

# MATEMÁTICA DISCRETA

**Norman L. Biggs**

Profesor de Matemáticas.  
Escuela de Economía de Londres.  
Universidad de Londres.

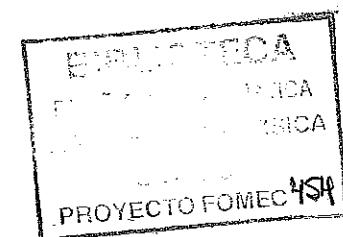
Traducido por:

**Marc Noy**

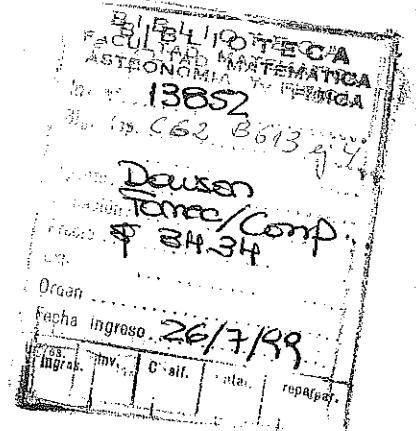
Doctor en Informática  
y profesor de Matemática Aplicada  
de la Universidad Politécnica de Cataluña.

Director de la Colección:

**Marc Noy**



**Vicens Vives**



A Cristina y Juliet

Primera edición, 1994  
Primera reimpresión, 1998

Originally published in English by Oxford University Press under the title:  
DISCRETE MATHEMATICS

© NORMAN L. BIGGS, 1985, 1989.  
© MARC NOY  
Sobre la versión en castellano  
© EDICIONES VIVES, S.A.  
Sobre la presente edición.

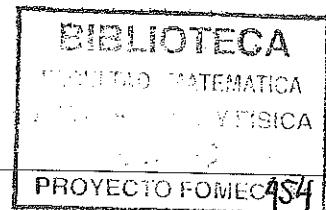
Obra protegida por la LEY 22/1987 de 11 de noviembre de Propiedad Intelectual. Los infractores de los derechos reconocidos a favor del titular o beneficiarios del © podrán ser demandados de acuerdo con los artículos 123 a 126 de dicha Ley y podrán ser sancionados con las penas señaladas en la Ley Orgánica 6/1987 por la que se modifica el artículo 534 del Código Penal. Prohibida la reproducción total o parcial por cualquier medio, incluidos los sistemas electrónicos de almacenaje, de reproducción, así como el tratamiento informático. Reservado a favor del Editor el derecho de préstamo público, alquiler o cualquier otra forma de cesión de uso de este ejemplar.

Depósito Legal: B. 41.625-1998  
ISBN: 84-316-3311-5  
Nº de Orden V.V.: J-700

IMPRESO EN ESPAÑA  
PRINTED IN SPAIN

Edited by EDICIONES VIVES, S.A. Avda. de Sarriá, 130. E-08017 Barcelona.  
Impreso por LIBERDUPLEX, S.L. Constitución, 19, bloque 8, núm. 19. E-08014 Barcelona.

## Prólogo



Este libro es el resultado de varios años de experiencia enseñando Matemática Discreta a los estudiantes de la Universidad de Londres. Cuándo empecé a enseñar la materia, existían pocos programas de interés y además muy dispares. Ahora tenemos muchos más, pero todavía no existe un acuerdo definitivo en cuanto a su forma y contenido. Espero que mi libro contribuya al desarrollo de un currículum coherente y completo. Pretende cubrir el material necesario para aquellos estudiantes que utilizan las matemáticas como una herramienta y, al mismo tiempo, proporcionar una base sólida para cursos avanzados de matemáticas especializadas.

Aunque los resultados del libro forman parte del conocimiento matemático común, el autor cree sinceramente que contiene algunos aspectos novedosos en su presentación. Como tales afirmaciones son muy poco convenientes, no abundaremos en ello y diremos solamente que la demostración del teorema 4.6 no es debida al autor, sino a David Bilington.

Estoy muy agradecido a todos aquellos que han leído y comentado partes del libro, especialmente a Lowell Beineke, Alan Boshier, Tony Gardiner, Gareth Jones, Keith Lloyd, Ann Penoyre, Fred Piper, John Shawe-Taylor, Anne Street, Art White y Douglas Woodall. La mayor parte del manuscrito fue mecanografiado, con gran cuidado y paciencia, por Marion Brooker.

Finalmente, debo agradecer a todos los estudiantes del Royal Holloway College que han asistido a mis clases y que han intentado, con un grado de éxito variable, resolver los ejercicios. Su trabajo ha contribuido enormemente a que este libro sea una realidad.

*Londres*  
Junio 1985

N.L.B.

# Índice

---

## PARTE I NÚMEROS Y ENUMERACIÓN

### 1. Enteros

1.1 Aritmética	3
1.2 Ordenación de los enteros	5
1.3 Definiciones recursivas	9
1.4 El principio de inducción	12
1.5 Cociente y resto	16
1.6 Divisibilidad	19
1.7 El máximo común divisor	20
1.8 Factorización en números primos	24
1.9 Ejercicios diversos	28

### 2. Funciones y enumeración

2.1 Funciones	31
2.2 Funciones exhaustivas, inyectivas y biyectivas	34
2.3 Contar	38
2.4 El principio de las cajas	42
2.5 ¿Finito o infinito?	44
2.6 Ejercicios diversos	48

### 3. Principios enumerativos

3.1 El principio de la adición	50
3.2 Contar conjuntos de pares	52
3.3 La función de Euler	56
3.4 Funciones, palabras y selecciones	59
3.5 Inyecciones como selecciones ordenadas sin repetición	61
3.6 Permutaciones	63
3.7 Ejercicios diversos	68

### 4. Subconjuntos y diseños

4.1 Números binomiales	70
------------------------	----

4.2 Selecciones no ordenadas con repetición	75
4.3 El teorema del binomio	77
4.4 El principio de la criba	80
4.5 Algunas aplicaciones aritméticas	84
4.6 Diseños	90
4.7 $t$ -diseños	94
4.8 Ejercicios diversos	98
<b>5. Particiones, clasificaciones y distribuciones</b>	
5.1 Particiones de un conjunto	101
5.2 Clasificación y relaciones de equivalencia	104
5.3 Distribuciones y números multinomiales	108
5.4 Particiones de un entero positivo	113
5.5 Clasificación de las permutaciones	115
5.6 Permutaciones pares e impares	118
5.7 Ejercicios diversos	125
<b>6. Aritmética modular</b>	
6.1 Congruencias	128
6.2 $\mathbb{Z}_m$ y su aritmética	131
6.3 Elementos invertibles de $\mathbb{Z}_m$	135
6.4 Construcciones cíclicas de diseños	138
6.5 Cuadrados latinos	143
6.6 Ejercicios diversos	147
<b>PARTE II GRAFOS Y ALGORITMOS</b>	
<b>7. Algoritmos y su eficiencia</b>	
7.1 ¿Qué es un algoritmo?	151
7.2 El lenguaje de los programas	153
7.3 Algoritmos y programas	158
7.4 Demostración de que un algoritmo es correcto	160
7.5 Eficiencia de los algoritmos	163
7.6 Órdenes de crecimiento: la notación $O$	167
7.7 Comparación de algoritmos	169
7.8 Introducción a los algoritmos de ordenación	172
7.9 Ejercicios diversos	176

<b>8. Grafos</b>	
8.1 Los grafos y su representación	178
8.2 Isomorfismo de grafos	181
8.3 Grados	184
8.4 Caminos y ciclos	186
8.5 Árboles	190
X8.6 Colorear los vértices de un grafo	193
X8.7 El algoritmo voraz para las vértice-coloraciones	195
8.8 Ejercicios diversos	200
<b>9. Árboles, ordenación y búsqueda</b>	
9.1 Contar las hojas de un árbol con raíz	203
9.2 Árboles y algoritmos de ordenación	208
9.3 Árboles generadores y el problema AGM	213
9.4 Búsqueda en profundidad	218
9.5 Búsqueda en anchura	222
9.6 El problema del camino más corto	225
9.7 Ejercicios diversos	228
<b>10. Grafos bipartidos y problemas de emparejamientos</b>	
10.1 Relaciones y grafos bipartidos	231
10.2 Arista-coloraciones de grafos	234
10.3 Arista-coloraciones y cuadrados latinos	237
10.4 Emparejamientos	242
10.5 Emparejamientos máximos	246
10.6 Transversales de familias de conjuntos finitos	250
10.7 Ejercicios diversos	252
<b>11. Digrafos, redes y flujos</b>	
11.1 Digrafos	255
11.2 Redes y caminos críticos	258
11.3 Flujos y cortes	262
11.4 El teorema del flujo máximo y el corte mínimo	265
11.5 El algoritmo de etiquetaje para flujos en redes	270
11.6 Ejercicios diversos	275

**12. Técnicas recursivas**

12.1 Generalidades sobre la recursividad	278
12.2 Recurrencias lineales	280
12.3 Bisección recursiva	283
12.4 Optimización recursiva	286
12.5 El marco de la programación dinámica	290
12.6 Ejemplos del método de la programación dinámica	293
12.7 Ejercicios diversos	297

**PARTE III MÉTODOS ALGEBRAICOS****13. Grupos**

13.1 Los axiomas de grupo	305
13.2 Ejemplos de grupos	307
13.3 Álgebra básica en grupos	310
13.4 El orden de un elemento en un grupo	313
13.5 Isomorfismo de grupos	316
13.6 Grupos cíclicos	317
13.7 Subgrupos	321
13.8 Clases laterales y el teorema de Lagrange	325
13.9 Caracterización de los grupos cíclicos	331
13.10 Ejercicios diversos	334

**14. Grupos de permutaciones**

14.1 Definiciones y ejemplos	338
14.2 Órbitas y estabilizadores	342
14.3 El tamaño de una órbita	345
14.4 El número de órbitas	348
14.5 Representación de grupos mediante permutaciones	353
14.6 Aplicaciones de la teoría de grupos	356
14.7 Ejercicios diversos	360

**15. Anillos, cuerpos y polinomios**

15.1 Anillos	362
15.2 Elementos inversibles de un anillo	364
15.3 Cuerpos	366

**15.4 Polinomios**

15.5 El algoritmo de división para polinomios	369
15.6 El algoritmo de Euclides para polinomios	372
15.7 Factorización teórica de polinomios	376
15.8 Factorización práctica de polinomios	379
15.9 Ejercicios diversos	380
	384

**16. Cuerpos finitos y aplicaciones**

16.1 Un cuerpo con nueve elementos	387
16.2 El orden de un cuerpo finito	389
16.3 Construcción de cuerpos finitos	392
16.4 El teorema del elemento primitivo	394
16.5 Cuerpos finitos y cuadrados latinos	399
16.6 Geometrías finitas y diseños	402
16.7 Planos proyectivos	406
16.8 Cuadrados en cuerpos finitos	410
16.9 Existencia de cuerpos finitos	414
16.10 Ejercicios diversos	419

**17. Códigos correctores de errores**

17.1 Palabras, códigos y errores	422
17.2 Códigos lineales	427
17.3 Construcción de códigos lineales	430
17.4 Corrección de errores en códigos lineales	433
17.5 Códigos cíclicos	437
17.6 Clasificación y propiedades de los códigos cíclicos	441
17.7 Ejercicios diversos	446

**18. Funciones generadoras**

18.1 Series de potencias y sus propiedades algebraicas	449
18.2 Fracciones simples	453
18.3 El teorema del binomio para exponentes negativos	459
18.4 Funciones generadoras	463
18.5 Recurrencias lineales homogéneas	466
18.6 Recurrencias lineales no homogéneas	471
18.7 Ejercicios diversos	474

<b>19. Particiones de un entero positivo</b>	
19.1 Particiones y diagramas	477
19.2 Particiones conjugadas	480
19.3 Particiones y funciones generadoras	482
19.4 Funciones generadoras de particiones restringidas	486
19.5 Una identidad misteriosa	489
19.6 El cálculo de $p(n)$	494
19.7 Ejercicios diversos	496
<b>20. Simetría y enumeración</b>	
20.1 El índice de ciclos de un grupo de permutaciones	499
20.2 Simetría cíclica y dieldral	502
20.3 Simetría en tres dimensiones	507
20.4 El número de coloraciones no equivalentes	511
20.5 Conjuntos de coloraciones y funciones generadoras	516
20.6 El teorema de Pólya	519
20.7 Ejercicios diversos	523
<b>Soluciones a ejercicios escogidos</b>	525
<b>Glosario</b>	541

## Parte I Números y enumeración

---

En la primera parte de este libro se estudian ideas simples pero fundamentales. Al aparecer con frecuencia en problemas de la vida cotidiana, muchos de los conceptos resultarán conocidos de un modo vago e intuitivo. El objetivo es proporcionar una base matemática sólida para analizar y resolver problemas más complicados que los habituales.

Los conocimientos que supondremos por parte del lector se cubren ampliamente con las matemáticas que se enseñan en la enseñanza secundaria a los jóvenes de entre 13 y 16 años. En particular, cierta habilidad con la aritmética y con la manipulación de expresiones algebraicas. También supondremos cierta familiaridad con el lenguaje y la notación de conjuntos aunque, para ser más completos, ofrecemos a continuación un breve repaso.

Un conjunto  $S$  puede describirse dando una lista de sus elementos, tal como

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

o indicando una propiedad que distinga sus elementos de los que no lo son; por ejemplo,

$$S = \{n \mid n \text{ es un número entero entre } 1 \text{ y } 9\}.$$

Esta última notación suele traducirse al lenguaje común en la forma “ $S$  es el conjunto de los  $n$  tales que  $n$  es un número entero entre 1 y 9”. Para el enunciado “ $x$  es un elemento de  $S$ ” utilizamos la notación  $x \in S$ .

Un conjunto  $B$  es un **subconjunto** de un conjunto  $A$  si todo elemento de  $B$  es un elemento de  $A$ ; se escribe  $A \subseteq B$ . Dados dos conjuntos  $X$  e  $Y$ , su **unión**  $X \cup Y$  es el conjunto cuyos elementos pertenecen a  $X$  o a  $Y$  (o a ambos) y su **intersección**  $X \cap Y$  es el conjunto cuyos elementos pertenecen a  $X$  y a  $Y$ . Un conjunto sin elementos se dice que es **vacío**

## 2 Números y enumeración

y se denota por  $\emptyset$ . Finalmente, la diferencia  $A \setminus B$  es el conjunto de los elementos de  $A$  que no son de  $B$ .

Cuando un estudiante se enfrenta por primera vez a las matemáticas de este nivel, confunde a menudo las relaciones lógicas entre los diversos enunciados que constituyen una demostración matemática. El flujo de una argumentación puede, en ocasiones, clarificarse mediante un uso prudente del símbolo  $\Rightarrow$ , que corresponde a la palabra "implica". Por ejemplo, los enunciados siguientes son correctos:

$$\begin{aligned}x = 2 &\Rightarrow x^2 = 4, \\x + 3 = 8 &\Rightarrow x = 5.\end{aligned}$$

El primero puede leerse " $x = 2$  implica  $x^2 = 4$ ", o bien "si  $x = 2$ , entonces  $x^2 = 4$ ". La dirección de la flecha deja bien claro que estas implicaciones son de un solo sentido y que, en general, no son reversibles. No podemos decir que si  $x^2 = 4$ , entonces  $x = 2$ , ya que existe la posibilidad alternativa de que  $x = -2$ . Cuando la implicación es válida en los dos sentidos, usamos el símbolo  $\iff$ , como en

$$x + 3 = 8 \iff x = 5.$$

Esto suele traducirse al lenguaje común como  $x + 3 = 8$  si, y sólo si,  $x = 5$ .

### Nota sobre los ejercicios

Antes de entrar en materia, unas palabras sobre el plan del libro. Cada apartado contiene unos cuantos ejercicios, pensados más para reforzar las ideas y técnicas discutidas, que para poner a prueba el ingenio del lector. Aconsejamos al estudiante que trabaje la mayor parte de los ejercicios antes de pasar al siguiente apartado. Al final de cada capítulo hay una selección de "ejercicios diversos". Algunos son de rutina, otros generalizaciones sencillas del material cubierto en el capítulo, y unos pocos introducen resultados importantes que debieran formar parte del compendio de conocimientos de todo matemático. De manera aproximada, los últimos ejercicios son los más difíciles.

## 1 Enteros

### 1.1 Aritmética

El lector de este libro estará familiarizado con los *enteros*. Encontramos los enteros positivos, o "números enteros"

$1, 2, 3, 4, 5$ , y así sucesivamente,

a una edad muy temprana. Más tarde se introduce el 0 (cero) y los números negativos

$-1, -2, -3, -4, -5$ , y así sucesivamente.

En matemáticas no solemos preocuparnos por las cuestiones lógicas y filosóficas acerca del sentido de estos objetos, pero sí necesitamos saber qué propiedades se les supone. Si hacemos todas las mismas suposiciones, todos llegaremos a los mismos resultados. Las suposiciones se conocen con el nombre de *axiomas*.

El punto de vista que se adopta en este libro es, a grandes rasgos, el que se acaba de exponer. Aceptamos sin discusión que existe un conjunto de objetos llamados *enteros*, que comprende el cero y los enteros positivos y negativos, y que nos es familiar a través de nuestra experiencia previa. El conjunto de los enteros se denota con el símbolo especial  $\mathbf{Z}$ . Las propiedades de  $\mathbf{Z}$  se dan como una lista de axiomas, de la que podremos deducir todos los resultados que necesitemos posteriormente sobre los enteros. Empezaremos con la lista de los axiomas relativos a las propiedades fundamentales de la suma y la multiplicación.

