$ . El subanillo de  $\text{Hom}(F[x])$  generado por  $X$  y  $Y$  y multiplicaciones por elementos de  $F$  es el álgebra de Weyl y es importante en mecánica cuántica. ■

### \*25.3 ANILLOS DE GRUPO Y ALGEBRA DE GRUPO

Sea  $G = \{g_i \mid i \in I\}$  cualquier grupo multiplicativo y sea  $R$  cualquier anillo con unitario. Sea  $R(G)$  el conjunto de todas las *sumas formales*

$$\sum_{i \in I} a_i g_i$$

para  $a_i \in R$  y  $g_i \in G$ , donde todas las  $a_i$  excepto un número finito son 0. Definamos la suma de dos elementos de  $R(G)$  por

$$\left( \sum_{i \in I} a_i g_i \right) + \left( \sum_{i \in I} b_i g_i \right) = \sum_{i \in I} (a_i + b_i) g_i.$$

Es claro que  $(a_i + b_i) = 0$  excepto por un número finito de índices  $i$ , de modo que  $\sum_{i \in I} (a_i + b_i) g_i$  está de nuevo en  $R(G)$ . Es inmediato que  $\langle R(G), + \rangle$  es un grupo abeliano con identidad aditiva  $\sum_{i \in I} 0 g_i$ .

La multiplicación de dos elementos de  $R(G)$  está definida por el uso de las multiplicaciones en  $G$  y  $R$  como sigue:

$$\left( \sum_{i \in I} a_i g_i \right) \left( \sum_{j \in I} b_j g_j \right) = \sum_{i \in I} \left( \sum_{g_j g_k = g_i} a_j b_k \right) g_i.$$

De manera intuitiva distribuimos formalmente la suma  $\sum_{i \in I} a_i g_i$  sobre la suma  $\sum_{j \in I} b_j g_j$  y al término  $a_j g_j b_k g_k$  lo nombramos  $a_j b_k g_i$ , donde  $g_j g_k = g_i$  en  $G$ . Como  $a_i$  y  $b_i$  son 0 para todos, excepto un número finito de  $i$ , la suma  $\sum_{g_j g_k = g_i} a_j b_k$  contiene sólo un número finito de sumandos diferentes de cero  $a_j b_k \in R$  y así pueden considerarse un elemento de  $R$ . Claramente, tenemos otra vez que a lo más un número finito de dichas sumas  $\sum_{g_j g_k = g_i} a_j b_k$  son distintas de cero. Así, la multiplicación es cerrada en  $R(G)$ .

La ley distributiva se sigue de inmediato a partir de la definición de suma y de la manera formal en que usamos la distributividad para definir multiplicación. Para la asociatividad de la multiplicación

$$\begin{aligned}
 & \left( \sum_{i \in I} a_i g_i \right) \left[ \left( \sum_{i \in I} b_i g_i \right) \left( \sum_{i \in I} c_i g_i \right) \right] = \left( \sum_{i \in I} a_i g_i \right) \left[ \sum_{i \in I} \left( \sum_{g_h g_k = g_i} b_j c_k \right) g_i \right] \\
 & = \sum_{i \in I} \left( \sum_{g_h g_j g_k = g_i} a_h b_j c_k \right) g_i \\
 & = \left[ \sum_{i \in I} \left( \sum_{g_h g_j = g_i} a_h b_j \right) g_i \right] \left( \sum_{i \in I} c_i g_i \right) \\
 & = \left[ \left( \sum_{i \in I} a_i g_i \right) \left( \sum_{i \in I} b_i g_i \right) \right] \left( \sum_{i \in I} c_i g_i \right).
 \end{aligned}$$

Así, hemos probado el siguiente teorema.

**Teorema 25.3** Si  $G$  es cualquier grupo multiplicativo, entonces  $\langle R(G), +, \cdot \rangle$  es un anillo.

Si nombramos ahora  $g_i$  al elemento  $\sum_{i \in I} a_i g_i$  de  $R(G)$  donde  $a_i = 0$  para  $i \neq j$  y  $a_j = 1$ , vemos que se puede considerar que, de manera natural,  $\langle R(G), \cdot \rangle$  contiene  $G$  como subsistema multiplicativo. Así, si  $G$  no es abeliano,  $R(G)$  no será un anillo comunitativo.

**Definición** El anillo  $R(G)$  definido antes, es el *anillo del grupo G sobre R*. Si  $F$  es un campo, entonces  $F(G)$  es el *álgebra de grupo de G sobre F*.

**Ejemplo 25.5** Demos las tablas de suma y multiplicación para el álgebra de grupo  $Z_2(G)$ , donde  $G = \{e, a\}$  es cíclico de orden 2. Los elementos de  $Z_2(G)$  son

$$0e + 0a, \quad 0e + 1a, \quad 1e + 0a \quad \text{y} \quad 1e + 1a.$$

Si denotamos estos elementos de la manera obvia y natural por

$$0, \quad a, \quad e \quad \text{y} \quad e + a,$$

respectivamente, obtenemos las tablas 25.1 y 25.2.

**Tabla 25.1**

+	0	$a$	$e$	$e + a$
0	0	$a$	$e$	$e + a$
$a$	$a$	0	$e + a$	$e$
$e$	$e$	$e + a$	0	$a$
$e + a$	$e + a$	$e$	$a$	0

**Tabla 25.2**

	0	$a$	$e$	$e + a$
0	0	0	0	0
$a$	0	$e$	$a$	$e + a$
$e$	0	$a$	$e$	$e + a$
$e + a$	0	$e + a$	$e + a$	0

Por ejemplo, para ver que  $(e + a)(e + a) = 0$  tenemos que

$$(1e + 1a)(1e + 1a) = (1 + 1)e + (1 + 1)a = 0e + 0a.$$

Este ejemplo muestra que un álgebra de grupo puede tener divisores de 0. En efecto, usualmente así sucede. ■

## \*25.4 CUATERNIONES

Hasta ahora no hemos visto un ejemplo de semicampo. Los *cuaterniones* de Hamilton son el ejemplo común de un semicampo; describámoslos.

Sea  $\mathcal{Q}$  el conjunto  $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ . Ahora,  $\langle \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}, + \rangle$  es un grupo bajo la suma por componentes, el producto directo de  $\mathbb{R}$  bajo la suma, por él mismo, cuatro veces. Esto da la operación de suma en  $\mathcal{Q}$ . Cambiemos el nombre a ciertos elementos de  $\mathcal{Q}$ . Hagamos

$$\begin{aligned} 1 &= (1, 0, 0, 0), & i &= (0, 1, 0, 0), \\ j &= (0, 0, 1, 0) & \text{y} & k = (0, 0, 0, 1). \end{aligned}$$

Además, acordamos hacer

$$\begin{aligned} a_1 &= (a_1, 0, 0, 0), & a_2i &= (0, a_2, 0, 0), \\ a_3j &= (0, 0, a_3, 0) & \text{y} & a_4k = (0, 0, 0, a_4). \end{aligned}$$

En vista de nuestra definición de suma, tenemos

$$(a_1, a_2, a_3, a_4) = a_1 + a_2i + a_3j + a_4k.$$

Así,

$$\begin{aligned} (a_1 + a_2i + a_3j + a_4k) + (b_1 + b_2i + b_3j + b_4k) &= \\ = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k. \end{aligned}$$

Para definir la multiplicación en  $\mathcal{Q}$ , comenzamos definiendo

$$\begin{aligned} 1a &= a1 = a & \text{para} & a \in \mathcal{Q}, \\ i^2 &= j^2 = k^2 = -1, \end{aligned}$$

y

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i \quad \text{y} \quad ik = -j.$$

Nótese la analogía con los llamados productos cruz de vectores. Estas fórmulas son fáciles de recordar si se piensa en la sucesión

$$i, j, k, i, j, k.$$

El producto de izquierda a derecha de dos elementos adyacentes es el siguiente a la derecha. El producto de derecha a izquierda de dos elementos adyacentes es el negativo del que les sigue a la izquierda. Entonces, definimos el producto como lo que debe ser, para que se cumplan las leyes distributivas, a saber,

$$\begin{aligned} (a_1 + a_2i + a_3j + a_4k)(b_1 + b_2i + b_3j + b_4k) &= \\ &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i + \\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j + \\ &\quad + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k. \end{aligned}$$

La verificación de que  $\mathcal{Q}$  es un semicampo es ahora una tarea tediosa, parte de ella se asigna como ejercicio. Como  $ij = k$  y  $ji = -k$ , vemos que la multiplicación no es conmutativa, de modo que  $\mathcal{Q}$  definitivamente no es campo. El único axioma que no puede verificarse en forma mecánica es la existencia del inverso multiplicativo para  $a = a_1 + a_2i + a_3j + a_4k$ , donde no todas las  $a_i = 0$ . El estudiante puede corroborar que

$$(a_1 + a_2i + a_3j + a_4k)(a_1 - a_2i - a_3j - a_4k) = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Si hacemos

$$|a|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2 \quad \text{y} \quad \bar{a} = a_1 - a_2i - a_3j - a_4k,$$

vemos que

$$\frac{\bar{a}}{|a|^2} = \frac{a_1}{|a|^2} - \left( \frac{a_2}{|a|^2} \right) i - \left( \frac{a_3}{|a|^2} \right) j - \left( \frac{a_4}{|a|^2} \right) k$$

es un inverso multiplicativo de  $a$ . Hemos demostrado el teorema siguiente.

**Teorema 25.4** *Los cuaterniones  $\mathcal{Q}$  forman un semicampo bajo la suma y la multiplicación.*

Nótese que  $G = \{\pm 1, \pm i, \pm j, \pm k\}$  es un grupo de orden 8 bajo la multiplicación de cuaterniones. En términos de generadores y relaciones, este grupo está generado por  $i$  y  $j$ , donde

$$i^4 = 1, \quad j^2 = i^2 \quad \text{y} \quad ji = i^3j.$$

Como en el ejemplo 22.5 vimos que  $G_2$  con presentación

$$(a, b : a^4 = 1, b^2 = a^2, ba = a^3b),$$

es un grupo de orden 8, debemos tener  $G_2 \simeq G$ . Esto explica por qué el grupo  $G_2$  del ejemplo 22.5 se llamó *grupo de cuaterniones*.

El álgebra no es tan rica en semicampos (estRICTOS) como lo es en campos. Por ejemplo, no hay semicampos finitos (que no sean campos). Este es el contenido de un famoso teorema de Wedderburn, el cual enunciamos sin demostración.

**Teorema 25.5 (Wedderburn)** *Un anillo de división, finito, es campo.*

**Demostración** Consultar la literatura para la demostración del teorema de Wedderburn.

## Ejercicios

---

\*25.1 Calcúlese

$$\begin{pmatrix} 3 & -4 \\ 1 & 5 \end{pmatrix} + \begin{pmatrix} 4 & 17 \\ 5 & -3 \end{pmatrix}$$

y

$$\begin{pmatrix} 3 & -4 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 4 & 17 \\ 5 & -3 \end{pmatrix}$$

en  $M_2(Q)$ .

\*25.2 Muéstrese que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

es elemento unitario en  $M_2(F)$ . Describáse el elemento unitario en  $M_n(F)$ .

\*25.3 Sea  $\phi$  el elemento de  $\text{Hom}(\langle \mathbb{Z} \times \mathbb{Z}, + \rangle)$  dado en el ejemplo 25.3. Este ejemplo mostró que  $\phi$  es un divisor izquierdo de 0. Muéstrese que  $\phi$  también es un divisor derecho de 0.

\*25.4 Sea  $G = \{e, a, b\}$  un grupo cíclico de orden 3 con elemento identidad  $e$ . Escribáse cada uno de los siguientes elementos del álgebra de grupo  $\mathbb{Z}_5(G)$  en la forma

$$re + sa + tb \quad \text{para } r, s, t \in \mathbb{Z}_5.$$

- a)  $(2e + 3a + 0b) + (4e + 2a + 3b)$
- b)  $(2e + 3a + 0b)(4e + 2a + 3b)$
- c)  $(3e + 3a + 3b)^4$

\*25.5 Escribanse los siguientes elementos de  $\mathcal{Z}$  en la forma  $a_1 + a_2i + a_3j + a_4k$  para  $a_i \in \mathbb{R}$ .

- a)  $(i + 3j)(4 + 2j - k)$
- b)  $i^2 j^3 k j i^5$
- c)  $(i + j)^{-1}$
- d)  $[(1 + 3i)(4j + 3k)]^{-1}$

\*25.6 ¿Falso o verdadero?

- a)  $M_n(F)$  no tiene divisores de 0 para ninguna  $n$ .
  - b) Todo elemento distinto de cero de  $M_2(\mathbb{Z}_2)$  es una unidad.
  - c)  $\text{Hom}(A)$  es siempre un anillo con unitario  $\neq 0$  para todo grupo abeliano  $A$ .
  - d)  $\text{Hom}(A)$  nunca es un anillo con unitario  $\neq 0$  para cualquier grupo abeliano  $A$ .
  - e) El subconjunto  $\text{Iso}(A)$  de  $\text{Hom}(A)$ , formado por los isomorfismos de  $A$  sobre  $A$  es un subanillo de  $\text{Hom}(A)$  para todo grupo abeliano  $A$ .
  - f)  $R(\langle \mathbb{Z}, + \rangle)$  es isomorfo a  $\langle \mathbb{Z}, +, \cdot \rangle$  para todo anillo conmutativo con unitario  $R$ .
  - g) El anillo de grupo  $R(G)$  de un grupo abeliano  $G$  es un anillo conmutativo para cualquier anillo conmutativo con unitario  $R$ .
  - h) Los cuaterniones son campo.
  - i)  $\langle \mathcal{Z}^*, \cdot \rangle$  es grupo, donde  $\mathcal{Z}^*$  es el conjunto de los cuaterniones distintos de cero.
  - j) Ningún subanillo de  $\mathcal{Z}$  es un anillo.
- 

\*25.7 Muéstrese que la matriz

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

en  $M_2(F)$  no sólo es un divisor izquierdo de 0, como se mostró en el ejemplo 25.2, sino también un divisor derecho de 0.

\*25.8 Pruébese la ley distributiva izquierda en  $M_2(F)$ .

\*25.9 Muéstrese que  $M_2(F)$  tiene al menos seis unidades para todo campo  $F$ . Exhibáanse estas unidades. [Sugerencia:  $F$  tiene al menos dos elementos, 0 y 1.]

\*25.10 Muéstrese que  $\text{Hom}(\langle \mathbb{Z}, + \rangle)$  es isomorfo de manera natural a  $\langle \mathbb{Z}, +, \cdot \rangle$  y que  $\text{Hom}(\langle \mathbb{Z}_n, + \rangle)$  es isomorfo de manera natural a  $\langle \mathbb{Z}_n, +, \cdot \rangle$ .

\*25.11 Muéstrese que  $\text{Hom}(\langle \mathbb{Z}_2 \times \mathbb{Z}_2, + \rangle)$  no es isomorfo a  $\langle \mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot \rangle$ .

\*25.12 Con respecto al ejemplo 25.4, muéstrese que  $XY - YX = 1$ .

\*25.13 Con respecto al grupo  $S_3$  dado en el ejemplo 4.1, calcúlese el producto

$$(0\rho_0 + 1\rho_1 + 0\rho_2 + 0\mu_1 + 1\mu_2 + 1\mu_3)(1\rho_0 + 1\rho_1 + 0\rho_2 + 1\mu_1 + 0\mu_2 + 1\mu_3)$$

en el álgebra de grupo  $\mathbb{Z}_2(S_3)$ .

\*25.14 Si  $G = \{e\}$ , el grupo de un elemento, muéstrese que  $R(G)$  es isomorfo a  $R$  para cualquier anillo  $R$ .

## **236 ALCUNOS EJEMPLOS NO CONMUTATIVOS**

- \*25.15 Encuéntrense dos subconjuntos de  $\mathcal{Q}$  diferentes de  $\mathbf{C}$  y diferentes entre ellos, cada uno de los cuales es un campo isomorfo a  $\mathbf{C}$  bajo la suma y multiplicación inducidas de  $\mathcal{Q}$ .
- \*25.16 Muéstrese, mediante un ejemplo, que una ecuación polinomial de grado  $n$  puede tener más de  $n$  soluciones en un semicampo. [Sugerencia: considérese  $n = 2$  y el semicampo  $\mathcal{Q}$ .]
- \*25.17 Pruébese la ley asociativa para la multiplicación en  $\mathcal{Q}$ . (Esto debería quitarles las ganas de verificar cualquier otro de los axiomas de semicampo para  $\mathcal{Q}$ .)
- \*25.18 Encuéntrese el centro del grupo  $\langle \mathcal{Q}^*, \cdot \rangle$  donde  $\mathcal{Q}^*$  es el conjunto de los cuaterniones distintos de cero.

## El campo de cocientes de un dominio entero

Si un dominio entero es tal que todo elemento distinto de cero tiene un inverso multiplicativo, entonces es un campo. Sin embargo, muchos dominios enteros, como los enteros  $\mathbb{Z}$ , no forman campo. El dilema no es tan serio. El propósito de este capítulo es mostrar que todo dominio entero puede considerarse contenido en cierto campo, *el campo de cocientes del dominio entero*. Este campo será un campo minimal que contiene el dominio entero en el sentido que describiremos. Por ejemplo, los enteros están contenidos en el campo  $\mathbb{Q}$ , cuyos elementos se pueden expresar como cocientes de enteros. Nuestra construcción de un campo de cocientes de un dominio entero es exactamente igual a la construcción de los números racionales, a partir de los enteros, que ya se habrá visto en un curso de fundamentos o de cálculo avanzado. Seguir esta construcción hasta el fin es un buen ejercicio para el uso de la definición y el concepto de isomorfismo que analizaremos con cierto detalle, aunque escribir, o leerlo hasta el último detalle sería tedioso. Podemos motivar cada paso por la forma en que se obtiene  $\mathbb{Q}$  a partir de  $\mathbb{Z}$ . Recuérdese que las diferentes representaciones de un número racional como cociente de enteros, fueron la motivación para el análisis de las relaciones de equivalencia de la sección 0.3.

### 26.1 LA CONSTRUCCION

Sea  $D$  un dominio entero que deseamos agrandar a un campo de cocientes  $F$ . Un esbozo a grandes rasgos de los pasos a seguir es el siguiente:

- 1 Definir cuáles serán los elementos de  $F$ .
- 2 Definir en  $F$  las operaciones binarias de suma y multiplicación.

- 3 Comprobar que se cumplen todos los axiomas de campo, para mostrar que  $F$  es un campo bajo estas operaciones.
- 4 Mostrar que  $F$  puede considerarse conteniendo a  $D$  como un subdominio entero.

Los pasos 1, 2 y 4 son muy interesantes, el paso 3 es muy aburrido. Procedemos a la construcción.

**PASO 1** Sea  $D$  un dominio entero dado, formar el producto cartesiano

$$D \times D = \{(a, b) \mid a, b \in D\}.$$

Se asume que un par ordenado  $(a, b)$  representa un *cociente formal*  $a/b$ , esto es, si  $D = \mathbf{Z}$  el par  $(2, 3)$  representará, finalmente,  $\frac{2}{3}$ . El par  $(2, 0)$  no representará elemento alguno de  $\mathbf{Q}$  y, también en el caso general, reduciremos un poco  $D \times D$ . Sea  $S$  el subconjunto de  $D \times D$  dado por

$$S = \{(a, b) \mid a, b \in D, b \neq 0\}.$$

Ahora,  $S$  no será nuestro campo todavía, debido a que con  $D = \mathbf{Z}$ , pares *diferentes* de enteros, como  $(2, 3)$  y  $(4, 6)$  pueden representar al *mismo* número racional. A continuación definiremos cuándo dos elementos de  $S$  representan al mismo elemento de  $F$  o, como diremos, cuándo dos elementos en  $S$  son *equivalentes*.

**Definición** Dos elementos  $(a, b)$  y  $(c, d)$  en  $S$  son *equivalentes* y lo denotamos por  $(a, b) \sim (c, d)$ , si y sólo si  $ad = bc$ .

Obsérvese que esta definición es razonable, puesto que el criterio para que  $(a, b) \sim (c, d)$ , es una ecuación  $ad = bc$  que involucra elementos de  $D$  y la multiplicación conocida en  $D$ . Nótese también, que para  $D = \mathbf{Z}$  el criterio da la definición usual de *igualdad*, por ejemplo,  $\frac{2}{3} = \frac{4}{6}$  porque  $(2)(6) = (3)(4)$ . El número racional que usualmente denotamos por  $\frac{2}{3}$  puede considerarse la colección de todos los cocientes de enteros que se reducen a, o son equivalentes a  $\frac{2}{3}$ .

**Lema 26.1** La relación descrita  $\sim$  entre elementos del conjunto  $S$  es una relación de equivalencia.

**Demostración** Debemos comprobar que se cumplen las tres propiedades de relación de equivalencia.

**Reflexividad**  $(a, b) \sim (a, b)$  pues  $ab = ba$ , porque la multiplicación en  $D$  es conmutativa.

**Simetría** Si  $(a, b) \sim (c, d)$ , entonces  $ad = bc$ . Como la multiplicación en  $D$  es conmutativa, deducimos que  $cb = da$  y, por tanto,  $(c, d) \sim (a, b)$ .

**Transitividad** Si  $(a, b) \sim (c, d)$  y  $(c, d) \sim (r, s)$ , entonces  $ad = bc$  y  $cs = dr$ . Usando estas relaciones y el hecho de que la multiplicación en  $D$  es conmutativa, tenemos que

$$asd = sad = sbc = bcs = hdr = brd.$$

Ahora,  $d \neq 0$  y  $D$  es un dominio entero, así que vale la cancelación; éste es un paso fundamental en el análisis. Por tanto, de  $asd = brd$  obtenemos  $as = br$  de modo que  $(a, b) \sim (r, s)$ . ■

Vale la pena comparar la demostración anterior con la del ejemplo 0.1. Los pasos son idénticos.

Sabemos ahora, en vista del teorema 0.1, que  $\sim$  da una partición de  $S$  en clases de equivalencia. Para evitar colocar líneas largas sobre expresiones extensas, escribiremos  $[(a, b)]$  en lugar de  $(a, b)$  para la clase de equivalencia de  $(a, b)$  en  $S$  bajo la relación  $\sim$ . Terminamos el paso 1 definiendo  $F$  como el conjunto de todas las clases de equivalencia  $[(a, b)]$  para  $(a, b) \in S$ .

**PASO 2** El siguiente lema sirve para definir suma y multiplicación en  $F$ . Debería corroborarse que si  $D = \mathbb{Z}$  y  $[(a, b)]$  se considera como  $(a/b) \in \mathbb{Q}$ , estas definiciones aplicadas a  $\mathbb{Q}$  dan las operaciones usuales.

**Lema 26.2** *Para  $[(a, b)]$  y  $[(c, d)]$  en  $F$ , las ecuaciones*

$$[(a, b)] + [(c, d)] = [(ad + bc), bd]$$

y

$$[(a, b)][(c, d)] = [(ac, bd)]$$

*dan operaciones bien definidas de suma y multiplicación en  $F$ .*

**Demostración** Nótese, primero, que si  $[(a, b)]$  y  $[(c, d)]$  están en  $F$ , entonces  $(a, b)$  y  $(c, d)$  están en  $S$ , de modo que  $b \neq 0$  y  $d \neq 0$ . Como  $D$  es un dominio entero,  $bd \neq 0$  así que  $(ad + bc, bd)$  y  $(ac, bd)$  están en  $S$ . (Nótese aquí, el uso fundamental que se da a que  $D$  no tiene divisores de 0.) Esto muestra que los lados derechos de las definiciones están, al menos, en  $F$ .

Nos falta mostrar que estas operaciones de suma y multiplicación están bien definidas. Esto es, se definieron mediante representantes en  $S$  de elementos de  $F$ . Debemos mostrar que si se escogen diferentes representantes en  $S$ , resultará el mismo elemento de  $F$ . Para ello, supongamos que  $(a_1, b_1) \in [(a, b)]$  y  $(c_1, d_1) \in [(c, d)]$ . Debemos mostrar que

$$(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd)]$$

y que

$$(a_1c_1, b_1d_1) \in [(ac, bd)].$$

Ahora bien,  $(a_1, b_1) \in [(a, b)]$  significa que  $(a_1, b_1) \sim (a, b)$ , esto es,

$$a_1b = b_1a.$$

De manera análoga,  $(c_1, d_1) \in [(c, d)]$  implica que

$$c_1d = d_1c.$$

Multiplicando la primera ecuación por  $d_1d$  y la segunda por  $b_1b$  y sumando las ecuaciones resultantes, obtenemos la siguiente ecuación en  $D$ :

$$a_1bd_1d + c_1db_1b = b_1ad_1d + d_1cb_1b.$$

Usando diversos axiomas para un dominio entero, vemos que

$$(a_1d_1 + b_1c_1)bd = b_1d_1(ad + bc),$$

de modo que

$$(a_1d_1 + b_1c_1, b_1d_1) \sim (ad + bc, bd),$$

con lo cual,  $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd)]$ . Esto por lo que se refiere a la suma en  $F$ . Para la multiplicación en  $F$ , al multiplicar las ecuaciones  $a_1b = b_1a$  y  $c_1d = d_1c$ , obtenemos

$$a_1bc_1d = b_1ad_1c,$$

de modo que, usando axiomas de  $D$ , obtenemos

$$a_1c_1bd = b_1d_1ac,$$

lo cual implica que

$$(a_1c_1, b_1d_1) \sim (ac, bd).$$

Así,  $(a_1c_1, b_1d_1) \in [(ac, bd)]$ , lo cual completa la demostración. ■

Hay que asegurarse de que se *entiende* el significado del último lema y la necesidad de probarlo. Esto completa el paso 2.

**PASO 3** El paso 3 es bastante aburrido, pero es bueno que se trabajen algunos detalles. La razón es que no se podrán trabajar, a menos que se *entienda* lo que hemos hecho. Trabajar los detalles ayudará a comprender esta construcción. Esbozaremos lo que debemos probar y probaremos algunas cosas. El resto lo dejamos para los ejercicios.

1 La suma en  $F$  es conmutativa.

*Demostración* Ahora, por definición,  $[(a, b)] + [(c, d)]$  es  $[(ad + bc, bd)]$ . Además,  $[(c, d)] + [(a, b)]$  es, por definición,  $[(cb + da, db)]$ . Necesitamos mostrar que  $(ad + bc, bd) \sim (cb + da, db)$ . Esto es claro, pues  $ad + bc = cb + da$  y  $bd = db$ , por los axiomas de  $D$ . ■

- 2 La suma es asociativa.
- 3  $[(0, 1)]$  es una identidad para la suma en  $F$ .
- 4  $[(-a, b)]$  es un inverso aditivo para  $[(a, b)]$  en  $F$ .
- 5 La multiplicación en  $F$  es asociativa.
- 6 La multiplicación en  $F$  es conmutativa.
- 7 Las leyes distributivas valen en  $F$ .
- 8  $[(1, 1)]$  es una identidad multiplicativa en  $F$ .
- 9 Si  $[(a, b)] \in F$  no es la identidad aditiva, entonces  $a \neq 0$  en  $D$  y  $[(b, a)]$  es un inverso multiplicativo para  $[(a, b)]$ .

*Demostración* Sea  $[(a, b)] \in F$ . Si  $a = 0$ , entonces

$$a1 = b0 = 0,$$

de modo que

$$(a, b) \sim (0, 1),$$

esto es,  $[(a, b)] = [(0, 1)]$ . Pero, por la parte 3,  $[(0, 1)]$  es la identidad aditiva. Así, si  $[(a, b)]$  no es la identidad aditiva en  $F$ , tenemos  $a \neq 0$ , de manera que tiene sentido hablar de  $[(b, a)]$  en  $F$ . Ahora  $[(a, b)][(b, a)] = [(ab, ba)]$ . Pero en  $D$ , tenemos que  $ab = ba$  o  $(ab)1 = (ba)1$ , de modo que

$$(ab, ba) \sim (1, 1).$$

Así,

$$[(a, b)][(b, a)] = [(1, 1)],$$

y  $[(1, 1)]$  es la identidad multiplicativa, por la parte 8. ■

Esto completa el paso 3.

**PASO 4** Nos falta mostrar que  $F$  se puede considerar conteniendo  $D$ . Para ello, mostramos que existe un isomorfismo  $i$  de  $D$  con un subdominio de  $F$ . A continuación, cambiamos los nombres de la imagen de  $D$  bajo  $i$  usando los nombres de los elementos de  $D$  y habremos terminado. El lema siguiente nos da este isomorfismo.

**Lema 26.3** La transformación  $i: D \rightarrow F$  dada por  $ai = [(a, 1)]$  es un isomorfismo de  $D$  con un subdominio de  $F$ .

**Demostración** Para  $a$  y  $b$  en  $D$  tenemos

$$(a + b)i = [(a + b, 1)].$$

Además,

$$(ai) + (bi) = [(a, 1)] + [(b, 1)] = [(a1 + 1b, 1)] = [(a + b, 1)],$$

de modo que  $(a + b)i = (ai) + (bi)$ . Más aún,

$$(ab)i = [(ab, 1)],$$

mientras que

$$(ai)(bi) = [(a, 1)][(b, 1)] = [(ab, 1)],$$

así,  $(ab)i = (ai)(bi)$ .

Falta mostrar que  $i$  es uno a uno. Si  $ai = bi$ , entonces

$$[(a, 1)] = [(b, 1)],$$

de modo que  $(a, 1) \sim (b, 1)$  que da  $a1 = 1b$ , esto es,

$$a = b.$$

Así,  $i$  es un isomorfismo de  $D$  con  $Di$  y, por supuesto,  $Di$  es, entonces, un subdominio de  $F$ . ■

Como claramente se cumple en  $F$  que  $[(a, b)] = [(a, 1)][(1, b)] = [(a, 1)]/[(b, 1)] = ai/bi$ , hemos probado el siguiente teorema.

**Teorema 26.1** Cualquier dominio entero  $D$  puede agrandarse (o incrustarse) en un campo  $F$ , tal que todo elemento de  $F$  puede expresarse como cociente de dos elementos de  $D$ . (Dicho campo  $F$  es un campo de cocientes de  $D$ .)

## 26.2 UNICIDAD

Al principio dijimos que  $F$  podría considerarse, en algún sentido, como un campo minimal contenido en  $D$ . Esto es bastante obvio, pues todo campo que contiene  $D$  debe contener todos los elementos  $a/b$  para toda  $a, b \in D$  con  $b \neq 0$ . El siguiente teorema mostrará que todo campo que contiene  $D$ , contiene un subcampo de cocientes de  $D$  y dos campos de cocientes de  $D$  son isomorfos.

**Teorema 26.2** Sea  $F$  un campo de cocientes de  $D$  y sea  $L$  cualquier campo que contenga  $D$ . Entonces, existe una transformación  $\psi : F \rightarrow L$  que da un isomorfismo de  $F$  con un subcampo de  $L$  tal que  $a\psi = a$  para  $a \in D$ .

**Demostración** El diagrama reticular y el de la transformación en la figura 26.1 pueden ayudar a visualizar la situación de este teorema.

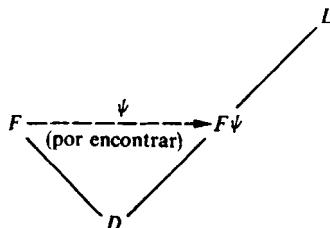


Figura 26.1

Un elemento de  $F$  es de la forma  $a/Fb$  donde  $/F$  denota el cociente de  $a \in D$  por  $b \in D$  considerados como elementos de  $F$ . Claramente, deseamos transformar  $a/Fb$  sobre  $a/Lb$  donde  $/L$  denota el cociente de elementos en  $L$ . Esto es tan trivial, que se podría pensar que hay trampa al definir la transformación  $\psi$ , pero lo haremos de cualquier manera.

Debemos definir  $\psi : F \rightarrow L$ , comenzamos definiendo

$$a\psi = a \quad \text{para} \quad a \in D.$$

Toda  $x \in F$  es un cociente  $a/Fb$  de algunos dos elementos  $a$  y  $b$ ,  $b \neq 0$ , de  $D$ . Tratemos de definir  $\psi$  por

$$(a/Fb)\psi = (a\psi)/_L(b\psi).$$

Primero debemos mostrar que esta transformación  $\psi$  es sensata y está bien definida. Como  $\psi$  es la identidad en  $D$ , para  $b \neq 0$  tenemos  $b\psi \neq 0$ ; así, nuestra definición de  $(a/Fb)\psi$  como  $(a\psi)/_L(b\psi)$  tiene sentido. Si  $a/Fb = c/Fd$  en  $F$ , entonces  $ad = bc$  en  $D$ , de modo que  $(ad)\psi = (bc)\psi$ . Pero como  $\psi$  es la identidad en  $D$ ,

$$(ad)\psi = (a\psi)(d\psi) \quad \text{y} \quad (bc)\psi = (b\psi)(c\psi).$$

Así,

$$(a\psi)/_L(b\psi) = (c\psi)/_L(d\psi)$$

en  $L$ , de modo que  $\psi$  está bien definida.

Las ecuaciones

$$(xy)\psi = (x\psi)(y\psi)$$

y

$$(x + y)\psi = x\psi + y\psi$$

se siguen fácilmente de la definición de  $\psi$  en  $F$  y del hecho de que  $\psi$  es la identidad en  $D$ .

Si  $(a_F b)\psi = (c_F d)\psi$ , tenemos

$$(a\psi)_L(b\psi) = (c\psi)_L(d\psi)$$

de modo que

$$(a\psi)(d\psi) = (b\psi)(c\psi).$$

Como  $\psi$  es la identidad en  $D$ , concluimos que  $ad = bc$ , por tanto,  $a_F b = c_F d$ . Así,  $\psi$  es uno a uno.

Por definición,  $a\psi = a$  para  $a \in D$ . ■

**Corolario** *Todo campo  $L$  que contiene a un dominio entero  $D$ , contiene al campo de cocientes de  $D$ .*

**Demostración** En la demostración del teorema 26.2, todo elemento del subcampo  $F\psi$  de  $L$  es un cociente en  $L$  de elementos de  $D$ . ■

**Corolario** *Cualesquiera dos campos de cocientes de un dominio entero  $D$  son isomorfos.*

**Demostración** En el teorema 26.2, supóngase que  $L$  es un campo de cocientes de  $D$ , de modo que todo elemento  $x$  de  $L$  puede expresarse en la forma  $a_L/b$  para  $a, b \in D$ . Entonces,  $L$  es el campo  $F\psi$  de la demostración del teorema 26.2 y es, así, isomorfo a  $F$ . ■

## Ejercicios

---

**26.1** Describase el campo  $F$  de cocientes del subdominio entero

$$D = \{n + mi \mid n, m \in \mathbb{Z}\}$$

de  $\mathbb{C}$ . «Describir» significa dar los elementos de  $\mathbb{C}$  que forman el campo de cocientes de  $D$  en  $\mathbb{C}$ .

**26.2** Describase (en el sentido del ejercicio 26.1) el campo  $F$  de cocientes del subdominio entero  $D = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$  de  $\mathbb{R}$ .

**26.3** Muéstrese, mediante un ejemplo, que un campo  $F'$  de cocientes de un subdominio propio  $D'$  de un dominio entero  $D$  también puede ser campo de cociente de  $D$ .

**†26.4** Pruébese la parte 7 del paso 3. Puede suponerse cualquier parte anterior al paso 3.

**26.5** ¿Falso o verdadero?

- a)  $\mathbb{Q}$  es un campo de cocientes de  $\mathbb{Z}$ .
- b)  $\mathbb{R}$  es un campo de cocientes de  $\mathbb{Z}$ .
- c)  $\mathbb{R}$  es un campo de cocientes de  $\mathbb{R}$ .
- d)  $\mathbb{C}$  es un campo de cocientes de  $\mathbb{R}$ .

- e) Si  $D$  es un campo, entonces, cualquier campo de cocientes de  $D$  es isomorfo a  $D$ .
  - f) El hecho de que  $D$  no tenga divisores de 0 se usó muchas veces en la construcción de un campo  $F$  de cocientes del dominio entero  $D$ .
  - g) Todo elemento de un dominio entero  $D$  es una unidad en un campo  $F$  de cocientes de  $D$ .
  - h) Todo elemento distinto de cero de un dominio entero  $D$  es una unidad en un campo  $F$  de cocientes de  $D$ .
  - i) Un campo de cocientes  $F'$  de un subdominio  $D'$  de un dominio entero  $D$  puede considerarse un subcampo de algún campo de cocientes de  $D$ .
  - j) Todo campo de cocientes de  $\mathbb{Z}$  es isomorfo a  $\mathbb{Q}$ .
- 

**26.6** Pruébese la parte 2 del paso 3. Puede suponerse cualquier parte anterior al paso 3.

**26.7** Pruébese la parte 3 del paso 3. Puede suponerse cualquier parte anterior al paso 3.

**26.8** Pruébese la parte 4 del paso 3. Puede suponerse cualquier parte anterior al paso 3.

**26.9** Pruébese la parte 5 del paso 3. Puede suponerse cualquier parte anterior al paso 3.

**26.10** Pruébese la parte 6 del paso 3. Puede suponerse cualquier parte anterior al paso 3.

**26.11** Sea  $R$  un anillo conmutativo y  $T \neq \{0\}$  un subconjunto no vacío de  $R$  cerrado bajo la multiplicación, sin divisores de 0. Comenzando con  $R \times T$  y siguiendo exactamente la construcción dada en este capítulo, podemos mostrar que se puede agrandar el anillo  $R$  hasta un *anillo parcial de cocientes*  $Q(R, T)$ . Piénsese en ello durante aproximadamente quince minutos; vuélvase sobre la construcción y véase por qué funciona. En particular, muéstrese lo siguiente:

- a)  $Q(R, T)$  tiene unitario aunque  $R$  no lo tenga.
- b) En  $Q(R, T)$  todo elemento de  $T$  distinto de cero es una unidad.

**26.12** Pruébese, a partir del ejercicio 26.11, que todo anillo conmutativo que contenga algún elemento  $a$  que no sea divisor de 0 puede agrandarse hasta un anillo conmutativo con unitario. Compárese con el ejercicio 24.16.

**26.13** Con respecto al ejercicio 26.11, ¿cuántos elementos hay en el anillo  $Q(\mathbb{Z}_4, \{1, 3\})$ ?

**26.14** Con respecto al ejercicio 26.11, descríbese el anillo  $Q(\mathbb{Z}, \{2^n \mid n \in \mathbb{Z}^+\})$  describiendo al subanillo de  $\mathbb{R}$  al cual es isomorfo.

**26.15** Con respecto al ejercicio 26.11, descríbese el anillo  $Q(3\mathbb{Z}, \{6^n \mid n \in \mathbb{Z}^+\})$  describiendo el subanillo de  $\mathbb{R}$  al cual es isomorfo.

**26.16** Con respecto al ejercicio 26.11, supóngase que anulamos la condición de que  $T$  no tiene divisores de cero y sólo se requiere, que el conjunto no vacío  $T \neq \{0\}$  sea cerrado bajo la multiplicación. El intento de agrandar  $R$  a un anillo conmutativo unitario, en el cual todo elemento de  $T$  distinto de cero sea unidad, puede fallar, si  $T$  contiene algún elemento  $a$  que sea divisor de 0, pues un divisor de 0 no puede ser, además, unidad. ¿Dónde se encuentra la primera dificultad al hacer una construcción paralela a la del texto, pero comenzando con  $R \times T$ ? En particular, para  $R = \mathbb{Z}_6$  y  $T = \{1, 2, 4\}$ , ilústrese la primera dificultad encontrada. [Sugerencia: está en el paso 1.]

## Nuestro objetivo fundamental

Este capítulo está diseñado para exponer una perspectiva adecuada de las partes no marcadas con asterisco del resto del libro. No hay ejercicios.

Los dos capítulos siguientes tratan temas de la teoría de anillos, análogos al material sobre grupos factores y homomorfismos en la teoría de grupos. Sin embargo, nuestro objetivo, al desarrollar estos conceptos, es diferente de nuestros objetivos en la teoría de grupos. En la teoría de grupos usamos (en parte en las secciones con asterisco) los conceptos de grupos factores y homomorfismos para estudiar la estructura de un grupo dado y para determinar los tipos de estructuras de grupo de ciertos órdenes que podrían existir. Disculpándonos con los matemáticos profesionales, explicaremos ahora, en términos conocidos y que se consideran sencillos, nuestro propósito al desarrollar esta construcción análoga para los anillos.

*Todo el material sin asteriscos del resto del libro está dedicado a encontrar y estudiar soluciones de ecuaciones polinomiales como*

$$x^2 + x - 6 = 0.$$

Hablemos por un momento acerca de este objetivo, a la luz de la historia de las matemáticas.

Comencemos remontándonos a la escuela pitagórica de matemáticas, alrededor del año 525 a. de J.C. Los pitagóricos afirmaban, con un fervor casi fanático, que todas las distancias son **commensurables**, esto es, que dadas las distancias  $a$  y  $b$ , debería existir una unidad de distancia  $u$  y enteros  $n$  y  $m$  tales que  $a = (n)(u)$  y  $b = (m)(u)$ . Entonces, en términos de números, al considerar  $u$  como unidad de distancia, sostenían que todos los números son enteros. Esta idea de commensurabilidad puede reformularse, de acuerdo con nuestro pensamiento, como la afir-

mación de que todos los números son racionales, pues si  $a$  y  $b$  son números racionales, entonces cada uno es un múltiplo entero del recíproco del mínimo común múltiplo de sus denominadores. Por ejemplo, si  $a = \frac{7}{12}$  y  $b = \frac{19}{15}$ , entonces  $a = (35)(\frac{1}{60})$  y  $b = (76)(\frac{1}{60})$ .

Obviamente, los pitagóricos conocían lo que hoy se llama *teorema de Pitágoras*, esto es, que para un triángulo rectángulo con catetos de longitud  $a$  y  $b$  e hipotenusa de longitud  $c$ , tenemos que

$$a^2 + b^2 = c^2.$$

Tuvieron que admitir también la existencia de la hipotenusa de un triángulo rectángulo con dos catetos de igual longitud, de digamos, una unidad cada uno. Como sabemos, la hipotenusa de dicho triángulo rectángulo tendría longitud  $\sqrt{2}$ . Imaginen entonces su consternación, desaliento e incluso furia cuando algún miembro de su sociedad —según algunas versiones fue el mismo Pitágoras— anunció el penoso hecho que se enuncia, según nuestra terminología, en el teorema siguiente.

**Teorema 27.1** *La ecuación  $x^2 = 2$  no tiene solución en los números racionales. Por tanto,  $\sqrt{2}$  no es un número racional.*

**Demostración** Supóngase que  $m/n$  para  $m, n \in \mathbb{Z}$  es un número racional tal que  $(m/n)^2 = 2$ . Entonces,

$$m^2 = 2n^2,$$

donde tanto  $m^2$  como  $2n^2$  son enteros. Como  $m^2$  y  $2n^2$  son el mismo entero y como 2 es un factor de  $2n^2$ , vemos que 2 debe ser uno de los factores de  $m^2$ . Pero, por ser un cuadrado,  $m^2$  tiene como factores los mismos de  $m$  repetidos dos veces. Así,  $m^2$  debe tener dos factores 2. Entonces,  $2n^2$  tiene dos factores 2, así que  $n^2$  debe tener 2 como factor. Pero, por ser un cuadrado,  $n^2$  debe tener dos factores 2. Por lo que  $2n^2$  tiene tres factores 2. Pero entonces,  $m^2$  debe tener tres factores 2 y de aquí, por ser cuadrado, debe tener cuatro factores 2. Pero, entonces,  $2n^2$  debe tener al menos cuatro factores 2 y por tanto . . . Yendo y viniendo así de  $m^2$  a  $n^2$  caemos en una situación imposible. Hemos demostrado, por contradicción, que  $2 \neq (m/n)^2$  para  $m, n \in \mathbb{Z}$ . Se puede hacer la deducción más concisa y elegante, pero no estamos de humor para ello. ■

Así, los pitagóricos fueron directo a la cuestión de la solución de una ecuación polinomial,  $x^2 - 2 = 0$ . Remitimos al estudiante a Shanks [35, capítulo 3] para un animado y absolutamente delicioso relato de este dilema pitagórico y su importancia en matemáticas.

En la motivación de la definición de grupo, comentamos la necesidad de tener números negativos, para que ecuaciones como  $x + 2 = 0$  tuvieran solución.

La presentación de los números negativos causó cierta consternación en algunos círculos filosóficos. Uno puede imaginar 1 manzana, 2 manzanas y aún  $\frac{13}{11}$  de manzana, pero, ¿cómo es posible señalar algo y decir que es  $-17$  manzanas? Por último, considerar la ecuación  $x^2 + 1 = 0$  condujo a la presentación del número  $i$ . El solo nombre de «número imaginario» dado a  $i$  muestra cómo se le consideró. Incluso ahora, este nombre hace que muchos estudiantes vean a  $i$  con cierta suspicacia. Los números negativos se presentan a tan temprana edad en el desarrollo matemático del alumno, que se aceptan sin cuestionarlos.

Hasta aquí la historia. Reiteramos:

*Las partes sin asterisco del resto del libro se dedican a encontrar y estudiar soluciones de ecuaciones polinomiales.*

Por primera vez vieron polinomios en álgebra de secundaria. Ahí, lo primero fue aprender a sumar, multiplicar y factorizar polinomios. Después, en los cursos posteriores de álgebra se puso un énfasis considerable en resolver ecuaciones polinomiales. Estos serán, precisamente, los temas que nos ocuparán. La diferencia está en que, en la secundaria, sólo se consideraban polinomios con coeficientes en los números reales, mientras que aquí trabajaremos con polinomios cuyos coeficientes forman cualquier campo arbitrario dado.

Como ya dijimos, los dos capítulos siguientes tratan de anillos factores y homomorfismos de anillos, material análogo, formalmente, a lo que hemos hecho acerca de grupos factores y homomorfismos de grupo. Ni siquiera se mencionarán los polinomios. Después, introduciremos polinomios y demostraremos cómo puede plantearse la idea de resolver una ecuación polinomial, en términos del lenguaje de homomorfismos. No se asusten con la terminología. Recuerden siempre que:

*Haremos lo mismo que en álgebra de secundaria, pero en un contexto más general.*

Y después, con una facilidad, elegancia, belleza y elaboración asombrosas, como estrella brillante que aparece súbitamente en su opaca vida matemática, alcanzaremos nuestro

**Objetivo fundamental:** *Mostrar que dada cualquier ecuación polinomial de grado  $\geq 1$ , donde los coeficientes del polinomio pueden ser de cualquier campo, existe una solución de la ecuación.*

Si piensan que todo esto es ridículo, piensen en la historia. *Esta es la culminación de más de 2000 años de esfuerzo matemático en el trabajo con ecuaciones polinomiales.* Después de alcanzar nuestro *objetivo fundamental*, emplearemos el resto en estudiar la naturaleza de estas soluciones de ecuaciones polinomiales. Insistimos en que no deben tener miedo al estudiar este material. *Trataremos temas conocidos de álgebra de secundaria. Este trabajo debería parecerles mucho más natural que la teoría de grupos.*

Para concluir, señalamos que esta maquinaria de anillos factores y homomorfismos de anillos no es estrictamente necesaria para alcanzar nuestro *objetivo fundamental*. Para una demostración directa, véase Artin [26, pág. 29]. Sin embargo, los anillos factores y los homomorfismos de anillos son ideas básicas que el lector debería comprender, y nuestro *objetivo fundamental* se desprenderá fácilmente una vez que las dominen. Además, usaremos eficazmente estos conceptos en el estudio de las propiedades de soluciones de ecuaciones polinomiales.

# Anillos cocientes e ideales

## 28.1 INTRODUCCION

El capítulo comienza con el estudio de anillos análogo al material acerca de grupos de los capítulos 11, 12 y 13, sobre grupos factores y homomorfismos. Como  $\langle R, + \rangle$  es un grupo para todo anillo  $R$ , de hecho,  $\langle R, + \rangle$  es un grupo abeliano, la parte aditiva de esta teoría ya está hecha. Sólo debemos ocuparnos de sus aspectos multiplicativos. Para hacer que la analogía con la situación para grupos sea lo más clara posible, desarrollaremos esta teoría de acuerdo con el mismo plan que usamos para grupos. Así, daremos otra oportunidad para dominarla.

Sea  $R$  un anillo. Nos ocupamos del estudio de una partición de  $R$  en subconjuntos ajenos o celdas, tal que estas celdas puedan considerarse elementos en un anillo donde *ambas* operaciones de suma y multiplicación de celdas son operaciones inducidas de  $R$ . Esto es, deseamos definir *ambas* operaciones, escogiendo representantes de las celdas, sumar o multiplicar, en  $R$ , estos representantes y *definir* suma o el producto de celdas, como la celda donde se halle la suma o producto de los representantes. *Ambas* operaciones deben estar *bien definidas*, esto es, ser independientes de la selección de representantes de las celdas.

**Teorema 28.1 (Análogo del teorema 11.1)** *Si un anillo  $R$  se puede partir en celdas con las dos operaciones inducidas descritas arriba bien definidas, y si las celdas forman un anillo bajo estas operaciones inducidas, entonces la celda que contiene la identidad aditiva  $0$  de  $R$  debe ser un subgrupo aditivo  $N$  del grupo aditivo  $\langle R, + \rangle$ . Además,  $N$  debe tener la propiedad adicional de que para todas las  $r \in R$  y  $n \in N$ , tanto  $rn \in N$ , como  $nr \in N$ . Expresamos esta última condición como  $rN \subseteq N$  y  $Nr \subseteq N$ .*

**Demostración** Considerando  $\langle R, + \rangle$  como grupo bajo la suma, sabemos, del teorema 11.1, que  $N$  debe ser un subgrupo aditivo de  $\langle R, + \rangle$ . En efecto, sabemos, del trabajo posterior al teorema 11.1, que  $N$  debe ser un subgrupo aditivo normal de  $\langle R, + \rangle$ , pero como la suma en  $R$  es conmutativa, todo subgrupo aditivo de  $\langle R, + \rangle$  es normal en  $\langle R, + \rangle$ .

Sólo necesitamos mostrar que para  $r \in R$  tenemos  $rN \subseteq N$  y  $Nr \subseteq N$ . Sea  $r \in R$ . Ahora bien,  $r$  está en alguna celda  $A \subseteq R$  y, por la hipótesis de que la multiplicación inducida de celdas está bien definida, podemos calcular los productos  $AN$  y  $NA$  escogiendo cualesquiera representantes. Escojamos  $r \in A$  y  $0 \in N$ . Entonces,  $AN$  y  $NA$  son las celdas que contienen a  $r0 = 0r = 0$ , esto es,  $AN = NA = N$ . Por tanto, para todos los representantes  $n \in N$  tenemos  $rn \in N$  y  $nr \in N$ . ■

## 28.2 CRITERIOS PARA LA EXISTENCIA DE UN ANILLO DE CLASES LATERALES

**Teorema 28.2 (Análogo del teorema 11.2)** *Si un anillo  $R$  se puede partir en celdas con ambas operaciones inducidas bien definidas y formando anillos, entonces las celdas deben ser precisamente las clases laterales izquierdas (y también las derechas) con respecto a la suma del subgrupo aditivo  $\langle N, + \rangle$  de  $\langle R, + \rangle$  donde  $N$  es la celda que contiene 0.*

**Demostración** La demostración del teorema 28.2 es inmediata a partir del teorema 11.2, si consideramos sólo  $\langle R, + \rangle$  como un grupo aditivo y nos olvidamos de la multiplicación. ■

Claramente, también se cumple aquí el teorema 11.3, esto es, estas clases laterales son ajenas. Como la suma es conmutativa, la clase lateral izquierda  $r + N$  es la misma que la clase lateral derecha  $N + r$ .

**Lema 28.1 (Análogo del lema 12.1)** *Si  $\langle N, + \rangle$  es un subgrupo aditivo de  $\langle R, + \rangle$  para un anillo  $R$  y si las operaciones inducidas de suma y multiplicación de clases laterales  $r + N$  para  $r \in R$  están bien definidas, esto es, son independientes de la selección de representantes, entonces, la colección de estas clases laterales  $r + N$  es un anillo bajo estas operaciones inducidas de clases laterales.*

**Demostración** El lema 12.1 muestra que las clases laterales forman grupo bajo la suma inducida. Los axiomas de anillo que incluyen la multiplicación se cumplen, puesto que también calculamos los productos escogiendo representantes y porque los axiomas de anillos valen en  $R$ . Por ejemplo, la ley distributiva izquierda

$$\begin{aligned} (r_1 + N)[(r_2 + N) + (r_3 + N)] &= \\ &= [(r_1 + N)(r_2 + N)] + [(r_1 + N)(r_3 + N)] \end{aligned}$$

se sigue, cuando escogemos a  $r_i \in (r_i + N)$  como representantes y observamos que el requisito

$$r_1(r_2 + r_3) \in [(r_1r_2 + r_1r_3) + N]$$

es cierto, pues  $r_1(r_2 + r_3) = (r_1r_2 + r_1r_3)$  por la ley distributiva izquierda en  $R$ . La otra ley distributiva y la ley asociativa para la multiplicación resultan de manera análoga. ■

**Teorema 28.3 (Análogo del teorema 12.1)** *Si  $\langle N, + \rangle$  es un subgrupo aditivo del grupo aditivo  $\langle R, + \rangle$  de un anillo  $R$ , entonces las operaciones de suma y multiplicación inducida están, ambas, bien definidas en las clases laterales  $r + N$  para  $r \in R$  si y sólo si  $rN \subseteq N$  y  $Nr \subseteq N$  para todas las  $r \in R$ .*

*Demostración* El hecho de que, si las operaciones están bien definidas, entonces  $rN \subseteq N$  y  $Nr \subseteq N$  resulta inmediatamente del lema 28.1 y del teorema 28.1.

Supóngase que  $\langle N, + \rangle$  es un subgrupo aditivo de  $\langle R, + \rangle$  tal que para todas las  $r \in R$  tenemos  $rN \subseteq N$  y  $Nr \subseteq N$ . Por el teorema 12.1 aplicado al subgrupo  $\langle N, + \rangle$  de  $\langle R, + \rangle$ , la suma de clases laterales está bien definida. Para la multiplicación, debemos mostrar que un producto  $(r_1 + N)(r_2 + N)$ , calculado mediante la selección de representantes, está bien definido. No se pierde generalidad al tomar, como dos representantes de  $r_1 + N$ , al elemento  $r_1$  mismo y a  $r_1 + n_1$  para  $n_1 \in N$ . Análogamente, sean  $r_2$  y  $r_2 + n_2$  dos elementos de  $r_2 + N$ . Debemos mostrar que  $(r_1 + n_1)(r_2 + n_2)$  está en la misma clase lateral  $r_1r_2 + N$  que  $r_1r_2$ . Ahora, por las leyes distributivas en  $R$ ,

$$(r_1 + n_1)(r_2 + n_2) = r_1r_2 + n_1n_2 + n_1r_2 + r_1n_2.$$

La hipótesis de que  $rN \subseteq N$  y  $Nr \subseteq N$  implica que  $r_1n_2 \in N$  y que  $n_1r_2 \in N$ . Considerando  $r_1$  como elemento de  $R$ , tenemos que  $n_1n_2 \in n_1N$  y  $n_1N \subseteq N$ , de modo que también  $n_1n_2 \in N$ . Entonces, como  $\langle N, + \rangle$  es un subgrupo aditivo de  $\langle R, + \rangle$ , vemos que  $(n_1r_2 + r_1n_2 + n_1n_2) \in N$ , de modo que  $(r_1 + n_1)(r_2 + n_2) \in (r_1r_2 + N)$ . ■

Es claro ahora que estos subgrupos aditivos particulares  $\langle N, + \rangle$  de un anillo  $R$  que tengan la propiedad de que  $rN \subseteq N$  y  $Nr \subseteq N$  para todas las  $r \in R$  desempeñarán un papel de fundamental importancia en la teoría de anillos, análogo al papel de un subgrupo normal en un grupo. Nótese que las condiciones  $rN \subseteq N$  y  $Nr \subseteq N$  implican, en particular para  $r \in N$ , que  $N$  es cerrado bajo la multiplicación de  $R$ . Así, podemos considerar  $N$ , con la suma y multiplicación inducida de  $R$ , como un subanillo de  $R$ . Sin embargo, no todo subanillo de todo anillo  $R$  satisface las condiciones  $rN \subseteq N$  y  $Nr \subseteq N$ . Por ejemplo,  $\mathbf{Q} \leq \mathbf{R}$ , pero  $\pi\mathbf{Q} \notin \mathbf{Q}$ .

## 28.3 IDEALES Y ANILLOS COCIENTES

**Definición (Análogo de la definición de un subgrupo normal)** Un subgrupo aditivo  $\langle N, + \rangle$  de un anillo  $R$  que satisface  $rN \subseteq N$  y  $Nr \subseteq N$  para todas las  $r \in R$  es un *ideal* (o un *ideal bilateral*) de  $R$ . Un subgrupo  $\langle N, + \rangle$  de  $R$  que satisface  $rN \subseteq N$  para todas las  $r \in R$  es un *ideal izquierdo de  $R$*  y uno que satisface  $Nr \subseteq N$  para todas las  $r \in R$  es un *ideal derecho de  $R$* .

Cuando nos referimos a un *ideal*, siempre lo supondremos un ideal bilateral. Los ideales izquierdos o derechos que no sean bilaterales no nos interesan. Reiteramos:

*Un ideal es a un anillo lo que un subgrupo normal es a un grupo.*

**Definición (Análogo de la definición de grupo factor)** Si  $N$  es un ideal en un anillo  $R$ , entonces, el anillo de las clases laterales  $r + N$  bajo las operaciones inducidas es el *anillo cociente*, o el *anillo factor*, o el *anillo de las clases residuales de  $R$  módulo  $N$* , y se denota por  $R/N$ . Las clases laterales son las *clases residuales módulo  $N$* .

**Ejemplo 28.1** Considérese el anillo  $\mathbf{Z}$ . Los únicos subgrupos aditivos de  $\langle \mathbf{Z}, + \rangle$  son, como hemos visto, los subgrupos  $n\mathbf{Z}$ . Claramente, si  $r$  es cualquier entero y  $m \in n\mathbf{Z}$ , entonces  $rm = mr$  es, de nuevo, un múltiplo de  $n$ , esto es, si  $m = ns$ , entonces,  $rm = mr = n(sr)$  y  $n(sr) \in n\mathbf{Z}$ . Así,  $n\mathbf{Z}$  es un ideal y las clases laterales  $a + n\mathbf{Z}$  de  $n\mathbf{Z}$  forman un anillo  $\mathbf{Z}/n\mathbf{Z}$  bajo las operaciones inducidas de suma y multiplicación. ■

En el ejemplo 23.2, definimos para  $a$  y  $b$  en  $\mathbf{Z}_n$ , el producto  $ab$  módulo  $n$  como el residuo cuando se divide entre  $n$  el producto usual de  $a$  y  $b$  en  $\mathbf{Z}$ . La transformación  $\phi : \mathbf{Z}_n \rightarrow \mathbf{Z}/n\mathbf{Z}$  dada por

$$a\phi = a + n\mathbf{Z}$$

claramente es una transformación uno a uno y sobre, tal que  $(a + b)\phi = a\phi + b\phi$  y  $(ab)\phi = (a\phi)(b\phi)$ . Entonces,  $\mathbf{Z}_n$  bajo la suma y la multiplicación módulo  $n$ , puede verse como  $\mathbf{Z}/n\mathbf{Z}$  con diferentes nombres y, por tanto, es un anillo bajo esta suma y multiplicación. Usamos este hecho en las secciones anteriores, con el comentario de que se justificaría más adelante en una situación general. *Esta es la justificación.* Con frecuencia, identificamos  $\mathbf{Z}/n\mathbf{Z}$  con  $\mathbf{Z}_n$  mediante este isomorfismo  $\phi$ , el cual es un isomorfismo natural o canónico.

**Ejemplo 28.2** Como se mostró en el corolario el teorema 24.4,  $\mathbf{Z}_p$ , que es isomorfo a  $\mathbf{Z}/p\mathbf{Z}$ , es un campo para un  $p$  primo. *Así, un anillo cociente de un dominio entero puede ser campo.* Diremos más acerca de esto en el capítulo siguiente. ■

**Ejemplo 28.3** Se ve fácilmente que el subconjunto  $N = \{0, 3\}$  de  $\mathbf{Z}_6$  es un ideal de  $\mathbf{Z}_6$  y  $\mathbf{Z}_6/N$  tiene tres elementos,  $0 + N$ ,  $1 + N$  y  $2 + N$ . Es obvio que se suman y multiplican de manera tal que se tiene que  $\mathbf{Z}_6/N \simeq \mathbf{Z}_3$  bajo la correspondencia

$$(0 + N) \leftrightarrow 0, \quad (1 + N) \leftrightarrow 1, \quad (2 + N) \leftrightarrow 2. \blacksquare$$

**Ejemplo 28.4** El anillo  $\mathbf{Z} \times \mathbf{Z}$  no es un dominio entero, pues

$$(0, 1)(1, 0) = (0, 0),$$

muestra que  $(0, 1)$  y  $(1, 0)$  son divisores de 0. Si  $N = \{(0, n) \mid n \in \mathbf{Z}\}$  es claro que  $N$  es un ideal de  $\mathbf{Z} \times \mathbf{Z}$  y que  $(\mathbf{Z} \times \mathbf{Z})/N$  es isomorfo a  $\mathbf{Z}$  bajo la correspondencia  $[(m, 0) + N] \leftrightarrow m$ , las clases residuales son de la forma  $(m, 0) + N$ , donde  $m \in \mathbf{Z}$ . Así, un anillo cociente de un anillo puede ser un dominio entero, aunque el anillo original no lo sea. Diremos más acerca de esto en la siguiente sección. ■

Los ejemplos anteriores señalan la gran importancia de los conceptos de ideales y de anillos cocientes. Todo anillo  $R$  tiene dos ideales, el **ideal impropio**  $R$  y el **ideal trivial**  $\{0\}$ . Para estos ideales, los anillos factores son  $R/R$ , que tiene un solo elemento y  $R/\{0\}$ , el cual es claramente isomorfo a  $R$ . Estos casos no son interesantes. Igual que para un subgrupo de un grupo, un **ideal no trivial propio** de un anillo  $R$  es un ideal  $N$  de  $R$  tal que  $N \neq R$  y  $N \neq \{0\}$ .

Mientras que los anillos cocientes de anillos y los dominios enteros pueden ser de gran interés, como lo indican los ejemplos anteriores, el corolario del siguiente y último teorema de esta sección, muestra que un anillo cociente de un campo no tiene mayor utilidad.

**Teorema 28.4** Si  $R$  es un anillo con unitario y  $N$  es un ideal de  $R$  que contiene una unidad, entonces  $N = R$ .

**Demostración** Sea  $N$  un ideal de  $R$ , supóngase que  $u \in N$  para alguna unidad  $u$  en  $R$ . Entonces, la condición  $rN \subseteq N$  para todas las  $r \in R$  implica, si tomamos  $r = u^{-1}$  y  $u \in N$ , que  $1 = u^{-1}$  está en  $N$ . Pero entonces,  $rN \subseteq N$ , para todas las  $r \in R$ , implica que  $rl = r$  está en  $N$  para todas las  $r \in R$ , de modo que  $N = R$ .

**Corolario** Un campo no contiene ideales propios no triviales.

**Demostración** Como todo elemento distinto de cero de un campo es una unidad, se sigue del teorema 28.4, que un ideal de un campo  $F$  es  $\{0\}$  o todo  $F$ . ■

## Ejercicios

28.1 Encuéntrense todos los ideales  $N$  de  $\mathbf{Z}_{12}$ . En cada caso, calcúlese  $\mathbf{Z}_{12}/N$ , esto es, encuéntrese un anillo conocido al cual sea isomorfo el anillo cociente.

**28.2** Dense las tablas de suma y multiplicación para  $2\mathbb{Z}/8\mathbb{Z}$ . ¿Son anillos isomorfos  $2\mathbb{Z}/8\mathbb{Z}$  y  $\mathbb{Z}_4$ ?

**28.3** Encuéntrese un subanillo del anillo  $\mathbb{Z} \times \mathbb{Z}$  que no sea un ideal de  $\mathbb{Z} \times \mathbb{Z}$ .

**28.4** Se pide a un estudiante que pruebe que un anillo cociente de un anillo  $R$  módulo un ideal  $N$  es comutativo si y sólo si  $(rs - sr) \in N$  para todas las  $r, s \in R$ . El estudiante comienza:

Supóngase que  $R/N$  es comutativo. Entonces,  $rs = sr$  para todas las  $r, s \in R/N$ .

- ¿Por qué el profesor que lea esto espera encontrar tonterías de aquí en adelante?
- ¿Qué debería haber escrito el estudiante?
- Pruébese la afirmación. ( Nótese el «si y sólo si».)

**28.5** ¿Falso o verdadero?

- a)  $\mathbb{Q}$  es un ideal en  $\mathbb{R}$ .
  - b) Todo ideal de un anillo es un subanillo del anillo.
  - c) Todo subanillo de un anillo es un ideal del anillo.
  - d) Todo anillo cociente de un anillo comutativo es, de nuevo, un anillo comutativo.
  - e) Los anillos  $\mathbb{Z}/4\mathbb{Z}$  y  $\mathbb{Z}_4$  son isomorfos.
  - f) Un ideal  $N$  en un anillo con unitario  $R$  es todo  $R$  si y sólo si  $1 \in N$ .
  - g) El concepto de ideal es al concepto de anillo lo que el concepto de subgrupo normal es al concepto de grupo.
  - h)  $\mathbb{Z}_4$  es un ideal de  $4\mathbb{Z}$ .
  - i) Si un anillo  $R$  tiene divisores de 0, entonces todo anillo cociente de  $R$  tiene divisores de 0.
  - j)  $\mathbb{Z}$  es un ideal en  $\mathbb{Q}$ .
- 

**28.6** Muéstrese que un anillo factor de un campo es el anillo trivial de un elemento o es isomorfo al campo.

**28.7** Muéstrese que si  $R$  es un anillo con unitario y  $N$  es un ideal de  $R$  tal que  $N \neq R$ , entonces  $R/N$  es un anillo con unitario  $\neq 0$ .

**28.8** Sea  $R$  un anillo comutativo y sea  $a \in R$ . Muéstrese que  $I_a = \{x \in R \mid ax = 0\}$  es un ideal de  $R$ .

**28.9** Muéstrese que la intersección de ideales de un anillo  $R$  es, de nuevo, un ideal de  $R$ .

**28.10** Determínense todos los ideales de  $\mathbb{Z} \times \mathbb{Z}$ .

**28.11** Un elemento  $a$  de un anillo  $R$  es **nilpotente** si  $a^n = 0$  para algún  $n \in \mathbb{Z}^+$ . Muéstrese que la colección de todos los elementos nilpotentes en un anillo comutativo  $R$  es un ideal, el **radical de  $R$** .

**28.12** Con referencia a la definición dada en el ejercicio 28.11, encuéntrese el radical del anillo  $\mathbb{Z}_{12}$  y obsérvese que es uno de los ideales de  $\mathbb{Z}_{12}$  encontrados en el ejercicio 28.1. ¿Cuál es el radical de  $\mathbb{Z}^2$ , ¿de  $\mathbb{Z}_{32}$ ?

**28.13** Con referencia al ejercicio 28.11, muéstrese que si  $N$  es el radical de un anillo comutativo  $R$ , entonces  $R/N$  tiene como radical el ideal trivial  $\{0 + N\}$ .

## 256 ANILLOS COCIENTES E IDEALES

**28.14** Sea  $R$  un anillo conmutativo y  $N$  un ideal de  $R$ . Con referencia al ejercicio 28.11, muéstrese que si todo elemento de  $N$  es nilpotente y el radical de  $R/N$  es  $R/N$ , entonces el radical de  $R$  es  $R$ .

**28.15** Sea  $R$  un anillo conmutativo y  $N$  un ideal de  $R$ . Muéstrese que el conjunto  $\sqrt{N}$  de todas las  $a \in R$  tales que  $a^n \in N$  para alguna  $n \in \mathbb{Z}^+$  es un ideal de  $R$ , el **radical de  $N$** . ¿Es consistente esta terminología con la del ejercicio 28.11?  $\blacktriangleleft$

**28.16** Con referencia al ejercicio 28.15, muéstrese, mediante ejemplos, que para ideales propios  $N$  de un anillo conmutativo  $R$ ,

- a)  $\sqrt{N}$  no necesariamente es igual a  $N$ .      b)  $\sqrt{N}$  puede ser igual a  $N$ .

**28.17** ¿Cuál es la relación del ideal  $\sqrt{N}$  del ejercicio 28.15, con el radical  $R/N$  (véase el ejercicio 28.11)? Formúlese cuidadosamente la respuesta.

*Hay una especie de aritmética de ideales en un anillo conmutativo. Los tres ejercicios siguientes definen suma, producto y cociente de ideales.*

**28.18** Si  $A$  y  $B$  son ideales de un anillo  $R$ , la **suma  $A + B$  de  $A$  y  $B$**  se define por

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

- a) Muéstrese que  $A + B$  es un ideal.      b) Muéstrese que  $A \subseteq A + B$  y  $B \subseteq A + B$ .

**28.19** Sean  $A$  y  $B$  ideales de un anillo  $R$ . El **producto  $AB$  de  $A$  y  $B$**  se define por

$$AB = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}.$$

- a) Muéstrese que  $AB$  es un ideal de  $R$ .      b) Muéstrese que  $AB \subseteq (A \cap B)$ .

**28.20** Sean  $A$  y  $B$  ideales de un anillo conmutativo  $R$ . El **cociente  $A : B$  de  $A$  por  $B$**  se define por

$$A : B = \{r \in R \mid rb \in A \text{ para toda } b \in B\}.$$

Muéstrese que  $A : B$  es un ideal de  $R$ .

\***28.21** Muéstrese que, para un campo  $F$ , el conjunto de todas las matrices de la forma

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

para  $a, b \in F$  es un ideal derecho, pero no un ideal izquierdo de  $M_2(F)$ .

\***28.22** Muéstrese que el anillo de matrices  $M_2(\mathbb{Z}_2)$  es un **anillo simple**, esto es,  $M_2(\mathbb{Z}_2)$  no tiene ideales propios no triviales.

## Homomorfismos de anillos

### 29.1 DEFINICIÓN Y PROPIEDADES ELEMENTALES

Nuestro análisis de los homomorfismos de anillos se mantendrá paralelo al del capítulo 13 sobre homomorfismos de grupos.

**Definición (Análogo de la definición de homomorfismo de grupo)** Una transformación  $\phi$  de un anillo  $R$  en un anillo  $R'$  es un *homomorfismo* si

$$(a + b)\phi = a\phi + b\phi$$

y

$$(ab)\phi = (a\phi)(b\phi)$$

para todos los elementos  $a$  y  $b$  en  $R$ .

**Teorema 29.1 (Análogo del teorema 13.1)** Si  $N$  es un ideal de un anillo  $R$ , entonces la transformación canónica  $\gamma: R \rightarrow R/N$  dada por  $a\gamma = a + N$  para  $a \in R$  es un homomorfismo.

**Demostración** El teorema 13.1 aplicado a  $\langle R, + \rangle$  como grupo aditivo con  $\langle N, + \rangle$ , un subgrupo normal, muestra que

$$(a + b)\gamma = a\gamma + b\gamma.$$

Además,

$$(ab)\gamma = ab + N = (a + N)(b + N) = (a\gamma)(b\gamma). \blacksquare$$

**Definición (Análogo de la definición del kernel de un homomorfismo de grupo)** El *kernel de un homomorfismo*  $\phi$  de un anillo  $R$  en un anillo  $R'$  es el conjunto de todos los elementos de  $R$  que van a dar a la identidad  $0'$  de  $R'$  bajo  $\phi$ .

**Teorema 29.2 (Análogo del teorema 13.2)** Sea  $\phi$  un homomorfismo de un anillo  $R$  en un anillo  $R'$ . Si  $0$  es la identidad aditiva en  $R$ , entonces  $0\phi = 0'$  es la identidad aditiva en  $R'$  y si  $a \in R$  entonces  $(-a)\phi = -(a\phi)$ . Si  $S$  es un subanillo de  $R$ , entonces,  $S\phi$  es un subanillo de  $R'$ , y  $S$  ideal de  $R$  implica que  $S\phi$  es ideal de  $R\phi$ . Ahora, en el otro sentido, si  $S'$  es un subanillo de  $R'$ , entonces  $S'\phi^{-1}$  es un subanillo de  $R$  y  $S'$  ideal de  $R\phi$  implica que  $S'\phi^{-1}$  es un ideal de  $R$ . Por último, si  $R$  tiene unitario  $1$  y  $1\phi \neq 0'$  entonces,  $1\phi = 1'$  es unitario para  $R\phi$ . Dicho en forma breve, bajo un homomorfismo de anillos, subanillos van a dar a subanillos, ideales a ideales y anillos con unitario a anillos con unitario.

**Demostración** Sea  $\phi$  un homomorfismo de un anillo  $R$  en un anillo  $R'$ . Como, en particular,  $\phi$  puede verse como un homomorfismo de grupo de  $\langle R, + \rangle$  en  $\langle R', +' \rangle$ , el teorema 13.2 dice que  $0\phi = 0'$  es la identidad aditiva de  $R'$  y que  $(-a)\phi = -(a\phi)$ .

El teorema 13.2 también dice que si  $S$  es un subanillo de  $R$ , entonces, considerando el grupo aditivo  $\langle S, + \rangle$  encontramos que  $\langle S\phi, +' \rangle$  es un subgrupo de  $\langle R', +' \rangle$ . Si  $s_1\phi$  y  $s_2\phi$  son dos elementos de  $S\phi$  entonces,

$$(s_1\phi)(s_2\phi) = (s_1s_2)\phi$$

y  $(s_1s_2)\phi \in S\phi$ , de modo que  $S\phi$  es cerrado bajo la multiplicación, y es, entonces, un subanillo de  $R'$ . Si  $S$  es un ideal de  $R$ , entonces, para  $s \in S$  y  $r \in R$  tenemos

$$(r\phi)(s\phi) = (rs)\phi$$

y  $(rs)\phi \in S\phi$ . Además,

$$(s\phi)(r\phi) = (sr)\phi$$

y  $(sr)\phi \in S\phi$ . Así,  $S\phi$  es un ideal en  $R\phi$ .

Ahora, en la otra dirección, de nuevo el teorema 13.2 muestra que si  $S'$  es un subanillo de  $R'$ , entonces  $\langle S'\phi^{-1}, + \rangle$  es un subgrupo de  $\langle R, + \rangle$ . Si  $a\phi \in S'$  y  $b\phi \in S'$ , entonces

$$(ab)\phi = (a\phi)(b\phi)$$

y  $[(a\phi)(b\phi)] \in S'$  de modo que  $S'\phi^{-1}$  es cerrado bajo la multiplicación y es, entonces, un subanillo de  $R$ . Si  $S'$  es un ideal de  $R\phi$  entonces, para  $a \in S'\phi^{-1}$  y cualquier  $r \in R$  tenemos

$$(ra)\phi = (r\phi)(a\phi)$$

y  $[(r\phi)(a\phi)] \in S'$ , de modo que  $ra \in S'\phi^{-1}$ . En forma análoga,  $ar \in S'\phi^{-1}$ . Así,  $S'\phi^{-1}$  es un ideal de  $R$ .

Por último, si  $R$  tiene unitario 1, entonces, para toda  $r \in R$ ,

$$r\phi = (1r)\phi = (r1)\phi = (1\phi)(r\phi) = (r\phi)(1\phi),$$

de modo que  $1' = 1\phi$  es una identidad multiplicativa para  $R\phi$ . Si  $1' \neq 0'$ , entonces  $1'$  es unitario para  $R\phi$ . ■

En el teorema 29.2 es importante notar que si  $\phi : R \rightarrow R'$  es un homomorfismo de anillo y  $A$  es un ideal de  $R$ , entonces,  $A\phi$  no necesariamente es un ideal de  $R'$  sino sólo un ideal de  $R\phi$ . Por ejemplo, sea  $\phi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  definida por  $n\phi = (n, n)$ . Ahora bien,  $2\mathbb{Z}$  es un ideal de  $\mathbb{Z}$ . Sin embargo,  $(2\mathbb{Z})\phi = \{(2n, 2n) \mid n \in \mathbb{Z}\}$  no es un ideal de  $\mathbb{Z} \times \mathbb{Z}$  puesto que  $(1, 2)(4, 4) = (4, 8) \notin (2\mathbb{Z})\phi$ .

El teorema 29.2 muestra, en particular, que para un homomorfismo  $\phi : R \rightarrow R'$  el kernel  $K = \{0'\}\phi^{-1}$  es un ideal de  $R$ .

**Teorema 29.3 (Teorema fundamental del homomorfismo, análogo del teorema 13.3)** *Sea  $\phi$  un homomorfismo de un anillo  $R$  en un anillo  $R'$  con kernel  $K$ . Entonces,  $R\phi$  es un anillo y existe un isomorfismo canónico de  $R\phi$  con  $R/K$ .*

*Demostración* El teorema 29.2 muestra que  $R\phi$  es un anillo. Sea  $(a + K) \in R/K$ , definase la transformación  $\psi : R/K \rightarrow R\phi$  por

$$(a + K)\psi = a\phi.$$

El teorema 13.3 muestra que  $\psi$  está bien definida, es uno a uno y sobre, con

$$[(a + K) + (b + K)]\psi = (a + K)\psi + (b + K)\psi.$$

Ahora bien,

$$\begin{aligned} [(a + K)(b + K)]\psi &= (ab + K)\psi = (ab)\phi = (a\phi)(b\phi) \\ &= [(a + K)\psi][(b + K)\psi]. \end{aligned}$$

Así,  $\psi$  es un homomorfismo de anillo.

De nuevo,  $\psi$  es canónico en el sentido de que si  $\gamma : R \rightarrow R/K$  es la transformación canónica, entonces  $\phi = \gamma\psi$ . ■

## 29.2 IDEALES MAXIMALES Y PRIMOS

Estudiaremos ahora la cuestión de cuándo un anillo cociente de un anillo es un campo y cuándo es un dominio entero. La analogía con grupos en el capítulo 13 puede ampliarse un poco más, para cubrir el caso en el cual el anillo cociente es un campo.

**Definición (Análogo de la definición de subgrupo normal maximal)** Un *ideal maximal de un anillo*  $R$  es un ideal  $M$  diferente de  $R$  tal que no existe ningún ideal propio  $N$  de  $R$  que contenga propiamente a  $M$ .

**Teorema 29.4 (Análogo del teorema 13.4)** Sea  $R$  un anillo conmutativo unitario. Entonces,  $M$  es un ideal maximal de  $R$  si y sólo si  $R/M$  es un campo.

**Demostración** Supóngase que  $M$  es un ideal maximal en  $R$ . Es fácil observar que si  $R$  es un anillo conmutativo con unitario, entonces  $R/M$  también es un anillo conmutativo con unitario cuando  $M \neq R$ , lo cual sucede si  $M$  es maximal. Sea  $(a + M) \in R/M$ , con  $a \notin M$ , de modo que  $a + M$  no es la identidad aditiva de  $R/M$ . Debemos mostrar que  $a + M$  tiene inverso multiplicativo en  $R/M$ . Sea

$$N = \{ra + m \mid r \in R, m \in M\}.$$

Entonces,  $\langle N, + \rangle$  es un grupo, pues

$$(r_1a + m_1) + (r_2a + m_2) = (r_1 + r_2)a + (m_1 + m_2),$$

y, claramente, lo último está en  $N$ , además,

$$0 = 0a + 0 \quad \text{y} \quad -(ra + m) = (-r)a + (-m).$$

Ahora,

$$r_1(ra + m) = (r_1r)a + r_1m$$

muestra que  $r_1(ra + m) \in N$  para  $r_1 \in R$  y, como  $R$  es un anillo conmutativo también,  $(ra + m)r_1 \in N$ . Así,  $N$  es un ideal. Pero,

$$a = 1a + 0.$$

muestra que  $a \in N$  y para  $m \in M$ , y

$$m = 0a + m$$

muestra que  $M \subseteq N$ . De aquí,  $N$  es un ideal de  $R$  que contiene propiamente  $M$ , pues  $a \in N$  y  $a \notin M$ . Como  $M$  es maximal, debemos tener  $N = R$ . En particular,  $1 \in N$ . Entonces, por definición de  $N$ , existe  $b \in R$  y  $m \in M$  tal que  $1 = ba + m$ . Por tanto,

$$1 + M = ba + M = (b + M)(a + M),$$

de modo que  $b + M$  es un inverso multiplicativo de  $a + M$ .

Recíprocamente, supóngase que  $R/M$  es un campo. Por el teorema 29.2, si  $N$  es cualquier ideal de  $R$ , tal que  $M \subset N \subset R$  y  $\gamma$  es el homomorfismo canónico de

$R$  sobre  $R/M$ , entonces  $N\gamma$  es un ideal de  $R/M$  con  $\{(0 + M)\} \subset N\gamma \subset R/M$ , contrario al corolario del teorema 28.4, el cual afirma que el campo  $R/M$  no contiene ideales no triviales propios. De aquí que si  $R/M$  es campo,  $M$  es maximal. ■

**Corolario** *Un anillo comutativo con unitario es un campo si y sólo si no contiene ideales propios no triviales.*

**Demostración** El corolario del teorema 28.4 muestra que un campo no tiene ideales propios no triviales.

Recíprocamente, si un anillo comutativo  $R$  con unitario no tiene ideales propios no triviales, entonces  $\{0\}$  es un ideal maximal y, por el teorema 29.4,  $R/\{0\}$ , el cual es isomorfo a  $R$ , es un campo. ■

Pasamos ahora a la cuestión de la caracterización de los ideales  $N \neq R$  para un anillo comutativo  $R$  con unitario, tal que  $R/N$  es un dominio entero. Aquí, la respuesta es bastante obvia. El anillo factor  $R/N$  será un dominio entero si y sólo si  $(a + N)(b + N) = N$  implica que

$$a + N = N \quad \text{o que} \quad b + N = N.$$

Esto equivale a la proposición de que  $R/N$  no tiene divisores de 0, puesto que la clase lateral  $N$  desempeña el papel de 0 en  $R/N$ . Observando los representantes, vemos que esta condición equivale a decir que  $ab \in N$  implica que  $a \in N$  o  $b \in N$ .

**Ejemplo 29.1** Los ideales de  $\mathbf{Z}$  son de la forma  $n\mathbf{Z}$ . Hemos visto que  $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$  y que  $\mathbf{Z}_n$  es un dominio entero si y sólo si  $n$  es primo. Así, los ideales  $n\mathbf{Z}$  tales que  $\mathbf{Z}/n\mathbf{Z}$  es un dominio entero, son de la forma  $p\mathbf{Z}$ , donde  $p$  es primo. Es claro que  $\mathbf{Z}/p\mathbf{Z}$  es, en realidad, un campo, de modo que  $p\mathbf{Z}$  es un ideal maximal de  $\mathbf{Z}$ . Nótese que para que un producto  $rs$  de enteros esté en  $p\mathbf{Z}$ , el primo  $p$  debe dividir  $r$  o  $s$ . El papel que desempeñan en este ejemplo, los enteros primos hacen que el uso de la palabra *primo* en la siguiente definición sea razonable. ■

**Definición** Un ideal  $N \neq R$  en un anillo comutativo  $R$  es un *ideal primo* si  $ab \in N$  implica que  $a \in N$  o  $b \in N$  para todas las  $a, b \in R$ .

Las observaciones anteriores al ejemplo 29.1 constituyen una demostración del siguiente teorema.

**Teorema 29.5** *Sea  $R$  un anillo comutativo con unitario y sea  $N \neq R$  un ideal en  $R$ . Entonces  $R/N$  es un dominio entero si y sólo si  $N$  es un ideal primo en  $R$ .*

**Corolario** *Todo ideal maximal en un anillo comutativo  $R$  con unitario, es un ideal primo.*

**Demostración** Si  $M$  es maximal en  $R$ , entonces  $R/M$  es un campo, por tanto, un dominio entero y, por el teorema 29.5,  $M$  es un ideal primo. ■

El material presentado, en lo que respecta a ideales maximales y primos, es muy importante y se usará a menudo. Deberán recordarse las ideas principales, aunque se hayan perdido en la fascinante demostración del teorema 29.4. Esto es, hay que saber y entender las definiciones de ideales maximales y primos y deben recordarse los siguientes hechos, que ya demostramos.

*Para un anillo conmutativo con unitario:*

- 1 *Un ideal  $M$  de  $R$  es maximal si y sólo si  $R/M$  es campo.*
- 2 *Un ideal  $N$  de  $R$  es primo si y sólo si  $R/N$  es un dominio entero.*
- 3 *Todo ideal maximal de  $R$  es un ideal primo.*

## 29.3 CAMPOS PRIMOS

Sea  $R$  cualquier anillo con unitario 1. Recuérdese que  $n \cdot 1$  significa  $1 + 1 + \cdots + 1$  con  $n$  sumandos para  $n > 0$ , y  $(-1) + (-1) + \cdots + (-1)$  para  $|n|$  sumandos para  $n < 0$ , mientras que  $n \cdot 1 = 0$  para  $n = 0$ .

**Teorema 29.6** *Si  $R$  es un anillo con unitario 1, entonces la transformación  $\phi : \mathbf{Z} \rightarrow R$  dada por*

$$n\phi = n \cdot 1$$

*para  $n \in \mathbf{Z}$  es un homomorfismo de  $\mathbf{Z}$  en  $R$ .*

**Demostración** Es obvio que

$$(n + m)\phi = (n + m) \cdot 1 = (n \cdot 1) + (m \cdot 1) = n\phi + m\phi.$$

La ley distributiva en  $R$  muestra que

$$\underbrace{(1 + 1 + \cdots + 1)}_{n \text{ sumandos}} \underbrace{(1 + 1 + \cdots + 1)}_{m \text{ sumandos}} = \underbrace{(1 + 1 + \cdots + 1)}_{nm \text{ sumandos}}$$

Así,  $(n \cdot 1)(m \cdot 1) = (nm) \cdot 1$  para  $n, m > 0$ . Argumentos similares, usando las leyes distributivas, muestran que para todo  $n, m \in \mathbf{Z}$  tenemos

$$(n \cdot 1)(m \cdot 1) = (nm) \cdot 1.$$

Así,

$$(nm)\phi = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1) = (n\phi)(m\phi). \blacksquare$$

**Corolario** Si  $R$  es un anillo con unitario y característica  $n > 1$ , entonces  $R$  contiene un subanillo isomorfo a  $\mathbf{Z}_n$ . Si  $R$  tiene característica 0, entonces  $R$  contiene un subanillo isomorfo a  $\mathbf{Z}$ .

**Demostración** Por el teorema 29.6, la transformación  $\phi: \mathbf{Z} \rightarrow R$  dada por  $m\phi = m \cdot 1$  para  $m \in \mathbf{Z}$  es un homomorfismo. El kernel debe ser un ideal en  $\mathbf{Z}$ . Todos los ideales en  $\mathbf{Z}$  son de la forma  $s\mathbf{Z}$  para alguna  $s \in \mathbf{Z}$ . Por el teorema 24.5, es claro que si  $R$  tiene característica  $n > 0$ , entonces el kernel de  $\phi$  es  $n\mathbf{Z}$ . Entonces, la imagen  $\mathbf{Z}\phi \leq R$  es isomorfa a  $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$ . Si la característica de  $R$  es 0, entonces  $m \cdot 1 \neq 0$  para todas las  $m \neq 0$ , de modo que el kernel de  $\phi$  es  $\{0\}$ . Así, la imagen  $\mathbf{Z}\phi \leq R$  es isomorfa a  $\mathbf{Z}$ . ■

**Teorema 29.7** Un campo  $F$ , o es de característica  $p$ ,  $p$  un primo y contiene un subcampo isomorfo a  $\mathbf{Z}_p$ , o es de característica 0 y contiene un subcampo isomorfo a  $\mathbf{Q}$ .

**Demostración** Si la característica de  $F$  no es 0, el corolario anterior muestra que  $F$  contiene un subanillo isomorfo a  $\mathbf{Z}_n$ . Entonces,  $n$  debe ser algún primo  $p$  o  $F$  tendría divisores de 0. Si  $F$  es de característica 0, entonces  $F$  debe contener un subanillo isomorfo a  $\mathbf{Z}$ . En este caso, los corolarios del teorema 26.2 muestran que  $F$  debe contener algún campo de cocientes de este subanillo y que este campo de cocientes debe ser isomorfo a  $\mathbf{Q}$ . ■

Así, todo campo contiene un subcampo isomorfo a  $\mathbf{Z}_p$  para algún primo  $p$  o un subcampo isomorfo a  $\mathbf{Q}$ . Estos campos  $\mathbf{Z}_p$  y  $\mathbf{Q}$  son las piezas constitutivas fundamentales en las cuales descansan todos los campos.

**Definición** Los campos  $\mathbf{Z}_p$  y  $\mathbf{Q}$  son *campos primos*.

## Ejercicios

---

**29.1** Describanse todos los homomorfismos de anillo de  $\mathbf{Z}$  en  $\mathbf{Z}$ . [Sugerencia: por la teoría de grupos, un homomorfismo de un anillo  $R$  está determinado por sus valores en un conjunto generador aditivo del grupo  $\langle R, + \rangle$ . Describanse los homomorfismos, dando sus valores en el generador 1 de  $\langle \mathbf{Z}, + \rangle$ .]

**29.2** Describanse todos los homomorfismos de anillos de  $\mathbf{Z} \times \mathbf{Z}$  en  $\mathbf{Z}$ . [Véase la sugerencia del ejercicio 29.1.]

**29.3** Dése un ejemplo de un homomorfismo de anillo  $\phi: R \rightarrow S$  donde  $R$  tiene unitario  $1_R$  y  $1_R\phi \neq 0$  pero donde  $1_R\phi$  no sea unitario en  $S$ .

**29.4** Encuéntrense todos los ideales primos y todos los ideales maximales de  $\mathbf{Z}_{12}$ .

**29.5** Encuéntrese un ideal maximal de  $\mathbf{Z} \times \mathbf{Z}$ . Encuéntrese un ideal primo de  $\mathbf{Z} \times \mathbf{Z}$  que no sea maximal. Encuéntrese un ideal propio de  $\mathbf{Z} \times \mathbf{Z}$  que no sea primo.

**29.6** Pruébese, directamente de las definiciones de ideal maximal y primo, que todo ideal maximal de un anillo comutativo  $R$  con unitario, es un ideal primo. [Sugerencia: supóngase que  $M$  es maximal en  $R$ ,  $ab \in M$  y  $a \notin M$ . Considerérese el ideal de  $R$  generado por  $a$  y  $M$ .]

**29.7** ¿Falso o verdadero?

- a) El concepto de homomorfismo de anillo está íntimamente relacionado con la idea de anillo factor.
  - b) Un homomorfismo es a un anillo lo que un isomorfismo es a un grupo.
  - c) Un homomorfismo de anillo es una transformación uno a uno si y sólo si el kernel es 0.
  - d) En cierto sentido, un campo es a la teoría de anillos comutativos con unitario, lo que un grupo simple es a la teoría de grupos.
  - e) El kernel de un homomorfismo de anillo es un ideal de todo el anillo.
  - f) Todo ideal primo de todo anillo comutativo con unitario es un ideal maximal.
  - g) Todo ideal maximal de todo anillo comutativo con unitario es un ideal primo.
  - h)  $\mathbb{Q}$  es su propio subcampo primo.
  - i) El subcampo primo de  $\mathbb{C}$  es  $\mathbb{R}$ .
  - j) Todo campo contiene un campo primo como subcampo.
- 

**29.8** Describanse todos los homomorfismos de anillo de  $\mathbb{Z} \times \mathbb{Z}$  en  $\mathbb{Z} \times \mathbb{Z}$ . [Véase la sugerencia del ejercicio 29.1.]

**29.9** Muéstrese que cada homomorfismo de un campo es uno a uno o transforma todo en 0.

**29.10** Muéstrese que si  $R$ ,  $R'$  y  $R''$  son anillos y si  $\phi: R \rightarrow R'$  y  $\psi: R' \rightarrow R''$  son homomorfismos, entonces la función compuesta  $\phi\psi: R \rightarrow R''$  es un homomorfismo. (Usese el ejercicio 13.14.)

**29.11** Sea  $R$  un anillo no comutativo con unitario, de característica  $p$ ,  $p$  un primo. Muéstrese qué la transformación  $\phi_p: R \rightarrow R$  dada por  $a\phi = a^p$  es un homomorfismo (el **homomorfismo de Frobenius**).

**29.12** Sean  $R$  y  $S$  anillos y sea  $\phi: R \rightarrow S$  un homomorfismo de anillo tal que  $R\phi \neq \{0\}$ . Muéstrese que si  $R$  tiene unitario  $1_R$  y  $S$  no tiene divisores de 0, entonces  $1_R\phi$  es unitario para  $S$ .

**29.13** Muéstrese que  $N$  es un ideal maximal en un anillo  $R$  si y sólo si  $R/N$  es un anillo simple, esto es, no tiene ideales propios no triviales. (Compárese con el teorema 13.4.)

**29.14** El corolario del teorema 29.6 nos dice que todo anillo unitario contiene un subanillo isomorfo a  $\mathbb{Z}$  o a algún  $\mathbb{Z}_n$ . ¿Es posible que un anillo unitario pueda contener simultáneamente dos subanillos isomorfos a  $\mathbb{Z}_n$  y  $\mathbb{Z}_m$  para  $n \neq m$ ? ¿Es posible que un anillo unitario pueda contener simultáneamente dos subanillos isomorfos a los campos  $\mathbb{Z}_p$  y  $\mathbb{Z}_q$  para dos primos diferentes  $p$  y  $q$ ? Si es imposible, debe probarse. Si es posible, debe ilustrarse. (Esto se relaciona con el ejercicio 23.10.)

**29.15** Siguiendo la idea del ejercicio 29.14, ¿es posible, para un dominio entero, contener dos subanillos isomorfos a  $\mathbb{Z}_p$  y a  $\mathbb{Z}_q$  para  $p \neq q$  y  $p$  y  $q$  ambos primos? Dense razones o ilústrese. (Esto se relaciona con el ejercicio 23.11.)

**29.16** Sean  $R$  y  $R'$  anillos y sean  $N$  y  $N'$  ideales de  $R$  y  $R'$ , respectivamente. Sea  $\phi$  un homomorfismo de  $R$  en  $R'$ . Muéstrese que  $\phi$  induce un homomorfismo natural  $\phi_* : R/N \rightarrow R'/N'$  si  $N\phi \subseteq N'$ . (Usese el ejercicio 13.17.)

**29.17** Sea  $\phi$  un homomorfismo de un anillo  $R$  con unitario, sobre un anillo  $R'$ . Sea  $u$  una unidad en  $R$ . Muéstrese que  $u\phi$  es una unidad en  $R'$  si y sólo si  $u$  no está en el kernel de  $\phi$ .

**\*29.18** (Segundo teorema del isomorfismo para anillos) Sean  $M$  y  $N$  ideales de un anillo  $R$  y sea

$$M + N = \{m + n \mid m \in M, n \in N\}.$$

Muéstrese que  $M + N$  es un ideal de  $R$  y que  $(M + N)/N$  es isomorfo, de manera natural, a  $M/(M \cap N)$ . (Usese el teorema 15.2.)

**\*29.19** (Tercer teorema del isomorfismo para anillos) Sean  $M$  y  $N$  ideales de un anillo  $R$  tal que  $M \leq N$ . Muéstrese que existe un isomorfismo natural de  $R/N$  con  $(R/M)/(N/M)$ . (Usese el teorema 15.3.)

**\*29.20** Muéstrese que  $\phi : \mathbf{C} \rightarrow M_2(\mathbf{R})$  dado por

$$(a + bi)\phi = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

para  $a, b \in \mathbf{R}$ , es un isomorfismo de  $\mathbf{C}$  en  $M_2(\mathbf{R})$ .

**\*29.21** Sea  $R$  un anillo con unitario y sea  $\text{Hom}(\langle R, + \rangle)$  el anillo de endomorfismos de  $\langle R, + \rangle$  como se describió en la sección 25.2. Sean  $a \in R$  y  $\rho_a : R \rightarrow R$  dada por

$$x\rho_a = xa$$

para  $x \in R$ .

- Muéstrese que  $\rho_a$  es un endomorfismo de  $\langle R, + \rangle$ .
- Muéstrese que  $R' = \{\rho_a \mid a \in R\}$  es un subanillo de  $\text{Hom}(\langle R, + \rangle)$ .
- Pruébese el análogo del teorema de Cayley para  $R$ , mostrando que  $R'$  de b) es isomorfo a  $R$ .

# Anillos de polinomios

## 30.1 POLINOMIOS EN UNA INDETERMINADA

Es probable ya que tengan una idea bastante manejable de lo que es un *polinomio en  $x$  con coeficientes en un anillo  $R$* . Ya saben cómo sumar y multiplicar dichos objetos, lo han hecho por años y saben lo que significa el *grado de un polinomio*. Si en efecto es así, sugerimos que procedan de inmediato a leer el enunciado del teorema 30.1, omitan la demostración por trivial y comiencen a leer después de la demostración. Diremos que consideramos  $x$  una *indeterminada* y no una variable.

Nuestro problema tiene dos aspectos: explicar qué es un polinomio y explicar qué es  $x$ . Si definimos un polinomio con coeficiente en un anillo  $R$  como una *suma formal finita*

$$\sum_{i=0}^n a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

donde  $a_i \in R$ , nos veremos en dificultades. Ciertamente,  $0 + a_1 x$  y  $0 + a_1 x + 0x^2$  son diferentes como sumas formales, pero queremos considerarlas como el mismo polinomio. Quizá la mejor manera es definir un polinomio como una *suma formal infinita*

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots,$$

donde  $a_i = 0$  para todos, salvo un número finito de valores de  $i$ . Ahora, ya no existe el problema de tener más de una suma formal representando lo que deseamos considerar como un solo polinomio.

Esto trae a colación la pregunta de qué es  $x$ . La manera *elegante* de hacerlo es quitar las  $x$ . Un polinomio  $a_0 + a_1x + \cdots + a_nx^n + \cdots$  está completamente determinado por la sucesión de sus coeficientes

$$a_0, a_1, \dots, a_n, \dots,$$

que no incorpora al niño problema  $x$ . Se podría *definir elegantemente* un polinomio como dicha sucesión. ¿Por qué cargar con la  $x$  cuando ni siquiera la necesitamos? Sencillamente, porque los matemáticos se han acostumbrado a la  $x$ . Tiene antigüedad, derecho de propiedad, o lo que haya que tener en la FMNM (Federación Mundial de Notaciones Matemáticas). Si un anillo tiene unitario 1 y se quiere tener  $x$ , la manera *elegante* es definir  $x$  como la sucesión

$$0, 1, 0, 0, 0, \dots$$

Pero, entonces, lo más probable es que la  $x$  proteste ante el Comité de Quejas por dicho tratamiento. Como, de cualquier forma, su papel es de exceso de equipaje, no hagamos tanto escándalo acerca de lo que realmente es. Simplemente, acordemos llamarle una *indeterminada*. El lector tendrá que admitir que es un término bastante bueno para algo que resulta difícil de analizar. Quizá sería mejor *indeterminable*. Una cosa es cierta, no es ni 0, ni 2, ni ningún otro número. *Así, de ahora en adelante, nunca escribiremos expresiones tales como  $x = 0$  o  $x = 2$ .*

Ya estamos casi listos para definir un polinomio con coeficientes en un anillo  $R$ , como una suma formal infinita

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots,$$

donde  $a_i \in R$ ,  $a_i = 0$  para todos, salvo un número finito de valores de  $i$ . Pero con  $R = \mathbf{Z}$ ,  $\sqrt{2} + x^2$  no sería un polinomio! Siempre tendríamos que escribir

$$2 + 0x + 1x^2 + 0x^3 + 0x^4 + \cdots$$

Así que cambiamos un poco la notación, después de la definición.

**Definición** Sea  $R$  un anillo. Un *polinomio  $f(x)$  con coeficientes en  $R$*  es una suma formal infinita

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots,$$

donde  $a_i \in R$  y  $a_i = 0$  para todos, excepto un número finito de valores de  $i$ .

Las  $a_i$  son los *coeficientes de  $f(x)$* . Si para alguna  $i > 0$  es cierto que  $a_i \neq 0$ , el mayor de dichos valores de  $i$  es el *grado de  $f(x)$* . De no existir dicha  $i > 0$ , entonces  $f(x)$  es de *grado cero*.

Acordemos que si  $f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$  tiene  $a_i = 0$  para  $i > n$ , entonces podemos denotar  $f(x)$  por  $a_0 + a_1x + \cdots + a_nx^n$ . También, si alguna  $a_i = 1$ , podemos quitarla de la suma formal, así que consideraremos, por ejemplo,  $2 + x$  como el polinomio  $2 + 1x$  con coeficientes en  $\mathbb{Z}$ . Por último, acordemos que es posible omitir de la suma formal cualquier término  $0x^i$  o  $a_0 = 0$ , si  $a_0 = 0$  pero no todas las  $a_i = 0$ . Así,  $0, 2, x$  y  $2 + x^2$  son, todos ellos, polinomios con coeficientes en  $\mathbb{Z}$ . Un elemento de  $R$  es un **polinomio constante**.

La suma y multiplicación de polinomios con coeficientes en un anillo  $R$  están definidas de la manera que les es formalmente conocida. Si

$$f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$$

y

$$g(x) = b_0 + b_1x + \cdots + b_nx^n + \cdots,$$

entonces, para el polinomio suma, tenemos

$$f(x) + g(x) = c_0 + c_1x + \cdots + c_nx^n + \cdots,$$

donde  $c_n = a_n + b_n$  y, para el polinomio multiplicación, tenemos

$$f(x)g(x) = d_0 + d_1x + \cdots + d_nx^n + \cdots,$$

donde  $d_n = \sum_{i=0}^n a_i b_{n-i}$ . Es claro que, de nuevo,  $c_i$  y  $d_i$  ambas son 0 para todos, salvo un número finito de valores de  $i$ , así que estas definiciones tienen sentido. Nótese que  $\sum_{i=0}^n a_i b_{n-i}$  no necesariamente es igual a  $\sum_{i=0}^n b_i a_{n-i}$  si  $R$  no es conmutativo. Con estas definiciones de suma y multiplicación, tenemos el siguiente teorema.

**Teorema 30.1** *El conjunto  $R[x]$  de todos los polinomios en una indeterminada  $x$  con coeficientes en un anillo  $R$ , es un anillo bajo la suma y multiplicación polinomial. Si  $R$  es conmutativo, entonces lo es  $R[x]$  y si  $R$  tiene unitario 1, entonces 1 también es unitario en  $R[x]$ .*

**Demostración** Es obvio que  $\langle R[x], + \rangle$  es un grupo abeliano. La ley asociativa para la multiplicación y las leyes distributivas, se prueban mediante cálculos directos, pero algo engorrosos. Ilustramos probando la ley asociativa.

Aplicando los axiomas de anillo a los elementos  $a_i, b_j, c_k \in R$ , obtenemos

$$\begin{aligned}
 & \left[ \left( \sum_{i=0}^{\infty} a_i x^i \right) \left( \sum_{j=0}^{\infty} b_j x^j \right) \right] \left( \sum_{k=0}^{\infty} c_k x^k \right) = \left[ \sum_{n=0}^{\infty} \left( \sum_{i=0}^n a_i b_{n-i} \right) x^n \right] \left( \sum_{k=0}^{\infty} c_k x^k \right) \\
 & = \sum_{s=0}^{\infty} \left[ \sum_{n=0}^s \left( \sum_{i=0}^n a_i b_{n-i} \right) c_{s-n} \right] x^s \\
 & = \sum_{s=0}^{\infty} \left( \sum_{i+j+k=s} a_i b_j c_k \right) x^s \\
 & = \sum_{s=0}^{\infty} \left[ \sum_{m=0}^s a_{s-m} \left( \sum_{j=0}^m b_j c_{m-j} \right) \right] x^s \\
 & = \left( \sum_{i=0}^{\infty} a_i x^i \right) \left[ \sum_{m=0}^{\infty} \left( \sum_{j=0}^m b_j c_{m-j} \right) x^m \right] \\
 & = \left( \sum_{i=0}^{\infty} a_i x^i \right) \left[ \left( \sum_{j=0}^{\infty} b_j x^j \right) \left( \sum_{k=0}^{\infty} c_k x^k \right) \right].
 \end{aligned}$$

¡Uf! Las leyes distributivas se prueban de manera análoga.

Los comentarios anteriores al enunciado del teorema, muestran que  $R[x]$  es un anillo conmutativo si  $R$  es conmutativo y un unitario 1 en  $R$  también es, obviamente, unitario para  $R[x]$ , en vista de la definición de multiplicación en  $R[x]$ . ■

Así,  $\mathbf{Z}[x]$  es el anillo de polinomios en la indeterminada  $x$  con coeficientes enteros;  $\mathbf{Q}[x]$  es el anillo de polinomios en  $x$  con coeficientes racionales y así sucesivamente.

**Ejemplo 30.1** En  $\mathbf{Z}_2[x]$  tenemos

$$(x + 1)^2 = (x + 1)(x + 1) = x^2 + (1 + 1)x + 1 = x^2 + 1.$$

Todavía en  $\mathbf{Z}_2[x]$ , obtenemos

$$(x + 1) + (x + 1) = (1 + 1)x + (1 + 1) = 0x + 0 = 0. ■$$

Si  $R$  es un anillo y  $x$  y  $y$  son indeterminadas, podemos formar el anillo  $(R[x])[y]$ , esto es, el anillo de polinomios en  $y$  con coeficientes que son polinomios en  $x$ . Es bastante obvio, pero algo tedioso, probar con cuidado que  $(R[x])[y]$  es naturalmente isomorfo a  $(R[y])[x]$ . Todo polinomio en  $y$  con coeficientes que son polinomios en  $x$ , puede reescribirse, de manera natural, como un polinomio en  $x$  con coeficientes que son polinomios en  $y$ . Identificaremos estos anillos mediante este isomorfismo natural y lo consideraremos el anillo  $R[x, y]$ , el anillo de polinomios en dos indeterminadas  $x$  y  $y$  con coeficientes en  $R$ . Se define de manera análoga el anillo  $R[x_1, \dots, x_n]$  de polinomios en  $n$  indeterminadas  $x_i$  con coeficientes en  $R$ .

Dejamos como ejercicio la sencilla demostración de que si  $D$  es un dominio entero, entonces también lo es  $D[x]$ . En particular, si  $F$  es un campo, entonces  $F[x]$  es un dominio entero. Nótese que  $F[x]$  no es un campo, pues  $x$  no es una unidad en  $F[x]$ . Esto es, no existe polinomio  $f(x) \in F[x]$  tal que  $xf(x) = 1$ . Por el teorema 26.1, podemos construir el campo de cocientes  $F(x)$  de  $F[x]$ . Cualquier elemento de  $F(x)$  se puede representar como un cociente  $f(x)/g(x)$  de dos polinomios en  $F[x]$  con  $g(x) \neq 0$ . Definimos de manera análoga  $F(x_1, \dots, x_n)$  como el campo de cocientes de  $F[x_1, \dots, x_n]$ . Este campo  $F(x_1, \dots, x_n)$  es el campo de funciones racionales en  $n$  indeterminadas sobre  $F$ . Estos campos desempeñan un papel muy importante en geometría algebraica.

## 30.2 HOMOMORFISMOS DE EVALUACION

Ya estamos preparados para mostrar, como lo prometimos en el capítulo 27, cómo se usa la maquinaria de homomorfismos y anillos factores para estudiar lo que los alumnos conocen como «resolver una ecuación polinomial». Sean  $E$  y  $F$  campos, con  $F$  un subcampo de  $E$ , esto es,  $F \leq E$ . El teorema siguiente asegura la existencia de homomorfismos muy importantes de  $F[x]$  en  $E$ . *Estos homomorfismos serán las herramientas fundamentales para el resto de nuestro trabajo.* Si en verdad los comprenden, así como la teoría de los homomorfismos en la sección anterior, están en magnífica posición para el resto del curso.

**Teorema 30.2 (Los homomorfismos de evaluación de la teoría de los campos)** *Sea  $F$  un subcampo de un campo  $E$ , sea  $\alpha$  cualquier elemento de  $E$  y sea  $x$  una indeterminada. La transformación  $\phi_\alpha: F[x] \rightarrow E$  definida por*

$$(a_0 + a_1x + \cdots + a_nx^n)\phi_\alpha = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

*para  $(a_0 + a_1x + \cdots + a_nx^n) \in F[x]$  es un homomorfismo de  $F[x]$  en  $E$ . Además,  $x\phi_\alpha = \alpha$ , y  $\phi_\alpha$  transforma, de manera isomorfa, a  $F$ , mediante la transformación idéntica, esto es,  $a\phi_\alpha = a$  para  $a \in F$ . El homomorfismo  $\phi_\alpha$  es la evaluación en  $\alpha$ .*

**Demostración** El diagrama reticular y de transformaciones, en la figura 30.1, puede ayudar a visualizar esta situación. Las líneas punteadas indican un elemento del conjunto. En realidad, el teorema es una consecuencia inmediata de nuestras definiciones de suma y multiplicación en  $F[x]$ . Está claro que la transformación  $\phi_\alpha$  está bien definida, esto es, es independiente de nuestra representación de  $f(x) \in F[x]$  como una suma finita.

$$a_0 + a_1x + \cdots + a_nx^n.$$

Dicha suma finita que representa a  $f(x)$  puede modificarse sólo por la inserción y eliminación de términos  $0x^i$ , lo cual, claramente, no afecta el valor de  $(f(x))\phi_\alpha$ .

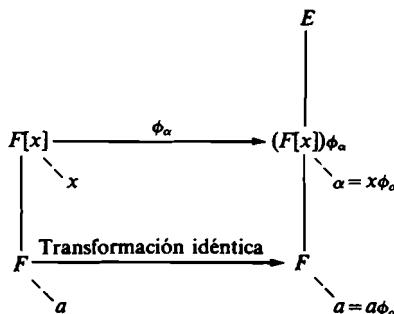


Figura 30.1

Si  $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ,  $g(x) = b_0 + b_1x + \cdots + b_mx^m$ , y  $h(x) = f(x) + g(x) = c_0 + c_1x + \cdots + c_rx^r$ , entonces,

$$(f(x) + g(x))\phi_\alpha = (h(x))\phi_\alpha = c_0 + c_1\alpha + \cdots + c_r\alpha^r,$$

mientras que

$$(f(x))\phi_\alpha + (g(x))\phi_\alpha = (a_0 + a_1\alpha + \cdots + a_n\alpha^n) + (b_0 + b_1\alpha + \cdots + b_m\alpha^m).$$

Como por definición de suma polinomial tenemos  $c_i = a_i + b_i$ , vemos que

$$(f(x) + g(x))\phi_\alpha = (f(x))\phi_\alpha + (g(x))\phi_\alpha.$$

Pasando a la multiplicación, vemos que

$$f(x)g(x) = d_0 + d_1x + \cdots + d_sx^s,$$

entonces

$$(f(x)g(x))\phi_\alpha = d_0 + d_1\alpha + \cdots + d_s\alpha^s,$$

mientras que

$$[(f(x))\phi_\alpha][(g(x))\phi_\alpha] = (a_0 + a_1\alpha + \cdots + a_n\alpha^n)(b_0 + b_1\alpha + \cdots + b_m\alpha^m).$$

Como por definición de multiplicación polinomial,  $d_j = \sum_{i=0}^j a_i b_{j-i}$ , vemos que

$$(f(x)g(x))\phi_\alpha = [(f(x))\phi_\alpha][(g(x))\phi_\alpha].$$

Así,  $\phi_\alpha$  es un homomorfismo.

La definición de  $\phi_\alpha$  aplicada a una constante polinomial  $a \in F[x]$ , donde  $a \in F$ , da  $a\phi_\alpha = a$ , de modo que  $\phi_\alpha$  transforma a  $F$  de manera isomorfa, mediante la transformación identidad. De nuevo, por definición de  $\phi_\alpha$ , tenemos que  $x\phi_\alpha = (1x)\phi_\alpha = 1\alpha = \alpha$ . ■

Señalamos que este teorema es válido con una demostración idéntica, si  $F$  y  $E$  fueran sólo anillos conmutativos con unitarios, en lugar de campos. Sin embargo, estamos interesados sólo en el caso de que sean campos.

Es difícil sobreestimar la importancia de este sencillo teorema. Es la base principal de todo nuestro trabajo posterior en teoría de campos. Es tan sencillo, que podría llamarse *observación* en lugar de teorema. Quizá no debimos haber escrito la demostración. La notación polinomial lo hace parecer tan complicada, que podría pensarse que se trata de un teorema difícil.

**Ejemplo 30.2** Sean  $F$  y  $E$ , del teorema 30.2, los campos  $\mathbf{Q}$  y  $\mathbf{R}$ , respectivamente, considérese el homomorfismo de evaluación  $\phi_0: \mathbf{Q}[x] \rightarrow \mathbf{R}$ . Aquí,

$$(a_0 + a_1x + \cdots + a_nx^n)\phi_0 = a_0 + a_10 + \cdots + a_n0^n = a_0.$$

Así, todo polinomio se transforma en su término constante. Nótese que el kernel de  $\phi_0$  es el ideal  $N$  de todos los polinomios con término constante 0. Por el teorema 29.3, la imagen  $(\mathbf{Q}[x])\phi_0 = \mathbf{Q}$  es isomorfa, de manera natural, a  $\mathbf{Q}[x]/N$ . Una clase lateral elemento de  $\mathbf{Q}[x]/N$  consta, precisamente, de todos los polinomios que tienen un término constante dado, fijo. ■

**Ejemplo 30.3** Sean  $F$  y  $E$ , del teorema 30.2, los campos  $\mathbf{Q}$  y  $\mathbf{R}$ , respectivamente, considérese el homomorfismo evaluación  $\phi_2: \mathbf{Q}[x] \rightarrow \mathbf{R}$ . Aquí,

$$(a_0 + a_1x + \cdots + a_nx^n)\phi_2 = a_0 + a_12 + \cdots + a_n2^n.$$

Nótese que

$$(x^2 + x - 6)\phi_2 = 2^2 + 2 - 6 = 0.$$

Así,  $x^2 + x - 6$  está en el kernel  $N$  de  $\phi_2$ . Es claro que

$$x^2 + x - 6 = (x - 2)(x + 3),$$

y, si se quiere, la razón por la cual  $(x^2 + x - 6)\phi_2 = 0$  es que  $(x - 2)\phi_2 = 2 - 2 = 0$ . Veremos más adelante que  $N$  es precisamente el ideal de todos los polinomios de la forma  $(x - 2)f(x)$  para  $f(x) \in \mathbf{Q}[x]$ . Aquí, la imagen de  $\mathbf{Q}[x]$  bajo  $\phi_2$  es de nuevo  $\mathbf{Q}$  y, otra vez por el teorema 29.3,  $\mathbf{Q}[x]/N$  es naturalmente isomorfo a  $\mathbf{Q}$ . ■

**Ejemplo 30.4** Sean  $F$  y  $E$ , del teorema 30.2, los campos  $\mathbf{Q}$  y  $\mathbf{C}$ , respectivamente; considérese el homomorfismo de evaluación  $\phi_i: \mathbf{Q}[x] \rightarrow \mathbf{C}$ . Aquí,

$$(a_0 + a_1x + \cdots + a_nx^n)\phi_i = a_0 + a_1i + \cdots + a_ni^n$$

y  $x\phi_i = i$ . Nótese que

$$(x^2 + 1)\phi_i = i^2 + 1 = 0,$$

de modo que  $x^2 + 1$  está en el kernel  $N$  de  $\phi_i$ . Veremos más adelante que  $N$  es precisamente el ideal de todos los polinomios de la forma  $(x^2 + 1)f(x)$  para  $f(x) \in \mathbf{Q}[x]$ . Por el teorema 29.3, la imagen  $(\mathbf{Q}[x])\phi_i$  es naturalmente isomorfa a  $\mathbf{Q}[x]/N$ . Veremos más adelante que este anillo  $(\mathbf{Q}[x])\phi_i$  consta de todos los números complejos de la forma  $q_1 + q_2i$  para  $q_1, q_2 \in \mathbf{Q}$  y que es un subcampo de  $C$ . ■

**Ejemplo 30.5** Sean  $F$  y  $E$ , del teorema 30.2, los campos  $\mathbf{Q}$  y  $\mathbf{R}$ , considérese el homomorfismo de evaluación  $\phi_\pi: \mathbf{Q}[x] \rightarrow \mathbf{R}$ . Aquí,

$$(a_0 + a_1x + \cdots + a_nx^n)\phi_\pi = a_0 + a_1\pi + \cdots + a_n\pi^n.$$

Puede probarse que  $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$  si y sólo si  $a_i = 0$  para  $i = 0, 1, \dots, n$ . Así, el kernel de  $\phi_\pi$  es  $\{0\}$  y  $\phi_\pi$  es una transformación isomorfa. Esto muestra que todos los *polinomios formales en  $\pi$  con coeficientes racionales*, forman un anillo isomorfo a  $\mathbf{Q}[x]$  de manera natural con  $x\phi_\pi = \pi$ . ■

### 30.3 EL NUEVO ENFOQUE

Completamos ahora la relación entre nuestras nuevas ideas y el concepto clásico de solución de una ecuación polinomial. En lugar de hablar de *resolver una ecuación polinomial* nos referimos a *encontrar un cero de un polinomio*.

**Definición** Sea  $F$  un subcampo de un campo  $E$  y sea  $\alpha$  un elemento de  $E$ . Sea  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  en  $F[x]$  y sea  $\phi_\alpha: F[x] \rightarrow E$  el homomorfismo de evaluación del teorema 30.2. Denotemos por  $f(\alpha)$

$$(f(x))\phi_\alpha = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Si  $f(\alpha) = 0$ , entonces  $\alpha$  es un *cero de  $f(x)$* .

En términos de esta definición podemos replantear el problema clásico de encontrar todas las soluciones reales de la ecuación polinomial  $r^2 + r - 6 = 0$  haciendo que  $F = \mathbf{Q}$  y  $E = \mathbf{R}$ , y *encontrando todas las  $\alpha \in \mathbf{R}$  tales que*

$$(x^2 + x - 6)\phi_\alpha = 0,$$

*esto es, encontrar todos los ceros de  $x^2 + x - 6$  en  $\mathbf{R}$ .* Ambos problemas tienen la misma respuesta, pues

$$\{\alpha \in \mathbf{R} \mid (x^2 + x - 6)\phi_\alpha = 0\} = \{r \in \mathbf{R} \mid r^2 + r - 6 = 0\} = \{2, -3\}.$$

Probablemente parezca que sólo hemos logrado que un problema sencillo sea bastante complicado. *Lo que hemos hecho es expresar el problema en lenguaje de transformaciones y podemos ahora, para resolverlo, usar toda la «maquinaria» referente a transformaciones que hemos desarrollado.* Recuérdese nuestro *objetivo fundamental* que podemos expresar ahora como sigue.

*Objetivo fundamental: mostrar que, para un campo  $F$ , todo polinomio no constante  $f(x) \in F[x]$  tiene un cero.*

Hagamos trampa y adelantémonos un poco para ver cómo se puede alcanzar nuestro *objetivo fundamental*. Si  $f(x)$  no tiene cero en  $F$ , tenemos que *construir*, de alguna manera, un campo  $E$  que contenga a  $F$  tal que exista  $\alpha$  en  $E$  con  $f(\alpha) = (f(x))\phi_\alpha = 0$ . ¿Cómo podemos construir  $E$ ?  $E$  debe contener a la imagen  $(F[x])\phi_\alpha$  de  $F[x]$  bajo nuestro homomorfismo de evaluación  $\phi_\alpha$ . Recuérdese, por el teorema 29.3, que  $(F[x])\phi_\alpha$  es isomorfo a  $F[x]/(\text{kernel de } \phi_\alpha)$ . Esto sugiere que tratemos de formar  $E$  construyendo un anillo factor  $F[x]/N$  para cierto ideal  $N$  en  $F[x]$ . Sabemos, por el teorema 29.4, que para que  $F[x]/N$  sea campo,  $N$  debe ser un *ideal maximal* de  $F[x]$ . Así, la tarea para la siguiente sección, como paso final para alcanzar nuestro *objetivo fundamental*, será examinar la naturaleza de los ideales en  $F[x]$ . Así es como entra en juego toda la «maquinaria» desarrollada para anillos factores y homomorfismos. Hay un dicho: «No exhiban un cañón a menos que pretendan dispararlo.» Ya exhibimos el cañón en los capítulos 28 y 29, y lo preparamos para disparar.

## Ejercicios

---

**30.1** Encuéntrense la suma y el producto de  $f(x) = 2x^3 + 4x^2 + 3x + 2$  y  $g(x) = 3x^4 + 2x + 4$  dado que  $f(x), g(x) \in \mathbf{Z}_5[x]$ .

**30.2** Considérese el elemento

$$f(x, y) = (3x^3 + 2x)y^3 + (x^2 - 6x + 1)y^2 + (x^4 - 2x)y + (x^4 - 3x^2 + 2)$$

de  $(\mathbf{Q}[x])[y]$ . Escribáse  $f(x)$  para que aparezca como un elemento de  $(\mathbf{Q}[y])[x]$ .

**30.3** Sea  $F = E = \mathbf{Z}_7$ , en el teorema 30.2. Evalúese lo siguiente para el homomorfismo de evaluación indicado  $\phi_5: \mathbf{Z}_7[x] \rightarrow \mathbf{Z}_7$ .

- |   |  |
|---|--|
| a) $(x^2 + 3)\phi_1$                    | b) $(2x^3 - x^2 + 3x + 2)\phi_0$                 |
| c) $[(x^4 + 2x)(x^3 - 3x^2 + 3)]\phi_3$ | d) $[(x^3 + 2)(4x^2 + 3)(x^7 + 3x^2 + 1)]\phi_5$ |

**30.4** Considérese el homomorfismo de evaluación  $\phi_5: \mathbf{Q}[x] \rightarrow \mathbf{R}$ . Encuéntrense seis elementos en el kernel de  $\phi_5$ .

**30.5** Encuéntrense todos los ceros en  $\mathbf{Z}_5$  de  $(x^5 + 3x^3 + x^2 + 2x) \in \mathbf{Z}_5[x]$ . [Sugerencia: sólo hay cinco candidatos. Inténtese trabajar con ellos.]

**30.6** Pruébese que si  $D$  es un dominio entero, entonces  $D[x]$  es un dominio entero.

## 30.7 ¿Falso o verdadero?

- a) El polinomio  $(a_nx^n + \cdots + a_1x + a_0) \in R[x]$  es cero si y sólo si  $a_i = 0$ , para  $i = 0, 1, \dots, n$ .
- b) Si  $R$  es un anillo comutativo, entonces  $R[x]$  es comutativo.
- c) Si  $D$  es un dominio entero, entonces  $D[x]$  es un dominio entero.
- d) Si  $R$  es un anillo que contiene divisores de cero, entonces  $R[x]$  tiene divisores de cero.
- e) Si  $R$  es un anillo y  $f(x)$  y  $g(x)$  en  $R[x]$  son de grado 3 y 4 respectivamente, entonces  $f(x)g(x)$  puede ser de grado 8 en  $R[x]$ .
- f) Si  $R$  es cualquier anillo y  $f(x)$  y  $g(x)$  en  $R[x]$  son de grado 3 y 4 respectivamente, entonces  $f(x)g(x)$  siempre es de grado 7.
- g) Si  $F$  es un subcampo de un campo  $E$  y  $a \in E$  es un cero de  $f(x) \in F[x]$ , entonces  $a$  es un cero de  $h(x) = f(x)g(x)$  para todas las  $g(x) \in F[x]$ .
- h) El homomorfismo de evaluación  $\phi_a$  del teorema 30.2 es una extensión de la transformación inyectiva  $i:F \rightarrow E$  a  $F[x]$  donde  $(a)i = a$  para  $a \in F$ .
- i) Si  $F$  es un subcampo de un campo  $E$  y  $f(x) \in F[x]$ , entonces el conjunto de todos los ceros de  $f(x)$  en  $E$  es un ideal de  $E$ .
- j) Si  $F$  es un subcampo de un campo  $E$  y  $\alpha \in E$ , entonces el conjunto de todos los  $f(x) \in F[x]$  tal que  $f(\alpha) = 0$  es un ideal de  $F[x]$ .

30.8 Pruébese la ley distributiva izquierda para  $R[x]$  donde  $R$  es un anillo y  $x$  es una indeterminada.

30.9 Sea  $F$  un campo y sea  $D$  la transformación de diferenciación formal de polinomios, de modo que

$$D(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

(Escribimos la  $D$  de la transformación a la izquierda, de acuerdo con la convención usual en análisis.)

- a) Muéstrese que  $D:F[x] \rightarrow F[x]$  es un automorfismo de grupo de  $\langle F[x], + \rangle$ . ¿Es  $D$  un automorfismo de anillo?
- b) Encuéntrese el kernel de  $D$ .
- c) Encuéntrese la imagen de  $F[x]$  bajo  $D$ .

30.10 Sea  $\phi_s:\mathbb{Z}_5[x] \rightarrow \mathbb{Z}_5$  un homomorfismo de evaluación, como en el teorema 30.2. Usese el teorema de Fermat para evaluar  $(x^{231} + 3x^{117} - 2x^{53} + 1)\phi_3$ .

30.11 Usese el teorema de Fermat para encontrar todos los ceros en  $\mathbb{Z}_5$  de

$$2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}.$$

30.12 Sea  $D$  un dominio entero y  $x$  una indeterminada.

- a) Describanse las unidades en  $D[x]$ .
- b) Encuéntrense las unidades en  $\mathbb{Z}[x]$ .
- c) Encuéntrense las unidades en  $\mathbb{Z}_7[x]$ .

## 276 ANILLOS DE POLINOMIOS

**30.13** Sea  $F$  un subcampo de un campo  $E$ .

a) Definase un *homomorfismo de evaluación*

$$\phi_{\alpha_1, \dots, \alpha_n}: F[x_1, \dots, x_n] \rightarrow E \quad \text{para } \alpha_i \in E,$$

y enúnciese el análogo del teorema 30.2.

- b) Con  $E = F = \mathbb{Q}$ , calcúlese  $(x_1^2 x_2^3 + 3x_1^4 x_2) \phi_{-3, 2}$ .
- c) Definase el concepto de *cero de un polinomio*  $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$  de manera análoga a la definición dada para cero de  $f(x)$ .

**30.14** Sea  $F$  un campo. Muéstrese que todos los polinomios con término constante  $a_0 = 0$  forman un ideal  $\langle x \rangle$  de  $F[x]$ .

**30.15** Sea  $F$  un campo y sea  $\langle x \rangle$  el ideal en  $F[x]$ , definido en el ejercicio 30.14. Muéstrese que  $F[x]/\langle x \rangle$  es un campo isomorfo a  $F$ .

- a) mostrando directamente que cada clase residual en  $F[x]/\langle x \rangle$  contiene exactamente un elemento de  $F$  que puede seleccionarse como representante para calcular en  $F[x]/\langle x \rangle$ ;
- b) considerando el homomorfismo de evaluación  $\phi_0: F[x] \rightarrow F$ , según se definió en el teorema 30.2, muéstrese que  $\langle x \rangle$  es el kernel de  $\phi_0$  y aplíquese el teorema 29.3.

**30.16** Sea  $R$  un anillo y  $R^R$  el conjunto de todas las funciones que van de  $R$  a  $R$ . Para  $\phi, \psi \in R^R$  definase la suma  $\phi + \psi$  por

$$r(\phi + \psi) = (r\phi) + (r\psi)$$

y el producto  $\phi \cdot \psi$  por

$$r(\phi \cdot \psi) = (r\phi)(r\psi)$$

para  $r \in R$ . Nótese que  $\cdot$  no es la composición de funciones. Muéstrese que  $\langle R^R, +, \cdot \rangle$  es un anillo.

**30.17** Con referencia al ejercicio 30.16, sea  $F$  un campo. Un elemento  $\phi$  de  $F^F$  es una función polinomial en  $F$ , si existe  $f(x) \in F[x]$  tal que  $a\phi = f(a)$  para todas las  $a \in F$ .

- a) Muéstrese que el conjunto  $P_F$  de todas las funciones polinomiales en  $F$  forma un subanillo de  $F^F$ .
- b) Muéstrese que el anillo  $P_F$  no necesariamente es isomorfo a  $F[x]$ . [Sugerencia: muéstrese que si  $F$  es un campo finito,  $P_F$  y  $F[x]$  ni siquiera tienen el mismo número de elementos.]

**30.18** Remítase a los ejercicios 30.16 y 30.17 para las siguientes preguntas:

- a) ¿Cuántos elementos hay en  $\mathbb{Z}_2^{\mathbb{Z}_2^2}$ ? ¿y en  $\mathbb{Z}_3^{\mathbb{Z}_3^3}$ ?
- b) Clasifiquense  $\langle \mathbb{Z}_2^{\mathbb{Z}_2^2}, + \rangle$  y  $\langle \mathbb{Z}_3^{\mathbb{Z}_3^3}, + \rangle$  mediante el teorema 9.3, el teorema fundamental de los grupos abelianos finitamente generados.
- c) Muéstrese que si  $F$  es un campo finito, entonces  $F^F = P_F$ . [Sugerencia: es claro que  $P_F \subseteq F^F$ . Sea  $F$  con elementos  $a_1, \dots, a_n$ . Nótese que si

$$f(x) = c(x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n),$$

entonces,  $f_j(a_j) = 0$  para  $j \neq i$ , y el valor  $f_i(a_i)$  puede controlarse con la selección de  $c \in F$ . Usese lo anterior para mostrar que toda función en  $F$  es una función polinomial.]

## 31

# Factorización de polinomios sobre un campo

## 31.1 EL ALGORITMO DE LA DIVISIÓN EN $F[x]$

Al final de la sección anterior, indicamos que el paso final para alcanzar nuestro *objetivo fundamental* sería el estudio de las estructuras de ideal en anillos de polinomios  $F[x]$  donde  $F$  es un campo. De particular interés es la caracterización de los ideales maximales de  $F[x]$  para determinar cuándo  $F[x]/N$  es un campo. Puede parecer extraño que debamos estudiar factorización de polinomios para esto, pero es razonable en dos sentidos. Primero, nuestro propósito principal es estudiar ceros de polinomios y suponer que  $f(x) \in F[x]$  se factoriza en  $F[x]$  de manera que  $f(x) = g(x)h(x)$  para  $g(x), h(x) \in F[x]$ . Si  $F \leq E$  y  $\alpha \in E$ , entonces  $f(x)$  se reduce al problema de encontrar un cero de un factor de  $f(x)$ . Segundo, deseamos encontrar ideales maximales de  $F[x]$ . Ahora, cualquier ideal maximal  $M$  es también un ideal primo. Por tanto, si  $f(x) = g(x)h(x)$  y  $f(x) \in M$  para un ideal maximal  $M$ , entonces, podemos tener que  $g(x) \in M$  o  $h(x) \in M$ . Estas dos consideraciones sugieren el estudio de factorización de polinomios en  $F[x]$ .

El siguiente teorema es la herramienta básica para nuestro trabajo en esta sección. El estudiante debe notar la analogía con el lema 6.1, el algoritmo de la división para  $\mathbf{Z}$ , cuya importancia ha quedado ampliamente establecida. El algoritmo de la división se tratará en un contexto más general en el capítulo 33, marcado con asterisco.

**Teorema 31.1 (Algoritmo de la división para  $F[x]$ )** Sean

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

y

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$$

dos elementos de  $F[x]$ , con  $a_n$  y  $b_m$  ambos elementos distintos del cero de  $F$  y  $m > 0$ . Entonces, existen polinomios únicos  $q(x)$  y  $r(x)$  en  $F[x]$  tales que  $f(x) = g(x)q(x) + r(x)$  donde el grado de  $r(x)$  es menor que  $m = \text{grado de } g(x)$ .

*Demostración* Considérese el conjunto  $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$ . Sea  $r(x)$  un elemento de grado minimal en  $S$ . Entonces,

$$f(x) = g(x)q(x) + r(x)$$

para alguna  $q(x) \in F[x]$ . Debemos mostrar que el grado de  $r(x)$  es menor que  $m$ . Supóngase que

$$r(x) = c_t x^t + c_{t-1} x^{t-1} + \cdots + c_0,$$

con  $c_j \in F$  y  $c_t \neq 0$  si  $t \neq 0$ . Si  $t \geq m$ , entonces

$$f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x) = r(x) - (c_t/b_m)x^{t-m}g(x), \quad [31.1]$$

y lo último es de la forma

$$r(x) - (c_t x^t + \text{ términos de grado menor}),$$

lo cual es un polinomio de grado menor que  $t$ , el grado de  $r(x)$ . Sin embargo, el polinomio en la ecuación [31.1] puede escribirse en la forma

$$f(x) - g(x)[q(x) + (c_t/b_m)x^{t-m}],$$

de modo que está en  $S$ , contradiciendo el hecho de que  $r(x)$  se seleccionó con grado minimal en  $S$ . Así, el grado de  $r(x)$  es menor que  $m = \text{grado } g(x)$ .

Para la unicidad, si

$$f(x) = g(x)q_1(x) + r_1(x)$$

y

$$f(x) = g(x)q_2(x) + r_2(x),$$

entonces, por sustracción tenemos

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Como el grado de  $r_2(x) - r_1(x)$  es menor que el grado de  $g(x)$ , esto puede valer sólo si  $q_1(x) - q_2(x) = 0$  o  $q_1(x) = q_2(x)$ . Entonces, debemos tener  $r_2(x) - r_1(x) = 0$  o  $r_1(x) = r_2(x)$ . ■

Pueden calcularse los polinomios  $q(x)$  y  $r(x)$  del teorema 31.1, mediante *división*, así como se dividían polinomios en  $\mathbb{R}[x]$  en la escuela secundaria. Después de los corolarios siguientes, damos algunos ejemplos.

Sin duda el lector conoce, por el álgebra de secundaria, el primer corolario para el caso particular  $\mathbf{R}[x]$ . Expresamos la demostración en términos del enfoque de transformaciones (homomorfismos), descrito en el capítulo 30.

**Corolario 1** *Un elemento  $a \in F$  es un cero de  $f(x) \in F[x]$  si y sólo si  $x - a$  es factor de  $f(x)$  en  $F[x]$ .*

*Demostración* Supóngase que para  $a \in F$  tenemos  $f(a) = 0$ . Por el teorema 31.1, existen  $q(x), r(x) \in F[x]$  tales que

$$f(x) = (x - a)q(x) + r(x),$$

donde el grado de  $r(x)$  es menor que 1. Entonces, debemos tener  $r(x) = c$  para  $c \in F$ , de modo que

$$f(x) = (x - a)q(x) + c.$$

Aplicando el homomorfismo de evaluación  $\phi_a: F[x] \rightarrow F$ , del teorema 30.2, encontramos que

$$0 = f(a) = 0q(a) + c,$$

de modo que  $c = 0$ . Entonces,  $f(x) = (x - a)q(x)$  de modo que  $(x - a)$  es un factor de  $f(x)$ .

Recíprocamente, si  $x - a$  es un factor de  $f(x)$  en  $F[x]$  donde  $a \in F$ , entonces, aplicando nuestro homomorfismo de evaluación  $\phi_a$  a  $f(x) = (x - a)q(x)$  tenemos que  $f(a) = 0q(a) = 0$ . ■

El siguiente corolario también parecerá conocido.

**Corolario 2** *Un polinomio distinto de cero  $f(x) \in F[x]$  de grado  $n$  puede tener a lo más  $n$  ceros en un campo  $F$ .*

*Demostración* El corolario anterior muestra que si  $a_1 \in F$  es un cero de  $f(x)$ , entonces

$$f(x) = (x - a_1)q_1(x),$$

donde, claramente, el grado de  $q_1(x)$  es  $n - 1$ . Un cero  $a_2 \in F$  de  $q_1(x)$  resultará en la factorización

$$f(x) = (x - a_1)(x - a_2)q_2(x).$$

Continuando este proceso, llegamos a

$$f(x) = (x - a_1) \cdots (x - a_r)q_r(x),$$

donde  $q_r(x)$  no tiene más ceros en  $F$ . Claramente,  $r \leq n$ . Además, si  $b \neq a_i$  para  $i = 1, \dots, r$  y  $b \in F$ , entonces

$$f(b) = (b - a_1) \cdots (b - a_r)q_r(b) \neq 0,$$

puesto que  $F$  no tiene divisores de 0 y, por construcción, ninguno de  $b = a_i$  o  $q_r(b)$  son 0. De aquí que las  $a_i$  para  $i = 1, \dots, r \leq n$  son, todas, ceros en  $F$  de  $f(x)$ . ■

**Ejemplo 31.1** Trabajemos con polinomios en  $\mathbf{Z}_5[x]$  y dividamos

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$$

entre  $g(x) = x^2 - 2x + 3$  para encontrar  $q(x)$  y  $r(x)$  del teorema 31.1. Debe ser fácil seguir la división; pero recuérdese que estamos en  $\mathbf{Z}_5[x]$ , de modo que, por ejemplo,  $4x - (-3x) = 2x$ .

$$\begin{array}{r} x^2 - x - 3 \\ \hline x^2 - 2x + 3 | x^4 - 3x^3 + 2x^2 + 4x - 1 \\ x^4 - 2x^3 + 3x^2 \\ \hline - x^3 - x^2 + 4x \\ - x^3 + 2x^2 - 3x \\ \hline - 3x^2 + 2x - 1 \\ - 3x^2 + x - 4 \\ \hline x + 3 \end{array}$$

Así,

$$x^4 - 3x^3 + 2x^2 + 4x - 1 = (x^2 - 2x + 3)(x^2 - x - 3) + (x + 3),$$

de modo que  $q(x) = x^2 - x - 3$  y  $r(x) = x + 3$ . ■

**Ejemplo 31.2** Al trabajar de nuevo en  $\mathbf{Z}_5[x]$ , nótese que 1 es un cero de

$$(x^4 + 3x^3 + 2x + 4) \in \mathbf{Z}_5[x].$$

Así, por el corolario 1 del teorema 31.1, podemos factorizar  $x^4 + 3x^3 + 2x + 4$  en  $(x - 1)q(x)$  en  $\mathbf{Z}_5[x]$ . Se usará de nuevo la división.

$$\begin{array}{r} x^3 + 4x^2 + 4x + 1 \\ \hline x - 1 | x^4 + 3x^3 + 2x + 4 \\ x^4 - x^3 \\ \hline 4x^3 + 2x \\ 4x^3 - 4x^2 \\ \hline 4x^2 + 2x \\ 4x^2 - 4x \\ \hline x + 4 \\ x - 1 \\ \hline 0 \end{array}$$

Así,  $x^4 + 3x^3 + 2x + 4 = (x - 1)(x^3 + 4x^2 + 4x + 1)$  en  $\mathbb{Z}_5[x]$ . Como 1 también es un cero de  $x^3 + 4x^2 + 4x + 1$ , podemos dividir este polinomio entre  $x - 1$  y obtener

$$\begin{array}{c} x^2 + 4 \\ \hline x - 1 | x^3 + 4x^2 + 4x + 1 \\ \quad x^3 - x^2 \\ \hline \quad 0 + 4x + 1 \\ \quad 4x - 4 \\ \hline \quad 0 \end{array}$$

Como  $x^2 + 4$  tiene todavía un cero, podemos dividir otra vez entre  $x - 1$  y obtener

$$\begin{array}{c} x + 1 \\ \hline x - 1 | x^2 + 4 \\ \quad x^2 - x \\ \hline \quad x + 4 \\ \quad x - 1 \\ \hline \quad 0 \end{array}$$

Así,  $x^4 + 3x^3 + 2x + 4 = (x - 1)^2(x + 1)$  en  $\mathbb{Z}_5[x]$ . ■

Es indudable que la técnica de *división sintética* es válida en  $F[x]$ , si se recuerda.

## 31.2 POLINOMIOS IRREDUCIBLES

Nuestra siguiente definición destaca un tipo de polinomios en  $F[x]$  que será de enorme importancia para nosotros. De nuevo, lo más probable es que ya se conozca el concepto. En realidad, se está haciendo álgebra de secundaria en un contexto más general.

**Definición** Un polinomio no constante  $f(x) \in F[x]$  es *irreducible sobre  $F$*  o es un *polinomio irreducible en  $F[x]$*  si  $f(x)$  no puede expresarse como producto  $g(x)h(x)$  de dos polinomios  $g(x)$  y  $h(x)$  en  $F[x]$ , ambos de grado menor que el grado de  $f(x)$ .

Nótese que la definición anterior trata del concepto de *irreducible sobre  $F$*  y no sólo del concepto de *irreducible*. Un polinomio  $f(x)$  puede ser irreducible sobre  $F$  pero puede no ser irreducible, visto sobre un campo mayor  $E$  que contenga a  $F$ . Ilustremos esto.

**Ejemplo 31.3** El teorema 27.1 mostró que  $x^2 - 2$  visto en  $\mathbb{Q}[x]$  no tiene ceros en  $\mathbb{Q}$ . Esto muestra que  $x^2 - 2$  es irreducible sobre  $\mathbb{Q}$ , pues una factorización  $x^2 - 2 = (ax + b)(cx + d)$  para  $a, b, c, d \in \mathbb{Q}$  daria lugar a ceros de  $x^2 - 2$  en  $\mathbb{Q}$ . Sin embargo,  $x^2 - 2$  visto en  $\mathbb{R}[x]$  no es irreducible sobre  $\mathbb{R}$ , pues  $x^2 - 2$  se factoriza en  $\mathbb{R}[x]$  en  $(x - \sqrt{2})(x + \sqrt{2})$ . ■

Es conveniente que el estudiante recuerde que *las unidades en  $F[x]$  son precisamente los elementos distintos de cero de  $F$* . Así, podríamos haber definido un polinomio irreducible  $f(x)$ , como un polinomio no constante, tal que en cualquier factorización  $f(x) = g(x)h(x)$  en  $F[x]$ ,  $g(x)$  o  $h(x)$  es una unidad. Este punto de vista se desarrollará en los siguientes capítulos, con asterisco, que tratan de factorización en anillos más generales que  $F[x]$ .

**Ejemplo 31.4** Mostrar que  $f(x) = x^3 + 3x + 2$  visto en  $\mathbb{Z}_5[x]$  es irreducible sobre  $\mathbb{Z}_5$ . Si  $x^3 + 3x + 2$  se factoriza en  $\mathbb{Z}_5[x]$  en polinomios de grado menor, entonces existiría al menos un factor lineal de  $f(x)$  de la forma  $x - a$  para algún  $a \in \mathbb{Z}_5$ . Pero entonces, por el corolario 1 del teorema 31.1,  $f(a)$  sería cero. Sin embargo,  $f(0) = 2$ ,  $f(1) = 1$ ,  $f(-1) = -2$ ,  $f(2) = 1$  y  $f(-2) = -2$ , lo cual muestra que  $f(x)$  no tiene ceros en  $\mathbb{Z}_5$ . Así,  $f(x)$  es irreducible sobre  $\mathbb{Z}_5$ . Esta prueba de irreducibilidad mediante la búsqueda de ceros, funciona muy bien para polinomios cuadráticos y cúbicos, sobre campo finito, con un pequeño número de elementos. ■

Los polinomios irreducibles desempeñarán de ahora en adelante un papel muy importante en nuestro trabajo. El problema de determinar si un  $f(x) \in F[x]$  dado es irreducible sobre  $F$ , puede ser difícil. Damos ahora algunos criterios de irreducibilidad útil en ciertos casos. En los ejemplos 31.3 y 31.4 se ilustró una técnica para determinar irreducibilidad de polinomios cuadráticos y cúbicos. La formalizamos en un teorema.

**Teorema 31.2** *Sea  $f(x) \in F[x]$  y sea  $f(x)$  de grado 2 ó 3. Entonces,  $f(x)$  es reducible sobre  $F$  si y sólo si tiene un cero en  $F$ .*

**Demostración** Si  $f(x)$  es reducible de modo que  $f(x) = g(x)h(x)$  donde el grado de  $g(x)$  y el grado de  $h(x)$  son ambos menores que el grado de  $f(x)$ , entonces como  $f(x)$  es cuadrática o cúbica,  $g(x)$  o  $h(x)$  es de grado 1. Si  $g(x)$  es de grado 1, entonces, excepto por un posible factor en  $F$ ,  $g(x)$  es de la forma  $x - a$ . Entonces,  $g(a) = 0$ , lo cual implica que  $f(a) = 0$ , de modo que  $f(x)$  tiene un cero en  $F$ .

Recíprocamente, el corolario 1 del teorema 31.1 muestra que si  $f(a) = 0$  para  $a \in F$ , entonces,  $x - a$  es un factor de  $f(x)$ , así,  $f(x)$  es reducible. ■

Pasemos a algunas condiciones para la irreducibilidad sobre  $\mathbb{Q}$ , de polinomios en  $\mathbb{Q}[x]$ . La condición más importante que daremos, está contenida en el siguiente teorema. No probaremos el teorema aquí; se demuestra en una situación más general en el capítulo 32, marcado con asterisco (véase el corolario del lema 32.6).

**Teorema 31.3** Si  $f(x) \in \mathbb{Z}[x]$ , entonces  $f(x)$  se factoriza en un producto de dos polinomios de grados menores  $r$  y  $s$  en  $\mathbb{Q}[x]$  si y sólo si tiene dicha factorización con polinomios de los mismos grados  $r$  y  $s$  en  $\mathbb{Z}[x]$ . ■

**Demostración** Véase el corolario del lema 32.6.

**Corolario** Si  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  está en  $\mathbb{Z}[x]$  con  $a_0 \neq 0$ , y si  $f(x)$  tiene un cero en  $\mathbb{Q}$ , entonces, tiene un cero  $m$  en  $\mathbb{Z}$ , y  $m$  debe dividir  $a_0$ .

**Demostración** Si  $f(x)$  tiene un cero  $a$  en  $\mathbb{Q}$ , entonces, por el corolario 1 del teorema 31.1,  $f(x)$  tiene un factor lineal  $x - a$  en  $\mathbb{Q}[x]$ . Pero entonces, por el teorema 31.3,  $f(x)$  tiene una factorización con un factor lineal en  $\mathbb{Z}[x]$  de modo que para algún  $m \in \mathbb{Z}$  debemos tener

$$f(x) = (x - m)(x^{n-1} + \cdots + a_0/m).$$

Así,  $a_0/m$  está en  $\mathbb{Z}$ , de modo que  $m$  divide  $a_0$ . ■

**Ejemplo 31.5** Este corolario del teorema 31.3 proporciona otra demostración de la irreducibilidad de  $x^2 - 2$  sobre  $\mathbb{Q}$ , pues, por el teorema 31.2,  $x^2 - 2$  se factoriza de manera no trivial en  $\mathbb{Q}[x]$  si y sólo si tiene un cero en  $\mathbb{Q}$ . Por el corolario del teorema 31.3, tiene un cero en  $\mathbb{Q}$  si y sólo si tiene un cero en  $\mathbb{Z}$  y, más aún, las únicas posibilidades son los divisores  $\pm 1$  y  $\pm 2$  de 2. Es fácil mostrar que ninguno de estos números es un cero de  $x^2 - 2$ . ■

**Ejemplo 31.6** Usemos el teorema 31.3 para mostrar que

$$f(x) = x^4 - 2x^2 + 8x + 1$$

visto en  $\mathbb{Q}[x]$  es irreducible sobre  $\mathbb{Q}$ . Si  $f(x)$  tiene un factor lineal en  $\mathbb{Q}[x]$ , entonces tiene un cero en  $\mathbb{Z}$  y, por el corolario del teorema 31.3, este cero sería divisor en  $\mathbb{Z}$  de 1, esto es,  $\pm 1$ . Pero  $f(1) = 8$  y  $f(-1) = -8$  así que dicha factorización es imposible.

Si  $f(x)$  se factoriza en dos factores cuadráticos en  $\mathbb{Q}[x]$ , entonces, por el teorema 31.3, tiene una factorización

$$(x^2 + ax + b)(x^2 + cx + d)$$

en  $\mathbb{Z}[x]$ . Al igualar los coeficientes de potencias de  $x$ , debemos tener

$$bd = 1, \quad ad + bc = 8, \quad ac + b + d = -2, \quad y \quad a + c = 0$$

para enteros,  $a, b, c, d \in \mathbb{Z}$ . De  $bd = 1$  vemos que  $b = d = 1$  o  $b = d = -1$ . Si  $b = d = 1$ , entonces  $ac + b + d = -2$  implica que  $ac = -4$ , lo cual, con  $a + c = 0$ , da  $a = -c = \pm 2$ . Si  $b = d = -1$ , entonces  $ac + b + d = -2$  implica que  $ac = 0$ ,

de modo que  $a = -c = 0$ . Ninguna combinación de los números que surgen de estas posibilidades puede hacer  $ad + bc$  tan grande como 8. Así, también es imposible una factorización en dos polinomios cuadráticos y  $f(x)$  es irreducible sobre  $\mathbb{Q}$ . ■

Concluimos nuestros criterios de irreducibilidad con el famoso criterio de Eisenstein para irreducibilidad. En el ejercicio 31.20 se da un criterio adicional y muy útil.

**Teorema 31.4 (Eisenstein)** *Sea  $p \in \mathbb{Z}$  un primo. Supóngase que  $f(x) = a_nx^n + \dots + a_0$  está en  $\mathbb{Z}[x]$  y  $a_n \not\equiv 0 \pmod{p}$ , pero  $a_i \equiv 0 \pmod{p}$  para  $i < n$ , con  $a_0 \not\equiv 0 \pmod{p^2}$ . Entonces,  $f(x)$  es irreducible sobre  $\mathbb{Q}$ .*

*Demostración* Por el teorema 31.3, sólo necesitamos mostrar que  $f(x)$  no se factoriza en polinomios de grado menor en  $\mathbb{Z}[x]$ . Si

$$f(x) = (b_r x^r + \dots + b_0)(c_s x^s + \dots + c_0)$$

es una factorización en  $\mathbb{Z}[x]$ , con  $b_r \neq 0$ ,  $c_s \neq 0$  y  $r, s < n$ , entonces,  $a_0 \not\equiv 0 \pmod{p^2}$  implica que  $b_0$  y  $c_0$  no son, ambas, congruentes con 0 módulo  $p$ . Supóngase que  $b_0 \not\equiv 0 \pmod{p}$  y  $c_0 \equiv 0 \pmod{p}$ . Ahora,  $a_n \not\equiv 0 \pmod{p}$  implica que  $b_r, c_s \not\equiv 0 \pmod{p}$ , puesto que  $a_n = b_r c_s$ . Sea  $m$  el menor valor de  $k$  tal que  $c_k \not\equiv 0 \pmod{p}$ . Entonces,

$$a_m = b_0 c_m + b_1 c_{m-1} + \dots + b_{m-i} c_i$$

para alguna  $i$ ,  $0 \leq i < m$ . Ahora, ni  $b_0$  ni  $c_m$  son congruentes con 0 módulo  $p$  y  $c_{m-1}, \dots, c_i$  congruentes todos con 0 módulo  $p$ , implica que  $a_m \not\equiv 0 \pmod{p}$ , de modo que  $m = n$ . En consecuencia,  $s = n$ , y se contradice la hipótesis de que  $s < n$ , esto es, que la factorización era no trivial. ■

Nótese que si tomamos  $p = 2$ , el criterio de Eisenstein presenta otra demostración de la irreducibilidad de  $x^2 - 2$  sobre  $\mathbb{Q}$ .

**Ejemplo 31.7** Sea  $p = 3$ ; por el teorema 31.4,

$$25x^5 - 9x^4 + 3x^2 - 12$$

es irreducible sobre  $\mathbb{Q}$ . ■

**Corolario** *El polinomio ciclotómico*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

*es irreducible sobre  $\mathbb{Q}$  para cualquier primo  $p$ .*

*Demostración* De nuevo, por el teorema 31.3, sólo necesitamos considerar factorizaciones en  $\mathbb{Z}[x]$ . Sea

$$g(x) = \Phi_p(x + 1) = \frac{(x + 1)^p - 1}{(x + 1) - 1} = \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + px}{x}.$$

Entonces,

$$g(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + p$$

satisface el criterio de Eisenstein para el primo  $p$  y es, así, irreducible sobre  $\mathbb{Q}$ . Pero claramente, si  $\Phi_p(x) = h(x)r(x)$  fuera una factorización no trivial de  $\Phi_p(x)$  en  $\mathbb{Z}[x]$ , entonces

$$\Phi_p(x + 1) = g(x) = h(x + 1)r(x + 1)$$

daría una factorización no trivial de  $g(x)$  en  $\mathbb{Z}[x]$ . Así,  $\Phi_p(x)$  también debe ser irreducible sobre  $\mathbb{Q}$ . ■

### 31.3 ESTRUCTURA DE IDEAL EN $F[x]$

Damos la siguiente definición para un anillo comunitativo  $R$  con unitario en general, aunque sólo nos interese el caso  $R = F[x]$ , donde  $F$  es un campo. Sabemos que para un anillo comunitativo  $R$  con unitario y  $a \in R$ , el conjunto  $\{ra \mid r \in R\}$  es un ideal en  $R$  que contiene el elemento  $a$ .

**Definición** Si  $R$  es un anillo comunitativo con unitario y  $a \in R$ , el ideal  $\{ra \mid r \in R\}$  de todos los múltiplos de  $a$  es el **ideal principal generado por  $a$**  y se denota por  $\langle a \rangle$ . Un ideal  $N$  de  $R$  es un **ideal principal** si  $N = \langle a \rangle$  para alguna  $a \in R$ .

**Ejemplo 31.8** Es claro que el ideal  $\langle x \rangle$  en  $F[x]$  consta de todos los polinomios en  $F[x]$  que tengan término constante cero. ■

El siguiente teorema es otra aplicación sencilla pero importante del teorema 31.1, que es la herramienta básica en esta sección. Quizás el lector ya esté preparado para probar el teorema, si su profesor pide demostraciones. La demostración de este teorema es al algoritmo de la división en  $F[x]$ , como la demostración de que un subgrupo de un grupo ciclico es ciclico lo es al algoritmo de la división en  $\mathbb{Z}$ .

**Teorema 31.5** Si  $F$  es un campo, todo ideal en  $F[x]$  es principal.

*Demostración* Sea  $N$  un ideal de  $F[x]$ . Si  $N = \{0\}$ , entonces  $N = \langle 0 \rangle$ . Supóngase que  $N \neq \{0\}$  y sea  $g(x)$  un elemento distinto de cero de  $N$  de grado minimal. Si el grado de  $g(x)$  es 0, entonces  $g(x) \in F$  y es una unidad, de modo que, por el teorema 28.4,  $N = F[x] = \langle 1 \rangle$  y, así,  $N$  es principal. Si el grado de  $g(x)$  es  $\geq 1$ , sea  $f(x)$  cualquier elemento de  $N$ . Entonces, por el teorema 31.1,  $f(x) = g(x)q(x) + r(x)$  donde  $(\text{grado } r(x)) < (\text{grado } g(x))$ . Ahora,  $f(x) \in N$  y  $g(x) \in N$  implica que  $f(x) - g(x)q(x) = r(x)$  está en  $N$ , por definición de ideal. Como  $g(x)$  era un elemento distinto de cero de grado minimal en  $N$ , debemos tener  $r(x) = 0$ . Así,  $f(x) = g(x)q(x)$  y  $N = \langle g(x) \rangle$ . ■

Ahora podemos alcanzar el objetivo de caracterizar los ideales maximales de  $F[x]$ .

**Teorema 31.6** *Un ideal  $\langle p(x) \rangle \neq \{0\}$  de  $F[x]$  es maximal si y sólo si  $p(x)$  es irreducible sobre  $F$ .*

*Demostración* Supóngase que  $\langle p(x) \rangle \neq \{0\}$  es un ideal maximal de  $F[x]$ . Entonces,  $\langle p(x) \rangle \neq F[x]$ , de modo que  $p(x) \notin F$ . Sea  $p(x) = f(x)g(x)$  una factorización de  $p(x)$  en  $F[x]$ . Como  $\langle p(x) \rangle$  es un ideal maximal y, por tanto, también un ideal primo,  $(f(x)g(x)) \in \langle p(x) \rangle$  implica que  $f(x) \in \langle p(x) \rangle$  o  $g(x) \in \langle p(x) \rangle$ , esto es,  $f(x)$  o  $g(x)$  tiene como factor a  $p(x)$ . Pero, entonces, no podemos tener que los grados de  $f(x)$  y de  $g(x)$  sean ambos menores que el grado de  $p(x)$ . Esto muestra que  $p(x)$  es irreducible sobre  $F$ .

En forma reciproca, si  $p(x)$  es irreducible sobre  $F$ , supóngase que  $N$  es un ideal tal que  $\langle p(x) \rangle \subseteq N \subseteq F[x]$ . Ahora, por el teorema 31.5,  $N$  es un ideal principal, de modo que  $N = \langle g(x) \rangle$  para algún  $g(x) \in N$ . Entonces,  $p(x) \in N$  implica que  $p(x) = g(x)q(x)$  para algún  $q(x) \in F[x]$ . Pero  $p(x)$  es irreducible, lo cual implica que  $g(x)$  o  $q(x)$  es de grado 0. Si  $g(x)$  es de grado 0, esto es, una constante en  $F$ , distinta de 0, entonces  $g(x)$  es una unidad en  $F[x]$ , de modo que  $\langle g(x) \rangle = N = F[x]$ . Si  $q(x)$  es de grado 0, entonces  $q(x) = c$  donde  $c \neq 0$  y  $g(x) = (1/c)p(x)$  está en  $\langle p(x) \rangle$ , luego  $N = \langle p(x) \rangle$ . Así,  $\langle p(x) \rangle \subset N \subset F[x]$  es imposible, de modo que  $\langle p(x) \rangle$  es maximal. ■

**Ejemplo 31.9** El ejemplo 31.4 muestra que  $x^3 - 3x + 2$  es irreducible en  $\mathbb{Z}[x]$ . Así,  $\mathbb{Z}_5[x]/\langle x^3 - 3x + 2 \rangle$  es un campo. De manera análoga, el teorema 7.1 muestra que  $x^2 - 2$  es irreducible en  $\mathbb{Q}[x]$ , de modo que  $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$  un campo. Se examinarán dichos campos con más detalle posteriormente. ■

## 31.4 UNICIDAD DE LA FACTORIZACION EN $F[x]$

Demostraremos que los polinomios en  $F[x]$  se pueden factorizar en un producto de polinomios irreducibles en  $F[x]$ , de manera esencialmente única, cosa que se puede deducir con facilidad del trabajo que el lector hizo en secundaria con  $\mathbb{Z}$ .

Consideraremos factorizaciones únicas en situaciones más generales en el siguiente capítulo, marcado con asterisco. Como ahora resulta fácil obtener el resultado para  $F[x]$ , decidimos incluir aquí este caso especial. Trataremos exclusivamente con campos en las partes restantes, no marcadas con asterisco, de modo que este caso particular es todo lo que necesitamos para el trabajo.

Para  $f(x), g(x) \in F[x]$  decimos que  $g(x)$  divide  $f(x)$  en  $F[x]$  si existe  $q(x) \in F[x]$  tal que  $f(x) = g(x)q(x)$ .

**Teorema 31.7** *Sea  $p(x)$  un polinomio irreducible en  $F[x]$ . Si  $p(x)$  divide  $r(x)s(x)$  para  $r(x), s(x) \in F[x]$ , entonces  $p(x)$  divide  $r(x)$  o  $p(x)$  divide a  $s(x)$ .*

*Demostración* Supóngase que  $p(x)$  divide  $r(x)s(x)$ . Entonces,  $r(x)s(x) \in \langle p(x) \rangle$  que, por el teorema 31.6, es maximal. Por tanto,  $\langle p(x) \rangle$  es un ideal primo, por el corolario al teorema 29.5. De aquí,  $r(x)s(x) \in \langle p(x) \rangle$  implica que  $r(x) \in \langle p(x) \rangle$ , de lo cual resulta que  $p(x)$  divide  $r(x)$ , o que  $s(x) \in \langle p(x) \rangle$ , de lo cual resulta que  $p(x)$  divide  $s(x)$ . ■

**Corolario** *Si  $p(x)$  es irreducible en  $F[x]$  y  $p(x)$  divide el producto  $r_1(x) \cdots r_n(x)$  para  $r_i(x) \in F[x]$ , entonces  $p(x)$  divide  $r_1(x)$  para al menos una  $i$ .*

*Demostración* Mediante inducción matemática encontramos que esto es una consecuencia inmediata del teorema 31.7. ■

**Teorema 31.8** *Si  $F$  es un campo, entonces todo polinomio no constante  $f(x) \in F[x]$  se puede factorizar en  $F[x]$  en un producto de polinomios irreducibles, los polinomios irreducibles son únicos, excepto por el orden y por factores unidad (esto es, constantes distintas de cero) en  $F$ .*

*Demostración* Sea  $f(x) \in F[x]$  un polinomio no constante. Si  $f(x)$  no es irreducible, entonces  $f(x) = g(x)h(x)$  con el grado de  $g(x)$  y el grado de  $h(x)$ , ambos menores que el grado de  $f(x)$ . Si  $g(x)$  y  $h(x)$  son irreducibles, nos detenemos aquí. De no ser así, al menos uno de ellos se factoriza en polinomios de grado menor. Continuando este proceso (en realidad un argumento de inducción), llegamos a la factorización

$$f(x) = p_1(x)p_2(x) \cdots p_r(x),$$

donde  $p_i(x)$  es irreducible.

Falta mostrar la unicidad. Supóngase que

$$f(x) = p_1(x)p_2(x) \cdots p_r(x) = q_1(x)q_2(x) \cdots q_s(x)$$

son dos factorizaciones de  $f(x)$  en polinomios irreducibles. Entonces, por el corolario del teorema 31.7,  $p_1(x)$  divide alguna  $q_j(x)$ , supongamos que  $q_1(x)$ . Como  $q_1(x)$  es irreducible,

$$q_1(x) = u_1 p_1(x),$$

donde  $u_1 \neq 0$ , pero  $u_1$  está en  $F$  y es, por tanto, una unidad. Entonces, al sustituir  $q_1(x)$  por  $u_1 p_1(x)$  y cancelar, obtenemos

$$p_2(x) \cdots p_r(x) = u_1 q_2(x) \cdots q_s(x).$$

Por un argumento similar, digamos que  $q_2(x) = u_2 p_2(x)$ , así que

$$p_3(x) \cdots p_r(x) = u_1 u_2 q_3(x) \cdots q_s(x).$$

Al continuar así, por último se llegará a que

$$1 = u_1 u_2 \cdots u_r q_{r+1}(x) \cdots q_s(x).$$

Claramente, esto es posible sólo si  $s = r$  de modo que esta ecuación es en realidad  $1 = u_1 u_2 \cdots u_r$ . Así, los factores irreducibles  $p_i(x)$  y  $q_j(x)$  fueron los mismos, excepto quizás, por el orden y por factores unidad. ■

**Ejemplo 31.10** El ejemplo 31.2 muestra que la factorización de  $x^4 + 3x^3 + 2x + 4$  en  $\mathbb{Z}_5[x]$  es  $(x - 1)^3(x + 1)$ . Estos factores irreducibles en  $\mathbb{Z}_5[x]$  están definidos, salvo unidades, en  $\mathbb{Z}_5[x]$ , esto es, constantes distintas de cero en  $\mathbb{Z}_5$ . Por ejemplo,  $(x - 1)^3(x + 1) = (x - 1)^2(2x - 2)(3x + 3)$ . ■

## Ejercicios

---

31.1 Sea  $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$  y  $g(x) = x^2 + 2x - 3$  en  $\mathbb{Z}_7[x]$ . Encuéntrense  $q(x)$  y  $r(x)$  en  $\mathbb{Z}_7[x]$  tal que  $f(x) = g(x)q(x) + r(x)$  con (grado  $r(x)$ ) < 2.

31.2 Sea  $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$  y  $g(x) = 3x^2 + 2x - 3$  en  $\mathbb{Z}_7[x]$ . Encuéntrense  $q(x)$  y  $r(x)$  en  $\mathbb{Z}_7[x]$  tal que  $f(x) = g(x)q(x) + r(x)$  con (grado  $r(x)$ ) < 2.

31.3 El polinomio  $x^4 + 4$  puede factorizarse en factores lineales en  $\mathbb{Z}_5[x]$ . Encuéntrese esta factorización.

31.4 ¿Es  $x^3 + 2x + 3$  un polinomio irreducible de  $\mathbb{Z}_5[x]$ ? ¿Por qué? Exprésese como producto de polinomios irreducibles de  $\mathbb{Z}_5[x]$ .

31.5 Muéstrese que  $f(x) = x^2 + 8x - 2$  es irreducible sobre  $\mathbb{Q}$ . ¿Es  $f(x)$  irreducible sobre  $\mathbb{R}$  y sobre  $\mathbb{C}$ ?

31.6 Repítase el ejercicio 31.5 con  $g(x) = x^2 + 6x + 12$  en lugar de  $f(x)$ .

31.7 a) Muéstrese que  $x^3 + 3x^2 - 8$  es irreducible sobre  $\mathbb{Q}$ .

b) Muéstrese que  $x^4 - 22x^2 + 1$  es irreducible sobre  $\mathbb{Q}$ .

31.8 Pruébese que si  $F$  es un campo, todo ideal primo propio de  $F[x]$  es maximal.

31.9 ¿Falso o verdadero?

- a)  $x - 2$  es irreducible sobre  $\mathbb{Q}$ .
- b)  $3x - 6$  es irreducible sobre  $\mathbb{Q}$ .
- c)  $x^2 - 3$  es irreducible sobre  $\mathbb{Q}$ .
- d)  $x^2 + 3$  es irreducible sobre  $\mathbb{Z}_7$ .

- e) Si  $F$  es un campo, las unidades de  $F[x]$  son precisamente los elementos de  $F$  distintos de cero.
  - f) Si  $F$  es un campo, las unidades de  $F(x)$  son precisamente los elementos de  $F$  distintos de cero.
  - g) Un polinomio  $f(x)$  de grado  $n$  con coeficientes en un campo  $F$ , puede tener a lo más  $n$  ceros en  $F$ .
  - h) Un polinomio  $f(x)$  de grado  $n$  con coeficientes en un campo  $F$ , puede tener a lo más  $n$  ceros en cualquier campo  $E$  tal que  $F \leq E$ .
  - i) Todo ideal de  $F[x]$  es principal.
  - j) Todo ideal principal en  $F[x]$  es un ideal maximal.

**31.10** Determinense cuáles de los siguientes polinomios en  $\mathbb{Z}[x]$  satisfacen un criterio de Eisenstein de irreducibilidad sobre  $\mathbb{Q}$ .

a)  $x^2 - 12$       b)  $8x^3 + 6x^2 - 9x + 24$   
 c)  $4x^{10} - 9x^3 + 24x - 18$       d)  $2x^{10} - 25x^3 + 10x^2 - 30$

**31.11** Muéstrese que el polinomio  $x^p + a$  en  $\mathbb{Z}_p[x]$  no es irreducible para ningún  $a \in \mathbb{Z}_p$ .

**31.12** Encuéntrense todos los números primos impares  $p$  tales que  $x + 2$  es un factor de  $x^4 + x^3 + x^2 - x + 1$  en  $\mathbf{Z}_p[x]$ .

**31.13** ¿Es  $2x^3 + x^2 + 2x + 2$  un polinomio irreducible en  $\mathbb{Z}_5[x]$ ? ¿Por qué? Expréssese como producto de polinomios irreducibles en  $\mathbb{Z}_5[x]$ .

**31.14** Encuéntrense todos los ceros de  $6x^4 + 17x^3 + 7x^2 + x - 10$  en  $\mathbb{Q}$ . (Este es un tedioso problema de álgebra de secundaria. *El lector* podría usar algo de geometría analítica y cálculo y hacer una gráfica, o usar el método de Newton para ver cuáles son los mejores candidatos a ceros.)

**31.15** Si  $F$  es un campo y  $a \neq 0$  es un cero de  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  en  $F[x]$ , muéstrese que  $1/a$  es un cero de  $a_n + a_{n-1}x + \cdots + a_0x^n$ .

**31.16** Encuéntrense todos los polinomios irreducibles de grado 2 ó 3 en  $\mathbb{Z}_2[x]$  y  $\mathbb{Z}_3[x]$ .

**31.17** ¿Es  $\mathbb{Q}[x]/\langle x^2 - 5x + 6 \rangle$  un campo? ¿Por qué? ¿Qué sucede con  $\mathbb{Q}[x]/\langle x^2 - 6x + 6 \rangle$ ?

**31.18** Sea  $F$  un campo y  $f(x), g(x) \in F[x]$ . Muéstrese que  $f(x)$  divide a  $g(x)$  si y sólo si  $g(x) \in \langle f(x) \rangle$ .

**31.19** Sea  $F$  un campo y sea  $f(x), g(x) \in F[x]$ . Muéstrese que

$$N = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in F\}$$

$$N = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in F[x]\}$$

es un ideal de  $F[x]$ . Muestrese que si  $f(x)$  y  $g(x)$  tienen grados diferentes y  $N \neq F[x]$ , entonces  $f(x)$  y  $g(x)$  no pueden ser ambos irreducibles sobre  $F$ .

31.20 Sea  $\sigma_m: \mathbb{Z} \rightarrow \mathbb{Z}_m$  el homomorfismo natural dado por  $a\sigma_m = (\text{residuo de } a \text{ al dividirlo entre } m)$  para  $a \in \mathbb{Z}$ .

a) Muéstrese que  $\tilde{\sigma}_m : \mathbb{Z}[x] \rightarrow \mathbb{Z}_m[x]$  dado por

$$(a_0 + a_1x + \cdots + a_nx^n)\overline{\sigma_m} = a_0\sigma_m + (a_1\sigma_m)x + \cdots + (a_n\sigma_m)x^n$$

es un homomorfismo de  $\mathbf{Z}[x]$  sobre  $\mathbf{Z}_m[x]$ .

- b) Muéstrese que si  $f(x) \in \mathbf{Z}[x]$  tiene grado  $n$  y  $(f(x))\overline{\sigma_m}$  no se factoriza en  $\mathbf{Z}_m[x]$  en dos polinomios de grado menor que  $n$ , entonces  $f(x)$  es irreducible en  $\mathbf{Q}[x]$ .
- c) Usese la parte b) para mostrar que  $x^3 + 17x + 36$  es irreducible en  $\mathbf{Q}[x]$ . [Sugerencia: inténtese con un valor primo de  $m$  que simplifique los coeficientes.]

31.21 Sea  $F$  un campo y sea  $S$  cualquier subconjunto de  $F \times F \times \cdots \times F$  para  $n$  factores. Muéstrese que el conjunto de todos los  $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$  que son cero en toda  $(a_1, \dots, a_n) \in S$  (véase el ejercicio 30.13) forma un ideal en  $F[x_1, \dots, x_n]$ . Esto es importante en geometría algebraica.

\* 32

# Dominios de factorización única

## \*32.1 INTRODUCCION

Este capítulo y los dos siguientes tratan de dominios enteros y del problema de la factorización de elementos en un dominio entero. El dominio entero  $\mathbb{Z}$  es el ejemplo usual de un dominio entero en el cual hay factorización única en primos (irreducibles). En la sección 31.4 se mostró que para un campo  $F$ ,  $F[x]$  también es uno de dichos dominios enteros, con factorización única. Para discutir ideas análogas en un dominio entero arbitrario, daremos varias definiciones, algunas de las cuales son repetición de otras anteriores. Es agradable tenerlas juntas como referencia.

**Definición** Sea  $D$  un dominio entero y  $a, b \in D$ . Si existe  $c \in D$  tal que  $b = ac$ , entonces  $a$  divide  $b$  (o  $a$  es un factor de  $b$ ), se denota  $a | b$ .

**Definición** Un elemento  $u$  de un dominio entero  $D$  es una unidad de  $D$ , si  $u$  divide 1, esto es, si  $u$  tiene inverso multiplicativo en  $D$ . Dos elementos  $a, b \in D$  son asociados en  $D$  si  $a = bu$ , donde  $u$  es una unidad en  $D$ .

En el ejercicio 32.7 pedimos demostrar que este criterio para que  $a$  y  $b$  sean asociados es una relación de equivalencia en  $D$ .

**Ejemplo 32.1** Las únicas unidades en  $\mathbb{Z}$  son 1 y  $-1$ . Así, los únicos asociados de 26 en  $\mathbb{Z}$  son 26 y  $-26$ . ■

Nótese que mientras la condición  $a = bu$  para que los elementos  $a, b \in D$  sean asociados no es formalmente simétrica, si  $a = bu$ , entonces  $b = au^{-1}$ , donde  $u^{-1}$  existe y es una unidad de  $D$ , ya que  $u$  es unidad de  $D$ .

**Definición** Un elemento  $p$  distinto de cero que no sea unidad de un dominio entero  $D$  es un *irreducible de  $D$* , si en cualquier factorización  $p = ab$  en  $D$ ,  $a$  o  $b$  es unidad.

Es fácil observar que un asociado de un irreducible es, a su vez, un irreducible.

**Definición** Un dominio entero  $D$  es un *dominio de factorización única* (DFU), si se satisfacen las siguientes condiciones:

- 1 Todo elemento de  $D$  que no sea ni 0 ni una unidad, se puede factorizar en un número finito de irreducibles.
- 2 Si  $p_1 \cdots p_r$  y  $q_1 \cdots q_s$  son dos factorizaciones en irreducibles del mismo elemento de  $D$ , entonces  $r = s$  y los  $q_j$  pueden reenumerarse de manera que  $p_i$  y  $q_i$  sean asociados.

**Ejemplo 32.2** El teorema 31.8 muestra que, para un campo  $F$ ,  $F[x]$  es un DFU. Se sabe además, que  $\mathbf{Z}$  es un DFU; usaremos esto con frecuencia, aunque no se haya demostrado. Por ejemplo, en  $\mathbf{Z}$  tenemos

$$24 = (2)(2)(3)(2) = (-2)(-3)(2)(2).$$

Aquí 2 y  $-2$  son asociados, como lo son 3 y  $-3$ . Así, excepto por el orden y asociados, los factores irreducibles en estas dos factorizaciones de 24 son los mismos. ■

Después de una definición más podremos describir lo que deseamos lograr en esta sección.

**Definición** Un dominio entero  $D$  es un *dominio de ideales principales* (DIP), si todo ideal en  $D$  es un ideal principal.

El objetivo de este capítulo es probar dos teoremas de suma importancia:

- 1 Todo DIP es un DFU. (Teorema 32.2.)
- 2 Si  $D$  es un DFU, entonces  $D[x]$  es un DFU. (Teorema 32.3.)

Nótese que el hecho de que  $F[x]$  sea un DFU, donde  $F$  es un campo (por el teorema 31.8), ilustra ambos teoremas. Por el teorema 31.5,  $F[x]$  es un DIP. Además, como  $F$  no tiene elementos distintos de cero que no son unidades,  $F$  satisface (en un sentido vacío que molesta a ciertos estudiantes) la definición de DFU. Así, el teorema 32.3 daría otra demostración de que  $F[x]$  es un DFU, excepto por el hecho de que, en realidad, usaremos con frecuencia el teorema 31.8 al probar el teorema 32.3. En el siguiente capítulo estudiaremos propiedades de cierta clase particular de DFU, los *dominios euclidianos*.

Procedamos a probar los dos teoremas. Al autor siempre le ha disgustado la demostración del segundo. Evitemoslo cuanto sea posible y demostremos primero el teorema 32.2.

## \*32.2 TODO DIP ES UN DFU

Los pasos que conducen al teorema 31.8 y a su demostración indican el camino a seguir para la demostración del teorema 32.2. La mayor parte del material será repetitivo. En el teorema 31.8, manejamos por separado y de manera ineficiente el caso particular de  $F[x]$ , pues era fácil y era el único caso que se emplearía en la teoría de campos en general.

Para probar que un dominio entero  $D$  es un DFU, es necesario mostrar que se satisfacen las condiciones 1 y 2 de la definición de un DFU. Para el caso particular de  $F[x]$ , en el teorema 31.8, la condición 1 fue muy fácil y resultó de un argumento de que en una factorización de un polinomio de grado  $> 0$  en un producto de dos polinomios no constantes, el grado de cada factor era menor que el grado del polinomio original. Así, no se podría factorizar indefinidamente sin llegar a factores unidad, es decir, polinomios de grado 0. Para el caso general de un DIP, es más difícil mostrar que así sucede. Abordemos este problema. Se necesitará un concepto más de teoría de conjuntos.

**Definición** Si  $\{A_i \mid i \in I\}$  es una colección de conjuntos, entonces la **unión**  $\bigcup_{i \in I} A_i$  de los conjuntos  $A_i$  es el conjunto de todas las  $x$  tales que  $x \in A_i$  para al menos una  $i \in I$ .

**Lema 32.1 (Condición de la cadena ascendente para un DIP)** *Sea  $D$  un DIP. Si  $N_1 \subseteq N_2 \subseteq \dots$  es una cadena de ideales monótona ascendente  $N_i$ , entonces existe un entero positivo  $r$  tal que  $N_r = N_s$  para todas las  $s \geq r$ . De manera equivalente, toda cadena de ideales estrictamente ascendente (todas las inclusiones son propias) en un DIP, es de longitud finita. Esto es, la condición de la cadena ascendente (CCA) vale para ideales en un DIP.*

**Demostración** Sea  $N_1 \subseteq N_2 \subseteq \dots$  una cadena de ideales,  $N_i$  monótona ascendente, en  $D$ . Sea  $N = \bigcup_i N_i$ . Es claro que  $N \subseteq D$ . Afírmamos que  $N$  es un ideal en  $D$ . Sea  $a, b \in N$ . Entonces, existen ideales  $N_{i_1}$  y  $N_{i_2}$  con  $a \in N_{i_1}$  y  $b \in N_{i_2}$ . Ahora,  $N_{i_1} \subseteq N_{i_2}$  o  $N_{i_2} \subseteq N_{i_1}$ ; supongamos que  $N_{i_1} \subseteq N_{i_2}$  de manera que tanto  $a$  como  $b$  están en  $N_{i_2}$ . Esto implica que  $a \pm b$  y  $ab$  están en  $N_{i_2}$ , de modo que  $a \pm b$  y  $ab$  están en  $N$ . Tomando  $a = 0$ , vemos que  $b \in N$  implica que  $-b \in N$ . Claramente,  $0 \in N$ . Así,  $N$  es un subanillo de  $D$ . Para  $a \in N$  y  $d \in D$ , debemos tener  $a \in N_{i_1}$  para algún  $N_{i_1}$ . Entonces, como  $N_{i_1}$  es un ideal,  $da = ad$  está en  $N_{i_1}$ . Por tanto,  $da \in \bigcup_i N_i$ , esto es,  $da \in N$ . De aquí que  $N$  es un ideal.

Ahora, como ideal en  $D$  que es un DIP,  $N = \langle c \rangle$  para alguna  $c \in D$ . Como  $N = \bigcup_i N_i$ , debemos tener  $c \in N$ , para alguna  $r \in \mathbb{Z}^+$ . Para  $s \geq r$ , tenemos

$$\langle c \rangle \subseteq N_r \subseteq N_s \subseteq N = \langle c \rangle.$$

Así,  $N_r = N_s$  para  $s \geq r$ .

La equivalencia con la CCA es obvia. ■

En lo que sigue, será útil recordar que para  $a, b \in D$ ,

- $\langle a \rangle \subseteq \langle b \rangle$  si y sólo si  $b$  es divisor de  $a$  y
- $\langle a \rangle = \langle b \rangle$  si y sólo si  $a$  y  $b$  son asociados.

La primera propiedad es obvia. Para la segunda propiedad, concluimos que  $a = bd_1$  y  $b = ad_2$  para algún  $d_1, d_2 \in D$ . Entonces,  $a = ad_1d_2$ . El caso  $a = 0$  es trivial, y para  $a \neq 0$  tenemos, entonces,  $1 = d_1d_2$ . Así,  $d_1$  y  $d_2$  son unidades, de modo que  $a$  y  $b$  son asociados.

Podemos probar ahora la condición 1 de la definición de DFU para un dominio entero que sea un DIP.

**Teorema 32.1** *Sea  $D$  un DIP. Todo elemento que no sea 0 ni unidad en  $D$  es producto de irreducibles.*

**Demostración** Sea  $a \in D$  donde  $a$  no es 0 ni unidad. Mostremos primero que  $a$  tiene al menos un factor irreducible. Si  $a$  es un irreducible, ya terminamos. Si  $a$  no es un irreducible, entonces  $a = a_1b_1$  donde ni  $a_1$  ni  $b_1$  es unidad. Ahora,

$$\langle a \rangle \subset \langle a_1 \rangle,$$

pues es obvio que  $\langle a \rangle \subseteq \langle a_1 \rangle$  y si  $\langle a \rangle = \langle a_1 \rangle$ , entonces  $a$  y  $a_1$  serían asociados y  $b_1$  sería unidad, lo cual contradice la construcción. Siguiendo entonces con este procedimiento y comenzando ahora con  $a_1$ , llegamos a una cadena de ideales estrictamente ascendente

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots.$$

Por la CCA del lema 32.1, esta cadena termina en algún  $\langle a_r \rangle$  y  $a_r$  debe ser irreducible. Así,  $a$  tiene un factor irreducible  $a_r$ .

Por lo que acabamos de probar, para un elemento  $a$  que no es 0 ni unidad en  $D$ ,  $a$  es irreducible o  $a = p_1c_1$  para  $p_1$  irreducible y  $c_1$  no unidad. Por un argumento similar al reciente, en el último caso podemos concluir que  $\langle a \rangle \subset \subset \langle c_1 \rangle$ . Si  $c_1$  no es irreducible, entonces  $c_1 = p_2c_2$  para un irreducible  $p_2$  con  $c_2$  no unidad. Al continuar se obtiene una cadena de ideales estrictamente ascendente.

$$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots.$$

Por la CCA del lema 32.1, esta cadena debe terminar con algún  $c_r = q$ , que sea irreducible. Entonces,  $a = p_1p_2 \cdots p_rq_r$  ■

Esto completa la demostración de la condición 1 de la definición de un DFU. Pasemos a la condición 2. Los argumentos, aquí, son paralelos a los que condujeron al teorema 31.8. Los resultados con los cuales nos encontramos en el camino tienen, en sí, algún interés.

**Lema 32.2 (Generalización del teorema 31.6)** *Un ideal  $\langle p \rangle$  en un DIP es maximal si y sólo si  $p$  es irreducible.*

**Demostración** Sea  $\langle p \rangle$  un ideal maximal de  $D$ , un DIP. Supóngase que  $p = ab$  en  $D$ . Claramente,  $\langle p \rangle \subseteq \langle a \rangle$ . Supóngase que  $\langle a \rangle = \langle p \rangle$ . Entonces,  $a$  y  $p$  serían asociados, de modo que  $b$  debe ser unidad. Si  $\langle a \rangle \neq \langle p \rangle$ , entonces debemos tener  $\langle a \rangle = \langle 1 \rangle = D$  puesto que  $\langle p \rangle$  es maximal. Pero entonces,  $a$  y  $1$  son asociados, de modo que  $a$  es unidad. Así, si  $p = ab$ ,  $a$  o  $b$  deben ser unidad. Por tanto,  $p$  es un irreducible de  $D$ .

De manera recíproca supóngase que  $p$  es un irreducible en  $D$ . Entonces, si  $\langle p \rangle \subseteq \langle a \rangle$ , debemos tener  $p = ab$ . Ahora, si  $a$  es unidad, entonces  $\langle a \rangle = \langle 1 \rangle = D$ . Si  $a$  no es unidad, entonces  $b$  debe ser unidad, de modo que existe  $u \in D$  tal que  $bu = 1$ . Entonces,  $pu = abu = a$ , de modo que  $\langle a \rangle \subseteq \langle p \rangle$ , y tenemos que  $\langle a \rangle = \langle p \rangle$ . Así,  $\langle p \rangle \subseteq \langle a \rangle$  implica que  $\langle a \rangle = D$  o  $\langle a \rangle = \langle p \rangle$  y  $\langle p \rangle \neq D$  o  $p$  sería unidad. Por tanto,  $\langle p \rangle$  es un ideal maximal. ■

**Lema 32.3 (Generalización del teorema 31.7)** *En un DIP, si un irreducible  $p$  divide  $ab$ , entonces,  $p \mid a$  o  $p \mid b$ .*

**Demostración** Sea  $D$  un DIP, supóngase que para un irreducible  $p$  en  $D$  tenemos  $p \mid ab$ . Entonces,  $(ab) \in \langle p \rangle$ . Como, por el corolario al teorema 29.5, todo ideal maximal en  $D$  es un ideal primo,  $(ab) \in \langle p \rangle$  implica que  $a \in \langle p \rangle$  o  $b \in \langle p \rangle$ , lo cual da  $p \mid a$  o  $p \mid b$ . ■

**Corolario** *Si  $p$  es un irreducible en un DIP y  $p$  divide el producto  $a_1 a_2 \cdots a_n$  para  $a_i \in D$ , entonces  $p \mid a_i$  para al menos una  $i$ .*

**Demostración** La demostración de este corolario es inmediata del lema 32.3, si usamos inducción matemática. ■

**Definición** Un elemento  $p$  de un dominio entero  $D$ , distinto de cero, no unidad, con la propiedad de que  $p \mid ab$  implica que  $p \mid a$  o  $p \mid b$ , es un **primo**.

El lema 32.3 concentra nuestra atención en la propiedad que define a un primo. En el ejercicio 32.5 pedimos mostrar que un primo en un dominio entero siempre es irreducible, y que en un DFU, un irreducible es, además, primo. Así, los conceptos de primo e irreducible coinciden en un DFU. El ejemplo 32.3 exhibirá un dominio entero que contiene algunos irreducibles que no son primos, de modo que los conceptos no coinciden en todo dominio.

**Ejemplo 32.3** Sea  $F$  un campo. Sea  $D$  el subdominio de  $F[x, y]$  generado por  $F$ ,  $x^3$ ,  $xy$  y  $y^3$ . Entonces,  $x^3$ ,  $xy$  y  $y^3$  son irreducibles en  $D$ , pero

$$(x^3)(y^3) = (xy)(xy)(xy).$$

Como  $xy$  divide  $x^3y^3$  pero no  $x^3$  ni  $y^3$ , vemos que  $xy$  no es primo. Argumentos análogos muestran que ni  $x^3$  ni  $y^3$  son primos. ■

La propiedad que define a un primo es precisamente lo requerido para establecer la propiedad 2 de unicidad, en la definición de un DFU. Completaremos la demostración del teorema 32.2 demostrando la propiedad 2 para un DIP.

**Teorema 32.2 (Generalización del teorema 31.8)** *Todo DIP es un DFU.*

**Demostración** El teorema 32.1 muestra que si  $D$  es un DIP, entonces, cada  $a \in D$ , donde  $a$  no es 0 ni unidad, tiene una factorización

$$a = p_1 p_2 \cdots p_r$$

en irreducibles. Falta mostrar la unicidad. Sea

$$a = q_1 q_2 \cdots q_s$$

otra de dichas factorizaciones en irreducibles. Entonces, tenemos  $p_1 | (q_1 q_2 \cdots q_s)$ , lo cual, por el corolario del lema 32.3, implica que  $p_1 | q_{j_1}$  para alguna  $j_1$ . Al intercambiar, si es necesario, el orden de las  $q_p$ , podemos suponer que  $j_1 = 1$  o  $p_1 | q_1$ . Entonces,  $q_1 = p_1 u_1$  y, como  $p_1$  es un irreducible,  $u_1$  es unidad, de modo que  $p_1$  y  $q_1$  son asociados. Tenemos entonces,

$$p_1 p_2 \cdots p_r = p_1 u_1 q_2 \cdots q_s$$

de modo que por la ley de cancelación en  $D$ ,

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

Al continuar este proceso, comenzando con  $p_2$  y así sucesivamente, se obtiene por último

$$1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s.$$

Como las  $q_j$  son irreducibles, debemos tener  $r = s$ . ■

Muchos libros de álgebra comienzan probando el siguiente corolario del teorema 32.2. Aquí se asumió que el lector lo conoce y se usó libremente.

**Corolario (Teorema fundamental de la aritmética)** *El dominio entero  $\mathbb{Z}$  es un DFU.*

**Demostración** Hemos visto que todos los ideales en  $\mathbb{Z}$  son de la forma  $n\mathbb{Z} = \langle n \rangle$  para  $n \in \mathbb{Z}$ . Así,  $\mathbb{Z}$  es un DIP y se aplica el teorema 32.2. ■

Vale la pena notar que la demostración de que  $Z$  es un DIP se encuentra en el corolario del teorema 6.2. Probamos el teorema 6.2 usando el algoritmo de la división para  $Z$ , exactamente como probamos, en el teorema 31.5, que  $F[x]$  es un DIP, usando el algoritmo de la división para  $F[x]$ . En el capítulo 33 examinaremos de cerca este paralelismo.