Adoptaremos las notaciones habituales:  $a + b$  para la suma de dos enteros  $a$  y  $b$ , y  $a \times b$  (o frecuentemente  $ab$ ) para su producto. Pensamos en  $+$  y  $\times$  como *operaciones* que, dados un par de enteros  $a$  y  $b$ , definen los enteros  $a + b$  y  $a \times b$ . Nuestra primera suposición (axioma I1) es el

hecho de que  $a + b$  y  $ab$  son a su vez enteros, y no un objeto cualquiera como, por ejemplo, un elefante. En la siguiente lista de axiomas,  $a$ ,  $b$  y  $c$  denotan enteros arbitrarios, y  $0$  y  $1$  denotan enteros específicos que tienen las propiedades enunciadas.

- I1.**  $a + b$  y  $ab$  son de  $\mathbf{Z}$ .
- I2.**  $a + b = b + a$ ;  $ab = ba$ .
- I3.**  $(a + b) + c = a + (b + c)$ ;  $(ab)c = a(bc)$ .
- I4.**  $a + 0 = a$ ;  $a1 = a$ .
- I5.**  $a(b + c) = ab + ac$ .
- I6.** Para cada  $a$  de  $\mathbf{Z}$  existe un único entero  $-a$  de  $\mathbf{Z}$  tal que  $a + (-a) = 0$ .
- I7.** Si  $a$  es distinto de  $0$  y  $ab = ac$ , entonces  $b = c$ .

Todos los axiomas corresponden a propiedades conocidas de los enteros que aprendemos mecánicamente en varias fases de nuestra educación matemática. La mayoría de las reglas aritméticas habituales pueden deducirse de ellos. Por ejemplo, podemos *definir* la operación de substracción diciendo que  $a - b$  es  $a + (-b)$ ; y podemos deducir reglas elementales de la substracción como la siguiente.

**Ejemplo.** Demostrar que para enteros  $m$  y  $n$  cualesquiera

$$m - (-n) = m + n.$$

**SOLUCIÓN:** Por la definición de substracción,  $m - (-n)$  es lo mismo que  $m + (-(-n))$ . Pero el axioma I6 nos dice que  $-(-n)$  es el único entero que sumado con  $-n$  da cero. Sin embargo, el propio  $n$  es un entero que lo cumple, ya que

$$\begin{aligned} (-n) + n &= n + (-n) && \text{(axioma I2)} \\ &= 0 && \text{(axioma I6)} \end{aligned}$$

Así pues,  $-(-n) = n$  y  $m - (-n) = m + n$ , como queríamos demostrar.  $\square$

En los ejercicios siguientes se encuentran resultados parecidos. No son particularmente excitantes, ya que no tenemos aún todos los axiomas

para los enteros, pero lo importante es recordar que pueden demostrarse utilizando únicamente los axiomas.

### Ejercicios 1.1

- 1 A continuación exponemos una demostración de la regla  $x0 = 0$  que sólo utiliza los axiomas enunciados hasta ahora. Desarrollar la demostración explicando qué axioma se utiliza en cada paso.

$$\begin{aligned} x(0 + 0) &= x0 \\ x0 + x0 &= x0 \\ -x0 + (x0 + x0) &= -x0 + x0 \\ (-x0 + x0) + x0 &= 0 \\ 0 + x0 &= 0 \\ x0 &= 0. \end{aligned}$$

2 Construir una demostración de la regla  $(a + b)c = ac + bc$  explicando cada paso como en el ejercicio 1.

3 Como de costumbre,  $x^2$  es  $xx$ . Demostrar que dados dos enteros cualesquiera  $a$  y  $b$ , existe un entero  $c$  tal que  $(a + b)c = a^2 - b^2$ .

4 Supóngase que hay dos enteros  $0$  y  $0'$  con la propiedad enunciada en el axioma I4, es decir,

$$a + 0 = a, \quad a + 0' = a$$

para cada  $a \in \mathbf{Z}$ . Demostrar que esto implica  $0 = 0'$ , con lo cual el axioma I4 caracteriza a  $0$  de forma única.

### 1.2 Ordenación de los enteros

El orden natural de los enteros es al menos tan importante como sus propiedades aritméticas. Desde pequeños aprendemos los números en el orden 1, 2, 3, 4, 5, y el hecho de que 4 es “mayor” que 3 se convierte pronto en algo importante.

La expresión formal de esta idea es que en  $\mathbf{Z}$  hay una *relación de orden*

$$m \leq n \quad (m, n \in \mathbf{Z})$$

que debe satisfacer ciertos axiomas. Resulta que son necesarios cinco axiomas para especificar las propiedades básicas del símbolo  $\leq$ ; los enunciamos a continuación siguiendo los números del apartado 1.1. Como antes,  $a, b$  y  $c$  denotarán enteros arbitrarios.

- I8.  $a \leq a$ .
- I9.  $a \leq b$  y  $b \leq a \Rightarrow a = b$ .
- I10.  $a \leq b$  y  $b \leq c \Rightarrow a \leq c$ .
- I11.  $a \leq b \Rightarrow a + c \leq b + c$ .
- I12.  $a \leq b$  y  $0 \leq c \Rightarrow ac \leq bc$ .

Apenas es necesario aprender estos axiomas, ya que contienen propiedades muy conocidas; lo importante es que nos permiten deducir otros hechos igualmente conocidos. Teniendo esto en cuenta, los ejercicios siguientes debieran resolverse utilizando sólo las propiedades contenidas en los axiomas I1-I12.

### Ejercicios 1.2

- 1 Supongámos que  $a \leq b$ . Añadiendo  $-a$  y  $-b$  a ambos lados de la desigualdad, demostrar que  $-b \leq -a$ . Deducir que si  $a \leq b$  y  $c \leq 0$ , entonces  $bc \leq ac$ .
- 2 Demostrar que  $0 \leq x^2$  para todo  $x$  de  $\mathbf{Z}$ , y deducir que  $0 \leq 1$ .
- 3 Deducir del ejercicio anterior que  $n \leq n + 1$  para todo  $n \in \mathbf{Z}$ .

Está claro que podemos definir los restantes símbolos de orden utilizados habitualmente,  $\geq$ ,  $<$  y  $>$ , en términos del símbolo  $\leq$ . Por ejemplo,  $m > n$  significa que  $n \leq m$  y  $m \neq n$ . Usaremos estos símbolos cuando resulte necesario.

Podría parecer que tenemos ya todas las propiedades de  $\mathbf{Z}$  que se necesitan en matemáticas, pero, sorprendentemente, falta un axioma vital.

Supongamos que  $X$  es un subconjunto de  $\mathbf{Z}$ ; decimos que el entero  $b$  es una **cota inferior** de  $X$  si

$$b \leq x \quad \text{para todo } x \in X.$$

Algunos conjuntos no tienen cotas inferiores: por ejemplo, está claro que el conjunto de los enteros negativos  $-1, -2, -3$ , etc., no las tiene. Por otra parte, el conjunto  $S$  formado por los números en negrita de la figura 1.1 tiene varias cotas inferiores. Una mirada rápida nos dice que  $-40$ , por ejemplo, es una cota inferior, mientras que una visión más detenida nos muestra que  $-27$  es la "mejor" cota inferior, ya que de hecho pertenece a  $S$ . En general, una cota inferior de un conjunto  $X$  que sea a su vez elemento de  $X$ , es un **mínimo** de  $X$ .

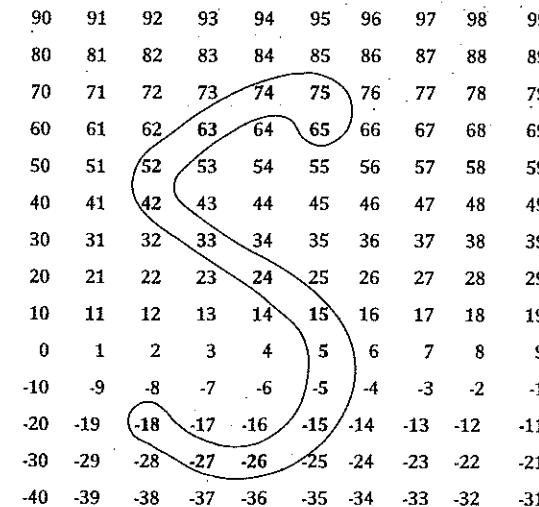


Fig. 1.1 El mínimo de  $S$  es  $-27$ .

Nuestro último axioma de  $\mathbf{Z}$  afirma lo que (en apariencia) es una propiedad evidente.

- I13. Si  $X$  es un subconjunto de  $\mathbf{Z}$  no vacío y tiene una cota inferior, entonces  $X$  tiene un mínimo.

El axioma I13 se conoce como el **axioma del buen orden**. Una manera de captar su significado es considerar un juego en el que dos personas eligen alternativamente un elemento de  $X$ , sujeto a la regla de que cada número debe ser estrictamente menor que el anterior. El axioma nos dice que, si exigimos que los números sean enteros, el juego ha de acabar; en efecto, el final llega en cuanto uno de los jugadores tiene el buen sentido de elegir el mínimo. Esta propiedad aparentemente evidente no se cumple necesariamente si permitimos números que no sean enteros, ya que  $X$  puede no tener un mínimo incluso si tiene una cota inferior. Por ejemplo, supongamos que  $X$  es el conjunto de las fracciones  $3/2, 4/3, 5/4$ , etcétera, que tienen  $(n+1)/n$  ( $n \geq 2$ ) por término general. Este conjunto tiene cotas inferiores (1, por ejemplo) pero no tiene mínimo, así que los jugadores pueden seguir jugando sin parar eligiendo fracciones cada vez más cercanas a 1.

El axioma del buen orden proporciona una justificación rigurosa de nuestra imagen intuitiva de los enteros como un conjunto de puntos regularmente espaciados en una recta que se extiende indefinidamente en las dos direcciones (fig. 1.2). En particular, nos dice que no podemos acercarnos más y más a un entero sin llegar finalmente a él, así que el dibujo de la fig. 1.3 es erróneo.

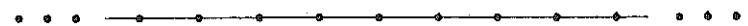


Fig. 1.2 El dibujo intuitivo correcto de  $\mathbb{Z}$ .



Fig. 1.3 Un dibujo incorrecto de  $\mathbb{Z}$ .

El hecho de que haya huecos entre los enteros nos lleva a decir que  $\mathbb{Z}$  es discreto, y es esta propiedad la que da nombre a la “matemática discreta”. En el cálculo y en el análisis, los procesos de paso al límite son fundamentales y es esencial usar sistemas de números que sean *continuos* en lugar de discretos.

### Ejercicios 1.2 (continuación)

4 En cada uno de los casos siguientes, dígase si el conjunto  $X$  tiene o no una cota inferior, y si tiene alguna, hállese su mínimo.

- (i)  $X = \{x \in \mathbb{Z} \mid x^2 \leq 16\}$ .
- (ii)  $X = \{x \in \mathbb{Z} \mid x = 2y \text{ para algún } y \in \mathbb{Z}\}$ .
- (iii)  $X = \{x \in \mathbb{Z} \mid x^2 \leq 100x\}$ .

5 Se dice que un subconjunto  $Y$  de  $\mathbb{Z}$  tiene una **cota superior**  $c$  si  $c \geq y$  para todo  $y \in Y$ . Una cota superior que a su vez pertenece a  $Y$  es un **máximo** de  $Y$ . Usar el axioma I13 para demostrar que si  $Y$  no es vacío y tiene una cota superior, entonces tiene un máximo. [Indicación: aplicar el axioma al conjunto cuyos elementos son  $-y$  ( $y \in Y$ ).]

6 Se ordenan los enteros  $n$  que satisfacen  $1 \leq n \leq 25$  en una tabla cuadrada de cinco filas y cinco columnas de forma arbitraria. Se selecciona el elemento máximo de cada fila; sea  $s$  el menor de estos. Igualmente, se selecciona el mínimo de cada columna y sea  $t$  el máximo de estos. Demostrar que  $s \geq t$  y dar un ejemplo en que  $s \neq t$ .

### 1.3 Definiciones recursivas

Sea  $\mathbb{N}$  el conjunto de los enteros positivos, es decir,

$$\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 1\},$$

y sea  $\mathbb{N}_0$  el conjunto  $\mathbb{N} \cup \{0\}$ , es decir,

$$\mathbb{N}_0 = \{n \in \mathbb{Z} \mid n \geq 0\}.$$

Todo subconjunto  $X$  de  $\mathbb{N}$  (o  $\mathbb{N}_0$ ) posee automáticamente una cota inferior, ya que todo elemento  $x$  de  $X$  satisface  $x \geq 1$  (o  $x \geq 0$ ). En este caso, el axioma del buen orden toma la forma

*si  $X$  es un subconjunto no vacío de  $\mathbb{N}$  o  $\mathbb{N}_0$   
entonces  $X$  tiene un mínimo.*

Ésta es la forma más utilizada en la práctica.

Nuestro primer uso del axioma del buen orden será la justificación de un procedimiento muy usual. Con frecuencia encontramos una expresión de la forma  $u_n$ , donde  $n$  indica un entero positivo cualquiera: por ejemplo, podría ser  $u_n = 3n + 2$ , o  $u_n = (n+1)(n+2)(n+3)$ . En estos ejemplos,  $u_n$  viene dado por una fórmula explícita y no hay dificultad en calcularlo para un valor específico de  $n$ . Sin embargo, en muchos casos no conocemos una fórmula para  $u_n$ ; de hecho, nuestro problema puede ser precisamente hallar una fórmula. En tales casos podemos disponer de algunos valores de  $u_n$  para enteros positivos  $n$  pequeños y una relación entre el término general  $u_n$  y otros  $u_r$  con  $r < n$ .

Por ejemplo, supongamos que tenemos

$$u_1 = 1, \quad u_2 = 2, \quad u_n = u_{n-1} + u_{n-2} \quad (n \geq 3).$$

Para calcular los valores de  $u_n$  para cada  $n$  de  $\mathbb{N}$  podríamos proceder así:

$$u_3 = u_2 + u_1 = 2 + 1 = 3,$$

$$u_4 = u_3 + u_2 = 3 + 2 = 5,$$

$$u_5 = u_4 + u_3 = 5 + 3 = 8,$$

y así sucesivamente. Este es un ejemplo de una *definición recursiva*. Es del todo “evidente” que el método proporciona un valor único de  $u_n$  para cada entero positivo  $n$ . Pero en sentido estricto necesitamos el axioma del buen orden para justificar esta conclusión, tal como veremos a continuación.

Supongamos que existe un entero positivo  $n$  para el cual  $u_n$  no está definido de forma única. Entonces, por el axioma del buen orden, existe un entero positivo  $m$  mínimo con esta propiedad. Puesto que  $u_1$  y  $u_2$  están definidos explícitamente,  $m$  no es ni 1 ni 2, y la ecuación  $u_m = u_{m-1} + u_{m-2}$  puede aplicarse. Por la definición de  $m$ ,  $u_{m-1}$  y  $u_{m-2}$  están definidos únicamente, y la ecuación da un valor único para  $u_m$ , contrariamente a la hipótesis. La contradicción proviene de suponer que  $u_n$  no está bien definido para algún  $n$ , y por lo tanto la suposición ha de ser falsa.

El lector no debe desanimarse por el uso de argumentos tan retorcidos para establecer algo que es “evidentemente” correcto. Para empezar, sólo lo haremos cuando sea necesario, y en segundo lugar, el hecho de que el resultado sea “evidente” no significa más que estamos trabajando con la imagen mental correcta de los conjuntos  $\mathbb{N}$  y  $\mathbb{Z}$ . Una vez establecida una

base firme para esta imagen, podemos extenderla y obtener resultados que pueden ser menos “evidentes”.

El método de la definición recursiva aparecerá a menudo en el resto del libro. Hay otras formas del método que a menudo quedan ocultas por la notación. ¿Qué significan las expresiones siguientes?

$$\sum_{r=1}^n 2r - 1, \quad 1 + 3 + 5 + \cdots + (2n - 1).$$

Está claro que no es suficiente decir que significan lo mismo, ya que cada una contiene un símbolo misterioso,  $\sum$  y  $\cdots$ , respectivamente. Lo correcto sería decir que cada una de ellas es igual a la expresión  $s_n$  dada por la siguiente definición recursiva:

$$s_1 = 1, \quad s_n = s_{n-1} + (2n - 1) \quad (n \geq 2).$$

Esto pone de manifiesto que los dos símbolos misteriosos no son más que abreviaturas de definiciones recursivas, y que, en consecuencia, las expresiones están definidas correctamente para todo  $n$  de  $\mathbb{N}$ .

Comentarios parecidos se aplican a la definición de productos como  $n!$  (se lee  $n$  factorial). Si decimos que

$$n! = \prod_{i=1}^n i, \quad \text{o} \quad n! = 1 \times 2 \times 3 \times \cdots \times n,$$

el significado debiera ser claro para todo el mundo. Pero para ser precisos (y para que el ordenador pueda entenderlo) debiéramos utilizar la definición recursiva

$$1! = 1, \quad n! = n \times (n-1)! \quad (n \geq 2).$$

### Ejercicios 1.3

1 En los casos siguientes calcular (si es posible) los valores de  $u_1, u_2, u_3, u_4$  y  $u_5$  dados por las ecuaciones. Si no pueden calcularse, explíquese por qué falla la definición.

- (i)  $u_1 = 1, \quad u_2 = 1, \quad u_n = u_{n-1} + 2u_{n-2} \quad (n \geq 3)$ .
- (ii)  $u_1 = 1, \quad u_n = u_{n-1} + 2u_{n-2} \quad (n \geq 2)$ .
- (iii)  $u_1 = 0, \quad u_n = nu_{n-1} \quad (n \geq 2)$ .

2 Dar una definición recursiva de la “ $n$ -ésima potencia”  $2^n$  para todo  $n \geq 1$ .

3 Supongamos que se define  $u_n$  mediante las ecuaciones

$$u_1 = 2, \quad u_n = 2^{u_{n-1}} \quad (n \geq 2).$$

¿Cuál es el mínimo valor de  $n$  para el que no es practicable calcular  $u_n$  con una calculadora de bolsillo?