### \* 32.3 SI $D$ ES UN DFU, ENTONCES $D[x]$ ES UN DFU

Procedamos ahora con la demostración del teorema 32.3, nuestro segundo resultado principal en este capítulo. La razón por la cual no nos gustan las demostraciones aquí, es que son muy intuitivamente obvias y al mismo tiempo muy complicadas de escribir. La idea es la siguiente: sea  $D$  un DFU; podemos formar un campo de cocientes  $F$  de  $D$ . Entonces, por el teorema 31.8,  $F[x]$  es un DFU, y mostraremos que es posible recobrar una factorización de  $f(x) \in D[x]$  de su factorización en  $F[x]$ . Por supuesto, será necesario comparar los irreducibles en  $F[x]$  con los de  $D[x]$ . Este enfoque, el cual preferimos por ser más intuitivo que otros modernos y más eficientes, se debe esencialmente a Gauss.

**Definición** Sea  $D$  un DFU. Un polinomio no constante

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

en  $D[x]$  es **primitivo** si los únicos divisores comunes de todas las  $a_i$  son unidades de  $D$ .

**Ejemplo 32.4** En  $Z[x]$ ,  $4x^2 + 3x + 2$  es primitivo, pero  $4x^2 + 6x + 2$  no, pues 2, que no es unidad en  $Z$ , es un divisor común de 4, 6 y 2. ■

Claramente, todo irreducible no constante en  $D[x]$  debe ser un polinomio primitivo.

**Lema 32.4** Si  $D$  es un DFU, entonces, para todo  $f(x) \in D[x]$  no constante, tenemos  $f(x) = cg(x)$ , donde  $c \in D$ ,  $g(x) \in D[x]$  y  $g(x)$  es primitivo. El elemento  $c$  es único, salvo un factor unidad en  $D$  y es el contenido de  $f(x)$ . Además,  $g(x)$  es único, salvo un factor unidad en  $D$ .

**Demuestra** Dado  $f(x) \in D[x]$ , donde  $f(x)$  es un polinomio no constante. Como  $D$  es un DFU, cada coeficiente de  $f(x)$  se puede factorizar de manera única, salvo el orden y asociados, en un producto finito de irreducibles en  $D$ . Imagínese cada coeficiente de  $f(x)$  factorizado de este modo.

El número  $c$  a construir es, en realidad, el máximo común divisor en  $D$  de los coeficientes de  $f(x)$ . Para formar  $c$  procedemos como sigue: si  $p$  es un irreducible particular que divide todo coeficiente en  $f(x)$ , todo asociado de  $p$  que aparezca en una factorización de un coeficiente, se reemplazará por  $pu$  para alguna unidad  $u$ .

Continuando este procedimiento con otro irreducible  $q$  que aparezca en la factorización de algún coeficiente de  $f(x)$  y así sucesivamente, llegaremos, al final, a una factorización de los coeficientes de  $f(x)$  en donde cada irreducible  $p_i$  presente en la factorización de un coeficiente y que divide a todos los coeficientes, aparece, en realidad, en la factorización de todos los coeficientes, pero ningún otro asociado de  $p_i$  aparece en la factorización de cualquier coeficiente. Sea  $c = \prod_i p_i^{v_i}$ , donde el producto se toma sobre todos los irreducibles  $p_i$  que aparecen en las factorizaciones de todos los coeficientes en esta nueva factorización y donde  $v_i$  es el mayor entero, tal que  $p_i^{v_i}$  divide todos los coeficientes. Claramente, tenemos que  $f(x) = (c)g(x)$  donde  $c \in D$ ,  $g(x) \in D[x]$  y, por construcción,  $g(x)$  es primitivo.

Para la unicidad, si además  $f(x) = (d)h(x)$  para  $d \in D$ ,  $h(x) \in D[x]$  y  $h(x)$  primitivo, entonces, cada factor irreducible de  $c$  debe dividir  $d$  y viceversa. Haciendo que  $(c)g(x) = (d)h(x)$  y cancelando los factores irreducibles de  $c$  en  $d$  llegamos a que  $(u)g(x) = (v)h(x)$  para alguna unidad  $u \in D$ . Pero entonces, es obvio que  $v$  debe ser también una unidad de  $D$  pues, de otra manera, podríamos cancelar los factores irreducibles de  $v$  en  $u$ . Así, tanto  $u$  como  $v$  son unidades, de modo que  $c$  es único, salvo un factor unidad. Vemos, de  $f(x) = (c)g(x)$ , que el polinomio primitivo  $g(x)$  también es único, salvo un factor unidad. ■

El lema anterior ilustra nuestra expresión acerca de que aquí, las demostraciones son obvias pero difíciles de escribir. Ciertamente este lema cae en la categoría de lo «intuitivamente obvio».

**Ejemplo 32.5** En  $\mathbb{Z}[x]$ ,

$$4x^2 + 6x - 8 = (2)(2x^2 + 3x - 4),$$

donde  $2x^2 + 3x - 4$  es primitivo. ■

**Lema 32.5 (Gauss)** Si  $D$  es un DFU, entonces el producto de dos polinomios primitivos en  $D[x]$  es primitivo.

**Demostración** Sea

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

y

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

primitivos en  $D[x]$  y sea  $h(x) = f(x)g(x)$ . Sea  $p$  un irreducible en  $D$ . Entonces,  $p$  no divide todas las  $a_i$  y  $p$  no divide todas las  $b_j$ , pues  $f(x)$  y  $g(x)$  son primitivos. Sea  $a_r$  el primer coeficiente de  $f(x)$  que no es divisible entre  $p$ , esto es,  $p \nmid a_i$  para  $i < r$ , pero  $p \mid a_r$  (esto es,  $p$  no divide  $a_r$ ). De manera análoga, sea  $p \mid b_j$  para  $j < s$ , pero,  $p \nmid b_s$ . El coeficiente de  $x^{r+s}$  en  $h(x) = f(x)g(x)$  es

$$c_{r+s} = (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0).$$

Ahora bien,  $p \mid a_i$  para  $i < r$  implica que

$$p \mid (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}),$$

y, además,  $p \mid b_j$  para  $j < s$  implica que

$$p \mid (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0).$$

Pero  $p$  no divide  $a_r$  ni  $b_s$ , de modo que  $p$  no divide  $a_r b_s$ , y, por tanto,  $p$  no divide  $c_{r+s}$ . Esto muestra que, dado cualquier irreducible  $p \in D$ , existe algún coeficiente de  $f(x)g(x)$  que no es divisible entre  $p$ . Así,  $f(x)g(x)$  es primitivo. ■

**Corolario** Si  $D$  es un DFU, entonces, el producto finito de polinomios primivos en  $D[x]$  es primitivo.

**Demuestra** La demostración de este corolario se sigue del lema 32.5, por inducción. ■

Sean ahora  $D$  un DFU y  $F$  un campo de cocientes de  $D$ . Por el teorema 31.8,  $F[x]$  es un DFU. Como ya se dijo, mostraremos que  $D[x]$  es un DFU, al trasladar una factorización en  $F[x]$  de  $f(x) \in D[x]$  de vuelta a  $D[x]$ . El siguiente lema relaciona los irreducibles no constantes de  $D[x]$  con los de  $F[x]$ . Este es el último paso importante.

**Lema 32.6** Sea  $D$  un DFU y sea  $F$  un campo de cocientes de  $D$ . Sea  $f(x) \in D[x]$  donde  $(\text{grado de } F(x)) > 0$ . Si  $f(x)$  es un irreducible en  $D[x]$ , entonces  $f(x)$  también es un irreducible en  $F[x]$ . Además, si  $f(x)$  es primitivo en  $D[x]$  e irreducible en  $F[x]$ , entonces  $f(x)$  es irreducible en  $D[x]$ .

**Demuestra** Supóngase que un  $f(x) \in D[x]$  no constante se factoriza en polinomios de grado menor en  $F[x]$ , esto es,

$$f(x) = r(x)s(x)$$

para  $r(x), s(x) \in F[x]$ . Entonces, como  $F$  es un campo de cocientes de  $D$ , cada coeficiente en  $r(x)$  y  $s(x)$  es de la forma  $a/b$  para alguna  $a, b \in D$ . Al eliminar denominadores podemos obtener

$$(d)f(x) = r_1(x)s_1(x)$$

para  $d \in D$  y  $r_1(x), s_1(x) \in D[x]$  donde los grados de  $r_1(x)$  y  $s_1(x)$  son los grados de  $r(x)$  y  $s(x)$ , respectivamente. Por el lema 32.4,  $f(x) = (c)g(x)$ ,  $r_1(x) = (c_1)r_2(x)$  y  $s_1(x) = (c_2)s_2(x)$  para polinomios primitivos  $g(x)$ ,  $r_2(x)$  y  $s_2(x)$ , y  $c, c_1, c_2 \in D$ . Entonces,

$$(dc)g(x) = (c_1c_2)r_2(x)s_2(x),$$

y por el lema 32.5,  $r_2(x)s_2(x)$  es primitivo. Por la parte sobre unicidad del lema 32.4,  $c_1 - c_2 = dcu$  para alguna unidad  $u$  en  $D$ . Pero entonces,

$$(dc)g(x) = (dcu)r_2(x)s_2(x),$$

de modo que

$$f(x) = (c)g(x) = (cu)r_2(x)s_2(x).$$

*Hemos demostrado que si  $f(x)$  se factoriza de manera no trivial en  $F[x]$ , entonces  $f(x)$  se factoriza de manera no trivial en polinomios de los mismos grados en  $D[x]$ . Así, si  $f(x) \in D[x]$  es un irreducible en  $D[x]$ , debe ser irreducible en  $F[x]$ .*

Es obvio que un  $f(x) \in D[x]$  no constante, que sea primitivo en  $D[x]$  e irreducible en  $F[x]$ , también es irreducible en  $D[x]$ , pues  $D[x] \subseteq F[x]$ . ■

**El lema 32.6 muestra que si  $D$  es un DFU, los irreducibles en  $D[x]$  son, precisamente, los irreducibles en  $D$  junto con los polinomios primitivos no constantes que son irreducibles en  $F[x]$ , donde  $F$  es un campo de cocientes de  $D[x]$ .**

En verdad, el lema anterior es muy importante por sí mismo. Esto se señala en el siguiente corolario, del cual el teorema 31.3 es un caso particular. (Admitimos que no parece sensato llamar teorema a un caso particular de un corolario de un lema. El nombre que se asigna a un resultado depende, de alguna manera, del contexto en el cual aparece.)

**Corolario** *Si  $D$  es un DFU y  $F$  es un campo de cocientes de  $D$ , entonces un  $f(x) \in D[x]$  no constante, se factoriza en un producto de dos polinomios de grados menores  $r$  y  $s$  en  $F[x]$  si y sólo si tiene factorización en polinomios de los mismos grados  $r$  y  $s$  en  $D[x]$ .*

**Demostración** En la demostración del lema 32.6, se mostró que si  $f(x)$  se factoriza en producto de dos polinomios de grado menor en  $F[x]$ , entonces, tiene factorización en polinomios de los mismos grados en  $D[x]$  (véase la penúltima frase del primer párrafo de la demostración).

El recíproco es obvio, pues  $D[x] \subseteq F[x]$ . ■

Ahora estamos preparados para demostrar el teorema principal. Repetiremos de nuevo la construcción de la demostración del lema 32.6; es el centro de toda esta discusión.

**Teorema 32.3** *Si  $D$  es un DFU, entonces  $D[x]$  es un DFU.*

**Demostración** Sea  $f(x) \in D[x]$  donde  $f(x)$  no es 0 ni es una unidad. Si  $f(x)$  es de grado 0, hemos terminado, pues  $D$  es un DFU. Supóngase que (grado de  $f(x)$ ) > 0 y considérese  $f(x)$  como elemento en  $F[x]$  donde  $F$  es un campo de cocientes de  $D$ . Por el teorema 31.8,  $f(x) = p_1(x) \cdots p_s(x)$  en  $F[x]$ , donde  $p_i(x)$  es irreducible en  $F[x]$ . Como  $F$  es un campo de cocientes de  $D$ , cada coeficiente en

cada  $p_i(x)$  es de la forma  $a/b$  para alguna  $a, b \in D$ . Al eliminar de manera usual todos los denominadores, llegamos a

$$(d)f(x) = q_1(x) \cdots q_r(x)$$

para  $d, q_i(x) \in D[x]$ . Como cada  $p_i(x)$  era irreducible en  $F[x]$ , vemos que  $q_i(x)$ , el cual es  $p_i(x)$  multiplicado por una *unidad* en  $F$ , también es irreducible en  $F[x]$ . Por el lema 32.4,  $f(x) = (c)g(x)$  y  $q_i(x) = (c_i)q'_i(x)$  en  $D[x]$  para  $g(x)$  y  $q'_i(x)$  primitivo. Entonces,

$$(dc)g(x) = (c_1 \cdots c_r)q'_1(x) \cdots q'_r(x),$$

donde, por el lema 32.5, el producto  $q'_1(x) \cdots q'_r(x)$  es primitivo. Por la parte sobre la unicidad del lema 32.4, vemos que

$$c_1 \cdots c_r = dcu$$

para alguna unidad  $u$  en  $D$ . Entonces,

$$(dc)g(x) = (dcu)q'_1(x) \cdots q'_r(x),$$

de modo que

$$f(x) = (c)g(x) = (cu)q'_1(x) \cdots q'_r(x).$$

Ahora bien,  $cu$  se puede factorizar en irreducibles en  $D$ . Además,  $q'_1(x), \dots, q'_r(x)$  son irreducibles en  $D[x]$  pues, por construcción, son primitivos e irreducibles en  $F[x]$ . Así, hemos demostrado que es posible factorizar  $f(x)$  en un producto de irreducibles en  $D[x]$ .

La unicidad de una factorización de  $f(x) \in D[x]$  está clara para  $f(x) \in D$  que no sea 0 ni sea unidad. Si  $(\text{grado de } f(x)) > 0$ , podemos considerar cualquier factorización de  $f(x)$  en irreducibles en  $D[x]$  como una factorización en  $F[x]$  en unidades (esto es, los factores en  $D$  son, por el lema 32.6, polinomios irreducibles en  $F[x]$ ). Por el teorema 31.8, estos polinomios son únicos, excepto por posibles factores constantes en  $F$ . Pero, en tanto irreducible en  $D[x]$ , cada polinomio de grado  $> 0$ , presente en la factorización de  $f(x)$  en  $D[x]$ , es primitivo. Por la parte sobre la unicidad del lema 32.4, esto muestra que estos polinomios son únicos en  $D[x]$ , salvo factores unidades, esto es, asociados. El producto de los irreducibles en  $D$  en la factorización de  $f(x)$  es el contenido de  $f(x)$  el cual, por el lema 32.4, es único, salvo un factor unidad. Así, todos los irreducibles en  $D[x]$  presentes en la factorización, son únicos, salvo el orden y asociados. ■

*Corolario* Si  $F$  es un campo y  $x_1, \dots, x_n$  son indeterminadas, entonces  $F[x_1, \dots, x_n]$  es un DFU.

*Demostración* Por el teorema 38.1,  $F[x_1]$  es un DFU. Por el teorema 32.3, lo es  $(F[x_1])[x_2] = F[x_1, x_2]$ . Continuando este procedimiento, vemos (por inducción) que  $F[x_1, \dots, x_n]$  es un DFU. ■

Hemos visto que un DIP es un DFU. El corolario del teorema 32.3 nos facilita un ejemplo para mostrar que *no todo DFU es un DIP*.

**Ejemplo 32.6** Sea  $F$  un campo y sean  $x$  y  $y$  indeterminadas. Entonces, por el corolario del teorema 32.3,  $F[x, y]$  es un DFU. Considerese el conjunto  $N$  de todos los polinomios en  $x$  y  $y$  en  $F[x, y]$  con término constante 0. Es claro que  $N$  es un ideal, pero no es un ideal principal. Así,  $F[x, y]$  no es un DIP. ■

Otro ejemplo de un DFU que no es DIP es  $\mathbb{Z}[x]$ , según se muestra en el ejercicio 33.5.

## Ejercicios

---

\*32.1 Indíquese cuáles de los elementos siguientes son irreducibles del dominio entero indicado.

- |                                 |                                      |
|---------------------------------|--------------------------------------|
| a) 5 en $\mathbb{Z}$            | b) $-17$ en $\mathbb{Z}$             |
| c) 14 en $\mathbb{Z}$           | d) $2x - 3$ en $\mathbb{Z}[x]$       |
| e) $2x - 10$ en $\mathbb{Z}[x]$ | f) $2x - 3$ en $\mathbb{Q}[x]$       |
| g) $2x - 10$ en $\mathbb{Q}[x]$ | h) $2x - 10$ en $\mathbb{Z}_{11}[x]$ |

\*32.2 De ser posible, dense cuatro asociados diferentes es de  $2x - 7$  considerado como elemento de  $\mathbb{Z}[x]$ ; de  $\mathbb{Q}[x]$ ; de  $\mathbb{Z}_{11}[x]$ .

\*32.3 Factorícese el polinomio  $4x^2 - 4x + 8$  en un producto de irreducibles, considerándolo elemento del dominio entero  $\mathbb{Z}[x]$ ; del dominio entero  $\mathbb{Q}[x]$ ; del dominio entero  $\mathbb{Z}_{11}[x]$ .

\*32.4 Exprésese cada uno de los polinomios dados como el producto de su contenido con un polinomio primitivo en el DFU indicado.

- |  |  |
|--|--|
| a) $18x^2 - 12x + 48$ en $\mathbb{Z}[x]$ | b) $18x^2 - 12x + 48$ en $\mathbb{Q}[x]$ |
| c) $2x^2 - 3x + 6$ en $\mathbb{Z}[x]$    | d) $2x^2 - 3x + 6$ en $\mathbb{Z}_7[x]$  |

†32.5 Pruébese lo siguiente:

- Si  $p$  es primo en un dominio entero  $D$ , entonces  $p$  es un irreducible.
- Si  $q$  es un irreducible en un DFU, entonces  $q$  es primo.

\*32.6 ¿Falso o verdadero?

- a) Todo campo es un DFU.
- b) Todo campo es un DIP.
- c) Todo DIP es un DFU.
- d) Todo DFU es un DIP.
- e)  $\mathbb{Z}[x]$  es un DFU.
- f) Cualesquiera dos irreducibles en cualquier DFU son asociados.
- g) Si  $D$  es un DIP, entonces  $D[x]$  es un DIP.
- h) Si  $D$  es un DFU, entonces  $D[x]$  es un DFU.
- i) En cualquier DFU, si  $p \mid a$  para un irreducible  $p$ , entonces  $p$  mismo aparece en toda factorización de  $a$ .
- j) Un DFU no tiene divisores de 0.

\*32.7 Para un dominio entero  $D$ , muéstrese que la relación  $a \sim b$  si  $a$  es un asociado de  $b$  (esto es, si  $a = bu$  para  $u$  unidad en  $D$ ), es una relación de equivalencia en  $D$ .

\*32.8 Sea  $D$  un DFU. Describanse los irreducibles en  $D[x]$  en términos de los irreducibles en  $D$  y los irreducibles en  $F[x]$ , donde  $F$  es un campo de cocientes de  $D$ .

\*32.9 Sea  $D$  un dominio entero. En el ejercicio 23.4 se mostró que  $\langle U, \cdot \rangle$  es un grupo, donde  $U$  es el conjunto de unidades de  $D$ . Muéstrese que el conjunto  $D^* - U$  de no unidades de  $D$ , excluyendo al 0, es cerrado bajo la multiplicación. ¿Acaso este conjunto es un grupo bajo la multiplicación de  $D$ ?

\*32.10 El lema 32.6 afirma que si  $D$  es un DFU con campo de cocientes  $F$ , entonces un irreducible no constante  $f(x)$  de  $D[x]$  también es un irreducible de  $F[x]$ . Muéstrese, mediante un ejemplo, que un  $g(x) \in D[x]$  que sea irreducible de  $F[x]$  no necesita ser un irreducible de  $D[x]$ .

\*32.11 En esta sección, restringimos nuestro trabajo a dominios enteros. Con las mismas definiciones de la sección 32.1, pero para un anillo comunitativo con unitario, considérese factorización en irreducibles en  $\mathbf{Z} \times \mathbf{Z}$ . ¿Qué puede suceder? Considerese en particular  $(1, 0)$ .

\*32.12 Sea  $D$  un DFU. Muéstrese que un divisor no constante de un polinomio primitivo en  $D[x]$  es, de nuevo, un polinomio primitivo.

\*32.13 Muéstrese que, en un DIP, todo ideal está contenido en un ideal maximal. [Sugerencia: úsese el lema 32.1.]

\*32.14 Factorícese  $x^3 - y^3$  en irreducibles en  $\mathbf{Q}[x, y]$  y pruébese que cada uno de los factores es irreducible.

*Hay algunos otros conceptos que con frecuencia se consideran de carácter similar a la condición de la cadena ascendente en ideales en un anillo. Los tres ejercicios siguientes tratan algunos de estos conceptos.*

\*32.15 Sea  $R$  cualquier anillo. La condición de la cadena ascendente (CCA) para ideales se cumple en  $R$  si cada sucesión estrictamente creciente  $N_1 \subset N_2 \subset N_3 \subset \dots$  de ideales en  $R$  es de longitud finita. La condición del máximo (CM) para ideales se cumple en  $R$ , si cada conjunto  $S$  no vacío, de ideales en  $R$  contiene algún ideal que no está contenido propiamente en ningún otro ideal del conjunto  $S$ . La condición de la base finita (CBF) para ideales se cumple en  $R$  si para cada ideal  $N$  en  $R$  existe algún conjunto finito  $B_N = \{b_1, \dots, b_n\} \subseteq N$  tal que  $N$  es la intersección de todos los ideales de  $R$  que contienen a  $B_N$ . El conjunto  $B_N$  es una base finita para  $N$ .

Muéstrese que para todo anillo  $R$  las condiciones CCA, CM y CBF son equivalentes.

\*32.16 Sea  $R$  cualquier anillo. La condición de la cadena descendente (CCD) para ideales se cumple en  $R$ , si cualquier sucesión estrictamente decreciente  $N_1 \supset N_2 \supset N_3 \supset \dots$  de ideales en  $R$  es de longitud finita. La condición del mínimo (Cm) para ideales se cumple en  $R$  si, dado cualquier conjunto  $S$  de ideales de  $R$ , existe algún ideal de  $S$  que no contiene propiamente a cualquier otro ideal en el conjunto  $S$ .

Muéstrese que para todo anillo, las condiciones CCD y Cm son equivalentes.

\*32.17 Dese un ejemplo de un anillo en el cual se cumpla CCA pero no CCD. (Véanse los ejercicios 32.15 y 32.16.)

# Dominios euclidianos

## \*33.1 INTRODUCCION Y DEFINICION

Hemos señalado varias veces la importancia de los algoritmos de división. Nuestro primer contacto con ellos fue el *algoritmo de división para  $\mathbf{Z}$*  (lema 6.1). Este algoritmo se usó de inmediato para probar el importante teorema de que un subgrupo de un grupo cíclico es cíclico, esto es, que tiene un solo generador. El *algoritmo de división para  $F[x]$*  apareció en el teorema 31.1 y se usó de manera análoga para mostrar que  $F[x]$  es un DIP, esto es, que todo ideal en  $F[x]$  tiene un solo generador. Ahora bien, una técnica moderna en matemáticas es tomar varias situaciones claramente relacionadas y tratar de reunirlas abstrayendo las ideas importantes que tienen en común. El estudiante se dará cuenta cómo la siguiente definición ilustra esta técnica. Veamos qué podemos desarrollar, comenzando con la existencia de un algoritmo de la división bastante general en un dominio entero.

**Definición** Una evaluación euclíadiana en un dominio entero  $D$  es una función  $v$  que transforma a los elementos distintos de cero de  $D$ , en los enteros no negativos tal que se satisfacen las condiciones siguientes:

- 1 Para todos los  $a, b \in D$  con  $b \neq 0$  existen  $q$  y  $r$  en  $D$  tales que  $a = bq + r$ , donde  $r = 0$  o  $v(r) < v(b)$ .
- 2 Para todos los  $a, b \in D$ , donde ni  $a$  ni  $b$  es 0,  $v(a) \leq v(ab)$ .

Un dominio entero  $D$  es un *dominio euclíadiano* si existe una evaluación euclíadiana en  $D$ .

La importancia de la condición 1 está clara a partir de la discusión inicial. La importancia de la condición 2 es que nos permitirá caracterizar las unidades de un dominio euclíadiano  $D$ .

**Ejemplo 33.1** El dominio entero  $\mathbb{Z}$  es un dominio euclíadiano, pues la evaluación  $v$  definida por  $v(n) = |n|$  para  $n \neq 0$  en  $\mathbb{Z}$  es una evaluación euclíadiana en  $\mathbb{Z}$ . Por el lema 6.1, se cumple la condición 1 y la condición 2 es obvia. ■

**Ejemplo 33.2** Si  $F$  es un campo, entonces  $F[x]$  es un dominio euclíadiano, pues la evaluación  $v$  definida por  $v(f(x)) = (\text{grado de } f(x))$  para  $f(x) \in F[x]$  y  $f(x) \neq 0$  es una evaluación euclíadiana. Por el teorema 31.1, se cumple la condición 1 y la condición 2 es obvia. ■

Por supuesto, deberíamos dar ejemplos de dominios euclidianos diferentes de éstos que motivaron la definición. Lo haremos en el siguiente capítulo. En vista de nuestras observaciones iniciales, seguramente estarán esperando el siguiente teorema.

**Teorema 33.1** *Todo dominio euclíadiano es un DIP.*

**Demostración** Sea  $D$  un dominio euclíadiano con evaluación euclíadiana  $v$  y sea  $N$  un ideal en  $D$ . Si  $N = \{0\}$ , entonces  $N = \langle 0 \rangle$  y  $N$  es principal. Supóngase que  $N \neq \{0\}$ . Entonces, existe  $b \neq 0$  en  $N$ . Escojamos  $b$  tal que  $(b)$  sea minimal de entre todas las  $v(n)$  para  $n \in N$ . Afirmamos que  $N = \langle b \rangle$ . Sea  $a \in N$ . Entonces, por la condición 1 para un dominio euclíadiano, existen  $q$  y  $r$  en  $D$  tales que

$$a = bq + r,$$

donde  $r = 0$  o  $v(r) < v(b)$ . Ahora,  $r = a - bq$  y  $a, b \in N$ , de modo que  $r \in N$ , puesto que  $N$  es un ideal. Así, es imposible que  $v(r) < v(b)$  debido a nuestra selección de  $b$ . De aquí,  $r = 0$ , de modo que  $a = bq$ . Como  $a$  es cualquier elemento de  $N$ , vemos que  $N = \langle b \rangle$ . ■

**Corolario** *Un dominio euclíadiano es un DFU.*

**Demostración** Por el teorema 33.1, un dominio euclíadiano es un DIP y, por el teorema 32.2, un DIP es un DFU. ■

Por último, mientras que, por el teorema 33.1, un dominio euclíadiano es un DIP, no todo DIP es un dominio euclíadiano. Sin embargo, no es fácil encontrar un DIP que no sea euclíadiano.

## \*33.2 ARITMETICA EN DOMINIOS EUCLIDIANOS

Investigaremos ahora algunas propiedades de los dominios euclidianos relacionados con su estructura multiplicativa. Debe aclararse que la estructura aritmética de un dominio euclíadiano es *intrínseca al dominio* y no se afecta de modo alguno por una evaluación euclíadiana  $v$  en el dominio. La evaluación euclíadiana es

simplemente una herramienta para arrojar posiblemente, alguna luz sobre esta estructura aritmética del dominio. La estructura aritmética de un dominio  $D$  está por completo determinada por el conjunto  $D$  y las dos operaciones binarias  $+$  y  $\cdot$  en  $D$ .

Sea  $D$  un dominio euclíadiano con evaluación euclíadiana  $v$ . Podemos usar la propiedad 2 de una evaluación euclíadiana para caracterizar las unidades de  $D$ .

**Teorema 33.2** *Para un dominio euclíadiano con evaluación euclíadiana  $v$ ,  $v(1)$  es minimal entre todas las  $v(a)$  para  $a \in D$  distinta de cero y  $u \in D$  es unidad si y sólo si  $v(u) = v(1)$ .*

*Demostración* La condición 2 para  $v$ , nos dice que para  $a \neq 0$

$$v(1) \leq v(1a) = v(a).$$

Por otro lado, si  $u$  es unidad en  $D$ , entonces

$$v(u) \leq v(uu^{-1}) = v(1).$$

Así,

$$v(u) = v(1)$$

para una unidad  $u$  en  $D$ .

En forma reciproca, supóngase que  $u \in D$  distinto de cero es tal que  $v(u) = v(1)$ . Entonces, por el algoritmo de la división, existen  $q$  y  $r$  en  $D$  tales que

$$1 = uq + r,$$

donde  $r = 0$  o  $v(r) < v(u)$ . Pero como  $v(u) = v(1)$  es minimal entre todas las  $v(d)$  para  $d \in D$  distinto de cero, es imposible que  $v(r) < v(u)$ . De aquí,  $r = 0$  y  $1 = uq$ , de modo que  $u$  es unidad. ■

**Ejemplo 33.3** Para  $\mathbf{Z}$  con  $v(n) = |n|$ , el mínimo de  $v(n)$  para  $n \in \mathbf{Z}$  distinto de cero, es 1. Es claro que 1 y  $-1$  son los únicos elementos de  $\mathbf{Z}$  con  $v(n) = 1$ . Por supuesto, el 1 y el  $-1$  son las unidades de  $\mathbf{Z}$ . ■

**Ejemplo 33.4** Para  $F[x]$  con  $v(f(x)) = (\text{grado de } f(x))$  para  $f(x) \neq 0$ , el valor mínimo de  $v(f(x))$  para todos los  $f(x) \in F[x]$  distintos de cero es 0. Los polinomios distintos de cero de grado 0 son precisamente los elementos distintos de cero de  $F$  y son éstos, las unidades de  $F[x]$ . ■

Es necesario comprender que todo lo demostrado aquí se cumple para todo dominio euclíadiano, en particular, para  $\mathbf{Z}$  y  $F[x]$ . Probaremos algunos resultados clásicos acerca de máximos comunes divisores en un dominio euclíadiano. Seguro que el lector tiene una idea intuitiva acerca de lo que debe ser un máximo común divisor (mcd) de dos elementos  $a$  y  $b$  en un DFU. Simplemente se toman  $a$  y  $b$ , se factorizan, se ajustan las factorizaciones mediante unidades, de

modo que si algún irreducible divide tanto  $a$  como  $b$ , sucede que, o aparece en ambas factorizaciones y no aparece ninguno de sus asociados, o no aparece en ninguna de las factorizaciones, esto es, en su lugar, aparece uno de sus asociados. Entonces, obtenemos un mcd de  $a$  y  $b$  multiplicando entre sí todos los irreducibles que aparecen en ambas factorizaciones, tomando cada irreducible elevado a la potencia más alta para la cual divide tanto  $a$  como  $b$ . Esto se ha dicho de manera torpe, pero quizás el lector comprendió la idea. Ya usamos libremente el concepto en  $\mathbb{Z}$ , en teoría de grupos. Como un irreducible presente en una factorización se define salvo un factor unidad, vemos que en un DFU, también debe definirse un mcd salvo un factor unidad. Es por esto que decimos «un» mcd en lugar de «el» mcd, de  $a$  y  $b$ . Se acostumbra dar la siguiente definición, más elegante, de un mcd en un DFU. El lector encontrará obvio que para un DFU, esta definición describe el mismo concepto que recién se analizó.

**Definición** Sea  $D$  un DFU. Un elemento  $d \in D$  es un **máximo común divisor** (mcd) **de los elementos  $a$  y  $b$  en  $D$**  si  $d | a$ ,  $d | b$  y además,  $c | d$  para todos los  $c$  que dividan  $a$  y  $b$ .

**Ejemplo 33.5** En  $\mathbb{Z}$ , un mcd de 18 y 48 es 6. Otro es  $-6$ . En  $\mathbb{Q}[x]$ , un mcd de  $x^2 - 2x + 1$  y  $x^2 + x - 2$  es  $x - 1$ . Otro es  $2(x - 1)$ , pues 2 es una unidad en  $\mathbb{Q}[x]$ . Otro más es  $(15/13)(x - 1)$ . Sin embargo, en  $\mathbb{Z}[x]$ , los únicos mcd de  $x^2 - 2x + 1$  y  $x^2 + x - 2$  son  $x - 1$  y  $-(x - 1)$ , pues 1 y  $-1$  son las únicas unidades en  $\mathbb{Z}[x]$ . ■

Como se indicó después del ejemplo 33.4, se puede mostrar que cualesquiera  $a$  y  $b$  en un DFU tienen un mcd, factorizando  $a$  y  $b$  en irreducibles. (En realidad, existe un mcd para cualquier número de elementos de un DFU. La demostración del lema 32.4 muestra con más detalle cómo se puede construir dicho mcd a partir de factorizaciones en irreducibles.) Todo DIP es un DFU, de modo que es claro que también existan los mcd en un DIP. Hay una bella demostración para los DIP, sin usar factorización, la cual nos gustaría que el lector observara.

**Teorema 33.3** Si  $D$  es un DIP y  $a$  y  $b$  son elementos distintos de cero de  $D$ , entonces existe algún mcd de  $a$  y  $b$ . Más aún, cada mcd de  $a$  y  $b$  puede expresarse en la forma  $\lambda a + \mu b$  para algunos  $\lambda, \mu \in D$ .

**Demostración** Considérese el conjunto

$$N = \{ra + sb \mid r, s \in D\}.$$

Como

$$(r_1a + s_1b) \pm (r_2a + s_2b) = (r_1 \pm r_2)a + (s_1 \pm s_2)b$$

y

$$t(ra + sb) = (tr)a + (ts)b$$

para  $t \in D$ , es inmediato que  $N$  es un ideal de  $D$ . Ahora,  $N = \langle d \rangle$  para algún  $d \in D$ . Entonces,  $d | (ra + sb)$  para todas las  $r, s \in D$  y, tomando primero  $s = 0$

con  $r = 1$ , y después  $r = 0$  con  $s = 1$ , vemos que  $d \mid a$  y  $d \mid b$ . Además, si  $c \mid a$  y  $c \mid b$ , entonces  $c \mid (ra + sb)$  para todas las  $ra + sb$ , esto es,  $c \mid n$  para todas las  $n \in N$ . De aquí que  $c \mid d$ . Así,  $d$  es un mcd de  $a$  y  $b$ .

Para  $d$ , tal como se acaba de construir,  $d \in N$  implica que existen  $\lambda, \mu \in D$  tales que  $d = \lambda a + \mu b$ . Pero la definición de mcd muestra que si  $d_1$ , también es un mcd de  $a$  y  $b$ , entonces  $d_1 \mid d$ , y  $d_1 \mid a$ . Así,

$$d_1 = vd = (v\lambda)a + (v\mu)b = \lambda_1 a + \mu_1 b. \blacksquare$$

La demostración anterior es muy elegante, pero nada constructiva. Claramente podemos encontrar un mcd de  $a$  y  $b$  si logramos factorizarlos en irreducibles, pero dichas factorizaciones pueden ser muy difíciles de obtener. Sin embargo, si un DFU es en realidad euclíadiano y conocemos una evaluación euclíadiana, hay una manera constructiva y sencilla de encontrar los mcd, según lo muestra el siguiente teorema.

**Teorema 33.4 (Algoritmo euclíadiano)** *Sea  $D$  un dominio euclíadiano con una evaluación euclíadiana  $v$  y sean  $a$  y  $b$  elementos de  $D$  distintos de cero. Sea  $r_1$  como en la condición 1 para una evaluación euclíadiana, esto es,*

$$a = bq_1 + r_1,$$

donde  $r_1 = 0$  o  $v(r_1) < v(b)$ . Si  $r_1 = 0$ , sea  $r_2$  tal que

$$b = r_1 q_2 + r_2,$$

donde  $r_2 = 0$  o  $v(r_2) < v(r_1)$ . En general, sea  $r_{i+1}$  tal que

$$r_{i-1} = r_i q_{i+1} + r_{i+1},$$

donde  $r_{i+1} = 0$  o  $v(r_{i+1}) < v(r_i)$ . Entonces, la sucesión  $r_1, r_2, \dots$  debe terminar con algún  $r_s = 0$ . Si  $r_1 = 0$ , entonces  $b$  es un mcd de  $a$  y  $b$ . Si  $r_1 \neq 0$  y  $r_s$  es el primer  $r_i = 0$ , entonces,  $r_{s-1}$  es un mcd de  $a$  y  $b$ .

**Demostración** Como  $v(r_i) < v(r_{i-1})$  y  $v(r_i)$  es un entero no negativo, es claro que llegaremos a alguna  $r_s = 0$  después de un número finito de pasos.

Si  $r_1 = 0$ , entonces  $a = bq_1$  y, obviamente,  $b$  es un mcd de  $a$  y  $b$ . Supóngase que  $r_1 \neq 0$ . Entonces, si  $d \mid a$  y  $d \mid b$ , tenemos

$$d \mid (a - bq_1),$$

de modo que  $d \mid r_1$ . Sin embargo, si  $d_1 \mid r_1$  y  $d_1 \mid b$ , entonces

$$d_1 \mid (bq_1 + r_1),$$

de modo que  $d_1 \mid a$ . Así, el conjunto de divisores comunes de  $a$  y  $b$  es el mismo conjunto que el conjunto de divisores comunes de  $b$  y  $r_1$ . Por un argumento

similar, si  $r_2 \neq 0$ , el conjunto de divisores comunes de  $b$  y  $r_1$  es el mismo conjunto que el conjunto de divisores comunes de  $r_1$  y  $r_2$ . Continuamos con este proceso y, al final, vemos que el conjunto de divisores comunes de  $a$  y  $b$  es el mismo conjunto que el conjunto de divisores comunes de  $r_{s-2}$  y  $r_{s-1}$  donde  $r_s$  es el primer  $r_i$  igual a 0. Así, un mcd de  $r_{s-2}$  y  $r_{s-1}$  es también un mcd de  $a$  y  $b$ . Pero la ecuación

$$r_{s-2} = q_s r_{s-1} + r_s = q_s r_{s-1}$$

muestra que un mcd de  $r_{s-2}$  y  $r_{s-1}$  es  $r_{s-1}$ . ■

**Ejemplo 33.6** Ilustremos el algoritmo eucliano para la evaluación euclidiana || en  $\mathbb{Z}$ , calculando un mcd de 22 471 y 3266. Tan sólo hay que aplicar una y otra vez el algoritmo de la división y el último residuo distinto de cero es un mcd. Denominamos los números obtenidos de la misma manera que en el teorema 33.4, para ilustrar el enunciado y la demostración del teorema. Es fácil corroborar los cálculos

$$\begin{array}{ll} a = 22\,471 & \\ b = 3266 & \\ 22\,471 = (3266)6 + 2875 & r_1 = 2875 \\ 3266 = (2875)1 + 391 & r_2 = 391 \\ 2875 = (391)7 + 138 & r_3 = 138 \\ 391 = (138)2 + 115 & r_4 = 115 \\ 138 = (115)1 + 23 & r_5 = 23 \\ 115 = (23)5 + 0 & r_6 = 0 \end{array}$$

Así,  $r_5 = 23$  es un mcd de 22 471 y 3266. Encontramos un mcd sin factorizar. Esto es importante, pues a veces es muy difícil encontrar una factorización de un entero en primos. ■

**Ejemplo 33.7** Nótese que el algoritmo de la división 1 de la definición de una evaluación euclidiana no dice nada acerca de que  $r$  sea «positiva». Al calcular un mcd en  $\mathbb{Z}$  mediante el algoritmo eucliano para ||, como en el ejemplo 33.6, seguramente nos interese que, en cada división,  $|r_i|$  sea lo más pequeño posible. Así, repitiendo el ejemplo 33.6 sería más eficaz escribir

$$\begin{array}{ll} a = 22\,471 & \\ b = 3266 & \\ 22\,471 = (3266)7 - 391 & r_1 = -391 \\ 3266 = (391)8 + 138 & r_2 = 138 \\ 391 = (138)3 - 23 & r_3 = -23 \\ 138 = (23)6 + 0 & r_4 = 0 \end{array}$$

El hecho de que podamos cambiar el signo de  $r_i$  de negativo a positivo según lo deseemos, se debe al hecho de que los divisores de  $r_i$  y  $-r_i$  son los mismos. ■

**Ejercicios**

\*33.1 Indíquese cuáles de las funciones dadas  $v$  son evaluaciones euclidianas para los dominios enteros dados.

- La función  $v$  para  $\mathbb{Z}$  dada por  $v(n) = n^2$  para  $n \in \mathbb{Z}$  distinto de cero.
- La función  $v$  para  $\mathbb{Z}[x]$  dada por  $v(f(x)) = (\text{grado } f(x))$  para  $f(x) \in \mathbb{Z}[x]$  distinto de cero.
- La función  $v$  para  $\mathbb{Z}[x]$  dada por  $v(f(x)) = (\text{valor absoluto del coeficiente del término de mayor grado distinto de cero de } f(x))$  para  $f(x) \in \mathbb{Z}[x]$  distinto de cero.
- La función  $v$  para  $\mathbb{Q}$  dada por  $v(a) = a^2$  para  $a \in \mathbb{Q}$  distinto de cero.
- La función  $v$  para  $\mathbb{Q}$  dada por  $v(a) = 50$  para  $a \in \mathbb{Q}$  distinto de cero.

\*33.2 Encuéntrese un mcd de 49 349 y 15 555 en  $\mathbb{Z}$ .

\*33.3 Encuéntrese un mcd de

$$x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3$$

y

$$x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2$$

en  $\mathbb{Q}[x]$ .

\*33.4 Con referencia al ejemplo 33.7 del libro, expóngase, realmente, el mcd 23 en la forma  $\lambda(22\ 471) + \mu(3266)$  para  $\lambda, \mu \in \mathbb{Z}$ . [Sugerencia: a partir de la penúltima línea del cálculo en el ejemplo 33.7,  $23 = (138)3 - 391$ . Del renglón anterior a ese,  $138 = 3266 - (391)8$ , así, por sustitución, obtenemos  $23 = [3266 - (391)8]3 - 391$  y así sucesivamente. Esto es, se trabaja hacia atrás hasta encontrar realmente los valores de  $\lambda$  y  $\mu$ .]

\*33.5 Considérese  $\mathbb{Z}[x]$ .

- ¿Es  $\mathbb{Z}[x]$  un DFU? ¿Por qué?
- Muéstrese que  $\{a + xf(x) \mid a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$  es un ideal en  $\mathbb{Z}[x]$ .
- ¿Es  $\mathbb{Z}[x]$  un DIP? (Considérese la parte b).)
- ¿Es  $\mathbb{Z}[x]$  un dominio eucliano? ¿Por qué?

\*33.6 Sea  $D$  un dominio eucliano y sea  $v$  una evaluación eucliana en  $D$ . Muéstrese que si  $a$  y  $b$  son asociados en  $D$ , entonces  $v(a) = v(b)$ .

\*33.7 ¿Falso o verdadero?

- a) Todo dominio eucliano es un DIP.
- b) Todo DIP es un dominio eucliano.
- c) Todo dominio eucliano es un DFU.
- d) Todo DFU es un dominio eucliano.
- e) Un mcd de 2 y 3 en  $\mathbb{Q}$  es  $\frac{1}{2}$ .
- f) El algoritmo eucliano proporciona un método constructivo para encontrar un mcd de dos enteros.
- g) Si  $v$  es una evaluación eucliana en un dominio eucliano  $D$ , entonces  $v(1) \leq v(a)$  para todas las  $a \in D$  distintas de cero.
- h) Si  $v$  es una evaluación eucliana en un dominio eucliano  $D$ , entonces  $v(1) < v(a)$  para todas las  $a \in D$ ,  $a \neq 1$ , distintas de cero.
- i) Si  $v$  es una evaluación eucliana en un dominio eucliano  $D$ , entonces  $v(1) < v(a)$  para todas las unidades  $a \in D$  distintas de cero.
- j) Para cualquier campo  $F$ ,  $F[x]$  es un dominio eucliano.

\*33.8 La selección de una evaluación euclíadiana  $v$  particular en un dominio euclíadiano  $D$ , ¿influye de alguna forma en la estructura aritmética de  $D$ ? Explíquese.

\*33.9 Siguiendo la idea del ejercicio 33.4 y refiriéndonos al ejercicio 33.2, exprésese el mcd positivo de 49 349 y 15 555 en  $\mathbb{Z}$ , en la forma  $\lambda(49\ 349) + \mu(15\ 555)$  para  $\lambda, \mu \in \mathbb{Z}$ .

\*33.10 Sea  $D$  un dominio euclíadiano y sea  $v$  una evaluación euclíadiana en  $D$ . Muéstrese que para  $a, b \in D$  distintos de cero, tenemos  $v(a) < v(ab)$  si y sólo si  $b$  no es unidad de  $D$ . [Sugerencia: del ejercicio 33.6, dedúzcase que  $v(a) < v(ab)$  implica que  $b$  no es unidad de  $D$ . Usando el algoritmo euclíadiano, muéstrese que  $v(a) = v(ab)$  implica  $\langle a \rangle = \langle ab \rangle$ . Conclúyase que si  $b$  no es unidad, entonces  $v(a) < v(ab)$ .]

\*33.11 Apruébese o rechácese el siguiente enunciado: si  $v$  es una evaluación euclíadiana en un dominio euclíadiano  $D$ , entonces  $\{a \in D \mid v(a) > v(1)\}$  es un ideal de  $D$ .

\*33.12 Muéstrese que todo campo es un dominio euclíadiano.

\*33.13 Sea  $v$  una evaluación euclíadiana en un dominio euclíadiano  $D$ .

- Muéstrese que si  $s \in \mathbb{Z}$  tal que  $s + v(1) > 0$ , entonces  $\eta: D^* \rightarrow \mathbb{Z}$  definida por  $\eta(a) = v(a) + s$  para  $a \in D$  distinta de cero, es una evaluación euclíadiana en  $D$ . Como es costumbre,  $D^*$  es el conjunto de los elementos de  $D$  distintos de cero.
- Muéstrese que para  $r \in \mathbb{Z}^+$ ,  $\lambda: D^* \rightarrow \mathbb{Z}$  dados por  $\lambda(a) = r(v(a))$  para  $a \in D$  distinta de cero, es una evaluación euclíadiana en  $D$ .
- Muéstrese que existe una evaluación euclíadiana  $\mu$  en  $D$  tal que  $\mu(1) = 1$  y  $\mu(a) > 100$  para todas las no unidades  $a \in D$  distintas de cero.

\*33.14 Sea  $D$  un DFU. Un elemento  $c$  en  $D$  es un **mínimo común múltiplo** (mcm) de dos elementos  $a$  y  $b$  en  $D$  si  $a \mid c$ ,  $b \mid c$  y si  $c$  divide a todo elemento de  $D$  que sea divisible entre  $a$  y entre  $b$ . Muéstrese que todos dos elementos distintos de cero  $a$  y  $b$  de un dominio euclíadiano  $D$  tienen algún mcm en  $D$ . [Sugerencia: muéstrese que todos los múltiplos comunes, en el sentido obvio, de  $a$  y  $b$ , forman un ideal de  $D$ .]

\*33.15 Usese la última afirmación del teorema 33.3, para mostrar que dos elementos distintos de cero  $r, s \in \mathbb{Z}$  generan al grupo  $\langle \mathbb{Z}, + \rangle$  si y sólo si  $r$  y  $s$ , vistos como enteros en el dominio  $\mathbb{Z}$ , son **primos relativos**, esto es, tienen un mcd igual a 1.

\*33.16 Usando la última afirmación del teorema 33.2, muéstrese que para  $a, b, n \in \mathbb{Z}$  distintos de cero, la congruencia  $ax \equiv b \pmod{n}$  tiene solución en  $\mathbb{Z}$  si y sólo si el mcd positivo de  $a$  y  $n$  en  $\mathbb{Z}$  divide a  $b$ . Interprétense este resultado en el anillo  $\mathbb{Z}_n$ .

\*33.17 Generalícese el ejercicio 33.16, mostrando que para  $a, b, n \in \mathbb{Z}$  distintos de cero, la congruencia  $ax \equiv b \pmod{n}$  tiene solución en  $\mathbb{Z}$  si y sólo si el mcd positivo de  $a$  y  $n$  en  $\mathbb{Z}$  divide a  $b$ . Interprétense este resultado en el anillo  $\mathbb{Z}_n$ .

\*33.18 Siguiendo la idea de los ejercicios 33.4 y 33.17, esbócese un método constructivo para encontrar una solución en  $\mathbb{Z}$  de la congruencia  $ax \equiv b \pmod{n}$  para  $a, b, n \in \mathbb{Z}$  distintos de cero, si es que la congruencia tiene solución. Usese este método para encontrar una solución de la congruencia  $22x \equiv 18 \pmod{42}$ .

## \* 34

# Enteros gaussianos y normas

## \* 34.1 ENTEROS GAUSSIANOS

Deberemos dar un ejemplo de un dominio euclíadiano distinto de  $\mathbf{Z}$  y  $F[x]$ .

**Definición** Un *entero gaussiano* es un número complejo  $a + bi$  donde  $a, b \in \mathbf{Z}$ . Para un entero gaussiano  $\alpha = a + bi$  la *norma*  $N(\alpha)$  de  $\alpha$  es  $a^2 + b^2$ .

Denotaremos por  $\mathbf{Z}[i]$  al conjunto de todos los enteros gaussianos. El lema siguiente da algunas propiedades básicas de la función norma  $N$  en  $\mathbf{Z}[i]$  y conduce a la demostración de que la función  $v$  definida por  $v(\alpha) = N(\alpha)$  para  $\alpha \in \mathbf{Z}[i]$  distinto de cero es una evaluación euclíadiana en  $\mathbf{Z}[i]$ . Nótese que los enteros gaussianos incluyen todos los **racionales enteros**, esto es, todos los elementos de  $\mathbf{Z}$ .

**Lema 34.1** En  $\mathbf{Z}[i]$  se cumplen las siguientes propiedades de la función norma  $N$  para todas las  $\alpha, \beta \in \mathbf{Z}[i]$ :

- 1  $N(\alpha) \geq 0$ .
- 2  $N(\alpha) = 0$  si y sólo si  $\alpha = 0$ .
- 3  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

**Demostración** Si hacemos  $\alpha = a_1 + a_2i$  y  $\beta = b_1 + b_2i$  todos estos resultados son o bien obvios o bien producto de un cálculo directo. Dejamos como ejercicio la demostración de estas propiedades (véase el ejercicio 34.8). ■

**Lema 34.2**  $\mathbf{Z}[i]$  es un dominio entero.

**Demostración** Es obvio que  $\mathbf{Z}[i]$  es un anillo commutativo con unitario. Mostremos que no hay divisores de 0. Sean  $\alpha, \beta \in \mathbf{Z}[i]$ . Usando el lema 34.1, si  $\alpha\beta = 0$ , entonces

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0.$$

Así,  $\alpha\beta = 0$  implica que  $N(\alpha) = 0$  o  $N(\beta) = 0$ . De nuevo, por el lema 34.1, esto implica que  $\alpha = 0$  o  $\beta = 0$ . Así,  $\mathbf{Z}[i]$  no tiene divisiones de 0, de modo que  $\mathbf{Z}[i]$  es un dominio entero. ■

Por supuesto que, como  $\mathbf{Z}[i]$  es un subanillo de  $\mathbf{C}$  donde  $\mathbf{C}$  es el campo de los números complejos, es realmente obvio que  $\mathbf{Z}[i]$  no tiene divisiones de 0. El argumento, en el lema 34.2, ilustró el uso de la propiedad multiplicativa 3 de la función norma  $N$  y evitó salir de  $\mathbf{Z}[i]$  durante la deducción.

**Teorema 34.1** *La función  $v$  dada por  $v(\alpha) = N(\alpha)$  para  $\alpha \in \mathbf{Z}[i]$  distinto de cero, es una evaluación euclíadiana en  $\mathbf{Z}[i]$ . Así,  $\mathbf{Z}[i]$  es un dominio euclíadiano.*

**Demostración** Nótese que para  $\beta = b_1 + b_2i \neq 0$ ,  $N(b_1 + b_2i) = b_1^2 + b_2^2$ , de modo que  $N(\beta) \geq 1$ . Entonces, para todas las  $\alpha, \beta \neq 0$  en  $\mathbf{Z}[i]$ ,  $N(\alpha)N(\beta) = N(\alpha\beta)$ . Esto prueba la condición 2 para una evaluación euclíadiana.

Falta probar el algoritmo de la división, condición 1, para  $N$ . Sea  $\alpha, \beta \in \mathbf{Z}[i]$ , con  $\alpha = a_1 + a_2i$  y  $\beta = b_1 + b_2i$ , donde  $\beta \neq 0$ . Debemos encontrar  $\sigma$  y  $\rho$  en  $\mathbf{Z}[i]$  tales que  $\alpha = \beta\sigma + \rho$ , donde  $\rho = 0$  o  $N(\rho) < N(\beta) = b_1^2 + b_2^2$ . Hagamos  $\sigma = q_1 + q_2i$  donde  $q_1$  y  $q_2$  son *racionales enteros* a determinar en  $\mathbf{Z}$ . Entonces,  $\rho$  deberá tener la forma

$$\begin{aligned}\rho &= (a_1 + a_2i) - (b_1 + b_2i)(q_1 + q_2i) \\ &= (a_1 - b_1q_1 + b_2q_2) + (a_2 - b_1q_2 - b_2q_1)i.\end{aligned}$$

Tenemos que encontrar *racionales enteros*  $q_1$  y  $q_2$  tales que

$$N(\rho) = (a_1 - b_1q_1 + b_2q_2)^2 + (a_2 - b_1q_2 - b_2q_1)^2 < b_1^2 + b_2^2$$

esto es, tales que

$$\frac{(a_1 - b_1q_1 + b_2q_2)^2}{b_1^2 + b_2^2} + \frac{(a_2 - b_1q_2 - b_2q_1)^2}{b_1^2 + b_2^2} < 1.$$

Ahora bien, se recordará que

$$\frac{(a_1 - b_1q_1 + b_2q_2)^2}{b_1^2 + b_2^2}$$

es precisamente el cuadrado de la distancia  $d$  en el plano euclíadiano de un punto  $(q_1, q_2)$  a la recta  $l$  con ecuación  $a_1 - b_1 X + b_2 Y = 0$ . De manera análoga,

$$\frac{(a_2 - b_1 q_2 - b_2 q_1)^2}{b_1^2 + b_2^2}$$

es el cuadrado de la distancia  $d'$  de  $(q_1, q_2)$  a la recta  $l'$  con ecuación  $a_2 - b_2 X - b_1 Y = 0$ . Nótese que  $l$  es perpendicular a  $l'$ . Sea  $P$  el punto de intersección de estas dos rectas, según se muestra en la figura 34.1. De la figura, se ve que  $d^2 + (d')^2$  es el cuadrado de la distancia de  $(q_1, q_2)$  a  $P$ . Así, debemos mostrar que existe un punto  $(q_1, q_2)$  con *coordenadas enteras* y tal que el cuadrado de la distancia a  $P$  es menor que 1. Como  $P$  está contenido en el interior o en la frontera de algún cuadrado de lado unitario, tal que ambas coordenadas de cada vértice son enteras, está claro que si se escoge  $(q_1, q_2)$  como el punto con coordenadas enteras más cercano a  $P$ , su distancia a  $P$  podrá ser a lo más, la mitad de la longitud de una diagonal del cuadrado, esto es, a lo más  $\sqrt{2}/2$  (véase la Fig. 34.2). Así, el cuadrado de esta distancia a  $P$  es a lo más  $\frac{1}{2}$ , lo cual es menor que 1. ■

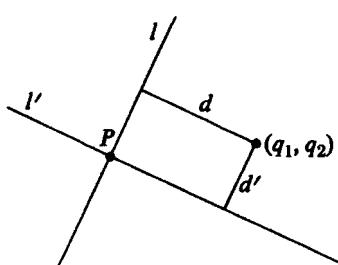


Figura 34.1

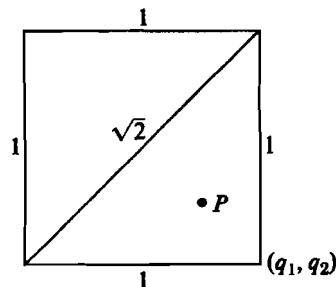


Figura 34.2

Pudimos haber probado el algoritmo de la división para la función  $N$  de manera exclusivamente algebraica; la demostración algebraica es más fácil, breve y útil para aplicar el algoritmo euclíadiano para  $N$  (véanse los ejercicios 34.4 y 34.12). Pero confesamos tener cierta debilidad por el argumento geométrico. Además, es agradable tener variedad en las demostraciones del libro. Dejamos una demostración algebraica para los ejercicios (véase el ejercicio 34.11).

**Ejemplo 34.1** Podemos aplicar ahora a  $\mathbb{Z}[i]$ , los resultados del capítulo 33. En particular, como  $N(1) = 1$ , las unidades de  $\mathbb{Z}[i]$  son exactamente las  $\alpha = a_1 + a_2 i$  con  $N(\alpha) = a_1^2 + a_2^2 = 1$ . Del hecho que  $a_1$  y  $a_2$  son enteros, se sigue que las únicas posibilidades son  $a_1 = \pm 1$  con  $a_2 = 0$ , o  $a_1 = 0$  con  $a_2 = \pm 1$ . Así, las unidades de  $\mathbb{Z}[i]$  son  $\pm 1$  y  $\pm i$ . También podemos usar el algoritmo euclíadiano para calcular el mcd de dos elementos distintos de cero. Dejamos dichos cálculos para los ejercicios. Por último, nótese que mientras 5 es un irreducible en  $\mathbb{Z}$ , 5 ya no es irreducible en  $\mathbb{Z}[i]$ , pues  $5 = (1 + 2i)(1 - 2i)$  y ni  $1 + 2i$  ni  $1 - 2i$  es unidad. ■

## \*34.2 NORMAS MULTIPLICATIVAS

Señalemos una vez más que para un dominio entero  $D$ , los conceptos aritméticos de irreducibles y unidades son intrínsecos al dominio entero mismo y de ninguna manera son afectados por una evaluación o norma, que pueda definirse en el dominio. Sin embargo, como lo muestra el capítulo anterior y nuestro trabajo hasta este punto del presente capítulo, una evaluación o norma definida convenientemente puede ayudar a determinar la estructura aritmética de  $D$ . Esto se ilustra de manera sorprendente en la teoría de números algebraicos, donde para un dominio de enteros algebraicos se consideran varias evaluaciones diferentes del dominio, cada una cumple su cometido para ayudar a determinar la estructura aritmética del dominio. En un dominio de enteros algebraicos, tenemos esencialmente una evaluación para cada irreducible (salvo asociados) y cada una de dichas evaluaciones da información acerca del comportamiento, en el dominio entero, del irreducible al cual corresponde. Este es un ejemplo de la importancia del estudio de propiedades de elementos en una estructura algebraica, mediante funciones asociadas con ellos. En las siguientes secciones lo haremos para ceros de polinomios.

Estudiemos dominios enteros que tengan una norma multiplicativa que satisfaga las propiedades de  $N$  en  $\mathbb{Z}[i]$  dadas en el lema 34.1.

**Definición** Sea  $D$  un dominio entero. Una **norma multiplicativa  $N$  en  $D$**  es una función que transforma  $D$  en los enteros  $\mathbb{Z}$  tal que se satisfacen las condiciones siguientes:

- 1  $N(\alpha) \geq 0$  para todas las  $\alpha \in D$ .
- 2  $N(\alpha) = 0$  si y sólo si  $\alpha = 0$ .
- 3  $N(\alpha\beta) = N(\alpha)N(\beta)$  para todas las  $\alpha, \beta \in D$ .

**Teorema 34.2** Si  $D$  es un dominio entero con norma multiplicativa  $N$ , entonces  $N(1) = 1$  y  $N(u) = 1$  para toda unidad  $u$  en  $D$ . Si, además, toda  $\alpha$  tal que  $N(\alpha) = 1$  es una unidad en  $D$ , entonces un elemento  $\pi$  en  $D$  con  $N(\pi) = p$  para  $p \in \mathbb{Z}$  primo, es un irreducible de  $D$ .

**Demostración** Sea  $D$  un dominio entero con norma multiplicativa  $N$ . Entonces,

$$N(1) = N((1)(1)) = N(1)N(1)$$

muestra que  $N(1) = 1$ . Además, si  $u$  es una unidad en  $D$ , entonces

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}).$$

Como  $N(u)$  es un entero no negativo, esto implica que  $N(u) = 1$ .

Supóngase ahora que las unidades de  $D$  son precisamente los elementos de norma 1. Sea  $\pi \in D$  tal que  $N(\pi) = p$  donde  $p$  es un primo en  $\mathbb{Z}$ . Entonces, si  $\pi = \alpha\beta$  tenemos

$$p = N(\pi) = N(\alpha)N(\beta),$$

así que  $N(\alpha) = 1$  o  $N(\beta) = 1$ . Por hipótesis, esto significa que  $\alpha$  o  $\beta$  es unidad de  $D$ . Así,  $\pi$  es un irreducible de  $D$ . ■

**Ejemplo 34.2** En  $\mathbb{Z}[i]$  la función  $N$  definida por  $N(a + bi) = a^2 + b^2$  da una norma multiplicativa en el sentido de nuestra definición. Vimos que la función  $v$  dada por  $v(\alpha) = N(\alpha)$  para  $\alpha \in \mathbb{Z}[i]$  distinto de cero, es una evaluación euclíadiana en  $\mathbb{Z}[i]$ , de modo que las unidades son precisamente los elementos  $\alpha$  de  $\mathbb{Z}[i]$  con  $N(\alpha) = N(1) = 1$ . Así, la segunda parte del teorema 34.2 se aplica en  $\mathbb{Z}[i]$ . En el ejemplo 34.1 vimos que 5 no es un irreducible en  $\mathbb{Z}[i]$ , pues  $5 = (1 + 2i)(1 - 2i)$ . Como  $N(1 + 2i) = N(1 - 2i) = 1^2 + 2^2 = 5$  y 5 es primo en  $\mathbb{Z}$ , vemos, del teorema 34.2, que  $1 + 2i$  y  $1 - 2i$  son ambos irreducibles en  $\mathbb{Z}[i]$ . ■

Como aplicación de las normas multiplicativas, daremos ahora otro ejemplo de dominio entero que *no* es un DFU. Vimos un ejemplo, en el ejemplo 32.3. Lo siguiente es la ilustración usual.

**Ejemplo 34.3** Sea  $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ . Como subconjunto de los números complejos, cerrado bajo la suma, resta y multiplicación, que contiene a 0 y 1,  $\mathbb{Z}[\sqrt{-5}]$  es un dominio entero. Definase  $N$  en  $\mathbb{Z}[\sqrt{-5}]$  por

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

(Aqui,  $\sqrt{-5} = i\sqrt{5}$ .) Es claro que  $N(\alpha) \geq 0$  y  $N(\alpha) = 0$  si y sólo si  $\alpha = a + b\sqrt{-5} = 0$ . Que  $N(\alpha\beta) = N(\alpha)N(\beta)$  es un cálculo directo que dejamos para los ejercicios (véase el ejercicio 34.9). Encontremos todos los candidatos a unidades en  $\mathbb{Z}[\sqrt{-5}]$  buscando todos los elementos  $\alpha$  en  $\mathbb{Z}[\sqrt{-5}]$  con  $N(\alpha) = 1$ . Si  $\alpha = a + b\sqrt{-5}$  y  $N(\alpha) = 1$  debemos tener  $a^2 + 5b^2 = 1$  para enteros  $a$  y  $b$ . Esto sólo es posible si  $b = 0$  y  $a = \pm 1$ . Por tanto,  $\pm 1$  son los únicos candidatos para unidades. Como  $\pm 1$  son unidades, son entonces, todas las unidades en  $\mathbb{Z}[\sqrt{-5}]$ .

Ahora, en  $\mathbb{Z}[\sqrt{-5}]$  tenemos  $21 = (3)(7)$  y también

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Si podemos mostrar que  $3, 7, 1 + 2\sqrt{-5}$  y  $1 - 2\sqrt{-5}$  son todos irreducibles en  $\mathbb{Z}[\sqrt{-5}]$ , sabremos entonces que  $\mathbb{Z}[\sqrt{-5}]$  no puede ser un DFU, pues ni 3 ni 7 es igual a  $\pm(1 + 2\sqrt{-5})$ .

Supóngase que  $3 = \alpha\beta$ . Entonces,

$$9 = N(3) = N(\alpha)N(\beta)$$

muestra que debemos tener  $N(\alpha) = 1, 3$  ó  $9$ . Si  $N(\alpha) = 1$ , entonces  $\alpha$  es unidad. Si  $\alpha = a + b\sqrt{-5}$ , entonces  $N(\alpha) = a^2 + 5b^2$  y para ninguna selección de enteros  $a$  y  $b$  se tiene  $N(\alpha) = 3$ . Si  $N(\alpha) = 9$ , entonces  $N(\beta) = 1$  de modo que  $\beta$  es unidad. Así, de  $3 = \alpha\beta$  podemos concluir que  $\alpha$  o  $\beta$  es unidad. Por tanto,  $3$  es un irreducible en  $\mathbb{Z}[\sqrt{-5}]$ . Un argumento análogo muestra que  $7$  también es un irreducible en  $\mathbb{Z}[\sqrt{-5}]$ . Si  $1 + 2\sqrt{-5} = \gamma\delta$ , tenemos

$$21 = N(1 + 2\sqrt{-5}) = N(\gamma)N(\delta),$$

de modo que  $N(\gamma) = 1, 3, 7$  ó  $21$ . Hemos visto que no hay elemento de  $\mathbb{Z}[\sqrt{-5}]$  de norma  $3$  ó  $7$ . Así, o  $N(\gamma) = 1$  y  $\gamma$  es unidad, o  $N(\gamma) = 21$  de modo que  $N(\delta) = 1$  y  $\delta$  es unidad. Por tanto,  $1 + 2\sqrt{-5}$  es un irreducible en  $\mathbb{Z}[\sqrt{-5}]$ .

En resumen, hemos mostrado que

$$\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$$

es un dominio entero pero no un DFU. En particular, hay dos factorizaciones diferentes

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

de  $21$  en irreducibles. Estos irreducibles no pueden ser primos, pues la propiedad de ser primo nos permite probar la unicidad de la factorización (véase la demostración del teorema 32.2). ■

## Ejercicios

---

\*34.1 Factorícese cada uno de los siguientes enteros gaussianos en un producto de irreducibles en  $\mathbb{Z}[i]$ . [Sugerencia: como un factor irreducible de  $\alpha \in \mathbb{Z}[i]$  debe tener norma  $> 1$  y dividir  $N(\alpha)$ , hay sólo un número finito de enteros gaussianos  $a + bi$  a considerar como posibles factores irreducibles de un  $\alpha$  dado. Divídase  $\alpha$  en  $\mathbb{C}$  entre cada uno de ellos y verifíquese para cuáles el cociente está en  $\mathbb{Z}[i]$ .]

- a)  $5$       b)  $7$       c)  $4 + 3i$       d)  $6 - 7i$

\*34.2 Muéstrese que  $6$  no se factoriza de manera única (sin considerar asociados) en irreducibles en  $\mathbb{Z}[\sqrt{-5}]$ . Exhiban dos factorizaciones diferentes.

\*34.3 Considérense  $\alpha = 7 + 2i$  y  $\beta = 3 - 4i$  en  $\mathbb{Z}[i]$ . Encuéntrense  $\sigma$  y  $\rho$  en  $\mathbb{Z}[i]$  tales que

$$\alpha = \beta\sigma + \rho \quad \text{con} \quad N(\rho) < N(\beta).$$

[Sugerencia: úsese la construcción de la sugerencia del ejercicio 34.11.]

\*34.4 Usese un algoritmo eucliano en  $\mathbb{Z}[i]$  para encontrar un mcd de  $8 + 6i$  y  $5 - 15i$  en  $\mathbb{Z}[i]$ . [Sugerencia: úsese la construcción de la sugerencia del ejercicio 34.11.]

\*34.5 Sea  $D$  un dominio entero con una norma multiplicativa  $N$ , tal que  $N(\alpha) = 1$  para  $\alpha \in D$  si y sólo si  $\alpha$  es una unidad de  $D$ . Sea  $\pi$  tal que  $N(\pi)$  es minimal de entre todos los  $N(\beta) > 1$  para  $\beta \in D$ . Muéstrese que  $\pi$  es un irreducible de  $D$ .

\*34.6 ¿Falso o verdadero?

- a)  $\mathbb{Z}[i]$  es un DIP.
  - b)  $\mathbb{Z}[i]$  es un dominio eucliano.
  - c) Todo entero en  $\mathbb{Z}$  es un entero gaussiano.
  - d) Todo número complejo es un entero gaussiano.
  - e) En  $\mathbb{Z}[i]$  se cumple un algoritmo eucliano.
  - f) Una norma multiplicativa en un dominio entero a veces es útil para encontrar irreducibles del dominio.
  - g) Si  $N$  es una norma multiplicativa en un dominio entero  $D$ , entonces  $N(u) = 1$  para toda unidad  $u$  de  $D$ .
  - h) Si  $F$  es un campo, entonces la función  $N$  definida por  $N(f(x)) = (\text{grado de } f(x))$  es una norma multiplicativa en  $F[x]$ .
  - i) Si  $F$  es un campo, entonces la función definida por  $N(f(x)) = 2^{(\text{grado de } f(x))}$  para  $f(x) \neq 0$  y  $N(0) = 0$  es una norma multiplicativa en  $F[x]$ , de acuerdo con nuestra definición.
  - j)  $\mathbb{Z}[\sqrt{-5}]$  es un dominio entero pero no un DFU.
- 

\*34.7 Muéstrese que  $1 + i$  es un irreducible de  $\mathbb{Z}[i]$ . [Sugerencia: aplíquese el teorema 34.2.] (Para una descripción de todos los primos gaussianos, véase Pollard [34].)

\*34.8 Pruébese el lema 34.1.

\*34.9 Pruébese que  $N$ , del ejemplo 34.3, es multiplicativa, esto es, que  $N(\alpha\beta) = N(\alpha)N(\beta)$  para  $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ .

\*34.10 Sea  $D$  un dominio entero con norma multiplicativa  $N$  tal que  $N(\alpha) = 1$  para  $\alpha \in D$  si y sólo si  $\alpha$  es una unidad de  $D$ . Muéstrese que toda no unidad distinta de cero de  $D$  tiene factorización en irreducibles en  $D$ .

\*34.11 Pruébese algebraicamente que el algoritmo de la división se cumple en  $\mathbb{Z}[i]$  para  $v$  dada por  $v(\alpha) = N(\alpha)$  para  $\alpha \in \mathbb{Z}[i]$  distinto de cero. [Sugerencia: para  $\alpha$  y  $\beta$  en  $\mathbb{Z}[i]$  con  $\beta \neq 0$ ,  $\alpha/\beta = r + si$  en  $\mathbb{C}$  para  $r, s \in \mathbb{Q}$ . Sean  $q_1$  y  $q_2$  enteros racionales en  $\mathbb{Z}$  lo más cercanos posible a los números racionales  $r$  y  $s$ , respectivamente. Muéstrese que para  $\sigma = q_1 + q_2i$  y  $\rho = \alpha - \beta\sigma$  tenemos  $N(\rho) < N(\beta)$ , mediante la demostración de que

$$N(\rho)/N(\beta) = |(\alpha/\beta) - \sigma|^2 < 1.$$

Aquí,  $||$  es el valor absoluto usual para los elementos de  $\mathbb{C}$ .]

\*34.12 Usese un algoritmo eucliano en  $\mathbb{Z}[i]$  para encontrar un mcd de  $16 + 7i$  y  $10 - 5i$  en  $\mathbb{Z}[i]$ . [Sugerencia: úsese la construcción de la sugerencia del ejercicio 34.11.]

\*34.13 Sea  $\langle \alpha \rangle$  un ideal principal distinto de cero en  $\mathbb{Z}[i]$ .

a) Muéstrese que  $\mathbb{Z}[i]/\langle \alpha \rangle$  es un anillo finito. [Sugerencia: úsese el algoritmo de división.]

- b) Muéstrese que si  $\pi$  es un irreducible de  $\mathbb{Z}[i]$ , entonces  $\mathbb{Z}[i]/\langle \pi \rangle$  es un campo.
- c) Con respecto a b), encuéntrese el orden y característica de cada uno de los campos siguientes.
- $\mathbb{Z}[i]/\langle 3 \rangle$
  - $\mathbb{Z}[i]/\langle 1 + i \rangle$
  - $\mathbb{Z}[i]/\langle 1 + 2i \rangle$

\*34.14 Sea  $n \in \mathbb{Z}^+$  libre de cuadrado, esto es, no es divisible entre el cuadrado de ningún entero primo. Sea  $\mathbb{Z}[\sqrt{-n}] = \{a + ib\sqrt{n} | a, b \in \mathbb{Z}\}$ .

- Muéstrese que la norma  $N$  definida por  $N(\alpha) = a^2 + nb^2$  para  $\alpha = a + ib\sqrt{n}$  es una norma multiplicativa en  $\mathbb{Z}[\sqrt{-n}]$ .
- Muéstrese que  $N(\alpha) = 1$  para  $\alpha \in \mathbb{Z}[\sqrt{-n}]$  si y sólo si  $\alpha$  es una unidad de  $\mathbb{Z}[\sqrt{-n}]$ .
- Muéstrese que todo  $\alpha \in \mathbb{Z}[\sqrt{-n}]$  distinto de cero que no sea unidad, tiene factorización en irreducibles en  $\mathbb{Z}[\sqrt{-n}]$ . [Sugerencia: úsese b).]

\*34.15 Repítase el ejercicio 34.14 para  $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n}/a, b \in \mathbb{Z}\}$  con  $N$  definida por  $N(\alpha) = |a^2 - nb^2|$  para  $\alpha = a + b\sqrt{n}$  en  $\mathbb{Z}[\sqrt{n}]$ .

\*34.16 Muéstrese, mediante una construcción análoga a la dada en la sugerencia del ejercicio 34.11, que el algoritmo de la división se cumple en los dominios enteros  $\mathbb{Z}[\sqrt{-2}]$ ,  $\mathbb{Z}[\sqrt{2}]$  y  $\mathbb{Z}[\sqrt{3}]$  para  $v(\alpha) = N(\alpha)$  para  $\alpha$  distinta de cero en uno de estos dominios (véanse los ejercicios 34.14 y 34.15). (Así, estos dominios son euclidianos. Véase Hardy and Wright [28] para un análisis acerca de cuáles de los dominios  $\mathbb{Z}[\sqrt{n}]$  y  $\mathbb{Z}[\sqrt{-n}]$  son euclidianos.)

# Introducción a los campos de extensión

## 35.1 EL OBJETIVO FUNDAMENTAL ALCANZADO

Ya estamos en posición de alcanzar nuestro *objetivo fundamental* que, enunciado informalmente, es mostrar que todo polinomio no constante tiene algún cero. Esto se enunciará de manera precisa y se probará en el teorema 35.1. Antes, se introducirá nueva terminología para algunas viejas ideas.

**Definición** Un campo  $E$  es un *campo de extensión de un campo  $F$*  si  $F \leq E$ .

Así,  $R$  es un campo de extensión de  $Q$ , y  $C$  es un campo de extensión tanto de  $R$  como de  $Q$ . Como en el estudio de grupos, con frecuencia será conveniente usar diagramas reticulares para ilustrar campos de extensión, donde el campo mayor estará arriba (véase la figura 35.1). Una configuración donde sólo hay una columna de campos, como en el lado izquierdo de la figura 35.1, suele denominarse, sin una definición precisa, una *torre de campos*. Usaremos libremente este término.

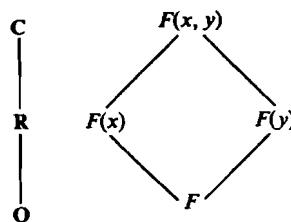


Figura 35.1

Ahora, nos dirigiremos al *objetivo fundamental*. Este gran e importante resultado se sigue fácilmente y de manera elegante, de las técnicas a nuestra disposición. Escojan un lugar agradable y tranquilo, donde tengan un cuarto de hora para leerlo, digerirlo y maravillarse todo lo que quieran sin interrupción. Escribimos la demostración con el espantoso detalle usual. (Un libro para nivel de posgrado no emplearía, a estas alturas, más de tres renglones.)

**Teorema 35.1 (Kronecker) (Objetivo fundamental)** *Sea  $F$  un campo y sea  $f(x)$  un polinomio no constante en  $F[x]$ . Entonces, existe un campo de extensión  $E$  de  $F$  y alguna  $\alpha \in E$  tal que  $f(\alpha) = 0$ .*

**Demostración** Por el teorema 31.8,  $f(x)$  tiene factorización en  $F[x]$  en polinomios que son irreducibles en  $F$ . Sea  $p(x)$  un polinomio irreducible presente en dicha factorización. Es claro que basta encontrar un campo de extensión  $E$  de  $F$  que contenga algún elemento  $\alpha$ , tal que  $p(\alpha) = 0$ .

Por el teorema 31.6,  $\langle p(x) \rangle$  es un ideal maximal en  $F[x]$  de modo que  $F[x]/\langle p(x) \rangle$  es un campo. Aseguramos que  $F$  puede identificarse con un subcampo de  $F[x]/\langle p(x) \rangle$  de manera natural, mediante la transformación  $\psi : F \rightarrow F[x]/\langle p(x) \rangle$  dada por

$$a\psi = a + \langle p(x) \rangle$$

para  $a \in F$ . Esta transformación es uno a uno, pues si  $a\psi = b\psi$ , esto es, si  $a + \langle p(x) \rangle = b + \langle p(x) \rangle$  para algunas  $a, b \in F$ , entonces  $(a - b) \in \langle p(x) \rangle$ , de modo que  $a - b$  debe ser un múltiplo del polinomio  $p(x)$ , el cual es de grado  $\geq 1$ . Ahora bien,  $a, b \in F$  implica que  $a - b$  está en  $F$ . Así, debemos tener  $a - b = 0$  de modo que  $a = b$ . Definimos suma y multiplicación en  $F[x]/\langle p(x) \rangle$  escogiendo cualesquiera representantes, así, podemos escoger  $a \in (a + \langle p(x) \rangle)$ . Entonces, es claro que esta transformación  $\psi$  es un isomorfismo de  $F$  en  $F[x]/\langle p(x) \rangle$ . Identificamos  $F$  con  $\{a + \langle p(x) \rangle | a \in F\}$  mediante este isomorfismo. Así, veremos  $E = F[x]/\langle p(x) \rangle$  como un campo de extensión de  $F$ . Hemos construido nuestro campo de extensión deseado  $E$  de  $F$ . Falta mostrar que  $E$  contiene algún cero de  $p(x)$ .

Hagamos

$$\alpha = x + \langle p(x) \rangle,$$

de modo que  $\alpha \in E$ . Considérese el homomorfismo de evaluación  $\phi_\alpha : F[x] \rightarrow E$  dado por el teorema 30.2. Si  $p(x) = a_0 + a_1x + \cdots + a_nx^n$  donde  $a_i \in F$ , entonces, tenemos

$$p(x)\phi_\alpha = a_0 + a_1(x + \langle p(x) \rangle) + \cdots + a_n(x + \langle p(x) \rangle)^n$$

en  $E = F[x]/\langle p(x) \rangle$ . Pero podemos calcular en  $F[x]/\langle p(x) \rangle$  escogiendo representantes y  $x$  es un representante de la clase lateral  $\alpha = x + \langle p(x) \rangle$ . Por tanto,

$$\begin{aligned} p(\alpha) &= (a_0 + a_1x + \cdots + a_nx^n) + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle = \langle p(x) \rangle = 0 \end{aligned}$$

en  $F[x]/\langle p(x) \rangle$ . Hemos encontrado un elemento  $\alpha$  en  $E = F[x]/\langle p(x) \rangle$  tal que  $p(\alpha) = 0$  y, por tanto,  $f(\alpha) = 0$ . ■

Ilustramos la construcción incluida en la demostración del teorema 35.1, mediante dos ejemplos.

**Ejemplo 35.1** Sean  $F = \mathbb{R}$  y  $f(x) = x^2 + 1$ , del cual se sabe que no tiene ceros en  $\mathbb{R}$  y, por el teorema 31.2, es irreducible en  $\mathbb{R}$ . Entonces,  $\langle x^2 + 1 \rangle$  es un ideal maximal en  $\mathbb{R}[x]$  de modo que  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  es un campo. Identificando  $r \in \mathbb{R}$  con  $r + \langle x^2 + 1 \rangle$  en  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  podemos considerar  $\mathbb{R}$  como subcampo de  $E = \mathbb{R}[x]/\langle x^2 + 1 \rangle$ . Sea

$$\alpha = x + \langle x^2 + 1 \rangle.$$

Calculando en  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ , encontramos que

$$\begin{aligned}\alpha^2 + 1 &= (x + \langle x^2 + 1 \rangle)^2 + (1 + \langle x^2 + 1 \rangle) \\ &= (x^2 + 1) + \langle x^2 + 1 \rangle = 0.\end{aligned}$$

Así,  $\alpha$  es un cero de  $x^2 + 1$ . Al final de este capítulo, identificaremos  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  con  $\mathbb{C}$ . ■

**Ejemplo 35.2** Sea  $F = \mathbb{Q}$  y sea  $f(x) = x^4 - 5x^2 + 6$ . Ahora,  $f(x)$  se factoriza en  $\mathbb{Q}[x]$  en  $(x^2 - 2)(x^2 - 3)$ , ambos factores son irreducibles en  $\mathbb{Q}$ , según ya vimos. Podemos empezar con  $x^2 - 2$  y construir un campo de extensión  $E$  de  $\mathbb{Q}$  que contenga  $\alpha$  tal que  $\alpha^2 - 2 = 0$  o podemos construir un campo de extensión  $K$  de  $\mathbb{Q}$  que contenga algún elemento  $\beta$  tal que  $\beta^2 - 3 = 0$ . En ambos casos, la construcción es como en el ejemplo 35.1. ■

## 35.2 ELEMENTOS ALGEBRAICOS Y TRASCENDENTES

Como ya dijimos, en el resto del libro, las secciones no marcadas con asterisco tratan del estudio de ceros de polinomios. Comencemos este estudio colocando un elemento de un campo de extensión  $E$  de un campo  $F$  en una de dos categorías.

**Definición** Un elemento  $\alpha$  de un campo de extensión  $E$  de un campo  $F$  es *algebraico sobre  $F$*  si  $f(\alpha) = 0$  para algún  $f(x) \in F[x]$  distinto de cero. Si  $\alpha$  no es algebraico sobre  $F$ , entonces  $\alpha$  es *trascendente sobre  $F$* .

**Ejemplo 35.3**  $C$  es un campo de extensión de  $\mathbb{Q}$ . Como  $\sqrt{2}$  es un cero de  $x^2 - 2$ ,  $\sqrt{2}$  es un elemento algebraico sobre  $\mathbb{Q}$ . Además,  $i$  es un elemento algebraico sobre  $\mathbb{Q}$ , pues es un cero de  $x^2 + 1$ . ■

**Ejemplo 35.4** Es bien conocido (aunque no es fácil probarlo), que los números reales  $\pi$  y  $e$  son trascendentes sobre  $\mathbb{Q}$ . Aquí,  $e$  es la base de los logaritmos naturales. ■

Así como no podemos hablar de un *polinomio irreducible «a secas»*, sino de un *polinomio irreducible sobre  $F$* , análogamente, no hablamos de un *elemento algebraico «a secas»*, sino de un *elemento algebraico sobre  $F$* . La siguiente ilustración muestra la razón.

**Ejemplo 35.5** El número real  $\pi$  es trascendente sobre  $\mathbb{Q}$ , según se afirmó en el ejemplo 35.4. Sin embargo,  $\pi$  es algebraico sobre  $\mathbb{R}$ , pues es un cero de  $(x - \pi) \in \mathbb{R}[x]$ . ■

**Ejemplo 35.6** Es fácil ver que el número real  $\sqrt{1 + \sqrt{3}}$  es algebraico sobre  $\mathbb{Q}$ . Pues si  $\alpha = \sqrt{1 + \sqrt{3}}$ , entonces  $\alpha^2 = 1 + \sqrt{3}$  de modo que  $\alpha^2 - 1 = \sqrt{3}$  y  $(\alpha^2 - 1)^2 = 3$ . Por tanto,  $\alpha^4 - 2\alpha^2 - 2 = 0$  de modo que  $\alpha$  es un cero de  $x^4 - 2x^2 - 2$  que está en  $\mathbb{Q}[x]$ . ■

Para conectar estas ideas con las de teoría de números, damos la siguiente definición.

**Definición** Un elemento de  $C$  que sea algebraico sobre  $\mathbb{Q}$  es un *número algebraico*. Un *número trascendente* es un elemento de  $C$  que es trascendente sobre  $\mathbb{Q}$ .

Existe una extensa y elegante teoría de los números algebraicos.

El siguiente teorema da una caracterización útil de los elementos algebraicos y trascendentes sobre  $F$  en un campo de extensión  $E$  de  $F$ . También ilustra la importancia de nuestros homomorfismos de evaluación  $\phi_\alpha$ . *Nótese que, una vez más, estamos expresando los conceptos en términos de transformaciones.*

**Teorema 35.2** *Sea  $E$  un campo de extensión de un campo  $F$  y sea  $\alpha \in E$ . Sea  $\phi_\alpha : F[x] \rightarrow E$  el homomorfismo de evaluación de  $F[x]$  en  $E$ , tal que  $a\phi_\alpha = a$  para  $a \in F$  y  $x\phi_\alpha = \alpha$ . Entonces,  $\alpha$  es trascendente sobre  $F$  si y sólo si  $\phi_\alpha$  es un isomorfismo que transforma  $F[x]$  en  $E$ , esto es, si y sólo si  $\phi_\alpha$  es una transformación uno a uno.*

**Demostración** Ahora bien,  $\alpha$  es trascendente sobre  $F$  si y sólo si  $f(\alpha) \neq 0$  para todos los  $f(x) \in F[x]$  no constantes, lo cual es cierto (por definición) si y sólo si  $f(x)\phi_\alpha \neq 0$  para todos los  $f(x) \in F[x]$  no constantes, lo cual es cierto si y sólo si el kernel de  $\phi_\alpha$  es  $\{0\}$ , esto es, si y sólo si  $\phi_\alpha$  es un isomorfismo que transforma  $F[x]$  en  $E$ . ■

### 35.3 EL POLINOMIO IRREDUCIBLE DE $\alpha$ SOBRE $F$

Considérese el campo de extensión  $R$  de  $Q$ . Sabemos que  $\sqrt{2}$  es algebraico sobre  $Q$  y es un cero de  $x^2 - 2$ . Es claro que  $\sqrt{2}$  también es un cero de  $x^3 - 2x$  y de  $x^4 - 3x^2 + 2 = (x^2 - 2)(x^2 - 1)$ . Todos estos otros polinomios que tiene a  $\sqrt{2}$  como cero, eran múltiplos de  $x^2 - 2$ . El siguiente teorema muestra que esto ilustra una situación general. Este teorema desempeña un papel central en nuestro trabajo posterior.

**Teorema 35.3** *Sea  $E$  un campo de extensión de  $F$  y sea  $\alpha \in E$  donde  $\alpha$  es algebraico sobre  $F$ . Entonces, existe algún polinomio irreducible  $p(x) \in F[x]$  tal que  $p(\alpha) = 0$ . Este polinomio irreducible  $p(x)$  está determinado de manera única salvo un factor constante en  $F$  y es un polinomio de grado minimal  $\geq 1$  en  $F[x]$  que tiene a  $\alpha$  como un cero. Si  $f(\alpha) = 0$  para  $f(x) \in F[x]$  con  $f(x) \neq 0$ , entonces  $p(x)$  divide a  $f(x)$ .*

**Demostración** Sea  $\phi_\alpha$  el homomorfismo de evaluación de  $F[x]$  en  $E$  dado por el teorema 30.2. El kernel de  $\phi_\alpha$  es un ideal y, por el teorema 31.5, debe ser un ideal principal generado por algún elemento  $p(x) \in F[x]$ . Es claro que  $\langle p(x) \rangle$  consta precisamente de aquellos elementos de  $F[x]$  que tienen como un cero a  $\alpha$ . Así, si  $f(\alpha) = 0$  para  $f(x) \neq 0$ , entonces  $f(x) \in \langle p(x) \rangle$ , de modo que  $p(x)$  divide a  $f(x)$ . Es claro que  $p(x)$  es un polinomio de grado minimal  $\geq 1$  que tiene a  $\alpha$  como un cero y cualquier otro de dichos polinomios del mismo grado que  $p(x)$  debe ser de la forma  $(a)p(x)$  para algún  $a \in F$ .

Sólo falta mostrar que  $p(x)$  es irreducible. Si  $p(x) = r(x)s(x)$  fuera una factorización de  $p(x)$  en polinomios de grado menor, entonces  $p(\alpha) = 0$  implicaría que  $r(\alpha)s(\alpha) = 0$ , de modo que  $r(\alpha) = 0$  o  $s(\alpha) = 0$ , pues  $E$  es un campo. Esto contradice el hecho de que  $p(x)$  es polinomio de grado minimal  $\geq 1$  tal que  $p(\alpha) = 0$ . Así,  $p(x)$  es irreducible. ■

Multiplicando por una constante adecuada en  $F$ , podemos suponer que el coeficiente de la potencia mayor de  $x$  que aparece en  $p(x)$  del teorema 35.3, es 1. Dicho polinomio con el coeficiente de la potencia mayor de  $x$  igual a 1 es un **polinomio mónico**.

**Definición** Sea  $E$  un campo de extensión del campo  $F$  y sea  $\alpha \in E$  algebraico sobre  $F$ . El único polinomio mónico  $p(x)$  del teorema 35.3 es el **polinomio irreducible para  $\alpha$  sobre  $F$**  y se denotará por  $\text{irr}(\alpha, F)$ . El grado de  $\text{irr}(\alpha, F)$  es el **grado de  $\alpha$  sobre  $F$**  y se denota por  $\text{grad}(\alpha, F)$ .

**Ejemplo 35.7** Es claro que  $\text{irr}(\sqrt{2}, Q) = x^2 - 2$ . Con referencia al ejemplo 35.6 vemos que  $\alpha = \sqrt{1 + \sqrt{3}}$  en  $R$   $\alpha$  es un cero de  $x^4 - 2x^2 - 2$  el cual está en

$\mathbb{Q}[x]$ . Como  $x^4 - 2x^2 - 2$  es irreducible sobre  $\mathbb{Q}$  (por Eisenstein con  $p = 2$  o bien por aplicación de la técnica del ejemplo 31.6), vemos que

$$\text{irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2.$$

Así,  $\sqrt{1 + \sqrt{3}}$  es algebraico de grado 4 sobre  $\mathbb{Q}$ . ■

Así como debemos hablar de un elemento  $\alpha$  como *algebraico sobre F*, en lugar de sólo *algebraico*, también debemos hablar del *grado de  $\alpha$  sobre F*, en lugar del *grado de  $\alpha$* . Para tomar una ilustración trivial,  $\sqrt{2} \in \mathbb{R}$  es algebraico de grado 2 sobre  $\mathbb{Q}$ , pero algebraico de grado 1 sobre  $\mathbb{R}$ , pues  $\text{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$ .

Esperamos que hayan quedado impresionados por la belleza y elegancia de esta teoría. Deberían comprender que la facilidad de su desarrollo aquí, se debe a la maquinaria de los homomorfismos y la teoría de ideales que tenemos ahora a nuestra disposición. Nótese, especialmente, el uso constante de los homomorfismos de evaluación  $\phi_\alpha$ .

## 35.4 EXTENSIONES SIMPLES

Sea  $E$  un campo de extensión de un campo  $F$  y sea  $\alpha \in E$ . Sea  $\phi_\alpha$  el homomorfismo de evaluación de  $F[x]$  en  $E$  con  $a\phi_\alpha = a$  para  $a \in F$  y  $x\phi_\alpha = \alpha$  como en el teorema 30.2. Consideremos dos casos.

**CASO I** *Supóngase que  $\alpha$  es algebraico sobre F.* Entonces, como en el teorema 35.3, el kernel de  $\phi_\alpha$  es  $\langle \text{irr}(\alpha, F) \rangle$  y, por el teorema 31.6,  $\langle \text{irr}(\alpha, F) \rangle$  es un ideal maximal de  $F[x]$ . Por tanto,  $F[x]/\langle \text{irr}(\alpha, F) \rangle$  es un campo y es isomorfo a la imagen  $(F[x])\phi_\alpha$  en  $E$ . Este subcampo  $(F[x])\phi_\alpha$  de  $E$  es, claramente, el menor subcampo de  $E$  que contiene a  $F$  y a  $\alpha$ . Denotaremos este campo por  $F(\alpha)$ .

**CASO II** *Supóngase que  $\alpha$  es trascendente sobre F.* Entonces, por el teorema 35.2,  $\phi_\alpha$  es un isomorfismo que transforma  $F[x]$  en  $E$ . Así, en este caso,  $(F[x])\phi_\alpha$  no es un campo sino un dominio entero que denotaremos por  $F[\alpha]$ . Por el corolario 1 del teorema 26.2,  $E$  contiene un campo de cocientes de  $F[\alpha]$  el cual es, claramente, el menor subcampo de  $E$  que contiene  $F$  y  $\alpha$ . Como en el caso I, denotamos este campo por  $F(\alpha)$ .

**Ejemplo 35.8** Como  $\pi$  es trascendente sobre  $\mathbb{Q}$ , el campo  $\mathbb{Q}(\pi)$  es isomorfo al campo  $\mathbb{Q}(x)$  de funciones racionales sobre  $\mathbb{Q}$  con indeterminada  $x$ . Así, desde un punto de vista estructural, un elemento trascendente sobre un campo  $F$  se comporta como si fuera una indeterminada sobre  $F$ . ■

**Definición** Un campo de extensión  $E$  de un campo  $F$  es una *extensión simple de F* si  $E = F(\alpha)$  para alguna  $\alpha \in E$ .

Muchos resultados importantes aparecen a lo largo de esta sección. Hemos desarrollado tanta maquinaria, que los resultados comienzan a brotar de nuestra eficiente fábrica a un ritmo alarmante. El siguiente teorema nos da idea de la naturaleza del campo  $F(\alpha)$  en el caso en que  $\alpha$  sea algebraico sobre  $F$ .

**Teorema 35.4** *Sea  $E$  una extensión simple  $F(\alpha)$  de un campo  $F$  y sea  $\alpha$  algebraico sobre  $F$ . Sea  $n \geq 1$  el grado de  $\text{irr}(\alpha, F)$ . Entonces, todo elemento  $\beta$  de  $E = F(\alpha)$  se puede expresar de manera única en la forma*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

donde las  $b_i$  están en  $F$ .

**Demostración** Para el homomorfismo de evaluación  $\phi_\alpha$  usual, todo elemento de

$$F(\alpha) = (F[x])\phi_\alpha$$

es de la forma  $(f(x))\phi_\alpha = f(\alpha)$ , un polinomio formal en  $\alpha$  con coeficientes en  $F$ . Sea

$$\text{irr}(\alpha, F) = p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Entonces,  $p(\alpha) = 0$ , de modo que

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

Esta ecuación en  $F(\alpha)$  se puede usar para expresar cualquier monomio  $\alpha^m$  para  $m = n$  en términos de potencias de  $\alpha$  que son menores que  $n$ . Por ejemplo,

$$\begin{aligned} \alpha^{n+1} &= \alpha\alpha^n = -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha. \end{aligned}$$

Así, si  $\beta = F(\alpha)$  es posible expresar  $\beta$  en la forma requerida

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

Para la unicidad, si

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b'_0 + b'_1\alpha + \cdots + b'_{n-1}\alpha^{n-1}$$

para  $b'_i \in F$ , entonces

$$(b_0 - b'_0) + (b_1 - b'_1)x + \cdots + (b_{n-1} - b'_{n-1})x^{n-1} = g(x)$$

está en  $F[x]$  y  $g(\alpha) = 0$ . Además, el grado de  $g(x)$  es menor que el grado de  $\text{irr}(\alpha, F)$ . Como  $\text{irr}(\alpha, F)$  es un polinomio distinto de cero de grado minimal en  $F[x]$

que tiene a  $\alpha$  como un cero, debemos tener  $g(x) = 0$ . Por tanto,  $b_i - b_i = 0$ , de modo que

$$b_i = b'_i,$$

con lo cual se demuestra la unicidad de las  $b_i$ . ■

Daremos un ejemplo impresionante que ilustra el teorema 35.4.

**Ejemplo 35.9** El polinomio  $p(x) = x^2 + x + 1$  en  $\mathbb{Z}_2[x]$  es irreducible sobre  $\mathbb{Z}_2$ , debido al teorema 31.2, pues ni el elemento 0 ni el elemento 1 de  $\mathbb{Z}_2$  son ceros de  $p(x)$ . Por el teorema 35.1, sabemos que existe un campo de extensión  $E$  de  $\mathbb{Z}_2$  que contiene algún cero  $\alpha$  de  $x^2 + x + 1$ . Por el teorema 35.4,  $\mathbb{Z}_2(\alpha)$  tiene como elementos a  $0 + 0\alpha, 1 + 0\alpha + 1\alpha$  y  $1 + 1\alpha$ , esto es  $0, 1, \alpha$  y  $1 + \alpha$ . *Esto nos da un nuevo campo finito de cuatro elementos (!).* En las tablas 35.1 y 35.2 se muestran las tablas de suma y multiplicación para este campo. Por ejemplo, para calcular  $(1 + \alpha)(1 + \alpha)$  en  $\mathbb{Z}_2(\alpha)$  uno observa que como  $p(\alpha) = \alpha^2 + \alpha + 1 = 0$ , entonces

$$\alpha^2 = -\alpha - 1 = \alpha + 1.$$

Por tanto,

$$(1 + \alpha)(1 + \alpha) = 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha^2 = 1 + \alpha + 1 = \alpha.$$

**Tabla 35.1**

+	0	1	$\alpha$	$1 + \alpha$
0	0	1	$\alpha$	$1 + \alpha$
1	1	0	$1 + \alpha$	$\alpha$
$\alpha$	$\alpha$	$1 + \alpha$	0	1
$1 + \alpha$	$1 + \alpha$	$\alpha$	1	0

**Tabla 35.2**

	0	1	$\alpha$	$1 + \alpha$
0	0	0	0	0
1	0	1	$\alpha$	$1 + \alpha$
$\alpha$	0	$\alpha$	$1 + \alpha$	1
$1 + \alpha$	0	$1 + \alpha$	1	$\alpha$

Por último podemos usar el teorema 35.4 para cumplir nuestra promesa del ejemplo 35.1 y mostrar que  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  es isomorfo al campo  $\mathbb{C}$  de números complejos. Vimos en el ejemplo 35.1, que podemos considerar  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  como un campo de extensión de  $\mathbb{R}$ . Sea

$$\alpha = x + \langle x^2 + 1 \rangle.$$

Entonces  $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2 + 1 \rangle$  y, por el teorema 35.4, consta de todos los elementos de la forma  $a + b\alpha$  para  $a, b \in \mathbb{R}$ . Pero como  $\alpha^2 + 1 = 0$ , vemos que  $\alpha$  desempeña el papel de  $i \in \mathbb{C}$  y  $a + b\alpha$  el papel de  $(a + bi) \in \mathbb{C}$ . Así,  $\mathbb{R}(\alpha) \simeq \mathbb{C}$ . Esta es la manera algebraica elegante de construir  $\mathbb{C}$  a partir de  $\mathbb{R}$ .

## Ejercicios

---

**35.1** Para cada uno de los números dados  $\alpha \in \mathbb{C}$ , muéstrese que  $\alpha$  es algebraico sobre  $\mathbb{Q}$ , encontrando  $f(x) \in \mathbb{Q}[x]$  tal que  $f(\alpha) = 0$

- |                   |   |
|-------------------|---|
| a) $1 + \sqrt{2}$ | b) $\frac{\sqrt{2} + \sqrt{3}}{\sqrt{1 + \sqrt[3]{2}}}$ |
| c) $1 + i$        | d) $\sqrt[3]{2 - i}$                                    |

**35.2** Para cada uno de los números algebraicos dados  $\alpha \in \mathbb{C}$ , encuéntrense  $\text{irr}(\alpha, \mathbb{Q})$  y  $\text{grad}(\alpha, \mathbb{Q})$ . El lector debe estar preparado para demostrar que sus polinomios son irreducibles sobre  $\mathbb{Q}$  en caso de que alguien lo rete a hacerlo.

- a)  $\sqrt{3 - \sqrt{6}}$       b)  $\sqrt{\frac{1}{3}} + \sqrt{7}$       c)  $\sqrt{2} + i$

**35.3** Clasifíquese cada uno de los  $\alpha \in \mathbb{C}$  dados, como algebraicos o trascendentes sobre el campo  $F$  dado. Si  $\alpha$  es algebraico sobre  $F$ , encuéntrese  $\text{gra}(\alpha, F)$ .

- |   |  |
|---|--|
| a) $\alpha = i, F = \mathbb{Q}$               | b) $\alpha = 1 + i, F = \mathbb{R}$        |
| c) $\alpha = \sqrt{\pi}, F = \mathbb{Q}$      | d) $\alpha = \sqrt{\pi}, F = \mathbb{R}$   |
| e) $\alpha = \sqrt{\pi}, F = \mathbb{Q}(\pi)$ | f) $\alpha = \pi^2, F = \mathbb{Q}$        |
| g) $\alpha = \pi^2, F = \mathbb{Q}(\pi)$      | h) $\alpha = \pi^2, F = \mathbb{Q}(\pi^3)$ |

**35.4** Remítase al ejemplo 35.9 del libro. El polinomio  $x^2 + x + 1$  tiene un cero  $\alpha$  en  $\mathbb{Z}_2(\alpha)$  y, por tanto, debe factorizarse en un producto de factores lineales en  $(\mathbb{Z}_2(\alpha))[x]$ . Encuéntrese esta factorización. [Sugerencia: divídase  $x^2 + x + 1$  entre  $x - \alpha$  y úsese el hecho de que  $\alpha^2 = \alpha + 1$ .]

**35.5** Sea  $E$  un campo de extensión de  $F$  y sean  $\alpha, \beta \in E$ . Supóngase que  $\alpha$  es trascendente sobre  $F$ , pero algebraico sobre  $F(\beta)$ . Muéstrese que  $\beta$  es algebraico sobre  $F(\alpha)$ .

**35.6** Sea  $E$  un campo de extensión de un campo finito  $F$ , donde  $F$  tiene  $q$  elementos. Sea  $\alpha \in E$  algebraico sobre  $F$  de grado  $n$ . Pruébese que  $F(\alpha)$  tiene  $q^n$  elementos.

- 35.7** a) Muéstrese que el polinomio  $x^2 + 1$  es irreducible en  $\mathbb{Z}_3[x]$ .  
 b) Sea  $\alpha$  un cero de  $x^2 + 1$  en un campo de extensión de  $\mathbb{Z}_3$ . Como en el ejemplo 35.9, elabórense las tablas de suma y multiplicación para los nueve elementos de  $\mathbb{Z}_3(\alpha)$  escritos en el orden  $0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha$  y  $2 + 2\alpha$ .

## 35.8 ¿Falso o verdadero?

- a) El número  $\pi$  es trascendente sobre  $\mathbb{Q}$ .
  - b)  $\mathbb{C}$  es una extensión simple de  $\mathbb{R}$ .
  - c) Todo elemento de un campo  $F$  es algebraico sobre  $F$ .
  - d)  $\mathbb{R}$  es un campo de extensión de  $\mathbb{Q}$ .
  - e)  $\mathbb{Q}$  es un campo de extensión de  $\mathbb{Z}_2$ .
  - f) Sea  $\alpha \in \mathbb{C}$  algebraico sobre  $\mathbb{Q}$  de grado  $n$ . Si  $f(\alpha) = 0$  para  $f(x) \in \mathbb{Q}[x]$  distinto de cero, entonces (grado de  $f(x)$ )  $\geq n$ .
  - g) Sea  $\alpha \in \mathbb{C}$  algebraico sobre  $\mathbb{Q}$  de grado  $n$ . Si  $f(\alpha) = 0$  para  $f(x) \in \mathbb{R}[x]$  distinto de cero, entonces (grado de  $f(x)$ )  $\geq n$ .
  - h) Todo polinomio no constante en  $F[x]$  tiene algún cero en algún campo de extensión de  $F$ .
  - i) Todo polinomio no constante en  $F[x]$  tiene algún cero en todo campo de extensión de  $F$ .
  - j) Si  $x$  es una indeterminada,  $\mathbb{Q}[\pi] \simeq \mathbb{Q}[x]$ .
- 

35.9 Sea  $E$  un campo de extensión de un campo  $F$  y sea  $\alpha \in E$  algebraico sobre  $F$ . El polinomio  $\text{irr}(\alpha, F)$  se denomina a veces el *polinomio minimal para  $\alpha$  sobre  $F$* . ¿Por qué es apropiada esta denominación?

- 35.10 a) Muéstrese que existe un polinomio irreducible de grado 3 en  $\mathbb{Z}_3[x]$ .  
 b) Muéstrese, de a), que existe un campo finito de veintisiete elementos. [Sugerencia: úsese el ejercicio 35.6.]

35.11 Considérese el campo primo  $\mathbb{Z}_p$  de característica  $p \neq 0$ .

- a) Muéstrese que para  $p \neq 2$ , no todo elemento en  $\mathbb{Z}_p$  es cuadrado de algún elemento de  $\mathbb{Z}_p$  [Sugerencia:  $1^2 = (p - 1)^2 = 1$  en  $\mathbb{Z}_p$ . Dedúzcase, *contando*, la conclusión deseada.]
- b) Usese la parte a) para mostrar que existen campos finitos de  $p^2$  elementos para todo primo  $p$  en  $\mathbb{Z}^+$ .

35.12 Hemos afirmado, sin demostrarlo, que  $\pi$  y  $e$  son trascendentes sobre  $\mathbb{Q}$ .

- a) Encuéntrese un subcampo  $F$  de  $\mathbb{R}$  tal que  $\pi$  sea algebraico de grado 3 sobre  $F$ .
- b) Encuéntrese un subcampo  $E$  de  $\mathbb{R}$  tal que  $e^2$  sea algebraico de grado 5 sobre  $E$ .

35.13 Sea  $E$  un campo de extensión de un campo  $F$  y sea  $\alpha \in E$  trascendente sobre  $F$ . Muéstrese que todo elemento de  $F(\alpha)$  que no esté en  $F$  también es trascendente sobre  $F$ .

35.14 a) Muéstrese que  $x^3 + x^2 + 1$  es irreducible sobre  $\mathbb{Z}_2$ .

- b) Sea  $\alpha$  un cero de  $x^3 + x^2 + 1$  en un campo de extensión de  $\mathbb{Z}_2$ . Muéstrese que  $x^3 + x^2 + 1$  se factoriza en tres factores lineales en  $(\mathbb{Z}_2(\alpha))[x]$  encontrando esta factorización. [Sugerencia: todo elemento de  $\mathbb{Z}_2(\alpha)$  es de la forma

$$a_0 + a_1\alpha + a_2\alpha^2 \quad \text{para } a_i = 0, 1.$$

Dividase  $x^3 + x^2 + 1$  entre  $x - \alpha$ . Muéstrese que el cociente también tiene un cero en  $\mathbb{Z}_2(\alpha)$ , simplemente probando los ocho elementos posibles. Después, complétense la factorización.]

- 35.15 Muéstrese que  $\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$  es un subcampo de  $\mathbb{R}$ , usando las ideas de esta sección, en lugar de una verificación formal de los axiomas de campo. [Sugerencia: úsese el teorema 35.4.]

**35.16** Sea  $E$  un campo de extensión de  $\mathbb{Z}_2$  y sea  $\alpha \in E$  algebraico de grado 3 sobre  $\mathbb{Z}_2$ . Clasifiquense los grupos  $\langle \mathbb{Z}_2(\alpha), + \rangle$  y  $\langle (\mathbb{Z}_2(\alpha))^*, \cdot \rangle$  de acuerdo con el teorema fundamental de los grupos abelianos finitamente generados. Como siempre,  $(\mathbb{Z}_2(\alpha))^*$  es el conjunto de los elementos distintos de cero en  $\mathbb{Z}_2(\alpha)$ .

**35.17** Siguiendo la idea del ejercicio 35.10, muéstrese que existe un campo de ocho elementos; de dieciséis elementos; de veinticinco elementos.

**35.18** Sea  $F$  un campo finito de característica  $p$ . Muéstrese que todo elemento de  $F$  es algebraico sobre el campo primo  $\mathbb{Z}_p \leq F$ . [Sugerencia: sea  $F^*$  el conjunto de los elementos de  $F$  distintos de cero. Aplíquese teoría de grupos al grupo  $\langle F^*, \cdot \rangle$  para mostrar que todo  $\alpha \in F^*$  es cero de algún polinomio en  $\mathbb{Z}_p[x]$  de la forma  $x^n - 1$ .]

**35.19** Usense los ejercicios 35.6 y 35.18 para mostrar que todo campo finito es de orden la potencia de un primo, esto es, que su número de elementos es la potencia de un primo.

## 36

# Espacios vectoriales

## 36.1 DEFINICIÓN Y PROPIEDADES ELEMENTALES

El tema de espacios vectoriales es la piedra angular del álgebra lineal. Como el álgebra lineal no es el objeto de estudio de este libro, el tratamiento de los espacios vectoriales será breve, y está diseñado para desarrollar sólo los conceptos de independencia lineal y dimensión que necesitamos para nuestra teoría de campos.

Es probable que el lector ya conozca los términos de *vector* y *escalar* por algún curso de cálculo. Aquí permitiremos que los escalares sean elementos de cualquier campo, no sólo de los números reales, y desarrollamos la teoría a partir de axiomas, así como lo hemos hecho para las otras estructuras algebraicas estudiadas. Las propiedades que aparecen en estos axiomas deben resultar conocidas para el lector.

**Definición** Sea  $F$  un campo. Un *espacio vectorial sobre  $F$*  (o  *$F$ -espacio vectorial*) consta de un grupo abeliano  $V$  bajo la suma, junto con una operación de multiplicación por un escalar por la izquierda, de cada elemento de  $V$  por cada elemento de  $F$ , tal que para todas las  $a, b \in F$  y  $\alpha, \beta \in V$  se satisfacen las siguientes condiciones:

- $\checkmark_1 \quad a\alpha \in V.$
- $\checkmark_2 \quad a(b\alpha) = (ab)\alpha.$
- $\checkmark_3 \quad (a + b)\alpha = (a\alpha) + (b\alpha).$
- $\checkmark_4 \quad a(\alpha + \beta) = (a\alpha) + (a\beta).$
- $\checkmark_5 \quad 1\alpha = \alpha.$

Los elementos de  $V$  son *vectores* y los elementos de  $F$  son *escalares*. Cuando sólo hay un campo  $F$  en la discusión, omitimos la referencia a  $F$  y nos referimos a un *espacio vectorial*.

Nótese que la multiplicación para un espacio vectorial no es una operación binaria en un conjunto, en el sentido en que la definimos en el capítulo 1. Más bien, es una regla que asigna un elemento  $a\alpha$  de  $V$  a cada par ordenado  $(a, \alpha)$  que consta de un elemento  $a$  de  $F$  y un elemento  $\alpha$  de  $V$ . Se puede considerar como una *función* que transforma  $F \times V$  en  $V$ . La *buenas* manera de definir una operación binaria en un conjunto  $S$ , es análoga a decir que es una función de  $S \times S$  en  $S$ , pero en el capítulo 1 quisimos ser más intuitivos. Tanto la identidad aditiva de  $V$ , el 0-vector como la identidad aditiva en  $F$ , el 0-escalar, se denotarán por 0.

**Ejemplo 36.1** Considérese el grupo abeliano  $\langle \mathbb{R}^n, + \rangle = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$  con  $n$  factores, que consta de las  $n$ -adas ordenadas bajo la suma por componentes. Definase la multiplicación por un escalar para escalares en  $\mathbb{R}$  como

$$r\alpha = (ra_1, \dots, ra_n)$$

para  $r \in \mathbb{R}$  y  $\alpha = (a_1, \dots, a_n) \in \mathbb{R}^n$ . Con estas operaciones  $\mathbb{R}^n$  es un espacio vectorial sobre  $\mathbb{R}$ . Los axiomas de espacio vectorial se verifican fácilmente. En particular, para  $n = 2$  no habrá dificultad para convencerse de que  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ , como espacio vectorial sobre  $\mathbb{R}$ , puede considerarse como todos los «vectores cuyos puntos iniciales están en el origen del plano euclíadiano» en el sentido en que con frecuencia se estudia en los cursos de cálculo. ■

**Ejemplo 36.2** Para cualquier campo  $F$ ,  $F[x]$  puede considerarse como un espacio vectorial sobre  $F$ , donde la suma de vectores es la suma ordinaria de polinomios en  $F[x]$  y la multiplicación por un escalar de un elemento de  $F[x]$  por un elemento de  $F$  es la multiplicación ordinaria en  $F[x]$ . Entonces, los axiomas del  $\mathcal{V}_1$  al  $\mathcal{V}_5$  de un espacio vectorial se deducen de inmediato de los axiomas del dominio entero  $F[x]$ . ■

**Ejemplo 36.3** Sea  $E$  un campo de extensión de un campo  $F$ . Entonces,  $E$  puede considerarse como un espacio vectorial sobre  $F$  donde la suma de vectores es la suma usual en  $E$  y la multiplicación por un escalar es la multiplicación usual de campo en  $E$  con  $a \in F$  y  $\alpha \in E$ . Los axiomas se siguen de inmediato de los axiomas de campo para  $E$ . Aquí, el campo de los escalares es, en realidad, un subconjunto de nuestro espacio de vectores. *Este es el ejemplo importante para nosotros.* ■

No suponemos nada acerca de espacios vectoriales y probaremos todo lo necesario a partir de la definición, aunque los resultados nos resulten familiares por los cursos de cálculo.

**Teorema 36.1** Si  $V$  es un espacio vectorial sobre  $F$ , entonces  $0\alpha = 0$ ,  $a0 = 0$  y  $(-a)\alpha = a(-\alpha) = -(a\alpha)$  para todas las  $a \in F$  y  $\alpha \in V$ .

*Demostración* La ecuación  $0\alpha = 0$  se lee «(0-escalar) $\alpha$  = 0-vector» y, de manera análoga,  $a0 = 0$  se lee « $a$ (0-vector) = 0-vector». Las demostraciones aquí, son muy similares a las del teorema 23.1 para un anillo y, de nuevo, dependen en gran medida de las leyes distributivas  $\mathcal{V}_3$  y  $\mathcal{V}_4$ . Ahora,

$$(0\alpha) = (0 + 0)\alpha = (0\alpha) + (0\alpha)$$

es una ecuación en el grupo abeliano  $\langle V, + \rangle$ , de modo que, por la ley de cancelación en el grupo,  $0 = 0\alpha$ . En forma análoga, de

$$a0 = a(0 + 0) = a0 + a0,$$

concluimos que  $a0 = 0$ . Entonces,

$$0 = 0\alpha = (a + (-a))\alpha = a\alpha + (-a)\alpha,$$

de modo que  $(-a)\alpha = -(a\alpha)$ . Del mismo modo, de

$$0 = a0 = a(\alpha + (-\alpha)) = a\alpha + a(-\alpha),$$

concluimos que, también,  $a(-\alpha) = -(a\alpha)$ . ■

## 36.2 INDEPENDENCIA LINEAL Y BASES

**Definición** Sea  $V$  un espacio vectorial sobre  $F$ . Los vectores en un subconjunto  $S = \{\alpha_i \mid i \in I\}$  de  $V$  **generan**  $V$ , si para toda  $\beta \in V$  tenemos

$$\beta = a_1\alpha_{i_1} + a_2\alpha_{i_2} + \cdots + a_n\alpha_{i_n}$$

para algunas  $a_j \in F$  y  $\alpha_{i_j} \in S$ ,  $j = 1, \dots, n$ . Un vector  $\sum_{j=1}^n a_j\alpha_{i_j}$  es una **combinación lineal de las**  $\alpha_{i_j}$ .

**Ejemplo 36.4** En el espacio vectorial  $\mathbf{R}^n$  sobre  $\mathbf{R}$  del ejemplo 36.1, los vectores

$$(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)$$

claramente generan  $\mathbf{R}^n$ , pues

$$(a_1, a_2, \dots, a_n) = a_1(1, 0, \dots, 0) + a_2(0, 1, \dots, 0) + \cdots + a_n(0, 0, \dots, 1).$$

Además, los monomios  $x^m$  para  $m \geq 0$  generan  $F[x]$  sobre  $F$ , el espacio vectorial del ejemplo 36.2. ■

**Ejemplo 36.5** Sea  $F$  un campo y  $E$  un campo de extensión de  $F$ . Sea  $\alpha \in E$  algebraico sobre  $F$ . Entonces,  $F(\alpha)$  es un espacio vectorial sobre  $F$  y, por el teorema 35.4, está generado por los vectores en  $\{1, \alpha, \dots, \alpha^{n-1}\}$  donde  $n = \text{grad}(\alpha, F)$ . *Este es el ejemplo importante para nosotros.* ■

**Definición** Un espacio vectorial  $V$  sobre un campo  $F$  es de **dimensión finita**, si existe algún subconjunto finito de  $V$  cuyos vectores generen  $V$ .

**Ejemplo 36.6** El ejemplo 36.4 muestra que  $\mathbf{R}^n$  es de dimensión finita. El espacio vectorial  $F[x]$  sobre  $F$  no es de dimensión finita, pues los polinomios de grado arbitrariamente grande, por supuesto, no pueden ser combinaciones lineales de elementos de cualquier conjunto *finito* de polinomios. ■

**Ejemplo 36.7** Si  $F \leq E$  y  $\alpha \in E$  es algebraico sobre el campo  $F$ , el ejemplo 36.5 muestra que  $F(\alpha)$  es un espacio vectorial sobre  $F$  de dimensión finita. *Este es el ejemplo más importante para nosotros.* ■

La siguiente definición contiene la idea más importante de esta sección.

**Definición** Los vectores en un subconjunto  $S = \{\alpha_i \mid i \in I\}$  de un espacio vectorial  $V$  sobre un campo  $F$  son **linealmente independientes sobre  $F$**  si  $\sum_{j=1}^n a_j \alpha_{i_j} = 0$  implica que  $a_j = 0$  para  $j = 1, \dots, n$ . Si los vectores no son linealmente independientes sobre  $F$ , son **linealmente dependientes sobre  $F$** .

Así, los vectores en  $\{\alpha_i \mid i \in I\}$  son linealmente independientes sobre  $F$ , si la única manera de que el 0-vector se pueda expresar como combinación lineal de los vectores  $\alpha_i$ , es tener todos los coeficientes escalares iguales a 0. Si los vectores son linealmente dependientes sobre  $F$ , entonces existen  $a_j \in F$  para  $j = 1, \dots, n$  tal que  $\sum_{j=1}^n a_j \alpha_{i_j} = 0$  donde no todos los  $a_j = 0$ .

**Ejemplo 36.8** Es claro que los vectores del conjunto de vectores que generan el espacio  $\mathbf{R}^n$  dados en el ejemplo 36.4 son linealmente independientes sobre  $\mathbf{R}$ . Así mismo, los vectores en  $\{x^m \mid m \geq 0\}$  son vectores linealmente independientes de  $F[x]$  sobre  $F$ . Nótese que  $(1, -1), (2, 1)$  y  $(-3, 2)$  son linealmente dependientes en  $\mathbf{R}^2$  sobre  $\mathbf{R}$ , pues

$$7(1, -1) + (2, 1) + 3(-3, 2) = (0, 0) = 0. \blacksquare$$

**Ejemplo 36.9** Sea  $E$  un campo de extensión de un campo  $F$  y sea  $\alpha \in E$  algebraico sobre  $F$ . Si  $\text{grad}(\alpha, F) = n$ , entonces, por el teorema 35.4, todo elemento de  $F(\alpha)$  puede expresarse *únicamente* en la forma

$$b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}$$

para  $b_i \in F$ . En particular,  $0 = 0 + 0\alpha + \cdots + 0\alpha^{n-1}$  debe ser la *única* de dichas expresiones para 0. Así, los elementos  $1, \alpha, \dots, \alpha^{n-1}$  son vectores linealmente

independientes en  $F(\alpha)$  sobre el campo  $F$ . Además, generan  $F(\alpha)$ , de modo que, por la definición siguiente,  $1, \alpha, \dots, \alpha^{n-1}$  forman una *base* para  $F(\alpha)$  sobre  $F$ . *Este es el ejemplo importante para nosotros.* De hecho, ésta es la razón por la cual estamos desarrollando este material acerca de espacios vectoriales. ■

**Definición** Si  $V$  es un espacio vectorial sobre un campo  $F$ , los vectores en un subconjunto  $B = \{\beta_i | i \in I\}$  de  $V$  forman una *base para V sobre F* si generan  $V$  y son linealmente independientes.

### 36.3 DIMENSION

Los demás resultados que deseamos probar acerca de espacios vectoriales son que todo espacio vectorial de dimensión finita tiene base y que dos bases de un espacio vectorial de dimensión finita tienen el mismo número de elementos. Estos dos hechos son ciertos, sin la hipótesis de que el espacio vectorial sea de dimensión finita, pero las demostraciones requieren mayor conocimiento de teoría de conjuntos del que estamos suponiendo y todo lo que necesitamos es el caso de dimensión finita. Daremos primero un lema sencillo.

**Lema 36.1** Sea  $V$  un espacio vectorial sobre un campo  $F$  y sea  $\alpha \in V$ . Si  $\alpha$  es combinación lineal de los vectores  $\beta_i$  para  $i = 1, \dots, m$  y cada  $\beta_i$  es combinación lineal de los vectores  $\gamma_j$  para  $j = 1, \dots, n$  entonces,  $\alpha$  es combinación lineal de las  $\gamma_j$ .

**Demostración** Sea  $\alpha = \sum_{i=1}^m a_i \beta_i$  y sea  $\beta_i = \sum_{j=1}^n b_{ij} \gamma_j$  donde  $a_i$  y  $b_{ij}$  están en  $F$ . Entonces,

$$\alpha = \sum_{i=1}^m a_i \left( \sum_{j=1}^n b_{ij} \gamma_j \right) = \left( \sum_{j=1}^n \sum_{i=1}^m a_i b_{ij} \gamma_j \right),$$

y  $(\sum_{i=1}^m a_i b_{ij}) \in F$ . ■

**Teorema 36.2** En un espacio vectorial de dimensión finita, todo conjunto finito de vectores que genere el espacio contiene un subconjunto que es una base.

**Demostración** Sea  $V$  de dimensión finita sobre  $F$  y sean  $\alpha_1, \dots, \alpha_n$  vectores en  $V$  que generan  $V$ . Listemos las  $\alpha_i$  una tras otra. Examíñese cada  $\alpha_i$  sucesivamente, comenzando por la izquierda con  $i = 1$  y descártense la primera  $\alpha_j$  que sea combinación lineal de las  $\alpha_i$  anteriores, para  $i < j$ . Continúese con la siguiente  $\alpha_{j+1}$  y descártense la siguiente  $\alpha_k$  que sea alguna combinación lineal de los restantes predecesores, y así sucesivamente. Llegaremos a  $\alpha_m$  después de un número finito de pasos, las  $\alpha_i$  que queden en nuestra lista son tales, que ninguna es combinación lineal de las  $\alpha_i$  anteriores en esta lista reducida. El lema 36.1

muestra que cualquier vector que sea combinación lineal de la colección original de las  $\alpha_i$  sigue siendo combinación lineal de nuestro conjunto reducido y quizás menor, en donde ninguna  $\alpha_i$  es combinación lineal de sus predecesores. Así, los vectores en el conjunto reducido de  $\alpha_i$  de nuevo generan  $V$ .

Supóngase que, para el conjunto reducido,

$$a_1\alpha_{i_1} + \cdots + a_r\alpha_{i_r} = 0$$

para  $i_1 < i_2 < \cdots < i_r$  y alguna  $a_j \neq 0$ . Podemos suponer, por el teorema 36.1, que  $a_r \neq 0$ , si no, podríamos quitar  $a_r\alpha_{i_r}$  del lado izquierdo de la ecuación. Entonces, usando de nuevo el teorema 36.1, obtenemos

$$\alpha_{i_r} = \left(-\frac{a_1}{a_r}\right)\alpha_{i_1} + \cdots + \left(-\frac{a_{r-1}}{a_r}\right)\alpha_{i_{r-1}},$$

lo cual muestra que  $\alpha_{i_r}$  es una combinación lineal de sus predecesores, y esto contradice nuestra construcción. Así, los vectores  $\alpha_i$  en el conjunto reducido, generan  $V$  y son linealmente independientes, de modo que forman una base para  $V$  sobre  $F$ . ■

**Corolario** *Un espacio vectorial de dimensión finita tiene una base finita.*

**Demostración** Por definición, un espacio vectorial de dimensión finita tiene un conjunto finito de vectores que generan el espacio. El teorema 36.2 completa la demostración. ■

El siguiente teorema culmina nuestro trabajo con espacios vectoriales.

**Teorema 36.3** *Sea  $S = \{\alpha_1, \dots, \alpha_r\}$  un conjunto finito de vectores linealmente independientes de un espacio vectorial  $V$  de dimensión finita, sobre un campo  $F$ . Entonces,  $S$  puede extenderse a una base de  $V$  sobre  $F$ . Aún más, si  $B = \{\beta_1, \dots, \beta_n\}$  es cualquier base de  $V$  sobre  $F$ , entonces  $r \leq n$ .*

**Demostración** Por el corolario del teorema 36.2, existe una base  $B = \{\beta_1, \dots, \beta_n\}$  de  $V$  sobre  $F$ . Considérese la sucesión finita de vectores

$$\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_n.$$

Estos vectores generan  $V$ , pues  $B$  es una base. Siguiendo la técnica usada en el teorema 36.2 de ir descartando cada vector que sea una combinación lineal de sus predecesores restantes, trabajando de izquierda a derecha, llegamos a una base para  $V$ . Es claro que ninguna  $\alpha_i$  se descarta, pues las  $\alpha_i$  son linealmente independientes. Así,  $S$  se puede extender a una base de  $V$  sobre  $F$ .

Para la segunda parte de la conclusión, considérese la sucesión

$$\alpha_1, \beta_1, \dots, \beta_n.$$

Estos vectores no son linealmente independientes, pues  $\alpha_1$  es una combinación lineal

$$\alpha_1 = b_1\beta_1 + \cdots + b_n\beta_n.$$

pues las  $\beta_i$  forman una base. Así,

$$\alpha_1 + (-b_1)\beta_1 + \cdots + (-b_n)\beta_n = 0.$$

Los vectores en la sucesión sí generan  $V$ , y si formamos una base mediante la técnica de trabajar de izquierda a derecha descartando cada vector que sea combinación lineal de sus predecesores restantes, deberá sacarse al menor una  $\beta_i$  dando la base

$$\{\alpha_1, \beta_1^{(1)}, \dots, \beta_m^{(1)}\},$$

donde  $m \leq n - 1$ . Al aplicar la misma técnica a la sucesión de vectores

$$\alpha_1, \alpha_2, \beta_1^{(1)}, \dots, \beta_m^{(1)},$$

llegamos a una nueva base

$$\{\alpha_1, \alpha_2, \beta_1^{(2)}, \dots, \beta_s^{(2)}\},$$

con  $s \leq n - 2$ . Continuando, llegamos por último a una base

$$\{\alpha_1, \dots, \alpha_r, \beta_1^{(r)}, \dots, \beta_t^{(r)}\},$$

donde  $0 \leq t \leq n - r$ . Así,  $r \leq n$ . ■

**Corolario** *Cualesquiera dos bases de un espacio vectorial de dimensión finita  $V$  sobre  $F$  tienen el mismo número de elementos.*

**Demostración** Sean  $B = \{\beta_1, \dots, \beta_n\}$  y  $B' = \{\beta'_1, \dots, \beta'_m\}$  dos bases. Entonces, por el teorema 36.3, considerando  $B$  como un conjunto independiente de vectores y  $B'$  como base, vemos que  $n \leq m$ . Un argumento simétrico da que  $m \leq n$ , de modo que  $m = n$ . ■

**Definición** Si  $V$  es un espacio vectorial de dimensión finita sobre un campo  $F$ , el número de elementos en una base (por teorema 36.3, es independiente de la selección de la base) es la *dimensión de  $V$  sobre  $F$* .

**Ejemplo 36.10** Sea  $E$  un campo de extensión de un campo  $F$ , y sea  $\alpha \in E$ . El ejemplo 36.9 muestra que si  $\alpha$  es algebraico sobre  $F$  y  $\text{grad}(\alpha, F) = n$ , entonces la dimensión de  $F[\alpha]$ , como espacio vectorial sobre  $F$ , es  $n$ . *Este es el ejemplo importante para nosotros.* ■

## 36.4 UNA APLICACION A LA TEORIA DE CAMPOS

Reunamos los resultados de teoría de los campos contenidos en los ejemplos 36.3, 36.5, 36.7, 36.9 y 36.10 e incorporémoslos en un teorema. La última frase de este teorema da una elegante aplicación adicional de estas ideas de espacios vectoriales a la teoría de campos.

**Teorema 36.4** *Sea  $E$  un campo de extensión de  $F$  y sea  $\alpha \in E$  algebraico sobre  $F$ . Si  $\text{grad}(\alpha, F) = n$ , entonces  $F(\alpha)$  es un espacio vectorial  $n$ -dimensional sobre  $F$  con base  $\{1, \alpha, \dots, \alpha^{n-1}\}$ . Más aún, todo elemento  $\beta$  de  $F(\alpha)$  es algebraico sobre  $F$  y  $\text{grad}(\beta, F) \leq \text{grad}(\alpha, F)$ .*

**Demostración** En los ejemplos anteriores ya mostramos todo, excepto el *resultado muy importante* enunciado en la última frase del teorema anterior. Sea  $\beta \in F(\alpha)$  donde  $\alpha$  es algebraico sobre  $F$  de grado  $n$ . Considérense los elementos

$$1, \beta, \beta^2, \dots, \beta^n.$$

Estos no pueden ser  $n + 1$  elementos distintos de  $F(\alpha)$  que sean linealmente independientes sobre  $F$  pues, por el teorema 36.3, cualquier base de  $F(\alpha)$  sobre  $F$ , contendría al menos tantos elementos como hubiera en cualquier conjunto de vectores linealmente independientes sobre  $F$ . Sin embargo, la base  $\{1, \alpha, \dots, \alpha^{n-1}\}$  tiene sólo  $n$  elementos. Si  $\beta^i = \beta^j$ , entonces  $\beta^i - \beta^j = 0$  luego, en todo caso, existe  $b_i \in F$  tal que

$$b_0 + b_1\beta + b_2\beta^2 + \dots + b_n\beta^n = 0,$$

donde no todas las  $b_i = 0$ . Entonces,  $f(x) = b_nx^n + \dots + b_1x + b_0$  es un elemento distinto de cero de  $F[x]$ , tal que  $f(\beta) = 0$ . Por tanto,  $\beta$  es algebraico sobre  $F$  y  $\text{grad}(\beta, F)$  es a lo más  $n$ . ■

### Ejercicios

**36.1** Encuéntrense tres bases para  $\mathbb{R}^2$  sobre  $\mathbb{R}$  donde no haya dos que tengan algún vector en común.

**36.2** Determíñese cuáles de los conjuntos dados de vectores son una base de  $\mathbb{R}^3$  sobre  $\mathbb{R}$ .

- a)  $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$
- b)  $\{(-1, 1, 2), (2, -3, 1), (10, -14, 0)\}$

**36.3** De acuerdo con el teorema 36.4 el elemento  $1 + \alpha$  de  $\mathbb{Z}_2(\alpha)$  del ejemplo 35.9 es algebraico sobre  $\mathbb{Z}_2$ . Encuéntrese el polinomio irreducible para  $1 + \alpha$  en  $\mathbb{Z}_2[x]$ .

**36.4** Obténgase una base para cada uno de los siguientes espacios vectoriales sobre los campos indicados.

- |   |  |
|---|--|
| a) $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$    | b) $\mathbb{R}(\sqrt{2})$ sobre $\mathbb{R}$             |
| c) $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$ | d) $\mathbb{C}$ sobre $\mathbb{R}$                       |
| e) $\mathbb{Q}(i)$ sobre $\mathbb{Q}$           | $\mathbb{R}(\sqrt{2})$ sobre $\mathbb{R}$ o $\mathbb{Q}$ |

**†36.5** Pruébese que si  $V$  es un espacio vectorial de dimensión finita, sobre un campo  $F$ , entonces un subconjunto  $\{\beta_i\}$  de  $V$  es una base para  $V$  sobre  $F$  si y sólo si todo vector en  $V$  puede expresarse de manera única como combinación lineal de los  $\beta_i$ .

**36.6** ¿Falso o verdadero?

- a) La suma de dos vectores es un vector.
  - b) La suma de dos escalares es un vector.
  - c) El producto de dos escalares es un escalar.
  - d) El producto de un escalar y un vector es un vector.
  - e) Todo espacio vectorial tiene base finita.
  - f) Los vectores en una base son linealmente dependientes.
  - g) El 0-vector puede ser parte de una base.
  - h) Si  $F \leq E$  y  $\alpha \in E$  es algebraico sobre el campo  $F$ , entonces  $\alpha^2$  es algebraico sobre  $F$ .
  - i) Si  $F \leq E$  y  $\alpha \in E$  es algebraico sobre el campo  $F$ , entonces  $\alpha + \alpha^2$  es algebraico sobre  $F$ .
  - j) Todo espacio vectorial tiene una base.
- 

*Los ejercicios que siguen se refieren al estudio ulterior de los espacios vectoriales. En muchos casos, se pide definir para espacios vectoriales algún concepto análogo a otro que ya estudiamos para otras estructuras algebraicas. Estos ejercicios mejorarán su habilidad para reconocer situaciones paralelas y relacionadas en álgebra. Los ejercicios pueden suponer el conocimiento de conceptos definidos en ejercicios anteriores.*

**36.7** Sea  $V$  un espacio vectorial sobre un campo  $F$ .

- a) Definase un *subespacio del espacio vectorial  $V$  sobre  $F$* .
- b) Pruébese que la intersección de subespacios de  $V$  es, de nuevo, un subespacio de  $V$  sobre  $F$ .

**36.8** Sea  $V$  un espacio vectorial sobre un campo  $F$  y sea  $S = \{\alpha_i \mid i \in I\}$  una colección de vectores en  $V$ .

- a) Usese el ejercicio 36.7 b) para definir el *subespacio de  $V$  generado por  $S$* .
- b) Pruébese que los vectores en el subespacio de  $V$  generado por  $S$  son, precisamente, las combinaciones lineales (finitas) de vectores en  $S$ . (Compárese con el teorema 9.1.)

**36.9** Sean  $V_1, \dots, V_n$  espacios vectoriales sobre el mismo campo  $F$ . Definase la *suma directa  $V_1 \oplus \dots \oplus V_n$  de los espacios vectoriales  $V_i$*  para  $i = 1, \dots, n$  y muéstrese que la suma directa es, de nuevo un espacio vectorial sobre  $F$ .

**36.10** Generalícese el ejemplo 36.1 para obtener el espacio vectorial  $F^n$  de  $n$ -adas ordenadas de elementos de  $F$  sobre el campo  $F$  para cualquier campo  $F$ . ¿Cuál es una base para  $F^n$ ?

36.11 Sea  $F$  cualquier campo. Considérese el «sistema de  $m$  ecuaciones lineales simultáneas en  $n$  incógnitas»

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n &= b_1, \\ a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n &= b_2, \\ \vdots & \\ a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n &= b_m, \end{aligned}$$

donde  $a_{ij}, b_i \in F$ .

- a) Muéstrese que el «sistema tiene solución» si y sólo si el vector  $\beta = (b_1, \dots, b_m)$  de  $F^m$  está en el subespacio de  $F^m$  generado por los vectores  $\alpha_j = (a_{1j}, \dots, a_{mj})$ . (Este resultado es trivial de demostrar, prácticamente es la definición de solución, pero, en realidad, debe contemplarse como el *teorema fundamental de la existencia de una solución simultánea de un sistema de ecuaciones lineales*.)
- b) De a) muéstrese que si  $n = m$  y  $\{\alpha_j | j = 1, \dots, n\}$  es una base para  $F^n$ , entonces el sistema siempre tiene solución única.

36.12 Definase un *isomorfismo de un espacio vectorial  $V$  sobre un campo  $F$  con un espacio vectorial  $V'$  sobre el mismo campo  $F$* .

36.13 Pruébese que todo espacio vectorial  $V$  de dimensión finita,  $n$ , sobre un campo  $F$  es isomorfo al espacio vectorial  $F^n$  del ejercicio 36.10.

36.14 Sean  $V$  y  $V'$  espacios vectoriales sobre el mismo campo  $F$ . Una función  $\phi : V \rightarrow V'$  es una *transformación lineal de  $V$  en  $V'$*  si se cumplen las siguientes condiciones para todas las  $\alpha, \beta \in V$  y  $a \in F$ :

$$\begin{aligned} (\alpha + \beta)\phi &= \alpha\phi + \beta\phi, \\ (a\alpha)\phi &= a(\alpha\phi). \end{aligned}$$

- a) Si  $\{\beta_i | i \in I\}$  es una base para  $V'$  sobre  $F$ , muéstrese que una transformación lineal  $\phi : V \rightarrow V'$  está por completo determinada por los vectores  $\beta_i\phi \in V'$ .
- b) Sea  $\{\beta_i | i \in I\}$  una base para  $V$  y sea  $\{\beta'_i | i \in I\}$  cualquier conjunto de vectores, no por fuerza distintos, de  $V'$ . Muéstrese que existe precisamente una transformación lineal  $\phi : V \rightarrow V'$  tal que  $\beta_i\phi = \beta'_i$ .

36.15 Sean  $V$  y  $V'$  espacios vectoriales sobre el mismo campo  $F$  y sea  $\phi : V \rightarrow V'$  una transformación lineal.

- a) ¿A cuál concepto que ya estudiamos para estructuras de grupos y anillos, corresponde el concepto de *transformación lineal*?
- b) Definase el *kernel* (o *espacio nulo*) de  $\phi$  y muéstrese que es un subespacio de  $V$ .
- c) Describase cuándo  $\phi$  es un isomorfismo de  $V$  en  $V'$ .

36.16 Sea  $V$  un espacio vectorial sobre un campo  $F$  y sea  $S$  un subespacio de  $V$ . Definase el *espacio cociente  $V/S$*  y demuéstrese que es un espacio vectorial sobre  $F$ .

36.17 Sean  $V$  y  $V'$  espacios vectoriales sobre el mismo campo  $F$  y sea  $V$  de dimensión finita sobre  $F$ . Sea  $\dim(V)$  la dimensión del espacio vectorial  $V$  sobre  $F$ . Sea  $\phi : V \rightarrow V'$  una transformación lineal.

- a) Muéstrese que  $V\phi$  es un subespacio de  $V'$ .
- b) Muéstrese que  $\dim(V\phi) = \dim(V) - \dim(\text{kernel } \phi)$ . [Sugerencia: elíjase una base conveniente para  $V$ , usando el teorema 36.3. Por ejemplo, extiéndase una base para  $(\text{kernel } \phi)$  a una base para  $V$ .]

\*36.18 Sean  $S$  y  $T$  subespacios de un espacio vectorial  $V$  sobre un campo  $F$ .

- Definase el *ensamblaje*  $S \vee T$  de  $S$  y  $T$  y muéstrese que  $S \vee T$  también es un subespacio de  $V$  sobre  $F$ . (Compárese con la sección 8.2. En la literatura, se denota  $S \vee T$  por  $S + T$ .)
- Describanse los elementos en  $S \vee T$  en términos de los de  $S$  y los de  $T$ .

\*36.19 Sea  $V$  un espacio vectorial de dimensión finita sobre un campo  $F$  y sea  $\dim(V)$  la dimensión de  $V$  sobre  $F$ . Muéstrese que si  $S$  y  $T$  son subespacios de  $V$  sobre  $F$ , entonces,

$$\dim(S \vee T) = \dim(S) + \dim(T) - \dim(S \cap T).$$

[*Sugerencia:* la dimensión de un espacio es el número de elementos en una base. Usese el teorema 36.3 para escoger bases convenientes, de modo que la demostración sea fácil. Primero elijase cualquier base  $\{\alpha_i\}$  para  $S \cap T$  y después, extiéndase con vectores  $\beta_j$  de modo que  $\{\alpha_i, \beta_j\}$  sea una base para  $S$ . Repítase el proceso de modo que  $\{\alpha_i, \beta_j, \gamma_k\}$  sea una base para  $T$ . Muéstrese que  $\{\alpha_i, \beta_j, \gamma_k\}$  es una base para  $S \vee T$ .]

## Otras estructuras algebraicas

Esta es una sección destinada a dar una idea de algunas otras estructuras algebraicas importantes y su relación con las estructuras estudiadas.

### \*37.1 GRUPOS CON OPERADORES

**Definición** Un *grupo con operadores* consta de un grupo  $G$  y un conjunto  $\mathcal{O}$ , el *conjunto de operadores*, junto con una operación de multiplicación externa de cada elemento de  $G$  por cada elemento de  $\mathcal{O}$  por la derecha, tal que para todas las  $\alpha, \beta \in G$  y  $a \in \mathcal{O}$  se satisfacen las condiciones siguientes:

- 1  $(\alpha a) \in G$ .
- 2  $(\alpha\beta)a = (\alpha a)(\beta a)$ .

Hablaremos, de manera algo incorrecta, del  *$\mathcal{O}$ -grupo  $G$* .

Nótese que hemos seguido de cerca la forma en que definimos un espacio vectorial en el capítulo 36. La operación de multiplicación externa es, en realidad, una función  $\phi: G \times \mathcal{O} \rightarrow G$  donde  $(\alpha, a)\phi$  se denota por  $\alpha a$  para  $\alpha \in G$  y  $a \in \mathcal{O}$ . Es claro que escribir el operador  $a$  a la derecha de  $\alpha$ , como lo hicimos aquí, o a la izquierda, es cuestión de gusto y de conveniencia.

Aunque en la definición no requerimos ninguna estructura para el conjunto  $\mathcal{O}$ , sucede con frecuencia que  $\mathcal{O}$  tiene alguna estructura algebraica natural. Demos algunos ejemplos.

**Ejemplo 37.1** Todo grupo abeliano  $G$  da lugar a un grupo natural con operadores. Escribamos de manera multiplicativa la operación de grupo de  $G$ . Sea  $\mathcal{O} = \mathbb{Z}$ , para  $\alpha \in G$  y  $n \in \mathbb{Z}$ , definase  $\alpha n = \alpha^n$ . Como  $G$  es abeliano, tenemos

$$(\alpha\beta)n = (\alpha\beta)^n = \alpha^n\beta^n = (\alpha n)(\beta n).$$

Así, todo grupo abeliano se puede considerar como un  $\mathbb{Z}$ -grupo. Aquí,  $\mathbb{Z}$  tiene una estructura natural de anillo. ■

**Ejemplo 37.2** Si  $V$  es un espacio vectorial sobre un campo  $F$ ,  $V$  se puede considerar, de manera natural, como un  $F$ -grupo (izquierdo). Aquí,  $F$  tiene una estructura de campo. ■

Considérese un  $\mathcal{O}$ -grupo  $G$ . Para  $a \in \mathcal{O}$  fija, la transformación  $\rho_a: G \rightarrow G$  definida por  $\alpha\rho_a = \alpha a$  para  $\alpha \in G$  es un homomorfismo de  $G$  en  $G$  puesto que  $(\alpha\beta)a = (\alpha a)(\beta a)$ . Esto sugiere el siguiente ejemplo.

**Ejemplo 37.3** Sea  $G$  cualquier grupo y sea  $\mathcal{O}$  cualquier conjunto de homomorfismos de  $G$  en él mismo (dichos homomorfismos son *endomorfismos* de  $G$ ). Para  $\alpha, \beta \in G$  y  $\phi \in \mathcal{O}$ , la propiedad  $(\alpha\beta)\phi = (\alpha\phi)(\beta\phi)$  para el endomorfismo  $\phi$ , muestra que podemos contemplar  $G$  de manera natural como un  $\mathcal{O}$ -grupo. ■

Una parte sustancial de nuestra teoría de grupos abelianos podría haberse aplicado a  $\mathcal{O}$ -grupos. Comenzando con los subgrupos, un **subgrupo admisible**, o un  **$\mathcal{O}$ -subgrupo** de un  $\mathcal{O}$ -grupo  $G$  es un subgrupo  $H$  de  $\langle G, \cdot \rangle$  tal que  $\alpha a \in H$  para todas las  $\alpha \in H$  y  $a \in \mathcal{O}$ , esto es, dicho  $H$  es cerrado bajo la multiplicación externa por elementos de  $\mathcal{O}$ . Si se trabaja constantemente con  $\mathcal{O}$ -grupos, tan sólo se omite el término *admissible* y se habla de un subgrupo del  $\mathcal{O}$ -grupo  $G$ , sobreentendiendo que se trata de un  $\mathcal{O}$ -subgrupo. Un par de ejemplos más, mostrarán la elegancia con que estas ideas se relacionan con nuestro trabajo anterior.

**Ejemplo 37.4** Sea  $G$  cualquier grupo y sea  $\mathcal{I}$  el conjunto de todos los automorfismos internos de  $G$ . Como en el ejemplo 37.3,  $G$  es un  $\mathcal{I}$ -grupo de manera natural. Un subgrupo (admisible)  $H$  de  $G$  debe tener, entonces la propiedad de que  $ai_g = g^{-1}ag$  está en  $H$  para todas las  $a \in H$  y todas las  $g \in G$ . Así, los  $\mathcal{I}$ -subgrupos  $H$  del  $\mathcal{I}$ -grupo  $G$  son esencialmente los subgrupos normales de  $G$ . ■

**Ejemplo 37.5** Sea  $R$  un anillo. El grupo aditivo  $\langle R, + \rangle$  de  $R$  puede considerarse como un  $R$ -grupo donde para un elemento  $a$  del grupo  $\langle R, + \rangle$  y  $r \in R$ , se define  $ar$  mediante la multiplicación en el anillo. La ley distributiva derecha en  $R$  da  $(a + b)r = (ar) + (br)$  lo cual es precisamente la condición para que  $\langle R, + \rangle$  sea un  $R$ -grupo. Un  $R$ -subgrupo  $N$  del  $R$ -grupo  $\langle R, + \rangle$  debe ser, entonces, un subgrupo de  $\langle R, + \rangle$  que satisfaga  $ar \in N$  para todas las  $a \in N$  y  $r \in R$ . Así, los  $R$ -subgrupos son esencialmente los ideales derechos de  $R$ . Si  $R$  es un anillo commutativo, entonces los  $R$ -subgrupos son esencialmente los ideales de  $R$ . ■

Podemos formar el grupo factor de un  $\mathcal{C}$ -grupo  $G$  módulo en  $\mathcal{C}$ -subgrupo normal; el grupo factor se vuelve  $\mathcal{C}$ -grupo de manera natural, cuando definimos la multiplicación externa en las clases laterales, usando representantes. Tenemos el concepto de  $\mathcal{C}$ -homomorfismo de un  $\mathcal{C}$ -grupo en otro. En los ejercicios pediremos definiciones apropiadas para estas ideas.

Por último, enunciamos sin demostración el teorema de Jordan-Hölder para un  $\mathcal{C}$ -grupo. Las definiciones de serie subnormal y series de composición son análogas a las definiciones en la parte I; sólo se requiere que todo subgrupo sea un  $\mathcal{C}$ -subgrupo.

**Teorema 37.1 (Jordan-Hölder)** *Cualesquiera dos series de composición de un  $\mathcal{C}$ -grupo  $G$  son isomorfas.*

Tomando  $\mathcal{C} = \{i\}$ , donde  $i$  es la transformación idéntica de un grupo  $G$  sobre sí mismo, recobramos el teorema de Jordan-Hölder para series de composición. Tomando  $\mathcal{C} = \mathcal{I}$ , el conjunto de automorfismos internos de  $G$ , recobramos el teorema de Jordan-Hölder del capítulo 14 para series principales. Por último, y de manera más impresionante, tomando el teorema de Jordan-Hölder para el  $F$ -grupo  $V$  donde  $V$  es un espacio vectorial de dimensión finita, sobre  $F$ , recobramos la invariancia de la dimensión de  $V$ , pues un  $F$ -grupo factor simple del  $F$ -grupo  $V$  será un espacio vectorial (un  $F$ -grupo) de dimensión 1 sobre  $F$ .

## \*37.2 MODULOS

**Definición** Sea  $R$  un anillo. Un  **$R$ -módulo (izquierdo)** consta de un grupo abeliano  $M$  junto con una operación de multiplicación externa de cada elemento de  $M$  por cada elemento de  $R$  por la izquierda, tal que para todas las  $\alpha, \beta \in M$  y  $r, s \in R$  se satisfacen las condiciones siguientes:

- 1  $(r\alpha) \in M$ .
- 2  $r(\alpha + \beta) = r\alpha + r\beta$ .
- 3  $(r + s)\alpha = r\alpha + s\alpha$ .
- 4  $(rs)\alpha = r(s\alpha)$ .

Hablaremos, de manera algo incorrecta, del  **$R$ -módulo  $M$** .

Un  $R$ -módulo se parece mucho a un espacio vectorial, pero los escalares sólo necesitan formar un anillo. Si  $R$  es un anillo con unitario y  $1\alpha = \alpha$  para toda  $\alpha \in M$ , entonces  $M$  es un  **$R$ -módulo unitario**.

**Ejemplo 37.6** Todo grupo abeliano  $G$  se puede considerar como un  $\mathbb{Z}$ -módulo si definimos  $n\alpha = \alpha^n$  para  $\alpha \in G$  y  $n \in \mathbb{Z}$ . Usamos notación multiplicativa para la operación en  $G$ . Los axiomas de módulo se verifican fácilmente. ■

**Ejemplo 37.7** Para un ideal  $N$  en  $R$ ,  $\langle N, + \rangle$  puede considerarse un  $R$ -módulo donde para  $x \in N$  y  $r \in R$ ,  $rx$  es la multiplicación ordinaria del anillo de  $r$  y  $x$ , ambos vistos como elementos del anillo  $R$ . ■

Podemos hablar de submódulos, módulos cocientes y  $R$ -homomorfismos de un  $R$ -módulo en otro, todo mediante definiciones naturales. Podemos tomar, además, sumas directas de  $R$ -módulos y obtener  $R$ -módulos.

**Definición** Un  $R$ -módulo  $M$  es *cíclico* si existe  $x \in M$  tal que  $M = \{rx \mid r \in R\}$ .

Así, un  $R$ -módulo cíclico está generado por un sólo elemento. La idea de un *conjunto de generadores de un  $R$ -módulo* es una generalización natural de la idea del conjunto de vectores generadores de un espacio vectorial. El siguiente teorema es un bello resultado; lo enunciamos sin demostración y después lo ilustramos para algunos casos particulares, a la luz de nuestro trabajo anterior.

**Teorema 37.2** Si  $R$  es un DIP, entonces todo  $R$ -módulo finitamente generado es isomorfo a una suma directa de  $R$ -módulos cíclicos.

Sea  $R = Z$  y refiriéndonos al ejemplo 37.6, vemos, del teorema, que todo grupo abeliano finitamente generado es isomorfo a una suma directa de grupos cíclicos. Esta es gran parte del teorema fundamental de los grupos abelianos finitamente generados. Para  $R = F$ , donde  $F$  es un campo, aplicamos el teorema 37.2 a un espacio vectorial  $V$  de dimensión finita, sobre  $F$ , y vemos que  $V$  es isomorfo a una suma directa de espacios vectoriales de dimensión 1 sobre  $F$ .

## \*37.3 ALGEBRAS

**Definición** Un *álgebra* consta de un espacio vectorial  $V$  sobre un campo  $F$ , junto con una operación binaria de multiplicación en el conjunto  $V$  de vectores, tal que para todas las  $a \in F$  y  $\alpha, \beta, \gamma \in V$  se satisfacen las condiciones siguientes:

- 1  $(a\alpha)\beta = a(\alpha\beta) = \alpha(a\beta)$ .
- 2  $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ .
- 3  $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ .

Hablaremos de manera algo incorrecta de un *álgebra  $V$  sobre  $F$* . También,  $V$  es un *álgebra asociativa sobre  $F$*  si además de las tres condiciones anteriores,

$$4 \quad (\alpha\beta)\gamma = \alpha(\beta\gamma) \quad \text{para toda } \alpha, \beta, \gamma \in V.$$

**Ejemplo 37.8** Si  $E$  es un campo de extensión de un campo  $F$ , entonces  $V = E$  puede considerarse como un álgebra asociativa sobre  $F$ , donde la suma y multi-

plicación de elementos de  $V$  son la suma y multiplicación del campo en  $E$  y la multiplicación por un escalar por elementos de  $F$  es, de nuevo, la multiplicación del campo en  $E$ . ■

**Ejemplo 37.9** Para cualquier grupo  $G$  y campo  $F$ , el *álgebra del grupo*  $F(G)$  definida en la sección 25.3 es un álgebra asociativa sobre  $F$ . ■

**Definición** Un álgebra  $V$  sobre un campo  $F$  es un *álgebra de división sobre  $F$*  si  $V$  tiene unitario para la multiplicación y contiene un inverso multiplicativo de cada elemento distinto de cero. ( Nótese que *no* se supone la asocia-  
tividad de la multiplicación.)

**Ejemplo 37.10** Un campo de extensión  $E$  de un campo  $F$ , puede considerarse como un álgebra de división asocia-  
tiva sobre  $F$ . También los cuaterniones  $\mathcal{Q}$  de la  
sección 25.4 forman un álgebra de división asocia-  
tiva sobre los números reales. ■

Concluimos, para dar información, con el enunciado de algunos resultados famo-  
sos acerca de álgebras de división sobre los números reales.

**Teorema 37.3** Los números reales, los números complejos y los cuaterniones son las únicas (salvo isomorfismo) álgebras de división asocia-  
tivas sobre los números reales (Frobenius, 1878). La única otra álgebra de división sobre los números reales es el álgebra de Cayley, que es un espacio vectorial de dimen-  
sión 8 sobre  $\mathbb{R}$  (Bott y Milnor, 1957).

## Ejercicios

---

\*37.1 Nuestra definición de  $\mathcal{O}$ -grupo *no* comenzó

Un  $\mathcal{O}$ -grupo  $\langle , , \dots, \rangle$  es ...

de manera similar a nuestras definiciones de grupo y de anillo. Si definiéramos un  $\mathcal{O}$ -grupo de esa manera, ¿qué sería  $\langle , , \dots, \rangle$ ? Asegúrese de considerar *todos* los conjuntos y *todas* las operaciones involucradas.

\*37.2 Repítase el ejercicio 37.1 para un  $R$ -módulo.

\*37.3 Repítase el ejercicio 37.1 para un álgebra.

\*37.4 Muéstrese que la intersección de subgrupos admisibles de un  $\mathcal{O}$ -grupo  $G$  es, de nuevo, un subgrupo admisible de  $G$ .

\*37.5 Sea  $G$  cualquier grupo y sea  $\mathcal{A}$  el conjunto de *todos* los automorfismos de  $G$ . Por el ejemplo 37.3,  $G$  puede considerarse un  $\mathcal{A}$ -grupo. Un  $\mathcal{A}$ -grupo de  $G$  es un **subgrupo característico de  $G$** .

Todo subgrupo de todo grupo abeliano es un subgrupo normal, esto es, un  $\mathcal{A}$ -subgrupo, pero dése un ejemplo para mostrar que no todo subgrupo de todo grupo abeliano es un subgrupo característico.

\*37.6 Muéstrese que el grupo factor de un  $\mathcal{O}$ -grupo,  $G$  módulo un subgrupo normal admisible, puede considerarse, de nuevo, un  $\mathcal{O}$ -grupo de manera natural. Esto es, definase la multiplicación externa en las clases laterales, muéstrese que está bien definida y verifíquense los axiomas para un  $\mathcal{O}$ -grupo.

\*37.7 Definase el concepto de  $\mathcal{O}$ -homomorfismo de un  $\mathcal{O}$ -grupo  $G$  en un  $\mathcal{O}$ -grupo  $G'$ . Muéstrese que el kernel es un  $\mathcal{O}$ -subgrupo de  $G$ .

\*37.8 Pruébese que para un  $R$ -módulo izquierdo  $M$

$$0\alpha = 0, \quad r0 = 0,$$

y

$$(-r)\alpha = -(r\alpha) = r(-\alpha)$$

para toda  $\alpha \in M$  y  $r \in R$ .

\*37.9 Sea  $M$  un  $R$ -módulo izquierdo y sea  $\alpha \in M$ . Muéstrese que  $L_\alpha = \{a \in R \mid a\alpha = 0\}$  es un ideal izquierdo de  $R$ .

\*37.10 Definase un submódulo de un  $R$ -módulo (izquierdo)  $M$  y un módulo cociente de un  $R$ -módulo (izquierdo)  $M$ , módulo un submódulo  $N$ .

\*37.11 Definase un  $R$ -homomorfismo de un  $R$ -módulo (izquierdo)  $M$  en un  $R$ -módulo (izquierdo)  $M'$ .

\*37.12 Muéstrese que el anillo  $\langle M_n(F), +, \cdot \rangle$  de la sección 25.1, se convierte en un álgebra de dimensión  $n^2$  sobre  $F$  si definimos la multiplicación por un escalar por  $b(a_{ij}) = (ba_{ij})$  para  $(a_{ij}) \in M_n(F)$  y  $b \in F$ .

\*37.13 Sea  $V$  un álgebra de dimensión finita con una base

$$B = \{\beta_i \mid i = 1, \dots, n\}$$

sobre un campo  $F$ . Muéstrese que la multiplicación de vectores en  $V$  está por completo determinada por los  $n^2$  productos  $\beta_r \beta_s$  para cada par ordenado  $(\beta_r, \beta_s)$  de vectores de la base de  $B$ .

\*37.14 Sea  $V$  un álgebra de dimensión finita con una base

$$B = \{\beta_i \mid i = 1, \dots, n\}$$

sobre un campo  $F$ . Muéstrese que  $V$  es un álgebra asociativa sobre  $F$  si y sólo si

$$\beta_r(\beta_s \beta_t) = (\beta_r \beta_s) \beta_t$$

Para cada una de las  $n^3$  ternas ordenadas  $(\beta_r, \beta_s, \beta_t)$  de vectores de la base  $B$ .

\*37.15 Sea  $V$  un espacio vectorial de dimensión finita, sobre un campo  $F$ , con una base  $B = \{\beta_i \mid i = 1, \dots, n\}$  sobre  $F$ . Sea  $\{c_{rst} \mid r, s, t = 1, \dots, n\}$  cualquier colección de  $n^3$  escalares en  $F$ . Muéstrese que existe exactamente una operación binaria de multiplicación en  $V$  tal que  $V$  es un álgebra sobre  $F$  bajo esta multiplicación y tal que

$$\beta_r \beta_s = \sum_t c_{rst} \beta_t$$

para todo par ordenado  $(\beta_r, \beta_s)$  de vectores de la base  $B$ . Los escalares  $c_{rst}$  son las constantes estructurales del álgebra.

# Extensiones algebraicas

## 38.1 EXTENSIONES FINITAS

En el teorema 36.4 vimos que si  $E$  es un campo de extensión de un campo  $F$  y  $\alpha \in E$  es algebraico sobre  $F$ , entonces todo elemento de  $F(\alpha)$  es algebraico sobre  $F$ . Al estudiar ceros de polinomios en  $F[x]$  estaremos interesados casi exclusivamente en extensiones de  $F$  que sólo contengan elementos algebraicos sobre  $F$ .

**Definición** Un campo de extensión  $E$  de un campo  $F$  es una *extensión algebraica de  $F$*  si todo elemento en  $E$  es algebraico sobre  $F$ .

**Definición** Si un campo de extensión  $E$  de un campo  $F$  es de dimensión finita  $n$  como espacio vectorial sobre  $F$ , entonces  $E$  es una *extensión finita de grado  $n$  sobre  $F$* . Denotamos por  $[E:F]$  el grado  $n$  de  $E$  sobre  $F$ .

Usaremos a menudo el hecho de que si  $E$  es una extensión finita de  $F$ , entonces  $[E:F] = 1$  si y sólo si  $E = F$ . Basta observar que, por el teorema 36.3, siempre puede extenderse  $\{1\}$  hasta una base para  $E$  sobre  $F$ . Entonces,  $[E:F] = 1$  implica que  $E = F(1) = F$ . El reciproco es obvio.

Repitamos el argumento del teorema 36.4 para mostrar que una extensión finita  $E$  de un campo  $F$  debe ser una extensión algebraica de  $F$ .

**Teorema 38.1** *Un campo de extensión finita  $E$  de un campo  $F$  es una extensión algebraica de  $F$ .*

**Demostración** Debemos mostrar que para  $\alpha \in E$ ,  $\alpha$  es algebraico sobre  $F$ . Por el teorema 36.3, si  $[E:F] = n$ , entonces

$$1, \alpha, \dots, \alpha^n$$

no pueden ser elementos linealmente independientes, de modo que existen  $a_i \in F$  tales que

$$a_n x^n + \cdots + a_1 x + a_0 = 0,$$

donde no todas las  $a_i = 0$ . Entonces,  $f(x) = a_n x^n + \cdots + a_1 x + a_0$  es un polinomio distinto de cero en  $F[x]$  y  $f(\alpha) = 0$ . Por tanto,  $\alpha$  es algebraico sobre  $F$ . ■

No se puede exagerar la importancia del siguiente teorema. Desempeña un papel importante en la teoría de campos, análogo al papel del teorema de Lagrange en teoría de grupos. A pesar de que su demostración se sigue fácilmente del breve trabajo con espacios vectoriales, es una herramienta de una fuerza increíble. Más adelante usaremos constantemente el teorema en los argumentos de la teoría de Galois. Además, una elegante aplicación de este teorema, en el siguiente capítulo con asterisco, muestra la imposibilidad de realizar ciertas construcciones geométricas con regla y compás. *Nunca hay que subestimar un teorema que cuente algo.* ■

**Teorema 38.2** *Si  $E$  es un campo de extensión finita de un campo  $F$  y  $K$  es un campo de extensión finita de  $E$ , entonces  $K$  es una extensión finita de  $F$ , y*

$$[K:F] = [K:E][E:F].$$

*Demostración* Sea  $\{\alpha_i \mid i = 1, \dots, n\}$  una base para  $E$  como espacio vectorial sobre  $F$  y sea  $\{\beta_j \mid j = 1, \dots, m\}$  una base para  $K$  como espacio vectorial sobre  $E$ . El teorema quedará probado si podemos mostrar que los  $mn$  elementos  $\alpha_i \beta_j$  forman una base para  $K$  considerado como espacio vectorial sobre  $F$ .

Sea  $\gamma$  cualquier elemento de  $K$ . Como las  $\beta_j$  forman una base para  $K$  sobre  $E$ , tenemos

$$\gamma = \sum_{j=1}^m b_j \beta_j$$

para  $b_j \in E$ . Como las  $\alpha_i$  forman una base para  $E$  sobre  $F$  tenemos

$$b_j = \sum_{i=1}^n a_{ij} \alpha_i$$

para  $a_{ij} \in F$ . Entonces,

$$\gamma = \sum_{j=1}^m \left( \sum_{i=1}^n a_{ij} \alpha_i \right) \beta_j = \sum_{i,j} a_{ij} (\alpha_i \beta_j),$$

de modo que los  $mn$  vectores  $\alpha_i \beta_j$  generan  $K$  sobre  $F$ .

Falta mostrar que los  $mn$  elementos  $\alpha_i\beta_j$  son independientes sobre  $F$ . Supóngase que  $\sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0$ , con  $c_{ij} \in F$ . Entonces,

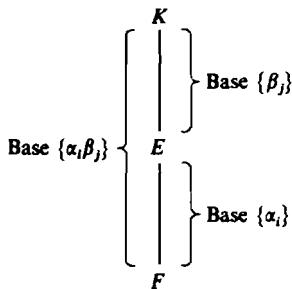
$$\sum_{j=1}^m \left( \sum_{i=1}^n c_{ij}\alpha_i \right) \beta_j = 0,$$

y  $(\sum_{i=1}^n c_{ij}\alpha_i) \in E$ . Como los elementos  $\beta_j$  son independientes sobre  $E$ , debemos tener

$$\sum_{i=1}^n c_{ij}\alpha_i = 0$$

para toda las  $j$ . Pero ahora las  $\alpha_i$  son independientes sobre  $F$ , de modo que  $\sum_{i=1}^n c_{ij}\alpha_i = 0$  implica que  $c_{ij} = 0$  para todas las  $i$  y  $j$ . Así, las  $\alpha_i\beta_j$  no sólo generan  $K$  sobre  $F$ , sino, además, son independientes sobre  $F$ . Así, forman una base para  $K$  sobre  $F$ . ■

Nótese que probamos el teorema exhibiendo una base. Es importante recordar que si  $\{\alpha_i \mid i = 1, \dots, n\}$  es una base para  $E$  sobre  $F$  y  $\{\beta_j \mid j = 1, \dots, m\}$  es una base para  $K$  sobre  $E$ , para campos  $F \leq E \leq K$ , entonces, el conjunto  $\{\alpha_i\beta_j\}$  de los  $mn$  productos, es una base para  $K$  sobre  $F$ . La figura 38.1 es un diagrama de la situación. En un momento, ilustraremos mejor todo esto.



**Figura 38.1**

**Corolario 1** Si  $F_i$  es un campo para  $i = 1, \dots, r$  y  $F_{i+1}$  es una extensión finita de  $F_i$ , entonces  $F_r$  es una extensión finita de  $F_1$  y

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

**Demostración** La demostración del corolario 1 es una extensión obvia por inducción, del teorema 38.2. ■

**Corolario 2** Si  $E$  es un campo de extensión de  $F$ ,  $\alpha \in E$  es algebraico sobre  $F$  y  $\beta \in F(\alpha)$ , entonces,  $\text{grad}(\beta, F)$  divide  $\text{grad}(\alpha, F)$ .

*Demostración* Por el teorema 36.4  $\text{grad}(\alpha, F) = [F(\alpha) : F]$  y  $\text{grad}(\beta, F) = [F(\beta) : F]$ . Tenemos  $F \leq F(\beta) \leq F(\alpha)$ , de modo que, por el teorema 38.2,  $[F(\beta) : F]$  divide  $[F(\alpha) : F]$ . ■

El siguiente ejemplo ilustra un tipo de argumentación que se hace a menudo utilizando el teorema 38.2 o sus corolarios.

**Ejemplo 38.1** Por el corolario 2 del teorema 38.2, no hay elemento de  $\mathbf{Q}(\sqrt{2})$  que sea un cero de  $x^3 - 2$ . Nótese que  $\text{grad}(\sqrt{2}, \mathbf{Q}) = 2$  mientras que un cero de  $x^3 - 2$  es de grado 3 sobre  $\mathbf{Q}$ , pero 3 no divide a 2. ■

Sea  $E$  un campo de extensión de un campo  $F$ , y sean  $\alpha_1, \alpha_2$  elementos de  $E$ , no necesariamente algebraicos, sobre  $F$ . Por definición,  $F(\alpha)$  es el menor campo de extensión de  $F$  en  $E$  que contiene a  $\alpha_1$ . En forma análoga,  $(F(\alpha_1))(\alpha_2)$  puede caracterizarse como el menor campo de extensión de  $F$  en  $E$  que contiene a  $\alpha_1$  y a  $\alpha_2$ . También podríamos haber comenzado con  $\alpha_2$ , de modo que, claramente,  $(F(\alpha_1))(\alpha_2) = (F(\alpha_2))(\alpha_1)$ . Denotamos este campo por  $F(\alpha_1, \alpha_2)$ . De manera análoga, para  $\alpha_i \in E$ ,  $F(\alpha_1, \dots, \alpha_n)$  es el menor campo de extensión de  $F$  que contiene todas las  $\alpha_i$  para  $i = 1, \dots, n$ . Obtenemos el campo  $F(\alpha_1, \dots, \alpha_n)$  a partir del campo  $F$  agregando a  $F$  los elementos  $\alpha_i$  en  $E$ . No habrá dificultad para verificar que, al igual que la intersección de subgrupos de un grupo, la intersección de subcampos de un campo  $E$  es, de nuevo, un subcampo de  $E$ . Es obvio que  $F(\alpha_1, \dots, \alpha_n)$  es la intersección de todos los subcampos de  $E$  que contienen  $F$  y todas las  $\alpha_i$  para  $i = 1, \dots, n$ .

**Ejemplo 38.2** Considérese  $\mathbf{Q}(\sqrt{2})$ . El teorema 36.4 muestra que  $\{1, \sqrt{2}\}$  es una base para  $\mathbf{Q}(\sqrt{2})$  sobre  $\mathbf{Q}$ . Calculando, encontramos que  $\text{irr}(\sqrt{2} + \sqrt{3}, \mathbf{Q}) = x^4 - 10x^2 + 1$ , de modo que  $[\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}] = 4$ . Así,  $(\sqrt{2} + \sqrt{3}) \notin \mathbf{Q}(\sqrt{2})$ , de modo que  $\sqrt{3} \in \mathbf{Q}(\sqrt{2})$ . Por tanto,  $\{1, \sqrt{3}\}$  es una base para  $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = (\mathbf{Q}(\sqrt{2}))(\sqrt{3})$  sobre  $\mathbf{Q}(\sqrt{2})$ . Entonces, la demostración del teorema 38.2 (véase el comentario que sigue al teorema) muestra que  $\{1, \sqrt{2}, \sqrt{3}\}$  es una base para  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbf{Q}$ . ■

**Ejemplo 38.3** Sea  $2^{1/3}$  la raíz cúbica real de 2 y  $2^{1/2}$  la raíz cuadrada positiva de 2. Entonces, como vimos en el ejemplo 38.1,  $2^{1/3} \notin \mathbf{Q}(2^{1/2})$ . Así,  $[\mathbf{Q}(2^{1/2}, 2^{1/3}) : \mathbf{Q}(2^{1/2})] = 3$ . Entonces,  $\{1, 2^{1/2}\}$  es una base para  $\mathbf{Q}(2^{1/2})$  sobre  $\mathbf{Q}$  y  $\{1, 2^{1/3}, 2^{2/3}\}$  es una base para  $\mathbf{Q}(2^{1/2}, 2^{1/3})$  sobre  $\mathbf{Q}(2^{1/2})$ . Más aún, por el teorema 38.2 (véase el comentario que sigue al teorema),

$$\{1, 2^{1/2}, 2^{1/3}, 2^{5/6}, 2^{2/3}, 2^{7/6}\}$$

es una base para  $\mathbf{Q}(2^{1/2}, 2^{1/3})$  sobre  $\mathbf{Q}$ . Es claro que como  $2^{7/6} = (2)2^{1/6}$ , tenemos  $2^{1/6} \in \mathbf{Q}(2^{1/2}, 2^{1/3})$ . Ahora,  $2^{1/6}$  es un cero de  $x^6 - 2$ , el cual, por el criterio de Eisenstein, es irreducible sobre  $\mathbf{Q}$ , con  $p = 2$ . Así,

$$\mathbf{Q} \leq \mathbf{Q}(2^{1/6}) \leq \mathbf{Q}(2^{1/2}, 2^{1/3})$$

y, por el teorema 38.2,

$$\begin{aligned} 6 &= [\mathbf{Q}(2^{1/2}, 2^{1/3}) : \mathbf{Q}] = [\mathbf{Q}(2^{1/2}, 2^{1/3}) : \mathbf{Q}(2^{1/6})][\mathbf{Q}(2^{1/6}) : \mathbf{Q}] \\ &= [\mathbf{Q}(2^{1/2}, 2^{1/3}) : \mathbf{Q}(2^{1/6})](6). \end{aligned}$$

Por tanto, debemos tener

$$[\mathbf{Q}(2^{1/2}, 2^{1/3}) : \mathbf{Q}(2^{1/6})] = 1,$$

de modo que, por el comentario anterior al teorema 38.1,  $\mathbf{Q}(2^{1/2}, 2^{1/3}) = \mathbf{Q}(2^{1/6})$ . ■

El ejemplo 38.3 muestra que es posible que una extensión  $F(\alpha_1, \dots, \alpha_n)$  de un campo  $F$  sea, en realidad, una extensión simple, aunque  $n > 1$ .

Caractericemos las extensiones de  $F$  de la forma  $F(\alpha_1, \dots, \alpha_n)$  en el caso en que todas las  $\alpha_i$  sean algebraicas sobre  $F$ .

**Teorema 38.3** *Sea  $E$  una extensión algebraica de un campo  $F$ . Entonces, existe un número finito de elementos  $\alpha_1, \dots, \alpha_n$  en  $E$  tal que  $E = F(\alpha_1, \dots, \alpha_n)$  si y sólo si  $E$  es un espacio vectorial de dimensión finita sobre  $F$ , esto es, si y sólo si  $E$  es una extensión finita de  $F$ .*

**Demostración** Supóngase que  $E = F(\alpha_1, \dots, \alpha_n)$ . Como  $E$  es una extensión algebraica de  $F$ , cada  $\alpha_i$  es algebraico sobre  $F$ , de modo que, claramente, cada  $\alpha_i$  es algebraico sobre todo campo de extensión de  $F$  en  $E$ . Así,  $F(\alpha_1)$  es algebraico sobre  $F$  y, en general,  $F(\alpha_1, \dots, \alpha_j)$  es algebraico sobre  $F(\alpha_1, \dots, \alpha_{j-1})$  para  $j = 2, \dots, n$ . Se aplica el corolario 1 del teorema 38.2 a la sucesión de extensiones finitas

$$F, F(\alpha_1), F(\alpha_1, \alpha_2), \dots, F(\alpha_1, \dots, \alpha_n) = E$$

y se muestra, entonces, que  $E$  es una extensión finita de  $F$ .

En forma recíproca, supóngase que  $E$  es una extensión algebraica finita de  $F$ . Si  $[E:F] = 1$  entonces,  $E = F(1) = F$ , y habremos terminado. Si  $E \neq F$ , sea  $\alpha_1 \in E$  donde  $\alpha_1 \notin F$ . Entonces,  $[F(\alpha_1) : F] > 1$ . Si  $F(\alpha_1) = E$ , ya terminamos; si no, sea  $\alpha_2 \in E$ , donde  $\alpha_2 \notin F(\alpha_1)$ . Continuando este proceso vemos, del teorema 38.2, que debido a que  $[E:F]$  es finito, debemos llegar a  $\alpha_n$  tal que

$$F(\alpha_1, \dots, \alpha_n) = E. \blacksquare$$

## 38.2 CAMPOS ALGEBRAICAMENTE CERRADOS Y CERRADURAS ALGEBRAICAS

Aún no hemos señalado que si  $E$  es una extensión de un campo  $F$  y  $\alpha, \beta \in E$  son algebraicos sobre  $F$ , entonces también lo son  $\alpha + \beta$ ,  $\alpha\beta$ ,  $\alpha - \beta$  y  $\alpha/\beta$ , si  $\beta \neq 0$ .

Esto se sigue fácilmente del teorema 38.3 y está incluido, además, en el teorema siguiente.

**Teorema 38.4** *Sea  $E$  un campo de extensión de  $F$ . Entonces*

$$\bar{F}_E = \{\alpha \in E \mid \alpha \text{ es algebraico sobre } F\}$$

*es un subcampo de  $E$ , la cerradura algebraica de  $F$  en  $E$ .*

**Demostración** Sea  $\alpha, \beta \in \bar{F}_E$ . Entonces, el teorema 38.3 muestra que  $F(\alpha, \beta)$  es una extensión finita de  $F$  y, por el teorema 38.1, todo elemento de  $F(\alpha, \beta)$  es algebraico sobre  $F$ , esto es,  $F(\alpha, \beta) \subseteq \bar{F}_E$ . Así  $\bar{F}_E$  contiene a  $\alpha + \beta, \alpha\beta, \alpha - \beta$  y también a  $\alpha/\beta$  para  $\beta \neq 0$ , de modo que  $\bar{F}_E$  es un subcampo de  $E$ . ■

**Corolario** *El conjunto de todos los números algebraicos forma un campo.*

**Demostración** La demostración de este corolario es inmediata del teorema 38.4, pues el conjunto de todos los números algebraicos es la cerradura algebraica de  $\mathbb{Q}$  en  $\mathbb{C}$ . ■

Es bien sabido que los números complejos tienen la propiedad de que todo polinomio no constante en  $\mathbb{C}[x]$  tiene un cero en  $\mathbb{C}$ . Esto se conoce como el *teorema fundamental del álgebra*. Más adelante en este capítulo, en un párrafo con asterisco, daremos una demostración analítica de este teorema. Por ahora, damos una definición para generalizar este importante concepto a otros campos.

**Definición** Un campo  $F$  está *algebraicamente cerrado* si todo polinomio no constante en  $F[x]$  tiene algún cero en  $F$ .

El siguiente teorema muestra que el concepto de un campo algebraicamente cerrado también se puede definir en términos de factorización de polinomios sobre el campo.

**Teorema 38.5** *Un campo  $F$  está algebraicamente cerrado si y sólo si todo polinomio no constante en  $F[x]$  se puede factorizar en  $F[x]$  en factores lineales.*

**Demostración** Sea  $F$  algebraicamente cerrado y sea  $f(x)$  un polinomio no constante en  $F(x)$ . Entonces,  $f(x)$  tiene un cero  $a \in F$ . Por el corolario 1 del teorema 31.1,  $x - a$  es un factor de  $f(x)$ , de modo que  $f(x) = (x - a)g(x)$ . Entonces, si  $g(x)$  no es constante, tiene un cero  $b \in F$  y  $f(x) = (x - a)(x - b)h(x)$ . Continuando, obtenemos una factorización de  $f(x)$  en  $F[x]$  en factores lineales.

En forma recíproca, supóngase que todo polinomio no constante de  $F[x]$  tiene una factorización en factores lineales. Si  $ax - b$  es un factor lineal de  $f(x)$ , entonces  $b/a$  es un cero de  $f(x)$ . Así,  $F$  es algebraicamente cerrado. ■

**Corolario** *Un campo  $F$  algebraicamente cerrado no tiene extensiones algebraicas propias, esto es, ninguna extensión algebraica  $F$  con  $F < E$ .*

**Demostración** Sea  $E$  una extensión algebraica de  $F$ , así  $F \leq E$ . Entonces, por el teorema 38.5, si  $\alpha \in E$  tenemos  $\text{irr}(\alpha, F) = x - \alpha$ , puesto que  $F$  es algebraicamente cerrado. Así,  $\alpha \in F$  y debemos tener  $F = E$ . ■

En la sección 38.3, con asterisco, mostraremos que así como existe una extensión algebraicamente cerrada  $C$  de los números reales  $R$ , para cualquier campo  $F$  existe análogamente una extensión algebraica  $\bar{F}$  de  $F$  con la propiedad de que  $\bar{F}$  está algebraicamente cerrada. En el capítulo 41 se mostrará que dicha extensión  $\bar{F}$  es única, salvo isomorfismo, por supuesto. De manera intuitiva, para encontrar  $\bar{F}$  se procede como sigue. Si no todo polinomio  $f(x)$  en  $F[x]$  tiene un cero, entonces agregar a  $F$  un cero  $\alpha$  de dicho  $f(x)$ , obteniendo así, el campo  $F(\alpha)$ . *Por supuesto, se usó aquí el teorema 35.1 de Kronecker.* Si  $F(\alpha)$  aún no es algebraicamente cerrado se continúa el proceso. El problema es que, a diferencia de la situación para la cerradura algebraica  $C$  de  $R$ , podemos seguir un número infinito (posiblemente grande) de veces. Se puede mostrar con facilidad (véanse los ejercicios 38.13 y 38.16) que  $\bar{Q}$  es isomorfo al campo de todos los números algebraicos y que no podemos obtener  $\bar{Q}$  de  $Q$  agregando un número finito de números algebraicos. Primero, tendremos que analizar algún material de teoría de conjuntos, el *lema de Zorn*, para poder manejar dicha situación. Este material es algo complejo, así que lo ponemos en un párrafo con asterisco. Sin embargo, el teorema de existencia para  $\bar{F}$  es muy importante y lo enunciamos aquí, de modo que se comprenda la necesidad de conocerlo. No hay problema si se asume su validez.

**Teorema 38.5** *Todo campo  $F$  tiene una cerradura algebraica, esto es, una extensión algebraica  $\bar{F}$  que está algebraicamente cerrada.*

### \*38.3 EXISTENCIA DE UNA CERRADURA ALGEBRAICA

Probaremos que todo campo tiene una extensión algebraica que está algebraicamente cerrada. Creemos que al final de un curso de álgebra, deben tener la oportunidad de ver alguna demostración que incluya el *axioma de selección*. Este es el lugar natural para dicha demostración. Usaremos una forma equivalente del axioma de selección, el *lema de Zorn*. Para enunciarlo requerimos una definición de teoría de conjuntos.

**Definición** *Un orden parcial en un conjunto  $S$  está dado por una relación  $\leq$  definida para ciertos pares ordenados de elementos de  $S$  tales que se satisfacen las siguientes condiciones:*

- 1  $a \leq a$  para todos los  $a \in S$  (*ley reflexiva*).
- 2 Si  $a \leq b$  y  $b \leq a$ , entonces  $a = b$  (*ley antisimétrica*).
- 3 Si  $a \leq b$  y  $b \leq c$ , entonces  $a \leq c$  (*ley transitiva*).

En un conjunto *parcialmente ordenado* no por fuerza son **comparables** cada par de elementos, esto es, para  $a, b \in S'$  no necesariamente se tiene  $a \leq b$  o  $b \leq a$ . Como siempre,  $a < b$  denota  $a \leq b$ , pero  $a \neq b$ .

Un subconjunto  $T$  de un conjunto parcialmente ordenado  $S'$  es una **cadena** si cada par de elementos  $a$  y  $b$  en  $T$  son comparables, esto es, si  $a \leq b$  o  $b \leq a$  (o ambos). Un elemento  $u \in S$  es una *cota superior* de un subconjunto  $A$  de un conjunto parcialmente ordenado  $S$  si  $a \leq u$  para todas las  $a \in A$ . Por último, un elemento  $m$  de un conjunto parcialmente ordenado  $S$  es **maximal** si no existe  $s \in S$  tal que  $m < s$ .

**Ejemplo 38.4** La colección de todos los subconjuntos de un conjunto forma un conjunto parcialmente ordenado bajo la relación  $\leq$  dada por  $\subseteq$ . Por ejemplo, si el conjunto es  $\mathbb{R}$ , tenemos  $\mathbb{Z} \subseteq \mathbb{Q}$ . Nótese, sin embargo, que para  $\mathbb{Z}$  y  $\mathbb{Q}^+$ , ni  $\mathbb{Z} \subseteq \mathbb{Q}^+$  ni  $\mathbb{Q}^+ \subseteq \mathbb{Z}$ .

**Lema de Zorn** Si  $S$  es un conjunto parcialmente ordenado tal que toda cadena en  $S$  tiene una cota superior en  $S$ , entonces  $S$  tiene al menos un elemento maximal.

El lema de Zorn no se *prueba*, no se trata de eso. El lema es equivalente al axioma de selección. Entonces, en realidad, tomamos aquí el lema de Zorn como un *axioma* de la teoría de conjuntos. El lector deberá remitirse a la bibliografía para el enunciado del axioma de selección y la demostración de su equivalencia con el lema de Zorn.

El lema de Zorn se usa con frecuencia cuando se quiere mostrar la existencia de una estructura mayor o maximal de algún tipo. Si un campo  $F$  tiene una extensión algebraica  $\bar{F}$  que sea algebraicamente cerrada, entonces  $\bar{F}$  será, con certeza, una extensión algebraica maximal de  $F$ , pues como  $\bar{F}$  es cerrada algebraicamente, no puede tener extensiones algebraicas propias.

La idea de la demostración del teorema 38.6 es muy sencilla. Dado un campo  $F$ , describiremos, primero, una clase de extensiones algebraicas de  $F$  que sea tan grande que deba contener (salvo isomorfismo) cualquier extensión algebraica concebible de  $F$ . Definimos luego un orden parcial, el orden común de subcampos, en esta clase y mostramos que se satisfacen las hipótesis del lema de Zorn. Por el lema de Zorn, existirá en esta clase una extensión algebraica maximal  $\bar{F}$  de  $F$ . Analizaremos entonces, que esta  $\bar{F}$  no puede tener extensiones algebraicas propias, de modo que debe ser algebraicamente cerrada.

Nuestra demostración difiere un poco de la que presentan varios textos. Nos gusta porque no usa más álgebra que la de los teoremas 35.1 y 38.2. Así, destaca con gran relieve la enorme fuerza del teorema de Kronecker y del lema de Zorn. La demostración parece larga sólo porque escribimos cada paso con exagerado detalle. Para el matemático profesional es cuestión de rutina la construcción de la demostración a partir de la información del párrafo anterior. Esta demostración fue sugerida al autor, en la época en que era estudiante de posgrado, por un compañero de clase, Norman Shapiro, quien también tenía una gran preferencia por ella.

Estamos listos ahora para realizar la demostración del teorema 38.6, que reenunciamos aquí.

**Teorema 38.6** *Todo campo  $F$  tiene cerradura algebraica  $\bar{F}$ .*

*Demostración* Puede demostrarse en teoría de conjuntos que, dado cualquier conjunto, existe un conjunto con *estRICTAMENTE MÁS* elementos. Supóngase que formamos un conjunto

$$A = \{\omega_{f_i} \mid f \in F[x]; i = 0, \dots, (\text{grado } f)\}$$

que tenga un elemento para todo cero posible de cualquier  $f(x) \in F[x]$ . Sea  $\Omega$  un conjunto con estrictamente más elementos que  $A$ . Formando  $\Omega \cup F$  si es necesario, podemos suponer que  $F \subset \Omega$ . Consideréngase todos los campos posibles que sean extensiones algebraicas de  $F$  y que, como conjuntos, consten de elementos de  $\Omega$ . Una de dichas extensiones algebraicas es  $F$  mismo. Si  $E$  es cualquier campo de extensión de  $F$ , y si  $\gamma \in E$  es un cero de  $f(x) \in F[x]$  donde  $\gamma \in F$  y  $\text{grad}(\gamma, F) = n$ , entonces, redenominando  $\gamma$  como  $\omega$  para  $\omega \in \Omega$  y  $\omega \notin F$ , y redenominando a los elementos  $a_0 + a_1\gamma + \dots + a_{n-1}\gamma^{n-1}$  de  $F(\gamma)$  como distintos elementos de  $\Omega$ , conforme  $a_i$  varía sobre  $F$ , podemos considerar nuestra  $F(\gamma)$  redenominada como un campo de extensión algebraica  $F(\omega)$  de  $F$ , con  $F(\omega) \subset \Omega$  y  $f(\omega) = 0$ . El conjunto  $\Omega$  tiene suficientes elementos para formar  $F(\omega)$ , pues  $\Omega$  tiene más que suficientes elementos para proporcionar  $n$  ceros diferentes para cada elemento de cada grado  $n$  en cualquier subconjunto de  $F[x]$ .

Todos los campos de extensión algebraica  $E_j$  de  $F$  con  $E_j \subseteq \Omega$ , forman un conjunto

$$S = \{E_j \mid j \in J\}$$

parcialmente ordenado bajo nuestra inclusión usual  $\leq$  de subcampos.  $F$  mismo es un elemento de  $S$ . El párrafo anterior muestra que si  $F$  está lejos de ser algebraicamente cerrado, habrá muchos campos  $E_j$  en  $S$ .

Sea  $T = \{E_{jk}\}$  una cadena en  $S$  y sea  $W = \bigcup_k E_{jk}$ . Ahora, haremos de  $W$  un campo. Sea  $\alpha, \beta \in W$ . Entonces, existen  $E_{j_1}, E_{j_2} \in S$  con  $\alpha \in E_{j_1}$  y  $\beta \in E_{j_2}$ . Como  $T$  es una cadena, uno de los campos  $E_{j_1}$  o  $E_{j_2}$  es un subcampo del otro, digamos  $E_{j_1} \leq E_{j_2}$ . Entonces,  $\alpha, \beta \in E_{j_2}$  y usamos las operaciones de  $E_{j_2}$  para definir la suma de  $\alpha$  y  $\beta$  en  $W$  como  $(\alpha + \beta) \in E_{j_2}$  y así mismo, el producto como  $(\alpha\beta) \in E_{j_2}$ . Estas operaciones están bien definidas en  $W$ ; son independientes de nuestra selección de  $E_{j_2}$ , pues si, además,  $\alpha, \beta \in E_{j_3}$  para  $E_{j_3}$  en  $T$ , entonces uno de los campos  $E_{j_2}$  o  $E_{j_3}$  es un subcampo del otro, ya que  $T$  es una cadena. Así, tenemos, definidas en  $W$ , las operaciones de suma y multiplicación.