4 Hallar fórmulas explícitas para las expresiones  $u_n$  definidas por las ecuaciones siguientes:

$$(i) u_1 = 1, \quad u_n = u_{n-1} + 3 \quad (n \geq 2).$$

$$(ii) u_1 = 1, \quad u_n = n^2 u_{n-1} \quad (n \geq 2).$$

#### 1.4 El principio de inducción

Supongamos que hemos de demostrar el resultado

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

En otras palabras, hemos de demostrar que la expresión de la izquierda definida recursivamente es igual a la definida explícitamente por la fórmula de la derecha, para todos los enteros positivos  $n$ . Podríamos proceder así.

La fórmula es desde luego correcta si  $n = 1$ , ya que  $1^2 = 1$ . Supongamos que es correcta para un valor específico de  $n$ , digamos  $n = k$ , con lo que

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2.$$

Podemos usar esto para simplificar el término de la izquierda si  $n = k + 1$  de la forma siguiente:

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k + 1) &= 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) \\ &= k^2 + (2k + 1) \\ &= (k + 1)^2. \end{aligned}$$

De modo que si el resultado es correcto para  $n = k$ , también lo es para  $n = k + 1$ . Notemos para empezar que es correcto si  $n = 1$  y, por lo tanto,

ha de ser correcto si  $n = 2$ . Por el mismo argumento, ya que es correcto para  $n = 2$ , tiene que serlo para  $n = 3$ . Prosiguiendo de esta forma vemos que es correcto para todos los enteros positivos  $n$ .

La esencia de este argumento se conoce a menudo como el *principio de inducción*. Es una técnica potente, fácil de aplicar y que usaremos con frecuencia. Pero antes hemos de examinar su fundamento lógico, aunque para ello necesitamos una formulación más general.

Sea  $S$  el subconjunto de  $\mathbb{N}$  para el que el resultado es correcto: desde luego, nuestro objetivo es demostrar que  $S$  es todo  $\mathbb{N}$ . El primer paso es demostrar que 1 está en  $S$ , y entonces demostrar que si  $k$  es de  $S$  también lo es  $k + 1$ . Ahora hacemos “chu-chu” (Fig. 1.4) y concluimos que  $S = \mathbb{N}$ . Afortunadamente, el “chu-chu” no es esencial, puesto que el principio de inducción es consecuencia de los axiomas de  $\mathbb{Z}$  y  $\mathbb{N}$  que hemos elegido tan cuidadosamente. En concreto, es una consecuencia del axioma del buen orden.

**Teorema 1.4.** Sea  $S$  un subconjunto de  $\mathbb{N}$  que satisface las condiciones

(i)  $1 \in S$ ,

(ii) para todo  $k \in S$ , si  $k \in S$  entonces  $k + 1 \in S$ .

Entonces se tiene que  $S = \mathbb{N}$ .

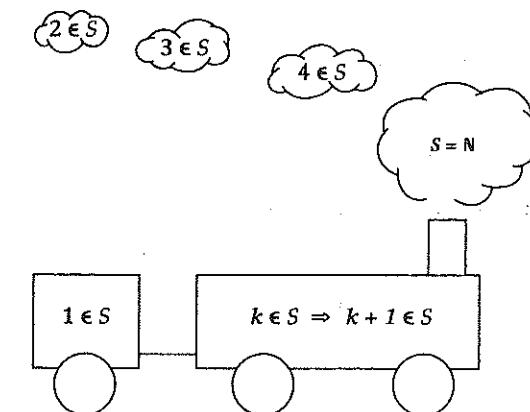


Fig. 1.4 El principio de inducción.

**DEMOSTRACIÓN:** Si la conclusión es falsa, entonces  $S \neq \mathbb{N}$  y el complementario  $\bar{S}$ , definido por

$$\bar{S} = \{r \in \mathbb{N} \mid r \notin S\}$$

no es vacío. Por el axioma del buen orden,  $\bar{S}$  tiene un mínimo  $m$ . Puesto que 1 pertenece a  $S$ , tenemos que  $m \neq 1$ . Pero  $m - 1$  es de  $\mathbb{N}$  y, ya que  $m$  es el mínimo de  $\bar{S}$ ,  $m - 1$  ha de ser de  $S$ . Poniendo  $k = m - 1$  en la condición (ii), concluimos que  $m$  es de  $S$ , lo que contradice el hecho de que  $m$  es de  $\bar{S}$ . Así pues, el enunciado  $S \neq \mathbb{N}$  nos lleva a una contradicción y debe ser  $S = \mathbb{N}$ .  $\square$

**Ejemplo.** Definimos el entero  $x_n$  recursivamente como

$$x_1 = 2 \quad y \quad x_n = x_{n-1} + 2n \quad (n \geq 2).$$

Demostrar que

$$x_n = n(n+1) \quad \text{para cada } n \in \mathbb{N}.$$

**SOLUCIÓN:** (*Base de la inducción*) El resultado es cierto para  $n = 1$  ya que  $2 = 1 \times 2$ .

(*Hipótesis de inducción*) Supongamos que el resultado es cierto para  $n = k$ , es decir,  $x_k = k(k+1)$ . Entonces

$$\begin{aligned} x_{k+1} &= x_k + 2(k+1) \quad (\text{por la definición recursiva}) \\ &= k(k+1) + 2(k+1) \quad (\text{por la hipótesis de inducción}) \\ &= (k+1)(k+2) \end{aligned}$$

El resultado es cierto para  $n = k+1$  y, por el principio de inducción, es cierto para todos los enteros positivos  $n$ .  $\square$

El principio de inducción tiene algunas variantes. A veces es conveniente tomar como base de la inducción el valor  $n = 0$ ; también puede ser apropiado tomar un valor como 2 o 3, ya que los primeros casos pueden ser excepcionales. Hay que abordar cada problema según su carácter. Otra modificación útil es tomar como hipótesis de inducción la suposición de que el resultado es cierto para *todos* los valores relevantes  $n \leq k$ , en lugar

de serlo únicamente para  $n = k$  (esta formulación se conoce a veces con el nombre de principio de inducción *fuerte*). Todas estas modificaciones pueden justificarse con cambios triviales en la demostración del teorema 1.4 tal como se indica en el ejercicio 1.4.6.

#### Ejercicios 1.4

- 1 Utilizar el principio de inducción para demostrar que

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

para todo entero positivo  $n$ .

- 2 Construir una tabla con los valores de

$$S_n = 1^3 + 2^3 + \cdots + n^3$$

para  $1 \leq n \leq 6$ . Conjeturar una fórmula para  $S_n$  basándose en la tabla (Indicación: los valores de  $S_n$  son cuadrados perfectos). Utilizar el principio de inducción para demostrar que la fórmula es correcta para todo  $n \geq 1$  (si el método falla, la fórmula es falsa!).

- 3 Utilizar la forma fuerte del principio de inducción para demostrar que si se define  $u_n$  recursivamente mediante

$$u_1 = 3 \quad u_2 = 5, \quad u_n = 3u_{n-1} - 2u_{n-2} \quad (n \geq 3),$$

entonces  $u_n = 2^n + 1$  para todo entero positivo  $n$ .

- 4 Hallar el menor entero positivo  $n_0$  para el cual  $n! \geq 2^n$ . Tomando el caso  $n = n_0$  como base de la inducción, demostrar que el resultado es cierto para todo  $n \geq n_0$ .

- 5 Hallar el valor apropiado de  $n_0$  como base de la inducción en los casos siguientes y demostrar que el enunciado es cierto para todo  $n \geq n_0$ .

$$(i) n^2 + 6n + 8 \geq 0 \quad (ii) n^3 \geq 6n^2.$$

- 6 El teorema siguiente incorpora todas las modificaciones del principio básico de inducción esbozadas anteriormente.

**Teorema 1.4\***. Sea  $n_0$  un entero cualquiera (no necesariamente positivo), y  $X$  el conjunto de los enteros  $n \geq n_0$ . Sea  $S$  un subconjunto de  $X$  que satisface las condiciones

- (i)  $n_0 \in S$ ,
  - (ii) si  $x \in S$  para todo  $x$  en el rango  $n_0 \leq x \leq k$ , entonces  $k + 1 \in S$ .
- Entonces se tiene  $S = X$ .

Reescribir la demostración del teorema 1.4 haciendo los cambios necesarios para demostrar el teorema 1.4\*.

## 1.5 Cociente y resto

De niños aprendemos que al dividir 27 entre 6, el *cociente* es 4 y el *resto* es 3, es decir,

$$27 = 6 \times 4 + 3.$$

Lo importante es que el resto ha de ser menor que 6. Aunque también es cierto, por ejemplo, que

$$27 = 6 \times 3 + 9,$$

se nos dice que debemos tomar como resto el valor mínimo, de forma que “lo que sobra” sea lo menor posible. El hecho de que el conjunto de posibles “restos” tenga un mínimo es una consecuencia del axioma del buen orden.

**Teorema 1.5.** Dados enteros  $a$  y  $b$  con  $b \in \mathbb{N}$ , existen enteros  $q$  y  $r$  tales que

$$a = bq + r \quad y \quad 0 \leq r < b.$$

**DEMOSTRACIÓN:** Apliquemos el axioma del buen orden al conjunto de “restos”

$$R = \{x \in \mathbb{N}_0 \mid a = by + x \text{ para algún } y \in \mathbb{Z}\}.$$

Primero demostraremos que  $R$  no es vacío. Si  $a \geq 0$ , la identidad

$$a = b0 + a$$

demuestra que  $a \in R$ , mientras que si  $a < 0$ , la identidad

$$a = ba + (1 - b)a$$

demuestra que  $(1 - b)a \in R$  (en ambos casos hay que comprobar que el elemento de  $R$  en cuestión no es negativo).

Ahora bien,  $R$  tiene un mínimo  $r$  por ser un subconjunto no vacío de  $\mathbb{N}_0$ , y puesto que  $r \in R$ , resulta que  $a = bq + r$  para algún  $q$  de  $\mathbb{Z}$ . Además,

$$a = bq + r \quad \Rightarrow \quad a = b(q + 1) + (r - b),$$

de forma que si  $r \geq b$ , entonces  $r - b$  está en  $R$ . Pero  $r - b$  es menor que  $R$ , contrariamente a la definición de  $r$  como el mínimo de  $R$ . Dado que la suposición  $r \geq b$  lleva a una contradicción, debe ser  $r < b$  como queríamos demostrar.  $\square$

Es fácil ver que el cociente  $q$  y el resto  $r$  del teorema son únicos. En efecto, supongamos que  $q'$  y  $r'$  también satisfacen las condiciones, es decir,

$$a = bq' + r' \quad y \quad 0 \leq r' < b.$$

Si  $q' < q$ , entonces  $q - q' \geq 1$ , de forma que

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b.$$

Puesto que  $r + b \geq b$ , resulta que  $r' \geq b$ , lo que contradice la segunda propiedad de  $r'$ . Por lo tanto, la suposición  $q' < q$  es falsa. Intercambiando  $q$  y  $q'$  se demuestra que  $q < q'$  es falsa, de donde  $q = q'$  y en consecuencia  $r = r'$ , ya que

$$r' = a - bq = a - bq' = r'.$$

Una consecuencia importante del teorema 1.5 es que justifica el método habitual de representar los enteros. Sea  $t \geq 2$  un entero al que llamaremos la **base** de cálculo. Para cualquier entero  $x$  tenemos, aplicando repetidamente el teorema 1.5,

$$x = tq_0 + r_0$$

$$q_0 = tq_1 + r_1$$

...

$$q_{n-2} = tq_{n-1} + r_{n-1}$$

$$q_{n-1} = tq_n + r_n.$$

Cada resto  $r_i$  es uno de los enteros  $0, 1, \dots, t - 1$ , y acabamos cuando  $q_n = 0$ . Si eliminamos los cocientes  $q_i$  obtenemos

$$x = r_n t^n + r_{n-1} t^{n-1} + \dots + r_1 t + r_0.$$

Hemos representado  $x$  (respecto de la base  $t$ ) por una sucesión de restos, y lo escribimos  $x = (r_n r_{n-1} \dots r_1 r_0)_t$ . La base convencional para calcular a mano es  $t = 10$  y se omite el subíndice; tenemos así la notación habitual

$$1984 = (1 \times 10^3) + (9 \times 10^2) + (8 \times 10) + 4.$$

La notación posicional requiere símbolos sólo para los enteros  $0, 1, \dots, t - 1$ . El caso  $t = 2$  es especialmente adecuado para el cálculo con máquinas, ya que los símbolos 0 y 1 pueden representarse físicamente por la ausencia o presencia de un pulso de electricidad o de luz.

**Ejemplo.** ¿Cuál es la representación de  $(109)_{10}$  en base 2?

**SOLUCIÓN:** Diviendo repetidamente por 2 se obtiene

$$\begin{aligned} 109 &= 2 \times 54 + 1 \\ 54 &= 2 \times 27 + 0 \\ 27 &= 2 \times 13 + 1 \\ 13 &= 2 \times 6 + 1 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1. \end{aligned}$$

Por lo tanto

$$(109)_{10} = (1101101)_2.$$

□

### Ejercicios 1.5

1 Hallar  $q$  y  $r$  que satisfagan el teorema 1.5 si

- (i)  $a = 1001, b = 11$ ;      (ii)  $a = 12345, b = 234$ .

2 Hallar la representación de  $(1985)_{10}$  en base 2, en base 5 y en base 11.

3 Hallar la representación usual (en base 10) de

- (i)  $(11011101)_2$ ;      (ii)  $(4165)_7$ .

### 1.6 Divisibilidad

Dados dos enteros  $x$  e  $y$ , decimos que  $y$  es un **divisor** de  $x$ , y lo escribimos  $y|x$ , si

$$x = yq \quad \text{para algún } q \in \mathbb{Z}.$$

También decimos que  $y$  es un **factor** de  $x$ , que  $y$  **divide** a  $x$ , que  $x$  es **divisible** por  $y$ , y que  $x$  es un **múltiplo** de  $y$ .

Si  $y|x$ , podemos usar el símbolo  $\frac{x}{y}$  (o bien  $x/y$ ) para denotar al entero  $q$  tal que  $x = yq$ . Si  $y$  no es un divisor de  $x$ , la fracción  $x/y$  no es un entero y tenemos que asignarle un nuevo significado. El lector estará sin duda familiarizado con las reglas para manipular fracciones; usaremos estas reglas de vez en cuando, pero es importante recordar que las fracciones no han sido ni siquiera definidas formalmente en este libro. Es todavía más importante recordar que  $x/y$  no es un elemento de  $\mathbb{Z}$ , a menos que  $y$  divida a  $x$ .

**Ejemplo.** Demostrar que si  $c, d$  y  $n$  son enteros tales que

$$d|n \quad \text{y} \quad c \mid \frac{n}{d}$$

entonces

$$c|n \quad \text{y} \quad d \mid \frac{n}{c}.$$

**SOLUCIÓN:** Puesto que  $d|n$ , existe un entero  $s$  tal que  $n = ds$  y  $n/d$  es el entero  $s$ . Puesto que  $c|n/d$ , existe un entero  $t$  tal que

$$s = \frac{n}{d} = ct.$$

Resulta que

$$n = ds = d(ct) = c(dt),$$

de forma que  $c|n$  y  $n/c$  denota al entero  $dt$ . Finalmente, ya que  $n/c = dt$ , tenemos que  $d|n/c$  como queríamos. □

**Ejercicios 1.6**

- 1 Demostrar que  $x|0$  para todo  $x \in \mathbb{Z}$ , pero que  $0|x$  sólo si  $x = 0$ .
- 2 Demostrar que si  $c|a$  y  $c|b$ , entonces  $c|xa + yb$  para  $x$  e  $y$  enteros cualesquiera.
- 3 Demostrar que si  $a$  y  $b$  son enteros tales que  $ab = 1$ , entonces  $a = b = 1$  o  $a = b = -1$  (Indicación: o bien  $a$  y  $b$  son positivos, o bien son negativos). Deducir que si  $x$  e  $y$  son enteros tales que  $x|y$  y  $y|x$ , entonces  $x = y$  o  $x = -y$ .
- 4 Utilizar el principio de inducción para demostrar que, para todo  $n \geq 0$ ,
  - (i)  $n^2 + 3n$  es divisible por 2 ;
  - (ii)  $n^3 + 3n^2 + 2n$  es divisible por 6.

**1.7 El máximo común divisor**

Dados enteros  $a$  y  $b$ , decimos que el entero  $d$  es un **máximo común divisor**, o **mcd**, de  $a$  y  $b$  si

- (i)  $d|a$  y  $d|b$ ;
- (ii) si  $c|a$  y  $c|b$ , entonces  $c|d$ .

La condición (i) dice que  $d$  es un divisor común de  $a$  y  $b$ , y la condición (ii) dice que cualquier otro divisor común es también un divisor de  $d$ . Por ejemplo, 6 es un divisor común de 60 y 84, pero no es un máximo divisor común, ya que  $12|60$  y  $12|84$  pero  $12\nmid 6$  (el símbolo  $\nmid$  significa "no divide").

Las condiciones (i) y (ii) no son del todo suficientes para asegurar que dos enteros dados tienen un único mcd. Ya que si  $d$  y  $d'$  satisfacen ambos las condiciones, resulta que

$$d|d' \quad \text{y} \quad d'|d.$$

Por lo tanto, por el ejercicio 1.6.3,  $d = d'$  o  $d = -d'$ . Para obtener un único mcd es suficiente imponer una tercera condición:

$$(iii) \quad d \geq 0.$$

Decimos que el único entero  $d$  que satisface (i), (ii) y (iii) es *el mcd* de  $a$  y  $b$ , y escribimos  $d = \text{mcd}(a, b)$ . Por ejemplo,  $12 = \text{mcd}(60, 84)$ .