Todos los axiomas de campo para  $W$  bajo estas operaciones se siguen ahora del hecho de que estas operaciones se definieron en términos de suma y multiplicación en campos. Así, por ejemplo,  $1 \in F$  sirve como identidad multiplicativa en  $W$  ya que para  $\alpha \in W$ , si  $1, \alpha \in E_{j_1}$ , entonces tenemos  $1\alpha = \alpha$  en  $E_{j_1}$ , de modo que  $1\alpha = \alpha$  en  $W$  por definición de multiplicación en  $W$ . Además, para mayor ilustración, para verificar las leyes distributivas, sean  $\alpha, \beta, \gamma \in W$ . Como  $T$  es una cadena podemos encontrar algún campo en  $T$  que contenga los tres elementos  $\alpha$ ,

$\beta$  y  $\gamma$ , y en este campo se cumplen las leyes distributivas para  $\alpha$ ,  $\beta$  y  $\gamma$ . Por tanto, se cumplen en  $W$ . Por consiguiente, podemos considerar  $W$  como un campo y por construcción,  $E_{j_k} \leq W$  para toda  $E_{j_k} \in T$ .

Si podemos mostrar que  $W$  es algebraico sobre  $F$ , entonces  $W \in S$  será una cota superior para  $T$ . Pero si  $\alpha \in W$ , entonces  $x \in E_j$ , para algún  $E_j$ , en  $T$ , de modo que  $\alpha$  es algebraica sobre  $F$ . De aquí que  $W$  es una extensión algebraica de  $F$  y es una cota superior para  $T$ .

Así, se satisface la hipótesis del lema de Zorn, de modo que existe algún elemento maximal  $\bar{F}$  de  $S$ . Afirmando que  $\bar{F}$  está algebraicamente cerrado. Sea  $f(x) \in \bar{F}[x]$ , donde  $f(x) \notin \bar{F}$ . Supóngase que  $f(x)$  no tiene ceros en  $\bar{F}$ . Como  $\Omega$  tiene muchos más elementos de los que tiene  $\bar{F}$ , podemos tomar  $\omega \in \Omega$  donde  $\omega \notin \bar{F}$  y formar un campo  $\bar{F}(\omega) \subseteq \Omega$  con  $\omega$  un cero de  $f(x)$ , como vimos en el primer párrafo de esta demostración. Sea  $\beta$  en  $\bar{F}(\omega)$ . Entonces, por el teorema 36.4,  $\beta$  es un cero de un polinomio

$$g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

en  $\bar{F}[x]$  con  $\alpha_i \in \bar{F}$  y, por tanto,  $\alpha_i$  es algebraico sobre  $F$ . Entonces, por el teorema 38.3,  $F(\alpha_0, \dots, \alpha_n)$  es una extensión finita de  $F$ , y como  $\beta$  es algebraico sobre  $F(\alpha_0, \dots, \alpha_n)$ , vemos, además, que  $F(\alpha_0, \dots, \alpha_n, \beta)$  es una extensión finita sobre  $F(\alpha_0, \dots, \alpha_n)$ . Entonces, el teorema 38.2, muestra que  $F(\alpha_0, \dots, \alpha_n, \beta)$  es una extensión finita de  $F$ , de modo que, por el teorema 38.1,  $\beta$  es algebraico sobre  $F$ . De aquí que  $\bar{F}(\omega) \in S$  y  $\bar{F} < \bar{F}(\omega)$  lo cual contradice la selección de  $\bar{F}$  como maximal en  $S$ . Así,  $f(x)$  debe tener algún cero en  $\bar{F}$ , de modo que  $\bar{F}$  está cerrado algebraicamente. ■

Para el matemático profesional, la mecánica de la demostración anterior es cuestión de rutina. Debido a que quizás ésta sea la primera demostración que se haya visto en donde se usa el lema de Zorn, la escribimos con todo detalle. Sin embargo, la construcción y los razonamientos empleados deben considerarse fáciles y rutinarios.

Es bien conocido que  $C$  es un campo cerrado algebraicamente. Aunque hay más demostraciones algebraicas de este hecho, damos una demostración analítica como la más accesible para el estudiante que haya llevado un curso de funciones de variable compleja.

**Teorema 38.7 (Teorema fundamental del álgebra)** *El campo  $C$  de números complejos es un campo algebraicamente cerrado.*

**Demostración** Sea  $f(z) \in C[z]$  el polinomio que no tenga cero en  $C$ . Entonces  $1/f(z)$  da una función entera, esto es,  $1/f$  es analítica en todas partes. Además, si  $f \notin C$ ,  $\lim_{|c| \rightarrow \infty} |f(c)| = \infty$ , de modo que  $\lim_{|c| \rightarrow \infty} |1/f(c)| = 0$ . Así,  $1/f$  debe ser acotada en el plano. Entonces, por el teorema de Liouville de la teoría de funciones de variable compleja,  $1/f$  es constante y así  $f$  es constante. Por tanto, un polinomio no constante en  $C[z]$  debe tener un cero en  $C$ , de modo que  $C$  está cerrado algebraicamente. ■

**Ejercicios**

**38.1** Encuéntrese el grado y una base para cada uno de los campos de extensión dados.

- a)  $\mathbb{Q}(\sqrt{2})$  sobre  $\mathbb{Q}$
- b)  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbb{Q}$
- c)  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  sobre  $\mathbb{Q}$
- d)  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$  sobre  $\mathbb{Q}$
- e)  $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  sobre  $\mathbb{Q}$

**38.2** Encuéntrese el grado de cada uno de los campos de extensión siguientes. Estar preparados para justificar las respuestas.

- a)  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  sobre  $\mathbb{Q}$
- b)  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbb{Q}$
- c)  $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$  sobre  $\mathbb{Q}$
- d)  $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24})$  sobre  $\mathbb{Q}$
- e)  $\mathbb{Q}(\sqrt{2}, \sqrt{6})$  sobre  $\mathbb{Q}(\sqrt{3})$
- f)  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  sobre  $\mathbb{Q}(\sqrt{3})$
- g)  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$
- h)  $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10})$  sobre  $\mathbb{Q}(\sqrt{3} + \sqrt{5})$

**38.3** Encuéntrese una base para cada uno de los campos de extensión dados del e) al h) del ejercicio 38.2.

**38.4** Muéstrese, mediante un ejemplo, que para un campo de extensión propio  $E$  de un campo  $F$ , la cerradura algebraica de  $F$  en  $E$  no es necesariamente cerrada algebraicamente.

**38.5** Sea  $(a + bi) \in \mathbb{C}$  para  $a, b \in \mathbb{R}$  con  $b \neq 0$ . Muéstrese que  $\mathbb{C} = \mathbb{R}(a + bi)$ .

**38.6** Muéstrese que si  $E$  es una extensión finita de un campo  $F$  y  $[E:F]$  es un número primo, entonces  $E$  es una extensión simple de  $F$  y, en efecto,  $E = F(\alpha)$  para toda  $\alpha \in E$  que no esté en  $F$ .

**38.7** ¿Falso o verdadero?

- a) Toda extensión finita de un campo es una extensión algebraica.
- b) Toda extensión algebraica de un campo es una extensión finita.
- c) El campo situado arriba de una torre finita de extensiones finitas de campos es una extensión finita del campo situado abajo.
- d)  $\mathbb{R}$  está algebraicamente cerrado.
- e)  $\mathbb{Q}$  es su propia cerradura algebraica en  $\mathbb{R}$ , esto es,  $\mathbb{Q}$  es algebraicamente cerrado en  $\mathbb{R}$ .
- f)  $\mathbb{C}$  es algebraicamente cerrado en  $\mathbb{C}(x)$ , donde  $x$  es una indeterminada.
- g)  $\mathbb{C}(x)$  es algebraicamente cerrado, donde  $x$  es una indeterminada.
- h) El campo  $\mathbb{C}(x)$  no tiene cerradura algebraica, pues  $\mathbb{C}$  ya contiene a todos los números algebraicos.
- i) Un campo algebraicamente cerrado debe tener característica 0.
- j) Si  $E$  es un campo de extensión algebraicamente cerrado de  $F$ , entonces  $E$  es una extensión algebraica de  $F$ .

**38.8** Pruébese que  $x^2 - 3$  es irreducible sobre  $\mathbb{Q}(\sqrt[3]{2})$ .

**38.9** ¿Qué grado pueden tener los campos de extensión que se logran mediante agregación sucesiva a un campo  $F$  de una raíz cuadrada de un elemento de  $F$  que no es un cuadrado en  $F$  y, después, una raíz cuadrada de algún no cuadrado en este nuevo campo y así sucesivamente? Dedúzcase de aquí, que un cero de  $x^{14} - 3x^2 + 12$  sobre  $\mathbb{Q}$  nunca se puede expresar como función racional de raíces cuadradas, de raíces cuadradas de funciones racionales de raíces cuadradas y así sucesivamente, de elementos de  $\mathbb{Q}$ .

**38.10** Sea  $E$  un campo de extensión finita de  $F$ . Sea  $D$  un dominio entero tal que  $F \subseteq D \subseteq E$ . Muéstrese que  $D$  es un campo.

**38.11** Pruébese en detalle que  $\mathbf{Q}(\sqrt{3} + \sqrt{7}) = \mathbf{Q}(\sqrt{3}, \sqrt{7})$ .

**38.12** Generalizando el ejercicio 38.11, muéstrese que si  $\sqrt{a} + \sqrt{b} \neq 0$ , entonces  $\mathbf{Q}(\sqrt{a} + \sqrt{b}) = \mathbf{Q}(\sqrt{a}, \sqrt{b})$ , para todas las  $a$  y  $b$  en  $\mathbf{Q}$  [Sugerencia: Calcúlese  $(\sqrt{a} + \sqrt{b})^2$ .]

**38.13** Sea  $E$  una extensión finita de un campo  $F$  y sea  $p(x) \in F[x]$  irreducible sobre  $F$  y de grado que no es divisor de  $[E : F]$ . Muéstrese que  $p(x)$  no tiene ceros en  $E$ .

**38.14** Sea  $E$  un campo de extensión de  $F$ . Sea  $\alpha \in E$  algebraico de grado impar sobre  $F$ . Muéstrese que  $\alpha^2$  es algebraico de grado impar sobre  $F$  y que  $F(\alpha) = F(\alpha^2)$ .

**38.15** Muéstrese que si  $F$ ,  $E$  y  $K$  son campos con  $F \leq E \leq K$ , entonces  $K$  es algebraico sobre  $F$  si y sólo si  $E$  es algebraico sobre  $F$  y  $K$  es algebraico sobre  $E$ . (No debe suponerse que las extensiones son finitas.)

**38.16** Sea  $E$  un campo de extensión de un campo  $F$ . Pruébese que toda  $\alpha \in E$  que no esté en la cerradura algebraica  $F_E$  de  $F$  en  $E$  es trascendente sobre  $F_E$ .

**38.17** Sea  $E$  un campo de extensión algebraicamente cerrado de un campo  $F$ . Muéstrese que la cerradura algebraica  $F_E$  de  $F$  en  $E$  es algebraicamente cerrada. (Si aplicamos este ejercicio a  $\mathbf{C}$  y  $\mathbf{Q}$ , vemos que el campo de todos los números algebraicos es un campo cerrado algebraicamente.)

**38.18** Muéstrese que si  $E$  es una extensión algebraica de un campo  $F$  y contiene todos los ceros en  $F$  de todo  $f(x) \in F[x]$ , entonces  $E$  es un campo algebraicamente cerrado.

**38.19** Muéstrese que ningún campo finito de característica impar es algebraicamente cerrado. (En realidad ningún campo finito de característica 2 está algebraicamente cerrado.) [Sugerencia: Muéstrese, contando, que para dicho campo finito  $F_1$  algún polinomio  $x^2 - a$ , para alguna  $a \in F$ , no tiene ceros en  $F$ . Véase el ejercicio 35.11.]

**38.20** Pruébese que, como se aseguró en el texto, la cerradura algebraica de  $\mathbf{Q}$  en  $\mathbf{C}$  no es una extensión finita de  $\mathbf{Q}$ .

\***38.21** Dedúzcase que todo campo de extensión finita de  $\mathbf{R}$  o es  $\mathbf{R}$  mismo o es isomorfo a  $\mathbf{C}$ .

\***38.22** Usese el lema de Zorn para mostrar que todo ideal propio de un anillo  $R$  con unitario está contenido en algún ideal maximal.

## Construcciones geométricas

En este capítulo, hacemos una breve desviación para dar una aplicación que demuestre la fuerza del teorema 38.2. Para un estudio más detallado de construcciones geométricas, véase Courant y Robbins [43, capítulo III].

Estamos interesados en los tipos de figuras que pueden construirse con regla y compás, en el sentido de la geometría plana euclíadiana clásica. Sin duda, el lector habrá escuchado que «es imposible trisecar el ángulo». Analizaremos esta y otras cuestiones clásicas.

### \*39.1 NUMEROS CONSTRUIBLES

Imaginemos que hay un solo segmento de recta que definiremos como de longitud *una unidad*. Un número real  $\alpha$  es **construible** si podemos construir un segmento de recta de longitud  $|\alpha|$  en un número finito de pasos, a partir de este segmento dado de longitud unitaria, usando una regla y un compás. Recuérdese que con regla y compás es posible, entre otras cosas, levantar una perpendicular a una recta dada en un punto conocido de la recta y trazar una recta que pase por un punto dado y sea paralela a una recta dada. Nuestro primer resultado es el siguiente teorema.

**Teorema 39.1** *Si  $\alpha$  y  $\beta$  son números reales construibles, entonces lo son  $\alpha + \beta$ ,  $\alpha - \beta$ ,  $\alpha\beta$  y  $\alpha/\beta$  si  $\beta \neq 0$ .*

**Demostración** Por hipótesis,  $\alpha$  y  $\beta$  son construibles, de modo que disponemos de segmentos de recta con longitudes  $|\alpha|$  y  $|\beta|$ . Para  $\alpha, \beta > 0$ , se traza, con la regla, un segmento de recta de longitud  $\alpha$ . Se inicia en un extremo del segmento original

de longitud  $\alpha$  y se traslada con el compás la longitud  $\beta$  sobre la recta que contiene el segmento de longitud  $\alpha$ . Esto construye un segmento de recta de longitud  $\alpha + \beta$ ; de manera análoga,  $\alpha - \beta$  es construible (véase la figura 39.1). Si  $\alpha$  y  $\beta$  no son ambos positivos, obviamente hay que dividir en casos, dependiendo de sus signos y se muestra que  $\alpha + \beta$  y  $\alpha - \beta$  aún son construibles.

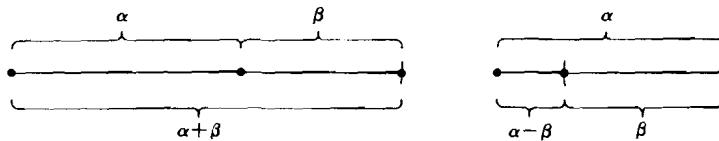


Figura 39.1

En la figura 39.2 se indica la construcción de  $\alpha\beta$ . Sea  $\overline{OA}$  el segmento de recta del punto  $O$  al punto  $A$  y sea  $|\overline{OA}|$  la longitud de este segmento de recta. Si  $\overline{OA}$  es de longitud  $|\alpha|$ , encontrar una recta  $l$  que pase por  $O$  y no contenga  $\overline{OA}$ . Despues, localizar los puntos  $P$  y  $B$  en  $l$  tales que  $\overline{OP}$  es de longitud 1 y  $\overline{OB}$  es de longitud  $|\beta|$ . Trazar  $\overline{PA}$  y construir  $l'$  que pase por  $B$  y sea paralela a  $\overline{PA}$  e interseque la extensión de  $\overline{OA}$  en  $Q$ . Por triángulos semejantes, tenemos

$$\frac{1}{|\alpha|} = \frac{|\beta|}{|\overline{OQ}|},$$

de modo que  $\overline{OQ}$  es de longitud  $|\alpha\beta|$ .

Por último, la figura 39.3 muestra que  $\alpha/\beta$  es construible si  $\beta \neq 0$ . Sea  $\overline{OA}$  de longitud  $|\alpha|$  y encontrar  $l$  que pase por  $O$  y no contenga  $\overline{OA}$ . Despues, hallar  $B$  y  $P$  en  $l$  tales que  $\overline{OB}$  sea de longitud  $|\beta|$  y  $\overline{OP}$  sea de longitud 1. Trazar  $\overline{BA}$  y construir  $l'$  que pase por  $P$  y sea paralela a  $\overline{BA}$  e interseque  $\overline{OA}$  en  $Q$ . De nuevo, por triángulos semejantes, tenemos

$$\frac{|\overline{OQ}|}{1} = \frac{|\alpha|}{|\beta|},$$

de modo que  $\overline{OQ}$  es de longitud  $|\alpha/\beta|$ . ■

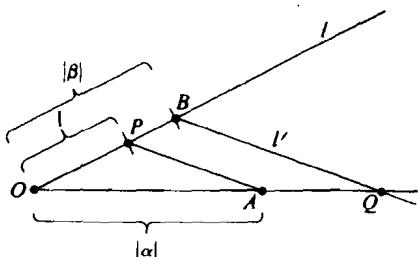


Figura 39.2

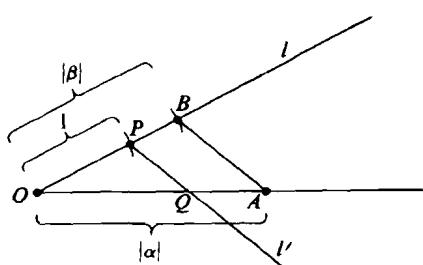


Figura 39.3

**Corolario** El conjunto de todos los números reales construibles forma un subcampo  $F$  del campo de los números reales.

**Demostración** La demostración de este corolario es inmediata del teorema 39.1. ■

Es claro que el campo  $F$  de todos los números reales construibles contiene  $\mathbb{Q}$ , el campo de los números racionales, pues  $\mathbb{Q}$  es el menor subcampo de  $\mathbb{R}$ .

De ahora en adelante procederemos en forma analítica. Podemos construir cualquier número racional. Si consideramos nuestro segmento dado

$$0 \rule{1cm}{0.4pt} 1$$

de longitud 1 como la unidad básica sobre el eje  $x$ , podemos localizar cualquier punto  $(q_1, q_2)$  en el plano, con ambas coordenadas racionales. Cualquier otro punto en el plano que podamos localizar usando regla y compás, puede hallarse en una de las tres maneras siguientes:

- 1 como intersección de dos rectas, cada una de las cuales pasa por dos puntos conocidos con coordenadas racionales;
- 2 como intersección de una recta que pasa por dos puntos con coordenadas racionales y un círculo cuyo centro tiene coordenadas racionales y el cuadrado de su radio es racional;
- 3 como intersección de dos círculos cuyos centros tienen coordenadas racionales y los cuadrados de sus radios son racionales.

Las ecuaciones de las rectas y círculos de los tipos discutidos en 1, 2 y 3 son de la forma

$$ax + by + c = 0$$

y

$$x^2 + y^2 + dx + ey + f = 0,$$

donde  $a, b, c, d, e$  y  $f$  están, todos, en  $\mathbb{Q}$ . Como en el caso 3, la intersección de dos círculos con ecuaciones

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$

y

$$x^2 + y^2 + d_2x + e_2y + f_2 = 0$$

es lo mismo que la intersección del primer círculo, con ecuación

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0,$$

y la recta (la cuerda común), con ecuación

$$(d_1 - d_2)x + (e_1 - e_2)y + f_1 - f_2 = 0,$$

es claro que el caso 3 se puede reducir al caso 2. Para el caso 1, una solución simultánea de dos ecuaciones lineales con coeficientes racionales sólo puede dar valores racionales de  $x$  y  $y$ , con lo cual no se obtienen puntos nuevos. Sin embargo, la búsqueda de una solución simultánea de una ecuación lineal con coeficientes racionales y una ecuación cuadrática con coeficientes racionales, como en el caso 2, conduce, mediante sustitución, a una ecuación cuadrática. Dicha ecuación, resuelta mediante la fórmula cuadrática, puede tener soluciones con raíces cuadradas de números que no sean cuadrados en  $\mathbb{Q}$ .

En el razonamiento anterior, en realidad no se usó  $\mathbb{Q}$  excepto por los axiomas de campo. Si  $H$  es el menor campo que contiene esos números reales construidos hasta ahora, el razonamiento muestra que el «nuevo número siguiente» construido está en un campo  $H(\sqrt{\alpha})$  para alguna  $\alpha \in H$ , donde  $\alpha > 0$ . Hemos probado la mitad del siguiente teorema

**Teorema 39.2** *El campo  $F$  de los números reales construibles, consta, precisamente, de todos los números reales que podemos obtener de  $\mathbb{Q}$ , tomando raíces cuadradas de números positivos un número finito de veces y aplicando un número finito de operaciones de campo.*

**Demostración** Hemos mostrado que  $F$  no puede contener más números que aquéllos obtenidos de  $\mathbb{Q}$ , tomando un número finito de raíces cuadradas de números positivos y aplicando un número finito de operaciones de campo. Sin embargo, si  $\alpha > 0$  es construible, entonces la figura 39.4 muestra que  $\sqrt{\alpha}$  también es construible. Sea  $\overline{OA}$  de longitud  $\alpha$ , localícese  $P$  en la extensión de  $\overline{OA}$  de modo que  $\overline{OP}$  tenga longitud 1. Encuéntrese el punto medio de  $\overline{PA}$  y trácese un semicírculo con diámetro  $\overline{PA}$ . Levántese una perpendicular a  $\overline{PA}$  en  $O$  que interseque al semicírculo en  $Q$ . Entonces, los triángulos  $OPQ$  y  $OQA$  son semejantes, de modo que

$$\frac{|OQ|}{|OA|} = \frac{|OP|}{|OQ|},$$

y  $|OQ|^2 = 1\alpha = \alpha$ . Así,  $\overline{OQ}$  es de longitud  $\sqrt{\alpha}$ . Por tanto, las raíces cuadradas de números construibles son construibles.

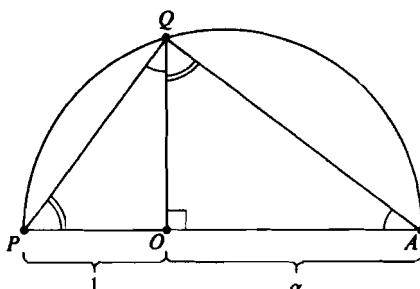


Figura 39.4

El teorema 39.1 mostró que las operaciones de campo son posibles por construcción. ■

**Corolario** Si  $\gamma$  es construible y  $\gamma \notin \mathbb{Q}$ , entonces existe una sucesión finita de números reales  $\alpha_1, \dots, \alpha_n = \gamma$  tal que  $\mathbb{Q}(\alpha_1, \dots, \alpha_i)$  es una extensión de  $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$  de grado 2. En particular,  $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$  para algún entero  $r \geq 0$ .

**Demostración** La existencia de las  $\alpha_i$  se sigue de inmediato del teorema 39.2. Entonces, por el teorema 38.2.

$$\begin{aligned} 2^n &= [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}], \end{aligned}$$

lo cual completa la demostración. ■

Esperamos que se comprenda que las ideas anteriores, aunque algo complicadas para escribir en detalle, son en realidad muy sencillas.

## \*39.2 IMPOSIBILIDAD DE CIERTAS CONSTRUCCIONES

Podemos demostrar, ahora, la imposibilidad de ciertas construcciones geométricas.

**Teorema 9.3** «Es imposible duplicar el cubo», esto es, dado el lado de un cubo, no siempre es posible construir con regla y compás el lado de un cubo que tenga el doble del volumen del cubo original.

**Demostración** Sea el cubo dado de lado 1 y, por tanto, de volumen 1. El cubo buscado debe tener volumen 2 y, por tanto, lado de longitud  $\sqrt[3]{2}$ . Pero  $\sqrt[3]{2}$  es un cero del irreducible  $x^3 - 2$  sobre  $\mathbb{Q}$ , de modo que

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

El corolario del teorema 39.2 muestra que para doblar este cubo de volumen 1, necesitaríamos que para algún entero  $r$ ,  $3 = 2^r$ . Es claro que no existe dicha  $r$ . ■

**Teorema 39.4** «Es imposible cuadrar el círculo» esto es, dado un círculo, no siempre es posible construir con regla y compás un cuadrado que tenga área igual al área del círculo dado.

*Demostración* Sea el círculo dado de radio 1 y, por tanto, de área  $\pi$ . Necesitaríamos construir un cuadrado de lado  $\sqrt{\pi}$ . Pero  $\pi$  es trascendente sobre  $\mathbb{Q}$ , de modo que también  $\sqrt{\pi}$  es trascendente sobre  $\mathbb{Q}$ . ■

**Teorema 39.5** «Es imposible trisecar el ángulo», esto es, existe algún ángulo que no puede trisecarse con regla y compás.

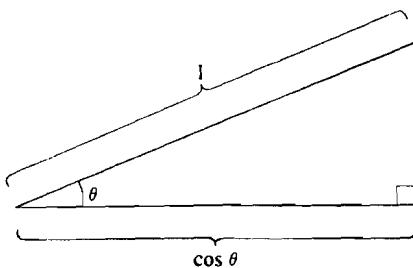


Figura 39.5

*Demostración* La figura 39.5 indica que el ángulo  $\theta$  puede construirse si y sólo si puede construirse un segmento de longitud  $|\cos \theta|$ . Ahora bien, el ángulo de  $60^\circ$  puede construirse y mostraremos que no puede trisecarse. Nótese que

$$\begin{aligned}\cos 3\theta &= \cos(2\theta + \theta) \\ &= \cos 2\theta \cos \theta - \sin 2\theta \sin \theta \\ &= (2\cos^2 \theta - 1)\cos \theta - 2\sin \theta \cos \theta \sin \theta \\ &= (2\cos^2 \theta - 1)\cos \theta - 2\cos \theta(1 - \cos^2 \theta) \\ &= 4\cos^3 \theta - 3\cos \theta.\end{aligned}$$

Sea  $\theta = 20^\circ$  de modo que  $\cos 3\theta = \frac{1}{2}$  y sea  $\alpha = \cos 20^\circ$ . De nuestra identidad  $4\cos^3 \theta - 3\cos \theta = \cos 3\theta$  vemos que

$$4x^3 - 3x = \frac{1}{2}.$$

Así,  $\alpha$  es un cero de  $8x^3 - 6x - 1$ . Este polinomio es irreducible en  $\mathbb{Q}[x]$ , pues, por el teorema 31.3, basta mostrar que no se factoriza en  $\mathbb{Z}[x]$ . Pero una factorización en  $\mathbb{Z}[x]$  incorporaría un factor lineal de la forma  $(8x \pm 1)$ ,  $(4x \pm 1)$ ,  $(2x \pm 1)$  o  $(x \pm 1)$ . Podemos corroborar con facilidad que ninguno de los números  $\pm \frac{1}{8}, \pm \frac{1}{4}, \pm \frac{1}{2}$  y  $\pm 1$  es un cero de  $8x^3 - 6x - 1$ . Así,

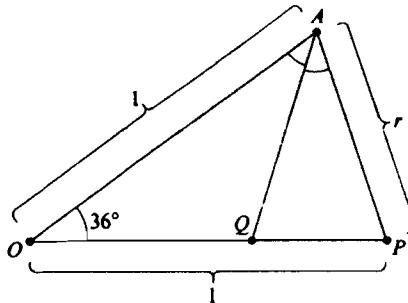
$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3,$$

de modo que, por el corolario del teorema 39.2,  $\alpha$  no es construible. Por tanto,  $60^\circ$  no se puede trisecar. ■

Nótese que el  $n$ -gono regular es construible para  $n \geq 3$ , si y sólo si el ángulo  $2\pi/n$  es construible, lo cual es el caso si y sólo si es construible un segmento de recta de longitud  $\cos(2\pi/n)$ . En el capítulo 48, regresaremos al estudio de la constructibilidad de ciertos  $n$ -gonos regulares.

## Ejercicios

- \*39.1 Usando el teorema 39.5, muéstrese que el 9-gono regular no es construible.
- \*39.2 Muéstrese algebraicamente que es posible construir un ángulo de  $30^\circ$ .
- \*39.3 Con referencia a la figura 39.6, donde  $\overline{AQ}$  biseca al ángulo  $OAP$ , muéstrese que el 10-gono regular es construible (y por tanto, que también lo es el pentágono regular). [Sugerencia: el triángulo  $OAP$  es semejante al triángulo  $APQ$ . Muéstrese algebraicamente que  $r$  es construible.]



**Figura 39.6**

- \*39.4 Usando los resultados del ejercicio 39.3 donde sea necesario, muéstrese que lo siguiente es cierto.

- El 20-gono regular es construible.
- El 30-gono regular es construible.
- El ángulo  $72^\circ$  se puede trisecar.
- El 15-gono regular se puede construir.

- \*39.5 ¿Falso o verdadero?

- Es imposible doblar, con regla y compás, ningún cubo de arista construible.
- Es imposible doblar, con regla y compás, cualquier cubo de arista construible.
- Es imposible cuadrar, con regla y compás, ningún círculo de radio construible.
- Ningún ángulo construible puede trisecarse con regla y compás.
- Todo número construible es de grado  $2^r$  sobre  $Q$  para algún entero  $r \geq 0$ .
- Hemos demostrado que todo número real de grado  $2^r$  sobre  $Q$  para algún entero  $r \geq 0$ , es construible.
- El hecho de que  $\mathbb{Z}$  es un DFU se usó fuertemente en la conclusión de los teoremas 39.3 y 39.5.

- h) Los razonamientos de conteo son herramientas matemáticas muy poderosas.
- i) Es posible encontrar cualquier número construible en un número finito de pasos, comenzando con un segmento dado de longitud unitaria y usando regla y compás.
- j) Es posible encontrar la totalidad de todos los números construibles en un número finito de pasos, comenzando con un segmento dado de longitud unitaria y usando regla y compás.

# Automorfismos de campos

## 40.1. ISOMORFISMOS BASICOS DE LA TEORIA DE LOS CAMPOS ALGEBRAICOS

Sea  $F$  un campo y  $\bar{F}$  una cerradura algebraica de  $F$ , esto es, una extensión algebraica de  $F$  que sea cerrada algebraicamente. Por el teorema 38.6, existen dichos campos  $\bar{F}$ . La selección de una  $\bar{F}$  particular no es crítica, pues, como demostraremos en el capítulo 41, cualesquiera dos cerraduras algebraicas de  $F$  son isomorfas bajo una transformación que deja fijo  $F$ . *De ahora en adelante, en nuestro trabajo, supondremos que todas las extensiones algebraicas y todos los elementos algebraicos sobre un campo  $F$  bajo consideración, están contenidos en una cerradura algebraica fija  $\bar{F}$  de  $F$ .*

Recuérdese que estamos en el estudio de ceros de polinomios. En la terminología del capítulo 38, estudiar ceros de polinomios en  $F[x]$  significa estudiar la estructura de extensiones algebraicas de  $F$  y de elementos algebraicos sobre  $F$ . Mostraremos que si  $E$  es una extensión algebraica de  $F$  con  $\alpha, \beta \in E$ , entonces  $\alpha$  y  $\beta$  tienen las mismas propiedades algebraicas si y sólo si  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ . Reescribiremos este hecho en términos de transformaciones, como lo hemos hecho con la teoría de campos. Lograremos esto mostrando la existencia de un isomorfismo  $\psi_{\alpha, \beta}$  de  $F(\alpha)$  sobre  $F(\beta)$  que transforme a cada elemento de  $F$  sobre sí mismo y transforme  $\alpha$  en  $\beta$ , en el caso de que  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ . El siguiente teorema exhibe este isomorfismo  $\psi_{\alpha, \beta}$ . Estos isomorfismos serán nuestras herramientas fundamentales para el estudio de extensiones algebraicas; sustituirán a los *homomorfismos de evaluación*  $\phi_\alpha$  del capítulo 30, que harán su última colaboración al definir estos isomorfismos. Por esta razón, nos referiremos al isomorfismo  $\psi_{\alpha, \beta}$  como un *isomorfismo básico de la teoría de los campos algebraicos*. Antes de enunciar y probar este teorema, veamos un poco más de terminología.

**Definición** Sea  $E$  una extensión algebraica de un campo  $F$ . Dos elementos  $\alpha, \beta \in E$  son *conjugados sobre  $F$*  si  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ , esto es, si  $\alpha$  y  $\beta$  son ceros del mismo polinomio irreducible sobre  $F$ .

**Ejemplo 40.1** El concepto de elementos conjugados, recién definido, concuerda con la idea clásica de *números complejos conjugados* si entendemos que números complejos conjugados significa que son *conjugados sobre  $\mathbb{R}$* . Si  $a, b \in \mathbb{R}$  y  $b \neq 0$ , los números complejos conjugados  $a + bi$  y  $a - bi$  son, ambos, ceros de  $x^2 - 2ax + a^2 + b^2$  que es irreducible en  $\mathbb{R}[x]$ . ■

**Teorema 40.1 (Isomorfismos básicos de la teoría de campos algebraicos)**

Sea  $F$  un campo y  $\alpha$  y  $\beta$  algebraicos sobre  $F$  con  $\text{grad}(\alpha, F) = n$ . La transformación  $\psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta)$  definida por

$$(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})\psi_{\alpha, \beta} = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$$

para  $c_i \in F$  es un isomorfismo de  $F(\alpha)$  sobre  $F(\beta)$  si y sólo si  $\alpha$  y  $\beta$  son conjugados sobre  $F$ .

**Demostración** Supóngase que  $\psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta)$ , según se definió en el enunciado del teorema, es un isomorfismo. Sea  $\text{irr}(\alpha, F) = a_0 + a_1x + \cdots + a_nx^n$ . Entonces,  $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$  de modo que

$$(a_0 + a_1\alpha + \cdots + a_n\alpha^n)\psi_{\alpha, \beta} = a_0 + a_1\beta + \cdots + a_n\beta^n = 0.$$

Por la última afirmación del enunciado del teorema 35.3, esto implica que  $\text{irr}(\beta, F)$  divide  $\text{irr}(\alpha, F)$ . Un razonamiento análogo, usando el isomorfismo  $(\psi_{\alpha, \beta})^{-1} = \psi_{\beta, \alpha}$  muestra que  $\text{irr}(\alpha, F)$  divide  $\text{irr}(\beta, F)$ . Por tanto, como ambos polinomios son monómicos,  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ , de modo que  $\alpha$  y  $\beta$  son conjugados sobre  $F$ .

En forma recíproca, supóngase que  $\text{irr}(\alpha, F) = \text{irr}(\beta, F) = p(x)$ . Entonces, los homomorfismos de evaluación  $\phi_{\alpha}: F[x] \rightarrow F(\alpha)$  y  $\phi_{\beta}: F[x] \rightarrow F(\beta)$  tienen, ambos, el mismo kernel  $\langle p(x) \rangle$ . Por el teorema 29.3, existe un isomorfismo natural  $\psi_{\alpha}$  correspondiente a  $\phi_{\alpha}: F[x] \rightarrow F(\alpha)$ , que transforma  $F[x]/\langle p(x) \rangle$  sobre  $(F[x])\phi_{\alpha} = F(\alpha)$ . De manera análoga,  $\phi_{\beta}$  da lugar a un isomorfismo  $\psi_{\beta}$  que transforma  $F[x]/\langle p(x) \rangle$  sobre  $F(\beta)$ . Sea  $\psi_{\alpha, \beta} = (\psi_{\alpha})^{-1}\psi_{\beta}$ . Estas transformaciones están diagramadas en la figura 40.1, donde las líneas punteadas indican elementos correspondientes bajo las transformaciones. Como composición de dos isomorfismos,  $\psi_{\alpha, \beta}$  es de nuevo un isomorfismo y transforma  $F(\alpha)$  sobre  $F(\beta)$ . Además, para  $(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) \in F(\alpha)$ , tenemos que

$$\begin{aligned} (c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})\psi_{\alpha, \beta} &= \\ &= (c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})(\psi_{\alpha}^{-1}\psi_{\beta}) \\ &= [(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) + \langle p(x) \rangle]\psi_{\beta} \\ &= c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}. \end{aligned}$$

Así,  $\psi_{\alpha, \beta}$  es la transformación definida en el enunciado del teorema. ■

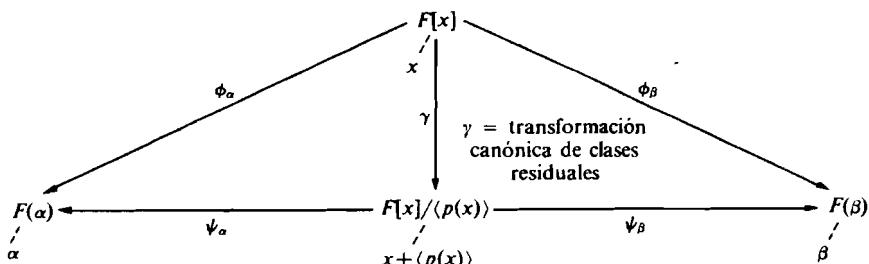


Figura 40.1

El siguiente corolario del teorema 40.1 es la piedra angular de la demostración del importante teorema de la extensión del isomorfismo del capítulo 41 y de la mayor parte de lo que resta de nuestro trabajo.

**Corolario 1** *Sea  $\alpha$  algebraico sobre un campo  $F$ . Todo isomorfismo  $\psi$  que transforme  $F(\alpha)$  en  $F$  tal que  $a\psi = a$  para  $a \in F$ , transforma  $\alpha$  sobre un conjugado  $\beta$  de  $\alpha$  sobre  $F$ . En forma reciproca, para cada conjugado  $\beta$  de  $\alpha$  sobre  $F$ , existe precisamente un isomorfismo  $\psi_{\alpha,\beta}$  de  $F(\alpha)$  en  $F$  que transforma  $\alpha$  en  $\beta$  y transforma cada  $a \in F$  en si misma.*

**Demostración** Sea  $\psi$  un isomorfismo que transforma  $F(\alpha)$  en  $F$  tal que  $a\psi = a$  para  $a \in F$ . Sea  $\text{irr}(\alpha, F) = a_0 + a_1x + \cdots + a_nx^n$ . Entonces,

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

de modo que

$$0 = (a_0 + a_1\alpha + \cdots + a_n\alpha^n)\psi = a_0 + a_1(\alpha\psi) + \cdots + a_n(\alpha\psi)^n,$$

y  $\beta = \alpha\psi$  es un conjugado de  $\alpha$ .

En forma reciproca, para cada conjugado  $\beta$  de  $\alpha$  sobre  $F$ , el isomorfismo  $\psi_{\alpha,\beta}$  del teorema 40.1, es un isomorfismo con las propiedades deseadas. Que  $\psi_{\alpha,\beta}$  sea el único de dichos isomorfismos, se sigue del hecho de que un isomorfismo de  $F(\alpha)$  está por completo determinado por sus valores en los elementos de  $F$  y su valor en  $\alpha$ . ■

Como segundo corolario del teorema 40.1, podemos probar un resultado que con seguridad el lector ya conoce.

**Corolario 2** *Sea  $f(x) \in \mathbb{R}[x]$ . Si  $f(a + bi) = 0$  para  $(a + bi) \in \mathbb{C}$ , donde  $a, b \in \mathbb{R}$ , entonces, también,  $f(a - bi) = 0$ . De manera informal, los ceros complejos de polinomios con coeficientes reales se dan en parejas conjugadas.*

*Demostración* Hemos visto que  $\mathbf{C} = \mathbf{R}(i)$  y que, por supuesto, también  $\mathbf{C} = \mathbf{R}(-i)$ . Ahora,

$$\text{irr}(i, \mathbf{R}) = \text{irr}(-i, \mathbf{R}) = x^2 + 1,$$

de modo que  $i$  y  $-i$  son conjugados sobre  $\mathbf{R}$ . Por el teorema 40.1, la transformación  $\psi_{i, -i}: \mathbf{C} \rightarrow \mathbf{C}$  dada por  $(a + bi)\psi_{i, -i} = a - bi$  es un isomorfismo. Así, si para  $a_i \in \mathbf{R}$ ,

$$f(a + bi) = a_0 + a_1(a + bi) + \cdots + a_n(a + bi)^n = 0,$$

entonces

$$\begin{aligned} 0 &= (f(a + bi))\psi_{i, -i} = a_0 + a_1(a - bi) + \cdots + a_n(a - bi)^n \\ &= f(a - bi), \end{aligned}$$

esto es, también  $f(a - bi) = 0$ . ■

**Ejemplo 40.2** Considérese  $\mathbf{Q}(\sqrt{2})$  sobre  $\mathbf{Q}$ . Los ceros de  $\text{irr}(\sqrt{2}, \mathbf{Q}) = x^2 - 2$  son  $\sqrt{2}$  y  $-\sqrt{2}$ , de modo que  $\sqrt{2}$  y  $-\sqrt{2}$  son conjugados sobre  $\mathbf{Q}$ . De acuerdo con el teorema 40.1, la transformación  $\psi_{\sqrt{2}, -\sqrt{2}}: \mathbf{Q}(\sqrt{2}) \rightarrow \mathbf{Q}(\sqrt{2})$  definida por

$$(a + b\sqrt{2})\psi_{\sqrt{2}, -\sqrt{2}} = a - b\sqrt{2}$$

es un isomorfismo de  $\mathbf{Q}(\sqrt{2})$  sobre sí mismo. ■

## 40.2 AUTOMORFISMOS Y CAMPOS FIJOS

Como se ilustró en el corolario y el ejemplo anteriores, un campo puede tener un isomorfismo no trivial sobre sí mismo. *Dicha transformación será de la mayor importancia en el trabajo que sigue.*

**Definición** Un isomorfismo de un campo sobre sí mismo es un *automorfismo del campo*.

**Definición** Si  $\sigma$  es un isomorfismo de un campo  $E$  en algún campo, entonces un elemento  $a$  de  $E$  queda *fijo bajo*  $\sigma$  si  $a\sigma = a$ . Una colección  $S$  de isomorfismos de  $E$  *deja fijo un subcampo*  $F$  de  $E$  si cada  $a \in F$  queda fijo bajo toda  $\sigma \in S$ . Si  $\{\sigma\}$  deja fijo  $F$ , entonces  $\sigma$  *deja fijo*  $F$ .

Nuestro propósito es estudiar la estructura de una extensión algebraica  $E$  de un campo  $F$ , mediante el estudio de los automorfismos de  $E$  que dejan fijo a cada

elemento de  $F$ . Mostraremos ahora que estos automorfismos forman un grupo de manera natural. Podremos, entonces, aplicar los resultados de la parte I acerca de la estructura de grupo para obtener información sobre la estructura de nuestro campo de extensión. De esta manera, se conjuntará buena parte del trabajo anterior. Los tres teoremas siguientes son fáciles de demostrar, sin embargo, las ideas que contienen constituyen la base de todo lo que sigue. Por tanto, estos teoremas son de gran importancia. Quizá sean observaciones más que teoremas; lo importante son las *ideas* que contienen. En matemáticas, un gran paso no siempre consiste en probar un teorema *fuerte*, sino que muchas veces radica en cómo relacionar ciertas matemáticas conocidas con situaciones nuevas. Aquí traemos la teoría de grupos al estudio de ceros de polinomios. El estudiante debe asegurarse de comprender los conceptos presentados. Aunque parezca poco probable, son la clave para la solución del *objetivo final* del texto.

*Objetivo final (a enunciar de manera precisa más adelante): mostrar que no todos los ceros de todo polinomio quintico (de grado 5)  $f(x)$  puede expresarse en términos de radicales comenzando con elementos en el campo de coeficientes de  $f(x)$ .*

Si  $\{\sigma_i \mid i \in I\}$  es una colección de automorfismos de un campo  $E$ , los elementos de  $E$  acerca de los cuales  $\{\sigma_i \mid i \in I\}$  da la menor información, son aquellos  $a \in E$  que quedan fijos bajo toda  $\sigma_i$  para  $i \in I$ . El primero de los tres teoremas contiene casi todo lo que puede decidirse acerca de estos elementos fijos de  $E$ .

**Teorema 40.2** *Sea  $\{\sigma_i \mid i \in I\}$  una colección de automorfismos de un campo  $E$ . Entonces, el conjunto  $E_{\{\sigma_i\}}$  de todos los  $a \in E$  que quedan fijos bajo toda  $\sigma_i$  para  $i \in I$ , forma un subcampo de  $E$ .*

**Demostración** Si  $a\sigma_i = a$  y  $b\sigma_i = b$  para todas las  $i \in I$ , entonces,

$$(a \pm b)\sigma_i = a\sigma_i \pm b\sigma_i = a \pm b$$

y

$$(ab)\sigma_i = (a\sigma_i)(b\sigma_i) = ab$$

para todas las  $i \in I$ . Además, si  $b \neq 0$ , entonces

$$(a/b)\sigma_i = (a\sigma_i)/(b\sigma_i) = a/b$$

para todas las  $i \in I$ . Como los  $\sigma_i$  son automorfismos, tenemos

$$0\sigma_i = 0 \quad \text{y} \quad 1\sigma_i = 1$$

para todas las  $i \in I$ . De aquí,  $0, 1 \in E_{\{\sigma_i\}}$ . Así,  $E_{\{\sigma_i\}}$  es un subcampo de  $E$ . ■

**Definición** El campo  $E_{\{\sigma_i\}}$  del teorema 40.2 es el *campo fijo de  $\{\sigma_i \mid i \in I\}$* . Para un solo automorfismo  $\sigma$ , nos referiremos a  $E_{\{\sigma\}}$  como el *campo fijo de  $\sigma$* .

**Ejemplo 40.3** Considérese el automorfismo  $\psi_{\sqrt{2}, -\sqrt{2}}$  de  $\mathbf{Q}(\sqrt{2})$  dado en el ejemplo 40.2. Para  $a, b \in \mathbf{Q}$  tenemos

$$(a + b\sqrt{2})\psi_{\sqrt{2}, -\sqrt{2}} = a - b\sqrt{2}$$

y  $a - b\sqrt{2} = a + b\sqrt{2}$  si y sólo si  $b = 0$ . Así, el campo fijo de  $\psi_{\sqrt{2}, -\sqrt{2}}$  es  $\mathbf{Q}$ . ■

Nótese que un automorfismo de un campo  $E$  es, en particular, una transformación uno a uno de  $E$  sobre  $E$ , esto es, una *permutación de  $E$* . Si  $\sigma$  y  $\tau$  son automorfismos de  $E$ , entonces la permutación  $\sigma\tau$  es, de nuevo, un automorfismo de  $E$ , puesto que, en general, la composición de homomorfismos es un homomorfismo. Es así como hace su entrada la teoría de grupos.

**Teorema 40.3** *El conjunto de todos los automorfismos de un campo  $E$  es un grupo bajo la composición de funciones.*

**Demostración** La multiplicación de automorfismos de  $E$  se define por la composición de funciones y, por tanto, es asociativa (*es multiplicación de permutaciones*). La permutación idéntica  $\iota: E \rightarrow E$  dada por  $\iota(x) = x$  para  $x \in E$  es obviamente, un automorfismo de  $E$ . Si  $\sigma$  es un automorfismo, entonces la permutación  $\sigma^{-1}$ , obviamente, también es un automorfismo. Así, todos los automorfismos de  $E$  forman un subgrupo de  $S_E$ , el grupo de todas las permutaciones de  $E$  dado por el teorema 4.1. ■

**Teorema 40.4** *Sea  $E$  un campo y sea  $F$  un subcampo de  $E$ . Entonces, el conjunto  $G(E/F)$  de todos los automorfismos de  $E$  que dejan fijo  $F$  forma un subgrupo del grupo de todos los automorfismos de  $E$ . Más aún,  $F \leq E_{G(E/F)}$ .*

**Demostración** Para  $\sigma, \tau \in G(E/F)$  y  $a \in F$ , tenemos

$$\sigma(\tau(a)) = (\sigma\tau)(a) = a\tau = a,$$

de modo que  $\sigma\tau \in G(E/F)$ . Es claro que el automorfismo identidad  $\iota$  está en  $G(E/F)$ . Además, si  $a\sigma = a$  para  $a \in F$ , entonces  $a = a\sigma^{-1}$ , de modo que  $\sigma \in G(E/F)$  implica que  $\sigma^{-1} \in G(E/F)$ . Así,  $G(E/F)$  es un subgrupo del grupo de todos los automorfismos de  $E$ .

Como todo elemento de  $F$  queda fijo por todo elemento de  $G(E/F)$ , se sigue de inmediato que el campo  $E_{G(E/F)}$  de todos los elementos de  $E$  que quedan fijos bajo  $G(E/F)$  contienen  $F$ . ■

**Definición** El grupo  $G(E/F)$  del teorema anterior es el *grupo de automorfismos de  $E$  que dejan fijo  $F$* , o, brevemente, el *grupo de  $E$  sobre  $F$* .

No hay que pensar que  $E/F$  denota algún tipo de espacio cociente, sino que significa que  $E$  es el campo de extensión de algún campo  $F$ .

Las ideas contenidas en los tres teoremas anteriores se ilustran en el ejemplo siguiente. Pedimos se estudie con cuidado este ejemplo.

**Ejemplo 40.4** Considérese el campo  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ . Si consideramos  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  como  $(\mathbf{Q}(\sqrt{3}))(\sqrt{2})$ , el isomorfismo básico  $\psi_{\sqrt{2}, -\sqrt{2}}$  del teorema 40.1, definido por

$$(a + b\sqrt{2})\psi_{\sqrt{2}, -\sqrt{2}} = a - b\sqrt{2}$$

para  $a, b \in \mathbf{Q}(\sqrt{3})$  es un automorfismo de  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  que tiene  $\mathbf{Q}(\sqrt{3})$  como campo fijo. En forma análoga, tenemos el automorfismo  $\psi_{\sqrt{3}, -\sqrt{3}}$  de  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  que tiene como campo fijo  $\mathbf{Q}(\sqrt{2})$ . Como el producto de dos automorfismos es un automorfismo, podemos considerar  $\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}$ , el cual mueve tanto a  $\sqrt{2}$  como a  $\sqrt{3}$ , esto es, no deja fijo ninguno de los dos números. Sea

$\iota$  = automorfismo identidad,

$$\sigma_1 = \psi_{\sqrt{2}, -\sqrt{2}},$$

$$\sigma_2 = \psi_{\sqrt{3}, -\sqrt{3}} \text{ y}$$

$$\sigma_3 = \psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}.$$

El grupo de todos los automorfismos de  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  tiene, por el teorema 40.2, un campo fijo. Este campo fijo debe contener  $\mathbf{Q}$  puesto que todo automorfismo de un campo deja fijo al 1 y, por tanto, al subcampo primo. Una base para  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbf{Q}$  es  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ . Como  $\sqrt{2}\sigma_1 = -\sqrt{2}, \sqrt{6}\sigma_1 = -\sqrt{6}$  y  $\sqrt{3}\sigma_2 = -\sqrt{3}$ , vemos que  $\mathbf{Q}$  es precisamente el campo fijo de  $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$ . Se ve con facilidad que  $G = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$  es un grupo bajo la multiplicación de automorfismos (composición de funciones). La tabla de grupo para  $G$  se da en la tabla 40.1. Por ejemplo,

$$\sigma_1\sigma_3 = \psi_{\sqrt{2}, -\sqrt{2}}(\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}) = \psi_{\sqrt{3}, -\sqrt{3}} = \sigma_2.$$

**Tabla 40.1**

	$\iota$	$\sigma_1$	$\sigma_2$	$\sigma_3$
$\iota$	$\iota$	$\sigma_1$	$\sigma_2$	$\sigma_3$
$\sigma_1$	$\sigma_1$	$\iota$	$\sigma_3$	$\sigma_2$
$\sigma_2$	$\sigma_2$	$\sigma_3$	$\iota$	$\sigma_1$
$\sigma_3$	$\sigma_3$	$\sigma_2$	$\sigma_1$	$\iota$

El grupo  $G$  es isomorfo al 4-grupo de Klein. Podemos mostrar que  $G$  es exactamente el grupo  $G(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$ , pues, por el corolario 1 del teorema 40.1, todo

automorfismo  $\tau$  de  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  transforma  $\sqrt{2}$  sobre alguno de  $\pm\sqrt{2}$ . De manera análoga,  $\tau$  transforma  $\sqrt{3}$  sobre alguno de  $\pm\sqrt{3}$ . Pero como  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$  es una base para  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbf{Q}$ , un automorfismo de  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$  que deje fijo  $\mathbf{Q}$  está determinado por sus valores en  $\sqrt{2}$  y  $\sqrt{3}$ . Es claro que  $\iota$ ,  $\sigma_1$ ,  $\sigma_2$  y  $\sigma_3$  dan, entonces, todas las posibles combinaciones de los valores en  $\sqrt{2}$  y  $\sqrt{3}$ , y, por tanto, son todos los automorfismos posibles de  $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ .

Nótese que  $G(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$  tiene orden 4, y que  $[\mathbf{Q}(\sqrt{2}, \sqrt{3}):\mathbf{Q}] = 4$ . *Esto no es un accidente*, sino un ejemplo de una situación bastante general, como lo veremos más adelante. ■

## 40.3 EL AUTOMORFISMO DE FROBENIUS

Sea  $F$  un campo finito. Mostraremos más adelante que el grupo de todos los automorfismos de  $F$  es cíclico. Por definición, un grupo cíclico tiene un elemento generador y puede tener varios elementos generadores. Para un grupo cíclico abstracto no hay manera de decir que un generador es más importante que cualquier otro. Sin embargo, para el grupo cíclico de todos los automorfismos de un campo finito, existe un generador canónico (natural), el automorfismo de Frobenius (clásicamente, la *sustitución de Frobenius*). Este hecho es de importancia considerable en parte del trabajo avanzado de álgebra. El siguiente teorema exhibe este automorfismo de Frobenius.

**Teorema 40.5** *Sea  $F$  un campo finito de característica  $p$ . Entonces, la transformación  $\sigma_p: F \rightarrow F$  definida por  $a\sigma_p = a^p$  para  $a \in F$  es un automorfismo, el automorfismo de Frobenius de  $F$ . Además,  $F_{\{\sigma_p\}} \simeq \mathbf{Z}_p$ .*

**Demostración** Sea  $a, b \in F$ . Aplicando el teorema del binomio  $(a + b)^p$ , tenemos

$$\begin{aligned}(a + b)^p &= a^p + (p \cdot 1)a^{p-1}b + \left(\frac{p(p-1)}{2} \cdot 1\right)a^{p-2}b^2 + \\&\quad + \cdots + (p \cdot 1)ab^{p-1} + b^p \\&= a^p + 0a^{p-1}b + 0a^{p-2}b^2 + \cdots + 0ab^{p-1} + b^p \\&= a^p + b^p.\end{aligned}$$

Tenemos, así,

$$(a + b)\sigma_p = (a + b)^p = a^p + b^p = a\sigma_p + b\sigma_p.$$

Por supuesto,

$$(ab)\sigma_p = (ab)^p = a^pb^p = (a\sigma_p)(b\sigma_p),$$

de modo que  $\sigma_p$  es al menos un homomorfismo. Si  $a\sigma_p = 0$ , entonces  $a^p = 0$  y  $a = 0$  de manera que el kernel de  $\sigma_p$  es  $\{0\}$  y  $\sigma_p$  es una transformación isomorfa. Por último, como  $F$  es finito, contando,  $\sigma_p$  es sobre. Así,  $\sigma_p$  es un automorfismo de  $F$ .

El campo primo  $\mathbf{Z}_p$  debe estar contenido (salvo isomorfismo) en  $F$ , puesto que  $F$  es de característica  $p$ . Por el teorema de Fermat, para  $c \in \mathbf{Z}_p$ , tenemos  $c\sigma_p = c^p = c$  (véase el corolario del teorema 24.6). Así, el polinomio  $x^p - x$  tiene  $p$  ceros en  $F$ , a saber, los elementos de  $\mathbf{Z}_p$ . Por el corolario 2 del teorema 31.1, un polinomio de grado  $n$  sobre un campo, puede tener a lo más  $n$  ceros en el campo. Como los elementos fijos bajo  $\sigma_p$  son precisamente los ceros en  $F$  de  $x^p - x$  vemos que

$$\mathbf{Z}_p = F_{\{\sigma_p\}}. \blacksquare$$

Incluso en los primeros años de universidad, hay estudiantes que cometan el error de decir que  $(a + b)^p = a^p + b^p$ . Vemos, aquí, que esta *exponenciación estudiantil*  $(a + b)^p = a^p + b^p$  con exponente  $p$  es válida, en realidad, en un campo  $F$  de característica  $p$ .

## Ejercicios

---

**40.1** Encuéntrense todos los conjugados de cada uno de los números dados sobre los campos dados.

- |   |   |
|---|---|
| a) $\sqrt{2}$ sobre $\mathbf{Q}$            | b) $\sqrt{2}$ sobre $\mathbf{R}$                      |
| c) $3 + \sqrt{2}$ sobre $\mathbf{Q}$        | d) $\sqrt{2} - \sqrt{3}$ sobre $\mathbf{Q}$           |
| e) $\sqrt{2} + i$ sobre $\mathbf{Q}$        | f) $\sqrt{2} + i$ sobre $\mathbf{R}$                  |
| g) $\sqrt{1 + \sqrt{2}}$ sobre $\mathbf{Q}$ | h) $\sqrt{1 + \sqrt{2}}$ sobre $\mathbf{Q}(\sqrt{2})$ |

**40.2** Considérese el campo  $E = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ . En la notación del teorema 40.1, tenemos los siguientes isomorfismos básicos (que son aquí los automorfismos de  $E$ ):

$$\begin{aligned}\psi_{\sqrt{2}, -\sqrt{2}}: & (\mathbf{Q}(\sqrt{3}, \sqrt{5}))(\sqrt{2}) \rightarrow (\mathbf{Q}(\sqrt{3}, \sqrt{5}))(-\sqrt{2}), \\ \psi_{\sqrt{3}, -\sqrt{3}}: & (\mathbf{Q}(\sqrt{2}, \sqrt{5}))(\sqrt{3}) \rightarrow (\mathbf{Q}(\sqrt{2}, \sqrt{5}))(-\sqrt{3}), \\ \psi_{\sqrt{5}, -\sqrt{5}}: & (\mathbf{Q}(\sqrt{2}, \sqrt{3}))(\sqrt{5}) \rightarrow (\mathbf{Q}(\sqrt{2}, \sqrt{3}))(-\sqrt{5}).\end{aligned}$$

Como notación breve, sea  $\tau_2 = \psi_{\sqrt{2}, -\sqrt{2}}$ ,  $\tau_3 = \psi_{\sqrt{3}, -\sqrt{3}}$  y  $\tau_5 = \psi_{\sqrt{5}, -\sqrt{5}}$ . Calcúlese lo siguiente:

- |   |  |
|---|--|
| a) $\sqrt{3}\tau_2$                               | b) $(\sqrt{2} + \sqrt{5})\tau_2$                                     |
| c) $(\sqrt{2} + 3\sqrt{5})(\tau_2\tau_3)$         | d) $\frac{\sqrt{2} - 3\sqrt{5}}{2\sqrt{3} - \sqrt{2}}(\tau_3\tau_5)$ |
| e) $(\sqrt{2} + \sqrt{45})(\tau_2\tau_3\tau_5^2)$ | f) $[(\sqrt{2} - \sqrt{3})\tau_5 + \sqrt{30}(\tau_5\tau_2)]\tau_3$   |

**40.3** Los campos  $\mathbf{Q}(\sqrt{2})$  y  $\mathbf{Q}(3 + \sqrt{2})$  son los mismos, desde luego. Sea  $\alpha = 3 + \sqrt{2}$ .

- Encuéntrese un conjugado  $\beta \neq \alpha$  de  $\alpha$  sobre  $\mathbf{Q}$ .
- Con respecto a a), compárese el automorfismo básico  $\psi_{\sqrt{2}, -\sqrt{2}}$  de  $\mathbf{Q}(\sqrt{2})$  con el automorfismo básico  $\psi_{\alpha, \beta}$ .

**40.4** Con respecto al ejemplo 40.4, encuéntrense los siguientes campos en  $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ .

a)  $E_{\{\sigma_1, \sigma_3\}}$       b)  $E_{\{\sigma_3\}}$       c)  $E_{\{\sigma_2, \sigma_3\}}$

**40.5** Con respecto al ejercicio 40.2, encuéntrese el campo fijo de cada uno de los siguientes automorfismos o conjuntos de automorfismos de  $E$ .

a)  $\tau_3$       b)  $\tau_3^2$       c)  $\{\tau_2, \tau_3\}$   
 d)  $\tau_2\tau_5$       e)  $\tau_2\tau_3\tau_5$       f)  $\{\tau_2, \tau_3, \tau_5\}$

**40.6** Sea  $x$  algebraico de grado  $n$  sobre  $F$ . Muéstrese, del corolario 1 del teorema 40.1, que hay a lo más  $n$  isomorfismos diferentes de  $F(x)$  en  $\bar{F}$ .

**40.7** ¿Falso o verdadero?

- a) Para todas las  $\alpha, \beta \in E$  hay siempre un automorfismo de  $E$  que transforma  $\alpha$  sobre  $\beta$ .
  - b) Para  $\alpha, \beta$  algebraicos sobre un campo  $F$ , hay siempre un isomorfismo de  $F(\alpha)$  sobre  $F(\beta)$ .
  - c) Para  $\alpha, \beta$  algebraicos y conjugados sobre un campo  $F$ , hay siempre un isomorfismo de  $F(\alpha)$  sobre  $F(\beta)$ .
  - d) Todo automorfismo de todo campo deja fijo a todo elemento del subcampo primo de  $E$ .
  - e) Todo automorfismo de todo campo  $E$  deja fijo a un número infinito de elementos de  $E$ .
  - f) Todo automorfismo de todo campo  $E$  deja fijo al menos dos elementos de  $E$ .
  - g) Todo automorfismo de todo campo  $E$  de característica 0, deja fijo un número infinito de elementos de  $E$ .
  - h) Todos los automorfismos de un campo  $E$  forman grupo bajo la composición de funciones.
  - i) El conjunto de todos los elementos de un campo  $E$  que queda fijo bajo un solo automorfismo de  $E$ , forma un subcampo de  $E$ .
  - j) Para los campos  $F \leq E \leq K$ ,  $G(K/E) \leq G(K/F)$ .
- 

**40.8** Refiérase al ejercicio 40.2 para lo siguiente:

- a) Muéstrese que cada uno de los automorfismos  $\tau_2, \tau_3$  y  $\tau_5$  es de orden 2 en  $G(E/\mathbb{Q})$ . (Recuérdese lo que significa el *orden* de un elemento de un grupo.)
- b) Encuéntrese el subgrupo  $H$  de  $G(E/\mathbb{Q})$  generado por los elementos  $\tau_2, \tau_3$  y  $\tau_5$  y dése la tabla del grupo. [Sugerencia: hay ocho elementos.]
- c) Así como se hizo en el ejemplo 40.4, pruébese que el grupo  $H$  de b) es exactamente el grupo  $G(E/\mathbb{Q})$ .

**40.9** Describase el valor del automorfismo de Frobenius  $\sigma_2$  en cada elemento del campo finito de los cuatro elementos dados en el ejercicio 35.9. Encuéntrese el campo fijo de  $\sigma_2$ .

**40.10** Describase el valor del automorfismo de Frobenius  $\sigma_3$  en cada elemento del campo finito de los nueve elementos dados en el ejercicio 35.7. Encuéntrese el elemento fijo de  $\sigma_3$ .

**40.11** Sea  $F$  un campo de característica  $p \neq 0$ . Dése un ejemplo para mostrar que la transformación  $\sigma_p: F \rightarrow F$  dada por  $a\sigma_p = a^p$  para  $a \in F$  no necesita ser un automorfismo en el caso de que  $F$  sea infinito. ¿Dónde puede haber dificultades?

**40.12** Sea  $F(\alpha_1, \dots, \alpha_n)$  un campo de extensión de  $F$ . Muéstrese que cualquier automorfismo  $\sigma$  de  $F(\alpha_1, \dots, \alpha_n)$  que deje fijo a  $F$  está por completo determinado por los  $n$  valores de  $\alpha_i\sigma$ .

**40.13** Sea  $E$  una extensión algebraica de un campo  $F$  y sea  $\sigma$  un automorfismo de  $E$  que deja fijo a  $F$ . Sea  $\alpha \in E$ . Muéstrese que  $\sigma$  induce una permutación del conjunto de todos los ceros de  $\text{irr}(\alpha, F)$  que están en  $E$ .

**40.14** Sea  $E$  una extensión algebraica de un campo  $F$ . Sea  $S = \{\sigma_i \mid i \in I\}$  una colección de automorfismos de  $E$ , tal que toda  $\sigma_i$  deja fijo cada elemento de  $F$ . Muéstrese que si  $S$  genera el subgrupo  $H$  de  $G(E/F)$ , entonces  $E_S = E_H$ .

**40.15** Vimos en el corolario del teorema 31.4, que el polinomio ciclotómico

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

es irreducible sobre  $\mathbf{Q}$  para todo primo  $p$ . Sea  $\zeta$  un cero de  $\Phi_p(x)$ , considérese el campo  $\mathbf{Q}(\zeta)$ .

- a) Muéstrese que  $\zeta, \zeta^2, \dots, \zeta^{p-1}$  son ceros distintos de  $\Phi_p(x)$  y conclúyase que son todos los ceros de  $\Phi_p(x)$ .
- b) Dedúzcase, del corolario 1 del teorema 40.1 y la parte a) de este ejercicio, que  $G(\mathbf{Q}(\zeta)/\mathbf{Q})$  es abeliano de orden  $p - 1$ .
- c) Muéstrese que el campo fijo de  $G(\mathbf{Q}(\zeta)/\mathbf{Q})$  es  $\mathbf{Q}$ . [Sugerencia: muéstrese que

$$\{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$$

es una base para  $\mathbf{Q}(\zeta)$  sobre  $\mathbf{Q}$  y considérese las combinaciones lineales de  $\zeta, \zeta^2, \dots, \zeta^{p-1}$  quedan fijas bajo todos los elementos de  $G(\mathbf{Q}(\zeta)/\mathbf{Q})$ .]

**40.16** En el teorema 40.1 se describieron los isomorfismos básicos para el caso donde  $\alpha$  y  $\beta$  fueran elementos conjugados algebraicos sobre  $F$ . ¿Existe algún isomorfismo semejante de  $F(\alpha)$  con  $F(\beta)$  en el caso en que  $\alpha$  y  $\beta$  sean ambos trascendentes sobre  $F$ ?

**40.17** Sea  $F$  un campo y  $x$  una indeterminada sobre  $F$ . Determiníense todos los automorfismos de  $F(x)$  que dejan fijo  $F$  describiendo sus valores en  $x$ .

**40.18** Pruébese la siguiente sucesión de teoremas.

- a) Un automorfismo de un campo  $E$  lleva a los elementos que son cuadrados de elementos en  $E$  sobre los elementos que son cuadrados de los elementos de  $E$ .
- b) Un automorfismo del campo  $\mathbf{R}$  de los números reales lleva números positivos sobre números positivos.
- c) Si  $\sigma$  es un automorfismo de  $\mathbf{R}$  y  $a < b$ , donde  $a, b \in \mathbf{R}$ , entonces  $a\sigma < b\sigma$ .
- d) Un automorfismo de  $\mathbf{R}$  está por completo determinado por sus valores en elementos de  $\mathbf{Q}$ .
- e) El único automorfismo de  $\mathbf{R}$  es el automorfismo identidad.

## 41

# El teorema de extensión de isomorfismos

## 41.1 EL TEOREMA DE EXTENSION

Continuemos el estudio de los automorfismos de campos. En este capítulo y en el siguiente, nos ocuparemos tanto de la existencia como del número de automorfismos de un campo  $E$ .

Supongamos que  $E$  es una extensión algebraica de  $F$  y que queremos encontrar algunos automorfismos de  $E$ . Sabemos, del teorema 40.1, que si  $\alpha, \beta \in E$  son conjugados sobre  $F$ , entonces existe un isomorfismo  $\psi_{\alpha, \beta}$  de  $F(\alpha)$  sobre  $F(\beta)$ . Es claro que  $\alpha, \beta \in E$  implica que  $F(\alpha) \leq E$  y  $F(\beta) \leq E$ . Es natural preguntarse si el dominio de definición de  $\psi_{\alpha, \beta}$  se puede extender de  $F(\alpha)$  a un campo más grande, quizás a todo  $E$ , y en qué caso ello conduce a un automorfismo de  $E$ . En la figura 41.1 se muestra un diagrama de transformaciones de esta situación. En lugar de hablar de «extender el dominio de definición de  $\psi_{\alpha, \beta}$ » se acostumbra hablar de «extender la transformación  $\psi_{\alpha, \beta}$  a una transformación  $\tau$ » que sea una transformación de todo  $E$ .

Recuérdese que siempre suponemos que todas las extensiones algebraicas de  $F$  consideradas están contenidas en una cerradura algebraica  $\bar{F}$  de  $F$ . El teorema de la extensión del isomorfismo muestra que, en efecto, la transformación  $\psi_{\alpha, \beta}$  siempre puede extenderse a un isomorfismo de  $E$  en  $\bar{F}$ . En qué caso esta extensión resulta un *automorfismo* de  $E$ , esto es, transforma a  $E$  sobre sí mismo, es una cuestión que trataremos en el capítulo 42. Así, este teorema de extensión, junto con nuestros isomorfismos básicos  $\psi_{\alpha, \beta}$ , garantizará la existencia de multitud de *transformaciones isomórfas*, al menos para muchos campos. Bien puede ser que este teorema sea el único teorema de extensión que se haya visto. Dichos teoremas son muy importantes en matemáticas, particularmente en situaciones algebraicas y topológicas.

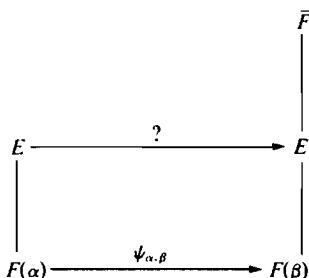


Figura 41.1

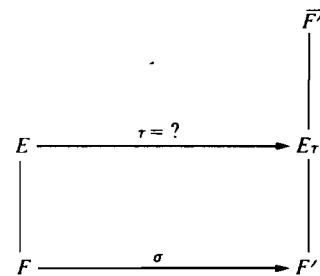


Figura 41.2

Veamos de manera más general esta situación. Supóngase que  $E$  es una extensión algebraica de un campo  $F$  y que tenemos un isomorfismo  $\sigma$  de  $F$  sobre un campo  $F'$ . Sea  $\bar{F}'$  una cerradura algebraica de  $F'$ . Nos gustaría extender  $\sigma$  a un isomorfismo  $\tau$  de  $E$  en  $\bar{F}'$ . Se muestra esta situación en la figura 41.2. De manera intuitiva, tomamos  $\alpha \in E$  pero no en  $F$  y tratamos de extender  $\sigma$  a  $F(\alpha)$ . Si

$$p(x) = \text{irr}(\alpha, F) = a_0 + a_1x + \cdots + a_nx^n,$$

sea  $\beta$  un cero en  $\bar{F}'$  de

$$q(x) = a_0\sigma + (a_1\sigma)x + \cdots + (a_n\sigma)x^n.$$

Aquí,  $q(x) \in F'[x]$ . Como  $\sigma$  es un isomorfismo, es claro que  $q(x)$  es irreducible en  $F'[x]$ . También es bastante claro que  $F(\alpha)$  puede transformarse isomórficamente sobre  $F'(\beta)$ , mediante una transformación que extiende  $\sigma$  y transforma  $\alpha$  sobre  $\beta$ . (Esto no es realmente el teorema 40.1, pero está cerca; unos cuantos elementos han cambiado de nombre bajo el isomorfismo  $\sigma$ .) Si  $F(\alpha) = E$ , hemos terminado. Si  $F(\alpha) \neq E$ , debemos encontrar otro elemento en  $E$  que no esté en  $F(\alpha)$  y continuar el proceso. Es una situación muy parecida a la construcción de una cerradura algebraica  $\bar{F}$  de un campo  $F$ . De nuevo la dificultad es que, en general, cuando  $E$  no es una extensión finita, el proceso puede repetirse un número infinito (quizá grande) de veces, de manera que necesitamos el lema de Zorn para manejar la situación. Por esta razón, damos la demostración general del teorema 41.1 en un párrafo con asterisco, al final de este capítulo.

**Teorema 41.1 (Teorema de la extensión de isomorfismos)** *Sea  $E$  una extensión algebraica de un campo  $F$ . Sea  $\sigma$  un isomorfismo de  $F$  sobre un campo  $F'$ . Sea  $\bar{F}'$  una cerradura algebraica de  $F'$ . Entonces,  $\sigma$  se puede extender a un isomorfismo  $\tau$  de  $E$  en  $\bar{F}'$  tal que  $a\tau = a\sigma$  para todas las  $a \in F$ .*

Damos como corolario la existencia de una extensión de uno de nuestros isomorfismos básicos  $\psi_{\alpha, \beta}$ , como se discutió al principio de esta sección.

**Corolario 1** Si  $E \leq \bar{F}$  es una extensión algebraica de  $F$ , y  $\alpha, \beta \in E$  son conjugadas sobre  $F$ , entonces el isomorfismo básico  $\psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta)$  dado por el teorema 40.1 puede extenderse a un isomorfismo de  $E$  en  $\bar{F}$ .

*Demostración* La demostración de este corolario se sigue de inmediato del teorema 41.1, si en el enunciado del teorema reemplazamos  $F$  por  $F(\alpha)$ ,  $F'$  por  $F(\beta)$  y  $\bar{F}'$  por  $\bar{F}$ . ■

Como otro corolario podemos demostrar, como lo prometimos, que una cerradura algebraica de  $F$  es única, salvo un isomorfismo que deje fijo  $F$ .

**Corolario 2** Sean  $\bar{F}$  y  $\bar{F}'$  dos cerraduras algebraicas de  $\bar{F}$ . Entonces,  $\bar{F}$  es isomorfo a  $\bar{F}'$  bajo un isomorfismo que deja fijo cada elemento de  $F$ .

*Demostración* Por el teorema 41.1, el isomorfismo identidad de  $F$  sobre  $F$  puede extenderse a un isomorfismo  $\tau$  que transforme a  $\bar{F}$  en  $\bar{F}'$ , dejando fijo  $F$  (véase la figura 41.3). Sólo necesitamos mostrar que  $\tau$  es sobre  $\bar{F}'$ . Pero, por el teorema 41.1, la transformación  $\tau^{-1}:\bar{F}\tau \rightarrow \bar{F}$  puede extenderse a un isomorfismo de  $\bar{F}'$  en  $\bar{F}$ . Como  $\tau^{-1}$  ya es sobre  $\bar{F}$ , debemos tener  $\bar{F}\tau = \bar{F}'$ . ■

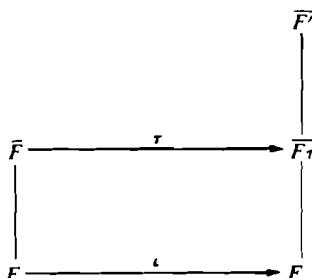


Figura 41.3

## 41.2 INDICE DE UN CAMPO DE EXTENSION

Una vez discutida la cuestión de *existencia*, pasamos a la cuestión de *cuántos*. Nos gustaría contar los isomorfismos que hay de  $E$  en  $\bar{F}$  que dejen fijo  $F$ , para una extensión finita  $E$  de un campo  $F$ . Mostraremos que hay sólo un número finito de dichos isomorfismos. Como todo automorfismo en  $G(E/F)$  es uno de dichos isomorfismos, al contar estos isomorfismos se incluirán todos los automorfismos. El ejemplo 40.4 mostró que  $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$  tiene cuatro elementos y que  $4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}]$ . Mientras que esta igualdad no siempre es cierta, si es cierta en un caso muy importante. El siguiente teorema es el primer gran paso para probarlo. Enunciamos el teorema en términos más generales de lo requerido, pero no por ello se dificulta más la demostración.

**Teorema 41.2** Sea  $E$  una extensión finita de un campo  $F$ . Sea  $\sigma$  un isomorfismo de  $F$  sobre un campo  $F'$  y sea  $\bar{F}'$  una cerradura algebraica de  $F'$ . Entonces, el número de extensiones de  $\sigma$  a un isomorfismo  $\tau$  de  $E$  en  $\bar{F}'$  es finito e independiente de  $F'$ ,  $\bar{F}'$  y  $\sigma$ . Esto es, este número de extensiones está completamente determinado por los dos campos  $E$  y  $F$ ; es intrínseco a ellos.

**Demostración** El diagrama de la figura 41.4 puede ayudarles a seguir la construcción que haremos. El diagrama se construye de la siguiente manera.

$$\begin{array}{ccccc}
 \bar{F}'_1 & \xrightarrow{\lambda} & \bar{F}'_2 \\
 \downarrow & \text{Extiende } \sigma_1^{-1}\sigma_2 & \downarrow \\
 E_{\tau_1} & \xleftarrow{\tau_1} & E & \xrightarrow{\tau_2} & E_{\tau_2} \\
 \downarrow & & \downarrow & (\alpha\tau_2 = \alpha\tau_1\lambda) & \downarrow \\
 F'_1 & \xleftarrow{\sigma_1} & F & \xrightarrow{\sigma_2} & F'_2
 \end{array}$$

Figura 41.4

Considérense dos isomorfismos

$$\sigma_1: F \xrightarrow{\text{sobre}} F'_1, \quad \sigma_2: F \xrightarrow{\text{sobre}} F'_2,$$

donde  $\bar{F}'_1$  y  $\bar{F}'_2$  son cerraduras algebraicas de  $F'_1$  y  $F'_2$ , respectivamente. Ahora,  $\sigma_1^{-1}\sigma_2$  es un isomorfismo de  $F'_1$  sobre  $F'_2$ . Entonces, por el teorema 41.1 y su segundo corolario, existe un isomorfismo

$$\lambda: \bar{F}'_1 \xrightarrow{\text{sobre}} \bar{F}'_2$$

que extiende este isomorfismo  $\sigma_1^{-1}\sigma_2: F'_1 \xrightarrow{\text{sobre}} F'_2$ . Con referencia a la figura 41.4, por cada  $\tau_1: E \rightarrow \bar{F}'_1$  que extiende  $\sigma_1$ , se obtiene un isomorfismo  $\tau_2: E \rightarrow \bar{F}'_2$ , comenzando en  $E$  y de ahí, primero a la izquierda, después hacia arriba y después a la derecha. En términos algebraicos,

$$\alpha\tau_2 = \alpha\tau_1\lambda$$

para  $\alpha \in E$ . Es claro que  $\tau_2$  extiende  $\sigma_2$ . El hecho de que podríamos haber comenzado con  $\tau_2$  y recobrado  $\tau_1$  definiendo

$$\alpha\tau_1 = \alpha\tau_2\lambda^{-1},$$

esto es, dando la vuelta por el otro lado del diagrama, muestra que la correspondencia entre  $\tau_1:E \rightarrow \bar{F}'$  y  $\tau_2:E \rightarrow F'_2$  es uno a uno. En vista de esta correspondencia uno a uno, el número de  $\tau$  que extiende a  $\sigma$  es independiente de  $F'$ ,  $\bar{F}'$  y  $\sigma$ .

Que el número de transformaciones  $\sigma$  es finita, se sigue del hecho de que como  $E$  es una extensión finita de  $F$ , por el teorema 38.3  $E^5 = F(\alpha_1, \dots, \alpha_n)$  para algunos  $\alpha_1, \dots, \alpha_n$  en  $E$ . Hay sólo un número finito de candidatos posibles para las imágenes  $\alpha_i\tau$  en  $F'$ , pues si

$$\text{irr}(\alpha_i, F) = a_{i0} + a_{i1}x + \cdots + a_{im_i}x^{m_i},$$

donde  $a_{ik} \in F$ , entonces  $\alpha_i\tau$  debe ser uno de los ceros en  $\bar{F}'$  de

$$[a_{i0}\sigma + (a_{i1}\sigma)x + \cdots + (a_{im_i}\sigma)x^{m_i}] \in F'[x]. \blacksquare$$

**Definición** Sea  $E$  una extensión finita de un campo  $F$ . El número de isomorfismos de  $E$  en  $\bar{F}$  que dejan fijo  $F$  es el *índice*  $\{E:F\}$  de  $E$  sobre  $F$ .

**Corolario** Si  $F \leq E \leq K$  donde  $K$  es un campo de extensión finita del campo  $F$ , entonces  $\{K:F\} = \{K:E\}\{E:F\}$ .

**Demostración** Del teorema 41.2, se sigue que cada uno de los  $\{E:F\}$  isomorfismos  $\tau_i:E \rightarrow \bar{F}$  que dejan fijo  $F$  tiene  $\{K:E\}$  extensiones a un isomorfismo de  $K$  en  $\bar{F}$ . ■

El corolario anterior era, en realidad, la cuestión importante que buscábamos. Nótese que cuenta algo. Nunca hay que subestimar un resultado que cuente algo, aunque se llame «corolario».

En el capítulo 43 mostraremos que a menos de que  $F$  sea un campo infinito de característica  $p \neq 0$ , siempre tendremos  $[E:F] = \{E:F\}$  para todo campo de extensión finita de  $F$ . Para el caso  $E = F(\alpha)$ , las  $\{F(\alpha):F\}$  extensiones de la transformación identidad  $\iota:F \rightarrow F$  a transformaciones de  $F(\alpha)$  en  $\bar{F}$  están dadas por los isomorfismos básicos  $\psi_{\alpha,\beta}$ , para cada conjugado  $\beta$  en  $\bar{F}$  de  $\alpha$  sobre  $F$ . Así, si  $\text{irr}(\alpha, F)$  tiene  $n$  ceros distintos en  $\bar{F}$ , tenemos  $\{E:F\} = n$ . Mostraremos más adelante que a menos de que  $F$  sea infinito y de característica  $p \neq 0$ , el número de ceros distintos de  $\text{irr}(\alpha, F)$  es  $\text{grad}(\alpha, F) = [F(\alpha):F]$ .

**Ejemplo 41.1** Considérese  $E = \mathbf{Q}(\sqrt{2}, \sqrt{3})$  sobre  $\mathbf{Q}$ , como en el ejemplo 40.4. Nuestro trabajo en el ejemplo 40.4 muestra que  $\{E:\mathbf{Q}\} = [E:\mathbf{Q}] = 4$ . Además,  $\{E:\mathbf{Q}(\sqrt{2})\} = 2$  y  $\{\mathbf{Q}(\sqrt{2}):\mathbf{Q}\} = 2$ , de modo que

$$4 = \{E:\mathbf{Q}\} = \{E:\mathbf{Q}(\sqrt{2})\}\{\mathbf{Q}(\sqrt{2}):\mathbf{Q}\} = (2)(2).$$

Esto ilustra el corolario del teorema 41.2. ■

### \*41.3 DEMOSTRACION DEL TEOREMA DE EXTENSION

Reenunciamos el teorema de extensión.

**Teorema 41.1 (Teorema de la extensión del isomorfismo)** *Sea  $E$  una extensión algebraica de un campo  $F$ . Sea  $\sigma$  un isomorfismo de  $F$  sobre un campo  $F'$ . Sea  $\bar{F}'$  una cerradura algebraica de  $F'$ . Entonces,  $\sigma$  puede extenderse a un isomorfismo  $\tau$  de  $E$  en  $\bar{F}'$  tal que  $a\tau = a\sigma$  para  $a \in F$ .*

**Demostración** Considérense todos los pares  $(L, \lambda)$  donde  $L$  es un campo tal que  $F \leq L \leq E$  y  $\lambda$  es un isomorfismo de  $L$  en  $\bar{F}'$  tal que  $a\lambda = a\sigma$  para  $a \in F$ . El conjunto  $S$  de dichos pares  $(L, \lambda)$  es no vacío, pues  $(F, \sigma)$  es uno de ellos. Defínase un orden parcial en  $S$  mediante  $(L_1, \lambda_1) \leq (L_2, \lambda_2)$  si  $L_1 \leq L_2$  y  $a\lambda_2 = a\lambda_1$  para  $a \in L_1$ . Se verifica fácilmente que esta relación  $\leq$  da un orden parcial de  $S$ .

Sea  $T = \{(H_i, \lambda_i) | i \in I\}$  una cadena de  $S$ . Afirmamos que  $H = \bigcup_{i \in I} H_i$  es un subcampo de  $E$ . Sea  $a, b \in H$  donde  $a \in H_1$  y  $b \in H_2$ ; entonces,  $H_1 \leq H_2$  o  $H_2 \leq H_1$ , puesto que  $T$  es una cadena. Si, digamos,  $H_1 \leq H_2$ , entonces,  $a, b \in H_2$  de modo que  $a \pm b, ab$  y  $a/b$  para  $b \neq 0$  están en  $H_2$  y, por tanto, en  $H$ . Como para cada  $i \in I$ ,  $F \leq H_i \leq E$ , tenemos  $F \leq H \leq E$ . Así,  $H$  es un subcampo de  $E$ .

Defínase  $\lambda: H \rightarrow \bar{F}'$  como sigue. Sea  $c \in H$ . Entonces,  $c \in H_i$  para alguna  $i \in I$  y sea

$$c\lambda = c\lambda_i.$$

La transformación  $\lambda$  está bien definida, porque si  $c \in H_1$  y  $c \in H_2$ , entonces,  $(H_1, \lambda_1) \leq (H_2, \lambda_2)$  o  $(H_2, \lambda_2) \leq (H_1, \lambda_1)$ , pues  $T$  es una cadena. En ambos casos,  $c\lambda_1 = c\lambda_2$ . Afirmamos que  $\lambda$  es un isomorfismo de  $H$  en  $\bar{F}'$ . Si  $a, b \in H$ , entonces existe algún  $H_i$  tal que  $a, b \in H_i$ , y

$$(a + b)\lambda = (a + b)\lambda_i = a\lambda_i + b\lambda_i = a\lambda + b\lambda.$$

En forma análoga,

$$(ab)\lambda = (ab)\lambda_i = (a\lambda_i)(b\lambda_i) = (a\lambda)(b\lambda).$$

Si  $a\lambda = 0$ , entonces  $a \in H_i$  para algún  $i$  implica que  $a\lambda_i = 0$ , de modo que  $a = 0$ . Por tanto,  $\lambda$  es un isomorfismo. Así,  $(H, \lambda) \in S$ , y es claro, por nuestras definiciones de  $H$  y  $\lambda$ , que  $(H, \lambda)$  es una cota superior para  $T$ .

Hemos mostrado que toda cadena de  $S$  tiene una cota superior en  $S$ , de modo que se satisfacen las hipótesis del lema de Zorn. Por tanto, existe un elemento maximal  $(K, \tau)$  de  $S$ . Sea  $K\tau = \bar{K}'$  donde  $\bar{K}' \leq \bar{F}'$ . Ahora, si  $K \neq E$ , sea

$\alpha \in E$ , pero  $\alpha \notin K$ . Ahora,  $\alpha$  es algebraico sobre  $F$ , de modo que  $\alpha$  es algebraico sobre  $K$ . Además, sea  $p(x) = \text{irr}(\alpha, K)$ . Sea  $\psi_\alpha$  el isomorfismo canónico

$$\psi_\alpha : K[x]/\langle p(x) \rangle \rightarrow K(\alpha),$$

correspondiente al homomorfismo básico  $\phi_\alpha : K[x] \rightarrow K(\alpha)$ . Si

$$p(x) = a_0 + a_1x + \cdots + a_nx^n,$$

considérese

$$q(x) = a_0\tau + (a_1\tau)x + \cdots + (a_n\tau)x^n$$

en  $K'[x]$ . Es obvio que como  $\tau$  es un isomorfismo,  $q(x)$  es irreducible en  $K'[x]$ . Como  $K' \leq \bar{F}$ , existe un cero  $\alpha'$  de  $q(x)$  en  $\bar{F}$ . Sea

$$\psi_{\alpha'} : K'[x]/\langle q(x) \rangle \rightarrow K'(\alpha')$$

el isomorfismo análogo a  $\psi_\alpha$ . Por último, sea

$$\bar{\tau} : K[x]/\langle p(x) \rangle \rightarrow K'[x]/\langle q(x) \rangle$$

el isomorfismo obvio que extiende  $\tau$  en  $K$  y transforma  $x + \langle p(x) \rangle$  sobre  $x + \langle q(x) \rangle$ . (Véase la figura 41.5.) Entonces, la composición de transformaciones

$$(\psi_\alpha)^{-1}\bar{\tau}\psi_{\alpha'} : K(\alpha) \rightarrow K'(\alpha')$$

es un isomorfismo de  $K(\alpha)$  en  $\bar{F}$ . Es claro que  $(K, \tau) < (K(\alpha), (\psi_\alpha)^{-1}\bar{\tau}\psi_{\alpha'})$ , lo cual contradice que  $(K, \tau)$  es maximal. Por tanto, debemos tener  $K = E$ . ■

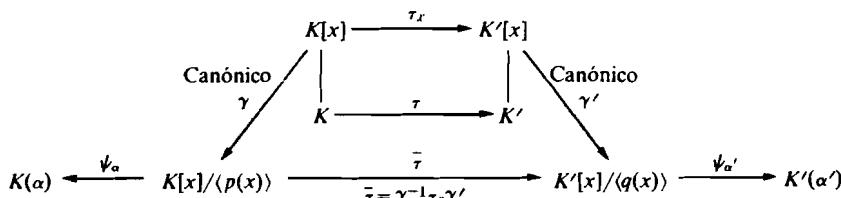


Figura 41.5

Desafortunadamente, es probable que consideren complicada sin remedio esta demostración. Para los algebraistas profesionales, esta construcción es tan común que, por lo general, sólo escribirían algo así como «la demostración se sigue del lema de Zorn» apenas hubieran definido el orden parcial  $\leq$  en el conjunto  $S$ . Escribimos la demostración con todo detalle, pues quizás sea la segunda demostración que el lector vea donde se usa el lema de Zorn.

**Ejercicios**

**41.1** Sea  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ . Para cada transformación isomorfa del subcampo de  $E$  dado a continuación, obténganse todas las extensiones de la transformación a una transformación isomorfa de  $E$  en  $\mathbb{Q}$ . Describanse las extensiones dando valores en el conjunto generador  $\{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$  para  $E$  sobre  $\mathbb{Q}$ .

- $\iota: \mathbb{Q}(\sqrt{2}, \sqrt{15}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{15})$ , donde  $\iota$  es la transformación idéntica
- $\sigma: \mathbb{Q}(\sqrt{2}, \sqrt{15}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{15})$ , donde  $\sqrt{2}\sigma = \sqrt{2}$  y  $\sqrt{15}\sigma = -\sqrt{15}$
- $\psi_{\sqrt{30}, -\sqrt{30}}: \mathbb{Q}(\sqrt{30}) \rightarrow \mathbb{Q}(\sqrt{30})$

**41.2** Es un hecho que se puede verificar elevando al cubo, el que los ceros de  $x^3 - 2$  en  $\mathbb{Q}$  son

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \sqrt[3]{2} \frac{-1 + i\sqrt{3}}{2} \quad \text{y} \quad \alpha_3 = \sqrt[3]{2} \frac{-1 - i\sqrt{3}}{2},$$

donde  $\sqrt[3]{2}$ , como siempre, es la raíz cúbica real de 2.

- Describanse todas las extensiones de la transformación identidad de  $\mathbb{Q}$  a un isomorfismo que transforme  $\mathbb{Q}(\sqrt[3]{2})$  en  $\mathbb{Q}$ .
- Describanse todas las extensiones de la transformación idéntica de  $\mathbb{Q}$  a un isomorfismo que transforme  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$  en  $\mathbb{Q}$ .
- Describanse todas las extensiones del automorfismo  $\psi_{\sqrt{3}, -\sqrt{3}}$  de  $\mathbb{Q}(\sqrt{3})$  a un isomorfismo que transforme  $\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$  en  $\mathbb{Q}$ .

**41.3** Sea  $\sigma$  el automorfismo de  $\mathbb{Q}(\pi)$  que transforma  $\pi$  sobre  $-\pi$ .

- Describase el campo fijo de  $\sigma$ .
- Describanse todas las extensiones de  $\sigma$  a un isomorfismo que transforme el campo  $\mathbb{Q}(\sqrt{\pi})$  en  $\mathbb{Q}(\pi)$ .

**†41.4** Sea  $K$  un campo algebraicamente cerrado. Muéstrese que todo isomorfismo  $\sigma$  de  $K$  en sí mismo, tal que  $K$  es algebraico sobre  $K\sigma$ , es un automorfismo de  $K$ , esto es, es una transformación sobre. [Sugerencia: aplíquese el teorema 41.1 a  $\sigma^{-1}$ .]

**41.5** ¿Falso o verdadero?

- a) Sea  $F(\alpha)$  cualquier extensión simple de un campo  $F$ . Entonces, todo isomorfismo de  $F$  en  $F$  tiene una extensión a un isomorfismo de  $F(\alpha)$  en  $F$ .
- b) Sea  $F(\alpha)$  cualquier extensión algebraica simple de un campo  $F$ . Entonces, todo isomorfismo de  $F$  en  $F$  tiene una extensión a un isomorfismo de  $F(\alpha)$  en  $F$ .
- c) Un isomorfismo de  $F$  en  $F$  tiene el mismo número de extensiones para cada extensión algebraica simple de  $F$ .
- d) Las cerraduras algebraicas de campos isomorfos siempre son isomorfas.
- e) Las cerraduras de campos que no son isomorfos nunca son isomorfas.
- f) Cualquier cerradura algebraica de  $\mathbb{Q}(\sqrt{2})$  es isomorfa a cualquier cerradura algebraica de  $\mathbb{Q}(\sqrt{17})$ .
- g) El índice de una extensión finita de  $E$  sobre un campo  $F$  es finito.
- h) El índice se comporta multiplicativamente respecto a torres finitas de extensiones finitas de campos.

- 
- i) Las observaciones anteriores al enunciado del teorema 41.1 de la sección 41.1 esencialmente constituyen una demostración de este teorema para una extensión finita de  $E$  sobre  $F$ .
  - j) El corolario 2 del teorema 41.1 muestra que  $\mathbb{C}$  es isomorfo a  $\bar{\mathbb{Q}}$ .
- 

41.6 Sea  $E$  una extensión algebraica de un campo  $F$ . Muéstrese que todo isomorfismo de  $E$  en  $\bar{F}$  que deja fijo  $F$  puede extenderse a un automorfismo de  $\bar{F}$ .

41.7 Pruébese que si  $E$  es una extensión algebraica de un campo  $F$ , entonces dos cerraduras algebraicas  $\bar{F}$  y  $\bar{E}$  de  $F$  y  $E$ , respectivamente, son isomorfas.

41.8 Pruébese que la cerradura algebraica de  $\mathbb{Q}(\sqrt{\pi})$  en  $\mathbb{C}$  es isomorfa a cualquier cerradura algebraica de  $\bar{\mathbb{Q}}(x)$  donde  $\bar{\mathbb{Q}}$  es el campo de números algebraicos y  $x$  es una indeterminada.

41.9 Pruébese que si  $E$  es una extensión finita de un campo  $F$ , entonces  $\{E:F\} \leq [E:F]$ . [Sugerencia: las observaciones anteriores al ejemplo 41.1 esencialmente lo mostraron, para una extensión algebraica simple  $F(x)$  de  $F$ . Usese el hecho de que una extensión finita es una torre de extensiones simples, junto con las propiedades multiplicativas del índice y del grado.]

## Campos de descomposición

Nos interesarán, principalmente, los *automorfismos* de un campo  $E$  más que las meras transformaciones isomorfas de  $E$ . Son los *automorfismos* de un campo los que forman grupo. Nos preguntamos si para algún campo de extensión de un campo  $F$ , *toda* transformación isomorfa de  $E$  en  $\bar{F}$  que deje fijo  $F$  es, en realidad, un automorfismo de  $E$ .

Supóngase que  $E$  es una extensión algebraica de un campo  $F$ . Si  $\alpha \in E$  y  $\beta \in \bar{F}$  es un conjugado de  $\alpha$  sobre  $F$ , entonces existe un isomorfismo básico

$$\psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta).$$

Por el corolario 1 del teorema 41.1,  $\psi_{\alpha, \beta}$  puede extenderse a una transformación isomorfa de  $E$  en  $\bar{F}$ . Ahora, si  $\beta \notin E$ , dicha transformación isomorfa de  $E$  no puede ser un automorfismo de  $E$ . Así, si una extensión algebraica  $E$  de un campo  $F$  es tal que todas sus transformaciones isomorfas en  $\bar{F}$  que dejan fijo a  $F$  son, en realidad, automorfismos de  $E$ , entonces, para toda  $\alpha \in E$  todos los conjugados de  $\alpha$  sobre  $F$  deben estar también en  $E$ . Da la impresión de que esta observación se obtiene muy fácilmente. Señalemos que se usaron muchos recursos, a saber, la existencia de los isomorfismos básicos y el teorema de la extensión del isomorfismo.

Estas ideas sugieren la formulación de la siguiente definición.

**Definición** Sea  $F$  un campo con cerradura algebraica  $\bar{F}$ . Sea  $\{f_i(x) \mid i \in I\}$  una colección de polinomios en  $F[x]$ . Un campo  $E \leq \bar{F}$  es el *campo de descomposición de  $\{f_i(x) \mid i \in I\}$  sobre  $F$*  si  $E$  es el menor subcampo de  $\bar{F}$  que contiene a  $F$  y a todos los ceros en  $\bar{F}$  de cada uno de los  $f_i(x)$  para  $i \in I$ . Un campo  $K \leq \bar{F}$  es un *campo de descomposición sobre  $F$*  si es el campo de descomposición de algún conjunto de polinomios en  $F[x]$ .

Para un polinomio  $f(x) \in F[x]$ , a menudo nos referiremos al campo de descomposición de  $\{f(x)\}$  sobre  $F$  como al **campo de descomposición de  $f(x)$  sobre  $F$** . Es claro que el campo de descomposición de  $\{f_i(x) | i \in I\}$  sobre  $F$  en  $\bar{F}$  es la intersección de todos los subcampos de  $\bar{F}$  que contienen  $F$  y a todos los ceros en  $\bar{F}$  para cada  $f_i(x)$  para  $i \in I$ . Así que dicho campo ciertamente sí existe.

Mostremos ahora que los campos de descomposición sobre  $F$  son precisamente aquellos campos  $E \leq \bar{F}$  con la propiedad de que todas las transformaciones isomorfas de  $E$  en  $\bar{F}$  que dejen fijo  $F$ , son automorfismos de  $E$ . Esto será un corolario del siguiente teorema. *Una vez más estamos caracterizando un concepto en términos de transformaciones.* Recuérdese que siempre suponemos que todas las extensiones algebraicas de un campo  $F$  que se consideran, están en una cerradura algebraica fija  $\bar{F}$  de  $F$ .

**Teorema 42.1** *Un campo  $E$ , donde  $F \leq E \leq \bar{F}$  es un campo de descomposición sobre  $F$  si y sólo si todo automorfismo de  $\bar{F}$  que deje fijo  $F$  lleva a  $E$  sobre sí mismo y así, induce un automorfismo de  $E$  que deja fijo  $F$ .*

**Demostración** Sea  $E$  un campo de descomposición sobre  $F$  en  $\bar{F}$  de  $\{f_i(x) | i \in I\}$ , y sea  $\sigma$  un automorfismo de  $\bar{F}$  que deja fijo  $F$ . Sea  $\{\alpha_j | j \in J\}$  la colección de todos los ceros en  $\bar{F}$  de los  $f_i(x)$  para  $i \in I$ . Ahora, nuestro trabajo anterior muestra que para una  $\alpha_j$  fija,  $F(\alpha_j)$  tiene como elementos todas las expresiones de la forma

$$g(\alpha_j) = a_0 + a_1\alpha_j + \cdots + a_{n_j-1}\alpha_j^{n_j-1},$$

donde  $n_j$  es el grado de  $\text{irr}(\alpha_j, F)$  y  $a_k \in F$ . Considérese el conjunto  $S$  de todas las sumas *finitas* de productos *finitos* de elementos de la forma  $g(\alpha_j)$  para todas las  $j \in J$ . El conjunto  $S$  es un subconjunto de  $E$ , obviamente cerrado bajo la suma y la multiplicación, y que contiene 0, 1 y el inverso aditivo de cada elemento. Como cada elemento de  $S$  está en algún  $F(\alpha_{j_1}, \dots, \alpha_{j_r}) \subseteq S$ , vemos que  $S$  también contiene el inverso multiplicativo de cada elemento distinto de cero. Así,  $S$  es un subcampo de  $E$  que contiene todas las  $\alpha_j$  para  $j \in J$ . Por definición de campo de descomposición  $E$  de  $\{f_i(x) | i \in I\}$ , vemos que debemos tener  $S = E$ . Todo este trabajo fue sólo para mostrar que  $\{\alpha_j | j \in J\}$  genera  $E$  sobre  $F$ , en el sentido de tomar sumas *finitas* y productos *finitos*. Sabiendo esto, vemos de inmediato que el valor de  $\sigma$  en cualquier elemento de  $E$  está por completo determinado por los valores  $\alpha_j\sigma$ . Pero, por el corolario 1 del teorema 40.1,  $\alpha_j\sigma$  debe ser un cero de  $\text{irr}(\alpha_j, F)$ . Por el teorema 35.3,  $\text{irr}(\alpha_j, F)$  divide aquellas  $f_i(x)$  que cumplen  $f_i(\alpha_j) = 0$ , de modo que, también,  $\alpha_j\sigma \in E$ . Así,  $\sigma$  transforma  $E$  en  $E$  de manera isomorfa. Sin embargo, lo mismo es cierto para el automorfismo  $\sigma^{-1}$  de  $\bar{F}$ . Como para  $\beta \in E$

$$\beta = (\beta\sigma^{-1})\sigma,$$

vemos que  $\sigma$  transforma  $E$  sobre  $E$  y, así, induce un automorfismo de  $E$ .

Supóngase, reciprocamente, que todo automorfismo de  $\bar{F}$  que deje fijo  $F$  induce un automorfismo de  $E$ . Sea  $g(x)$  un polinomio *irreducible* en  $F[x]$  que

tiene un cero  $\alpha$  en  $E$ . Si  $\beta$  es cualquier cero de  $g(x)$  en  $\bar{F}$ , entonces, por el teorema 40.1, hay un isomorfismo básico  $\psi_{\alpha, \beta}$  de  $F(\alpha)$  sobre  $F(\beta)$  que deja fijo  $F$ . Por el teorema 41.1,  $\psi_{\alpha, \beta}$  puede extenderse a un isomorfismo  $\tau$  de  $\bar{F}$  en  $\bar{F}$ . Pero, entonces,

$$\tau^{-1} : \bar{F}\tau \rightarrow \bar{F}$$

puede extenderse a un isomorfismo que transforme  $\bar{F}$  en  $\bar{F}$ . Como la imagen de  $\tau^{-1}$  ya es todo  $\bar{F}$ , vemos que  $\tau$  debe ser sobre  $\bar{F}$ , de modo que  $\tau$  es un automorfismo de  $\bar{F}$  que deja fijo  $F$ . Entonces, por hipótesis,  $\tau$  induce un automorfismo de  $E$ , de modo que  $\alpha\tau = \beta$  está en  $E$ . Hemos mostrado que si  $g(x)$  es un polinomio irreducible en  $F[x]$  con un cero en  $E$ , entonces, todos los ceros de  $g(x)$  en  $\bar{F}$  están en  $E$ . De aquí, si  $\{g_k(x)\}$  es el conjunto de *todos* los polinomios irreducibles en  $F[x]$  con al menos un cero en  $E$ , entonces  $E$  es el campo de descomposición de  $\{g_k(x)\}$ . ■

**Definición** Sea  $E$  un campo de extensión de un campo  $F$ . Un polinomio  $f(x) \in F[x]$  se *descompone en  $E$*  si se factoriza en un producto de factores lineales en  $E[x]$ .

**Corolario 1** Si  $E \leq F$  es un campo de descomposición sobre  $F$ , entonces todo polinomio irreducible en  $F[x]$ , con al menos un cero en  $E$ , se descompone en  $E$ .

**Demostración** Si  $E$  es un campo de descomposición sobre  $F$  en  $\bar{F}$ , entonces todo automorfismo de  $\bar{F}$  induce un automorfismo de  $E$ . En la segunda mitad de la demostración del teorema 42.1, se mostró, precisamente, que  $E$  también es el campo de descomposición sobre  $F$  del conjunto  $\{g_k(x)\}$  de *todos* los polinomios irreducibles en  $F[x]$  que tienen un cero en  $E$ . Así, un polinomio irreducible  $f(x)$  de  $F[x]$  con algún cero en  $E$ , tiene todos sus ceros en  $\bar{F}$  en  $E$ . Por tanto, su factorización en factores lineales en  $\bar{F}[x]$ , dada por el teorema 38.5, en realidad tiene lugar en  $E[x]$ , de modo que  $f(x)$  se descompone en  $E$ . ■

**Corolario 2** Si  $E \leq \bar{F}$  es un campo de descomposición sobre  $F$ , entonces toda transformación isomorfa de  $E$  en  $\bar{F}$  que deje fijo  $F$  es, en realidad, un automorfismo de  $E$ . En particular, si  $E$  es un campo de descomposición de grado finito sobre  $F$ , entonces

$$\{E : F\} = |G(E/F)|.$$

**Demostración** Todo isomorfismo  $\sigma$  que transforme  $E$  en  $\bar{F}$  y deje fijo  $F$ , puede extenderse a un automorfismo  $\tau$  de  $\bar{F}$ , debido al teorema 41.1, junto con el argumento que prueba que es *sobre* de la segunda mitad de la demostración del teorema 42.1. Si  $E$  es un campo de descomposición sobre  $F$ , entonces, por el teorema 4.2.1,  $\tau$  restringido a  $E$ , esto es,  $\sigma$  es un automorfismo de  $E$ . Así, para un campo de descomposición  $E$  sobre  $F$ , toda transformación isomorfa de  $E$  en  $\bar{F}$  que deje fijo  $F$  es un automorfismo de  $E$ .

La ecuación  $\{E:F\} = |G(E/F)|$  se sigue, entonces, inmediatamente, para un campo de descomposición  $E$  de grado finito sobre  $F$ , pues  $\{E:F\}$  se definió como el número de las diferentes transformaciones isomorfas de  $E$  en  $\bar{F}$  que dejan fijo  $F$ . ■

**Ejemplo 42.1** Es obvio que  $\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{3})$  es el campo de descomposición de

$$\{x^2 - 2, x^2 - 3\}$$

sobre  $\mathbf{Q}$ . En el ejemplo 40.4 se mostró que las transformaciones  $\iota, \sigma_1, \sigma_2$  y  $\sigma_3$  son todos los automorfismos de  $\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{3})$  que dejan fijo a  $\mathbf{Q}$ . (En realidad, como todo automorfismo de un campo debe dejar fijo el subcampo primo, vemos que estos son los únicos automorfismos de  $\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ .) Entonces,

$$\{\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{3}): \mathbf{Q}\} = |G(\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{3})/\mathbf{Q})| = 4,$$

lo cual ilustra el corolario 2. ■

Deseamos determinar las condiciones bajo las cuales

$$|G(E/F)| = \{E:F\} = [E:F]$$

para extensiones finitas  $E$  de  $F$ . Este es nuestro siguiente tema. En la siguiente sección mostraremos que esta ecuación siempre vale cuando  $E$  es un campo de descomposición sobre un campo  $F$  de característica 0, o cuando  $F$  es un campo finito. Esta ecuación no es necesariamente cierta cuando  $F$  es un campo infinito de característica  $p \neq 0$ .

**Ejemplo 42.2** Sea  $\sqrt[3]{2}$ , como siempre, la raíz cúbica real de 2. Ahora,  $x^3 - 2$  no se descompone en  $\mathbf{Q}(\sqrt[3]{2})$ , pues  $\mathbf{Q}(\sqrt[3]{2}) < \mathbf{R}$ , y sólo un cero de  $x^3 - 2$  es real. Así,  $x^3 - 2$  se factoriza en  $(\mathbf{Q}(\sqrt[3]{2}))[\mathbf{x}]$  en un factor lineal  $x - \sqrt[3]{2}$  y en un factor cuadrático irreducible. El campo de descomposición  $E$  de  $x^3 - 2$  sobre  $\mathbf{Q}$  es, por tanto, de grado 2 sobre  $\mathbf{Q}(\sqrt[3]{2})$ . Entonces,

$$[E:\mathbf{Q}] = [E:\mathbf{Q}(\sqrt[3]{2})][\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}] = (2)(3) = 6.$$

Hemos mostrado que el campo de descomposición sobre  $\mathbf{Q}$  de  $x^3 - 2$  es de grado 6 sobre  $\mathbf{Q}$ .

Elevando al cubo, puede verificarse que

$$\frac{-\sqrt[3]{2} - 1 + i\sqrt{3}}{2} \quad \text{y} \quad \frac{\sqrt[3]{2} - 1 - i\sqrt{3}}{2}$$

son los otros ceros de  $x^3 - 2$  en  $C$ . Así, el campo de descomposición  $E$  de  $x^3 - 2$  sobre  $\mathbb{Q}$  es  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ . (Este campo *no* es igual a  $\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$ , el cual es de grado 12 sobre  $\mathbb{Q}$ .) Se deja como ejercicio un estudio más amplio de este interesante ejemplo (véanse los ejercicios 42.3, 42.8, 42.12 y 42.14). ■

## Ejercicios

**42.1** Para cada uno de los polinomios dados en  $\mathbb{Q}[x]$ , encuéntrese el grado sobre  $\mathbb{Q}$  del campo de descomposición sobre  $\mathbb{Q}$  del polinomio.

- a)  $x^2 + 3$
- b)  $x^4 - 1$
- c)  $(x^2 - 2)(x^2 - 3)$
- d)  $x^3 - 3$
- e)  $x^3 - 1$
- f)  $(x^2 - 2)(x^3 - 2)$

**42.2** Sea  $f(x)$  un polinomio en  $F[x]$  de grado  $n$ . Sea  $E \leq \bar{F}$  el campo de descomposición de  $f(x)$  sobre  $F$  en  $\bar{F}$ . ¿Qué cotas se pueden poner a  $[E:F]$ ?

**42.3** Referirse al ejemplo 42.2 para responder las siguientes preguntas.

- a) ¿Cuál es el orden de  $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ ?
- b) ¿Cuál es el orden de  $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})$ ?
- c) ¿Cuál es el orden de  $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2}))$ ?

**42.4** Sea  $\alpha$  un cero de  $x^3 + x^2 + 1$  sobre  $\mathbb{Z}_2$ . Muéstrese que  $x^3 + x^2 + 1$  se descompone en  $\mathbb{Z}_2(\alpha)$ . [Sugerencia: hay ocho elementos en  $\mathbb{Z}_2(\alpha)$ . Exhiban dos ceros más de  $x^3 + x^2 + 1$ , además de  $\alpha$ , de entre estos elementos.]

**42.5** Muéstrese que si una extensión finita  $E$  de un campo  $F$  es un campo de descomposición sobre  $F$ , entonces  $E$  es un campo de descomposición de algún polinomio en  $F[x]$ .

**42.6** ¿Falso o verdadero?

- a) Sea  $\alpha, \beta \in E$  donde  $E \leq \bar{F}$  es un campo de descomposición sobre  $F$ . Entonces, existe un automorfismo de  $E$  que deja fijo  $F$  y transforma  $\alpha$  sobre  $\beta$  si y sólo si  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ .
- b)  $\mathbb{R}$  es un campo de descomposición sobre  $\mathbb{Q}$ .
- c)  $\mathbb{R}$  es un campo de descomposición sobre  $\mathbb{R}$ .
- d)  $C$  es un campo de descomposición sobre  $\mathbb{R}$ .
- e)  $\mathbb{Q}(i)$  es un campo de descomposición sobre  $\mathbb{Q}$ .
- f)  $\mathbb{Q}(\pi)$  es un campo de descomposición sobre  $\mathbb{Q}(\pi^2)$ .
- g) Para todo campo de descomposición  $E$  sobre  $F$ , donde  $E \leq \bar{F}$ , toda transformación isomorfa de  $E$  en  $\bar{F}$  es un automorfismo de  $E$ .
- h) Para todo campo de descomposición  $E$  sobre  $F$ , donde  $E \leq \bar{F}$ , todo isomorfismo que transforma  $E$  en  $\bar{F}$  es un automorfismo de  $E$ .
- i) Para todo campo de descomposición  $E$  sobre  $F$ , donde  $E \leq \bar{F}$ , todo isomorfismo que lleva  $E$  en  $\bar{F}$  y deja fijo  $F$  es un automorfismo de  $E$ .
- j) Toda cerradura algebraica  $\bar{F}$  de un campo  $F$  es un campo de descomposición sobre  $F$ .

**42.7** Muéstrese, mediante un ejemplo, que el corolario 1 del teorema 42.1 no se cumple, si se quita la palabra *irreducible*.

**42.8** a) ¿Es  $|G(E/F)|$  multiplicativo para torres finitas de extensiones finitas, esto es,

$$|G(K/F)| = |G(K/E)| |G(E/F)| \quad \text{para } F \leq E \leq K \leq \bar{F}?$$

¿Por qué? [Sugerencia: úsese el ejercicio 42.3.]

b) ¿Es  $|G(E/F)|$  multiplicativo para torres finitas de extensiones finitas, cada una de las cuales es un campo de descomposición sobre el campo de abajo? ¿Por qué?

**42.9** Muéstrese que si  $[E:F] = 2$ , entonces  $E$  es un campo de descomposición sobre  $F$ .

**42.10** Muéstrese que para  $F \leq E \leq \bar{F}$ ,  $E$  es un campo de descomposición sobre  $F$  si y sólo si  $E$  contiene todos los conjugados sobre  $F$  en  $\bar{F}$  de cada uno de sus elementos.

**42.11** Muéstrese que  $\mathbb{Q}(\sqrt[3]{2})$  tiene sólo el automorfismo identidad.

**42.12** Con respecto al ejemplo 42.2, muéstrese que

$$G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3})) \simeq \langle \mathbf{Z}_3, + \rangle.$$

**42.13** a) Muéstrese que un automorfismo de un campo de descomposición  $E$  sobre  $F$  de un polinomio  $f(x) \in F[x]$  permuta los ceros de  $f(x)$  en  $E$ .

b) Muéstrese que un automorfismo de un campo de descomposición  $E$  sobre  $F$  de un polinomio  $f(x) \in F[x]$  está por completo determinado por la permutación de los ceros de  $f(x)$  en  $E$  dada en a).

c) Muéstrese que si  $E$  es un campo de descomposición sobre  $F$  de un polinomio  $f(x) \in F[x]$ , entonces  $G(E/F)$  puede considerarse, de manera natural, como cierto grupo de permutaciones.

**42.14** Sea  $E$  el campo de descomposición de  $x^3 - 2$  sobre  $\mathbb{Q}$ , como en el ejemplo 42.2.

a) ¿Cuál es el orden de  $G(E/\mathbb{Q})$ ? [Sugerencia: úsese el corolario 2 del teorema 42.2 y el corolario del teorema 41.1 aplicado a la torre  $\mathbb{Q} \leq \mathbb{Q}(i\sqrt{3}) \leq E$ .]

b) Muéstrese que  $G(E/\mathbb{Q}) \simeq S_3$ , el grupo simétrico en tres letras. [Sugerencia: úsese el ejercicio 42.13, junto con a).]

**42.15** Muéstrese que para un primo  $p$ , el campo de descomposición sobre  $\mathbb{Q}$  de  $x^p - 1$  es de grado  $p - 1$  sobre  $\mathbb{Q}$ . [Sugerencia: remítase al corolario del teorema 31.4.]

**42.16** Sean  $\bar{F}$  y  $\bar{F}'$  dos cerraduras algebraicas de un campo  $F$  y sea  $f(x) \in F[x]$ . Muéstrese que el campo de descomposición  $E$  sobre  $F$  de  $f(x)$  en  $\bar{F}$  es isomorfo al campo de descomposición  $E'$  sobre  $F$  de  $f(x)$  en  $\bar{F}'$ . [Sugerencia: úsese el teorema 41.1.]

## Extensiones separables

### 43.1 MULTIPLICIDAD DE LOS CEROS DE UN POLINOMIO

Recuérdese que suponemos que todas las extensiones algebraicas de un campo  $F$  que se consideran, están contenidas en una cerradura algebraica fija  $\bar{F}$  de  $F$ .

Nuestra siguiente tarea es determinar, para una extensión finita  $E$  de  $F$ , bajo qué condiciones  $\{E:F\} = [E:F]$ . La clave para responder a esto es considerar la multiplicidad de los ceros de los polinomios.

**Definición** Sea  $f(x) \in F[x]$ . Un elemento  $\alpha$  de  $\bar{F}$  tal que  $f(\alpha) = 0$  es un *cero de  $f(x)$  de multiplicidad  $v$*  si  $v$  es el mayor entero tal que  $(x - \alpha)^v$  es un factor de  $f(x)$  en  $\bar{F}[x]$ .

El siguiente teorema muestra que las multiplicidades de los ceros de un polinomio *irreducible* dado sobre un campo, son todas iguales. La facilidad con que podemos probar este teorema es otra indicación acerca de la fuerza de nuestros isomorfismos básicos y de todo nuestro enfoque del estudio de ceros de polinomios, mediante transformaciones.

**Teorema 43.1** *Sea  $f(x)$  irreducible en  $\bar{F}[x]$ . Entonces, todos los ceros de  $f(x)$  en  $\bar{F}$  tienen la misma multiplicidad.*

**Demostración** Sean  $\alpha$  y  $\beta$  ceros de  $f(x)$  en  $\bar{F}$ . Entonces, por el teorema 40.1 existe un isomorfismo básico  $\psi_{\alpha,\beta}: F(\alpha) \xrightarrow{\text{sobre}} F(\beta)$ . Por el corolario 1 del teorema 41.1,  $\psi_{\alpha,\beta}$  puede extenderse a un isomorfismo  $\tau: \bar{F} \rightarrow \bar{F}$ . Entonces,  $\tau$  induce un iso-

morfismo natural  $\tau_x: \bar{F}[x] \rightarrow \bar{F}[x]$  con  $x\tau_x = x$ . Ahora,  $\tau_x$  deja fijo  $f(x)$ , pues  $f(x) \in F[x]$  y  $\psi_{\alpha, \beta}$  deja fijo  $F$ . Sin embargo,

$$((x - \alpha)^v)\tau_x = (x - \beta)^v,$$

lo cual muestra que la multiplicidad de  $\beta$  en  $f(x)$  es mayor o igual a la multiplicidad de  $\alpha$ . Un razonamiento análogo da la desigualdad recíproca, de modo que la multiplicidad de  $\alpha$  es igual a la de  $\beta$ . ■

**Corolario** Si  $f(x)$  es irreducible en  $F[x]$ , entonces  $f(x)$  tiene una factorización en  $\bar{F}[x]$  de la forma

$$a \prod_i (x - \alpha_i)^{v_i},$$

donde las  $\alpha_i$  son los distintos ceros de  $f(x)$  en  $\bar{F}$  y  $a \in F$ .

**Demostración** La demostración del corolario es inmediata del teorema 43.1. ■

A estas alturas, deberíamos mostrar mediante un ejemplo que puede ocurrir el fenómeno de un cero de multiplicidad mayor que 1 de un polinomio irreducible. Mostraremos más adelante en este capítulo, que sólo puede suceder para un polinomio sobre un campo infinito de característica  $p \neq 0$ .

**Ejemplo 43.1** Sea  $E = \mathbf{Z}_p(y)$  donde  $y$  es una indeterminada. Sea  $t = y^p$  y sea  $F$  el subcampo  $\mathbf{Z}_p(t)$  de  $E$ . (Véase la figura 43.1.) Ahora,  $E = F(y)$  es algebraico sobre  $F$ , pues  $y$  es un cero de  $(x^p - t) \in F[x]$ . Por el teorema 35.3,  $\text{irr}(y, F)$  debe dividir a  $x^p - t$  en  $F[x]$ . [En realidad,  $\text{irr}(y, F) = x^p - t$ . Dejamos la demostración para los ejercicios (véase el ejercicio 43.4).] Como claramente  $F(y)$  no es igual a  $F$ , debemos tener que el grado de  $\text{irr}(y, F) \geq 2$ . Pero nótese que

$$x^p - t = x^p - y^p = (x - y)^p,$$

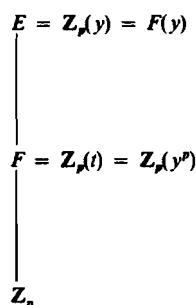


Figura 43.1

pues  $E$  tiene característica  $p$  (véase el teorema 40.5 y el comentario que le sigue). Así,  $y$  es un cero de  $\text{irr}(y, F)$  de multiplicidad  $> 1$ . En realidad,  $x^p - t = \text{irr}(y, F)$ , de modo que la multiplicidad de  $y$  es  $p$ . ■

A partir de aquí nos basaremos fuertemente en el teorema 41.2 y su corolario. El teorema 40.1 y su corolario muestran que para una extensión algebraica simple  $F(\alpha)$  de  $F$ , existe, para todo cero distinto, de  $\text{irr}(\alpha, F)$ , una extensión del isomorfismo identidad  $\iota$  de  $F$  en  $F$ , y que éstas son las únicas extensiones de  $\iota$ . Así,  $\{F(\alpha) : F\}$  es el número de los distintos ceros de  $\text{irr}(\alpha, F)$ .

De nuestro trabajo con el teorema de Lagrange y del teorema 38.2, debería reconocerse la fuerza potencial de un teorema como el siguiente.

**Teorema 43.2** *Si  $E$  es una extensión finita de  $F$ , entonces  $\{E : F\}$  divide  $[E : F]$ .*

*Demostración* Por el teorema 38.3, si  $E$  es finito sobre  $F$ , entonces  $E = F(\alpha_1, \dots, \alpha_n)$ , donde  $\alpha_i \in \bar{F}$ . Sea  $\text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$  donde  $\alpha_i$  es uno de los  $n_i$  distintos ceros que, por el teorema 43.1, tienen multiplicidad  $v_i$ . Entonces,

$$\begin{aligned}[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] &= n_i v_i \\ &= \{F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})\} v_i.\end{aligned}$$

Por el teorema 38.2 y el corolario del teorema 41.2,

$$[E : F] = \prod_i n_i v_i$$

y

$$\{E : F\} = \prod_i n_i.$$

Por tanto,  $\{E : F\}$  divide  $[E : F]$ . ■

## 43.2 EXTENSIONES SEPARABLES

**Definición** Una extensión finita  $E$  de  $F$  es una *extensión separable de  $F$*  si  $\{E : F\} = [E : F]$ . Un elemento  $\alpha$  de  $\bar{F}$  es *separable sobre  $F$*  si  $F(\alpha)$  es una extensión separable de  $F$ . Un polinomio irreducible  $f(x) \in F[x]$  es *separable sobre  $F$*  si todo cero de  $f(x)$  en  $\bar{F}$  es separable sobre  $F$ .

Para facilitar las cosas al estudiante, hemos restringido nuestra definición de extensión separable de un campo  $F$  a extensiones *finitas*  $E$  de  $F$ . Para la definición correspondiente a extensiones infinitas, véase el ejercicio 43.6.

Sabemos que  $\{F(\alpha) : F\}$  es el número de ceros distintos de  $\text{irr}(\alpha, F)$ . Además, por el teorema 43.1, la multiplicidad de  $\alpha$  en  $\text{irr}(\alpha, F)$  es la misma que la

multiplicidad de cada conjugado de  $\alpha$  sobre  $F$ . Así,  $\alpha$  es separable sobre  $F$  si y sólo si  $\text{irr}(\alpha, F)$  tiene todos los ceros de multiplicidad 1. De inmediato, esto nos dice que  $\alpha$  es un polinomio irreducible  $f(x) \in F[x]$  es separable sobre  $F$  si y sólo si  $f(x)$  tiene todos los ceros de multiplicidad 1.

**Teorema 43.3** Si  $K$  es una extensión finita de  $E$  y  $E$  es una extensión finita de  $F$ , esto es, si  $F \leq E \leq K$ , entonces  $K$  es separable sobre  $F$  si y sólo si  $K$  es separable sobre  $E$  y  $E$  es separable sobre  $F$ .

*Demostración* Se tiene,

$$[K:F] = [K:E][E:F]$$

y

$$\{K:F\} = \{K:E\}\{E:F\}.$$

Entonces, si  $K$  es separable sobre  $F$ , de modo que  $[K:F] = \{K:F\}$ , debemos tener  $[K:E] = \{K:E\}$  y  $[E:F] = \{E:F\}$ , pues en cada caso, por el teorema 43.2, el índice divide al grado. Así, si  $K$  es separable sobre  $F$ , entonces  $K$  es separable sobre  $E$  y  $E$  es separable sobre  $F$ .

El recíproco es igualmente fácil, pues  $[K:E] = \{K:E\}$  y  $[E:F] = \{E:F\}$  implica que

$$[K:F] = [K:E][E:F] = \{K:E\}\{E:F\} = \{K:F\}. \blacksquare$$

El teorema 43.3 se puede extender de manera obvia, por inducción, a cualquier torre finita de extensiones finitas. El campo de arriba es una extensión separable del campo de abajo si y sólo si cada campo es una extensión separable del que está inmediatamente abajo de él.

**Corolario** Si  $E$  es una extensión finita de  $F$ , entonces  $E$  es separable sobre  $F$  si y sólo si cada  $\alpha$  en  $E$  es separable sobre  $F$ .

*Demostración* Supóngase que  $E$  es separable sobre  $F$  y sea  $\alpha \in E$ . Entonces,

$$F \leq F(\alpha) \leq E.$$

y el teorema 43.3 muestran que  $F(\alpha)$  es separable sobre  $F$ .

Supóngase, de manera recíproca, que toda  $\alpha \in E$  es separable sobre  $F$ . Como  $E$  es finito sobre  $F$ , existen  $\alpha_1, \dots, \alpha_n$  tales que

$$F < F(\alpha_1) < F(\alpha_1, \alpha_2) < \cdots < E = F(\alpha_1, \dots, \alpha_n).$$

Ahora, debido a que  $\alpha_i$  es separable sobre  $F$ , es claro que  $\alpha_i$  es separable sobre  $F(\alpha_1, \dots, \alpha_{i-1})$ , ya que

$$q(x) = \text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$$

divide a  $\text{irr}(\alpha_i, F)$  de modo que  $\alpha_i$  es un cero de  $q(x)$  de multiplicidad 1. Así,  $F(\alpha_1, \dots, \alpha_i)$  es separable sobre  $F(\alpha_1, \dots, \alpha_{i-1})$ , entonces, por el teorema 43.3, extendido por inducción,  $E$  es separable sobre  $F$ . ■

### 43.3 CAMPOS PERFECTOS

Pasemos ahora a la tarea de probar que  $\alpha$  puede no ser separable sobre  $F$ , sólo si  $F$  es un campo infinito de característica  $p \neq 0$ . Un método es introducir derivadas formales de polinomios. Aunque esta técnica es elegante y útil, en aras de la brevedad usaremos el lema siguiente. Las derivadas formales se desarrollan en los ejercicios 43.8 al 43.15.

**Lema 43.1** *Sea  $\bar{F}$  una cerradura algebraica de  $F$  y sea*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

*cualquier polinomio mónico en  $\bar{F}[x]$ . Si  $(f(x))^m \in F[x]$  y  $m \cdot 1 \neq 0$  en  $F$ , entonces  $f(x) \in F[x]$ , esto es, todas las  $a_i \in F$ .*

*Demostración* Debemos mostrar que  $a_i \in F$ , y procedemos, por inducción en  $r$ , a mostrar que  $a_{n-r} \in F$ . Para  $r = 1$ ,

$$(f(x))^m = x^{mn} + (m \cdot 1)a_{n-1}x^{mn-1} + \cdots + a_0^m.$$

Pues  $(f(x))^m \in F[x]$ , en particular, tenemos que

$$(m \cdot 1)a_{n-1} \in F.$$

Así,  $a_{n-1} \in F$ , pues  $m \cdot 1 \neq 0$  en  $F$ .

Como hipótesis de inducción, supongamos que  $a_{n-r} \in F$  para  $r = 1, 2, \dots, k$ . Entonces, el coeficiente de  $x^{mn-(k+1)}$  en  $(f(x))^m$  es de la forma

$$(m \cdot 1)a_{n-(k+1)} + g_{k+1}(a_{n-1}, a_{n-2}, \dots, a_{n-k}),$$

donde  $g_{k+1}(a_{n-1}, a_{n-2}, \dots, a_{n-k})$  es un polinomio formal en  $a_{n-1}, a_{n-2}, \dots, a_{n-k}$ . Por la hipótesis de inducción,  $g_{k+1}(a_{n-1}, a_{n-2}, \dots, a_{n-k}) \in F$ , así que, de nuevo,  $a_{n-(k+1)} \in F$  pues  $m \cdot 1 \neq 0$  en  $F$ . ■

Estamos ahora en posición de manejar campos  $F$  de característica cero y mostrar que, para una extensión finita  $E$  de  $F$ , tenemos que  $\{E:F\} = [E:F]$ . Por definición, esto equivale a probar que toda extensión finita de un campo de característica cero es una extensión separable. Primero daremos una definición.

**Definición** Un campo es **perfecto** si toda extensión finita es una extensión separable.

**Teorema 43.4** *Todo campo de característica cero es perfecto.*

**Demostración** Sea  $E$  una extensión finita de un campo  $F$  de característica cero y sea  $\alpha \in E$ . Entonces,  $f(x) = \text{irr}(\alpha, F)$  se factoriza en  $\bar{F}[x]$  en  $\prod_i (x - \alpha_i)^v$ , donde  $\alpha_i$  son los ceros distintos de  $\text{irr}(\alpha, F)$ , y digamos que  $\alpha = \alpha_1$ . Así,

$$f(x) = \left( \prod_i (x - \alpha_i)^v \right),$$

y como  $v \cdot 1 \neq 0$  para un campo  $F$  de característica 0, debemos tener, por el lema 43.1,

$$\left( \prod_i (x - \alpha_i) \right) \in F[x].$$

Como  $f(x)$  es irreducible y de grado minimal en  $F[x]$  con  $\alpha$  como cero, vemos entonces que  $v = 1$ . Por tanto,  $\alpha$  es separable sobre  $F$  para todas las  $\alpha \in E$ . Por el corolario del teorema 43.3, esto significa que  $E$  es una extensión separable de  $F$ . ■

El lema 43.1 también nos servirá para el caso de un campo finito, aunque la demostración sea un poco difícil. No hay que pensar que no se puede entender el significado de un teorema, sólo porque uno se pierde en la demostración.

**Teorema 43.5** *Todo campo finito es perfecto.*

**Demostración** Sea  $F$  un campo finito de característica  $p$  y sea  $E$  una extensión finita de  $F$ . Sea  $\alpha \in E$ . Necesitamos mostrar que  $\alpha$  es separable sobre  $F$ . Ahora,  $f(x) = \text{irr}(\alpha, F)$  se factoriza en  $\bar{F}$  en  $\prod_i (x - \alpha_i)^v$ , donde las  $\alpha_i$  son los distintos ceros de  $f(x)$  y, digamos,  $\alpha = \alpha_1$ . Sea  $v = p^e$  donde  $p$  no divide a  $e$ . Entonces,

$$f(x) = \prod_i (x - \alpha_i)^v = \left( \prod_i (x - \alpha_i)^{p^e} \right)^e$$

está en  $F[x]$  y, por el lema 43.1,  $\prod_i (x - \alpha_i)^{p^e}$  está en  $F[x]$ , pues  $e \cdot 1 \neq 0$  en  $F$ . Como  $f(x) = \text{irr}(\alpha, F)$  es de grado minimal sobre  $F$  con  $\alpha$  como cero, debemos tener  $e = 1$ .

El teorema 40.5 y la observación que le sigue muestran, entonces, que

$$f(x) = \prod_i (x - \alpha_i)^{p^e} = \prod_i (x^{p^e} - \alpha_i^{p^e}).$$

Así, si vemos  $f(x)$  como  $g(x^{p^t})$  debemos tener que  $g(x) \in F[x]$ . Ahora,  $g(x)$  es separable sobre  $F$  y sus distintos ceros son  $x^{p^t}$ . Considerese  $F(\alpha^{p^t}) = F(x^{p^t})$ . Entonces,  $F(x^{p^t})$  es separable sobre  $F$ . Como  $x^{p^t} - x^{p^t} = (x - \alpha)^{p^t}$ , vemos que  $\alpha$  es el único cero de  $x^{p^t} - x^{p^t}$  en  $\bar{F}$ . Entonces, como espacio vectorial finito sobre un campo finito  $F$ ,  $F(x^{p^t})$  debe ser, de nuevo, un campo finito. Por tanto, por el teorema 40.5, la transformación

$$\sigma_p : F(\alpha^{p^t}) \rightarrow F(\alpha^{p^t})$$

dada por  $a\sigma_p = a^p$  para  $a \in F(\alpha^{p^t})$  es un automorfismo de  $F(\alpha^{p^t})$ . En consecuencia,  $(\sigma_p)^t$  también es un automorfismo de  $F(\alpha^{p^t})$ , y

$$a((\sigma_p)^t) = a^{p^t}.$$

Como un automorfismo de  $F(\alpha^{p^t})$  es una transformación sobre, existe  $\beta \in F(\alpha^{p^t})$  tal que  $\beta((\sigma_p)^t) = x^{p^t}$ . Pero, entonces,  $\beta^{p^t} = x^{p^t}$ , y vimos que  $\alpha$  es el único cero de  $x^{p^t} - \alpha^{p^t}$  de modo que debemos tener  $\beta = \alpha$ . Como  $\beta \in F(\alpha^{p^t})$ , tenemos  $F(\alpha) = F(\alpha^{p^t})$ . Como  $F(\alpha^{p^t})$  era separable sobre  $F$ , vemos ahora que  $F(\alpha)$  es separable sobre  $F$ . Por tanto,  $\alpha$  es separable sobre  $F$  y  $t = 0$ .

Hemos mostrado que para  $\alpha \in E$ ,  $\alpha$  es separable sobre  $F$ . Entonces, por el corolario del teorema 43.3,  $E$  es una extensión separable de  $F$ . ■

Hemos alcanzado nuestro objetivo, el cual ha mostrado que campos de característica 0 y campos finitos, tienen sólo extensiones finitas separables, esto es, estos campos son perfectos. *Para extensiones finitas  $E$  de dichos campos perfectos  $F$  tenemos  $[E:F] = \{E:F\}$ .*

## \*43.4 TEOREMA DEL ELEMENTO PRIMITIVO

En otro párrafo con asterisco usaremos el interesante teorema siguiente.

**Teorema 43.6 (Teorema del elemento primitivo)** *Sea  $E$  una extensión separable finita de un campo infinito  $F$ . Entonces, existe  $\alpha \in E$  tal que  $E = F(\alpha)$ . (Dicho elemento  $\alpha$  es un elemento primitivo.) Esto es, una extensión separable finita de un campo infinito es una extensión simple.*

**Demostración** Lo probamos en el caso en que  $E = F(\beta, \gamma)$ . El razonamiento de inducción es obvio. Supóngase que  $\text{irr}(\beta, F)$  tiene ceros distintos  $\beta = \beta_1, \dots, \beta_m$   $\text{irr}(\gamma, F)$  ceros distintos  $\gamma = \gamma_1, \dots, \gamma_n$  en  $\bar{F}$ , donde todos los ceros son de multiplicidad 1, ya que  $E$  es una extensión separable de  $F$ . Como  $F$  es infinito, podemos encontrar  $a \in F$  tal que

$$a \neq (\beta_i - \beta_j)/(\gamma - \gamma_j)$$

para todas las  $i$  y  $j$ , con  $j \neq 1$ . Esto es,  $a(\gamma - \gamma_j) \neq \beta_i - \beta$ . Haciendo  $\alpha = \beta + a\gamma$ , tenemos  $\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j$ , de modo que

$$\alpha - a\gamma_j \neq \beta_i$$

para todas las  $i$  y todas las  $j \neq 1$ . Sea  $f(x) = \text{irr}(\beta, F)$ , considérese

$$h(x) = f(\alpha - ax) \in (F(\alpha))[x].$$

Ahora,  $h(\gamma) = f(\beta) = 0$ . Sin embargo, por construcción,  $h(\gamma_j) \neq 0$  para  $j \neq 1$ , pues las  $\beta_i$  fueron los únicos ceros de  $f(x)$ . Por tanto,  $h(x)$  y  $g(x) = \text{irr}(\gamma, F)$  tienen un factor común en  $(F(\alpha))[x]$ , a saber,  $\text{irr}(\gamma, F(\alpha))$  que debe ser lineal, pues  $\gamma$  es el único cero común de  $g(x)$  y  $h(x)$ . Así,  $\gamma \in F(\alpha)$  y, por tanto,  $\beta = \alpha - a\gamma$  está en  $F(\alpha)$ . De aquí,  $F(\beta, \gamma) = F(\alpha)$ . ■

**Corolario** Una extensión finita de un campo de característica cero es una extensión simple.

**Demostración** La demostración de este corolario se sigue del teorema 43.6 y del hecho de que todo campo de característica 0 es infinito y perfecto. ■

En realidad, una extensión finita de un campo finito  $F$  también es una extensión simple de  $F$ . Esto se mostrará en el capítulo 45. Así, una vez más, el único posible «caso malo» es una extensión de un campo infinito de característica  $p \neq 0$ . En resumen, *una extensión separable finita de un campo  $F$  es una extensión simple de  $F$* .

## Ejercicios

---

**43.1** Dése un ejemplo de un  $f(x) \in \mathbb{Q}[x]$  que no tenga ceros en  $\mathbb{Q}$ , pero cuyos ceros en  $\mathbb{C}$  sean todos de multiplicidad 2. Explíquese en qué medida esto es consistente con el teorema 43.4, el cual muestra que  $\mathbb{Q}$  es perfecto.

**43.2** Muéstrese que si  $\alpha, \beta \in F$  son ambos separables sobre  $F$ , entonces,  $\alpha \pm \beta, \alpha\beta$  y  $\alpha/\beta$  si  $\beta \neq 0$ , son, todos, separables sobre  $F$ . [Sugerencia: úsese el teorema 43.3 y su corolario.]

**43.3** ¿Falso o verdadero?

- a) Toda extensión finita de todo campo  $F$  es separable sobre  $F$ .
- b) Toda extensión finita de todo campo finito  $F$  es separable sobre  $F$ .
- c) Todo campo de característica 0 es perfecto.
- d) Todo polinomio de grado  $n$  sobre todo campo  $F$  siempre tiene  $n$  ceros distintos en  $F$ .
- e) Todo polinomio de grado  $n$  sobre todo campo perfecto  $F$  siempre tiene  $n$  ceros distintos en  $F$ .
- f) Todo polinomio irreducible de grado  $n$  sobre todo campo perfecto  $F$  siempre tiene  $n$  ceros distintos en  $F$ .
- g) Todo campo algebraicamente cerrado es perfecto.

- h) Todo campo  $F$  tiene alguna extensión algebraica  $E$ , perfecta.
  - i) Si  $E$  es un campo de extensión de descomposición de  $F$  separable finito, entonces  $|G(E/F)| = [E : F]$ .
  - j) Si  $E$  es un campo de extensión de descomposición finito de  $F$ , entonces  $|G(E/F)|$  divide a  $[E : F]$ .
- 

**43.4** Muéstrese que  $\{1, y, \dots, y^{p-1}\}$  es una base para  $\mathbf{Z}_p(y)$  sobre  $\mathbf{Z}_p(y^p)$ , donde  $y$  es una indeterminada. Con referencia al ejemplo 43.1, conclúyase, mediante un razonamiento de grado, que  $x^p - t$  es irreducible sobre  $\mathbf{Z}_p(t)$  donde  $t = y^p$ .

**43.5** Pruébese que si  $E$  es una extensión algebraica de un campo perfecto  $F$ , entonces  $E$  es perfecto.

**43.6** Una extensión algebraica (quizás infinita)  $E$  de un campo  $F$  es una **extensión separable de  $F$**  si para toda  $\alpha \in E$ ,  $f(\alpha)$  es una extensión separable de  $F$ , en el sentido definido en el texto. Muéstrese que si  $E$  es una extensión separable (quizás infinita) e  $F$  y  $K$  es una extensión separable (quizás infinita) de  $E$ , entonces  $K$  es una extensión separable de  $F$ .

**43.7** Sea  $E$  una extensión algebraica de un campo  $F$ . Muéstrese que el conjunto de todos los elementos en  $E$  que son separables sobre  $F$  forman un subcampo de  $E$ , la **cerradura separable de  $F$  en  $E$** . [Sugerencia: úsese el ejercicio 43.2.]

*Los ejercicios 43.8 al 43.15 presentan las derivadas formales en  $F[x]$ .*

**43.8** Sea  $F$  cualquier campo y sea  $f(x) = a_0 + a_1x + \dots + a_ix^i + \dots + a_nx^n$  en  $F[x]$ . La **derivada**  $f'(x)$  de  $f(x)$  es el polinomio

$$f'(x) = a_1 + \dots + (i \cdot 1)a_i x^{i-1} + \dots + (n \cdot 1)a_n x^{n-1},$$

donde  $i \cdot 1$  tiene su significado usual para  $i \in \mathbf{Z}^+$  y  $1 \in F$ . *Estas derivadas son formales; no implican «límites».*

- a) Pruébese que la transformación  $D: F[x] \rightarrow F[x]$  dada por  $D(f(x)) = f'(x)$  es un homomorfismo de  $\langle F[x], + \rangle$ .
- b) Encuéntrese el kernel de  $D$  en el caso que  $F$  sea de característica 0.
- c) Encuéntrese el kernel de  $D$  en el caso que  $F$  sea de característica  $p \neq 0$ .

**43.9** Siguiendo la idea del ejercicio 43.8, muéstrese que:

- a)  $D(af(x)) = aD(f(x))$  para todos los  $f(x) \in F[x]$  y  $a \in F$ .
- b)  $D(f(x)g(x)) = f(x)g'(x) + f'(x)g(x)$  para todos los  $f(x), g(x) \in F[x]$ . [Sugerencia: se ve la parte a) de este ejercicio y el ejercicio anterior y procedase por inducción el grado de  $f(x)g(x)$ .]
- c)  $D((f(x))^m) = (m \cdot 1)f(x)^{m-1}f'(x)$  para todas las  $f(x) \in F[x]$ . [Sugerencia: úsese .]

**43.10** Sea  $f(x) \in F[x]$  y  $\alpha \in F$  un cero de  $f(x)$  de multiplicidad  $v$ . Muéstrese que  $v > 1$  si y sólo si  $\alpha$  es, además, un cero de  $f'(x)$ . [Sugerencia: aplíquese b) y c) del ejercicio 43.1 a la factorización  $f(x) = (x - \alpha)^v g(x)$  de  $f(x)$  en  $F[x]$ .]

**43.11** Muéstrese, del ejercicio 43.10, que todo polinomio irreducible sobre un campo de característica 0 es separable. [Sugerencia: úsese el hecho de que  $\text{irr}(\alpha, F)$  es el polinomio minimal para  $\alpha$  sobre  $F$ .]

**43.12** Muéstrese, del ejercicio 43.10, que un polinomio irreducible  $q(x)$  sobre un campo  $F$  de característica  $p \neq 0$  no es separable si y sólo si cada exponente de cada término de  $q(x)$  es divisible entre  $p$ .

**43.13** Generalícese el ejercicio 43.10, mostrando que  $f(x) \in F[x]$  no tiene ceros de multiplicidad  $> 1$  si y sólo si  $f(x)$  y  $f'(x)$  no tienen factor común no constante en  $\bar{F}[x]$ .

**\*43.14** Con algo más de trabajo que en el ejercicio 43.13, muéstrese que  $f(x) \in F[x]$  no tiene cero de multiplicidad  $> 1$  si y sólo si  $f(x)$  y  $f'(x)$  no tienen factor común no constante en  $F[x]$ . [Sugerencia: úsese el teorema 33.3 para mostrar que si  $l$  es un  $\text{mcd}$  de  $f(x)$  y  $f'(x)$  en  $F[x]$ , también es un  $\text{mcd}$  de estos polinomios en  $\bar{F}[x]$ .]

**\*43.15** Describase un procedimiento factible de cálculo para determinar en qué casos  $f(x) \in F[x]$  tiene un cero de multiplicidad  $> 1$ , sin tener que encontrar, en realidad, los ceros de  $f(x)$ . [Sugerencia: úsese el ejercicio 43.14.]

**\*43.16** Encuéntrese  $\alpha \in Q(\sqrt{2}, \sqrt{3})$  tal que  $Q(\sqrt{2}, \sqrt{3}) = Q(\alpha)$ . Verifíquese, mediante cálculo directo, que  $\sqrt{2}$  y  $\sqrt{3}$  pueden, en efecto, expresarse como polinomios formales en dicha  $\alpha$ , con coeficientes en  $Q$ .

**\*43.17** Obsérvese dónde se usaron, en el teorema 43.6, las hipótesis de que  $F$  era infinito. Muéstrese que si  $F$  es finito con  $s$  elementos y si  $\beta$  y  $\gamma$  son algebraicos sobre  $F$  y de grados  $n$  y  $m$ , respectivamente, entonces existe  $\alpha$  tal que  $F(\beta, \gamma) = F(\alpha)$  siempre que  $s > mn$ . (Este resultado será desplazado por el trabajo del capítulo 45.)

# Extensiones totalmente inseparables

## \* 44.1 EXTENSIONES TOTALMENTE INSEPARABLES

Desarrollamos la teoría de las extensiones totalmente inseparables de manera paralela a nuestro desarrollo de las extensiones separables.

**Definición** Una extensión finita  $E$  de un campo  $F$  es una *extensión totalmente inseparable de  $F$*  si  $\{E:F\} = 1 < [E:F]$ . Un elemento  $\alpha$  de  $\bar{F}$  es *totalmente inseparable sobre  $F$*  si  $F(\alpha)$  es totalmente inseparable sobre  $F$ .

Sabemos que  $\{F(\alpha) : F\}$  es el número de ceros distintos de  $\text{irr}(\alpha, F)$ . Así,  $\alpha$  es *totalmente inseparable sobre  $F$*  si y sólo si  $\text{irr}(\alpha, F)$  tiene sólo un cero de multiplicidad  $> 1$ .

**Ejemplo 44.1** Con respecto al ejemplo 43.1, es claro que  $\mathbf{Z}_p(y)$  es totalmente inseparable sobre  $\mathbf{Z}_p(y^p)$  donde  $y$  es una indeterminada. ■

**Teorema 44.1 (Contraparte del teorema 43.3)** Si  $K$  es una extensión finita de  $E$ ,  $E$  es una extensión finita de  $F$  y  $F < E < K$ , entonces  $K$  es totalmente inseparable sobre  $F$  si y sólo si  $K$  es totalmente inseparable sobre  $E$  y  $E$  es totalmente inseparable sobre  $F$ .

**Demostración** Como  $F < E < K$ , tenemos  $[K:E] > 1$  y  $[E:F] > 1$ . Supóngase que  $K$  es totalmente inseparable sobre  $F$ . Entonces,  $\{K:F\} = 1$  y

$$\{K : F\} = \{K:E\}\{\bar{E}:F\},$$

de modo que debemos tener

$$\{K:E\} = 1 < [K:E] \quad \text{y} \quad [E:F] = 1 < [E:F].$$

Así  $K$  es totalmente inseparable sobre  $E$  y  $E$  es totalmente inseparable sobre  $F$ .

Recíprocamente, si  $K$  es totalmente inseparable sobre  $E$  y  $E$  es totalmente inseparable sobre  $F$ , entonces

$$\{K:F\} = \{K:E\}[E:F] = (1)(1) = 1,$$

y  $[K:F] < 1$ . Así,  $K$  es totalmente inseparable sobre  $F$ . ■

El teorema 44.1 se puede extender de manera obvia, por inducción, a cualquier torre propia finita de extensiones finitas. El campo de arriba es una extensión totalmente inseparable del de abajo si y sólo si cada campo es una extensión totalmente inseparable del que se encuentra inmediatamente debajo de él.

**Corolario (Contraparte del corolario del teorema 43.3)** *Si  $E$  es una extensión finita de  $F$ , entonces  $E$  es totalmente inseparable sobre  $F$  si y sólo si cada  $\alpha$  en  $E$ ,  $\alpha \notin F$ , es totalmente inseparable sobre  $F$ .*

*Dem.:* Supóngase que  $E$  es totalmente inseparable sobre  $F$  y sea  $\alpha \in E$ , con  $\alpha \notin F$ . Entonces,

$$F < F(\alpha) \leq E.$$

Si  $F(\alpha) = E$ , entonces, por la definición de  $\alpha$  totalmente inseparable sobre  $F$ , ya terminamos. Si  $F < F(\alpha) < E$ , entonces el teorema 44.1 muestra que como  $E$  es totalmente inseparable sobre  $F$ ,  $F(\alpha)$  es totalmente inseparable sobre  $F$ .

En forma recíproca, supóngase que para toda  $\alpha \in E$ , con  $\alpha \notin F$ ,  $\alpha$  es totalmente inseparable sobre  $F$ . Como  $E$  es finito sobre  $F$ , existen  $\alpha_1, \dots, \alpha_n$  tales que

$$F < F(\alpha_1) < F(\alpha_1, \alpha_2) < \cdots < E = F(\alpha_1, \dots, \alpha_n).$$

Ahora, como  $\alpha_i$  es totalmente inseparable sobre  $F$ ,  $\alpha_i$  es totalmente inseparable sobre  $F(\alpha_1, \dots, \alpha_{i-1})$ , pues  $q(x) = \text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$  divide  $\text{irr}(\alpha_i, F)$ , de modo que  $\alpha_i$  es el único cero de  $q(x)$  y es de multiplicidad  $> 1$ . Así,  $F(\alpha_1, \dots, \alpha_i)$  es totalmente inseparable sobre  $F(\alpha_1, \dots, \alpha_{i-1})$  y  $E$  es totalmente inseparable sobre  $F$ , por el teorema 44.1, extendido por inducción. ■

Es evidente que hasta ahora hemos seguido un camino paralelo al trabajo del capítulo 43, tanto es así que bien pudimos haber manejado juntas estas ideas.

**\*44.2 CERRADURAS SEPARABLES**

Veamos ahora la razón principal para incluir este material.

**Teorema 44.2** *Sea  $F$  de característica  $p \neq 0$  y sea  $E$  una extensión finita de  $F$ . Entonces,  $\alpha \in E$ ,  $\alpha \notin F$ , es totalmente inseparable sobre  $F$  si y sólo si existe algún entero  $t \geq 1$  tal que  $\alpha^{p^t} \in F$ . Más aún, hay una extensión única  $K$  de  $F$ , con  $F \leq K \leq E$ , tal que  $K$  es separable sobre  $F$ , y  $E = K$  o  $E$  es totalmente inseparable sobre  $K$ .*

**Demostración** Sea  $\alpha \in E$ ,  $\alpha \notin F$ , totalmente inseparable sobre  $F$ . Entonces,  $\text{irr}(\alpha, F)$  tiene un solo cero  $\alpha$  de multiplicidad  $> 1$  y, como se muestra en la demostración del teorema 43.5,  $\text{irr}(\alpha, F)$  debe ser de la forma

$$x^{p^t} - \alpha^{p^t}.$$

De aquí,  $\alpha^{p^t} \in F$  para alguna  $t \geq 1$ .

En forma recíproca, si  $\alpha^{p^t} \in F$  para alguna  $t \geq 1$ , donde  $\alpha \in E$  y  $\alpha \notin F$ , entonces

$$x^{p^t} - \alpha^{p^t} = (x - \alpha)^{p^t},$$

y  $(x^{p^t} - \alpha^{p^t}) \in F[x]$ , lo cual muestra que  $\text{irr}(\alpha, F)$  divide  $(x - \alpha)^{p^t}$ . Así,  $\text{irr}(\alpha, F)$  tiene  $\alpha$  como único cero y este cero es de multiplicidad  $> 1$ , de modo que  $\alpha$  es totalmente inseparable sobre  $F$ .

Para la segunda parte del teorema, sea  $E = F(\alpha_1, \dots, \alpha_n)$ . Entonces, si

$$\text{irr}(\alpha_i, F) = \prod_j (x^{p^{t_{ij}}} - \alpha_{ij}^{p^{t_{ij}}}),$$

con  $\alpha_{i1} = \alpha_i$ , sea  $\beta_{ij} = \alpha_{ij}^{p^{t_{ij}}}$ . Tenemos  $F(\beta_{11}, \beta_{21}, \dots, \beta_{n1}) \leq E$  y  $\beta_{i1}$  es un cero de

$$f(x) = \prod_j (x - \beta_{ij}),$$

donde  $f(x) \in F[x]$ . Ahora bien, como elevar a la potencia  $p$  es un isomorfismo  $\sigma_p$  de  $E$  en  $E$ , elevar a la potencia  $p^t$  es la transformación isomorfa  $(\sigma_p)^t$  de  $E$  en  $E$ . Luego, como las  $\alpha_{ij}$  son todas distintas para  $i$  fija, también lo son las  $\beta_{ij}$  para  $i$  fija. Por tanto,  $\beta_{ij}$  es separable sobre  $F$  porque es un cero de un polinomio  $f(x)$  en  $F[x]$  con ceros de multiplicidad 1. Entonces, por la demostración del corolario del teorema 43.3,

$$K = F(\beta_{11}, \beta_{21}, \dots, \beta_{n1})$$

es separable sobre  $F$ . Si todas las  $p^{t_{ii}} = 1$ , entonces  $K = E$ . Si alguna  $p^{t_{ii}} \neq 1$ , entonces  $K \neq E$  y  $\alpha_i^{p^{t_{ii}}} = \beta_{i1}$  está en  $K$ , lo cual muestra que cada  $\alpha_i \notin K$  es

totalmente inseparable sobre  $K$ , debido a la primera parte de este teorema. De aquí que, por la demostración del corolario del teorema 44.1,  $E = K(x_1, \dots, x_n)$  es totalmente inseparable sobre  $K$ .

Se sigue de los corolarios de los teoremas 43.3 y 44.1 que el campo  $K$  del teorema 44.2 consta de todos los elementos  $\alpha$  en  $E$  que son separables sobre  $F$ . Así,  $K$  es único. ■

**Definición** El campo único  $K$  del teorema 44.2 es la *cerradura separable de  $F$  en  $E$* .

El teorema anterior muestra la estructura precisa de las extensiones totalmente inseparables de un campo de característica  $p$ . Dicha extensión se puede obtener agregando repetidamente raíces  $p$ -ésimas de elementos (que no sean ya potencias  $p$ -ésimas) para obtener campos cada vez mayores.

Insistimos en que el teorema 44.2 se cumple para extensiones algebraicas infinitas  $E$  de  $F$ . La demostración de la primera afirmación del teorema también es válida para el caso de extensiones infinitas. Para la segunda parte, como  $\alpha \pm \beta$ ,  $\alpha\beta$  y  $\alpha/\beta$  para  $\beta \neq 0$  están contenidos en el campo  $F(\alpha, \beta)$ , todos los elementos de  $E$  separables sobre  $F$  forman un subcampo  $K$  de  $E$ , la *cerradura separable de  $F$  en  $E$* . Se sigue que un  $\alpha \in E$ ,  $\alpha \notin K$  es totalmente inseparable sobre  $K$ , puesto que  $\alpha$  y todos los coeficientes de  $\text{irr}(\alpha, K)$  están en una extensión finita de  $F$  y, entonces, se puede aplicar el teorema 44.2.

## Ejercicios

---

\*44.1 Sean  $y$  y  $z$  indeterminadas y sean  $u = y^{12}$  y  $v = z^{18}$ . Describase la cerradura separable de  $Z_3(u, v)$  en  $Z_3(y, z)$ .

\*44.2 Sean  $y$  y  $z$  indeterminadas, y sean  $u = y^{12}$  y  $v = y^2z^{18}$ . Describase la cerradura separable de  $Z_3(u, v)$  en  $Z_3(y, z)$ .

\*44.3 Muéstrese que si  $E$  es una extensión algebraica de un campo  $F$ , entonces el conjunto de todos los elementos de  $E$  totalmente inseparables sobre  $F$  forman un subcampo de  $E$ , la *cerradura totalmente inseparable de  $F$  en  $E$* .

\*44.4 Con respecto al ejercicio 44.1, describase la cerradura totalmente inseparable (véase el ejercicio 44.3) de  $Z_3(u, v)$  en  $Z_3(y, z)$ .

\*44.5 Respecto al ejercicio 44.2, describase la cerradura totalmente inseparable de  $Z_3(u, v)$  en  $Z_3(y, z)$ .

\*44.6 ¿Falso o verdadero?

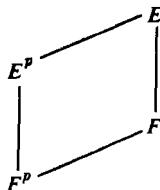
- a) Ninguna extensión algebraica propia de un campo infinito de característica  $p \neq 0$ , es una extensión separable.
- b) Si  $F(\alpha)$  es totalmente inseparable sobre  $F$  de característica  $p \neq 0$ , entonces  $\alpha^{p^t} \in F$  para alguna  $t > 0$ .
- c) Para una indeterminada  $y$ ,  $Z_5(y)$  es separable sobre  $Z_5(y^5)$ .
- d) Para una indeterminada  $y$ ,  $Z_5(y)$  es separable sobre  $Z_5(y^{10})$ .
- e) Para una indeterminada  $y$ ,  $Z_5(y)$  es totalmente inseparable sobre  $Z_5(y^{10})$ .

## 408 EXTENSIONES TOTALMENTE INSEPARABLES

- f) Si  $F$  es un campo y  $\alpha$  es algebraico sobre  $F$ , entonces o bien  $\alpha$  es separable o bien es totalmente inseparable sobre  $F$ .
  - g) Si  $E$  es una extensión algebraica de un campo  $F$ , entonces  $F$  tiene una cerradura separable en  $E$ .
  - h) Si  $E$  es una extensión algebraica de un campo  $F$ , entonces  $E$  es totalmente inseparable sobre la cerradura separable de  $F$  en  $E$ .
  - i) Si  $E$  es una extensión algebraica de un campo  $F$  y  $E$  no es una extensión separable de  $F$ , entonces  $E$  es totalmente inseparable sobre la cerradura separable de  $F$  en  $E$ .
  - j) Si  $\alpha$  es totalmente inseparable sobre  $F$ , entonces  $\alpha$  es el único cero de  $\text{irr}(\alpha, F)$ .
- 

\*44.7 Muéstrese que un campo  $F$  de característica  $p \neq 0$  es perfecto si y sólo si  $F^p = F$ , esto es, todo elemento de  $F$  es una potencia  $p$ -ésima de algún elemento de  $F$ .

\*44.8 Sea  $E$  una extensión finita de un campo  $F$  de característica  $p$ . En la notación del ejercicio 44.7, muéstrese que  $E^p = E$  si y sólo si  $F^p = F$ . [Sugerencia: considérese que la transformación  $\sigma_p: E \rightarrow E$  definida por  $\alpha\sigma_p = \alpha^p$  para  $\alpha \in E$  es un isomorfismo. Considérese el diagrama en la figura 44.1 y dense razonamientos de grados.]



**Figura 44.1**

## Campos finitos

El propósito de este capítulo es determinar la estructura de todos los campos finitos. Mostraremos que para todo primo  $p$  y entero positivo  $n$ , hay exactamente un campo finito (salvo isomorfismo) de orden  $p^n$ . Por lo común, nos referimos a este campo  $\text{CG}(p^n)$  como al **campo de Galois de orden  $p^n$** . Usaremos buena parte de nuestro material de grupos cíclicos. Las demostraciones son sencillas y elegantes.

### 45.1 ESTRUCTURA DE UN CAMPO FINITO

Es fácil ver que todos los campos finitos deben tener orden igual a la potencia de un primo.

**Teorema 45.1** *Sea  $E$  una extensión finita de grado  $n$  sobre un campo finito  $F$ . Si  $F$  tiene  $q$  elementos, entonces  $E$  tiene  $q^n$  elementos.*

**Demostración** Sea  $\{\alpha_1, \dots, \alpha_n\}$  una base para  $E$  como espacio vectorial sobre  $F$ . Entonces, toda  $\beta \in E$  puede escribirse de manera única en la forma

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$$

para  $b_i \in F$ . Como cada  $b_i$  puede ser alguno de los  $q$  elementos de  $F$ , entonces el número total de dichas combinaciones lineales distintas de las  $\alpha_i$  es  $q^n$ . ■

**Corolario** *Si  $E$  es un campo finito de característica  $p$ , entonces  $E$  contiene*

*Demostración* Todo campo finito  $E$  es una extensión finita de un campo primo isomorfo al campo  $\mathbf{Z}_p$ , donde  $p$  es la característica de  $E$ . El corolario se sigue inmediatamente del teorema 45.1. ■

Pasemos ahora al estudio de la estructura multiplicativa de un campo finito. El siguiente teorema mostrará cómo puede formarse cualquier campo finito del subcampo primo.

**Teorema 45.2** *Un campo finito  $E$  de  $p^n$  elementos es el campo de descomposición de  $x^{p^n} - x$  sobre su subcampo primo  $\mathbf{Z}_p$  (salvo isomorfismo).*

*Demostración* Sea  $E$  un campo finito con  $p^n$  elementos donde  $p$  es la característica de  $E$ . El conjunto  $E^*$  de elementos distintos de cero de  $E$  forma un grupo multiplicativo de orden  $p^n - 1$  bajo la multiplicación de campo. Para  $\alpha \in E^*$ , el orden de  $\alpha$  en este grupo divide el orden  $p^n - 1$  del grupo. Así, para  $\alpha \in E^*$  tenemos  $\alpha^{p^n-1} = 1$ , de modo que  $\alpha^{p^n} = \alpha$ . Por tanto, todo elemento en  $E$  es un cero de  $x^{p^n} - x$ . Como  $x^{p^n} - x$  puede tener a lo más  $p^n$  ceros, vemos que  $E$  es el campo de descomposición de  $x^{p^n} - x$  sobre  $\mathbf{Z}_p$ . ■

**Definición** Un elemento  $\alpha$  de un campo es una **raíz  $n$ -ésima del unitario** si  $\alpha^n = 1$ . Es una **raíz  $n$ -ésima primitiva del unitario** si  $\alpha^n = 1$  y  $\alpha^m \neq 1$  para  $0 < m < n$ .

Así, los elementos distintos de cero de un campo finito de  $p^n$  elementos son todos raíces  $(p^n - 1)$ -ésimas del unitario.

Sea  $F$  cualquier campo y sea  $U_n$  el conjunto de todas las raíces  $n$ -ésimas del unitario en  $F$ . Es fácil ver que  $U_n$  es un grupo bajo la multiplicación de campo. Si  $a^n = 1$  y  $b^n = 1$ , entonces

$$(ab)^n = a^n b^n = 1,$$

de modo que la multiplicación es cerrada en  $U_n$ . Es igualmente trivial verificar los axiomas de grupo. Aseguramos que  $U_n$  es un grupo cíclico. De hecho, se cumple el siguiente resultado más general.

**Teorema 45.3** *Si  $G$  es un subgrupo finito multiplicativo del grupo multiplicativo  $\langle F^*, \cdot \rangle$  de los elementos distintos de cero de un campo  $F$ , entonces  $G$  es cíclico.*

*Demostración* Por el teorema 9.3, como grupo abeliano finito,  $G$  es isomorfo a un producto directo  $\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r}$  de grupos cíclicos, donde  $m_i$  divide a  $m_{i+1}$ . Pensemos que cada  $\mathbf{Z}_{m_i}$  es un grupo de orden  $m_i$  en notación multiplicativa. Entonces, para  $a_i \in \mathbf{Z}_{m_i}$ ,  $a_i^{m_i} = 1$ , de modo que  $a_i^{m_r} = 1$ , pues  $m_i$  divide a  $m_r$ . Así, para todas las  $\alpha \in G$ , tenemos  $\alpha^{m_r} = 1$ , de modo que todo elemento de  $G$  es un cero de  $x^{m_r} - 1$ . Pero  $G$  tiene  $\prod_{i=1}^r m_i$  elementos, mientras que  $x^{m_r} - 1$  tiene a lo más  $m_r$  ceros en un campo. Por tanto, debemos tener  $r = 1$ , de modo que  $G$  es cíclico. ■

**Corolario 1** *El grupo multiplicativo de todos los elementos distintos de cero de un campo finito bajo la multiplicación de campo es cíclico.*

**Demostración** La demostración del corolario 1 es inmediata del teorema 45.3. ■

**Corolario 2** *Una extensión finita  $E$  de un campo finito  $F$  es una extensión simple de  $F$ .*

**Demostración** Sea  $\alpha$  un generador para el grupo cíclico  $E^*$  de elementos distintos de cero de  $E$ . Entonces, obviamente  $E = F(\alpha)$ . ■

**Ejemplo 45.1** Considérese el campo finito  $\mathbf{Z}_{11}$ . Por el corolario 1 del teorema 45.3,  $\langle \mathbf{Z}_{11}^*, \cdot \rangle$  es cíclico. Tratemos de encontrar un generador de  $\mathbf{Z}_{11}^*$  mediante fuerza bruta e ignorancia. Comencemos por 2. Como  $|\mathbf{Z}_{11}^*| = 10$ , 2 debe ser un elemento de  $\mathbf{Z}_{11}^*$  de orden que divida a 10, esto es, 2, 5 ó 10. Ahora,

$$2^2 = 4, \quad 2^4 = 4^2 = 5 \quad \text{y} \quad 2^5 = (2)(5) = 10 = -1.$$

Entonces, ni  $2^2$ , ni  $2^5$  son 1, pero es claro que  $2^{10} = 1$ , de modo que 2 es un generador de  $\mathbf{Z}_{11}^*$ , esto es, 2 es una raíz décima primitiva del unitario en  $\mathbf{Z}_{11}$ . Tuvimos suerte.

Por la teoría de los grupos cíclicos, todos los generadores de  $\mathbf{Z}_{11}^*$ , esto es, todas las raíces décimas primitivas del unitario en  $\mathbf{Z}_{11}$  son, entonces, de la forma  $2^n$  donde  $n$  es primo relativo con 10. Estos elementos son

$$\begin{aligned} 2^1 &= 2, & 2^3 &= 8, \\ 2^7 &= 7, & 2^9 &= 6. \end{aligned}$$

Las raíces quintas primitivas del unitario en  $\mathbf{Z}_{11}$  son de la forma  $2^m$  donde el mcd de  $m$  y 10 es 2, esto es,

$$\begin{aligned} 2^2 &= 4, & 2^4 &= 5, \\ 2^6 &= 9, & 2^8 &= 3. \end{aligned}$$

La raíz cuadrada primitiva del unitario en  $\mathbf{Z}_{11}$  es  $2^5 = 10 = -1$ . ■

## 45.2 LA EXISTENCIA DE CG( $p^n$ )

Pasemos ahora a la cuestión de la existencia de un campo finito de orden  $p^r$  para toda potencia de primo  $p^r$ ,  $r > 0$ . Necesitamos el lema siguiente.

**Lema 45.1** *Si  $F$  es un campo finito de característica  $p$ , entonces  $x^{p^n} - x$  tiene  $p^n$  ceros distintos en el campo de descomposición  $K \leq \bar{F}$  de  $x^{p^n} - x$  sobre  $F$ .*

*Demostración* Sea  $F$  un campo finito de característica  $p$  y sea  $K$  el campo de descomposición en  $\bar{F}$  del polinomio  $x^{p^n} - x$  sobre  $F$ . Se mostrará que  $x^{p^n} - x$  tiene  $p^n$  ceros distintos en  $K$ . Como no hemos tenido tiempo para presentar una teoría algebraica de las derivadas, no disponemos de esta elegante técnica, así que procederemos mediante la fuerza bruta. Obviamente, 0 es un cero de  $x^{p^n} - x$  de multiplicidad 1. Supóngase que  $\alpha \neq 0$  es un cero de  $x^{p^n} - x$  y, por tanto, es un cero de  $f(x) = x^{p^n-1} - 1$ . Entonces,  $x - \alpha$  es un factor de  $f(x)$  en  $K[x]$  y, mediante división, encontramos que

$$\begin{aligned}\frac{f(x)}{(x - \alpha)} &= g(x) \\ &= x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \cdots + \alpha^{p^n-3} x + \alpha^{p^n-2}.\end{aligned}$$

Ahora,  $g(x)$  tiene  $p^n - 1$  sumandos y en  $g(\alpha)$  cada sumando es

$$\alpha^{p^n-2} = \frac{\alpha^{p^n-1}}{\alpha} = \frac{1}{\alpha}.$$

Así,

$$g(\alpha) = [(p^n - 1) \cdot 1] \frac{1}{\alpha} = -\frac{1}{\alpha}.$$

puesto que estamos en un campo de característica  $p$ . Por tanto,  $g(\alpha) \neq 0$ , de modo que  $\alpha$  es un cero de  $f(x)$  de multiplicidad 1. ■

**Teorema 45.4** *Existe un campo finito  $CG(p^n)$  de  $p^n$  elementos para toda potencia de primo  $p^n$ .*

*Demostración* Sea  $K \leq \mathbf{Z}_p$  el campo de descomposición de  $x^{p^n} - x$  sobre  $\mathbf{Z}_p$ , y sea  $F$  el subconjunto de  $K$  formado por todos los ceros de  $x^{p^n} - x$  en  $K$ . Entonces, para  $\alpha, \beta \in F$  las ecuaciones

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$$

y

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$$

muestran que  $F$  es cerrado bajo la suma, resta y multiplicación. Es claro que 0 y 1 son ceros de  $x^{p^n} - x$ . Para  $\alpha \neq 0$ ,  $\alpha^{p^n} = \alpha$  implica que  $(1/\alpha)^{p^n} = 1/\alpha$ . Así,  $F$  es un subcampo de  $K$  que contiene a  $\mathbf{Z}_p$ . Como  $K$  es la menor extensión de  $\mathbf{Z}_p$  que contiene los ceros de  $x^{p^n} - x$ , vemos que se debe tener  $K = F$ . Por tanto,  $K$  es el campo deseado de  $p^n$  elementos, ya que en el lema 45.1 se mostró que  $x^{p^n} - x$  tiene  $p^n$  ceros distintos en  $\mathbf{Z}_p$ . ■

**Corolario** Si  $F$  es cualquier campo finito, entonces para todo entero positivo  $n$  existe un polinomio irreducible en  $F[x]$  de grado  $n$ .

**Demostración** Sea  $F$  con  $q = p^r$  elementos, donde  $p$  es la característica de  $F$ . Por el teorema 45.4, existe un campo (salvo isomorfismo)  $K \leq F$  que contiene  $\mathbf{Z}_p$  y consta, precisamente, de los ceros de  $x^{p^r} - x$ . Por el teorema 45.2, todo elemento de  $F$  es un cero de  $x^{p^r} - x$ . Ahora,  $p^{rs} = p^r p^{(s-1)}$ . Al aplicar en forma repetida esta ecuación a los exponentes y al usar el hecho de que para  $\alpha \in F$  tenemos que  $\alpha^{p^r} = \alpha$ , vemos que para  $\alpha \in F$ ,

$$\alpha^{p^{rn}} = \alpha^{p^{r(n-1)}} = \alpha^{p^{r(n-2)}} = \cdots = \alpha^{p^r} = \alpha.$$

Así,  $F \leq K$ . Entonces, el teorema 45.1 muestra que debemos tener  $[K : F] = n$ . En el corolario 2 del teorema 45.3 vimos que  $K$  es simple sobre  $F$ , de modo que  $K = F(\beta)$  para alguna  $\beta \in K$ . Por tanto,  $\text{irr}(\beta, F)$  debe ser de grado  $n$ . ■

## Ejercicios

---

**45.1** Encuéntrense todos los generadores de cada uno de los siguientes grupos cíclicos. (Recuérdese la teoría de los grupos cíclicos.)

- a)  $\langle \mathbf{Z}_{17}^*, \cdot \rangle$       b)  $\langle \mathbf{Z}_{17}, \cdot \rangle$       c)  $\langle \mathbf{Z}_{23}^*, \cdot \rangle$

**45.2** (Recuérdese la teoría de los grupos cíclicos.)

- a) Encuéntrese el número de raíces octavas primitivas del unitario en  $\text{CG}(9)$ .  
 b) Encuéntrese el número de raíces 18-ésimas primitivas del unitario en  $\text{CG}(19)$ .  
 c) Encuéntrese el número de raíces 15-ésimas primitivas del unitario en  $\text{CG}(31)$ .  
 d) Encuéntrese el número de raíces décimas primitivas del unitario en  $\text{CG}(23)$ .

**45.3** Sea  $\mathbf{Z}_2$  una cerradura algebraica de  $\mathbf{Z}_2$  y sean  $\alpha, \beta \in \mathbf{Z}_2$  ceros de  $x^3 + x^2 + 1$  y  $x^3 + x + 1$ , respectivamente. Usando los resultados de esta sección, muéstrese que  $\mathbf{Z}_2(\alpha) = \mathbf{Z}_2(\beta)$ .

**45.4** Muéstrese que todo polinomio irreducible en  $\mathbf{Z}_p[x]$  es un divisor de  $x^{p^n} - x$  para alguna  $n$ .

**45.5** ¿Falso o verdadero?

- a) Los elementos distintos de cero de todo campo finito forman un grupo cíclico bajo la multiplicación.
- b) Los elementos de todo campo finito forman un grupo cíclico bajo la suma.
- c) Los ceros en  $\mathbf{C}$  de  $(x^{28} - 1) \in \mathbf{Q}[x]$  forman grupo cíclico bajo la multiplicación.
- d) Existe un campo finito de 60 elementos.
- e) Existe un campo finito de 125 elementos.
- f) Existe un campo finito de 36 elementos.
- g) El número complejo  $i$  es una raíz cuarta primitiva del unitario.
- h) Existe un polinomio irreducible de grado 58 en  $\mathbf{Z}_2[x]$ .
- i) Los elementos distintos de cero de  $\mathbf{Q}$  forman un grupo cíclico  $\mathbf{Q}^*$  bajo la multiplicación del campo.

- j) Si  $F$  es un campo finito, entonces todo isomorfismo que transforma  $F$  en una cerradura algebraica  $\bar{F}$  de  $F$ , es un automorfismo de  $F$ .

**45.6** Sea  $F$  un campo finito de  $p^n$  elementos que contiene el subcampo primo  $\mathbb{Z}_p$ . Muéstrese que si  $\alpha \in F$  es un generador del grupo cíclico  $\langle F^*, \cdot \rangle$  de elementos distintos de cero de  $F$ , entonces  $\text{grad}(\alpha, \mathbb{Z}_p) = n$ .

**45.7** Muéstrese que un campo finito de  $p^n$  elementos tiene, exactamente, un subcampo de  $p^m$  elementos para cada divisor  $m$  de  $n$ .

**45.8** Muéstrese que  $x^{p^n} - x$  es el producto de todos los polinomios mónicos irreducibles en  $\mathbb{Z}_p[x]$  de grado  $d$  que divide a  $n$ .

**45.9** Sea  $p$  un primo impar.

- Muéstrese que para  $a \in \mathbb{Z}$ , donde  $a \not\equiv 0 \pmod{p}$ , la congruencia  $x^2 \equiv a \pmod{p}$  tiene solución en  $\mathbb{Z}$  si y sólo si  $a^{(p-1)/2} \equiv 1 \pmod{p}$ . [Sugerencia: formúlese un enunciado equivalente en el campo finito  $\mathbb{Z}_p$  y úsese la teoría de los grupos cíclicos.]
- Usando la parte a), determínese si el polinomio  $x^2 - 6$  es irreducible o no en  $\mathbb{Z}_{17}[x]$ .

**45.10** Muéstrese que dos campos finitos del mismo orden son isomorfos.

**45.11** Usese el ejercicio 43.10 para mostrar que  $x^{p^n} - x$  no tiene ceros de multiplicidad  $> 1$  en  $\mathbb{Z}_p$ . (Véase la demostración del lema 45.1.)

**45.12** Sea  $E$  un campo finito de orden  $p^n$ .

- Muéstrese que el automorfismo de Frobenius  $\sigma_p$  tiene orden  $n$ .
- Dedúzcase de a) que  $G(E/\mathbb{Z}_p)$  es cíclico de orden  $n$  con generador  $\sigma_p$ . [Sugerencia: recuérdese que

$$|G(E/F)| = \{E : F\} = [E : F]$$

para un campo de descomposición  $E$  que sea extensión finita y separable de  $F$ .]

## 46

## Teoría de Galois

### 46.1 RESUMEN

Quizás este capítulo sea el clímax de la elegancia del tema tratado en este libro. La teoría de Galois da una bella interrelación entre la teoría de grupos y la de campos. Desde el capítulo 40, hemos dirigido nuestro trabajo para alcanzar este objetivo. Comenzaremos recordando los principales resultados desarrollados.

- 1 Sean  $F \leq E \leq \bar{F}$ ,  $\alpha \in E$  y  $\beta$  un conjugado de  $\alpha$  sobre  $F$ , esto es,  $\beta$  es también un cero de  $\text{irr}(\alpha, F)$ . Entonces, existe un isomorfismo  $\psi_{\alpha, \beta}$  que transforma  $F(\alpha)$  sobre  $F(\beta)$ , deja fijo  $F$  y transforma  $\alpha$  en  $\beta$ .
- 2 Si  $F \leq E \leq \bar{F}$  y  $\alpha \in E$ , entonces, un automorfismo  $\sigma$  de  $\bar{F}$  que deje fijo  $F$  debe transformar  $\alpha$  sobre algún conjugado de  $\alpha$  sobre  $F$ .
- 3 Si  $F \leq E$ , la colección de todos los automorfismos de  $E$  que dejan fijo  $F$  forman un grupo  $G(E/F)$ . Para cualquier subconjunto  $S$  de  $G(E/F)$ , el conjunto de todos los elementos de  $E$  que quedan fijos bajo todos los elementos de  $S$ , es un campo  $E_S$ . Además,  $F \leq E_{G(E/F)}$ .
- 4 Un campo  $E$ ,  $F \leq E \leq \bar{F}$  es un campo de descomposición sobre  $F$  si y sólo si todo isomorfismo de  $E$  en  $\bar{F}$  que deje fijo  $F$  es un automorfismo de  $E$ . Si  $E$  es una extensión finita y un campo de descomposición sobre  $F$ , entonces,  $|G(E/F)| = [E:F]$ .
- 5 Si  $E$  es una extensión finita de  $F$ , entonces  $[E:F]$  divide  $[E:\bar{F}]$ . Si, además,  $F$  es separable sobre  $F$ , entonces  $[E:F] = [E:\bar{F}]$ . Además,  $E$  es separable sobre  $F$  si y sólo si  $\text{irr}(\alpha, F)$  tiene todos los ceros de multiplicidad 1 para toda  $\alpha \in E$ .
- 6 Si  $E$  es una extensión finita de  $F$  y es un campo de descomposición separable sobre  $F$ , entonces  $|G(E/F)| = [E:F] = [E:\bar{F}]$ .

## 46.2 EXTENSIONES NORMALES

Estaremos interesados en extensiones finitas  $K$  de  $F$  tales que todo isomorfismo de  $K$  que deje fijo  $F$  sea un automorfismo de  $K$  y tal que

$$[K:F] = \{K:F\}.$$

En vista de los números 4 y 5 del resumen, éstas son las extensiones finitas de  $F$  que son campos de descomposición separables sobre  $F$ .

**Definición** Una extensión finita  $K$  de  $F$  es una *extensión normal finita de  $F$* , si  $K$  es un campo de descomposición separable sobre  $F$ .

Supóngase que  $K$  es una extensión normal finita de  $F$ , donde, como es usual,  $K \leq \bar{F}$ . Entonces, por el resultado 4, todo automorfismo de  $\bar{F}$  que deja fijo  $F$  induce un automorfismo de  $K$ . Como antes, hacemos  $G(K/F)$  el grupo de todos los automorfismos de  $K$  que dejan fijo  $F$ . Después de un resultado más, estaremos listos para ilustrar el teorema principal.

**Teorema 46.1** Sea  $K$  una extensión normal finita de  $F$  y sea  $E$  una extensión de  $F$ , donde  $F \leq E \leq K \leq \bar{F}$ . Entonces,  $K$  es una extensión normal finita de  $E$  y  $G(K/E)$  es, precisamente, el subgrupo de  $G(K/F)$  formado por todos aquellos automorfismos que dejan fijo  $E$ . Más aún, dos automorfismos  $\sigma$  y  $\tau$  en  $G(K/F)$  inducen el mismo isomorfismo de  $E$  en  $\bar{F}$  si y sólo si están en la misma clase lateral derecha de  $G(K/E)$  en  $G(K/F)$ .

**Demostración** Si  $K$  es el campo de descomposición de un conjunto  $\{f_i(x) \mid i \in I\}$  de polinomios en  $F[x]$ , entonces, claramente,  $K$  es el campo de descomposición sobre  $E$  del mismo conjunto de polinomios considerados como elementos de  $E[x]$ . El teorema 43.3 muestra que  $K$  es separable sobre  $E$ , pues  $K$  es separable sobre  $F$ . Así,  $K$  es una extensión normal de  $E$ . Esto demuestra la primera contención.

Es claro que todo elemento de  $G(K/E)$  es un automorfismo de  $K$  que deja fijo  $F$ , pues incluso, deja fijo el campo  $E$  posiblemente mayor. Así,  $G(K/E)$  puede considerarse un subconjunto de  $G(K/F)$ . Como  $G(K/E)$  también es grupo bajo la composición de funciones, vemos que  $G(K/E) \leq G(K/F)$ .

Por último, para  $\sigma$  y  $\tau$  en  $G(K/F)$ ,  $\sigma$  y  $\tau$  están en la misma clase lateral derecha de  $G(K/E)$  si y sólo si  $\sigma\tau^{-1} \in G(K/E)$  o si y sólo si  $\sigma = \mu\tau$  para  $\mu \in G(K/E)$ . Pero si  $\sigma = \mu\tau$  para  $\mu \in G(K/E)$ , entonces, para  $\alpha \in E$ , tenemos

$$\alpha\sigma = \alpha(\mu\tau) = (\alpha\mu)\tau = \alpha\tau,$$

pues  $\alpha\mu = \alpha$  para  $\alpha \in E$ . En forma recíproca, si  $\alpha\sigma = \alpha\tau$  para todas las  $\alpha \in E$ , entonces

$$\alpha(\sigma\tau^{-1}) = \alpha$$

para todas las  $\alpha \in E$ , de modo que  $\sigma\tau^{-1}$  deja fijo  $E$  y  $\mu = \sigma\tau^{-1}$  está, entonces, en  $G(K/E)$ . ■

El teorema anterior muestra que existe una correspondencia uno a uno entre clases laterales derecha de  $G(K/E)$  en  $G(K/F)$  y los isomorfismos de  $E$  que dejan fijo  $F$ . Nótese que no podemos decir que estas clases laterales derechas correspondan a *automorfismos* de  $E$  sobre  $F$ , pues entonces,  $E$  no sería un campo de descomposición sobre  $F$ . Ahora, si  $E$  es una extensión *normal* de  $F$ , entonces estos isomorfismos serán automorfismos de  $E$  sobre  $F$ . Quizás el lector piense que esto sucederá si y sólo si  $G(K/E)$  es un subgrupo *normal* de  $G(K/F)$  y, en efecto, así es; esto es, los dos usos diferentes de la palabra *normal* están, en realidad, íntimamente relacionados. Así, si  $E$  es una extensión normal de  $F$ , entonces las clases laterales derechas de  $G(K/E)$  en  $G(K/F)$  pueden considerarse elementos del *grupo factor*  $G(K/F)/G(K/E)$  que es, entonces, un grupo de automorfismos actuando en  $E$  y que deja fijo  $F$ . Mostraremos que este grupo factor es isomorfo a  $G(E/F)$ .

## 46.3 EL TEOREMA PRINCIPAL

El teorema principal de la teoría de Galois afirma que para una extensión normal finita  $K$  de un campo  $F$ , existe una correspondencia uno a uno entre los subgrupos de  $G(K/F)$  y los campos intermedios  $E$ , donde  $F \leq E \leq K$ . Esta correspondencia asocia a cada campo intermedio  $E$ , el subgrupo  $G(K/E)$ . Por supuesto, podemos ir en la otra dirección y comenzar con un subgrupo  $H$  de  $G(K/F)$  y asociar a  $H$  su campo fijo  $K_H$ . Ilustraremos esto con un ejemplo fácil y después enunciaremos el teorema y analizaremos su demostración.

**Ejemplo 46.1** Sea  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Ahora,  $K$  es una extensión normal de  $\mathbb{Q}$ , y en el ejemplo 40.4 se mostró que hay cuatro automorfismos de  $K$  que dejan fijo  $\mathbb{Q}$ . Los recordaremos dando sus valores en la base  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  para  $K$  sobre  $\mathbb{Q}$ .

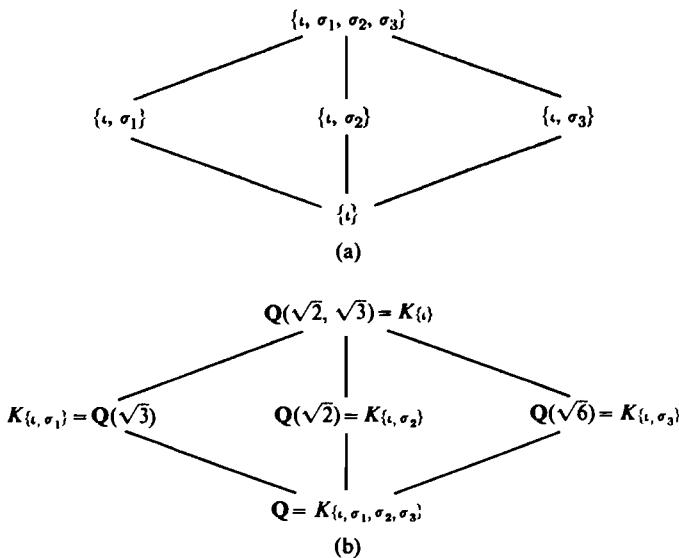
- i: La transformación identidad.
- $\sigma_1$ : Transforma  $\sqrt{2}$  sobre  $-\sqrt{2}$ ,  $\sqrt{6}$  sobre  $-\sqrt{6}$  y deja fijos los demás.
- $\sigma_2$ : Transforma  $\sqrt{3}$  sobre  $-\sqrt{3}$ ,  $\sqrt{6}$  sobre  $-\sqrt{6}$  y deja fijos los demás.
- $\sigma_3$ : Transforma  $\sqrt{2}$  sobre  $-\sqrt{2}$ ,  $\sqrt{3}$  sobre  $-\sqrt{3}$  y deja fijos los demás.

Vimos que  $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$  es isomorfo al 4-grupo de Klein. La lista completa de los subgrupos, con cada subgrupo apareado con el campo intermedio correspondiente que deja fijo, es como sigue:

$$\begin{aligned} \{\iota, \sigma_1, \sigma_2, \sigma_3\} &\leftrightarrow \mathbb{Q}, \\ \{\iota, \sigma_1\} &\leftrightarrow \mathbb{Q}(\sqrt{3}), \\ \{\iota, \sigma_2\} &\leftrightarrow \mathbb{Q}(\sqrt{2}), \\ \{\iota, \sigma_3\} &\leftrightarrow \mathbb{Q}(\sqrt{6}), \\ \{\iota\} &\leftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}). \end{aligned}$$

Todos los subgrupos del grupo abeliano  $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$  son subgrupos normales y, claramente, todos los campos intermedios son extensiones normales de  $\mathbb{Q}$ . ¿No es elegante?

Nótese que si un subgrupo está contenido en otro, entonces el mayor de los dos subgrupos corresponde al menor de los dos campos fijos correspondientes. La razón es clara. Cuanto mayor sea el subgrupo, esto es, cuantos más automorfismos haya, tanto menor será el campo fijo, esto es, tantos menos elementos quedan fijos. En la figura 46.1 se dan los diagramas reticulares correspondientes a los subgrupos y a los campos intermedios. Nótese, nuevamente, que los grupos más arriba corresponden a los campos más abajo. Esto es, un retículo se ve como el otro, pero invertido, o con la parte de arriba hacia abajo. Como aquí, en realidad, cada retículo se ve como es, pero invertido; éste no es un buen ejemplo para ilustrar este principio de inversión reticular. Si se observa la figura 47.2, se verán diagramas cuyos retículos no se parecen a sus propias figuras invertidas.



**Fig. 46.1** (a) Diagrama reticular de grupos. (b) Diagrama reticular de campos.

**Definición** Si  $K$  es una extensión finita de un campo  $F$ ,  $G(K/F)$  es el *grupo de Galois de  $K$  sobre  $F$* .

Enunciaremos ahora el teorema principal, después daremos otro ejemplo y, por último, en un párrafo con asterisco, completaremos la demostración del teorema principal.

**Teorema 46.2 (Teorema principal de la teoría de Galois)** Sea  $K$  una extensión normal finita de un campo  $F$ , con grupo de Galois  $G(K/F)$ . Para un campo  $E$  donde  $F \leq E \leq K$ , sea  $E\lambda$  el subgrupo de  $G(K/F)$  que deja fijo  $E$ . Entonces,  $\lambda$

es una transformación uno a uno del conjunto de todos estos campos intermedios  $E$  sobre el conjunto de todos los subgrupos de  $G(K/F)$ . Se cumplen las siguientes propiedades para  $\lambda$ :

- 1  $E\lambda = G(K/E)$ .
- 2  $E = K_{G(K/E)} = K_{E\lambda}$ .
- 3 Para  $H \leq G(K/F)$ ,  $K_H\lambda = H$ .
- 4  $[K:E] = |E\lambda|$ ;  $[E:F] = \{G(K/F) : E\lambda\}$ , el número de clases laterales de  $E\lambda$  en  $G(K/F)$ .
- 5  $E$  es una extensión normal de  $F$  si y sólo si  $E\lambda$  es un subgrupo normal de  $G(K/F)$ . Cuando  $E\lambda$  es un subgrupo normal de  $G(K/F)$ , entonces

$$G(E/F) \simeq G(K/F)/G(K/E).$$

- 6 El retículo de los subgrupos de  $G(K/F)$  es el retículo invertido de los campos intermedios de  $K$  sobre  $F$ .