Existe un método muy conocido para calcular el mcd de dos enteros dados que se basa en la técnica del cociente y el resto. Depende del hecho de que

$$a = bq + r \quad \Rightarrow \quad \text{mcd}(a, b) = \text{mcd}(b, r).$$

Para demostrarlo notemos que si  $d$  es un divisor de  $a$  y  $b$ , entonces también lo es sin duda de  $a - bq$ ; pero  $a - bq = r$ , con lo que  $d$  divide a  $r$ . Así que cualquier divisor común de  $a$  y  $b$  también lo es de  $b$  y  $r$ . Recíprocamente, si  $d$  divide a  $b$  y  $r$ , también divide a  $a = bq + r$ . Una aplicación reiterada de este hecho proporciona el método para calcular el mcd.

**Ejemplo.** Hallar el mcd de 2406 y 654.

**SOLUCIÓN:** Tenemos

$$\begin{aligned} \text{mcd}(2406, 654) &= \text{mcd}(654, 444) && \text{ya que } 2406 = 654 \times 3 + 444, \\ &= \text{mcd}(444, 210) && \text{ya que } 654 = 444 \times 1 + 210, \\ &= \text{mcd}(210, 24) && \text{ya que } 444 = 210 \times 2 + 24, \\ &= \text{mcd}(24, 18) && \text{ya que } 210 = 24 \times 8 + 18, \\ &= \text{mcd}(18, 6) && \text{ya que } 24 = 18 \times 1 + 6, \\ &= 6 && \text{ya que } 18 = 6 \times 3. \end{aligned}$$

□

En general, para calcular el mcd de dos enteros  $a$  y  $b$  (ambos  $\geq 0$ ) definimos  $q_i$  y  $r_i$  recursivamente mediante las ecuaciones

$$\begin{aligned} a &= bq_1 + r_1 \quad (0 \leq r_1 < b) \\ b &= r_1 q_2 + r_2 \quad (0 \leq r_2 < r_1) \\ r_1 &= r_2 q_3 + r_3 \quad (0 \leq r_3 < r_2) \\ &\dots \end{aligned}$$

Está claro que el proceso tiene que terminar finalmente, ya que cada resto  $r_i$  es estrictamente menor que el precedente. De forma que los últimos pasos son éstos:

$$\begin{aligned} r_{k-4} &= r_{k-3} q_{k-2} + r_{k-2} \quad (0 \leq r_{k-2} < r_{k-3}) \\ r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} \quad (0 \leq r_{k-1} < r_{k-2}) \\ r_{k-2} &= r_{k-1} q_k, \end{aligned}$$

donde  $r_k$  se anula, y el mcd buscado es  $r_{k-1}$ . Este procedimiento se conoce como **algoritmo de Euclides**, en recuerdo del matemático griego Euclides (hacia 300 a.C.). Es extremadamente útil en la práctica y tiene importantes consecuencias teóricas.

**Teorema 1.7.** Sean  $a$  y  $b$  enteros con  $b \geq 0$ , y sea  $d = \text{mcd}(a, b)$ . Entonces existen enteros  $m$  y  $n$  tales que

$$d = ma + nb.$$

**DEMOSTRACIÓN:** De acuerdo con la notación anterior,  $d = r_{k-1}$ , y utilizando la penúltima ecuación tenemos que

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}.$$

Así pues,  $d$  puede escribirse como  $m'r_{k-2} + n'r_{k-3}$ , donde  $m' = -q_{k-1}$  y  $n' = 1$ . Sustituyendo  $r_{k-2}$  por su expresión en términos de  $r_{k-3}$  y  $r_{k-4}$  obtenemos

$$d = m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3},$$

que puede escribirse como  $m''r_{k-3} + n''r_{k-4}$  con  $m'' = n' - m'q_{k-2}$  y  $n'' = m'$ . Continuando con estas sustituciones llegaremos finalmente a una expresión de  $d$  de la forma pedida.  $\square$

Por ejemplo, a partir de los cálculos efectuados para obtener el mcd de 2406 y 654 obtenemos

$$\begin{aligned} 6 &= 24 - 18 \times 1 = 1 \times 24 + (-1) \times 18 \\ &= 24 + (-1) \times (210 - 24 \times 8) = (-1) \times 210 + 9 \times 24 \\ &= -210 + 9 \times (444 - 210 \times 2) = 9 \times 444 + (-19) \times 210, \\ &= 9 \times 444 + (-19) \times (654 - 444 \times 1) = (-19) \times 654 + 28 \times 444 \\ &= (-19) \times 654 + 28 \times (2406 - 654 \times 3) = 28 \times 2406 + (-103) \times 654. \end{aligned}$$

Por lo tanto, la expresión requerida  $d = ma + nb$  es

$$6 = 28 \times 2406 + (-103) \times 654.$$

Si  $\text{mcd}(a, b) = 1$  decimos que  $a$  y  $b$  son **primos entre sí**, y en este caso el teorema 1.7 asegura que existen enteros  $m$  y  $n$  tales que

$$ma + nb = 1.$$

Esta es una observación muy útil; por ejemplo, en la reducción de una fracción a la forma  $a/b$  donde  $a$  y  $b$  son primos entre sí. El ejemplo siguiente demuestra que esta forma es única y, como veremos, el hecho clave en la demostración es la posibilidad de expresar 1 como  $ma + nb$ .

**Ejemplo.** Supongamos que los enteros positivos  $a, a', b, b'$  satisfacen

$$(i) ab' = a'b; \quad (ii) \text{mcd}(a, b) = \text{mcd}(a', b') = 1.$$

Entonces  $a = a'$  y  $b = b'$ .

(La condición (i) puede escribirse como  $a/b = a'/b'$ , pero preferimos utilizar una forma que no presuponga nada sobre fracciones.)

**SOLUCIÓN:** Puesto que  $\text{mcd}(a, b) = 1$ , existen enteros  $m$  y  $n$  tales que  $ma + nb = 1$ . En consecuencia,

$$b' = (ma + nb)b' = mab' + nb'b' = (ma' + nb')b,$$

de forma que  $b|b'$ . Con un argumento similar, utilizando el hecho de que  $\text{mcd}(a', b') = 1$ , deducimos que  $b'|b$ . Así que  $b = b'$  o  $b = -b'$ , y como  $b$  y  $b'$  son positivos, ha de ser  $b = b'$ . De (i) se desprende que  $a = a'$  y el resultado está demostrado.  $\square$

### Ejercicios 1.7

- Hallar el mcd de 721 y 448 y expresarlo en la forma  $721m + 448n$  con  $n$  y  $m$  de  $\mathbb{Z}$ .
- Demostrar que si existen enteros  $m$  y  $n$  tales que  $mu + nv = 1$ , entonces  $\text{mcd}(u, v) = 1$ .
- Usar el teorema 1.7 y el ejercicio 2 para demostrar que si  $\text{mcd}(a, b) = d$ , entonces

$$\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

4 Sean  $a$  y  $b$  enteros positivos y sea  $d = \text{mcd}(a, b)$ . Demostrar que existen enteros  $x$  e  $y$  que satisfacen la ecuación  $ax + by = c$  si, y sólo si,  $d|c$ .

5 Hallar enteros  $x$  e  $y$  que satisfagan

$$966x + 686y = 70.$$

## 1.8 Factorización en números primos

Se dice que un entero positivo  $p$  es **primo** si  $p \geq 2$  y los únicos enteros positivos que dividen a  $p$  son 1 y el propio  $p$ . Por lo tanto, un entero  $m \geq 2$  no es primo si, y sólo si, puede escribirse como  $m = m_1 m_2$ , donde  $m_1$  y  $m_2$  son enteros estrictamente entre 1 y  $m$ .

Notemos que según la definición, 1 *no* es primo. Los primeros primos son:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Casi seguro que el lector está familiarizado con la idea de que cualquier entero positivo puede expresarse como un producto de primos; por ejemplo,

$$825 = 3 \times 5 \times 5 \times 11.$$

La existencia de tal *factorización en primos* para cada entero positivo  $n \geq 2$  es consecuencia del axioma del buen orden. En efecto, sea  $B$  el conjunto de los enteros positivos  $n \geq 2$  que *no* poseen una factorización en primos; si  $B$  no es vacío, entonces el axioma del buen orden nos dice que tiene un mínimo  $m$ . Si  $m$  fuera primo  $p$  tendríamos la factorización trivial  $m = p$ ; luego,  $m$  no es un primo y  $m = m_1 m_2$  donde  $1 < m_1 < m$  y  $1 < m_2 < m$ . Puesto que suponemos que  $m$  es el mínimo entero ( $\geq 2$ ) que no factoriza en primos, tanto  $m_1$  como  $m_2$  deben factorizar. Pero entonces la ecuación  $m = m_1 m_2$  nos da una factorización de  $m$ , en contradicción con la suposición de que  $m$  es un elemento de  $B$ . En consecuencia,  $B$  es vacío y la afirmación está demostrada.

### Ejercicios 1.8

1 Hallar todos los primos  $p$  entre 100 y 120.

- 2 Escribir las factorizaciones de 201, 1001 y 201000.
- 3 Demostrar que si  $p$  y  $p'$  son primos y  $p'|p$ , entonces  $p = p'$ .
- 4 Demotrar que si  $n \geq 2$  y  $n$  no es primo, entonces existe un primo  $p$  que divide a  $n$  y tal que  $p^2 \leq n$ .
- 5 Utilizar el resultado del ejercicio 4 para demostrar que si 467 no fuera primo tendría un divisor primo  $p \leq 19$ . Deducir que 467 es primo.

La facilidad con que hemos establecido la existencia de factorizaciones esconde dos dificultades importantes. En primer lugar, el problema de hallar los factores primos no es en modo alguno trivial; y en segundo, no es evidente que exista una **única** factorización en primos para un entero cualquiera  $n \geq 2$ . El siguiente resultado es un paso clave en la demostración de la unicidad.

**Teorema 1.8.1.** Si  $p$  es primo y  $x_1, x_2, \dots, x_n$  son enteros tales que

$$p|x_1 x_2 \dots x_n,$$

entonces  $p|x_i$  para algún  $x_i$  ( $1 \leq i \leq n$ ).

**DEMOSTRACIÓN:** Utilizaremos el principio de inducción. El resultado es claramente cierto si  $n = 1$  (base de la inducción). Para la hipótesis de inducción, supongamos que es cierto para  $n = k$ .

Súpongamos que  $p|x_1 x_2 \dots x_k x_{k+1}$  y sea  $x = x_1 x_2 \dots x_k$ . Si  $p|x$  entonces, por la hipótesis de inducción,  $p|x_i$  para algún  $x_i$  con  $1 \leq i \leq k$ . Si  $p \nmid x$ , entonces (puesto que  $p$  no tiene divisores excepto 1 y él mismo) tenemos  $\text{mcd}(p, x) = 1$ . Por el teorema 1.7, existen enteros  $r$  y  $s$  tales que  $rp + sx = 1$ . Por lo tanto,

$$x_{k+1} = (rp + sx)x_{k+1} = (rx_{k+1})p + s(xx_{k+1}),$$

y como  $p$  divide a ambos términos resulta que  $p|x_{k+1}$ . En cualquier caso,  $p$  divide a uno de los  $x_i$  ( $1 \leq i \leq k+1$ ) y, por el principio de inducción, el resultado es cierto para todos los enteros positivos  $n$ .  $\square$

Un error muy frecuente es suponer que el teorema 1.8.1 mantiene su validez si sustituimos  $p$  por un entero cualquiera. Pero esto es claramente absurdo: por ejemplo

$$6|3 \times 8 \text{ pero } 6 \nmid 3 \text{ y } 6 \nmid 8.$$

Ejemplos como éstos nos ayudan a entender que el teorema 1.8.1 expresa una propiedad muy significativa de los números primos. De hecho, veremos que esta propiedad juega un papel crucial en el resultado siguiente, conocido a veces como el *Teorema fundamental de la aritmética*.

**Teorema 1.8.2.** *La factorización en primos de un entero positivo  $n \geq 2$  es única, salvo por el orden de los factores.*

**DEMOSTRACIÓN:** Por el axioma del buen orden, si existe un entero para el que el teorema es falso, entonces existe un entero mínimo  $n_0 \geq 2$  con esta propiedad. Supóngase entonces que

$$n_0 = p_1 p_2 \dots p_k \quad y \quad n_0 = p'_1 p'_2 \dots p'_l,$$

donde los  $p_i$  son primos no necesariamente distintos y lo mismo los  $p'_i$ . La primera ecuación implica que  $p_1 | n_0$ , y la segunda ecuación implica que  $p_1 | p'_1 p'_2 \dots p'_l$ . Según el teorema 1.8.1,  $p_1$  divide a  $p'_j$  para algún  $j$  ( $1 \leq j \leq l$ ). Reordenando la segunda factorización podemos suponer que  $p_1 | p'_1$ , y puesto que ambos son primos resulta que  $p_1 = p'_1$  (ejercicio 1.8.3). Por el axioma I7 podemos cancelar los factores  $p_1$  y  $p'_1$  y obtener

$$p_2 p_3 \dots p_k = p'_2 p'_3 \dots p'_l = n_1.$$

Pero hemos supuesto que las factorizaciones de  $n_0$  eran distintas y hemos eliminado sólo los factores iguales  $p_1$  y  $p'_1$ , de forma que  $n_1$  tiene dos factorizaciones distintas. Esto contradice el hecho de que  $n_0$  fuera el menor entero con esta propiedad y demuestra el teorema.  $\square$

En la práctica se suelen agrupar los primos iguales en la factorización de  $n$  y escribimos

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

donde  $p_1, p_2, \dots, p_r$  son primos distintos y  $e_1, e_2, \dots, e_r$  son enteros positivos. Por ejemplo,  $7000 = 2^3 \times 5^3 \times 7$ .

**Ejemplo.** Demostrar que si  $m$  y  $n$  son enteros tales que  $m \geq 2$  y  $n \geq 2$ , entonces  $m^2 \neq 2n^2$ .

**SOLUCIÓN:** Supongamos que la factorización de  $n$  contiene el primo 2 elevado a la potencia  $x$  (donde  $x$  es cero si 2 no es un factor de  $n$ ). Entonces  $n = 2^x h$ , donde  $h$  es un producto de primos mayores que 2, de forma que

$$2n^2 = 2(2^x h)^2 = 2^{2x+1} h^2.$$

Así que en la factorización de  $2n^2$ , 2 está elevado a una potencia *impar*.

Por otra parte, si  $m = 2^y g$ , donde  $g$  es un producto de primos mayores que 2, entonces

$$m^2 = (2^y g)^2 = 2^{2y} g^2,$$

de forma que 2 está elevado a una potencia *par* (posiblemente cero) en la factorización de  $m^2$ . Si  $m^2 = 2n^2$  tendríamos dos factorizaciones distintas de un mismo entero, contrariamente al teorema 1.8.2. Así que  $m^2 \neq 2n^2$ .  $\square$

Está claro que la conclusión del ejemplo anterior también es válida si  $m$  o  $n$  son iguales a 1. Podemos expresar el resultado diciendo que no existen enteros positivos  $m$  y  $n$  tales que

$$\left(\frac{m}{n}\right)^2 = 2$$

o, equivalentemente, diciendo que la raíz cuadrada de 2 no puede expresarse como una fracción  $m/n$ .

### Ejercicios 1.8 (continuación)

6 Sean  $m$  y  $n$  enteros positivos cuyas factorizaciones son

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \quad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

Demostrar que el  $\text{mcd}$  de  $m$  y  $n$  es  $d = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  donde  $k_i$  es el menor de  $e_i$  y  $f_i$  para cada  $i$  tal que  $1 \leq i \leq k$ .

7 Demostrar que si  $m$  y  $n$  son enteros positivos tales que  $m \geq 2$ ,  $n \geq 2$  y  $m^2 = kn^2$ , entonces  $k$  es el cuadrado de un entero.

8 Utilizar la identidad

$$2^{rs} - 1 = (2^r - 1)(2^{(s-1)r} + 2^{(s-2)r} + \dots + 2^r + 1)$$

para demostrar que si  $2^n - 1$  es primo, también lo es  $n$ .

9 Hallar el mínimo valor de  $n$  para el que el recíproco del ejercicio 8 es falso: es decir,  $n$  es primo pero  $2^n - 1$  no lo es.

## 1.9 Ejercicios diversos

1 Utilizar el principio de inducción para demostrar que  $2^n > n+1$  para cualquier entero  $n \geq 2$ .

2 Demostrar que

$$1^4 + 2^4 + \dots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

3 Demostrar que  $4^{2n} - 1$  es divisible por 15 para cualquier entero  $n \geq 1$ .

4 Hallar el mcd de 1320 y 714, y expresar el resultado en la forma  $1320x + 714y$ , con  $x, y$  de  $\mathbb{Z}$ .

5 Demostrar que 725 y 441 son primos entre sí y hallar enteros  $x$  e  $y$  tales que  $725x + 441y = 1$ .

6 Hallar una solución en números enteros de la ecuación

$$325x + 26y = 91.$$

7 Se define el entero  $f_n$  recursivamente mediante las ecuaciones

$$f_1 = 1, \quad f_2 = 1, \quad f_{n+1} = f_n + f_{n-1} \quad (n \geq 2).$$

Demostrar que  $\text{mcd}(f_{n+1}, f_n) = 1$  para todo  $n \geq 1$ .

8 Sean  $a$  y  $b$  dos enteros positivos. Se define el **mínimo común múltiplo** de  $a$  y  $b$  como el entero

$$l = \frac{ab}{\text{mcd}(a, b)}$$

Demostrar que

(i)  $a|l$  y  $b|l$ ;

(ii) si  $m$  es un entero positivo tal que  $a|m$  y  $b|m$ , entonces  $l|m$ .

9 Demostrar las siguientes propiedades del mcd.

(i)  $\text{mcd}(ma, mb) = m \text{mcd}(a, b)$ .

(ii) Si  $\text{mcd}(a, x) = d$  y  $\text{mcd}(b, x) = 1$ , entonces  $\text{mcd}(ab, x) = d$ .

10 Se dispone de un suministro ilimitado de agua, un gran cubo con un desague y dos garrafas que contienen 7 y 9 litros respectivamente. ¿Cómo podría ponerse un litro de agua en el cubo? Explicar la relación entre la respuesta y el teorema 1.

11 Siguiendo la línea de la definición del  $\text{mcd}(a, b)$ , dar una definición del mcd de  $n$  enteros  $a_1, a_2, \dots, a_n$ . Demostrar que si  $d = \text{mcd}(a_1, a_2, \dots, a_n)$ , entonces existen enteros  $x_1, x_2, \dots, x_n$  tales que

$$d = x_1a_1 + x_2a_2 + \dots + x_na_n.$$

12 Sea  $n$  un entero positivo con las siguientes propiedades:

(i)  $n$  no contiene cuadrados (es decir, no hay factores repetidos en la factorización de  $n$  en números primos);

(ii) para cada primo  $p$  se tiene que  $p|n$  si, y sólo si,  $p-1|n$ .

Hallar el valor de  $n$ .

13 Se define el entero  $u_n$  mediante las ecuaciones

$$u_1 = 2, \quad u_{n+1} = u_n^2 - u_n + 1 \quad (n \geq 1).$$

Hallar el mínimo valor de  $n$  para el cual  $u_n$  no es primo y hallar los factores de este  $u_n$ . ¿Es primo  $u_6$ ?

14 Demostrar que los enteros definidos en el ejercicio 13 satisfacen

$$u_{n+1} = 1 + u_1u_2 \dots u_n.$$

Deducir que  $u_{n+1}$  tiene un factor primo diferente de los factores primos de  $u_1, u_2, \dots, u_n$ . Deducir que el conjunto de los números primos no tiene máximo.

15 ¿Es primo 65537?

16 Demostrar que si  $n$  es un entero positivo, ninguno de los  $n$  enteros consecutivos empezando por  $(n+1)! + 2$  es primo.

17 Demostrar que no existen enteros  $x, y, z, t$  para los que

$$x^2 + y^2 - 3z^2 - 3t^2 = 0.$$

18 Demostrar que si  $\text{mcd}(u, v) = 1$  y  $uv = z^2$  para algún entero  $z$ , entonces  $u = n^2$  y  $v = m^2$  para ciertos enteros  $m$  y  $n$ .

19 Demostrar que si  $\text{mcd}(a, b) = 1$ , entonces  $\text{mcd}(a+b, a-b)$  es igual a 1 o 2.

20 Demostrar que si tenemos pesos de 1, 2, 4, ...,  $2^{n-1}$  gramos, es posible equilibrar cualquier peso entero entre 1 y  $2^{n-1}$  gramos. Demostrar que no es posible hacerlo con ningún otro conjunto de  $n$  pesos.

## 2 Funciones y enumeración

### 2.1 Funciones

Sean  $X$  e  $Y$  dos conjuntos. Decimos que tenemos una **función  $f$  de  $X$  en  $Y$**  si para cada  $x$  de  $X$  podemos especificar un único elemento de  $Y$ , al que denotaremos por  $f(x)$ . La figura 2.1 ilustra esta situación; de ella proviene la notación estándar  $f : X \rightarrow Y$  para una función  $f$  de  $X$  en  $Y$ .

Es conveniente pensar en  $f$  como en una regla que asigna a cada objeto  $x$  de  $X$  un único objeto  $f(x)$  de  $Y$ . Al objeto  $f(x)$  se le suele llamar el **valor de  $f$  en  $x$** . Lo importante es que  $f(x)$  está definido para cada  $x$  de  $X$  y que sólo hay un objeto para cada  $x$ .

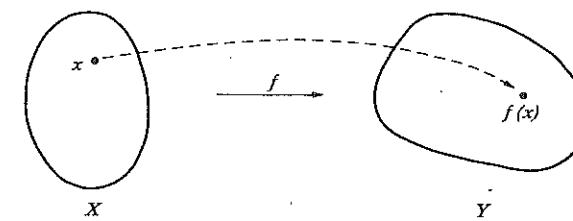


Fig. 2.1 Una función  $f : X \rightarrow Y$ .

Las funciones más comunes en las matemáticas elementales son aquellas en las que  $X$  e  $Y$  son los conjuntos  $\mathbb{N}$  o  $\mathbb{Z}$ , o algún otro conjunto de números. En este caso, la forma más sencilla de especificar una función es mediante una fórmula. Por ejemplo, la regla

$$f(n) = 3n + 4 \quad (n \in \mathbb{N})$$

define una función  $f$  de  $\mathbb{N}$  en  $\mathbb{N}$  cuyo valor en  $n$  es  $3n+4$ . Algunas funciones requieren una definición a trozos, como la función  $g$  de  $\mathbb{Z}$  en  $\mathbb{Z}$  dada por

la regla

$$g(x) = \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

Esta función asigna a cada entero  $x$  su *valor absoluto*, que habitualmente se escribe  $|x|$ . Por ejemplo,  $|5| = |-5| = 5$ .

Cuando  $X = \mathbb{N}$ , podemos especificar una función mediante una definición recursiva, tal como se indica en el apartado 1.3. Allí hablábamos (de una forma un tanto vaga) de una expresión  $u_n$  definida para cada  $n$  de  $\mathbb{N}$ . Sería más preciso decir que  $u_n$  no es más que una notación alternativa de  $u(n)$ , donde  $u$  es una función de  $\mathbb{N}$  en un conjunto adecuado  $Y$ . Por ejemplo, las ecuaciones

$$u(1) = 1, \quad u(2) = 2, \quad u(n) = u(n-1) + u(n-2) \quad (n \geq 3)$$

proporcionan una definición recursiva de una función  $u$  de  $\mathbb{N}$  en sí mismo. A menudo nos referimos a la lista de valores de una función de este tipo como una *sucesión*; en este caso la sucesión es

$$1, 2, 3, 5, 8, 13, 21, \dots$$

donde los tres puntos del final indican que la lista continúa indefinidamente. En general, una sucesión de elementos de un conjunto  $Y$  no es más que otro nombre para una función de  $\mathbb{N}$  en  $Y$ . (A veces es conveniente sustituir  $\mathbb{N}$  por  $\mathbb{N}_0$  u otro conjunto de enteros.) Una sucesión puede definirse recursivamente mediante una fórmula o de algún otro modo, pero en cualquier caso debemos tener definido un único elemento de  $Y$  para cada entero  $n$  que interviene en la definición.

Una propiedad útil de las funciones es que, en ocasiones, pueden combinarse tal como indica la figura 2.2. En concreto, si tenemos funciones  $f$  de  $X$  en  $Y$  y  $g$  de  $Y$  en  $Z$ , entonces existe una función de  $X$  en  $Z$  definida de la siguiente forma: para todo  $x$  de  $X$ , el valor  $f(x)$  está en  $Y$ , y el valor de  $g$  en  $f(x)$  es el elemento  $g(f(x))$  de  $Z$ . Si miramos esta doble operación como una sola, tenemos una función de  $X$  en  $Z$  que envía  $x$  a  $g(f(x))$ . Se la conoce como **composición** de las funciones  $f : X \rightarrow Y$  y  $g : Y \rightarrow Z$ , y se escribe  $gf$ . Así pues,

$$(gf)(x) = g(f(x)).$$

Es conveniente recordar que (en este libro)  $gf$  significa “primero  $f$ , después  $g$ ”. Aunque  $gf$  es una especie de producto de  $g$  y  $f$ , la idea se presta a confusiones. Si  $X$ ,  $Y$  y  $Z$  son conjuntos distintos, entonces  $gf$  está definida, pero  $fg$  no tiene ningún sentido. Incluso si  $gf$  y  $fg$  están ambas definidas, por ejemplo cuando  $X = Z$ , no hay ninguna razón para que sean la misma función.

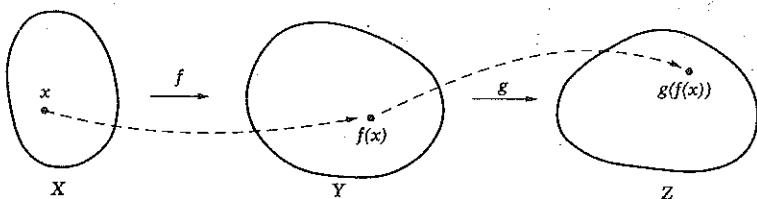


Fig. 2.2 La composición de  $f : X \rightarrow Y$  y  $g : Y \rightarrow Z$ .

### Ejercicios 2.1

1 Se definen las funciones  $s$  y  $t$  de  $\mathbb{Z}$  en  $\mathbb{Z}$  mediante

$$s(x) = x + 1, \quad t(x) = 2x \quad (x \in \mathbb{Z}).$$

Demostrar que  $st \neq ts$ .

2 Sea  $X = \{1, 2, 3, 4, 5\}$  y sea  $f : X \rightarrow X$  la función definida por

$$f(1) = 1, \quad f(2) = 2, \quad f(3) = 4, \quad f(4) = 4, \quad f(5) = 4.$$

Demostrar que  $ff = f$ . Hallar una función  $g \neq f$  tal que  $gf = f$  y  $fg = f$ .

3 Sea  $U$  el conjunto de ciudadanos del estado de Utopía. ¿Cuáles de las siguientes afirmaciones especifican de manera correcta una función de  $U$  en  $U$ ? (Cualquier suposición acerca de la población de Utopía debe hacerse explícitamente.)

(i)  $f(x)$  es la madre de  $x$ .      (ii)  $g(x)$  es la hermana de  $x$ .

(iii)  $h(x)$  es la esposa de  $x$ .

4 Supongamos que  $f$ ,  $g$  y  $h$  son funciones tales que la composición  $h(gf)$  está definida. Demostrar que  $(hg)f$  también está definida y que  $(hg)f = h(gf)$ .

## 2.2 Funciones exhaustivas, inyectivas y biyectivas

Hay clases de funciones especiales que reciben nombres especiales. Los diagramas de la figura 2.3 ilustran las definiciones siguientes (aconsejamos al lector el uso de esquemas de este tipo).



Fig. 2.3 Una función exhaustiva, una inyectiva y una biyectiva.

**Definición.** Una función  $f$  de  $X$  en  $Y$  es **exhaustiva** si cada  $y$  de  $Y$  es el valor  $f(x)$  de *al menos* un  $x$  de  $X$ . Es **inyectiva** (o una **inyección**) si cada  $y$  de  $Y$  es el valor  $f(x)$  de un  $x$  de  $X$  *como máximo*. Es **biyectiva** (o una **biyección**) si es inyectiva y exhaustiva al mismo tiempo, es decir, si cada  $y$  de  $Y$  es el valor  $f(x)$  de *exactamente* un  $x$  de  $X$ .

**Ejemplo.** Las fórmulas siguientes definen funciones de  $\mathbf{Z}$  en  $\mathbf{Z}$ . ¿Cuáles de ellas son exhaustivas, cuáles inyectivas y cuáles biyectivas?

$$(i) f(x) = x^2; \quad (ii) g(x) = x^2; \quad (iii) h(x) = x + 2.$$

**SOLUCIÓN:** (i) Puesto que  $f(x) = x^2$  y  $x^2$  no es nunca negativo, un entero negativo como  $-1$  no puede ser un valor de  $f$ , con lo que no existe ningún entero  $x$  tal que  $f(x) = -1$  y  $f$  no es exhaustiva. Además, hay enteros  $y$  tales que la ecuación  $f(x) = y$  tiene dos soluciones; por ejemplo, si  $y = 4$ ,  $f(2)$  y  $f(-2)$  son ambos iguales a 4. En consecuencia,  $f$  no es inyectiva.

(ii) Puesto que  $g(x) = 2x$  y  $2x$  es par, un entero impar como 3 no puede ser un valor de  $g$ . Por lo tanto,  $g$  no es exhaustiva. Por otra parte,  $g$  es

inyectiva. Para demostrarlo, supongamos que  $g$  toma el mismo valor  $y$  en dos enteros  $x$  y  $x'$ , es decir,  $y = 2x = 2x'$ . De acuerdo con el axioma I7, podemos eliminar el factor 2 y obtenemos  $x = x'$ , lo cual implica que la ecuación  $g(x) = y$  tiene como máximo una solución  $y$ , por lo tanto, que  $g$  es inyectiva.

(iii) Dado un entero  $y$ , tomamos  $x = y - 2$  y obtenemos

$$h(x) = x + 2 = y.$$

Así pues, existe al menos un entero  $x$  tal que  $h(x) = y$  y  $h$  es exhaustiva. Si hubiera dos enteros  $x$  y  $x'$  con la misma propiedad, tendríamos que  $x + 2 = x' + 2$ , lo cual implicaría que  $x = x'$ . Por lo tanto,  $h$  es inyectiva y, de hecho, biyectiva.  $\square$

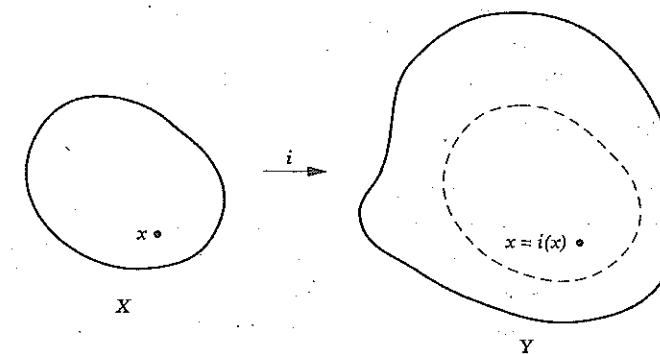


Fig. 2.4 La función inclusión  $i : X \rightarrow Y$ .

La técnica que acabamos de utilizar para demostrar que  $g$  y  $h$  son inyectivas es la más conveniente en la práctica. En general, para demostrar que una función  $f$  es inyectiva, suponemos que  $f(x) = f(x')$  y deducimos que  $x = x'$ .

Hay un tipo particular de inyección que tiene un nombre especial. Si  $X$  es un subconjunto de  $Y$ , la función **inclusión**  $i : X \rightarrow Y$  (fig. 2.4), definida por  $i(x) = x$  es claramente inyectiva. Si  $X = Y$ , se trata de una biyección, y se conoce como la función **identidad** de  $X$ . El siguiente teorema es muy útil.

- 2 Se define recursivamente la función  $u$  de  $\mathbb{N}$  en  $\mathbb{N}$  mediante las reglas

$$u(1) = 1, \quad u(n+1) = \begin{cases} \frac{1}{2}u(n) & \text{si } u(n) \text{ es par;} \\ 5u(n) + 1 & \text{en otro caso.} \end{cases}$$

Demuéstrese que  $u$  no es ni inyectiva ni exhaustiva.

- 3 Demostrar que si  $f$  y  $g$  son biyectivas y  $gf$  está definida, la inversa de  $gf$  es  $f^{-1}g^{-1}$ .

- 4 Se dice que la función  $f : X \rightarrow Y$  tiene una **inversa por la izquierda** si  $lf$  es la función identidad en  $X$ . Demostrar que

- (i) si  $f$  tiene una inversa por la izquierda, entonces es inyectiva;
- (ii) si  $f$  es inyectiva, entonces tiene una inversa por la izquierda.

- 5 Formular y demostrar resultados análogos a los del ejercicio anterior sobre inversas por la *derecha* de  $f : X \rightarrow Y$ .

### 2.3 Contar

¿Qué significa que un conjunto tenga  $n$  elementos? Una forma de contestar a la pregunta es recordar cómo contamos conjuntos sencillos. Decimos las palabras un, dos, tres, etcétera, y señalamos cada vez un objeto. Cuando cada objeto ha recibido un número nos detenemos, y el último número pronunciado es el número de elementos del conjunto.

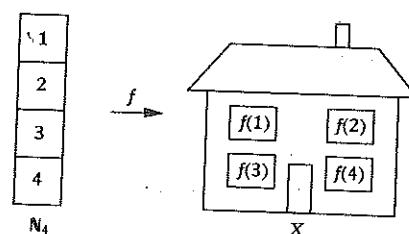


Fig. 2.6 Cómo contar ventanas.

Si queremos traducir esta técnica de numerar en lenguaje matemático, debemos definir, para cada entero positivo  $n$ , el conjunto

$$\mathbb{N}_n = \{1, 2, 3, \dots, n\}.$$

La técnica de numerar asigna a cada elemento de  $\mathbb{N}_n$  un elemento del conjunto  $X$  que queremos contar; en otras palabras, determina una función  $f$  de  $\mathbb{N}_n$  en  $X$  (figura 2.6). Además está claro que la función es *biyectiva*, puesto que si hemos contado correctamente, cada elemento de  $X$  recibe exactamente un número. Así pues, si  $X$  es un conjunto,  $n$  un entero positivo, y existe una biyección entre  $\mathbb{N}_n$  y  $X$ , decimos que  $X$  tiene  $n$  elementos.

Nótese que la definición no excluye explícitamente la posibilidad de que un conjunto tenga al mismo tiempo  $n$  y  $m$  elementos con  $m \neq n$ . De hecho, todos hemos tenido la experiencia de contar y volver a contar un conjunto moderadamente grande de objetos, como las ovejas de un rebaño, y obtener una respuesta diferente cada vez. El siguiente teorema es la pieza clave en la demostración de que esto es debido únicamente a una incapacidad práctica y de que realmente existe una sola respuesta correcta. En otras palabras, un conjunto con  $n$  elementos no puede tener al mismo tiempo  $m$  elementos si  $m \neq n$ .

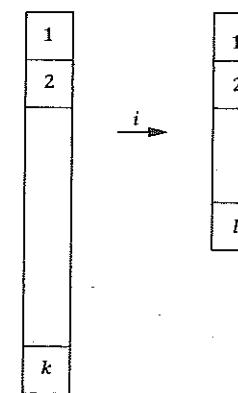


Fig. 2.7 La supuesta inyección  $i : \mathbb{N}_k \rightarrow \mathbb{N}_l$ .

**Teorema 2.3.** Si  $m$  y  $n$  son enteros positivos tales que  $m < n$ , entonces no existe ninguna inyección de  $\mathbb{N}_n$  en  $\mathbb{N}_m$ .