*Observaciones acerca de la demostración* En realidad, ya probamos buena parte de este teorema. Veamos sólo lo que hemos dejado sin probar.

La propiedad 1 no es más que la definición de  $\lambda$  en el enunciado del teorema.

Para la propiedad 2, el teorema 40.4 muestra que

$$E \leq K_{G(K/E)}.$$

Sea  $\alpha \in K$  donde  $\alpha \notin E$ . Como  $K$  es una extensión normal de  $E$ , usando un isomorfismo básico y el teorema de extensión de isomorfismos, podemos encontrar un automorfismo de  $K$  que deje fijo  $E$  y transforme  $\alpha$  en un cero diferente de  $\text{irr}(\alpha, F)$ . Esto implica que

$$K_{G(K/E)} \leq E,$$

de modo que  $E = K_{G(K/E)}$ . Esto da cuenta de la propiedad 2 y nos dice, además, que  $\lambda$  es uno a uno, pues si  $E_1\lambda = E_2\lambda$ , entonces, por la propiedad 2, tenemos que

$$E_1 = K_{E_1\lambda} = K_{E_2\lambda} = E_2.$$

Nuestra tarea principal será la propiedad 3. Esto equivale, precisamente, a mostrar que  $\lambda$  es una transformación sobre. Claro que para  $H \leq G(K/F)$ , tenemos  $H \leq K_H\lambda$ , pues, con certeza,  $H$  está incluido en el conjunto de todos los automorfismos que dejan fijo  $K_H$ . Aquí se usará fuertemente la propiedad  $[K:E] = \{K:E\}$ .

La propiedad 4 es clara de  $[K:E] = \{K:E\}$ ,  $[E:F] = \{E:F\}$  y el último enunciado del teorema 46.1.

Para la propiedad 5 tendremos que mostrar que corresponden los dos sentidos de la palabra *normal*.

En el ejemplo 46.1 demostramos la propiedad 6.

Así, sólo falta probar las propiedades 3 y 5.

El teorema principal de la teoría de Galois es una herramienta poderosa en el estudio de ceros de polinomios. Si  $f(x) \in F[x]$  es tal que todo factor irreducible de  $f(x)$  es separable sobre  $F$ , entonces, el campo de descomposición  $K$  de  $f(x)$  sobre  $F$  es una extensión normal de  $F$ . El grupo de Galois  $G(K/F)$  es el **grupo del polinomio  $f(x)$  sobre  $F$** . La estructura de este grupo nos puede dar considerable información respecto a los ceros de  $f(x)$ . Esto se ilustrará de manera admirable en el capítulo 49, cuando alcancemos nuestro *objetivo final*.

## 46.4 GRUPOS DE GALOIS SOBRE CAMPOS FINITOS

Sea  $K$  una extensión finita de un *campo finito*  $F$ . Hemos visto que  $K$  es una extensión separable de  $F$  (un campo finito es perfecto). Supóngase que el orden de  $F$  es  $p^r$  y  $[K:F] = n$  de modo que el orden de  $K$  es  $p^{rn}$ . Entonces, hemos visto que  $K$  es el campo de descomposición de  $x^{p^{rn}} - x$  sobre  $F$ . Por tanto,  $K$  es una extensión normal de  $F$ .

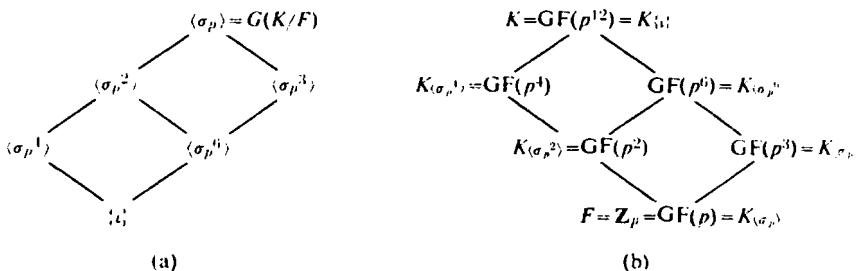
Ahora,  $\sigma_{p^r}$  es un automorfismo de  $K$  que deja fijo  $F$ , donde para  $\alpha \in K$ ,  $\alpha\sigma_{p^r} = \alpha^{p^r}$ . Nótese que  $\alpha(\sigma_{p^r})^i = \alpha^{p^ri}$ . Como un polinomio de grado  $p^r$  puede tener a lo más  $p^{ri}$  ceros en un campo, vemos que la menor potencia de  $\sigma_{p^r}$  que podría dejar fijos todos los  $p^{rn}$  elementos de  $K$  es la  $n$ -ésima potencia. Esto es, el orden del elemento  $\sigma_{p^r}$  en  $G(K/F)$  es por lo menos  $n$ . Por tanto, como  $|G(K/F)| = [K:F] = n$ , tenemos que  $G(K/F)$  es cíclico y generado por  $\sigma_{p^r}$ . Resumimos estos argumentos en un teorema.

**Teorema 46.3** *Sea  $K$  una extensión finita de grado  $n$  de un campo finito  $F$  de  $p^r$  elementos. Entonces,  $G(K/F)$  es cíclico de orden  $n$  y está generado por  $\sigma_{p^r}$  donde para  $\alpha \in K$ ,  $\alpha\sigma_{p^r} = \alpha^{p^r}$ .*

Usamos este teorema para dar otra ilustración del teorema principal de la teoría de Galois.

**Ejemplo 46.2** Sea  $F = \mathbb{Z}_p$  y sea  $K = CG(p^{12})$ , de modo que  $[K:F] = 12$ . Entonces,  $G(K/F)$  es isomorfo al grupo cíclico  $\langle \mathbb{Z}_{12}, + \rangle$ . En la figura 46.2 se da el diagrama reticular para los subgrupos y para los campos intermedios. De nuevo, cada retículo no sólo es la inversión del otro sino que, desafortunadamente, también se ve como la inversión de si mismo. En la sección siguiente (con asterisco), se dan ejemplos en donde los retículos no se parecen a sus propias inversiones. Describimos los subgrupos cíclicos de  $G(K/F) = \langle \sigma_p \rangle$  dando los generadores, por ejemplo,

$$\langle \sigma_p^4 \rangle = \{\iota, \sigma_p^4, \bar{\sigma}_p^8\}. \blacksquare$$



**Fig. 46.2** (a) Diagrama reticular de grupos. (b) Diagrama reticular de campos.

## \*46.5 FINAL DE LA DEMOSTRACION DEL TEOREMA PRINCIPAL

Vimos que todo lo que falta probar en el teorema principal de la teoría de Galois son las propiedades 3 y 5.

*Demostración* Volviendo a la propiedad 3, debemos mostrar que para  $H \leq G(K/F)$ ,  $K_H\lambda = H$ . Sabemos que  $H \leq K_H\lambda \leq G(K/F)$ . Así, lo que realmente debemos mostrar es que es imposible que  $H$  sea un subgrupo propio de  $K_H\lambda$ . Supondremos que

$$H < K_H\lambda,$$

y deduciremos una contradicción. Si  $K_H$  es infinito, entonces, por ser una extensión separable finita de un campo infinito,  $K = K_H(\alpha)$  para alguna  $\alpha \in K$ , por el teorema 43.6. Por otro lado, si  $K_H$  es finito, entonces tendremos aún que  $K = K_H(\alpha)$  para alguna  $\alpha \in K$ , por el corolario 2 del teorema 45.3. Sea

$$n = [K : K_H] = \{K : K_H\} = |G(K/K_H)|.$$

Entonces,  $H < G(K/K_H)$  implica que  $|H| < |G(K/K_H)| = n$ . Así, deberíamos tener  $|H| < [K : K_H] = n$ . Sean  $\sigma_1, \dots, \sigma_{|H|}$  los elementos de  $H$ , considérese el polinomio

$$f(x) = \prod_{i=1}^{|H|} (x - \alpha\sigma_i).$$

Entonces,  $f(x)$  es de grado  $|H| < n$ . Ahora, los coeficientes de cada potencia de  $x$  en  $f(x)$  son expresiones simétricas en las  $\alpha\sigma_i$ . Por ejemplo, el coeficiente de  $x^{|H|-1}$  es  $-\alpha\sigma_1 - \alpha\sigma_2 - \dots - \alpha\sigma_{|H|}$ . Así, estos coeficientes son invariantes bajo cada isomorfismo  $\sigma_i \in H$  ya que si  $\sigma \in H$ , entonces

$$\sigma_1\sigma, \dots, \sigma_{|H|}\sigma$$

es de nuevo la sucesión  $\sigma_1, \dots, \sigma_{|H|}$  excepto por el orden, pues  $H$  es un grupo. De aquí,  $f(x)$  tiene coeficientes en  $K_H$  y, como algún  $\sigma_i$  es  $i$ , vemos que alguna  $x\sigma_i$  es  $x$ , de modo que  $f(\alpha) = 0$ . Por tanto, tendríamos

$$\deg(\alpha, K_H) \leq |H| < n = [K : K_H] = [K_H(\alpha) : K_H].$$

Esto es imposible. Por tanto, hemos probado la propiedad 3.

Pasemos a la propiedad 5. Por el teorema 43.3, toda extensión  $E$  de  $F$ ,  $F \leq E \leq K$  es separable sobre  $F$ . Así,  $E$  es normal sobre  $F$  si y sólo si  $E$  es un campo de descomposición sobre  $F$ . Por el teorema de extensión de isomorfismos, todo isomorfismo de  $E$  en  $\bar{F}$  que deje fijo  $F$  puede extenderse a un *automorfismo* de  $K$ , pues  $K$  es *normal* sobre  $F$ . Así, los automorfismos de  $G(K/F)$  inducen todos los isomorfismos posibles de  $E$  en  $\bar{F}$  que dejan fijo  $F$ . Por el teorema 42.1, esto muestra que  $E$  es un campo de descomposición sobre  $F$  y, por tanto, normal sobre  $F$  si y sólo si para todas las  $\sigma \in G(K/F)$  y  $\alpha \in E$ ,

$$(\alpha\sigma) \in E.$$

Por la propiedad 2,  $E$  es el campo fijo de  $G(K/E)$ , de modo que  $(\alpha\sigma) \in E$  si y sólo si para todas las  $\tau \in G(K/E)$ ,

$$(\alpha\sigma)\tau = \alpha\sigma.$$

Esto a su vez si y sólo si

$$\alpha(\sigma\tau\sigma^{-1}) = \alpha$$

para todas las  $\alpha \in E$ ,  $\sigma \in G(K/F)$  y  $\tau \in G(K/E)$ . Pero esto significa que para todas las  $\sigma \in G(K/F)$  y  $\tau \in G(K/E)$ ,  $\sigma\tau\sigma^{-1}$  deja fijo todo elemento de  $E$ , esto es,

$$(\sigma\tau\sigma^{-1}) \in G(K/E).$$

Esta es precisamente la condición para que  $G(K/E)$  sea un subgrupo normal de  $G(K/F)$ .

Falta mostrar que cuando  $E$  es una extensión normal de  $F$ ,  $G(E/F) \simeq G(K/F)/G(K/E)$ . Para  $\sigma \in G(K/F)$ , sea  $\sigma_E$  el *automorfismo* de  $E$  inducido por  $\sigma$  (suponiendo que  $E$  es una extensión *normal* de  $F$ ). Así,  $\sigma_E \in G(E/F)$ . La transformación  $\phi: G(K/F) \rightarrow G(E/F)$  dada por

$$\sigma\phi = \sigma_E$$

para  $\sigma \in G(K/F)$  es, obviamente, un homomorfismo. Por el teorema de la extensión de isomorfismos, todo automorfismo de  $E$  que deje fijo  $F$  puede extenderse a algún automorfismo de  $K$ , esto es, es  $\tau_E$  para alguna  $\tau \in G(K/F)$ . Así,  $\phi$  es sobre  $G(E/F)$ . Es claro que el kernel de  $\phi$  es  $G(K/E)$ . Por tanto, por el teorema fundamental del isomorfismo,  $G(E/F) \simeq G(K/F)/G(K/E)$ . Más aún, este isomorfismo es el natural. ■

**Ejercicios**

**46.1** El campo  $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  es una extensión normal finita de  $\mathbf{Q}$ . Llénense los espacios en blanco. La notación es la del teorema 46.2.

- |   |  |
|---|--|
| a) $[K : \mathbf{Q}] = \underline{\hspace{2cm}}$ .                  | b) $ G(K/\mathbf{Q})  = \underline{\hspace{2cm}}$ .                |
| c) $ \mathbf{Q}\lambda  = \underline{\hspace{2cm}}$ .               | d) $ (Q(\sqrt{2}, \sqrt{3}))\lambda  = \underline{\hspace{2cm}}$ . |
| e) $ (Q(\sqrt{6}))\lambda  = \underline{\hspace{2cm}}$ .            | f) $ (Q(\sqrt{30}))\lambda  = \underline{\hspace{2cm}}$ .          |
| g) $ (Q(\sqrt{2} + \sqrt{6}))\lambda  = \underline{\hspace{2cm}}$ . | h) $ K\lambda  = \underline{\hspace{2cm}}$ .                       |

**46.2** Describase el grupo del polinomio  $(x^4 - 1) \in \mathbf{Q}[x]$  sobre  $\mathbf{Q}$ .

**46.3** Dése el orden y describase un generador del grupo  $G(CG(729)/CG(9))$ .

**46.4** Dése un ejemplo de dos extensiones normales finitas  $K_1$  y  $K_2$  del mismo campo  $F$ , tales que  $K_1$  y  $K_2$  no sean campos isomorfos pero  $G(K_1/F) \cong G(K_2/F)$ .

**46.5** Sea  $K$  el campo de descomposición de  $x^3 - 2$  sobre  $\mathbf{Q}$  (remítase al ejemplo 42.2).

- a) Describanse los seis elementos de  $G(K/\mathbf{Q})$ , dando sus valores en  $\sqrt[3]{2}$  e  $i\sqrt{3}$ . (Por el ejemplo 42.2,  $K = \mathbf{Q}(\sqrt[3]{2}, i\sqrt{3})$ .)
- b) ¿A qué grupo de los ya vistos es isomorfo  $G(K/\mathbf{Q})$ ?
- c) Usando la notación dada en la respuesta de a) al final del libro, dense los diagramas reticulares para los subcampos de  $K$  y para los subgrupos de  $G(K/\mathbf{Q})$ , indicando los campos intermedios y subgrupos correspondientes, como lo hicimos en la figura 46.1.

<sup>†</sup>**46.6** Una extensión normal finita  $K$  del campo  $F$  es **abeliana sobre  $F$**  si  $G(K/F)$  es un grupo abeliano. Muéstrese que si  $K$  es abeliano sobre  $F$  y  $E$  es una extensión normal de  $F$ , donde  $F \leq E \leq K$ , entonces  $K$  es abeliano sobre  $E$  y  $E$  es abeliano sobre  $F$ .

**46.7** ¿Falso o verdadero?

- a) Dos subgrupos diferentes de un grupo de Galois pueden tener el mismo campo fijo.
- b) En la notación del teorema 46.2, si  $F \leq E \leq L \leq K$ , entonces  $E\lambda < L\lambda$ .
- c) Si  $K$  es una extensión normal finita de  $F$ , entonces  $K$  es una extensión normal de  $E$ , donde  $F \leq E \leq K$ .
- d) Si dos extensiones normales finitas  $E$  y  $L$  de un campo  $F$  tienen grupos de Galois isomorfos, entonces  $[E : F] = [L : F]$ .
- e) Si  $E$  es una extensión normal finita de  $F$  y  $H$  es un subgrupo normal de  $G(E/F)$ , entonces  $E_H$  es una extensión normal de  $F$ .
- f) Si  $E$  es cualquier extensión simple normal finita de un campo  $F$ , entonces el grupo de Galois  $G(E/F)$  es un grupo simple.
- g) Ningún grupo de Galois es simple.
- h) El grupo de Galois de una extensión finita de un campo finito, es abeliano.
- i) Una extensión  $E$  de grado 2 sobre un campo  $F$  es siempre una extensión normal de  $F$ .
- j) Una extensión  $E$  de grado 2 sobre un campo  $F$  es siempre una extensión normal de  $F$  si la característica de  $F$  no es 2.

**46.8** Sea  $K$  una extensión normal finita de un campo  $F$ . Pruébese que para toda  $\alpha \in K$  la norma de  $\alpha$  sobre  $F$  dada por

$$N_{K/F}(\alpha) = \prod_{\sigma \in G(K/F)} \alpha\sigma,$$

y la traza de  $\alpha$  sobre  $F$ , dada por

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in G(K/F)} \alpha\sigma,$$

son elementos de  $F$ .

**46.9** Considérese  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Con referencia al ejercicio 46.8, calcúlese lo siguiente (véase el ejemplo 46.1).

- |                                  |   |
|----------------------------------|---|
| a) $N_{K/\mathbb{Q}}(\sqrt{2})$  | b) $N_{K/\mathbb{Q}}(\sqrt{2} + \sqrt{3})$  |
| c) $N_{K/\mathbb{Q}}(\sqrt{6})$  | d) $N_{K/\mathbb{Q}}(2)$                    |
| e) $Tr_{K/\mathbb{Q}}(\sqrt{2})$ | f) $Tr_{K/\mathbb{Q}}(\sqrt{2} + \sqrt{3})$ |
| g) $Tr_{K/\mathbb{Q}}(\sqrt{6})$ | h) $Tr_{K/\mathbb{Q}}(2)$                   |

**46.10** Sea  $K$  una extensión normal de  $F$  y sea  $K = F(\alpha)$ . Sea

$$\text{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

Con referencia al ejercicio 46.8, muéstrese que

a)  $N_{K/F}(\alpha) = (-1)^n a_0$ ,      b)  $Tr_{K/F}(\alpha) = -a_{n-1}$ .

**46.11** Describase el grupo del polinomio  $(x^4 - 5x^2 + 6) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$ .

**46.12** Describase el grupo del polinomio  $(x^3 - 1) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$ .

**46.13** Sea  $f(x) \in F[x]$  un polinomio de grado  $n$  tal que cada factor irreducible es separable sobre  $F$ . Muéstrese que el orden del grupo de  $f(x)$  sobre  $F$  divide a  $n!$ .

**46.14** Sea  $f(x) \in F[x]$  un polinomio tal que todo factor irreducible de  $f(x)$  es un polinomio separable sobre  $F$ . Muéstrese que el grupo de  $f(x)$  sobre  $F$  puede considerarse de manera natural como un grupo de permutaciones de los ceros de  $f(x)$  en  $F$ .

**46.15** Sea  $F$  un campo y sea  $\zeta$  una raíz  $n$ -ésima primitiva del unitario en  $F$  donde la característica de  $F$  es 0 o no divide a  $n$ .

- a) Muéstrese que  $F(\zeta)$  es una extensión normal de  $F$ .  
 b) Muéstrese que  $G(F(\zeta)/F)$  es abeliano. [Sugerencia: toda  $\sigma \in G(F(\zeta)/F)$  transforma a  $\zeta$  sobre algún  $\zeta'$  y está completamente determinada por este valor  $r$ .]

**4.16** Una extensión normal finita  $K$  de un campo  $F$  es cíclica sobre  $F$  si  $G(K/F)$  es un grupo cíclico.

- a) Muéstrese que si  $K$  es cíclico sobre  $F$ , y  $E$  es una extensión normal de  $F$ , donde  $F \leq E \leq K$ , entonces  $E$  es cíclico sobre  $F$  y  $K$  es cíclico sobre  $E$ .  
 b) Muéstrese que si  $K$  es cíclico sobre  $F$ , entonces existe precisamente un campo  $E$ ,  $F \leq E \leq K$  de grado  $d$  sobre  $F$  para cada divisor  $d$  de  $[K:F]$ .

**46.17** Sea  $K$  una extensión normal finita de  $F$ .

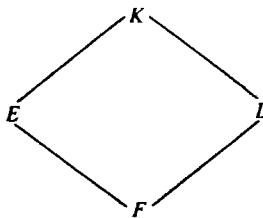
- a) Para  $\alpha \in K$ , muéstrese que

$$f(x) = \prod_{\sigma \in G(K/F)} (x - \alpha\sigma)$$

está en  $F[x]$ .

- b) Con referencia a a), muéstrese que  $f(x)$  es una potencia de  $\text{irr}(\alpha, F)$  y  $f(x) = \text{irr}(\alpha, F)$  si y sólo si  $E = F(\alpha)$ .

**46.18** Sea  $K$  una extensión normal finita de un campo  $F$  y sean  $E$  y  $L$  extensiones de  $F$  contenidas en  $K$ , como se muestra en la figura 46.3. Describáse  $G\{K/(E \vee L)\}$  en términos de  $G(K/E)$  y  $G(K/L)$ .



**Figura 46.3**

**\*46.19** Con referencia a la situación en el ejercicio 46.18, describáse  $G\{K/(E \cap L)\}$  en términos de  $G(K/E)$  y  $G(K/L)$ .

## Ilustraciones de la teoría de Galois

### \*47.1 FUNCIONES SIMETRICAS

Sea  $F$  un campo y sean  $y_1, \dots, y_n$ ,  $n$  indeterminadas. Hay algunos automorfismos obvios de  $F(y_1, \dots, y_n)$  que dejan fijo  $F$ , a saber, aquellos definidos por permutaciones de  $\{y_1, \dots, y_n\}$ . Para ser menos claro, pero más explícito, sea  $\sigma$  una permutación de  $\{1, \dots, n\}$ , esto es,  $\sigma \in S_n$ . Entonces,  $\sigma$  da lugar a una transformación natural  $\tilde{\sigma} : F(y_1, \dots, y_n) \rightarrow F(y_1, \dots, y_n)$  dada por

$$\frac{f(y_1, \dots, y_n)}{g(y_1, \dots, y_n)} \tilde{\sigma} = \frac{f(y_{1\sigma}, \dots, y_{n\sigma})}{g(y_{1\sigma}, \dots, y_{n\sigma})}$$

para  $f(y_1, \dots, y_n), g(y_1, \dots, y_n) \in F[y_1, \dots, y_n]$  con  $g(y_1, \dots, y_n) \neq 0$ . Es inmediato que  $\tilde{\sigma}$  es un automorfismo de  $F(y_1, \dots, y_n)$  que deja fijo  $F$ . Los elementos de  $F(y_1, \dots, y_n)$  que quedaron fijos bajo todas las  $\tilde{\sigma}$ , para todas las  $\sigma \in S_n$ , son aquellas funciones racionales que son *simétricas* en las indeterminadas  $y_1, \dots, y_n$ .

**Definición** Un elemento de  $F(y_1, \dots, y_n)$  es una *función simétrica en  $y_1, \dots, y_n$  sobre  $F$*  si queda fijo bajo todas las permutaciones de  $y_1, \dots, y_n$  en el sentido recién explicado.

- Sea  $\bar{S}_n$  el grupo de todos los automorfismos  $\tilde{\sigma}$  para  $\sigma \in S_n$ . Obviamente,  $\bar{S}_n$  es un isomorfismo natural a  $S_n$ . Sea  $K$  el subcampo de  $F(y_1, \dots, y_n)$  que es el campo fijo de  $\bar{S}_n$ . Considérese el polinomio

$$f(x) = \prod_{i=1}^n (x - y_i);$$

este polinomio  $f(x) \in (F(y_1, \dots, y_n))[x]$  es un **polinomio general de grado  $n$** . Sea  $\tilde{\sigma}_x$  la extensión de  $\tilde{\sigma}$ , de manera natural, a  $(F(y_1, \dots, y_n))[x]$ , donde  $x\tilde{\sigma}_x = x$ . Es claro que ahora  $f(x)$  queda fijo bajo cada transformación  $\tilde{\sigma}_x$  para  $\sigma \in S_n$ , esto es,

$$\prod_{i=1}^n (x - y_i) = \prod_{i=1}^n (x - y_{i\sigma}).$$

Así, los coeficientes de  $f(x)$  están en  $K$ ; son funciones simétricas en las  $y_1, \dots, y_n$ . Como ilustración, nótese que el término constante de  $f(x)$  es

$$(-1)^n y_1 y_2 \cdots y_n,$$

el coeficiente de  $x^{n-1}$  es  $-(y_1 + y_2 + \cdots + y_n)$  y así sucesivamente. Estas son, de manera obvia, funciones simétricas en  $y_1, \dots, y_n$ .

**Definición** La  $i$ -ésima función simétrica elemental en  $y_1, \dots, y_n$  es  $s_i = (-1)^i a_i$ , donde  $a_i$  es el coeficiente de  $x^{n-i}$  en el polinomio general  $\prod_{i=1}^n (x - y_i)$ .

Así, la primera función simétrica elemental en  $y_1, \dots, y_n$  es

$$s_1 = y_1 + y_2 + \cdots + y_n,$$

la segunda es  $s_2 = y_1 y_2 + y_1 y_3 + \cdots + y_{n-1} y_n$  y así sucesivamente, y la  $n$ -ésima es  $s_n = y_1 y_2 \cdots y_n$ .

Considérese el campo  $E = F(s_1, \dots, s_n)$ . Es claro que  $E \leq K$ , donde  $K$  es el campo de todas las funciones simétricas en  $y_1, \dots, y_n$  sobre  $F$ . Pero  $F(y_1, \dots, y_n)$  es una extensión normal finita de  $E$ , a saber, el campo de descomposición de

$$f(x) = \prod_{i=1}^n (x - y_i)$$

sobre  $E$ . Como el grado de  $f(x)$  es  $n$ , tenemos en seguida que

$$[F(y_1, \dots, y_n) : E] \leq n!$$

(véase el ejercicio 42.2). Sin embargo, como  $K$  es el campo fijo de  $\bar{S}_n$  y

$$|\bar{S}_n| = |S_n| = n!,$$

tenemos además

$$n! \leq \{F(y_1, \dots, y_n) : K\} \leq [F(y_1, \dots, y_n) : K].$$

Por tanto,

$$n! \leq [F(y_1, \dots, y_n) : K] \leq [F(y_1, \dots, y_n) : E] \leq n!,$$

de modo que

$$K = E.$$

Entonces, todo el grupo de Galois de  $F(y_1, \dots, y_n)$  sobre  $E$  es  $\bar{S}_n$ . El hecho de que  $K = E$ , muestra que toda función simétrica puede expresarse como función racional de las funciones simétricas elementales  $s_1, \dots, s_n$ . Resumimos estos resultados en un teorema.

**Teorema 47.1** *Sean  $s_1, \dots, s_n$  las funciones simétricas elementales en las indeterminadas  $y_1, \dots, y_n$ . Entonces, toda función simétrica de  $y_1, \dots, y_n$  sobre  $F$  es una función racional de las funciones simétricas elementales. Además,  $F(y_1, \dots, y_n)$  es una extensión normal finita de grado  $n!$  de  $F(s_1, \dots, s_n)$ , y el grupo de Galois de esta extensión es naturalmente isomorfo a  $S_n$ .*

En vista del teorema de Cayley, podemos deducir del teorema 47.1, que cualquier grupo finito puede presentarse como un grupo de Galois (salvo isomorfismo). (Véase el ejercicio 47.13.)

## \*47.2 EJEMPLOS

Demos ahora el ejemplo prometido de una extensión normal finita que tenga grupo de Galois cuyo retículo de subgrupos no se vea como su propia invertida.

**Ejemplo 47.1** Considérese el campo de descomposición en  $C$  de  $x^4 - 2$  sobre  $Q$ . Ahora, por el criterio de Eisenstein con  $p = 2$ ,  $x^4 - 2$  es irreducible sobre  $Q$ . Sea  $\alpha = \sqrt[4]{2}$  el número real positivo que es cero de  $x^4 - 2$ . Entonces, los cuatro ceros de  $x^4 - 2$  en  $C$  son, obviamente,  $\alpha, -\alpha, i\alpha$  y  $-i\alpha$ , donde  $i$  es el cero usual de  $x^2 + 1$  en  $C$ . El campo de descomposición  $K$  de  $x^4 - 2$  sobre  $Q$  contiene, así,  $(i\alpha)/\alpha = i$ . Como  $\alpha$  es un número real,  $Q(\alpha) < R$ , de modo que  $Q(\alpha) \neq K$ . Sin embargo, como  $Q(\alpha, i)$  contiene a todos los ceros de  $x^4 - 2$ , vemos que  $Q(\alpha, i) = K$ . Al hacer que  $E = Q(\alpha)$  tenemos el diagrama de la figura 47.1.

Ahora,  $\{1, \alpha, \alpha^2, \alpha^3\}$  es una base para  $E$  sobre  $Q$  y  $\{1, i\}$  es una base para  $K$  sobre  $E$ . Así,

$$\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$$

es una base para  $K$  sobre  $Q$ . Como  $[K : Q] = 8$ , debemos tener  $|G(K/Q)| = 8$ , de modo que necesitamos encontrar ocho automorfismos de  $K$  que dejen fijo  $Q$ .

$$\begin{array}{c}
 K = \mathbb{Q}(\alpha, i) \\
 | \\
 E = \mathbb{Q}(\alpha) \\
 | \\
 \mathbb{Q}
 \end{array}$$

**Figura 47.1**

Sabemos que cualquiera de dichos automorfismos  $\sigma$  está completamente determinado por sus valores en los elementos de la base  $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$  y, a su vez, estos valores están determinados por  $\alpha\sigma$  e  $i\sigma$ . Pero  $\alpha\sigma$  debe ser siempre conjugado de  $\alpha$  sobre  $\mathbb{Q}$ , esto es, uno de los cuatro ceros de  $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 2$ . Así mismo,  $i\sigma$  debe ser un cero de  $\text{irr}(i, \mathbb{Q}) = x^2 + 1$ . Así, las cuatro posibilidades para  $\alpha, \sigma$  combinadas con las dos posibilidades de  $i\sigma$  deben dar los ocho automorfismos. Describimos esto en la tabla 47.1

**Tabla 47.1**

	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\mu_1$	$\delta_1$	$\mu_2$	$\delta_2$
$\alpha \rightarrow$	$\alpha$	$i\alpha$	$-\alpha$	$-i\alpha$	$\alpha$	$i\alpha$	$-\alpha$	$-i\alpha$
$i \rightarrow$	$i$	$i$	$i$	$i$	$-i$	$-i$	$-i$	$-i$

Por ejemplo,  $\alpha\rho_3 = -i\alpha$  e  $i\rho_3 = i$ , mientras que  $\rho_0$  es el automorfismo identidad. Ahora,

$$\alpha(\rho_1\mu_1) = (\alpha\rho_1)\mu_1 = (i\alpha)\mu_1 = (i\mu_1)(\alpha\mu_1) = -i\alpha,$$

y, de manera análoga,

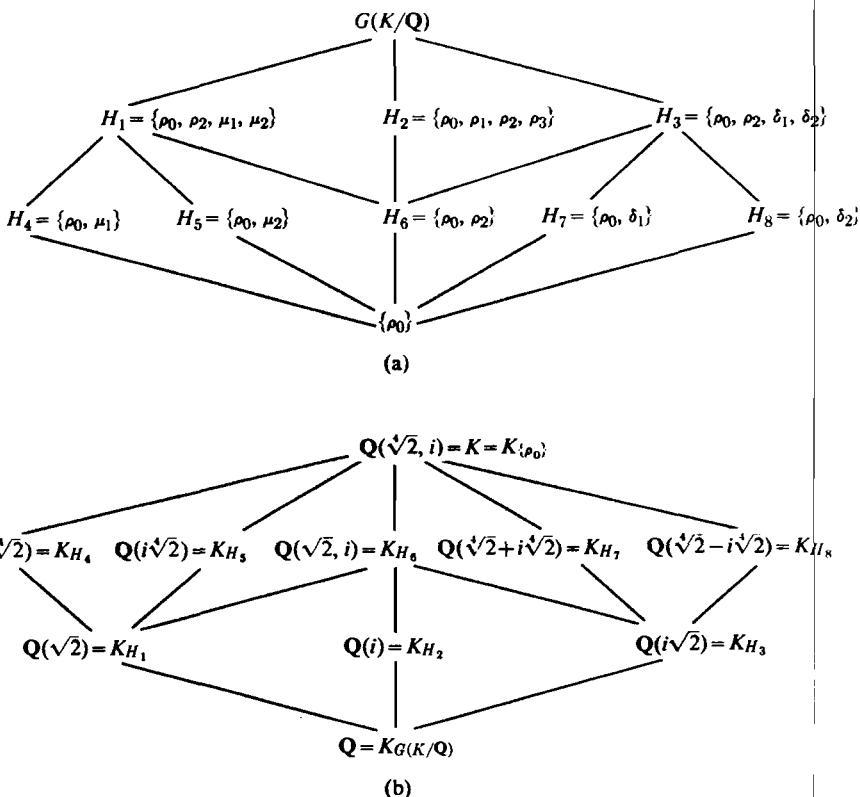
$$i(\rho_1\mu_1) = -i,$$

de modo que  $\rho_1\mu_1 = \delta_2$ . Un cálculo análogo muestra que

$$\alpha(\mu_1\rho_1) = i\alpha \quad \text{y} \quad i(\mu_1\rho_1) = -i.$$

Así,  $\mu_1\rho_1 = \delta_1$ , de modo que  $\rho_1\mu_1 \neq \mu_1\rho_1$  y  $G(K/\mathbb{Q})$  no es abeliano. Por tanto,  $G(K/\mathbb{Q})$  debe ser isomorfo a uno de los dos grupos no abelianos de orden 8 descritos en el ejemplo 22.5. Calculando a partir de la tabla 47.1, vemos que  $\rho_1$  es de orden 4,  $\mu_1$  es de orden 2,  $\{\rho_1, \mu_1\}$  genera  $G(K/\mathbb{Q})$  y  $\mu_1\rho_1 = \rho_1^3\mu_1 = \delta_1$ . Así,  $G(K/\mathbb{Q})$  es isomorfo al grupo  $G_1$  del ejemplo 22.5, el *grupo octal*. Escogemos la

notación para los elementos de  $G(K/\mathbb{Q})$  de modo que su tabla de grupo coincidiera con la tabla para el grupo octal en la tabla 4.2. El retículo de los subgrupos  $H_i$  de  $G(K/\mathbb{Q})$  está dado en la figura 4.7. Lo repetimos aquí, en la figura 47.2 y damos además el retículo correspondiente de los campos intermedios entre  $\mathbb{Q}$  y  $K$ . Esto, finalmente, es una bella ilustración de que un retículo es la inversión del otro.



**Fig. 47.2** (a) Diagrama reticular de grupos. (b) Diagrama reticular de campos.

A veces requiere un poco de ingenio determinar los campos fijos  $K_{H_i}$ . Ilustraremos. Encontrar  $K_{H_2}$  es fácil, pues sólo tenemos que encontrar una extensión de  $\mathbb{Q}$  de grado 2 que quede fija bajo  $\{\rho_0, \rho_1, \rho_2, \rho_3\}$ . Como todos los  $\rho_j$  dejan fijo  $i$ , claramente  $\mathbb{Q}(i)$  es el campo que buscamos. Para encontrar  $K_{H_4}$ , tenemos que encontrar una extensión de  $\mathbb{Q}$  de grado 4 que quede fija bajo  $\rho_0$  y  $\mu_1$ . Como  $\mu_1$  deja fija  $\alpha$  y  $\alpha$  es un cero de  $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 2$ , vemos que  $\mathbb{Q}(\alpha)$  es de grado 4 sobre  $\mathbb{Q}$  y queda fijo bajo  $\{\rho_0, \mu_1\}$ . Por la teoría de Galois, es el único de dichos campos. Aquí usamos fuertemente la correspondencia uno a uno dada por la teoría de Galois. Si encontramos un campo que satisfaga las condiciones, ése es el que buscamos. Encontrar  $K_{H_7}$  requiere más habilidad. Como  $H_7 = \{\rho_0, \delta_1\}$  es un grupo, para cualquier  $\beta \in K$  vemos que  $\beta\rho_0 + \beta\delta_1$  queda fijo bajo  $\rho_0$  y  $\delta_1$ .

Tomando  $\beta = \alpha$  vemos que  $\alpha\rho_0 + \alpha\delta_1 = \alpha + i\alpha$  queda fijo bajo  $H_7$ . Podemos verificar y ver que  $\rho_0$  y  $\delta_1$  son los únicos automorfismos que dejan fijo  $\alpha + i\alpha$ . Así, por la correspondencia uno a uno, debemos tener

$$\mathbf{Q}(\alpha + i\alpha) = \mathbf{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) = K_{H_7},$$

Supóngase que deseamos encontrar  $\text{irr}(\alpha + i\alpha, \mathbf{Q})$ . Si  $\gamma = \alpha + i\alpha$ , entonces para todo conjugado de  $\gamma$  sobre  $\mathbf{Q}$  existe un automorfismo de  $K$  que transforma  $\gamma$  en ese conjugado. Sólo necesitamos calcular los distintos valores  $\gamma\sigma$  para  $\sigma \in G(K/\mathbf{Q})$  para encontrar los otros ceros de  $\text{irr}(\gamma, \mathbf{Q})$ . Por el teorema 46.1 se pueden encontrar elementos  $\sigma$  de  $G(K/\mathbf{Q})$  que den estos valores diferentes, si se toma un conjunto de representantes de las clases laterales derechas de  $G(K/\mathbf{Q}(\gamma)) = \{\rho_0, \delta_1\}$  en  $G(K/\mathbf{Q})$ . Un conjunto de representantes de estas clases laterales derechas es

$$\{\rho_0, \rho_1, \rho_2, \rho_3\}.$$

Los conjugados de  $\gamma = \alpha + i\alpha$  son, entonces,  $\alpha + i\alpha, i\alpha - \alpha, -\alpha - i\alpha$  y  $-i\alpha + \alpha$ . De aquí,

$$\begin{aligned}\text{irr}(\gamma, \mathbf{Q}) &= [(x - (\alpha + i\alpha))(x - (i\alpha - \alpha))] \cdot \\ &\quad \cdot [(x - (-\alpha - i\alpha))(x - (-i\alpha + \alpha))] \\ &= (x^2 - 2i\alpha x - 2\alpha^2)(x^2 + 2i\alpha x - 2\alpha^2) \\ &= x^4 + 4\alpha^4 = x^4 + 8.\blacksquare\end{aligned}$$

Hemos visto ejemplos en los cuales el campo de descomposición de una cuártica (polinomio de grado 4) sobre un campo  $F$  es una extensión de  $F$  de grado 8 (ejemplo 47.1) y de grado 24 (teorema 47.1 con  $n = 4$ ). El grado de una extensión de un campo  $F$  que es un campo de descomposición de una cuártica sobre  $F$ , claramente debe dividir siempre a  $4! = 24$ . Claro que el campo de descomposición de  $(x - 2)^4$  sobre  $\mathbf{Q}$  es  $\mathbf{Q}$ , una extensión de grado 1 y el campo de descomposición de  $(x^2 - 2)^2$  sobre  $\mathbf{Q}$  es  $\mathbf{Q}(\sqrt{2})$ , una extensión de grado 2. Nuestro último ejemplo dará una extensión de grado 4 para el campo de descomposición de una cuártica.

**Ejemplo 47.2** Considérese el campo de descomposición de  $x^4 + 1$  sobre  $\mathbf{Q}$ . Por el teorema 31.3, podemos mostrar que  $x^4 + 1$  es irreducible sobre  $\mathbf{Q}$ , argumentando que no se factoriza en  $\mathbf{Z}[x]$ . Esto es fácil de mostrar (véase el ejercicio 47.1). Puede verificarse fácilmente, mediante cálculos, que los ceros de  $x^4 + 1$  son  $(1 \pm i)/\sqrt{2}$  y  $(-1 \pm i)/\sqrt{2}$ . Al calcular vemos que si

$$\alpha = \frac{1+i}{\sqrt{2}},$$

entonces

$$\alpha^3 = \frac{-1+i}{\sqrt{2}}, \quad \alpha^5 = \frac{-1-i}{\sqrt{2}} \quad \text{y} \quad \alpha^7 = \frac{1-i}{\sqrt{2}}.$$

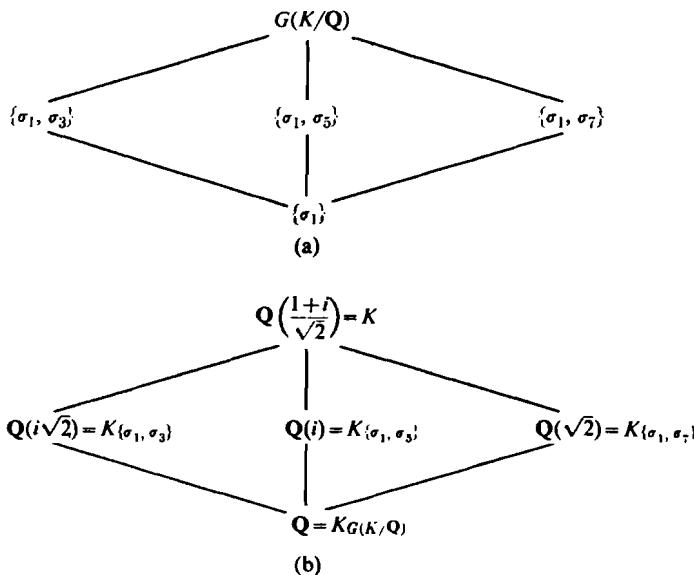
(Estos hechos, «sacados de la manga», se cubren en las primeras semanas de un curso de funciones de variable compleja, o pueden deducirse del siguiente capítulo.) Así, el campo de descomposición  $K$  de  $x^4 + 1$  sobre  $\mathbb{Q}$  es  $\mathbb{Q}(\alpha)$  y  $[K:\mathbb{Q}] = 4$ . Calculemos  $G(K/\mathbb{Q})$  y demos los diagramas reticulares de los grupos y de los campos. Como existen automorfismos de  $K$  que transforman  $\alpha$  sobre cada conjugado de  $\alpha$ , y como un automorfismo  $\sigma$  de  $\mathbb{Q}(\alpha)$  está por completo determinado por  $\alpha\sigma$ , vemos que los cuatro elementos de  $G(K/\mathbb{Q})$  están definidos por la tabla 47.2. Como

$$\alpha(\sigma_j\sigma_k) = \alpha^j\sigma_k = (\alpha\sigma_k)^j = (\alpha^k)^j = \alpha^{jk}$$

**Tabla 47.2**

	$\sigma_1$	$\sigma_3$	$\sigma_5$	$\sigma_7$
$\alpha \rightarrow$	$\alpha$	$\alpha^3$	$\alpha^5$	$\alpha^7$

y  $\alpha^8 = 1$ , vemos que  $G(K/\mathbb{Q})$  es isomorfo al grupo  $\{1, 3, 5, 7\}$  bajo la multiplicación módulo 8. Este es el grupo  $G_8$  del teorema 24.7. Como  $\sigma_j^2 = \sigma_1$ , la identidad, para todas las  $j$ ,  $G(K/\mathbb{Q})$  debe ser isomorfo al 4-grupo de Klein. Los diagramas reticulares están dados en la figura 47.3.



**Fig. 47.3** (a) Diagrama reticular de grupos. (b) Diagrama reticular de campos.

Para encontrar  $K_{\{\sigma_1, \sigma_3\}}$  sólo es necesario encontrar un elemento de  $K$  que no esté en  $\mathbf{Q}$  y quede fijo bajo  $\{\sigma_1, \sigma_3\}$ , pues  $[K_{\{\sigma_1, \sigma_3\}} : \mathbf{Q}] = 2$ . Claramente,  $x\sigma_1 + x\sigma_3$  queda fijo bajo  $\sigma_1$  y bajo  $\sigma_3$ , pues  $\{\sigma_1, \sigma_3\}$  es un grupo. Tenemos

$$x\sigma_1 + x\sigma_3 = x + x^3 = i\sqrt{2}.$$

De manera análoga,

$$x\sigma_1 + x\sigma_7 = x + x^7 = \sqrt[7]{2}$$

queda fijo bajo  $\{\sigma_1, \sigma_7\}$ . Esta técnica no es útil para encontrar  $E_{\{\sigma_1, \sigma_5\}}$ , pues

$$x\sigma_1 + x\sigma_5 = x + x^5 = 0,$$

y  $0 \in \mathbf{Q}$ . Pero, por un razonamiento análogo,  $(x\sigma_1)(x\sigma_5)$  queda fijo bajo  $\sigma_1$  y bajo  $\sigma_5$ , y

$$(x\sigma_1)(x\sigma_5) = x\alpha^5 = -i.$$

Así,  $\mathbf{Q}(-i) = \mathbf{Q}(i)$  es el campo que buscamos. ■

## Ejercicios

---

\*47.1 Muéstrese que  $x^4 + 1$  es irreducible en  $\mathbf{Q}[x]$ , según se afirmó en el ejemplo 47.2.

\*47.2 Verifíquese que los campos intermedios dados en el diagrama reticular de campos, en la figura 47.3, son los correctos. (Algunos se verificaron en el texto. Verifíquese el resto.)

\*47.3 Para cada campo en el diagrama reticular de campos en la figura 47.2, encuéntrese un elemento primitivo que genere el campo sobre  $\mathbf{Q}$  (véase el teorema 43.6) y dése su polinomio irreducible sobre  $\mathbf{Q}$ .

\*47.4 Sea  $\zeta$  una raíz quinta primitiva del unitario en  $\mathbf{C}$ .

- Muéstrese que  $\mathbf{Q}(\zeta)$  es el campo de descomposición de  $x^5 - 1$  sobre  $\mathbf{Q}$ .
- Muéstrese que todo automorfismo de  $K = \mathbf{Q}(\zeta)$  transforma  $\zeta$  sobre alguna potencia  $\zeta'$  de  $\zeta$ .
- Usando b), describanse los elementos de  $G(K/\mathbf{Q})$ .
- Dense los diagramas reticulares de grupo y de campo para  $\mathbf{Q}(\zeta)$  sobre  $\mathbf{Q}$ , calculando el campo intermedio como lo hicimos en los ejemplos 47.1 y 47.2.

\*47.5 Describase el grupo del polinomio  $(x^5 - 2) \in (\mathbf{Q}(\zeta))[x]$  sobre  $\mathbf{Q}(\zeta)$  donde  $\zeta$  es una raíz quinta primitiva del unitario.

\*47.6 Repítase el ejercicio 47.4 para  $\zeta$  una raíz séptima primitiva del unitario en  $\mathbf{C}$ .

\*47.7 Describase, de la manera más fácil posible, el grupo del polinomio

$$(x^8 - 1) \in \mathbf{Q}[x]$$

sobre  $\mathbf{Q}$ .

\*47.8 Encuéntrese el campo de descomposición  $K$  en  $\mathbb{C}$  del polinomio  $(x^4 - 4x^2 - 1) \in \mathbb{Q}[x]$ . Calcúlese el grupo del polinomio sobre  $\mathbb{Q}$  y exhibase la correspondencia entre los subgrupos de  $G(K/\mathbb{Q})$  y los campos intermedios. En otras palabras, hágase todo el trabajo.

\*47.9 Exprésese cada una de las siguientes funciones simétricas en  $y_1, y_2, y_3$  sobre  $\mathbb{Q}$  como una función racional de las funciones elementales simétricas  $s_1, s_2, s_3$ .

- $y_1^2 + y_2^2 + y_3^2$
- $(y_1 - y_2)^2(y_1 - y_3)^2(y_2 - y_3)^2$
- $\frac{y_1}{y_2} + \frac{y_2}{y_1} + \frac{y_1}{y_3} + \frac{y_3}{y_1} + \frac{y_2}{y_3} + \frac{y_3}{y_2}$

\*40.10 Sean  $\alpha_1, \alpha_2, \alpha_3$  ceros en  $\mathbb{C}$  del polinomio

$$(x^3 - 4x^2 + 6x - 2) \in \mathbb{Q}[x].$$

Encuéntrese el polinomio que tenga como ceros precisamente a:

- $\alpha_1 + \alpha_2 + \alpha_3$
- $\alpha_1^2, \alpha_2^2, \alpha_3^2$
- $(\alpha_1 - \alpha_2)^2, (\alpha_1 - \alpha_3)^2, (\alpha_2 - \alpha_3)^2$

\*47.11 Sea  $f(x) \in F[x]$  un polinomio mónico de grado  $n$  con todos sus factores irreducibles separables sobre  $F$ . Sea  $K \leq F$  el campo de descomposición de  $f(x)$  sobre  $F$ , y supóngase que  $f(x)$  se factoriza en  $K[x]$  en

$$\prod_{i=1}^n (x - \alpha_i).$$

Sea

$$\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j);$$

el producto  $(\Delta(f))^2$  es el **discriminante de  $f(x)$** .

- Muéstrese que  $\Delta(f) = 0$  si y sólo si  $f(x)$  tiene como factor el cuadrado de algún polinomio irreducible en  $F[x]$ .
- Muéstrese que  $(\Delta(f))^2 \in F$ .
- $G(K/F)$  puede considerarse un subgrupo de  $S_n$  donde  $S_n$  es el grupo de todas las permutaciones de  $\{\alpha_i \mid i = 1, \dots, n\}$ . Muéstrese que  $G(K/F)$ , considerado de esta manera, es un subgrupo de  $\bar{A}_n$ , el grupo formado por todas las permutaciones pares de  $\{\alpha_i \mid i = 1, \dots, n\}$  si y sólo si  $\Delta(f) \in F$ .

\*47.12 Un elemento de  $\mathbb{C}$  es un **entero algebraico** si es un cero de algún polinomio mónico en  $\mathbb{Z}[x]$ . Muéstrese que el conjunto de todos los enteros algebraicos forma un subanillo de  $\mathbb{C}$ .

\*47.13 Muéstrese que todo grupo finito es isomorfo a algún grupo de Galois  $G(K/F)$  para alguna extensión normal finita  $K$  de algún campo  $F$ .

## \*48

# Extensiones ciclotómicas

## \*48.1 EL GRUPO DE GALOIS DE UNA EXTENSION CICLOTOMICA

Esta sección trata de las extensiones de un campo  $F$ , obtenido mediante la agregación a  $F$  de algunas raíces del unitario. En el capítulo 45 se cubrió el caso de un campo finito  $F$ , de modo que trataremos principalmente el caso donde  $F$  es infinito.

**Definición** El campo de descomposición de  $x^n - 1$  sobre  $F$  es la  $n$ -ésima extensión ciclotómica de  $F$ .

Supóngase que  $F$  es cualquier campo y considérese  $(x^n - 1) \in F[x]$ . Como en la demostración del lema 45.1, vemos, por división, que si  $\alpha$  es un cero de  $x^n - 1$  y  $g(x) = (x^n - 1)/(x - \alpha)$ , entonces  $g(\alpha) = (n \cdot 1)(1/\alpha) \neq 0$ , siempre que la característica de  $F$  no divida  $n$ . Por tanto, bajo esta condición, el campo de descomposición de  $x^n - 1$  es separable y, en consecuencia, es una extensión normal de  $F$ .

Supóngase, de ahora en adelante, que así sucede, y sea  $K$  el campo de descomposición de  $x^n - 1$  sobre  $F$ . Entonces  $x^n - 1$  tiene  $n$  ceros distintos en  $K$  y, por el teorema 45.3, forman un grupo cíclico de orden  $n$  bajo la multiplicación de campo. Vimos en el corolario del teorema 6.4 que un grupo cíclico de orden  $n$  tiene  $\varphi(n)$  generadores, donde  $\varphi$  es la función si de Euler, presentada antes del teorema 24.8. En esta situación, estos  $\varphi(n)$  generadores son exactamente las raíces  $n$ -ésimas primitivas del unitario.

**Definición** El polinomio

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i),$$

donde las  $\alpha_i$  son las raíces  $n$ -ésimas primitivas del unitario en  $\bar{F}$ , es el  $n$ -ésimo *polinomio ciclotómico sobre  $F$* .

Como un automorfismo del grupo de Galois  $G(K/F)$  debe permutar las raíces  $n$ -ésimas primitivas del unitario, vemos que  $\Phi_n(x)$  queda fijo bajo todo elemento de  $G(K/F)$  considerado como extendido de manera natural hasta  $K[x]$ . Así,  $\Phi_n(x) \in F[x]$ . En particular, para  $F = \mathbb{Q}$ ,  $\Phi_n(x) \in \mathbb{Q}[x]$  y  $\Phi_n(x)$  es un divisor de  $x^n - 1$ . Así, sobre  $\mathbb{Q}$ , debemos tener en realidad, por el teorema 31.3, que  $\Phi_n(x) \in \mathbb{Z}[x]$ . Hemos visto en el corolario del teorema 31.4, que  $\Phi_p(x)$  es irreducible sobre  $\mathbb{Q}$ . Mientras que  $\Phi_n(x)$  no necesariamente es irreducible en el caso de los campos  $\mathbb{Z}_p$ ; se puede mostrar que sobre  $\mathbb{Q}$ ,  $\Phi_n(x)$  es irreducible.

Limitemos ahora nuestro análisis a la característica 0, en particular, a subcampos de los números complejos. Sea  $i$  el cero complejo usual de  $x^2 + 1$ . Usando identidades trigonométricas, el estudiante puede verificar formalmente que

$$(\cos \theta_1 + i \operatorname{sen} \theta_1)(\cos \theta_2 + i \operatorname{sen} \theta_2) = \cos (\theta_1 + \theta_2) + i \operatorname{sen} (\theta_1 + \theta_2).$$

Entonces es inmediato, por inducción, que

$$(\cos \theta + i \operatorname{sen} \theta)^n = \cos n\theta + i \operatorname{sen} n\theta.$$

En particular, si  $\theta = 2\pi/n$ , tenemos que

$$\left( \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n} \right)^n = \cos 2\pi + i \operatorname{sen} 2\pi = 1,$$

de modo que  $\cos (2\pi/n) + i \operatorname{sen} (2\pi/n)$  es una raíz  $n$ -ésima del unitario. La figura 48.1 puede ayudar a visualizar todo esto. Es bastante obvio, a partir de la figu-

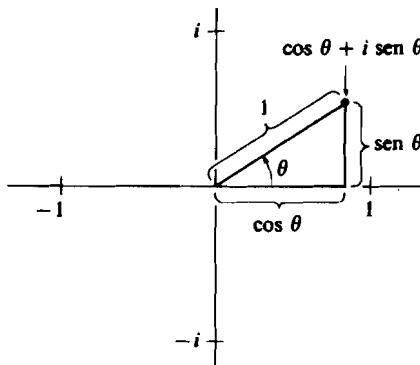


Figura 48.1

ra, que el menor entero  $m$  tal que  $((\cos 2\pi/n) + i \operatorname{sen} (2\pi/n))^m = 1$  es  $n$ . Así,  $\cos (2\pi/n) + i \operatorname{sen} (2\pi/n)$  es una raíz  $n$ -ésima primitiva del unitario, un cero de

$$\Phi_n(x) \in \mathbf{Q}[x].$$

**Ejemplo 48.1** Una raíz octava primitiva del unitario en  $\mathbf{C}$  es

$$\begin{aligned}\zeta &= \cos \frac{2\pi}{8} + i \operatorname{sen} \frac{2\pi}{8} \\ &= \cos \frac{\pi}{4} + i \operatorname{sen} \frac{\pi}{4} \\ &= \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} = \frac{1+i}{\sqrt{2}}.\end{aligned}$$

Por la teoría de los grupos cíclicos, en particular por el corolario del teorema 6.4, todas las raíces octavas primitivas en  $\mathbf{Q}$  son  $\zeta, \zeta^3, \zeta^5$  y  $\zeta^7$ , de modo que

$$\Phi_8(x) = (x - \zeta)(x - \zeta^3)(x - \zeta^5)(x - \zeta^7).$$

Los estudiantes pueden obtener directamente de esta expresión que  $\Phi_8(x) = x^4 + 1$  (véase el ejercicio 48.1). Compárese esto con el ejemplo 47.2. ■

Restringamos nuestro trabajo a  $F = \mathbf{Q}$  y supongamos, sin demostración, que  $\Phi_n(x)$  es irreducible sobre  $\mathbf{Q}$ . Sea

$$\zeta = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n},$$

de modo que  $\zeta$  es una raíz  $n$ -ésima primitiva del unitario. Nótese que  $\zeta$  es un generador del grupo cíclico multiplicativo de orden  $n$  formado por *todas* las raíces  $n$ -ésimas del unitario. Todas las raíces  $n$ -ésimas primitivas del unitario, esto es, todos los generadores de este grupo son de la forma  $\zeta^m$  para  $1 \leq m \leq n$  y  $m$  primo relativo con  $n$ . El campo  $\mathbf{Q}(\zeta)$  es el campo de descomposición de  $x^n - 1$  sobre  $\mathbf{Q}$ . Sea  $K = \mathbf{Q}(\zeta)$ . Si  $\zeta^m$  es otra raíz  $n$ -ésima primitiva del unitario, entonces, como  $\zeta$  y  $\zeta^m$  son conjugados sobre  $\mathbf{Q}$ , existe un automorfismo  $\tau_m$  en  $G(K/\mathbf{Q})$  que transforma  $\zeta$  en  $\zeta^m$ . Sea  $\tau$ , el automorfismo análogo en  $G(K/\mathbf{Q})$  correspondiente a la raíz  $n$ -ésima primitiva del unitario  $\zeta^n$ . Entonces

$$\zeta(\tau, \tau_m) = (\zeta^n)\tau_m = (\zeta\tau_m)^n = (\zeta^m)^n = \zeta^{nm}.$$

Esto muestra que el grupo de Galois  $G(K/\mathbf{Q})$  es isomorfo al grupo  $G_n$  del teorema 24.7, formado por los elementos de  $\mathbf{Z}_n$  primos relativos con  $n$  bajo la multiplicación módulo  $n$ . Este grupo tiene  $\phi(n)$  elementos y es, por supuesto, abeliano.

Este material es fácil. En el texto y en los ejercicios han aparecido varias veces casos particulares. Por ejemplo,  $\alpha$  del ejemplo 47.2 es una raíz octava primitiva del unitario, y en ese ejemplo hicimos razonamientos idénticos a los dados aquí. Resumiremos estos resultados en un teorema.

**Teorema 48.1** *El grupo de Galois de la  $n$ -ésima extensión ciclotómica de  $\mathbb{Q}$  tiene  $\varphi(n)$  elementos y es isomorfo al grupo formado por los enteros positivos menores que  $n$  y primos relativos con  $n$  bajo la multiplicación módulo  $n$ .*

**Ejemplo 48.2** El ejemplo 47.2 ilustra este teorema, pues es fácil ver que el campo de descomposición de  $x^4 + 1$  es igual al campo de descomposición de  $x^8 - 1$  sobre  $\mathbb{Q}$ . Esto se sigue del hecho de que  $\Phi_8(x) = x^4 + 1$  (véanse el ejemplo 48.1 y el ejercicio 48.1). ■

**Corolario** *El grupo de Galois de la  $p$ -ésima extensión ciclotómica de  $\mathbb{Q}$  para un primo  $p$  es cíclico de orden  $p - 1$ .*

**Demostración** Por el teorema 48.1, el grupo de Galois de la  $p$ -ésima extensión ciclotómica de  $\mathbb{Q}$  tiene  $\varphi(p) = p - 1$  elementos y es isomorfo al grupo de enteros positivos menores que  $p$  y primos relativos con  $p$  bajo la multiplicación módulo  $p$ . Este es, exactamente, el grupo multiplicativo  $\langle \mathbb{Z}_p^*, \cdot \rangle$  de elementos distintos de cero del campo  $\mathbb{Z}_p$ , bajo la multiplicación de campo. Por el corolario 1 del teorema 45.3, este grupo es cíclico. ■

## \*48.2 POLIGONOS CONSTRUIBLES

Concluimos con una aplicación para determinar cuáles  $n$ -gonos regulares son construibles con regla y compás. Vimos en el capítulo 39 que el  $n$ -gono regular es construible si y sólo si  $\cos(2\pi/n)$  es un número real construible. Sea ahora

$$\zeta = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n}.$$

Entonces,

$$\frac{1}{\zeta} = \cos \frac{2\pi}{n} - i \operatorname{sen} \frac{2\pi}{n},$$

para

$$\left( \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n} \right) \left( \cos \frac{2\pi}{n} - i \operatorname{sen} \frac{2\pi}{n} \right) = \cos^2 \frac{2\pi}{n} + \operatorname{sen}^2 \frac{2\pi}{n} = 1.$$

Pero entonces,

$$\zeta + \frac{1}{\zeta} = 2 \cos \frac{2\pi}{n}.$$

Así, el corolario del teorema 39.2 muestra que el  $n$ -gono regular es construible sólo si  $\zeta + 1/\zeta$  genera una extensión de  $\mathbf{Q}$  de grado una potencia de 2.

Si  $K$  es el campo de descomposición de  $x^n - 1$  sobre  $\mathbf{Q}$ , entonces  $[K:\mathbf{Q}] = \varphi(n)$ , por el teorema 48.1. Si  $\sigma \in G(K/\mathbf{Q})$  y  $\zeta\sigma = \zeta^r$ , entonces

$$\begin{aligned} \left(\zeta + \frac{1}{\zeta}\right)\sigma &= \zeta^r + \frac{1}{\zeta^r} \\ &= \left(\cos \frac{2\pi r}{n} + i \sin \frac{2\pi r}{n}\right) + \left(\cos \frac{2\pi r}{n} - i \sin \frac{2\pi r}{n}\right) \\ &= 2 \cos \frac{2\pi r}{n}. \end{aligned}$$

Pero para  $1 < r < n$  tenemos  $2 \cos(2\pi r/n) = 2 \cos(2\pi/n)$  sólo en el caso de que  $r = n - 1$ . Así, los únicos elementos de  $G(K/\mathbf{Q})$  que llevan a  $\zeta + 1/\zeta$  sobre sí mismo son el automorfismo identidad y el automorfismo  $\tau$ , con  $\zeta\tau = \zeta^{n-1} = 1/\zeta$ . Esto muestra que el subgrupo de  $G(K/\mathbf{Q})$  que deja fijo  $\mathbf{Q}(\zeta + 1/\zeta)$ , es de orden 2, de modo que, por la teoría de Galois,

$$\left[\mathbf{Q}\left(\zeta + \frac{1}{\zeta}\right):\mathbf{Q}\right] = \frac{\varphi(n)}{2}.$$

De aquí que el  $n$ -gono regular es construible sólo si  $\varphi(n)/2$ , y por tanto también  $\varphi(n)$ , es una potencia de 2.

Se puede mostrar, mediante argumentos elementales en teoría de números, que si

$$n = 2^v p_1^{s_1} \cdots p_t^{s_t},$$

donde las  $p_i$  son primos impares distintos que dividen a  $n$ , entonces

$$\varphi(n) = 2^{v-1} p_1^{s_1-1} \cdots p_t^{s_t-1} (p_1 - 1) \cdots (p_t - 1). \quad [48.1]$$

Si  $\varphi(n)$  es una potencia de 2, entonces todo primo impar que divide  $n$  debe aparecer sólo a la primera potencia y debe ser uno más que una potencia de 2. Así, debemos tener que cada

$$p_i = 2^m + 1$$

para alguna  $m$ . Como  $-1$  es un cero de  $x^q + 1$  para  $q$  un primo impar,  $x + 1$  divide  $x^q + 1$  para  $q$  un primo impar. Así, si  $m = qu$ , donde  $q$  es un primo impar,

entonces  $2^m + 1 = (2^u)^q + 1$  es divisible entre  $2^u + 1$ . Por tanto, para que  $p_i = 2^m + 1$  sea primo, debe tenerse que  $m$  sea divisible sólo entre 2, de modo que  $p_i$  tiene que ser de la forma

$$p_i = 2^{(2^k)} + 1,$$

un **primo de Fermat**. Fermat conjeturó que estos números  $2^{(2^k)} + 1$  eran primos para todos los enteros  $k$  no negativos. Euler mostró que mientras  $k = 0, 1, 2, 3$  y 4 dan los primos 3, 5, 17, 257 y 65 537, para  $k = 5$  encontramos que  $2^{(2^5)} + 1$  es divisible entre 641. Se ha mostrado que para  $5 \leq k \leq 16$ , todos los números  $2^{(2^k)} + 1$  son compuestos. El caso  $k = 17$  no se ha resuelto, al menos hasta que este libro fue a la imprenta. No se sabe si el número de primos de Fermat es finito o infinito.

Hemos demostrado, entonces, que los únicos  $n$ -gonos regulares que pueden construirse son aquéllos en que los primos impares que dividen  $n$  son primos de Fermat cuyo cuadrado no divide  $n$ . En particular, los únicos  $p$ -gonos regulares que pueden ser construibles para  $p$  primo mayor que 2, son aquéllos donde  $p$  es un primo de Fermat.

**Ejemplo 48.3** El 7-gono regular no es construible, pues 7 no es un primo de Fermat. Análogamente, el 18-gono regular no es construible, pues aunque 3 es un primo de Fermat, su cuadrado divide al 18. ■

Es un hecho, que se demostrará ahora, que todos estos  $n$ -gonos regulares que son candidatos a ser construibles, en efecto, son construibles. Sea nuevamente  $\zeta$  la raíz  $n$ -ésima primitiva del unitario  $\cos(2\pi/n) + i \sin(2\pi/n)$ . Vimos antes que

$$2 \cos \frac{2\pi}{n} = \zeta + \frac{1}{\zeta},$$

y que

$$\left[ \mathbf{Q}\left(\zeta + \frac{1}{\zeta}\right) : \mathbf{Q} \right] = \frac{\varphi(n)}{2}.$$

Supóngase ahora que  $\varphi(n)$  es una potencia  $2^s$  de 2. Sea  $E = \mathbf{Q}(\zeta + 1/\zeta)$ . Vimos antes que  $\mathbf{Q}(\zeta + 1/\zeta)$  es el subcampo de  $K = \mathbf{Q}(\zeta)$  que queda fijo bajo  $H_1 = \{i, \tau\}$  donde  $i$  es el elemento identidad de  $G(K/\mathbf{Q})$  y  $\zeta\tau = 1/\zeta$ . Por la teoría de Sylow, existen subgrupos adicionales  $H_j$  de orden  $2^j$  de  $G(\mathbf{Q}(\zeta)/\mathbf{Q})$  para  $j = 0, 2, 3, \dots, s$  tales que

$$\{i\} = H_0 < H_1 < \cdots < H_s = G(\mathbf{Q}(\zeta)/\mathbf{Q}).$$

Por la teoría de Galois,

$$\mathbf{Q} = K_{H_s} < K_{H_{s-1}} < \cdots < K_{H_1} = \mathbf{Q}\left(\zeta + \frac{1}{\zeta}\right),$$

y  $[K_{H_{j-1}} : K_{H_j}] = 2$ . Nótese que  $(\zeta + 1/\zeta) \in \mathbb{R}$ , de modo que  $\mathbb{Q}(\zeta + 1/\zeta) < \mathbb{R}$ . Si  $K_{H_{j-1}} = K_{H_j}(x_j)$ , entonces  $x_j$  es un cero de algún  $(a_jx^2 + b_jx + c_j) \in K_{H_j}[x]$ . Por la «fórmula cuadrática» conocida, tenemos

$$K_{H_{j-1}} = K_{H_j}(\sqrt{b_j^2 - 4a_jc_j}).$$

Como se vio en el capítulo 39 que la construcción de raíces cuadradas de números construibles positivos puede realizarse mediante regla y compás, se sabe que todo elemento en  $\mathbb{Q}(\zeta + 1/\zeta)$ , en particular,  $\cos(2\pi/n)$ , es construible. De aquí que los  $n$ -gonos regulares donde  $\varphi(n)$  es una potencia de 2, son construibles.

Resumamos el trabajo de este párrafo en un teorema.

**Teorema 48.2** *El  $n$ -gono regular es construible con regla y compás si y sólo si todos los primos impares que dividen  $n$  son primos de Fermat cuyo cuadrado no divide  $n$ .*

**Ejemplo 48.4** El 60-gono regular es construible, ya que  $60 = (2^2)(3)(5)$  y 3 y 5 son ambos primos de Fermat.

## Ejercicios

\*48.1 Con referencia al ejemplo 48.1, complétense los cálculos indicados para mostrar que  $\Phi_8(x) = x^4 + 1$ . [Sugerencia: calcúlese el producto en términos de  $\zeta$  y después úsese el hecho de que  $\zeta^8 = 1$  y  $\zeta^4 = -1$  para simplificar los coeficientes.]

\*48.2 Clasifíquese el grupo del polinomio  $(x^{20} - 1) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$  de acuerdo con el teorema fundamental de los grupos abelianos finitamente generados. [Sugerencia: úsese el teorema 48.1.]

\*48.3 Usese la fórmula para  $\varphi(n)$  en términos de la factorización de  $n$  como se dio en la ecuación [48.1] de la sección 48.2, para calcular lo siguiente:

a)  $\varphi(60)$       b)  $\varphi(1000)$       c)  $\varphi(8100)$

\*48.4 Dízase los primeros 30 valores de  $n \geq 3$  para los cuales el  $n$ -gono regular es construible con regla y compás.

\*48.5 Muéstrese que si  $F$  es un campo de característica que no divide  $n$ , entonces,

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

en  $F[x]$ , donde el producto es sobre todos los divisores  $d$  de  $n$ .

\*48.6 Encuéntrese el polinomio ciclotómico  $\Phi_n(x)$  sobre  $\mathbb{Q}$  para  $n = 1, 2, 3, 4, 5$  y  $6$ . [Sugerencia: úsese el ejercicio 48.5.]

\*48.7 ¿Falso o verdadero?

- a)  $\Phi_n(x)$  es irreducible sobre todo campo de característica 0.
- b) Todo cero en  $\mathbb{C}$  de  $\Phi_n(x)$  es una raíz  $n$ -ésima primitiva del unitario.

- c) El grupo de  $\Phi_n(x) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$  tiene orden  $n$ .
  - d) El grupo de  $\Phi_n(x) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$  es abeliano.
  - e) El grupo de Galois del campo de descomposición de  $\Phi_n(x)$  sobre  $\mathbb{Q}$  tiene orden  $\phi(n)$ .
  - f) El 25-gono regular es construible con regla y compás.
  - g) El 17-gono regular es construible con regla y compás.
  - h) Para un primo  $p$ , el  $p$ -gono regular es construible si y sólo si  $p$  es un primo de Fermat.
  - i) Todos los enteros de la forma  $2^{(2^k)} + 1$  para enteros no negativos  $k$  son primos de Fermat.
  - j) Todos los primos de Fermat son números de la forma  $2^{(2^k)} + 1$  para enteros no negativos  $k$ .
- 

\*48.8 Encuéntrese el menor ángulo de grado entero, esto es,  $1^\circ$ ,  $2^\circ$ ,  $3^\circ$  y así sucesivamente, construible con regla y compás. [Sugerencia: construir un ángulo de  $1^\circ$  equivale a construir el 360-gono regular, y así sucesivamente.]

\*48.9 Sea  $K$  el campo de descomposición de  $x^{12} - 1$  sobre  $\mathbb{Q}$ .

- a) Encuéntrese  $[K : \mathbb{Q}]$ .
- b) Muéstrese que para  $\sigma \in G(K/\mathbb{Q})$ ,  $\sigma^2$  es el automorfismo identidad. Clasifíquese  $G(K/\mathbb{Q})$  de acuerdo con el teorema fundamental de los grupos abelianos finitamente generados.

\*48.10 Encuéntrese  $\Phi_3(x)$  sobre  $\mathbb{Z}_2$ . Encuéntrese  $\Phi_8(x)$  sobre  $\mathbb{Z}_3$ .

\*48.11 ¿Cuántos elementos hay en el campo de descomposición de  $x^6 - 1$  sobre  $\mathbb{Z}_3$ ?

\*48.12 Encuéntrese  $\Phi_{12}(x)$  en  $\mathbb{Q}[x]$ . [Sugerencia: úsese los ejercicios 48.5 y 48.6.]

\*48.13 Muéstrese que en  $\mathbb{Q}[x]$ ,  $\Phi_{2n}(x) = \Phi_n(-x)$  para enteros impares  $n > 1$ . [Sugerencia: úsese el ejercicio 48.5 y la factorización  $x^{2^n} - 1 = -(x^n - 1)((-x)^n - 1)$ . Procédase por inducción.]

\*48.14 Sean  $n, m \in \mathbb{Z}^+$  primos relativos. Muéstrese que el campo de descomposición en  $\mathbb{C}$  de  $x^{nm} - 1$  sobre  $\mathbb{Q}$  es el mismo que el campo de descomposición en  $\mathbb{C}$  de  $(x^n - 1)(x^m - 1)$  sobre  $\mathbb{Q}$ .

\*48.15 Sean  $n, m \in \mathbb{Z}^+$  primos relativos. Muéstrese que el grupo de  $(x^{nm} - 1) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$  es isomorfo al producto directo de los grupos de  $(x^n - 1) \in \mathbb{Q}[x]$  y de  $(x^m - 1) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$ . [Sugerencia: úsese la teoría de Galois y muéstrese que los grupos de  $x^n - 1$  y  $x^m - 1$  pueden ambos considerarse subgrupos del grupo  $x^{nm} - 1$ . Después, úsese el teorema 8.6.]

## 49

# Insolubilidad de la quíntica

## 49.1 EL PROBLEMA

Ya se conoce el hecho de que un polinomio cuadrático  $f(x) = ax^2 + bx + c$ ,  $a \neq 0$ , con coeficientes reales, tiene como ceros en  $\mathbb{C}$  a  $(-b \pm \sqrt{b^2 - 4ac})/2a$ . En realidad, esto es cierto para  $f(x) \in F[x]$  donde  $F$  es cualquier campo de característica  $\neq 2$  y los ceros están en  $F$ . En el ejercicio 49.1 se pide mostrarlo. Así, por ejemplo,  $(x^2 + 2x + 3) \in \mathbb{Q}[x]$  tiene sus ceros en  $\mathbb{Q}(\sqrt{-2})$ . Uno se pregunta si los ceros de un polinomio cúbico sobre  $\mathbb{Q}$  también pueden expresarse siempre en términos de radicales. La respuesta es si y, en efecto, incluso los ceros de un polinomio de grado 4 sobre  $\mathbb{Q}$  pueden expresarse en términos de radicales. Después de que los matemáticos trataron por años de encontrar la «fórmula radical» para los ceros de un polinomio de grado 5, fue un triunfo cuando Abel probó que una quíntica no necesariamente es soluble por radicales. Nuestra primera tarea será describir de manera precisa lo que esto significa. Al lector le encantará ver que una gran cantidad del álgebra que hemos desarrollado se usa en el análisis que presentamos a continuación.

## 49.2 EXTENSIONES POR RADICALES

**Definición** Una extensión  $K$  de un campo  $F$  es una *extensión de  $F$  por radicales* si existen elementos  $\alpha_1, \dots, \alpha_r \in K$  y enteros positivos  $n_1, \dots, n_r$  tales que  $K = F(\alpha_1, \dots, \alpha_r)$ ,  $\alpha_1^{n_1} \in F$  y  $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$  para  $1 < i \leq r$ . Un polinomio  $f(x) \in F[x]$  es *sóluble por radicales sobre  $F$*  si el campo de descomposición  $E$  de  $f(x)$  sobre  $F$  está contenido en una extensión de  $F$  por radicales.

Entonces, un polinomio  $f(x) \in F[x]$  es soluble por radicales sobre  $F$  si podemos obtener todo cero de  $f(x)$  usando una sucesión finita de operaciones de suma, resta, multiplicación, división y extracción de raíces  $n$ -ésimas, comenzando con elementos de  $F$ . Ahora bien, decir que la quintica no es soluble en el caso clásico, esto es, característica 0, no es decir que ninguna quíntica es soluble, como lo muestra el ejemplo siguiente.

**Ejemplo 49.1** El polinomio  $x^5 - 1$  es soluble por radicales sobre  $\mathbb{Q}$ . El campo de descomposición  $K$  de  $x^5 - 1$  está generado sobre  $\mathbb{Q}$  por una raíz quinta primitiva  $\zeta$  del unitario. Entonces,  $\zeta^5 = 1$  y  $K = \mathbb{Q}(\zeta)$ . De manera análoga,  $x^5 - 2$  es soluble por radicales sobre  $\mathbb{Q}$ , pues su campo de descomposición sobre  $\mathbb{Q}$  está generado por  $\sqrt[5]{2}$  y  $\zeta$ , donde  $\sqrt[5]{2}$  es el cero real de  $x^5 - 2$ . ■

Decir que la quíntica es insoluble en el caso clásico, significa que existe algún polinomio de grado 5, con coeficientes reales, que no es soluble por radicales. Mostraremos esto. En este capítulo supondremos que todos los campos mencionados tienen característica 0.

El esbozo del argumento es muy fácil de dar y vale la pena tratar de recordarlo.

- 1 *Mostraremos que un polinomio  $f(x) \in F[x]$  es soluble por radicales sobre  $F$  (si y) sólo si su campo de descomposición  $E$  sobre  $F$  tiene un grupo de Galois soluble.* Recuérdese que un grupo soluble es aquél que tiene una serie de composición con coeficientes abelianos. Aunque este teorema vaya en los dos sentidos, no probaremos la parte «si».
- 2 *Mostraremos que existe un subcampo  $F$  de los números reales y un polinomio  $f(x) \in F[x]$  de grado 5 con un campo de descomposición  $E$  sobre  $F$  tal que  $G(E/F) \cong S_5$ , el grupo simétrico en 5 letras.* Recuérdese que una serie de composición para  $S_5$  es  $\{\{1\}\} < A_5 < S_5$ . Como  $A_5$  no es abeliano, habremos terminado.

El lema siguiente hace la mayor parte del trabajo para el paso 1.

**Lema 49.1** *Sea  $F$  un campo de característica 0 y sea  $a \in F$ . Si  $K$  es el campo de descomposición de  $x^n - a$  sobre  $F$ , entonces  $G(K/F)$  es un grupo soluble.*

**Demostración** Supóngase primero que  $F$  contiene todas las raíces  $n$ -ésimas del unitario. Por el teorema 45.3 y los comentarios precedentes, las raíces  $n$ -ésimas del unitario forman un subgrupo cíclico de  $\langle F^*, \cdot \rangle$ . Sea  $\zeta$  un generador del subgrupo. (En realidad, los generadores son precisamente las raíces  $n$ -ésimas *primitivas* del unitario.) Entonces, las raíces  $n$ -ésimas del unitario son

$$1, \zeta, \zeta^2, \dots, \zeta^{n-1}.$$

Si  $\beta \in \bar{F}$  es un cero de  $(x^n - a) \in F[x]$ , entonces todos los ceros de  $x^n - a$  son

$$\beta, \zeta\beta, \zeta^2\beta, \dots, \zeta^{n-1}\beta.$$

Como  $K = F(\beta)$ , un automorfismo de  $\sigma$  en  $G(K/F)$  está determinado por el valor  $\beta\sigma$  del automorfismo  $\sigma$  en  $\beta$ . Si  $\beta\sigma = \zeta^i\beta$  y  $\beta\tau = \zeta^j\beta$ , donde  $\tau \in G(K/F)$ , entonces

$$\beta(\sigma\tau) = (\beta\sigma)\tau = (\zeta^i\beta)\tau = \zeta^i(\beta\tau) = \zeta^i\zeta^j\beta,$$

pues  $\zeta^i \in F$ . De manera análoga,

$$\beta(\tau\sigma) = \zeta^j\zeta^i\beta.$$

Así,  $\sigma\tau = \tau\sigma$  y  $G(K/F)$  es abeliano y, por tanto, soluble.

Supóngase ahora que  $F$  no contiene una raíz  $n$ -ésima primitiva del unitario. Sea  $\zeta$  un generador del grupo cíclico de raíces  $n$ -ésimas del unitario bajo la multiplicación en  $\bar{F}$ . Sea  $\beta$  nuevamente un cero de  $x^n - a$ . Como  $\beta$  y  $\zeta\beta$  están ambos en el campo de descomposición  $K$  de  $x^n - a$ ,  $\zeta = (\zeta\beta)/\beta$  está en  $K$ . Sea  $F = F(\zeta)$ , de modo que tenemos  $F < F \leq K$ . Ahora,  $F$  es una extensión normal de  $F$  puesto que  $F$  es el campo de descomposición de  $x^n - 1$ . Como  $F' = F(\zeta)$ , un automorfismo  $\eta$  en  $G(F'/F)$  está determinado por  $\zeta\eta$  y debemos tener  $\zeta\eta = \zeta^i$  para alguna  $i$ , ya que todos los ceros de  $x^n - 1$  son potencias de  $\zeta$ . Si  $\zeta\mu = \zeta^j$  para  $\mu \in G(F'/F)$ , entonces

$$\zeta(\eta\mu) = (\zeta\eta)\mu = \zeta^i\mu = (\zeta\mu)^i = (\zeta^j)^i = \zeta^{ij},$$

y, en forma análoga,

$$\zeta(\mu\eta) = \zeta^{ij}.$$

Así,  $G(F'/F)$  es abeliano. Por el teorema principal de la teoría de Galois,

$$\{1\} \leq G(K/F) \leq G(F/F)$$

es una serie normal y, por tanto, una serie subnormal de grupos. La primera parte de la demostración muestra que  $G(K/F)$  es abeliano, y la teoría de Galois afirma que  $G(K/F)/(G(K/F))$  es isomorfo a  $G(F/F)$ , el cual es abeliano. Es fácil ver que si un grupo tiene una serie subnormal de subgrupos con grupos cociente abelianos, entonces, cualquier refinamiento de esta serie también tiene grupos cociente abelianos. (Véase el ejercicio 49.6.) Así, una serie de composición de  $G(K/F)$  debe tener grupos cociente abelianos, de modo que  $G(K/F)$  es soluble. ■

El siguiente teorema muestra que si  $K$  es una extensión normal de  $F$  por radicales, entonces  $G(K/F)$  es soluble. El ejercicio 49.8 muestra, entonces, que si  $f(x) \in F[x]$  es soluble por radicales y tiene campo de descomposición  $E$ ,  $G(E/F)$  es soluble. Esto completará la parte 1 de nuestro programa.

**Teorema 49.1** *Si  $K$  es una extensión normal por radicales de un campo  $F$  de característica 0, entonces  $G(K/F)$  es soluble.*

**Demostración** Sabemos que existen  $\alpha_1, \dots, \alpha_r \in K$  y enteros positivos  $n_1, \dots, n_r$  tales que  $K = F(\alpha_1, \dots, \alpha_r)$ ,  $\alpha_i^{n_i} \in F$  y  $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$  para  $1 < i \leq r$ . Sea  $K_0 = F$  y sea  $K_i$  el campo de descomposición de  $x^{n_i} - \alpha_i^{n_i}$  sobre  $K_{i-1}$ . Entonces,  $K \leq K_r$ , y el lema 49.1 muestra que  $G(K_i/K_{i-1})$  es soluble. Como  $G(K_i/K_{i-1}) \simeq G(K_r/K_{r-1})/G(K_r/K_i)$ , la serie normal

$$\{i\} \leq G(K_r/K_{r-1}) \leq G(K_r/K_{r-2}) \leq \cdots \leq G(K_r/K_0) = G(K_r/F)$$

tiene grupos cociente solubles. El ejercicio 49.7 muestra que esta serie tiene, entonces, un refinamiento que es una serie de composición con cocientes abelianos, de modo que  $G(K_r/F)$  es soluble. Como  $G(K_r/F) \simeq G(K_r/F)/G(K_r/K)$ , el ejercicio 15.16 muestra que  $G(K_r/F)$  es soluble. ■

### 49.3 INSOLUBILIDAD DE LA QUINTICA

Nos falta mostrar que existe un subcampo  $F$  de los números reales y un polinomio  $f(x) \in F[x]$  de grado 5 tal que el campo de descomposición  $E$  de  $f(x)$  sobre  $F$  tiene grupo de Galois isomorfo a  $S_5$ .

Sea  $y_1 \in R$  trascendente sobre  $Q$ ,  $y_2 \in R$  trascendente sobre  $Q(y_1)$  y así sucesivamente, hasta obtener  $y_5 \in R$  trascendente sobre  $Q(y_1, \dots, y_4)$ . Resulta fácil mostrar, mediante un razonamiento de conteo, que existen dichos números reales trascendentes. Los trascendentes hallados de esta manera son **elementos trascendentes independientes sobre  $Q$** . Sea  $E = Q(y_1, \dots, y_5)$ , y sea

$$f(x) = \prod_{i=1}^5 (x - y_i).$$

Así,  $f(x) \in E[x]$ . Ahora, los coeficientes de  $f(x)$  están, excepto quizás por el signo, entre las llamadas *funciones simétricas elementales* en las  $y_i$ , a saber,

$$\begin{aligned} s_1 &= y_1 + y_2 + \cdots + y_5, \\ s_2 &= y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + \\ &\quad + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5, \\ &\vdots \\ s_5 &= y_1y_2y_3y_4y_5. \end{aligned}$$

El coeficiente para  $x^i$  en  $f(x)$  es  $\pm s_{5-i}$ . Sea  $F = Q(s_1, s_2, \dots, s_5)$ ; entonces,  $f(x) \in F[x]$  (véase la figura 49.1). Claramente,  $E$  es el campo de descomposición sobre  $F$  de  $f(x)$ . Como las  $y_i$  se comportan como indeterminadas sobre  $Q$ , para cada  $\sigma \in S_5$ , el grupo simétrico de cinco letras,  $\sigma$  induce un automorfismo  $\bar{\sigma}$  de  $E$  definido por  $a\bar{\sigma} = a$  para  $a \in Q$  y  $y_i\bar{\sigma} = y_{i\sigma}$ . Como  $\prod_{i=1}^5 (x - y_{i\sigma})$  es el mismo polinomio que  $\prod_{i=1}^5 (x - y_i)$ , tenemos

$$s_i\bar{\sigma} = s_{i\sigma}$$

$$\begin{array}{c} E = \mathbb{Q}(y_1, \dots, y_5) \\ \downarrow \\ F = \mathbb{Q}(s_1, \dots, s_5) \\ \downarrow \\ \mathbb{Q} \end{array}$$

**Figura 49.1**

para cada  $i$ , de modo que  $\bar{\sigma}$  deja fijo  $F$  y, por tanto,  $\bar{\sigma} \in G(E/F)$ . Ahora,  $S_5$  tiene orden  $5!$  de modo que

$$|G(E/F)| \geq 5!.$$

Como el campo de descomposición de un polinomio de grado 5 sobre  $F$  tiene grado a lo más  $5!$  sobre  $F$ , vemos que

$$|G(E/F)| \leq 5!.$$

Así,  $|G(E/F)| = 5!$  y los automorfismos  $\bar{\sigma}$  forman todo el grupo de Galois  $G(E/F)$ . Por tanto,  $G(E/F) \cong S_5$ , de modo que  $G(E/F)$  no es soluble. Por los comentarios anteriores al teorema 49.1,  $f(x)$  no es soluble por radicales sobre  $F$ . Resumimos esto en un teorema.

**Teorema 49.2** *Sean  $y_1, \dots, y_5$  números reales trascendentales independientes sobre  $\mathbb{Q}$ . El polinomio*

$$f(x) = \prod_{i=1}^5 (x - y_i)$$

*no es soluble por radicales sobre  $F = \mathbb{Q}(s_1, \dots, s_5)$ , donde  $s_i$  es la  $i$ -ésima función simétrica elemental en  $y_1, \dots, y_5$ .*

Es evidente que una generalización de estos argumentos muestra que (*objetivo final*) un polinomio de grado  $n$  no necesariamente es soluble por radicales para  $n \geq 5$ .

En conclusión, comentamos que existen polinomios de grado 5 en  $\mathbb{Q}[x]$  que no son solubles por radicales sobre  $\mathbb{Q}$ . La demostración se deja para los ejercicios (véase el ejercicio 49.9).

**Ejercicios**

**49.1** Sea  $F$  un campo y sea  $f(x) = ax^2 + bx + c$  en  $F[x]$  donde  $a \neq 0$ . Muéstrese que si la característica de  $F$  no es 2, el campo de descomposición de  $f(x)$  sobre  $F$  es  $F(\sqrt{b^2 - 4ac})$ . [Sugerencia: complétense el cuadrado, como se hacía en la escuela secundaria, para deducir la «fórmula cuadrática».]

**49.2** ¿Se puede obtener el campo de descomposición  $K$  de  $x^2 + x + 1$  sobre  $\mathbb{Z}_2$  agregando una raíz cuadrada a  $\mathbb{Z}_2$  de un elemento en  $\mathbb{Z}_2$ ? ¿Es  $K$  una extensión de  $\mathbb{Z}_2$  por radicales?

**49.3** Muéstrese que si  $F$  es un campo de característica diferente de 2 y

$$f(x) = ax^4 + bx^2 + c,$$

donde  $a \neq 0$ , entonces  $f(x)$  es soluble por radicales sobre  $F$ .

**49.4** ¿Es soluble por radicales sobre  $F$  todo polinomio en  $F[x]$  de la forma  $ax^8 + bx^6 + cx^4 + dx^2 + e$ , donde  $a \neq 0$ , si  $F$  es de característica 0? ¿Por qué?

**49.5** ¿Falso o verdadero?

- a) Sea  $F$  un campo de característica 0. Un polinomio en  $F[x]$  es soluble por radicales si y sólo si su campo de descomposición en  $F$  está contenido en una extensión por radicales de  $F$ .
- b) Sea  $F$  un campo de característica 0. Un polinomio en  $F[x]$  es soluble por radicales si y sólo si su campo de descomposición en  $F$  tiene grupo de Galois soluble sobre  $F$ .
- c) El campo de descomposición de  $x^{17} - 5$  sobre  $\mathbb{Q}$  tiene grupo de Galois soluble.
- d) Los números  $\pi$  y  $\sqrt{\pi}$  son números trascendentes independientes sobre  $\mathbb{Q}$ .
- e) El grupo de Galois de una extensión finita de un campo finito es soluble.
- f) Ningún polinomio quinto es soluble por radicales sobre cualquier campo.
- g) Todo polinomio de grado 4 sobre un campo de característica 0 es soluble por radicales.
- h) Los ceros de un polinomio cúbico sobre un campo  $F$  de característica 0 siempre pueden alcanzarse mediante una sucesión finita de operaciones de suma, resta, multiplicación, división y extracción de raíces cuadradas, comenzando con elementos en  $F$ .
- i) Los ceros de un polinomio cúbico sobre un campo  $F$  de característica 0 nunca pueden alcanzarse mediante una sucesión finita de operaciones de suma, resta, multiplicación, división y extracción de raíces cuadradas, comenzando con elementos en  $F$ .
- j) La teoría de series normales de grupos desempeña un papel importante en las aplicaciones de la teoría de Galois.

\***49.6** Muéstrese que, para un grupo finito, todo refinamiento de una serie subnormal con cocientes abelianos también tiene cocientes abelianos, completando así la demostración del lema 49.1. [Sugerencia: úsese el teorema 15.3.]

\***49.7** Muéstrese que, para un grupo finito, una serie subnormal con grupos cociente solubles se puede refinar hasta una serie de composición con cocientes abelianos, completando así la demostración del teorema 49.1. [Sugerencia: úsese el teorema 15.3.]

\*49.8 Sea  $K$  una extensión normal por radicales de un campo  $F$  de característica 0 y sea  $E$  una extensión normal de  $F$ ,  $F \leq E < K$ . Muéstrese que  $G(E/F)$  es soluble. [Sugerencia: úsese la teoría de Galois, el teorema 49.1 y el ejercicio 15.16.]

\*49.9 Este ejercicio exhibe un polinomio de grado 5 en  $\mathbb{Q}[x]$  que no es soluble por radicales sobre  $\mathbb{Q}$ .

- a) Muéstrese que si un subgrupo  $H$  de  $S_5$  contiene un ciclo de longitud 5 y una transposición  $\tau$ , entonces  $H = S_5$ . [Sugerencia: muéstrese que  $H$  contiene toda transposición de  $S_5$  y aplíquese el corolario del teorema 5.1. Véase el ejercicio 9.15.]
- b) Muéstrese que si  $f(x)$  es un polinomio irreducible en  $\mathbb{Q}[x]$  de grado 5 con exactamente dos ceros complejos y tres reales en  $\mathbb{C}$ , entonces el grupo de  $f(x)$  sobre  $\mathbb{Q}$  es  $S_5$ . [Sugerencia: úsese la teoría de Sylow para mostrar que el grupo tiene un elemento de orden 5. Usese el hecho de que  $f(x)$  tiene exactamente dos ceros complejos para mostrar que el grupo tiene un elemento de orden 2. Después, aplíquese a).]
- c) El polinomio  $f(x) = 2x^5 - 5x^4 + 5$  es irreducible en  $\mathbb{Q}[x]$ , por el criterio de Eisenstein, con  $p = 5$ . Usense técnicas de cálculo para encontrar los máximos y mínimos relativos y para «graficar la función polinomial  $f$ » lo suficiente para ver que  $f(x)$  debe tener exactamente tres ceros reales en  $\mathbb{C}$ . Conclúyase, a partir de b) y del teorema 49.1, que  $f(x)$  no es soluble por radicales sobre  $\mathbb{Q}$ .

## APENDICE

# Inducción matemática

En ocasiones queremos probar que una afirmación acerca de enteros positivos se cumple para todos los enteros positivos, o quizás para alguna sucesión finita o infinita de enteros consecutivos. Dichas demostraciones se hacen usando inducción matemática. La validez del método se basa en un axioma de los enteros positivos.

**Axioma de inducción** *Sea  $S$  un subconjunto de  $\mathbf{Z}^+$  que satisface*

*$1 \in S$  y*

*si  $k \in S$ , entonces  $(k + 1) \in S$ .*

*Entonces,  $S = \mathbf{Z}^+$ .*

De este axioma obtenemos, de inmediato, el método de inducción matemática.

**Inducción matemática** *Sea  $P(n)$  una afirmación acerca del entero  $n$ . Supóngase que*

*$P(1)$  es cierto y*

*si  $P(k)$  es cierto, entonces  $P(k + 1)$  es cierto.*

*Entonces,  $P(n)$  es cierto para todos los  $n \in \mathbf{Z}^+$ .*

Casi siempre se quiere mostrar que  $P(n)$  vale para todos los  $n \in \mathbf{Z}^+$ . Si se desea mostrar que vale sólo para  $r, r + 1, r + 2, \dots, s - 1, s$ , entonces se muestra que  $P(r)$  es cierto y que  $P(k)$  implica  $P(k + 1)$  para  $r \leq k \leq s - 1$ . Nótese que  $r$  puede ser cualquier entero en  $\mathbf{Z}$ , positivo, negativo o cero.