**DEMOSTRACIÓN:** Sea  $S$  el conjunto de los enteros positivos  $n$  para los que existe una inyección de  $\mathbb{N}_n$  en  $\mathbb{N}_m$  para algún  $m < n$ . Si  $S$  no es vacío

ha de tener un mínimo  $k$ , y puesto que  $k$  es de  $S$ , existe una inyección  $i$  de  $N_k$  en  $N_l$  para algún  $l < k$ . No es posible que  $l = 1$ , ya que cualquier función de  $N_k$  en  $N_1$  sólo puede tomar el valor 1, de forma que no puede existir ninguna inyección definida en  $N_k$  si  $k > 1$ . Por lo tanto,  $l - 1$  es un entero positivo y la situación puede describirse con la figura 2.7.

Si ninguno de los valores  $i(1), i(2), \dots, i(k-1)$  es igual a  $l$ , la restricción de  $i$  al conjunto  $N_{k-1}$  nos da una inyección de  $N_{k-1}$  en  $N_{l-1}$ . Por otra parte, si  $i(b) = l$  para algún  $b$  tal que  $1 \leq b \leq k-1$ , debe ser  $i(k) = c \neq l$ , puesto que  $i$  es una inyección. En este caso podemos construir una inyección  $i^*$  de  $N_{k-1}$  en  $N_{l-1}$  tal como muestra la figura 2.8; es decir,

$$i^*(b) = c, \quad i^*(r) = i(r) \quad (r \neq b).$$

En cualquier caso, la existencia de una inyección de  $N_{k-1}$  en  $N_{l-1}$  contradice la definición de  $k$  como el mínimo de  $S$ . Así pues,  $S$  debe ser vacío y el resultado está demostrado.  $\square$

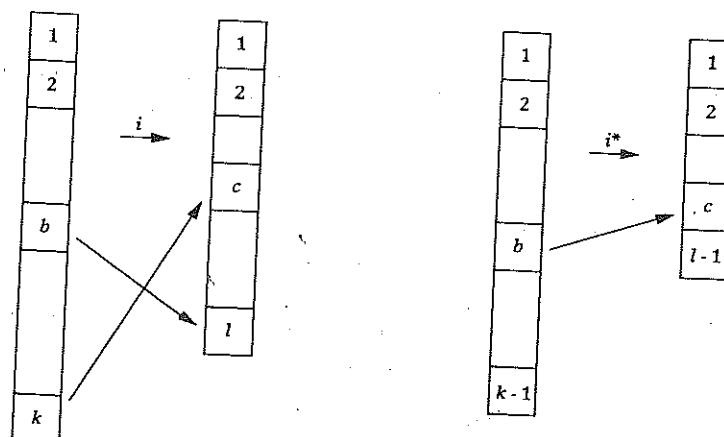


Fig. 2.8 Construcción de  $i^*$  cuando  $i(b) = l$ .

Supongamos que existe un conjunto  $X$  con  $n$  y  $m$  elementos al mismo tiempo para algún  $m < n$ . Entonces existen biyecciones

$$\beta : N_n \rightarrow X, \quad \gamma : N_m \rightarrow X,$$

y, por los resultados del apartado anterior, tanto  $\gamma^{-1}$  como  $\gamma^{-1}\beta$  son también biyecciones. En particular,  $\gamma^{-1}\beta$  es una inyección de  $N_n$  en  $N_m$ , contrariamente al teorema 2.3. Por lo tanto, la afirmación “ $X$  tiene  $n$  elementos” sólo puede cumplirse para un entero positivo a lo sumo.

Si  $X$  tiene  $n$  elementos, escribimos  $|X| = n$  y decimos que el **cardinal** (o **tamaño**) de  $X$  es  $n$ . Para el conjunto vacío  $\emptyset$  tenemos una definición especial pero razonable,

$$|\emptyset| = 0.$$

Si  $|X| = n$ , a menudo escribiremos

$$X = \{x_1, x_2, \dots, x_n\},$$

lo que realmente es otra forma de decir que existe una biyección  $\beta : N_n \rightarrow X$  tal que  $\beta(i) = x_i$  ( $1 \leq i \leq n$ ).

Para acabar, un aviso: muchos conjuntos no tienen un cardinal de acuerdo con la definición anterior. El conjunto  $N$  es un ejemplo. Volveremos a esta cuestión en el apartado 2.5.

### Ejercicios 2.3

1 En cada uno de los casos siguientes, hallar el valor apropiado de  $n$  y escribir una fórmula que dé una biyección  $f : N_n \rightarrow X$ .

- (i)  $X = \{2, 4, 6, 8, 10\}$ .
- (ii)  $X = \{-3, -8, -13, -18, -23, -28\}$ .
- (iii)  $X = \{10, 17, 26, 37, 50, 65, 82, 101\}$ .
- (iv)  $X = \{k \in N \mid \text{el } k\text{-ésimo día de este mes es lunes}\}$ .

2 Discutir las dificultades que pueden surgir al usar el método de numeración en los siguientes conjuntos.

- (i) El conjunto de las ovejas en un campo.
- (ii) El conjunto de los antepasados de uno.
- (iii) El conjunto de los enteros positivos pares.

3 Demostrar que si  $|X| = n$  y existe una biyección de  $X$  en  $Y$ , entonces  $|Y| = n$ .

## 2.4 El principio de las cajas

El teorema 2.3 que hemos demostrado para justificar nuestra definición de cardinalidad, puede usarse también en situaciones más prácticas. Supongamos que tenemos un conjunto  $X$ , a cuyos elementos nos referiremos como "objetos", y un conjunto  $Y$  cuyos elementos son "cajas". Una *distribución* de los objetos en las cajas es simplemente una función  $f$  de  $X$  en  $Y$ : si el objeto  $x$  va a parar a la caja  $y$ , entonces  $f(x) = y$ . Por ejemplo, la distribución de la figura 2.9 corresponde a la función que se muestra en la derecha.

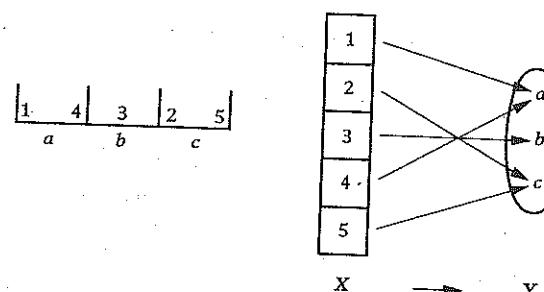


Fig. 2.9 Una distribución y su correspondiente función.

En este modelo, la función es exhaustiva si cada caja recibe al menos un objeto, e inyectiva si ninguna caja recibe más de un objeto. Ahora bien, está claro que si hay más objetos que cajas, entonces alguna caja debe recibir al menos dos objetos; en otras palabras, la función no puede ser inyectiva. Formalmente, esto es una consecuencia del teorema 2.3. En efecto, supongamos que  $|X| = m$  e  $|Y| = n$ , con  $m > n$ ; entonces una inyección de  $X$  en  $Y$  nos daría una inyección de  $\mathbb{N}_m$  en  $\mathbb{N}_n$ , lo que, según el teorema, es imposible. Esta observación se conoce comúnmente como el principio de las cajas:

*si se distribuyen  $m$  objetos en  $n$  cajas y  $m > n$ , entonces al menos una de las cajas recibe como mínimo dos objetos.*

Existen muchas aplicaciones obvias del principio de las cajas, como las siguientes:

(i) En un conjunto de 13 o más personas, al menos dos de ellas han nacido en el mismo mes.

(ii) En un conjunto de 51 o más personas nacidas en los Estados Unidos, al menos dos han nacido en el mismo estado.

(iii) En un conjunto de un millón de personas, al menos dos tienen el mismo número de cabellos.

También hay aplicaciones más sutiles.

**Ejemplo.** Demostrar que si  $X$  es un conjunto de personas, existen dos elementos de  $X$  que tienen el mismo número de amigos en  $X$ . (Se supone que si  $x$  es amigo de  $x'$ , entonces  $x'$  lo es de  $x$ .)

**SOLUCIÓN:** Consideremos la función  $f$  definida en  $X$  mediante la regla

$$f(x) = \text{número de amigos de } x \text{ en } X,$$

para cada  $x$  de  $X$ . Si  $|X| = m$ , los posibles valores de  $f(x)$  son  $0, 1, \dots, m - 1$ , ya que los amigos de  $x$  pueden ser cualquier elemento de  $X$  salvo el propio  $x$ . Tenemos, pues, una función  $f$  de  $X$  en el conjunto  $Y = \{0, 1, \dots, m - 1\}$ .

Llegados a este punto, no podemos aplicar directamente el principio de las cajas, ya que  $Y$  tiene el mismo cardinal que  $X$ . Sin embargo, si hay una persona  $x^*$  que tiene  $m - 1$  amigos, entonces todos son amigos de  $x^*$  y no hay nadie sin amigos. En otras palabras, los números  $m - 1$  y 0 no pueden ser ambos valores de  $f$ , de donde  $f$  es una función de un conjunto de tamaño  $m$  en uno de tamaño  $m - 1$  (o menos), y el principio de las cajas nos dice que existen al menos dos personas  $x_1$  y  $x_2$  tales que  $f(x_1) = f(x_2)$ , tal como queríamos demostrar.  $\square$

### Ejercicios 2.4

1 Un hombre ciego tiene un montón de 10 calcetines grises y 10 calcetines marrones en un cajón. ¿Cuántos ha de coger para asegurarse de que entre ellos hay un par que hace juego? ¿Cuántos ha de coger para asegurarse de que hay un par gris?

2 Se toman cinco puntos en el interior de un triángulo equilátero de lado 1. Demostrar que al menos un par de puntos están a una

distancia menor que  $1/2$ . [Indicación: dividir el triángulo en cuatro partes convenientes.]

3 Demostrar que en un conjunto de 12 enteros hay dos cuya diferencia es divisible por 11.

4 Sea  $|X|$  un subconjunto de  $\{1, 2, \dots, 2n\}$ , y sea  $Y$  el conjunto de números impares  $\{1, 3, \dots, 2n - 1\}$ . Se define una función  $f : X \rightarrow Y$  mediante la regla

$$f(x) = \text{máximo entero impar que divide a } x.$$

Demostrar que si  $|X| \geq n + 1$ , entonces  $f$  no es una inyección, y deducir que en este caso  $X$  contiene dos enteros distintos  $x_1$  y  $x_2$  tales que  $x_1 | x_2$ .

5 Demostrar que es posible hallar un subconjunto  $X$  de  $\{1, 2, \dots, 2n\}$  con  $n$  elementos, tal que ningún elemento de  $X$  divide a ningún otro elemento.

## 2.5 ¿Finito o infinito?

Hemos tenido cuidado en evitar las palabras “finito” e “infinito” hasta el momento, pero ahora estamos en condiciones de dar una definición formal.

**Definición.** Un conjunto  $X$  es **finito** si es vacío o si  $|X| = n$  para algún entero positivo  $n$ . Un conjunto que no es finito se dice que es **infinito**.

Según la definición,  $X$  es infinito si no es vacío y no existe ninguna biyección de  $\mathbb{N}_n$  en  $X$  con  $n$  entero positivo. Por supuesto, el candidato más evidente a conjunto infinito es el propio  $\mathbb{N}$ , y empezaremos por convencernos de que  $\mathbb{N}$  es efectivamente infinito de acuerdo con nuestra definición.

Supongamos que no sabemos si  $\mathbb{N}$  es finito o infinito. Ciertamente no es vacío, ya que contiene el 1. Si  $\mathbb{N}$  fuera finito, según la definición existiría una correspondencia biyectiva con un conjunto de la forma  $\{1, 2, \dots, n\}$ , y podríamos enumerar sus elementos como  $i_1, i_2, \dots, i_n$ .

Ahora bien,  $i_1 + i_2 + \dots + i_n + 1$  es un elemento de  $\mathbb{N}$  (axioma I1) estrictamente mayor que cualquier entero  $i_r$  de nuestra lista. (Ejercicio: explicar cómo se demostraría utilizando los axiomas I2, I3 e I11.) Nuestra lista no es completa y la suposición de que  $\mathbb{N}$  es finito ha de ser falsa:  $\mathbb{N}$  es infinito.

**Ejemplo.** El conjunto  $P$  de los números primos es infinito.

**SOLUCIÓN:** Puesto que 2 es primo,  $P$  no es vacío. Supongamos que  $P$  es finito, de forma que los primos, al estar en correspondencia biyectiva con un conjunto  $\{1, 2, \dots, n\}$ , pueden darse como una lista  $p_1, p_2, \dots, p_n$ . Vamos a demostrar que la lista no puede contener a todos los primos.

Consideremos el entero positivo

m = p\_1 p\_2 \cdots p\_n + 1.

Ninguno de los primos  $p_1, p_2, \dots, p_n$  divide a  $m$ ; por otra parte, sabemos por el apartado 1.8 que  $m$  factoriza de forma única en números primos. Esta factorización debe contener primos distintos de  $p_1, p_2, \dots, p_n$ , de donde la lista es incompleta.  $\square$

Mucha gente tiene la vaga idea de que, dado un conjunto infinito, podemos proseguir la técnica de contar enumerando indefinidamente sin llegar nunca al final. El siguiente teorema expresa esta idea de una manera más precisa.

**Teorema 2.5.** Un conjunto  $X$  no vacío es infinito si, y sólo si, existe una inyección de  $\mathbb{N}$  en  $X$ .

**DEMOSTRACIÓN:** Si  $X$  es infinito, podemos definir una función  $f$  de  $\mathbb{N}$  en  $X$  recursivamente de la manera siguiente. Tómese como  $f(1)$  cualquier elemento de  $X$ ; habiendo definido  $f(1), \dots, f(k)$ , tómese  $f(k+1)$  cualquier elemento de  $X$  diferente de  $f(1), \dots, f(k)$ . Esto significa que no hay dos valores de  $f$  iguales, con lo que  $f$  es inyectiva. Además, la definición de  $f(k+1)$  siempre es posible, puesto que si no hubiese valores disponibles para  $f(k+1)$ , debería ser  $X = \{f(1), \dots, f(k)\}$  y  $f$  sería una biyección de  $\mathbb{N}_n$  en  $X$ , contrariamente a la hipótesis de que  $X$  es infinito.

Recíprocamente, supongamos que existe una inyección  $f : \mathbb{N} \rightarrow X$ . Si  $X$  fuera finito, deberíamos tener una biyección  $\beta : \mathbb{N}_n \rightarrow X$  para algún entero positivo  $n$ , y por lo tanto una cadena de inyecciones

$$\mathbb{N}_{n+1} \xrightarrow{i} \mathbb{N} \xrightarrow{f} X \xrightarrow{\beta^{-1}} \mathbb{N}_n,$$

donde  $i$  es la función de inclusión. Ahora bien, la composición de estas inyecciones es una inyección de  $\mathbb{N}_{n+1}$  en  $\mathbb{N}_n$ , en oposición al teorema 2.3 (una vez más). Por lo tanto,  $X$  ha de ser infinito.  $\square$

Según el teorema 2.5, dado un conjunto infinito  $X$ , siempre podemos intentar “contarlo” construyendo una inyección  $f$  de  $\mathbb{N}$  en  $X$ . Pueden producirse dos resultados. En algunos casos, seremos capaces de construir  $f$  de forma que cualquier elemento de  $X$  reciba eventualmente un número. De ser así,  $f$  es exhaustiva además de inyectiva (y, en consecuencia, biyectiva), y en este caso decimos que  $X$  es **enumerable**. Por el contrario, puede ser imposible construir una biyección entre  $\mathbb{N}$  y  $X$ , y en este caso decimos que  $X$  es **no numerable**.

Repitamos brevemente las distinciones entre los términos finito e infinito, numerable y no numerable. Si existe un recuento que termina, el conjunto es *finito* o, en otras palabras, puede ser *contado*. Si existe un recuento que no termina pero que puede alcanzar eventualmente cualquier elemento, el conjunto es *infinito* y *enumerable*. De manera aproximada, la matemática discreta trata de los conjuntos finitos o numerables, mientras que el cálculo y el análisis tratan con conjuntos no numerables como el conjunto  $\mathbf{R}$  de los números reales.

Acabaremos este capítulo con una advertencia. Las propiedades de los conjuntos finitos nos son muy conocidas y por eso nuestra intuición es una buena guía para tratar con ellos. Por ejemplo, aceptamos sin discusión la afirmación de que si  $A$  es un subconjunto de un conjunto finito  $B$ , entonces  $A$  es finito y  $|A| \leq |B|$ . (De hecho, demostrarlo es algo intrincado, pero una vez más, el ubicuo teorema 2.3.) Por otra parte, la intuición puede ser una mala guía si tratamos con conjuntos infinitos. Esto es así porque las definiciones lógicamente consistentes halladas por los matemáticos no siempre se corresponden con nuestra experiencia de los conjuntos, necesariamente finitos.

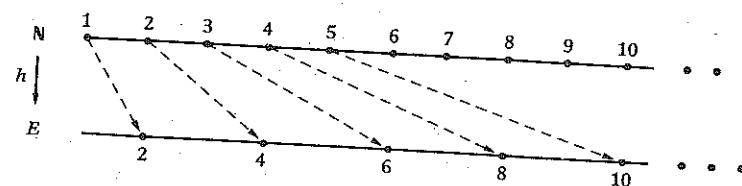


Fig. 2.10 ¡La función  $h : \mathbb{N} \rightarrow E$  es una biyección!

Veamos un ejemplo sobre el extraño comportamiento de los conjuntos

infinitos. Sea  $E$  el conjunto de los enteros positivos pares,  $E = \{2, 4, 6, \dots\}$ . Es evidente que la función  $h$  de  $\mathbb{N}$  en  $E$  definida por  $h(n) = 2n$  es una *biyección* (figura 2.10), y que  $E$  es un subconjunto *propio* del conjunto  $\mathbb{N}$ , es decir, un conjunto que no es todo  $\mathbb{N}$ . Así pues, un conjunto infinito puede tener un subconjunto propio que está en correspondencia biyectiva con el conjunto total.