**Ejemplo A1** Probemos la fórmula

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2} \quad [A1]$$

para la suma de la progresión aritmética, usando inducción matemática.

Sea  $P(n)$  la afirmación de que la fórmula [A1] es cierta. Para  $n = 1$  obtenemos

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

de modo que  $P(1)$  es cierto.

Supóngase que  $P(k)$  es cierto, esto es,

$$1 + 2 + \cdots + k = \frac{k(k + 1)}{2}.$$

Entonces,

$$\begin{aligned} 1 + 2 + \cdots + (k + 1) &= (1 + 2 + \cdots + k) + (k + 1) \\ &= \frac{k(k + 1)}{2} + (k + 1) = \frac{k^2 + k + 2k + 2}{2} \\ &= \frac{k^2 + 3k + 2}{2} = \frac{(k + 1)(k + 2)}{2} \end{aligned}$$

de modo que se cumple  $P(k + 1)$ . Así, la fórmula [A1] es cierta para todos los  $n \in \mathbb{Z}^+$ . ■

**Ejemplo A2** Mostremos que un conjunto de  $n$  elementos tiene, en total,  $2^n$  subconjuntos para  $n \in \{0, 1, 2, 3, \dots\} = \mathbb{Z}^+ \cup \{0\}$ .

Esta vez comenzamos la inducción con  $n = 0$ . Sea  $S$  el conjunto finito tal que  $|S| = n$ , deseamos mostrar que

$$P(n): S \text{ tiene } 2^n \text{ subconjuntos.}$$

[A2]

Si  $|S| = 0$ , entonces  $S = \emptyset$  y tiene un solo subconjunto, a saber,  $\emptyset$ . Como  $2^0 = 1$  vemos que  $P(0)$  es cierto.

Supóngase que  $P(k)$  es cierto y sea  $S$  con  $k + 1$  elementos. Sea  $c$  un elemento de  $S$ . Entonces,  $S - \{c\}$  tiene  $k$  elementos y, por tanto,  $2^k$  subconjuntos. Ahora bien, todo subconjunto de  $S$  contiene  $c$  o no contiene  $c$ . Aquéllos que no contienen  $c$  son subconjuntos de  $S - \{c\}$  y hay  $2^k$  de ellos, por la hipótesis de inducción. Cada subconjunto que contiene  $c$  consta de alguno de los  $2^k$  subconjuntos que no contienen  $c$ , agregando  $c$ . Hay, también,  $2^k$  de dichos subconjuntos.

El número total de subconjuntos de  $S$  es, entonces,

$$2^k + 2^k = 2^k(2) = 2^{k+1},$$

de modo que  $P(k + 1)$  es cierto. Así,  $P(n)$  es cierto para  $n = 0$  y para  $n \in \mathbf{Z}^+$ . ■

**Ejemplo A3** Sea  $x \in \mathbf{R}$ ,  $x > -1$ ,  $x \neq 0$ . Mostremos que  $(1 + x^n) > 1 + nx$  para toda  $n \geq 2$ ,  $n \in \mathbf{Z}^+$ .

Sea  $P(n)$  la afirmación

$$(1 + x)^n > 1 + nx. \quad [\text{A3}]$$

( Nótese que  $P(1)$  es falso.) Entonces,  $P(2)$  es la afirmación  $(1 + x)^2 > 1 + 2x$ . Ahora,  $(1 + x)^2 = 1 + 2x + x^2$  y  $x^2 > 0$ , pues  $x \neq 0$ . Así,  $(1 + x)^2 > 1 + 2x$  de modo que  $P(2)$  es cierto.

Supóngase que  $P(k)$  es cierta, de modo que

$$(1 + x)^k > 1 + kx. \quad [\text{A4}]$$

Ahora,  $1 + x > 0$ , pues  $x > -1$ . Multiplicando ambos lados de la ecuación [A4] por  $1 + x$  obtenemos

$$(1 + x)^{k+1} > (1 + kx)(1 + x) = 1 + (k + 1)x + kx^2.$$

Como  $kx^2 \geq 0$ , vemos que  $P(k + 1)$  es cierto. Así,  $P(n)$  es cierto para  $n \geq 2$ ,  $n \in \mathbf{Z}^+$ . ■

Para concluir, mencionamos que ya se tendrá ocasión de usar la *inducción completa*, donde la afirmación

si  $P(k)$  es cierto, entonces  $P(k + 1)$  es cierto

se reemplaza por la afirmación

si  $P(m)$  es cierto para  $1 \leq m \leq k$ , entonces  $P(k + 1)$  es cierto.

De nuevo se trata de mostrar que  $P(k + 1)$  es cierto, sabiendo que  $P(k)$  es cierto. Pero si ya se alcanzó el paso de inducción donde se ha probado  $P(k)$ , entonces se sabe que  $P(m)$  es cierto si  $1 \leq m \leq k$ , de modo que la hipótesis reforzada de la segunda afirmación es permisible.

## Ejercicios

---

A1 Muéstrese que  $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}$  para  $n \in \mathbf{Z}^+$ .

A2 Muéstrese que  $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n + 1)^2}{4}$  para  $n \in \mathbf{Z}^+$ .

**A3** Muéstrese que  $1 + 3 + 5 + \cdots + (2n - 1) = n^2$  para  $n \in \mathbb{Z}^+$ .

**A4** Muéstrese que  $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$  para  $n \in \mathbb{Z}^+$ .

**A5** Pruébese por inducción que si  $a, r \in \mathbb{R}$  y  $r \neq -1$ , entonces  $a + ar + ar^2 + \cdots + ar^n = a(1 - r^{n+1})/(1 - r)$  para  $n \in \mathbb{Z}^+$ .

**A6** Encuéntrese la falla en este razonamiento.

Mostremos por inducción que dos números enteros positivos cualesquiera, son iguales. Usemos inducción en el máximo de los dos números. Sea  $P(n)$  la afirmación de que dos enteros positivos con valor máximo  $n$  son iguales.

Como los dos únicos enteros positivos cuyo valor máximo es 1 son 1 y 1, vemos que  $P(1)$  es cierto.

Supóngase que  $P(k)$  es cierto y sean  $r$  y  $s$  números positivos con valor máximo  $k + 1$ . Entonces, el valor máximo de  $r - 1$  y  $s - 1$  es  $k$ , de modo que  $r - 1 = s - 1$  por la hipótesis de inducción. Por tanto,  $r = s$ . Así,  $P(k + 1)$  es cierto, de modo que  $P(n)$  es cierto para todas las  $n \in \mathbb{Z}^+$ .

**A7** Critíquese este razonamiento.

Mostremos que todo entero positivo tiene alguna propiedad interesante. Sea  $P(n)$  la afirmación de que  $n$  tiene una propiedad interesante. Usemos inducción completa.

Claro que  $P(1)$  es cierto, pues 1 es la identidad multiplicativa, lo cual ciertamente es una propiedad interesante del 1.

Supóngase que  $P(m)$  es cierto para  $1 \leq m \leq k$ . Si  $P(k + 1)$  no fuera cierto, entonces  $k + 1$  sería el menor entero sin una propiedad interesante, lo cual sería, por sí mismo, una propiedad interesante de  $k + 1$ . De modo que  $P(k + 1)$  debe ser cierto. Así,  $P(n)$  es cierto para todas las  $n \in \mathbb{Z}^+$ .

**A8** En realidad, nunca hemos podido encontrar una falla en a). El lector deberá probar su suerte y después responder b).

- a) Un asesino recibe la sentencia de ser ejecutado; pide al juez que no se le diga el día de la ejecución. El juez dice: «Lo sentencio a ser ejecutado a las 10 a.m. de algún día del próximo enero, pero le prometo que no se dará cuenta de que será ejecutado ese día, sino hasta que vayan por usted a las 8 a.m.» El criminal va a su celda y procede a demostrar que no puede ser ejecutado en enero, de la siguiente manera:

Sea  $P(n)$  la afirmación de que no puedo ser ejecutado en enero ( $31 - n$ ). Quiero probar  $P(n)$  para  $0 \leq n \leq 30$ . Ahora bien, no puedo ser ejecutado el 31 de enero, pues es el último día del mes y como seré ejecutado ese mes, sabría que ése es el día, antes de las 8 a.m., lo cual contradice la sentencia del juez. Así,  $P(0)$  es cierto. Supóngase que  $P(m)$  es cierto para  $0 \leq m \leq k$  donde  $k \leq 29$ . Esto es, supóngase que no puedo ser ejecutado de enero ( $31 - k$ ) a enero 31. Entonces, enero ( $31 - k - 1$ ) debe ser el último día posible para la ejecución y lo sabría antes de las 8 a.m., lo cual contradice la sentencia del juez. Así, no puedo ser ejecutado en enero ( $31 - (k + 1)$ ), de modo que  $P(k + 1)$  es cierto. Por tanto, no puedo ser ejecutado en enero.

(Por supuesto, el criminal fue ejecutado el 17 de enero.)

- b) Una profesora imparte una clase cinco días a la semana, de lunes a viernes. Le comunica a sus alumnos que hará un examen más, algún día de la última semana de clases, pero que los alumnos no sabrán si el examen será ese día, sino hasta llegar al aula. ¿Cuál es el último día de la semana en que puede hacer el examen, para satisfacer estas condiciones?

## BIBLIOGRAFIA

### OBRAS CLASICAS

1. Bourbaki, N., *Éléments de Mathématique*, libro II de la parte I, *Algèbre*, París, Hermann, 1942-58.
2. Jacobson, N., *Lectures in Abstract Algebra*; Princeton, Nueva Jersey, Van Nostrand, vols. I, 1951; II, 1953, y III, 1964.
3. Schreier, O., y Sperner, E., *Introduction to Modern Algebra and Matrix Theory* (versión inglesa), 2.<sup>a</sup> ed., Nueva York, Chelsea, 1959.
4. Van der Waerden, B. L., *Modern Algebra* (versión inglesa), Nueva York, Ungar, vols. I, 1949, y II, 1950.

### TEXTOS DE ALGEBRA GENERAL

5. Albert, A. A., *Fundamental Concepts of Higher Algebra*, Chicago, University of Chicago Press, 1956.
6. Birkhoff, G., y Mac Lane, S., *A Survey of Modern Algebra*, 3.<sup>a</sup> ed., Nueva York, Macmillan, 1965.
7. Dean, R. A., *Elements of Abstract Algebra*, Nueva York, Wiley, 1966.
8. Herstein, I. N., *Topics in Algebra*, Nueva York, Blaisdell, 1964.
9. Hungerford, T. W., *Algebra*, Nueva York, Holt, Rinehart and Winston, 1974.
10. Johnson, R. E., *University Algebra*; Englewood Cliffs, Nueva Jersey, Prentice-Hall, 1966.
11. Lang, S., *Algebra*; Reading, Massachusetts, Addison-Wesley, 1965.
12. McCoy, N. H., *Introduction to Modern Algebra*, Boston, Allyn and Bacon, 1960.
13. Mostow, G. D.; Sampson, J. H., y Meyer, J., *Fundamental Structures of Algebra*, Nueva York, McGraw-Hill, 1963.
14. Sawyer, W. W., *A Concrete Approach to Abstract Algebra*, San Francisco, Freeman, 1959.
15. Warner, S., *Modern Algebra*; Englewood Cliffs, Nueva Jersey, Prentice-Hall, vols. I y II, 1965.

## TEORIA DE GRUPOS

16. Burnside, W., *Theory of Groups of Finite Order*, 2.<sup>a</sup> ed., Nueva York, Dover, 1955.
17. Coxeter, H. S. M., y Moser, W. O., *Generators and Relations for Discrete Groups*, 2.<sup>a</sup> ed., Berlin, Springer, 1965.
18. Hall, M. J. (Jr.), *The Theory of Groups*, Nueva York, Macmillan, 1959.
19. Kurosh, A. G., *The Theory of Groups* (versión inglesa), Nueva York, Chelsea, vols. I, 1955, y II, 1956.
20. Ledermann, W., *Introduction to the Theory of Finite Groups*, 4.<sup>a</sup> ed., revisada, Nueva York, Interscience, 1961.
21. Thompson, J. G., y Feit, W., «Solvability of Groups of Odd Order», *Pac. J. Math.*, 13 (1963), 775-1029.
22. Rabin, M. A., «Recursive Unsolvability of Group Theoretic Problems», *Ann. Math.*, 67 (1958), 192-194.

## TEORIA DE ANILLOS

23. Artin, E.; Nesbitt, C. J., y Thrall, R. M., *Rings with Minimum Condition*, Ann Arbor, University of Michigan Press, 1944.
24. McCoy, N. H., *Rings and Ideals* (Carus Monograph, núm. 8), Búfalo, The Mathematical Association of America; LaSalle, Illinois, Open Court, 1948.
25. ———, *The Theory of Rings*, Nueva York, Macmillan, 1964.

## TEORIA DE CAMPOS

26. Artin, E., *Galois Theory* (Notre Dame Mathematical Lecture, núm. 2), 2.<sup>a</sup> ed., Notre Dame, Indiana, University of Notre Dame Press, 1944.
27. Zariski, O., y Samuel, P., *Commutative Algebra*; Princeton, Nueva Jersey, Van Nostrand, vol. I, 1958.

## TEORIA DE NUMEROS

28. Hardy, G. H., y Wright, E. M., *An Introduction to the Theory of Numbers*, 4.<sup>a</sup> ed., Oxford, Clarendon Press, 1960.
29. Lang, S., *Algebraic Numbers*; Reading, Massachusetts, Addison-Wesley, 1964.
30. LeVeque, W. J., *Elementary Theory of Numbers*; Reading, Massachusetts, Addison-Wesley, 1962.
31. ———, *Topics in Number Theory*; Reading, Massachusetts, Addison-Wesley, 2 vols., 1956.
32. Nagell, T., *Introduction to Number Theory*, Nueva York, Wiley, 1951.
33. Niven, I., y Zuckerman, H. S., *An Introduction to the Theory of Numbers*, Nueva York, Wiley, 1960.
34. Pollard, H., *The Theory of Algebraic Numbers* (Carus Monograph, núm. 9), Búfalo, The Mathematical Association of America, Nueva York, Wiley, 1950.
35. Shanks, D., *Solved and Unsolved Problems in Number Theory*, Washington, Spartan Books, vol. I, 1962.

## **456 BIBLIOGRAFIA**

36. Stewart, B. M., *Theory of Numbers*, 2.<sup>a</sup> ed. Nueva York, Macmillan, 1964.
37. Uspensky, J. V., y Heaslet, M. H., *Elementary Number Theory*, Nueva York, McGraw-Hill, 1939.
38. Weiss, E., *Algebraic Number Theory*, Nueva York, McGraw-Hill, 1963.

## **ALGEBRA HOMOLOGICA**

39. Jans, J. P., *Rings and Homology*, Nueva York, Holt, 1964.
40. Mac Lane, S., *Homology*, Berlin, Springer, 1963.

## **OTRAS REFERENCIAS**

41. Albert, A. A. (editor), *Studies in Modern Algebra* (MAA Studies in Mathematics, vol. 2), Búfalo, The Mathematical Association of America; Englewood Cliffs, Nueva Jersey, Prentice-Hall, 1963.
42. Artin, E., *Geometric Algebra*, Nueva York, Interscience, 1957.
43. Courant, R., y Robbins, R., *What Is Mathematics?*, Oxford, Oxford University Press, 1941.
44. Coxeter, H. S. M., *Introduction to Geometry*, Nueva York, Wiley, 1961.
45. Crowell, R. H., y Fox, R. H., *Introduction to Knot Theory*, Nueva York, Ginn, 1963.

# Respuestas y comentarios

## CAPITULO 0

- 0.1  $\{-\sqrt{3}, \sqrt{3}\}$
- 0.3  $\{1, -1, 2, -2, 3, -3, 4, -4, 5, -5, 6, -6, 10, -10, 12, -12, 15, -15, 20, -20, 30, -30, 60, -60\}$
- 0.5 No es conjunto (no está bien definido).
- 0.7 Conjunto  $\emptyset$ .
- 0.9 Conjunto  $\mathbb{Q}$ .
- 0.11 No es una relación de equivalencia.
- 0.13 Es una relación de equivalencia;  $\bar{0} = \{0\}$ ,  $\bar{a} = \{a, -a\}$  para cada  $a \in \mathbb{R}$  diferente de cero.
- 0.15 Es una relación de equivalencia;  $\bar{1} = \{1, 2, \dots, 9\}$ ,  $\bar{10} = \{10, 11, \dots, 99\}$ ,  $\bar{100} = \{100, 101, \dots, 999\}$ , y en general  $\bar{10^n} = \{10^n, 10^n + 1, \dots, 10^{n+1} - 1\}$ .
- 0.17 Es una relación de equivalencia;  
 $\bar{1} = \{1, 3, 5, 7, \dots\} = \{2(n - 1) + 1 \mid n \in \mathbb{Z}^+\}$ ,  
 $\bar{2} = \{2, 4, 6, 8, \dots\} = \{2n \mid n \in \mathbb{Z}^+\}$ .
- 0.19 (No queremos estropear su diversión.)
- 0.21 2
- 0.23 15

## CAPITULO 1

- 1.1 a)  $e, b, a$ . b)  $a, a$ . No se puede decir. c)  $a, c \cdot *$  no es asociativa.  
d) No,  $b * e \neq e * b$ .

1.3  $d, c, c, d$ 

1.7 F V F F F V V V V F

1.9 1. 16. 19 683.  $n^{(n^2)}$ 

- 1.11 a) Dos operaciones binarias  $*$  y  $\circ$  en el mismo conjunto  $S$  dan **estructuras algebraicas del mismo tipo** si cada  $x \in S$  tiene una contraparte  $x' \in S$  tal que la correspondencia  $x \leftrightarrow x'$  es uno a uno y tal que  $(a * b)' = a' * b'$  para todas las  $a, b \in S$ . (Esto se puede expresar de otras maneras.)  
 b) 10

**CAPITULO 2**2.1 a) No, falla  $\mathcal{G}_3$ . b) No, falla  $\mathcal{G}_1$ . c) Sí. d) No, falla  $\mathcal{G}_3$  en  $a = 0$ . e) Sí. f) Sí.2.3 *Respuesta parcial:*  $(a * b' * c)' = c' * b * a'$ 

	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$e$	$e$
$b$	$b$	$e$	$e$

(Son posibles otras respuestas.)

2.9 c)  $-\frac{1}{3}$ **CAPITULO 3**

3.1 a) Sí. b) No. c) Sí. d) Sí. e) Sí. f) No.

3.3 a) 0,25, 50,  $-25$ ,  $-50$  b)  $1, \frac{1}{2}, 2, 4, \frac{1}{4}$   
c)  $1, \pi, \pi^2, 1/\pi, 1/\pi^2$ . (Son posibles otras respuestas.)

a)	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

b)  $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$  $\langle 3 \rangle = \{0, 3\}$  $\langle 1 \rangle = \langle 5 \rangle = \mathbf{Z}_6$ 

c) 1 y 5

3.7 V F V F F V F F V F

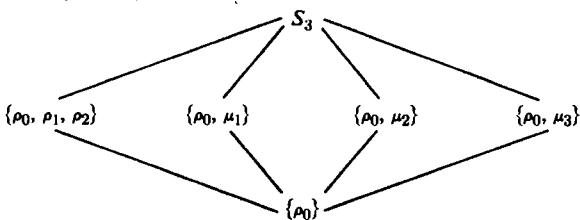
d) Un grupo  $\{e\}$  de un solo elemento sólo tiene un subgrupo (impropio).3.19 Un ejemplo es el 4-grupo  $V$  de Klein.

## CAPITULO 4

- 4.1    a)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$    b)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}$   
 c)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$    d)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 4 & 3 \end{pmatrix}$    e)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$

- 4.3    a)  $\langle \rho_1 \rangle = \langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$   
 $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$

b)



- 4.7     $S_3$  es un ejemplo. Véase el ejercicio 4.3b).

- 4.9     $|D_n| = 2n$

- 4.13    a) Sí.   b) No (no es cerrado).   c) No (no hay inverso).   d) Sí.

## CAPITULO 5

- 5.1    a)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 3 & 7 & 1 & 6 & 8 & 2 \end{pmatrix}$    b)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 2 & 8 & 5 & 4 & 1 & 6 \end{pmatrix}$   
 c)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 3 & 2 & 7 & 6 & 1 & 4 \end{pmatrix}$
- 5.5    a) 4   b) Un ciclo de longitud  $n$  tiene orden  $n$ .  
 c)  $\sigma$  tiene orden 6,  $\tau$  tiene orden 4.   d) (a) 6 (b) 6 (c) 8  
 e) El orden de una permutación expresada como un producto de ciclos ajenos es el mínimo común múltiplo de las longitudes de los ciclos.

## CAPITULO 6

- 6.1    2, 4, 4, 16

- 6.3    a) 6   b) 7   c) 4   d) 8   e) Un número infinito de elementos.

- 6.5     $Z_6$ : 1, 2, 3, 6

- $Z_8$ : 1, 2, 4, 8

- $Z_{12}$ : 1, 2, 3, 4, 6, 12

- $Z_{60}$ : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

- $Z_{17}$ : 1, 17

- 6.7     $S_3$  da un contraejemplo.

- 6.9    Considérese  $(xax^{-1})^2$ .

- 6.11     $(p - 1)(q - 1)$

## CAPITULO 7

- 7.1** 1)  $\mathbb{Z}_4$  es cíclico mientras que  $V$  no lo es.  
 2)  $\mathbb{Z}_4$  tiene sólo dos elementos que son solución de  $x + x = 0$ , mientras que  $V$  tiene cuatro soluciones a la ecuación correspondiente  $x^2 = e$ .
- 7.5** V V F V F V V V F V
- 7.15** *Respuesta parcial:*  $a\psi = a - 1$

## CAPITULO 8

8.1	Elemento	Orden	Elemento	Orden	
	(0, 0)	1		(0, 2)	2
	(1, 0)	2		(1, 2)	2
	(0, 1)	4		(0, 3)	4
	(1, 1)	4		(1, 3)	4

El grupo no es cíclico.

- 8.5**  $\mathbb{Z}_{20} \times \mathbb{Z}_3, \mathbb{Z}_{15} \times \mathbb{Z}_4, \mathbb{Z}_{12} \times \mathbb{Z}_5, \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_4$
- 8.7** V V F V F F F F F V
- 8.9** *Respuesta parcial:* Hay siete de ellos.
- 8.13**  $S_3$
- 8.15** Si un grupo  $G$  es el producto directo interno de subgrupos abelianos, entonces  $G$  es abeliano.
- 8.19**  $HK = \{\rho_0, \rho_2, \mu_1, \mu_2\}; H \vee K = S_3$

## CAPITULO 9

- 9.1** Para 720:  $\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{720},$   
 $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{360},$   
 $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_4 \times \mathbb{Z}_{180},$   
 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{180},$   
 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90},$   
 $\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{240},$   
 $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_6 \times \mathbb{Z}_{120},$   
 $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{12} \times \mathbb{Z}_{60},$   
 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{60},$   
 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30},$
- Para 1089:  $\mathbb{Z}_9 \times \mathbb{Z}_{121} \simeq \mathbb{Z}_{1089},$   
 $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{121} \simeq \mathbb{Z}_3 \times \mathbb{Z}_{363},$   
 $\mathbb{Z}_9 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \simeq \mathbb{Z}_{11} \times \mathbb{Z}_{99},$   
 $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \simeq \mathbb{Z}_{33} \times \mathbb{Z}_{33}$
- 9.3**  $\{2, 3\}$  genera  $\mathbb{Z}_{12}$ .  $\{4, 6\}$  genera  $\langle 2 \rangle$ .  $\{8, 6, 10\}$  genera  $\langle 2 \rangle$ .
- 9.7** Hay tres de orden 24. Hay dos de orden 25. Hay seis de orden (24)(25).
- 9.9** 49
- 9.13** Los números son los mismos.

**9.17** Un *subgrupo* de  $S_n$  no puede ser generado por dos elementos.

**9.19** c)  $\phi: G \rightarrow \mathbb{Z} \times \mathbb{Z}$  donde  $(a, b)\phi = \left(a, \frac{b-a}{10}\right)$ .

## CAPITULO 10

**10.5** *Respuesta parcial:* El grupo tiene orden 48.

**10.7** c) 432 d)  $|H| = 6$ ;  $H \cong S_3$

## CAPITULO 11

**11.1** a) 18 b) 8 c) 6

**11.3** *Respuesta parcial:* Las clases laterales izquierdas son

$$\begin{aligned} e &= (0, 0) + \langle(1, 2)\rangle = \{(0, 0), (1, 2)\}, \\ a &= (1, 0) + \langle(1, 2)\rangle = \{(1, 0), (0, 2)\}, \\ b &= (0, 1) + \langle(1, 2)\rangle = \{(0, 1), (1, 3)\}, \\ c &= (1, 1) + \langle(1, 2)\rangle = \{(1, 1), (0, 3)\}. \end{aligned}$$

La operación inducida en las clases laterales izquierdas está bien definida, y si forman grupo. Este grupo de clases laterales es isomorfo a  $\mathbb{Z}_4$ .

## CAPITULO 12

**12.1** a) Al trabajar con un grupo factor  $G/H$ ,  $a$  y  $b$  se harían elementos de  $G$ , no de  $G/H$ . Quizás el estudiante no entiende cómo se ven los elementos de  $G/H$  y no podrá escribir algo sensato acerca de ellos.

b) Debemos demostrar que  $G/H$  es abeliano. Sean  $aH$  y  $bH$  dos elementos de  $G/H$ .

**12.3** a) 3 b) 4 c) 8 d) 4 e) 6

**12.5** a)  $\mathbb{Z}$  b)  $\mathbb{Z}$  c)  $\mathbb{Z} \times \mathbb{Z}$

**12.7**  $\{\rho_0, \mu_1\}$ ,  $\{\rho_0, \mu_2\}$  y  $\{\rho_0, \mu_3\}$

**12.9** V V V V F V F V F

f)  $\mathbb{Z}$  es libre de torsión, pero  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ , un grupo de torsión.

h) Para  $n > 2$ ,  $S_n$  es no abeliano, pero  $S_n/A_n \cong \mathbb{Z}_2$ , y  $\mathbb{Z}_2$  es abeliano.

j)  $n\mathbb{R} = \mathbb{R}$ , de modo que  $\mathbb{R}/n\mathbb{R}$  es de orden 1.

**12.23**  $G' = \{\rho_0, \rho_2\}$

## CAPITULO 13

**13.1** a) Sí. (Imagen  $\phi$ ) =  $\mathbb{Z}$ . (Kernel  $\phi$ ) =  $\{0\}$ .

b) No.  $2 = (\frac{3}{2})\phi + (\frac{3}{2})\phi \neq 3\phi = 3$ .

c) Sí. (Imagen  $\phi$ ) =  $\mathbb{R}^+$ . (Kernel  $\phi$ ) =  $\{1, -1\}$ .

d) Sí. (Imagen  $\phi$ ) =  $\mathbb{Z}_2$ . (Kernel  $\phi$ ) =  $\{0, 2, 4\}$ .

e) No. En  $\mathbb{Z}_2$ ,  $0 = 1 + 1 = 5\phi + 5\phi \neq (5 + 5)\phi = 1\phi = 1$ .

**13.3** 2 de  $\mathbb{Z}$  sobre  $\mathbb{Z}$ ; 2 de  $\mathbb{Z}$  en  $\mathbb{Z}_2$ ; 1 de  $\mathbb{Z}$  sobre  $\mathbb{Z}_2$ .

- 13.5** 0 de  $Z_{12}$  sobre  $Z_5$ ; 6 de  $Z_{12}$  en  $Z_6$ ; 2 de  $Z_{12}$  sobre  $Z_6$ ; 2 de  $Z_{12}$  en  $Z_{14}$ ; 4 de  $Z_{12}$  en  $Z_{16}$ .
- 13.7** V V F V F F V V V F
- e) Si  $\phi$  es un homomorfismo de  $G$ , entonces  $|G\phi| = |G|/|(\text{Kernel } \phi)|$ . f) Véase e).
- g) Una transformación de todo elemento de un grupo  $G$  sobre la identidad de cualquier grupo siempre es un homomorfismo.
- h) Véase g). i) Véase el ejercicio 13.6. j) Véase el ejemplo 13.1.
- 13.11** *Respuesta parcial:*  $(\text{Imagen } \phi) = \langle a \rangle$ .  $(\text{Kernel } \phi) = nZ$  para algún  $n \in \mathbb{Z}$  no negativo (incluyendo  $n = 0, 1$ ).
- 13.13** b) *Respuesta parcial:* Si  $r$  no es primo relativo con  $|G|$ ,  $(\text{kernel } \phi_r) \neq \{e\}$  y  $\phi_r$  no es una transformación sobre  $G$ . Así, para algún  $a \in G$ ,  $x^r = a$  no tiene solución. En el caso extremo de que  $|G|$  divida  $r$ ,  $x^r = a$  no tiene solución para ningún  $a \in G$ ,  $a \neq e$ .
- 13.15** *Respuesta parcial:*  $\phi$  es un isomorfismo si  $(\text{kernel } \phi) = \{e\}$ , esto es, si el centro de  $G$  es el grupo trivial  $\{e\}$ .

## CAPITULO 14

- 14.1** Los refinamientos  $\{0\} < 2940Z < 60Z < 20Z < 4Z < Z$  de  $\{0\} < 60Z < 20Z < Z$  y  $\{0\} < 2940Z < 980Z < 245Z < 49Z < Z$  de  $\{0\} < 245Z < 49Z < Z$  son isomorfos.
- 14.3** Todos son de la forma  $\{(0, 0)\} < H < Z_5 \times Z_5$ , donde  $H$  puede ser cualquiera de los subgrupos  $\langle(0, 1)\rangle$ ,  $\langle(1, 0)\rangle$ ,  $\langle(1, 1)\rangle$ ,  $\langle(1, 2)\rangle$ ,  $\langle(1, 3)\rangle$ , y  $\langle(1, 4)\rangle$  de  $Z_5 \times Z_5$ . Así, hay seis en total.
- 14.11**  $\{\rho_0\} \times Z_4$
- 14.13**  $\{\rho_0\} \times Z_4 \leq \{\rho_0\} \times Z_4 \leq \{\rho_0\} \times Z_4 \leq \dots$

## CAPITULO 15

- 15.3** b)  $G/L$
- 15.5** a)  $K = \{0, 3, 6, 9\}$   
 b)  $0 + K = \{0, 3, 6, 9\}$ ,  $1 + K = \{1, 4, 7, 10\}$ ,  $2 + K = \{2, 5, 8, 11\}$   
 c)  $(0 + K)\psi = 0$ ,  $(1 + K)\psi = 1$ ,  $(2 + K)\psi = 2$
- 15.7** a)  $HN = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$ ,  $H \cap N = \{0, 12\}$   
 b)  $0 + N = \{0, 6, 12, 18\}$ ,  $2 + N = \{2, 8, 14, 20\}$ ,  $4 + N = \{4, 10, 16, 22\}$   
 c)  $0 + (H \cap N) = \{0, 12\}$ ,  $4 + (H \cap N) = \{4, 16\}$ ,  $8 + (H \cap N) = \{18, 20\}$   
 d)  $(0 + N)\psi = 0 + (H \cap N)$ ,  $(2 + N)\psi = 8 + (H \cap N)$ ,  $(4 + N)\psi = 4 + (H \cap N)$
- 15.9** a)  $0 + H = \{0, 4, 8, 12, 16, 20\}$ ,  $1 + H = \{1, 5, 9, 13, 17, 21\}$ ,  
 $2 + H = \{2, 6, 10, 14, 18, 22\}$ ,  $3 + H = \{3, 7, 11, 15, 19, 23\}$   
 b)  $0 + K = \{0, 8, 16\}$ ,  $1 + K = \{1, 9, 17\}$ ,  $2 + K = \{2, 10, 18\}$ ,  $3 + K = \{3, 11, 19\}$ ,  
 $4 + K = \{4, 12, 20\}$ ,  $5 + K = \{5, 13, 21\}$ ,  $6 + K = \{6, 14, 22\}$ ,  $7 + K = \{7, 15, 23\}$   
 c)  $0 + K = \{0, 8, 16\}$ ,  $4 + K = \{4, 12, 20\}$

d)  $(0 + K) + (H/K) = H/K = \{0 + K, 4 + K\} = \{\{0, 8, 16\}, \{4, 12, 20\}\}$

$(1 + K) + (H/K) = \{1 + K, 5 + K\} = \{\{1, 9, 17\}, \{5, 13, 21\}\}$

$(2 + K) + (H/K) = \{2 + K, 6 + K\} = \{\{2, 10, 18\}, \{6, 14, 22\}\}$

$(3 + K) + (H/K) = \{3 + K, 7 + K\} = \{\{3, 11, 19\}, \{7, 15, 23\}\}$

e)  $(0 + H)\psi = (0 + K) + (H/K), (1 + H)\psi = (1 + K) + (H/K),$

$(2 + H)\psi = (2 + K) + (H/K), (3 + H)\psi = (3 + K) + (H/K)$

**15.11 Cadena (3)**

$$\begin{aligned} \{0\} &\leq \{0\} \leq \langle 12 \rangle \\ &\leq \langle 6 \rangle \leq \langle 3 \rangle \\ &\leq \langle 3 \rangle \leq \mathbf{Z}_{36} \end{aligned}$$

**Cadena (4)**

$$\begin{aligned} \{0\} &\leq \{0\} \leq \langle 18 \rangle \leq \langle 18 \rangle \\ &\leq \langle 6 \rangle \leq \langle 3 \rangle \leq \mathbf{Z}_{36} \end{aligned}$$

**Isomorfismos**

$$\begin{aligned} \{0\}/\{0\} &\simeq \{0\}/\{0\} \simeq \{0\} \\ \langle 12 \rangle/\langle 0 \rangle &\simeq \langle 6 \rangle/\langle 18 \rangle \simeq \mathbf{Z}_3 \\ \langle 6 \rangle/\langle 12 \rangle &\simeq \langle 18 \rangle/\langle 0 \rangle \simeq \mathbf{Z}_2 \\ \langle 3 \rangle/\langle 6 \rangle &\simeq \langle 3 \rangle/\langle 6 \rangle \simeq \mathbf{Z}_2 \\ \langle 3 \rangle/\langle 3 \rangle &\simeq \langle 18 \rangle/\langle 18 \rangle \simeq \{0\} \\ \mathbf{Z}_{36}/\langle 3 \rangle &\simeq \mathbf{Z}_{36}/\langle 3 \rangle \simeq \mathbf{Z}_3 \end{aligned}$$

## CAPITULO 16

**16.1**  $X_{\rho_0} = X, X_{\rho_1} = \{C\}, X_{\rho_2} = \{m_1, m_2, d_1, d_2, C\}, X_{\rho_3} = \{C\},$

$X_{s_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}, X_{s_2} = \{s_2, s_4, m_1, m_2, C, P_2, P_4\},$

$X_{d_1} = \{2, 4, d_1, d_2, C\}, X_{d_2} = \{1, 3, d_1, d_2, C\}$

**16.3**  $\{1, 2, 3, 4\}, \{s_1, s_2, s_3, s_4\}, \{m_1, m_2\}, \{d_1, d_2\}, \{C\}, \{P_1, P_2, P_3, P_4\}$

**16.5** Todo sub- $G$ -conjunto de un  $G$ -conjunto  $X$  consta de una unión de órbitas en  $X$  bajo  $G$ .

**16.7** a) No.

b)  $\{1, 2, 3, 4\}, \{s_1, s_2, s_3, s_4\}, \{P_1, P_2, P_3, P_4\}$

**16.11** b) El conjunto de puntos en el círculo con centro en el origen y que pasa por  $P$ .

c) El subgrupo cíclico  $\langle 2\pi \rangle$  de  $G = \mathbb{R}$ .

**16.15** a)  $K = g_0^{-1}Hg_0$

b) Conjetura:  $H$  y  $K$  deben ser subgrupos conjugados de  $G$ .

**16.17**  $X \quad Y \quad Z \quad$  Hay tres de ellos.

	a	a	b	a	b	c
0	a	a	b	a	b	c
1	a	b	a	b	c	a
2	a	a	b	c	a	b
3	a	b	a	a	b	c
4	a	a	b	b	c	a
5	a	b	a	c	a	b

**CAPITULO 17**

17.1 5

17.3 2

17.5 11 712

17.7 a) 45 b) 231

17.9 a) 90 b) 6426

**CAPITULO 18**

18.1 a) 3 b) 27 c) 1, 3 d) 1, 85, 1, 51

18.7 V V V F V F V V F F

18.9  $H = \{i, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), (1, 3), (2, 4), (1, 2)(3, 4), (1, 4)(2, 3)\}$ ,  
 $K = \{i, (1, 3, 2, 4), (1, 2)(3, 4), (1, 4, 2, 3), (1, 2), (3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ ,  
 $K = (2, 3)H(2, 3)$ **CAPITULO 19**

19.3 V V F V V V V V F F

e) Es cuestión de opinión.

i) Un grupo de orden 42 no puede tener ningún subgrupo de orden 8, pues 8 no divide a 42.

19.7 e)  $p(1) = 1$ .  $p(2) = 2$ .  $p(3) = 3$ .  $p(4) = 5$ .  $p(5) = 7$ .  $p(6) = 11$ .  $p(7) = 15$ 19.9  $120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$ , $720 = 1 + 15 + 45 + 40 + 15 + 120 + 90 + 40 + 90 + 144 + 120$ **CAPITULO 20**20.3 *Respuesta parcial:* Sí.20.5  $|ad - bc| = 1$ 

20.7 V V V V V F F V V F

**CAPITULO 21**21.1 a)  $a^2b^2a^3c^3b^{-2}, b^2c^{-3}a^{-3}b^{-2}a^{-2}$     b)  $a^{-1}b^3a^4c^6a^{-1}, ac^{-6}a^{-4}b^{-3}a$ 

21.3 a) 16 b) 36 c) 36

21.5 a) 16 b) 36 c) 18

21.9 a) *Respuesta parcial:* {1} es una base para  $\mathbb{Z}_4$ . c) Si.21.11 c) Un grupo blop en  $S$  es isomorfo al grupo libre  $F[S]$  en  $S$ .**CAPITULO 22**22.1  $(a : a^4 = 1), (a, b : a^4 = 1, b = a^2), (a, b, c : a = 1, b^4 = 1, c = 1)$ . (Son posibles otras respuestas.)

## 22.3 Grupo octal:

	1	$a$	$a^2$	$a^3$	$b$	$ab$	$a^2b$	$a^3b$
1	1	$a$	$a^2$	$a^3$	$b$	$ab$	$a^2b$	$a^3b$
$a$	$a$	$a^2$	$a^3$	1	$ab$	$a^2b$	$a^3b$	$b$
$a^2$	$a^2$	$a^3$	1	$a$	$a^2b$	$a^3b$	$b$	$ab$
$a^3$	$a^3$	1	$a$	$a^2$	$a^3b$	$b$	$ab$	$a^2b$
$b$	$b$	$a^3b$	$a^2b$	$ab$	1	$a^3$	$a^2$	$a$
$ab$	$ab$	$b$	$a^3b$	$a^2b$	$a$	1	$a^3$	$a^2$
$a^2b$	$a^2b$	$ab$	$b$	$a^3b$	$a^2$	$a$	1	$a^3$
$a^3b$	$a^3b$	$a^2b$	$ab$	$b$	$a^3$	$a^2$	$a$	1

Grupo de cuaterniones: la misma tabla que para el grupo octal, excepto que los dieciséis lugares en la esquina inferior derecha son

$a^2$	$a$	1	$a^3$
$a^3$	$a^2$	$a$	1
1	$a^3$	$a^2$	$a$
$a$	1	$a^3$	$a^2$

22.9  $Z_{21} \cdot (a, b : a^7 = 1, b^3 = 1, ba = a^2b)$

22.11  $Z_{12}, Z_2 \times Z_6$

$$A_4 \cong (a, b, c : a^2 = b^2 = c^3 = 1, ab = ba, ca = bc, cb = abc, cab = ac) \\ \cong (s, t : s^3 = 1, t^2 = 1, (st)^3 = 1)$$

$$D_6 \cong (a, b : a^6 = 1, b^2 = 1, ba = a^5b)$$

$$(a, b : a^3 = 1, b^4 = 1, ba = a^2b)$$

(Véase Dean [7, pág. 246] para una solución completa.)

## CAPITULO 23

23.1 a) Sí. b) No.  $Z^+$  no tiene identidad para la suma. c) Sí. d) Sí. e) Sí. f) Sí.  
g) No. La multiplicación no es cerrada en  $\{ri \mid r \in \mathbb{R}\}$ .

23.3 a) 1, -1 b) (1, 1), (1, -1), (-1, 1), (-1, -1) c) 1, 2, 3, 4

d) Todas las  $q \in \mathbb{Q}$  distintas de cero.

e)  $(1, q, 1), (1, q, -1), (-1, q, 1), (-1, q, -1)$  para todas las  $q \in \mathbb{Q}$  distintas de cero.  
f) 1, 3

+	$\emptyset$	$\{a\}$	$\{b\}$	$S$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$S$
$\{a\}$	$\{a\}$	$\emptyset$	$S$	$\{b\}$
$\{b\}$	$\{b\}$	$S$	$\emptyset$	$\{a\}$
$S$	$S$	$\{b\}$	$\{a\}$	$\emptyset$

$\cdot$	$\emptyset$	$S$	$\{a\}$	$\{b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$S$	$\emptyset$	$S$	$\{a\}$	$\{b\}$
$\{a\}$	$\emptyset$	$\{a\}$	$\{a\}$	$\emptyset$
$\{b\}$	$\emptyset$	$\{b\}$	$\emptyset$	$\{b\}$

**CAPITULO 24**

**24.1** 0, 3, 5, 8, 9, 11

**24.3** a) 0 b) 0 c) 0 d) 3 e) 12 f) 30

**24.7** No hay soluciones de  $x^2 + 2x + 2 = 0$ . 2 es una solución de  $x^2 + 2x + 4 = 0$ .

**24.17**

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Es isomorfo a  $\langle \mathbf{Z}_2 \times \mathbf{Z}_2, + \rangle$ .

**24.19** 1

**CAPITULO 25**

**25.1**  $\begin{pmatrix} 7 & 13 \\ 6 & 2 \end{pmatrix}$  y  $\begin{pmatrix} -8 & 63 \\ 29 & 2 \end{pmatrix}$

**25.5** a)  $-6 + i + 13j + 2k$  b)  $j$  c)  $-\frac{1}{2}i - \frac{1}{2}j$  d)  $\frac{1}{50}j - \frac{3}{50}k$

**25.9**  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  y  $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$  son unidades en  $M_2(F)$ .

**25.13**  $1\rho_0 + 0\rho_1 + 1\rho_2 + 0\mu_1 + 1\mu_2 + 1\mu_3$

**25.15**  $\{a_1 + a_3j \mid a_1, a_3 \in \mathbf{R}\}$  y  $\{a_1 + a_4k \mid a_1, a_4 \in \mathbf{R}\}$

**CAPITULO 26**

**26.1**  $\{q_1 + q_2i \mid q_1, q_2 \in \mathbf{Q}\}$

**26.3**  $D = \mathbf{Q}$  y  $D' = \mathbf{Z}$  da un ejemplo.

**26.5** V F V F V V F V V V

**26.13** 4, pues 1 y 3 ya son unidades en  $\mathbf{Z}_4$ .

**26.15**  $\left\{ \frac{m}{6^n} \mid m \in \mathbf{Z}, n \in \mathbf{Z}^+ \right\}$

**CAPITULO 28**

**28.1**  $N_1 = \{0\}$ ,  $\mathbf{Z}_{12}/N_1 \cong \mathbf{Z}_{12}$ ;  
 $N_2 = \{0, 2, 4, 6, 8, 10\}$ ,  $\mathbf{Z}_{12}/N_2 \cong \mathbf{Z}_2$ ;  
 $N_3 = \{0, 3, 6, 9\}$ ,  $\mathbf{Z}_{12}/N_3 \cong \mathbf{Z}_3$ ;  
 $N_4 = \{0, 4, 8\}$ ,  $\mathbf{Z}_{12}/N_4 \cong \mathbf{Z}_4$ ;  
 $N_5 = \{0, 6\}$ ,  $\mathbf{Z}_{12}/N_5 \cong \mathbf{Z}_6$ ;  
 $N_6 = \mathbf{Z}_{12}$ ,  $\mathbf{Z}_{12}/N_6 \cong \{0\}$

**28.3**  $\{(n, n) \mid n \in \mathbf{Z}\}$ . (Otras respuestas son posibles.)

**28.5 F V F V V V V F F**

**28.15** *Respuesta parcial:* Por la definición en el ejercicio 28.15,  $\sqrt{R} = R$  para todo anillo  $R$ . Sin embargo, de acuerdo con la definición del ejercicio 28.11, el radical de  $R$  no siempre es todo  $R$ . Así, esta terminología es inconsistente si  $N = R$ .

**28.17** Si  $\sqrt{N}/N$  se considera como un subanillo de  $R/N$ , entonces es el radical de  $R/N$  en el sentido de la definición del ejercicio 28.11.

## CAPITULO 29

**29.1**  $\phi_1$  tal que  $1\phi_1 = 1$ .  $\phi_2$  tal que  $1\phi_2 = 0$ .

**29.3** Sea  $\phi: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  dado por  $n\phi = (n, 0)$  para  $n \in \mathbb{Z}$ .

**29.5**  $2\mathbb{Z} \times \mathbb{Z}$  es un ideal maximal de  $\mathbb{Z} \times \mathbb{Z}$ .  $\mathbb{Z} \times \{0\}$  es un ideal primo que no es maximal.  $4\mathbb{Z} \times \{0\}$  es un ideal que no es primo.

**29.7** **V F V V V F V V F V**

d) Un campo no tiene ideales propios y un grupo simple no tiene subgrupos normales propios. En ambos casos todas las estructuras cocientes son triviales o bien isomorfas a la estructura original.

**29.15** No. Si se agrandara el dominio hasta un campo de cocientes, se tendría un campo que contendría dos campos primos diferentes  $\mathbb{Z}_p$  y  $\mathbb{Z}_q$ , lo cual es imposible.

## CAPITULO 30

**30.1**  $f(x) + g(x) = 3x^4 + 2x^3 + 4x^2 + 1$ ,  
 $f(x)g(x) = x^7 + 2x^6 + 4x^5 + x^3 + 2x^2 + x + 3$

**30.3** a) 0 b) 2 c) 2 d) -1

**30.5**  $0, 4 = -1$

**30.7** **V V V V F F V V F V**

f) En  $\mathbb{Z}_6[x]$ ,  $(2x^3)(3x^4) = 0$ .

**30.9** b)  $F$  c)  $F[x]$

**30.11** 0, 1, 2, 3

**30.13** a) Sea  $F$  un subcampo de un campo  $E$ , sean  $x_1, \dots, x_n$  elementos cualesquiera de  $E$  y sean  $x_1, \dots, x_n$  indeterminadas. La transformación  $\phi_{x_1, \dots, x_n}: F[x_1, \dots, x_n] \rightarrow E$  definida por

$$\left(\sum a_{m_1, \dots, m_n} x_1^{m_1} \cdots x_n^{m_n}\right) \phi_{x_1, \dots, x_n} = \sum a_{m_1, \dots, m_n} x_1^{m_1} \cdots x_n^{m_n}$$

para

$$\left(\sum a_{m_1, \dots, m_n} x_1^{m_1} \cdots x_n^{m_n}\right) \in F[x_1, \dots, x_n]$$

es un homomorfismo de  $F[x_1, \dots, x_n]$  en  $E$ . Además,  $x_i \phi_{x_1, \dots, x_n} = x_i$ , y  $\phi_{x_1, \dots, x_n}$  transforma  $F$  isomórficamente, mediante la transformación identidad.  $\phi_{x_1, \dots, x_n}$  es un homomorfismo de evaluación.

b) 558

c) Sea  $F$  un subcampo de un campo  $E$ . Entonces,  $(x_1, \dots, x_n) \in \underbrace{(E \times E \times \cdots \times E)}_{n \text{ factores}}$

es un cero de  $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ , si  $f(x_1, \dots, x_n) \phi_{x_1, \dots, x_n} = 0$ .

**CAPITULO 31**

- 31.1**  $q(x) = x^4 + x^3 + x^2 + x - 2, r(x) = 4x + 3$
- 31.3**  $(x - 1)(x + 1)(x - 2)(x + 2)$
- 31.5** *Respuesta parcial:*  $f(x)$  no es irreducible sobre **R** y no es irreducible sobre **C**.
- 31.9** V V V F V F V V V F
- 31.11** Sí. Es de grado 3 sin ceros en **Z**,  $2x^3 + x^2 + 2x + 2$ .
- 31.15** No.  $\langle x^2 - 5x + 6 \rangle$  no es un ideal maximal de **Q[x]** pues  $x^2 - 5x + 6 = (x - 3)(x - 2)$  no es irreducible sobre **Q**. Sí,  $\langle x^2 - 6x + 6 \rangle$  es un ideal maximal de **Q[x]**.

**CAPITULO 32**

- 32.1** a) Sí. b) Sí. c) No. d) Sí. e) No. f) Sí. g) Sí. h) Sí.
- 32.3** En **Z[x]**:  $(2)(2)(x^2 - x + 2)$ .  
En **Q[x]**:  $4x^2 - 4x + 8$ .  
En **Z<sub>11</sub>[x]**:  $(4x + 2)(x + 4)$ .
- 32.9** *Respuesta parcial:*  $D^* - U$  no es un grupo bajo la multiplicación, pues  $1 \notin (D^* - U)$ .
- 32.11** No toda no unidad  $\neq 0$  de **Z**  $\times$  **Z** tiene una factorización en irreducibles. Por ejemplo,  $(1, 0)$  no es unidad y toda factorización de  $(1, 0)$  tiene un factor de la forma  $(\pm 1, 0)$ , el cual no es irreducible, pues  $(\pm 1, 0) = (\pm 1, 0)(1, 50)$ . Los únicos irreducibles de **Z**  $\times$  **Z** son  $(\pm 1, p)$  y  $(q, \pm 1)$ , donde  $p$  y  $q$  son irreducibles en **Z**.
- 32.17** Z

**CAPITULO 33**

- 33.1** a) Sí. b) No. Se viola (1). c) No. Se viola (1).  
d) No. Se viola (2). e) Sí.
- 33.3**  $x^3 + 2x - 1$
- 33.5** a) Sí. **Z** es un DFU y se aplica el teorema 32.3. c) No.  
d) No. Por el teorema 33.1, **Z[x]** dominio euclidianoy implicaría **Z[x]** DIP, contradiciendo c).
- 33.7** V F V F V V V F V V
- 33.9**  $61 = 29(49\ 349) + (-92)(15\ 555)$
- 33.17** *Respuesta parcial:* La ecuación  $ax = b$  tiene una solución en **Z<sub>n</sub>** para  $a, b \in \mathbf{Z}_n$  distintos de cero, si y sólo si el mcd positivo de  $a$  y  $n$  en **Z** divide  $b$ .

**CAPITULO 34**

- 34.1** a)  $5 = (1 + 2i)(1 - 2i)$  b) 7 es irreducible en **Z[i]**.  
c)  $4 + 3i = (1 + 2i)(2 - i)$  d)  $6 - 7i = (1 - 2i)(4 + i)$
- 34.3**  $\sigma = 1 + i, \rho = 3i$

- 34.13** c) (i) orden 9, característica 3. (ii) orden 2, característica 2. (iii) orden 5, característica 5.

## CAPITULO 35

**35.1** a)  $x^2 - 2x + 1$  b)  $x^4 - 10x^2 + 1$  c)  $x^2 - 2x + 2$   
 d)  $x^6 - 3x^4 + 3x^2 - 3$  e)  $x^{10} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5$

- 35.3** a) Algebraico,  $\text{grad}(z, F) = 2$ . b) Algebraico,  $\text{grad}(z, F) = 2$ . c) Transcendente.  
 d) Algebraico,  $\text{grad}(z, F) = 1$ . e) Algebraico,  $\text{grad}(z, F) = 2$ . f) Transcendente.  
 g) Algebraico,  $\text{grad}(z, F) = 1$ . h) Algebraico,  $\text{grad}(z, F) = 3$ .

- 35.7** b)

+	0	1	2	$\alpha$	$2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	1	2	$\alpha$	$2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	$\alpha$	$2\alpha$
2	2	0	1	$2+\alpha$	$2+2\alpha$	$\alpha$	$2\alpha$	$1+\alpha$	$1+2\alpha$
$\alpha$	$\alpha$	$1+\alpha$	$2+\alpha$	$2\alpha$	0	$1+2\alpha$	$1$	$2+2\alpha$	2
$2\alpha$	$2\alpha$	$1+2\alpha$	$2+2\alpha$	0	$\alpha$	1	$1+\alpha$	2	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+\alpha$	$\alpha$	$1+2\alpha$	1	$2+2\alpha$	2	$2\alpha$	0
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	$2\alpha$	1	$1+\alpha$	2	$2+\alpha$	0	$\alpha$
$2+\alpha$	$2+\alpha$	$\alpha$	$1+\alpha$	$2+2\alpha$	2	$2\alpha$	0	$1+2\alpha$	1
$2+2\alpha$	$2+2\alpha$	$2\alpha$	$1+2\alpha$	2	$2+\alpha$	0	$\alpha$	1	$1+\alpha$

	0	1	2	$\alpha$	$2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\alpha$	$2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	$2\alpha$	$\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
$\alpha$	0	$\alpha$	$2\alpha$	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
$2\alpha$	0	$2\alpha$	$\alpha$	1	2	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	$2+\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$2\alpha$	2	1	$\alpha$
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	2	$\alpha$	$2\alpha$	1
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	1	$2\alpha$	$\alpha$	2
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$\alpha$	1	2	$2\alpha$

- 35.9** Es el polinomio mónico en  $F[x]$  de grado *minimal* que tiene como cero  $\alpha$ .

**CAPITULO 36**

- 36.1**  $\{(0, 1), (1, 0)\}, \{(1, 1), (-1, 1)\}, \{(2, 1), (2, -1)\}$ . (Son posibles otras respuestas.)
- 36.3**  $x^2 + x + 1$
- 36.7** a) Un subconjunto  $W$  de un espacio vectorial  $V$  sobre un campo  $F$  es un **subespacio de  $V$  sobre  $F$**  si las operaciones inducidas de suma vectorial y multiplicación por un escalar están cerradas en  $W$ , y  $W$  es un espacio vectorial sobre  $F$  bajo estas operaciones.
- 36.9** *Respuesta parcial:* La **suma directa**  $V_1 \oplus \cdots \oplus V_n$  de espacios vectoriales  $V_i$  es el conjunto  $V_1 \times \cdots \times V_n$  de vectores, junto con las operaciones de suma vectorial y multiplicación por un escalar, definidas por
- $$(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$$
- $$\text{y } a(\alpha_1, \dots, \alpha_n) = (a\alpha_1, \dots, a\alpha_n) \text{ para } \alpha_i, \beta_i \in V_i \text{ y } a \in F.$$
- 36.15** a) Un homomorfismo.  
 b) *Respuesta parcial:* el **kernel** (o **espacio nulo**) de  $\phi$  es  $\{\alpha \in V \mid \alpha\phi = 0\}$ .  
 c)  $\phi$  es un **isomorfismo** de  $V$  con  $V'$  si  $(\text{kernel } \phi) = \{0\}$  y  $\phi$  transforma a  $V$  sobre  $V'$ .

**CAPITULO 37**

- 37.1**  $\langle G, \mathcal{O}, *, \cdot \rangle$ . (Son posibles otras notaciones.)
- 37.3**  $\langle V, F, \oplus, \odot, +, \cdot, \times \rangle$ . (Son posibles otras notaciones.)
- 37.5**  $\mathbf{Z}_2 \times \{0\}$  no es un subgrupo característico de  $\langle \mathbf{Z}_2 \times \mathbf{Z}_2, + \rangle$ , pues existe un automorfismo de  $\mathbf{Z}_2 \times \mathbf{Z}_2$  que transforma a  $\mathbf{Z}_2 \times \{0\}$  sobre  $\{0\} \times \mathbf{Z}_2$ .
- 37.7** *Respuesta parcial:* una transformación  $\phi: G \rightarrow G'$  es un  **$\mathcal{O}$ -homomorfismo del  $\mathcal{O}$ -grupo  $G$  en el  $\mathcal{O}$ -grupo  $G'$**  si para todas las  $\alpha, \beta \in G$  y  $a \in \mathcal{O}$ , se tiene  $(\alpha + \beta)\phi = a\phi + \beta\phi$  y  $(\alpha a)\phi = (\alpha\phi)a$ .
- 37.11** Un **homomorfismo de un  $R$ -módulo (izquierdo)  $M$  en un  $R$ -módulo (izquierdo)  $M'$**  es una función  $\phi: M \rightarrow M'$  tal que  $(\alpha + \beta)\phi = \alpha\phi + \beta\phi$  y  $(r\alpha)\phi = r(\alpha\phi)$  para todas las  $\alpha, \beta \in M$  y  $r \in R$ .

**CAPITULO 38**

- 38.1** a)  $2, \{1, \sqrt{2}\}$   
 b)  $4, \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$   
 c)  $8, \{1, \sqrt{3}, \sqrt{5}, \sqrt{15}, \sqrt{2}, \sqrt{6}, \sqrt{10}, \sqrt{30}\}$   
 d)  $6, \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt[3]{3}, \sqrt[3]{2}\sqrt[3]{3}, (\sqrt[3]{2})^2(\sqrt[3]{3})\}$   
 e)  $6, \{1, \sqrt[3]{2}, \sqrt[3]{2}(\sqrt[3]{2}), (\sqrt[3]{2})^2, \sqrt[3]{2}(\sqrt[3]{2})^2\}$
- 38.2** a) 4   b) 2   c) 6   d) 9   e) 2   f) 2   g) 1   h) 2
- 38.3** e)  $\{1, \sqrt{2}\}$    f)  $\{1, \sqrt{2}\}$    g)  $\{1\}$    h)  $\{1, \sqrt{2}\}$

**38.7** V F V F F V F F F F

**38.9** *Respuesta parcial:* se obtienen extensiones de grado  $2^n$  para  $n \in \mathbb{Z}^+$ .

## CAPITULO 39

**39.5** V V V F V F V V V F

## CAPITULO 40

- 40.1** a)  $\sqrt{2}, -\sqrt{2}$  b)  $\sqrt{2}$  c)  $3 + \sqrt{2}, 3 - \sqrt{2}$   
d)  $\sqrt{2} - \sqrt{3}, \sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}$   
e)  $\sqrt{2} + i, \sqrt{2} - i, -\sqrt{2} + i, -\sqrt{2} - i$  f)  $\sqrt{2} + i, \sqrt{2} - i$   
g)  $\sqrt{1 + \sqrt{2}}, -\sqrt{1 + \sqrt{2}}, \sqrt{1 - \sqrt{2}}, -\sqrt{1 - \sqrt{2}}$   
h)  $\sqrt{1 + \sqrt{2}}, -\sqrt{1 + \sqrt{2}}$
- 40.3** a)  $3 - \sqrt{2}$  b) Son las mismas transformaciones.
- 40.5** a)  $\mathbf{Q}(\sqrt{2}, \sqrt{5})$  b)  $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  c)  $\mathbf{Q}(\sqrt{5})$  d)  $\mathbf{Q}(\sqrt{3}, \sqrt{10})$   
e)  $\mathbf{Q}(\sqrt{6}, \sqrt{10})$  f)  $\mathbf{Q}$
- 40.7** F F V V F V V V V V
- 40.9**  $0\sigma_2 = 0$ ,  $1\sigma_2 = 1$ ,  $\alpha\sigma_2 = 1 + \alpha$ ,  $(1 + \alpha)\sigma_2 = \alpha$ .  $\mathbf{Z}_2(\alpha)_{(\sigma_2)} = \mathbf{Z}_2$
- 40.11** Sea  $F = \mathbf{Z}_p(x)$  donde  $x$  es una indeterminada. Entonces, la imagen de  $F$  bajo  $\sigma_p$  es  $\mathbf{Z}_p(x^p)$ , un subcampo propio de  $\mathbf{Z}_p(x)$ . Mientras  $\sigma_p$  es una transformación isomorfa para todos los campos  $E$  de característica  $p$ ,  $\sigma_p$  no necesariamente es sobre  $E$ , de modo que no necesariamente es un automorfismo.
- 40.17** Todo automorfismo de  $F(x)$  transforma  $x$  sobre algún  $y = (ax + b)/(cx + d)$ , donde  $a, b, c, d \in F$  y  $ad - bc \neq 0$ . En forma reciproca, cada una de dichas  $y \in F(x)$  da lugar a un automorfismo de  $F(x)$  que transforma  $x$  sobre  $y$  y deja fijo  $F$ .

## CAPITULO 41

- 41.1** a) La transformación idéntica de  $E$  en  $\mathbf{Q}$ .  
τ dada por  $\sqrt{2}\tau = \sqrt{2}, \sqrt{3}\tau = -\sqrt{3}, \sqrt{5}\tau = -\sqrt{5}$ .  
b)  $\tau_1$  dada por  $\sqrt{2}\tau_1 = \sqrt{2}, \sqrt{3}\tau_1 = \sqrt{3}, \sqrt{5}\tau_1 = -\sqrt{5}$ .  
τ<sub>2</sub> dada por  $\sqrt{2}\tau_2 = \sqrt{2}, \sqrt{3}\tau_2 = -\sqrt{3}, \sqrt{5}\tau_2 = \sqrt{5}$ .  
c)  $\tau_1$  dada por  $\sqrt{2}\tau_1 = \sqrt{2}, \sqrt{3}\tau_1 = \sqrt{3}, \sqrt{5}\tau_1 = -\sqrt{5}$ .  
τ<sub>2</sub> dada por  $\sqrt{2}\tau_2 = \sqrt{2}, \sqrt{3}\tau_2 = -\sqrt{3}, \sqrt{5}\tau_2 = \sqrt{5}$ .  
τ<sub>3</sub> dada por  $\sqrt{2}\tau_3 = -\sqrt{2}, \sqrt{3}\tau_3 = \sqrt{3}, \sqrt{5}\tau_3 = \sqrt{5}$ .  
τ<sub>4</sub> dada por  $\sqrt{2}\tau_4 = -\sqrt{2}, \sqrt{3}\tau_4 = -\sqrt{3}, \sqrt{5}\tau_4 = -\sqrt{5}$ .
- 41.3** a)  $\mathbf{Q}(\pi^2)$  b)  $\tau_1$  dada por  $\sqrt{\pi}\tau_1 = i\sqrt{\pi}$ ;  $\tau_2$  dada por  $\sqrt{\pi}\tau_2 = -i\sqrt{\pi}$ .
- 41.5** F V F V F V V V V F  
c)  $\mathbf{Q}$  y  $\mathbf{Q}(\sqrt{2})$  no son isomorfos, pero tienen cerraduras algebraicas isomorfas.

**CAPITULO 42**

42.1 a) 2 b) 2 c) 4 d) 6 e) 2 f) 12

42.3 a) 1 b) 6 c) 2

42.7 Sean  $F = \mathbf{Q}$  y  $E = \mathbf{Q}(\sqrt{2})$ . Entonces

$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$$

tiene un cero en  $E$  pero no se descompone en  $E$ .**CAPITULO 43**43.1  $f(x) = x^4 - 4x^2 + 4 = (x^2 - 2)^2$ . Aquí,  $f(x)$  no es un polinomio irreducible. Todo factor irreducible de  $f(x)$  tiene sólo ceros de multiplicidad 1.

43.3 F V V F F V V V V V

43.15 Calcúlese un  $\text{mcd}$  de  $f(x)$  y  $f'(x)$  usando el algoritmo euclíadiano. Entonces,  $f(x)$  tiene un cero de multiplicidad  $> 1$  si y sólo si este  $\text{mcd}$  es de grado  $> 0$ .**CAPITULO 44**44.1  $\mathbf{Z}_3(y^3, z^9)$ 44.5  $\mathbf{Z}_3(y^4, z^4)$ **CAPITULO 45**45.1 a) 3, 5 b) 3, 10, 5, 11, 14, 7, 12, 6  
c) 5, 10, 20, 17, 11, 21, 19, 15, 7, 14

45.5 V F V F V F V V F V

45.9 b) Es irreducible.

**CAPITULO 46**

46.1 a) 8 b) 8 c) 8 d) 2 e) 4 f) 4 g) 2 h) 1

46.3 El orden es 3. Un generador del grupo es  $\sigma_9$ , donde  $\alpha\sigma_9 = \alpha^9$  para  $\alpha \in CG(729)$ .46.5 a) Sean  $\alpha_1 = \sqrt[3]{2}$ ,  $\alpha_2 = \frac{\sqrt[3]{2} - 1 + i\sqrt{3}}{2}$  y  $\alpha_3 = \frac{\sqrt[3]{2} - 1 - i\sqrt{3}}{2}$ .

Las transformaciones son

 $\rho_0$ , donde  $\rho_0$  es la transformación idéntica; $\rho_1$ , donde  $\alpha_1\rho_1 = \alpha_2$  y  $i\sqrt{3}\rho_1 = i\sqrt{3}$ ; $\rho_2$ , donde  $\alpha_1\rho_2 = \alpha_3$  y  $i\sqrt{3}\rho_2 = i\sqrt{3}$ ; $\mu_1$ , donde  $\alpha_1\mu_1 = \alpha_1$  y  $i\sqrt{3}\mu_1 = -i\sqrt{3}$ ; $\mu_2$ , donde  $\alpha_1\mu_2 = \alpha_3$  y  $i\sqrt{3}\mu_2 = -i\sqrt{3}$ ; $\mu_3$ , donde  $\alpha_1\mu_3 = \alpha_2$  y  $i\sqrt{3}\mu_3 = -i\sqrt{3}$ .

b)  $S_3$ . La notación en a) se escogió para que coincidiera con la notación para  $S_3$  en el ejemplo 4.1.

c)

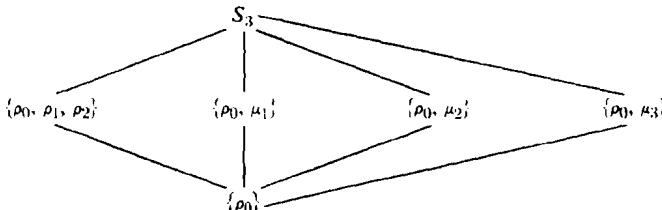


Diagrama reticular de grupos

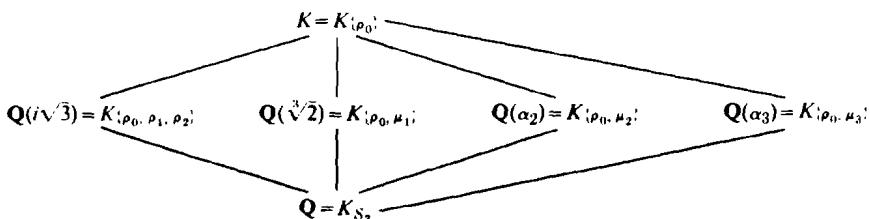


Diagrama reticular de campos

**46.7** F F V V V F F V F V

**46.9** a) 4 b) 1 c) 36 d) 16 e) 0 f) 0 g) 0 h) 8

**46.11** El campo de descomposición de  $(x^4 - 5x^2 + 6) \in \mathbb{Q}[x]$  es  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ , y el grupo es el del ejemplo 40.4.

**46.19**  $G(K/(E \cap L)) = G(K/E) \vee G(K/L)$

## CAPITULO 47

**47.3**  $\mathbb{Q}(\sqrt[4]{2}, i) : \sqrt[4]{2} + i, x^8 + 4x^6 + 2x^4 + 28x^2 + 1;$

$\mathbb{Q}(\sqrt[4]{2}) : \sqrt[4]{2}, x^4 - 2;$

$\mathbb{Q}(i\sqrt[4]{2}) : i\sqrt[4]{2}, x^4 - 2;$

$\mathbb{Q}(\sqrt{2}, i) : \sqrt{2} + i, x^4 - 2x^2 + 9;$

$\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) : \sqrt[4]{2} + i\sqrt[4]{2}, x^4 + 8;$

$\mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2}) : \sqrt[4]{2} - i\sqrt[4]{2}, x^4 + 8;$

$\mathbb{Q}(\sqrt{2}) : \sqrt{2}, x^2 - 2;$

$\mathbb{Q}(i) : i, x^2 + 1;$

$\mathbb{Q}(i\sqrt[4]{2}) : i\sqrt[4]{2}, x^2 + 2;$

$\mathbb{Q} : 1, x - 1$

**47.5** El grupo es cíclico de orden 5 y sus elementos son

$\zeta\sqrt[5]{2} \rightarrow$	$\sigma_1$	$\sigma_2$	$\sigma_3$	$\sigma_4$
$\zeta\sqrt[5]{2}$	$\zeta\sqrt[5]{2}$	$\zeta^2\sqrt[5]{2}$	$\zeta^3\sqrt[5]{2}$	$\zeta^4\sqrt[5]{2}$

dondere  $\sqrt[5]{2}$  es la raíz 5.<sup>a</sup> real de 2.

**47.7** El campo de descomposición de  $x^8 - 1$  sobre  $\mathbf{Q}$  es el mismo que el campo de descomposición de  $x^4 + 1$  sobre  $\mathbf{Q}$ , de modo que una descripción completa está contenida en el ejemplo 47.2. (Es la manera más fácil de resolver el problema.)

**47.9** a)  $s_1^2 - 2s_2$     b)  $s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2$

c) 
$$\frac{s_1s_2 - 3s_3}{s_3}$$

## CAPITULO 48

**48.3** a) 16    b) 400    c) 2160

**48.7** V V F V V F V V F V

**48.9** a) 4    b) *Respuesta parcial:*  $G(K/\mathbf{Q}) \simeq \langle \mathbf{Z}_2 \times \mathbf{Z}_2, + \rangle$ .

**48.11**  $\sqrt[3]{-1}$ ;  $\mathbf{Z}_3$  es el campo de descomposición.

## CAPITULO 49

**49.5** V V V F V F V F F V

i)  $x^3 - 2x$  sobre  $\mathbf{Q}$  es un contraejemplo.

## APENDICE

**A7** El concepto de «propiedad interesante» no se ha precisado; no está bien definido. Además, trabajamos en matemáticas con lógica de dos valores; una afirmación es verdadera o falsa, *pero no ambas cosas*. La afirmación de que no tener una propiedad interesante sería una propiedad interesante parece contradecir esta lógica bivalente. Estariamos diciendo que el entero tiene y no tiene una propiedad interesante.

# Notaciones

$\epsilon, a \in S$	pertenencia, 3
$\emptyset$	conjunto vacío, 2
$\notin, a \notin S$	no pertenencia, 3
$\{x   P(x)\}$	conjunto de todas las $x$ tales que $P(x)$ , 3
$\mathbb{Z}$	enteros, 3
	grupo aditivo de los enteros, 60
	anillo de los enteros, 209
$\mathbb{Z}^+$	enteros positivos, 3
$\mathbb{Q}$	números racionales, 3
	campo de los números racionales, 208
$\mathbb{Q}^+$	números racionales positivos, 3
$\mathbb{R}$	números reales, 3
	campo de los números reales, 208
$\mathbb{R}^+$	números reales positivos, 3
$\mathbb{C}$	números complejos, 3
	campo de los números complejos, 208
$\equiv, a \equiv b \pmod{n}$	congruencia, 7, 120
$\ast, a \ast b$	operación binaria, 11
$\langle G, \ast \rangle$	grupo, 19
$\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$	axiomas de grupo, 19
$e$	elemento identidad, 19
$a^{-1}, -a$	inverso de $a$ , 30
$ S $	orden de $S$ , 30
$B \subseteq A$	contención de conjuntos; inclusión, 30
$B \subset A$	subconjunto $B \neq A$ , 30
$H \leqslant G; K \leqslant L$	inclusión de subgrupos, 31; inclusión de subestructura, 212
$H < G; K < L$	subgrupo $H \neq G$ , 31; subestructura $K \neq L$ , 212
$\langle a \rangle$	subgrupo cíclico generado por $a$ , 34, 57
	ideal principal generado por $a$ , 285

$n\mathbf{Z}$	subgrupo de $\mathbf{Z}$ generado por $n$ , 34
$\phi(a), a\phi, a^\phi$	subanillo (ideal) de $\mathbf{Z}$ generado por $n$ , 212
$\phi: A \rightarrow B$	imagen de $a$ bajo $\phi$ , 38 39
$\phi\psi$	transformación de $A$ en $B$ , 38
$S_A$	función compuesta, 39
$S_i$	grupo de permutaciones de $A$ , 41
$S_n$	transformación identidad o idéntica, 42
$n!$	grupo simétrico de $n$ letras, 42
$D_n$	$n$ factorial, 42
$A_n$	$n$ -ésimo grupo diédrico, 43, 44
$\mathbf{Z}_n$	grupo alternante de $n$ letras, 54
	grupo cíclico $\{0, 1, \dots, n - 1\}$ bajo la suma módulo $n$ , 61
	grupo de clases residuales módulo $n$ , 120
	anillo $\{0, 1, \dots, n - 1\}$ bajo la suma y multiplicación módulo $n$ , 209
	anillo de clases residuales módulo $n$ , 253
$\text{mcd}$	máximo común divisor, 62, 307
$\simeq, G \simeq G'$	grupos isomorfos, 66
$S^*$	elementos de $S$ distintos de cero, 71
$\prod_{i=1}^n S_i$	producto cartesiano de conjunto, 78
$S_1 \times S_2 \times \dots \times S_n$	
$\prod_{i=1}^n G_i$	producto directo de grupos, 79
$\oplus_{i=1}^n G_i$	suma directa de grupos, 79
$\tilde{G}_i$	subgrupo natural de $\prod_{i=1}^n G_i$ , 82
$\bigcap_{i \in I} S_i$	intersección de conjuntos, 82
$S_1 \cap S_2 \cap \dots \cap S_n$	
$HK$	conjunto de productos, 83
$H \vee K$	ensamble de subgrupos, 84
$aH, a + H$	clase lateral izquierda, 108
$Ha, H + a$	clase lateral derecha, 108
$(G:H)$	índice de $H$ en $G$ , 113
$\varphi$	función $\varphi$ de Euler, 115, 221
$i_g$	conjugación por $g$ , 118
$G/N: R/N$	grupo factor, 120; anillo factor, 253
$G'$	subgrupo conmutador, 124
$\gamma$	transformación canónica de clases residuales, 131, 257
$\mathcal{I}_G$	conjunto de automorfismos internos de $G$ , 138
$Z(G)$	centro de $G$ , 144
$X_g$	subconjunto de elementos de $x$ que quedan fijos bajo $g$ , 157
$G_x$	subgrupo de isotropía de elementos de $G$ que dejan fija $x$ , 158
$xG$	órbita de $x$ bajo $G$ , 158
$G_Y$	subgrupo de $G$ que deja fijo cada elemento de $Y$ , 160
$X_G$	subconjunto de elementos de $X$ que quedan fijos bajo $G$ , 168
$N[H]$	normalizador de $H$ , 170

$F[A]$	grupo libre en $A$ , 192
$(x_j; r_i), (x_j; r_i = 1)$	presentación de grupo, 198
$\langle R, +, \cdot \rangle$	anillo, 208
$\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$	axiomas de anillo, 208
$n \cdot a$	$n$ sumandos de $a$ , 209
$R_1 \times R_2 \times \dots \times R_n$	producto directo de anillos, 212
$b/a$	cociente, 217
$(a_{ij})$	matriz, 224
$M_n(F)$	anillo de matrices de $n \times n$ sobre $F$ , 226
$\text{Hom}(A)$	anillo de endomorfismos de $A$ , 227
$R(G)$	anillo de grupo de $G$ sobre $R$ , 231
$F(G)$	álgebra de grupo de $G$ sobre $F$ , 231
$\mathcal{Q}$	cuaterniones, 232
$f(x)$	polinomios en $x$ , 267
$R[x]$	anillo de polinomios en $x$ sobre $R$ , 268
$R[x_1, \dots, x_n]$	anillo de polinomios en $x_1, \dots, x_n$ sobre $R$ , 269
$F(x)$	campo de funciones racionales en $x$ sobre $F$ , 270
$F(x_1, \dots, x_n)$	campo de funciones racionales en $x_1, \dots, x_n$ sobre $F$ , 270
$\phi_\alpha$	homomorfismo de evaluación, 270
$f(\alpha)$	imagen de $f(x)$ bajo $\phi_\alpha$ , 273
$a b$	$a$ divide a $b$ , 291
DFU	dominio de factorización única, 292
DIP	dominio de ideales principales, 292
$\bigcup_{i \in I} A_i$	unión de conjuntos, 293
CCA	condición de la cadena ascendente, 293
$v$	evaluación, 304
$\mathbb{Z}[i]$	anillo de enteros gaussianos, 312
$N(\alpha)$	norma de $\alpha$ , 312, 315
$\text{irr}(\alpha, F)$	polinomio irreducible mónico para $\alpha$ sobre $F$ , 324
$\text{grad}(\alpha, F)$	grado de $\alpha$ sobre $F$ , 324
$F(\alpha)$	extensión simple de $F$ por $\alpha$ , 325
$\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3, \mathcal{V}_4, \mathcal{V}_5$	axiomas de espacio vectorial, 331
$[E:F]$	grado de $E$ sobre $F$ , 348
$F(\alpha_1, \dots, \alpha_n)$	extensión de $F$ por $\alpha_1, \dots, \alpha_n$ , 351
$F_E$	cerradura algebraica de $F$ en $E$ , 353
$F$	cerradura algebraica de $F$ , 354
$\psi_{\alpha, \beta}$	isomorfismo básico, 368, 369
$E_{(\sigma_i)}$	campo fijo de $\{\sigma_i\}$ , 372
$G(E/F)$	grupo de $E$ sobre $F$ , 373
$\sigma_p$	automorfismo de Frobenius, 375
$\{E:F\}$	índice de $E$ sobre $F$ , 383
$\text{CG}(p^n)$	campo de Galois de orden $p^n$ , 409
$\Phi_n(x)$	$n$ -ésimo polinomio ciclotómico, 435



# Índice de materias

- Abel, N. H., 443
- acción de un grupo en un conjunto, 155
- acción fiel, 160
- agregación de elementos a un campo, 351
- alfabeto, 190
- álgebra, 345
  - asociativa, 345
  - constantes estructurales del, 347
  - de división, 346
  - de grupo, 231
  - teorema fundamental del, 357
- algebraicamente cerrado en un campo de extensión, 358
- algoritmo de la división
  - para  $F[x]$ , 277
  - para un dominio euclíadiano, 304
  - para  $Z$ , 58
- algoritmo euclíadiano, 308
- algoritmo(s)
  - de la división para  $F[x]$ , 277
  - de la división para  $Z$ , 58
  - euclíadiano, 308
  - general de la división, 304
- anillo(s), 208
  - booleano, 214
  - característica de un, 218
  - cociente, 253
  - conmutativo, 211
  - con unitario, 211
  - de clases residuales, 253
  - de división, 212, 234
  - de endomorfismos, 228
  - del grupo, 231
- de matrices, 226
- de polinomios, 268
- factor, 253
- homomorfismo de, 257
- isomorfismo de, 211
- isomorfos, 210
- producto directo de, 212
- radical de un, 255
- simple, 256
- aritmética
  - en dominios euclidianos, 305
  - teorema fundamental de la, 145, 296
- Artin, E., 249
- Aschbacher, M., 123
- asociados, 291
- automorfismo(s), 371
  - de Frobenius, 375
  - del campo, 371
  - del grupo, 76, 118
  - internos, 118
- axioma de selección, 354
- base
  - finita para ideales, 303
  - para un espacio vectorial, 335
  - para un grupo abeliano finitamente generado, 195
  - para un grupo abeliano libre, 182
- biyección, 40
- Bott, R. H., 346
- Bourbaki, N., 40, 195

- Burnside, W., 123, 176  
 teorema del conteo de, 163
- cadena, en un conjunto parcialmente ordenado, 355  
 campo(s), 212  
 algebraicamente cerrado, 353  
 automorfismo de, 371  
 cerradura algebraica de un, 353, 354  
 de cocientes, 242  
 de descomposición, 388  
 de extensión, 320  
 de funciones racionales, 270  
 de Galois, 409  
 fijo, 372  
 perfecto, 398  
 primos, 263  
 torre de, 320  
 canónica, 131  
 Cauchy, teorema de, 168  
 Cayley, teorema de, 72  
 celda, 4, 106  
 centro de un grupo, 138, 144  
 cero,  
   de un polinomio, 273  
   divisor de, 216  
   multiplicidad del, 394  
 cerradura  
   algebraica, 352, 354  
   separable, 407  
   totalmente inseparable, 407  
 ciclo(s), 49  
   ajenos, 50  
 clase(s)  
   conjugada, 175  
   conjugada de equivalencia, 6  
   conjugada residual, 7, 120  
   de equivalencia, 6  
   laterales, 108  
     derechas, 108  
     izquierdas, 108  
   residuales módulo  $N$ , 120, 253  
 cociente(s), 217  
   campo de, 242  
 codominio, 40  
 coeficientes de torsión, 91, 93  
 coeficientes de un polinomio, 268  
 colineación, 104  
 combinación lineal, 333  
 condición  
   de base finita, 303  
   de la cadena ascendente, 293, 303  
   de la cadena descendente, 303  
   del máximo, 303  
   del mínimo, 303  
 conector, 198  
 congruencia módulo  $H$ , 109  
 congruente módulo  $n$ , 7, 61, 120  
 conjugación en un grupo, 118  
 conjunto(s).  
   acción de grupo en un, 155  
   ajenos, 4  
   bien definido, 3  
   cerrado bajo una operación, 14, 20, 31  
    $G$ -, 155  
   intersección de, 82  
   partición de, 4  
   producto cartesiano de, 78  
   sub- $G$ -, 160  
   transformación de, 97  
   unión de, 293  
   vacío, 2  
 commensurables, distancias, 246  
 comutador, 124  
 consecuencia de conectores, 198  
 constantes estructurales, 347  
 contenido de un polinomio, 297  
 contracciones elementales, 190  
 cota superior, 355  
 Coxeter, H. S. M., 99  
 Crowell, R. H., 190  
 cuadratura del círculo, 364  
 cuaterniones, 232  
 cubo, grupo de movimientos rígidos de un, 46  
 dependencia lineal, 334  
 derivadas, 402  
 diagrama  
   comutativo, 76, 134  
   reticular, 32, 320  
 dimensión de un espacio vectorial, 337  
 discriminante de un polinomio, 434  
 división, 287, 291  
   sintética, 281  
 divisores de cero, 216  
 dominio  
   de factorización única, 292  
   de ideales principales, 292  
   de una transformación, 40  
   entero, 217  
   euclidianos, 304  
 duplicación del cubo, 364  
 ecuación de clase, 175  
 Eisenstein, criterio de, 284  
 elemento(s),  
   agregación de, 351  
   algebraico, 322

- conjugados sobre un campo, 368  
 conmutantes, 83  
 de un conjunto, 2  
 identidad, 19  
 independientes, 446  
 inverso, 19  
 maximal, 355  
 nilpotente, 214, 255  
*norma de un*, 316, 424  
 orden de un, 55, 81  
 primitivo, 400  
 que conmuta, 83  
 separable, 396  
 totalmente inseparable, 404  
 trascendentes, 322  
 endomorfismo, 227  
 ensamble, 84  
 entero  
     algebraico, 315, 434  
     gaussiano, 312  
     libre de cuadrado, 94  
     racional, 312  
 epimorfismo, 136  
 Erlanger, programa de, 97  
 escalar, 332  
 espacio topológico, 102  
 espacio vectorial, 331  
     base de un, 335  
     de dimensión finita, 334  
     dimensión de un, 337  
     generar un, 333  
 Euler, L., 221, 440  
     función  $\pi$  de, 115, 221  
     teorema de, 221  
 evaluación euclíadiana, 304  
 extensión(es),  
     abeliana, 423  
     algebraica, 348  
     cíclica, 424  
     ciclotómica, 435  
     de una transformación, 379  
     finita, 348  
     grado de una, 348  
     normal, 416  
     por radicales, 443  
     separable, 396, 402  
     simple, 325  
     totalmente inseparable, 404  
 factor, 291  
 Feit, W., 123, 176  
 Fermat, P., 440  
     primo de, 440  
     teorema pequeño de, 219  
 Fox, R. H., 190  
 Frobenius, G., 346  
     automorfismo de, 375  
 función(es), 38  
     automorfas, 103  
     codominio de, 40  
     compuesta, 39  
     dblemente periódicas, 103  
     dominio de, 40  
     elípticas, 103  
     fi de Euler, 115, 221  
     imagen bajo una, 38, 40  
     periódica, 102  
     polinomial, 276  
     racionales, 270  
     simétrica, 426  
     simétricas elementales, 427, 446  
     sobre, 39  
     uno a uno, 39  
 Galois,  
     campo de, 409  
     grupo de, 418  
     teorema principal de la teoría de, 418  
 Gauss, C. F., 297  
     lema de, 298  
 $G$ -conjunto(s), 155  
     isomorfos, 160  
     sub-, 160  
     transitivo, 159  
     unión ajena de, 161  
     unión de, 161  
 $G$ -conjunto transitivo, 159  
 generador(es),  
     de un grupo, 57, 89  
     de un grupo cíclico, 34, 57  
     en una presentación, 198  
     libres, 192  
 geometría, 97  
     afín, 104  
     euclíadiana, 97  
     proyectiva, 101  
 grado  
     de  $\alpha$  sobre  $F$ , 324  
     de una extensión, 348  
     de un polinomio, 268  
 Griess, R. L., 123  
 grupo(s), 19  
     abeliano, 21  
     abeliano finitamente generado, 92  
     base para un, 195  
     abeliano libre, 182, 194  
     base para un, 182  
     rango de un, 184  
     acción de un, 155  
     afín, 104

## 482 INDICE DE MATERIAS

- alternante, 54, 123
- automorfismo del, 76, 118
- automorfismo interno de, 118
- centro de un, 138, 144
- cíclico, 34, 57
- con descomposición, 93
- comutador de un, 124
- con operadores, 342
- de cuaterniones, 203, 234
- de Galois, 418
- del álgebra, 231
- del anillo, 231
- de torsión, 89
- de un campo de extensión, 373
- de un polinomio, 420
- diédrico, 44, 46
- factor, 120
- finitamente generado, 89
- generadores de, 57, 89
- homomorfismo de, 130
- isomorfismo de, 66
- isomorfos, 26, 66
- libre, 192
  - rango de un, 192
- libre de torsión, 89
- octal, 44, 219
- orden de un, 30
- $p$ -, 168
- presentación de un, 198
- propiedad estructural de un, 70
- simétrico, 42
- simple, 123
- sin descomposición, 93
- soluble, 143
- versión abelianizada de un, 124
- principal, 285
- propio, 254
- radical de un, 256
- trivial, 254
- idempotente, 27, 222
- identidad izquierda, 23
- imagen
  - bajo una transformación, 38, 40, 132
  - inversa, 132
- independencia lineal, 334
- indeterminada, 267
- índice
  - de una extensión de campo, 383
  - de un subgrupo, 113
- inducción,
  - axioma de, 450
  - matemática, 450
- intersección de conjuntos, 82
- inverso
  - izquierdo, 23
  - multiplicativo, 212
- inyección, 40
- irreducible en un dominio, 292
- isometría, 98
- isomorfismo(s),
  - básicos, 369
  - de anillos, 210
  - de  $G$ -conjuntos, 160
  - de grupos, 66
- primer teorema del, 146
- segundo teorema del, 147
- tercer teorema del, 148
- Jordan-Hölder, teorema de, 142, 150, 344
- kernel de un homomorfismo, 131, 258
- Klein, F., 97
- 4-grupo de, 31
- Kronecker, L., 321
- Lagrange, teorema de, 112
- lema de Gauss, 298
- lema de Zassenhaus, 150
- lema de Zorn, 354, 355, 380
- letra, 190
- ley distributiva, 208
- leyes de cancelación, 20
  - en un anillo, 216
  - en un grupo, 20
- matriz, 224
- máximo común divisor (mcd), 307
- McKay, J. H., 168

- medida  
 de Haar, 104  
 invariante derecha, 104  
 invariante izquierda, 104
- Milnor, J., 346
- mínimo común múltiplo (mcm), 311
- monomorfismo, 136
- multiplicación de permutaciones, 40
- multiplicación módulo  $n$ , 209
- multiplicidad del cero, 394
- módulo, 344  
 cíclico, 345  
 unitario, 344
- módulo  $n$ .  
 congruencia, 7, 61, 120  
 multiplicación, 209  
 suma, 61
- módulo  $N$ .  
 anillo cociente, 253  
 anillo de clases residuales, 253  
 anillo factor, 253  
 grupo factor, 120
- $n$ -ésima raíz primitiva del unitario, 410
- $n$ -gono regular construible, 441
- norma  
 de un elemento de campo, 424  
 de un entero gaussiano, 312  
 multiplicativa, 315
- normalizador, 170
- notación cíclica, 48
- número  
 algebraico, 323  
 complejo conjugado, 369  
 construible, 354  
 de betti, 91, 93  
 trascendente, 323
- objetivo fundamental, 248, 274, 320
- operación(es).  
 asociativa, 12  
 bien definida, 107  
 binaria, 11, 155  
 conmutativa, 12  
 inducida en las clases laterales, 107  
 inducida en un subconjunto, 31  
 tablas para, 13
- operadores, 342
- órbita, 47, 158
- orden  
 de un conjunto, 30  
 de un elemento, 55, 81  
 de un grupo, 30  
 parcial, 354
- $p$ -grupo, 167  
 $p$ -subgrupo, 168  
 $p$ -subgrupo de Sylow, 171
- palabra, 190  
 reducida, 190  
 vacía, 190
- particiones  
 de  $n$ , 180  
 de un conjunto, 4
- permutación(es).  
 impares, 53  
 pares, 53  
 signo de una, 137  
 transitiva, 47
- Pitágoras, 247
- pitagóricos, 246
- plano proyectivo, 101
- polinomio(s), 268  
 cero de un, 273  
 ciclotómico, 284, 436  
 coeficientes de, 268  
 con  $n$  indeterminadas, 269  
 constantes, 268  
 contenido de un, 297  
 derivada de un, 402  
 discriminante de un, 434  
 general, 427  
 grado de un, 268  
 grupo de, 420  
 irreducible, 281  
 para  $\alpha$  sobre  $F$ , 324
- minimal, 329  
 para  $\alpha$ , 329  
 móniaco, 324  
 primitivo, 297  
 que se descompone, 390  
 separable, 396
- presentación(es), 198  
 finita, 198  
 isomorfas, 198
- primo, 291, 295  
 de Fermat, 440  
 relativo, 62, 311
- problema de la palabra, 199
- producto cartesiano, 78
- producto directo de grupos  
 externo, 79  
 interno, 83, 125
- programa de Erlanger, 97
- propiedad estructural, 70
- proyección, 101
- Rabin, M., 199
- radical(es),  
 de un anillo, 255

de un ideal, 256  
 extensión por, 443  
 soluble por, 443  
 raíz del unitario, 410  
 $n$ -ésima primitiva, 410  
 rango  
     de un grupo abeliano libre, 184  
     de un grupo libre, 192  
 razón cruzada, 101  
 recta al infinito, 101  
 refinamiento de una serie, 140  
 reflexiones, 99, 111  
 relación  
     de equivalencia, 6  
     en una presentación, 198  
 representación regular,  
     derecha, 74  
     izquierda, 74  
 representante de la celda, 106  
 rotaciones, 98, 111

Schreier, teorema de, 141, 150

selección, axioma de, 354

semi campo, 212

semigrupo, 23

serie(s),

    central ascendente, 144

    de composición, 141

    invariantes, 139

    isomorfas, 140

    normales, 139

    principal, 141

    refinamiento de una, 140

    subinvariante, 139

    subnormal, 139

Shanks, D., 247

Shapiro, N., 355

sílaba, 190

signo de una permutación, 137

solubilidad por radicales, 443

subanillo, 212

    generado por  $a$ , 214

subcampo, 212

subconjunto, 30

    impropio, 31

    propio, 31

subestructura, 212

sub- $G$ -conjunto, 160

subgrupo(s), 31

    admissible, 343

    característico, 346

    conjugados, 119

    comutador, 124

    cíclico, 34, 57

    de torsión, 90

ensamble dc, 84

generado por  $a$ , 89

impropio, 31

índice de un, 113

invariante, 119

isotrópicos, 158

normal, 119

normalizador de un, 170

normal maximal, 135

$\mathbb{C}$ , 342

$P$ , 168

    de Sylow, 171

propio, 31

trivial, 31

suma directa

    de anillos, 212

    de grupos, 79

suma módulo  $n$ , 61

suprayección, 40

Sylow, teoremas de, 169-72

tablas

    de grupo, 23

    para una operación, 13

teorema(s)

    de Cauchy, 168

    de Cayley, 72

    de Euler, 221

    de Jordan-Hölder, 142, 150, 344

    de la extensión de isomorfismos, 380, 384

    de Schreier, 141, 150

    de Sylow, 169-72

    de Wedderburn, 234

    de Wilson, 222

    pequeño de Fermat, 220

    principal de la teoría de Galois, 418

teorema de factorización única

    en un dominio euclíadiano, 305

para  $D[x]$ , 300

para  $F[x]$ , 287

para un DIP, 296

para  $\mathbb{Z}$ , 296

teorema fundamental,

    de la aritmética, 145, 296

    del álgebra, 357

de los grupos abelianos finitamente generados, 92, 184

teoría de Galois, teorema principal de la, 418

Thompson, J. G., 123, 176

topología, 102

torre de campos, 320

transformación(es), 38

    biyectiva, 40

codominio de una, 40

compuesta, 39

- continua, 102
- de un conjunto, 97
- dominio de una, 40
- extensión de una, 379
- imagen bajo una, 38, 40, 132
- inversa de una, 47
- inyectiva, 40
- lineal, 340
- proyectiva, 101
- sobre, 39
- suprayectiva, 40
- uno a uno, 39
- transposición, 51
- trascendentes independientes, 446
- traslación, 98
  - derecha, 104
  - izquierda, 104
- traza, 424
- trisección del ángulo, 365
- unidad, 212, 291
- unión de conjuntos, 293
- unitario, 211
  - raíz del, 410
- vector(es), 332
  - linealmente dependientes, 334
  - linealmente independientes, 334
- versión abelianizada de un grupo, 124
- tiergruppe*, 31
- Wedderburn, teorema de, 234
- Wilson, teorema de, 222
- Zassenhaus, lema de, 150
- Zorn, lema de, 354, 355, 380