### Ejercicios 2.5

1 Demostrar que cada uno de los conjuntos siguientes  $X$  es infinito construyendo una biyección de  $\mathbb{N}$  en  $X$ :

$$(i) \mathbb{Z}, \quad (ii) \{x \in \mathbb{Z} \mid x < 0\}, \quad (iii) \{n \in \mathbb{N} \mid n \geq 10^6\}.$$

2 Demostrar que la función  $f : \mathbb{N} \rightarrow \mathbb{Z}$  definida por

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par,} \\ -(n-1)/2 & \text{si } n \text{ es impar,} \end{cases}$$

es una biyección. Utilizar este resultado para mostrar otro ejemplo del “comportamiento extraño” al que nos referímos al final del párrafo anterior.

3 Cualquier primo salvo 2 y 3 es de la forma  $6m + 1$  o  $6m + 5$  para algún entero  $m$ . Utilizar el método de Euclides para demostrar que el conjunto de los primos de la forma  $6m + 5$  es **infinito**. [Indicación: sustituir el  $+1$  de la construcción de Euclides por  $-1$ .]

4 Utilizar el teorema 2.5 para demostrar que si  $X$  es un subconjunto de  $Y$  y  $X$  es infinito, entonces  $Y$  es infinito.

5 Sea  $X$  un subconjunto no vacío de  $\mathbb{Z}$  que no tiene mínimo. Demostrar que podemos elegir una sucesión  $x_1, x_2, \dots$  de elementos de  $X$  tal que  $x_n < x_{n-1}$  ( $n \in \mathbb{N}$ ). Deducir que  $X$  es infinito.

6 De acuerdo con el ejercicio 5, un subconjunto  $S$  *finito* no vacío de  $\mathbb{Z}$  ha de tener un mínimo, al que denotaremos por  $\min S$ . Demostrar que si  $S$  y  $T$  son subconjuntos finitos no vacíos de  $\mathbb{Z}$  entonces

$$\min(S \cup T) \leq \min S,$$

$$\min(S \cap T) \geq \min S.$$

Formular propiedades parecidas para el máximo de  $\varsigma$  (en condiciones adecuadas).

## 2.6 Ejercicios diversos

1 ¿Cuál de las siguientes funciones de  $\mathbf{Z}$  en  $\mathbf{Z}$  son exhaustivas, cuáles son inyectivas y cuáles son biyectivas?

$$(i) f(x) = 1 + x^2, \quad (ii) g(x) = 1 + x^3, \quad (iii) h(x) = 1 + x^2 + x^3.$$

2 Sea  $X$  un conjunto con  $|X| = 3$ . ¿Cuántas biyecciones  $f$  distintas existen de  $X$  en  $X$ ? ¿Cuántas de ellas satisfacen  $f = f^{-1}$ ?

3 Demostrar que si  $X$  es un conjunto finito y la función  $g : X \rightarrow X$  es una inyección, entonces  $g$  es una biyección.

4 Demostrar que si  $X$  es un conjunto finito y la función  $g : X \rightarrow X$  es exhaustiva, entonces  $g$  es biyectiva.

5 Sea  $X$  un conjunto finito y  $f : X \rightarrow X$  una función tal que  $g^2(x) = x$  para todo  $x \in X$ . Demostrar que  $g$  es una biyección.

6 Nos referiremos a los siguientes subconjuntos de  $\mathbf{Z}$  como *bloques*:

$$\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}.$$

Se define

$$f(x, y) = \begin{cases} z & \text{si } x \neq y \text{ y } \{x, y, z\} \text{ es un bloque,} \\ x & \text{si } x = y. \end{cases}$$

¿Es  $f$  una función? ¿Es inyectiva?

7 Demostrar que si se eligen cinco puntos cualesquiera en un cuadrado de lado 2, al menos dos de ellos se encuentran a una distancia no superior a  $\sqrt{2}$ .

8 Demostrar que si se eligen diez puntos cualesquiera en un triángulo equilátero de lado 1, al menos dos de ellos se encuentran a una distancia no superior a  $1/3$ .

9 ¿Cuántos puntos han de elegirse en un cuadrado de lado 2 para asegurar que al menos dos de ellos estarán a una distancia no superior a  $\sqrt{2}/n$ ?

10 Demostrar que en un conjunto de 172 enteros existe al menos un par cuya diferencia es divisible por 171. ¿Es cierto el resultado si cambiamos "diferencia" por "suma"?

11 Demostrar que el conjunto de los enteros positivos cuyos dígitos (en la representación ordinaria en base 10) son todos distintos es finito. ¿Cuántos hay?

12 Un *punto reticular* en el espacio tridimensional es un punto que tiene coordenadas enteras. Demostrar que dados 9 puntos reticulares, existe al menos un par de ellos tal que el punto medio del segmento que los une es también un punto reticular.

13 Un jugador de golf tiene  $d$  días para preparar un torneo y debe practicar jugando al menos un recorrido al día. Para evitar el cansancio, no debe jugar más de  $m$  recorridos en total. Demostrar que si  $r$  es tal que  $1 \leq r \leq 2d - m - 1$ , entonces existe una sucesión de días consecutivos en los que juega exactamente  $r$  recorridos.

14 Sea  $x_1, x_2, \dots, x_r$  una sucesión de enteros distintos. Para cada  $i$  ( $1 \leq i \leq r$ ) sea  $m_i$  la longitud de la mayor subsucesión creciente que empieza por  $x_i$  y sea  $n_i$  la longitud de la mayor subsucesión decreciente que empieza por  $x_i$ . Demostrar que la función que asigna a  $i$  el par  $(m_i, n_i)$  es inyectiva.

Deducir que una sucesión de  $mn + 1$  enteros distintos ha de contener una subsucesión creciente de longitud  $m$ , o bien una subsucesión decreciente de longitud  $n$ .

15 Demostrar que un subconjunto de un conjunto numerable es finito o numerable.

16 Demostrar que la unión de dos conjuntos numerables es numerable.

17 Demostrar que la unión de una colección numerable de conjuntos numerables es numerable.

18 Sea  $X$  un conjunto cualquiera y sea  $Y$  el conjunto de todos los subconjuntos de  $X$ . Demostrar que no existe ninguna biyección entre  $X$  e  $Y$ .

19 Demostrar que el conjunto de todos los subconjuntos de  $\mathbf{N}$  es un conjunto no numerable.

20 Demostrar que si  $A$  es un subconjunto de un conjunto finito  $B$ , entonces  $A$  es finito y  $|A| \leq |B|$ .

### 3 Principios enumerativos

#### 3.1 El principio de la adición

Uno de los temas principales de este libro es el desarrollo de técnicas efectivas para contar un conjunto finito  $X$ . Cuando  $X$  aparece en un problema complejo, pueden ser necesarios métodos de enumeración bastante alejados de la técnica de señalar y numerar utilizada para construir una biyección entre  $\mathbf{N}_n$  y  $X$ . En este capítulo empezaremos a desarrollar tales métodos.

Nuestra primera regla es tan sencilla que ha sido utilizada en la práctica desde el comienzo de la civilización. Sólo en tiempos recientes, y en el contexto de un desarrollo matemático estricto del tema, ha recibido un tratamiento formal.

**Teorema 3.1.** Si  $A$  y  $B$  son conjuntos finitos no vacíos disjuntos (es decir,  $A \cap B = \emptyset$ ), entonces

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

**DEMOSTRACIÓN:** Dado que  $A$  y  $B$  son finitos y no vacíos, podemos escribirlos en forma de lista de la manera estándar:

$$A = \{a_1, a_2, \dots, a_r\}, \quad B = \{b_1, b_2, \dots, b_s\}.$$

Puesto que  $A$  y  $B$  son disjuntos,  $A \cup B$  puede listarse de forma similar:

$$A \cup B = \{c_1, c_2, \dots, c_r, c_{r+1}, \dots, c_{r+s}\},$$

donde

$$c_i = a_i \quad (1 \leq i \leq r) \quad \text{y} \quad c_{r+i} = b_i \quad (1 \leq i \leq s).$$

Así pues,  $|A \cup B| = |A| + |B|$  como se afirmaba.

Está claro que la regla sigue siendo válida si  $A$  o  $B$  (o ambos) son vacíos. Aún más, la regla puede extenderse a la unión de un número cualquiera de conjuntos disjuntos  $A_1, A_2, \dots, A_n$  de forma evidente:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

La demostración es un sencillo ejercicio utilizando el principio de inducción (ejercicio 3.1.3).

Una simple aplicación de esta regla proporciona una forma ligeramente más general del principio de las cajas que el dado en el apartado 2.4. Supongamos que un cierto número de objetos se distribuyen en  $n$  cajas, y que  $A_i$  denota el conjunto de los objetos que están en la caja  $i$ . Puesto que los conjuntos  $A_i$  son disjuntos, el número total de objetos es  $|A_1| + |A_2| + \dots + |A_n|$ , y si ninguna caja contiene más de  $r$  objetos, este número es como máximo

$$r + r + \dots + r = nr.$$

Dando la vuelta al argumento, hemos generalizado el principio de las cajas:

si se distribuyen  $m$  objetos en  $n$  cajas y  $m > nr$ ,  
entonces al menos una caja contiene como mínimo  $r + 1$  objetos.

**Ejemplo.** Demostrar que en un conjunto de seis personas hay tres que se conocen mutuamente o tres mutuamente extrañas.

**SOLUCIÓN:** Sea  $\alpha$  una de las personas y distribuyamos las otras cinco en dos "cajas", la caja 1 con la gente que conoce a  $\alpha$  y la caja 2 con las que le son extrañas. Como  $5 > 2 \times 2$ , una de las cajas contiene al menos tres personas.

Supongamos que la caja 1 contiene a  $\beta, \gamma$  y  $\delta$  (y posiblemente más gente). Si algún par de entre  $\{\beta, \gamma, \delta\}$  se conocen, digamos  $\beta$  y  $\gamma$ , entonces  $\{\alpha, \beta, \gamma\}$  es un conjunto de conocidos mutuos. Por otra parte, si ningún par de  $\{\beta, \gamma, \delta\}$  se conocen entre sí, el conjunto  $\{\beta, \gamma, \delta\}$  está formado por extraños mutuos.

Si es la caja 2 la que contiene tres o más personas, un argumento similar intercambiando conocidos y extraños nos lleva a la misma conclusión.

### Ejercicios 3.1

1 Las reglas del campeonato de baloncesto de la Universidad de Folornia requieren que los miembros de cada equipo hayan nacido el mismo mes. ¿Cuántos estudiantes de matemáticas son necesarios para garantizar que pueden formar un equipo?

2 ¿Qué falla en el siguiente argumento? Puesto que la mitad de los números entre 1 y 60 son múltiplos de 2, 30 de ellos no pueden ser primos; puesto que una tercera parte son múltiplos de 3, 20 de ellos no pueden ser primos. Por lo tanto, hay como máximo 10 primos.

3 Escribir una demostración (por inducción sobre  $n$ ) del hecho de que si  $A_1, A_2, \dots, A_n$  son conjuntos disjuntos, entonces

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

4 Demostrar que en un conjunto de 10 personas hay cuatro que se conocen mutuamente o tres mutuamente extrañas.

### 3.2 Contar conjuntos de pares

A menudo hemos de contar cosas que admiten una descripción más natural como pares de objetos que como objetos individuales. Supongamos, por ejemplo, que el Departamento de Matemáticas de la Universidad de Folornia ha de calcular su carga docente para este curso. Para ello el profesor McBrain construye una tabla como la tabla 3.2.1.

Tabla 3.2.1

	Cálculo	Mat. Discreta	...	Álgebra
Angus	✓	✓		
Benjamin		✓		
Clare	✓	✓		✓
...				
Zoot	✓	✓		✓

Cada fila de la tabla corresponde a un estudiante, cada columna a una asignatura, y si el estudiante  $x$  hace la asignatura  $y$ , se marca la posición correspondiente  $(x, y)$  de la tabla. El número total de marcas es la carga docente del departamento. En otras palabras, el problema es contar el conjunto  $S$  de pares  $(x, y)$  tales que el estudiante  $x$  hace la asignatura  $y$ . En general, dados dos conjuntos  $X$  e  $Y$  podemos definir el **conjunto producto**  $X \times Y$  como el conjunto de *todos* los pares ordenados  $(x, y)$ ; el problema general es contar subconjuntos  $S$  de  $X \times Y$ .

A partir de la tabla del profesor McBrain, está claro que hay dos formas de hacer el cálculo. Podemos contar el número de asignaturas que hace cada estudiante y sumar las cantidades, o podemos contar el número de estudiantes que hacen cada asignatura y sumar estas cantidades. Naturalmente, esperamos obtener el mismo resultado en cada caso.

Podemos precisar estas ideas de la manera siguiente: supongamos que se especifica un subconjunto  $S$  de  $X \times Y$  (donde  $X$  e  $Y$  son conjuntos finitos) mediante marcas en la forma usada por McBrain, tal como muestra la tabla 3.2.2.

Tabla 3.2.2

		$y$	...	Total fila
$x$		✓		✓
		✓		✓
	✓	✓		✓
	✓	✓	✓	✓
		✓		✓
Total columna			$c_y(S)$	$ S $

Con el primer método se cuentan las marcas en la fila  $x$  y se obtiene el total de la fila  $r_x(S)$  para cada  $x$  de  $X$ . El total general se obtiene sumando los totales por filas, es decir

$$|S| = \sum_{x \in X} r_x(S).$$

En el segundo método, se cuentan las marcas de la columna  $y$  para hallar el total  $c_y(S)$  para cada  $y$  de  $Y$ . El total general se obtiene sumando los totales por columnas:

$$|S| = \sum_{y \in Y} c_y(S).$$

El hecho de que tenemos dos expresiones distintas de  $|S|$  se utiliza a menudo en la práctica para comprobar los cálculos. El mismo hecho puede ser muy útil en la teoría, ya que a veces pueden obtenerse resultados inesperados igualando las dos expresiones. Pero antes de pasar a las aplicaciones, formularemos el principio y algunas de sus consecuencias más inmediatas.

**Teorema 3.2.** Sean  $X$  e  $Y$  conjuntos finitos no vacíos, y sea  $S$  un subconjunto de  $X \times Y$ . Entonces se cumplen los siguientes resultados:

(i) El cardinal de  $S$  viene dado por

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S),$$

donde  $r_x(S)$  y  $c_y(S)$  son los totales por filas y columnas descritos anteriormente.

(ii) Si  $r_x(S)$  es una constante  $r$ , independiente de  $x$ , y  $c_y(S)$  es una constante  $c$ , independiente de  $y$ , entonces

$$r|X| = c|Y|.$$

(iii) (El principio de la multiplicación) El cardinal de  $X \times Y$  es igual a

$$|X \times Y| = |X| \times |Y|.$$

**DEMOSTRACIÓN:** (i) El conjunto de “marcas en la fila  $x$ ” puede definirse formalmente como el conjunto de los pares de  $S$  cuyo primer componente es  $x$ , de forma que  $r_x(S)$  es el cardinal de este conjunto. Dado que los conjuntos son disjuntos, el principio de adición implica que  $|S|$  es igual a la suma de los números  $r_x(S)$ . El resultado para las columnas se demuestra de la misma manera.

(ii) Si  $r_x(S) = r$  para todo  $x \in S$ , entonces hay  $|X|$  términos en la primera expresión de  $|S|$ , todos ellos iguales a  $r$ . Por lo tanto,

$$|S| = r|X|.$$

Análogamente,  $|S| = c|Y|$  y el resultado está demostrado.

(iii) En el caso especial en que  $S = X \times Y$ , el total de cada fila es  $r_x(S) = |Y|$  para cada  $x$  de  $X$ . Según el apartado (ii), se tiene que  $|X \times Y| = |X| \times |Y|$ .  $\square$

**Ejemplo.** El profesor McBrain ha decretado que, por necesidades administrativas, cada estudiante ha de hacer exactamente cuatro asignaturas de entre siete posibles. Los profesores informan que el número de asistentes a las asignaturas es 52, 30, 30, 20, 25, 12, 18. ¿Qué puede deducirse?

**SOLUCIÓN:** Sea  $n$  el número total de estudiantes. Puesto que cada estudiante ha de asistir a cuatro asignaturas, la carga docente total calculada “por filas” es  $4n$ . Por otra parte, los totales “por columnas”, según los profesores, nos dan

$$4n = 52 + 30 + 30 + 20 + 25 + 12 + 18 = 187.$$

Pero esto es imposible, ya que 187 no es divisible por 4. Hemos de rechazar la idea de que los profesores se han equivocado al contar, así que la única conclusión posible es que algunos estudiantes faltan a clase, lo cual, ¡ay!, no es ninguna novedad.

### Ejercicios 3.2

1 En la clase de Análisis de la doctora Cynthia Angst, 32 de los estudiantes son chicos. Cada chico conoce a cinco de las chicas de la clase, y cada chica conoce a ocho de los chicos. ¿Cuántas chicas hay en la clase?

2 Supongamos que tenemos un cierto número de subconjuntos de  $N_8$  con la propiedad de que cada uno de ellos contiene cuatro elementos y de que cada elemento de  $N_8$  pertenece a tres subconjuntos exactamente. ¿Cuántos subconjuntos hay? Escribir una colección de subconjuntos que satisfaga las condiciones.

3 ¿Es posible hallar una colección de subconjuntos de  $N_8$  tal que cada uno de ellos tenga tres elementos y cada elemento de  $N_8$  pertenezca a cinco de los subconjuntos exactamente?

4 Si  $X_1, X_2, \dots, X_n$  son conjuntos, se define el **conjunto producto**  $X_1 \times X_2 \times \dots \times X_n$  como el conjunto de todas las  $n$ -plas ordenadas  $(x_1, x_2, \dots, x_n)$  con  $x_i \in X_i$  ( $1 \leq i \leq n$ ). Utilizar el principio de inducción para demostrar que

$$|X_1 \times X_2 \times \dots \times X_n| = |X_1| \times |X_2| \times \dots \times |X_n|.$$

5 Considérese un lenguaje muy sencillo que utiliza las 26 letras habituales pero en el que todas las palabras tienen cuatro letras. Se admite cualquier combinación de las letras, incluyendo repeticiones. ¿Cuántas palabras hay? ¿Cuántas de ellas no contienen la letra *b*?

### 3.3 La función de Euler

En este apartado demostraremos un teorema útil e importante utilizando únicamente los principios enumerativos más básicos.

El teorema tiene que ver con las propiedades de divisibilidad de los enteros. Recordemos que dos enteros  $x$  e  $y$  son *primos entre sí* si  $\text{mcd}(x, y) = 1$ . Para cada  $n \geq 1$ , sea  $\phi(n)$  el número de enteros  $x$  del intervalo  $1 \leq x \leq n$  tales que  $x$  y  $n$  son primos entre sí. Podemos calcular los primeros valores de  $\phi(n)$  construyendo una tabla (tabla 3.3.1).

La función  $\phi(n)$  se conoce como **función de Euler**, en recuerdo de Leonhard Euler (1707-1783). Si  $p$  es primo, todos los enteros  $1, 2, \dots, p-1$  son primos con  $p$ , de forma que

$$\phi(p) = p - 1 \quad \text{si } p \text{ es primo.}$$

En el apartado 4.4 obtendremos una fórmula general para  $\phi(n)$ .

Nuestro próximo objetivo es demostrar un resultado relativo a la suma de los valores  $\phi(d)$  para los divisores  $d$  de un entero positivo dado  $n$ . Por ejemplo, si  $n = 12$  los divisores de  $d$  son  $1, 2, 3, 4, 6$  y  $12$ , y obtenemos

$$\begin{aligned} \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) &= \\ 1 + 1 + 2 + 2 + 2 + 4 &= \\ 12. \end{aligned}$$

Demostraremos que la suma es siempre igual al entero  $n$ .

Tabla 3.3.1

$n$	Primo con $n$	$\phi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4

**Teorema 3.3.** Para cualquier entero positivo  $n$ ,

$$\sum_{d|n} \phi(d) = n.$$

**DEMOSTRACIÓN:** Sea  $S$  el conjunto de pares de enteros  $(d, f)$  que cumplen

$$d|n, \quad 1 \leq f \leq d \quad \text{y} \quad \text{mcd}(f, d) = 1.$$

La tabla 3.3.2 ilustra el conjunto  $S$  en el caso  $n = 12$ ; la “marca” que indica que  $(d, f)$  pertenece a  $S$  es un número cuyo significado explicaremos dentro de un momento. En general, el número de “marcas” en la fila  $d$  es precisamente el número de enteros  $f$  entre  $1$  y  $d$  tales que  $\text{mcd}(d, f) = 1$ , es decir,  $\phi(d)$ . Si contamos  $S$  por filas obtenemos

$$|S| = \sum_{d|n} \phi(d).$$

Para demostrar que  $|S| = n$ , construiremos una biyección  $\beta$  entre  $S$  y  $N_n$ . Dado un par  $(d, f)$  de  $S$  definimos

$$\beta(d, f) = fn/d.$$

En la tabla,  $\beta(d, f)$  es la “marca” de la fila  $d$  y columna  $f$ . Puesto que  $d|n$ , se trata de un número entero, y puesto que  $1 \leq f \leq d$ , está en  $N_n$ .

Tabla 3.3.2

d	f												$\phi(d)$
	1	2	3	4	5	6	7	8	9	10	11	12	
1	12												1
2	6												1
3	4	8											2
4	3		9										2
6	2			10									2
12	1				5	7			11				4
													12

Para demostrar que  $\beta$  es inyectiva, notemos que

$$\beta(d, f) = \beta(d', f') \Rightarrow fn/d = f'n/d' \Rightarrow fd' = f'd.$$

Pero  $f$  y  $d$  son primos entre sí, al igual que  $f'$  y  $d'$  y, como en el ejemplo del apartado 1.7, concluimos que  $d = d'$  y  $f = f'$ .

Para demostrar que  $\beta$  es exhaustiva, tomemos un  $x$  de  $\mathbb{N}_n$ . Sea  $g_x$  el mcd de  $x$  y  $n$ , y sean

$$d_x = n/g_x, \quad f_x = x/g_x.$$

Puesto que  $g_x$  es un divisor de  $x$  y de  $n$ , resulta que  $d_x$  y  $f_x$  son enteros, y puesto que es el mcd,  $d_x$  y  $f_x$  son primos entre sí. Ahora bien,

$$\beta(d_x, f_x) = f_x n / d_x = x,$$

de forma que  $\beta$  es exhaustiva. Por lo tanto,  $\beta$  es biyectiva y  $|S| = n$  como queríamos demostrar.  $\square$

### Ejercicios 3.3

- Hallar los valores de  $\phi(19)$ ,  $\phi(20)$  y  $\phi(21)$ .
- Demostrar que si  $x$  y  $n$  son primos entre sí, también lo son  $n - x$  y  $n$ . Deducir que  $\phi(n)$  es par si  $n \geq 3$ .

3 Demostrar que si  $p$  es primo y  $m$  un entero positivo, un entero  $x$  en el intervalo  $1 \leq x \leq p^m$  no es primo con  $p^m$  si, y sólo si, es un múltiplo de  $p$ . Deducir que  $\phi(p^m) = p^m - p^{m-1}$ .

4 Hallar un contraejemplo a la conjectura según la cual  $\phi(a)\phi(b) = \phi(ab)$  para cualesquiera enteros positivos  $a$  y  $b$ . Intentar modificar la conjectura de forma que no pueda ser contradicha.

### 3.4 Funciones, palabras y selecciones

Consideraremos funciones (no necesariamente biyectivas) definidas en un conjunto de enteros positivos  $\mathbb{N}_m$  y con valores en un cierto conjunto  $Y$ . Los valores de una función de este tipo determinan una  $m$ -pla

$$(f(1), f(2), \dots, f(m))$$

de elementos de  $Y$ . De acuerdo con la definición general de un conjunto producto (ejercicio 3.2.4) esta  $m$ -pla pertenece al conjunto  $Y \times Y \times \dots \times Y$  ( $m$  factores), al que denotaremos por  $Y^m$ . Cada elemento de  $Y^m$  es de la forma  $(y_1, y_2, \dots, y_m)$  y corresponde a una función  $f$  de  $\mathbb{N}_m$  en  $Y$  definida por las ecuaciones

$$f(1) = y_1, \quad f(2) = y_2, \dots, f(m) = y_m.$$

Estas reflexiones nos llevan a la conclusión de que una función de  $\mathbb{N}_m$  en  $Y$  es lógicamente lo mismo que un elemento del conjunto producto  $Y^m$ .

Hay otra manera de ver esta relación, muy útil en la práctica. Si pensamos en los elementos de  $Y$  como letras de un alfabeto, la sucesión  $f(1), f(2), \dots, f(m)$  puede verse como las  $m$  letras de una palabra. Por ejemplo, si  $Y$  es el alfabeto  $\{a, b, c, d\}$ , las palabras *cab* y *dad* corresponden a las funciones  $f$  y  $g$  definidas por

$$\begin{aligned} f(1) &= c, & f(2) &= a, & f(3) &= b, \\ g(1) &= d, & g(2) &= a, & g(3) &= d. \end{aligned}$$

La función  $f$ , el triplete  $(c, a, b)$  y la palabra *cab* son formalmente idénticas, de forma que definimos una **palabra de longitud  $m$**  en el **alfabeto  $Y$**  como una función de  $\mathbb{N}_m$  en  $Y$ .

Antes de desarrollar esta idea, demostraremos el resultado más general sobre cómo contar conjuntos de funciones.

**Teorema 3.4.** Sean  $X$  e  $Y$  conjuntos finitos no vacíos y sea  $F$  el conjunto de las funciones de  $X$  en  $Y$ . Si  $|X| = m$  y  $|Y| = n$ , entonces

$$|F| = n^m.$$

**DEMOSTRACIÓN:** Sea  $X = \{x_1, x_2, \dots, x_m\}$ . Cada elemento  $f$  de  $F$  es una función de  $X$  en  $Y$  y está determinada únicamente por la  $m$ -pla de sus valores  $(f(x_1), f(x_2), \dots, f(x_m))$ . Esta  $m$ -pla pertenece a  $Y^m$ , de forma que

$$|F| = |Y^m| = n^m. \quad \square$$

De forma equivalente, podemos decir que el número de palabras de longitud  $m$  de un alfabeto  $Y$  de  $n$  símbolos es  $n^m$ . Por ejemplo, hay  $26^3$  palabras de tres letras en el alfabeto latino (suponiendo, desde luego, que no hay ninguna restricción en el léxico).

Hay otra forma importante de interpretar una función de  $N_m$  en  $Y$  o, equivalentemente, una palabra de longitud  $m$  en el alfabeto  $Y$ . Pensemos en el trabajo de un impresor en la época de la composición manual. Para componer la palabra *cab*, primero selecciona una *c* de su caja correspondiente, después una *a* y finalmente una *b*. Suponemos que tiene tantas letras como hagan falta, de forma que para componer *dad*, por ejemplo, selecciona una *d*, una *a* y después otra *d*. Cada palabra representa una selección ordenada de letras del alfabeto  $Y = \{a, b, \dots, z\}$ , y se permiten tantas repeticiones como se quiera.

En general, podemos decir que una función de  $N_m$  en  $Y$  es un modelo matemático de una *selección ordenada con repeticiones* de  $m$  objetos del conjunto  $Y$ . Por el teorema 3.4, el número de selecciones es  $n^m$ , donde  $|Y| = n$ . (En los apartados siguientes veremos cómo tratar con selecciones ordenadas o no, con o sin repeticiones.)

Esta regla sencilla para contar funciones (o palabras, o selecciones ordenadas con repetición) puede aplicarse para obtener resultados bastante generales, tal como muestra el siguiente ejemplo:

**Ejemplo:** Si  $X$  es un conjunto con  $n$  elementos, demostrar que el número total de subconjuntos de  $X$  es  $2^n$ .

**SOLUCIÓN:** Sea  $X = \{x_1, x_2, \dots, x_n\}$  y sea  $Y$  el alfabeto  $\{0, 1\}$ . Un subconjunto de  $X$  corresponde a una palabra de longitud  $n$  en  $Y$ , definida por

$$S(i) = \begin{cases} 0 & \text{si } x_i \notin S, \\ 1 & \text{si } x_i \in S. \end{cases}$$

Por ejemplo, si  $n = 7$  y  $S = \{x_2, x_4, x_5\}$ , la palabra es 0101100. Podemos pensar convenientemente en el 0 como una representación de **falso** y en el 1 como **cierto**; la palabra se construye mirando todos los elementos de  $X$  y anotando **cierto** si es de  $S$  y **falso** si no lo es. En consecuencia, el número de subconjuntos distintos de  $X$  es el mismo que el número de palabras de longitud  $n$  en el alfabeto  $\{0, 1\}$ , es decir,  $2^n$ .  $\square$

### Ejercicios 3.4

1. ¿Cuántas banderas nacionales pueden construirse con tres barras verticales iguales y los colores rojo, blanco, azul y verde? (Se supone que los colores pueden repetirse y que uno de los lados verticales de la bandera se distingue como el "lado del asta".)
2. Escribir todos los subconjuntos de  $\{a, b, c\}$  y usar la correspondencia dada en el ejemplo para comprobar que la lista es completa.
3. Una llave se fabrica haciendo incisiones de profundidad variable en ciertas posiciones de una llave virgen. Si hay ocho profundidades posibles, ¿cuántas posiciones se necesitan para fabricar un millón de llaves diferentes? [Indicación: para facilitar el cálculo, utilícese el hecho de que  $2^{10}$  es ligeramente mayor que  $10^3$ .]
4. Demostrar que el conjunto de los subconjuntos de un conjunto de 8 elementos posee más de  $10^{76}$  subconjuntos.

### 3.5 Inyecciones como selecciones ordenadas sin repetición

Con frecuencia hay que hacer selecciones ordenadas *sin repetición*. Aunque un impresor debe tener una cantidad ilimitada de letras disponible, puede ocurrir que sólo haya un objeto de cada clase. Por ejemplo, si estamos

seleccionando un equipo de béisbol según el orden de bateo, ningún jugador puede ser seleccionado más de una vez.

El lenguaje de las funciones proporciona directamente un modelo para esta situación. Hemos visto que una selección ordenada de  $m$  cosas de un conjunto  $Y$  corresponde a una función  $f$  de  $\mathbb{N}_m$  en  $Y$ , donde  $f(1)$  es el primer elemento de  $Y$  seleccionado, etc. Si permitimos repeticiones, es posible que un objeto sea seleccionado más de una vez, de forma que  $f(r) = f(s)$  para  $r$  y  $s$  de  $\mathbb{N}_m$  distintos. Si no permitimos esta situación, es decir, si  $f$  es inyectiva, tenemos un modelo de una selección ordenada sin repetición.

**Teorema 3.5.** El número de selecciones ordenadas sin repetición de  $m$  objetos de un conjunto  $Y$  de tamaño  $n$  es el número de inyecciones de  $\mathbb{N}_m$  en  $Y$ , es decir,

$$n(n-1)(n-2)\cdots(n-m+1). \quad \square^1$$

**DEMOSTRACIÓN:** Cada inyección  $i$  de  $\mathbb{N}_m$  en  $Y$  queda determinada de forma única por la selección ordenada de los valores distintos  $i(1), i(2), \dots, i(m)$ . La primera selección  $i(1)$  puede ser cualquiera de los  $n$  objetos de  $Y$ . Puesto que no están permitidas repeticiones, la segunda selección  $i(2)$  debe ser uno de los  $n-1$  objetos restantes. Igualmente, hay  $n-2$  posibilidades para  $i(3)$ , y así sucesivamente. Cuando llegamos a la selección de  $i(m)$ , ya han sido seleccionados  $m-1$  objetos, de forma que  $i(m)$  ha de ser uno de los  $n-(m-1)$  restantes. Así pues, el número total es el que se afirma en el teorema.  $\square$

Por ejemplo, si tenemos un banquillo de 16 jugadores, el número de maneras de seleccionar un equipo de béisbol según el orden de bateo es

$$16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8 = 4\,151\,347\,200.$$

### Ejercicios 3.5

- 1 ¿De cuántas maneras podemos seleccionar un orden de bateo de 11 jugadores con un banquillo de 14?
- 2 ¿Cuántas letras de cuatro palabras pueden hacerse con un alfabeto de 10 símbolos si no hay restricciones de léxico salvo en que ninguna letra puede aparecer más de una vez?

3 Explicar brevemente cómo fabricar sistemáticamente una lista, con todas las selecciones ordenadas sin repetición de tres objetos del conjunto  $\{a, b, c, d, e, f\}$ .

4 Sea  $(n)_m = n(n-1)\cdots(n-m+1)$ . Demostrar que

$$(n)_m \times (n-m)_{r-m} = (n)_r$$

para enteros positivos cualesquiera  $n > r > m$ , interpretando el resultado en términos de selecciones ordenadas.

### 3.6 Permutaciones

Una **permutación** de un conjunto finito no vacío  $X$  es una biyección de  $X$  en sí mismo. (A menudo tomaremos  $X$  igual a  $\mathbb{N}_n = \{1, 2, \dots, n\}$ .) Por ejemplo, una permutación de  $\mathbb{N}_5$  puede ser la función  $\alpha$  definida por las ecuaciones

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(3) = 5, \quad \alpha(4) = 1, \quad \alpha(5) = 3.$$

Una biyección de un conjunto en sí mismo es necesariamente una inyección y, recíprocamente, si el conjunto es finito, una inyección es una biyección (ejercicio 2.6.3). Así pues, el número de permutaciones de un  $n$ -conjunto es el mismo que el número de inyecciones de  $\mathbb{N}_n$  en sí mismo y, por el teorema 3.5, este número es

$$n \times (n-1) \times \cdots \times 1 = n!.$$

Denotaremos el conjunto de todas las permutaciones de  $\mathbb{N}_n$  por  $S_n$ . Por ejemplo,  $S_3$  contiene las siguientes  $3! = 6$  permutaciones:

1 2 3	1 2 3	1 2 3
↓ ↓ ↓	↓ ↓ ↓	↓ ↓ ↓
1 2 3	1 3 2	2 1 3
1 2 3	1 2 3	1 2 3
↓ ↓ ↓	↓ ↓ ↓	↓ ↓ ↓
2 3 1	3 1 2	3 2 1

En la práctica, los elementos de  $S_n$  suelen tener una interpretación concreta. Podemos interpretarlos, como hicimos en el apartado previo, como "selecciones ordenadas sin repetición" donde, en este caso, seleccionamos los elementos de  $\{1, 2, \dots, n\}$  en un cierto orden hasta que no quede ninguno. Una interpretación parecida es que una permutación efectúa una reordenación de  $\{1, 2, \dots, n\}$ ; por ejemplo, la permutación  $\alpha$  dada anteriormente efectúa la reordenación de 12345 en 24513, es decir:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 1 & 3 \end{array}$$

En ciertas circunstancias es conveniente mirar una permutación y la correspondiente reordenación como una misma cosa, pero esto puede producir dificultades al considerar reordenaciones sucesivas. En cualquier caso, es recomendable recordar que

*una permutación es un tipo de función.*

Queda claro cómo combinar permutaciones cuando las tratamos como funciones. Sea  $\alpha$  la permutación de  $N_5$  anterior y  $\beta$  la permutación dada por

$$\beta(1) = 3, \quad \beta(2) = 5, \quad \beta(3) = 1, \quad \beta(4) = 4, \quad \beta(5) = 2.$$

La función compuesta  $\beta\alpha$  es la permutación definida por  $\beta\alpha(i) = \beta(\alpha(i))$  ( $1 \leq i \leq 5$ ), es decir,

$$\beta\alpha(1) = 5, \quad \beta\alpha(2) = 4, \quad \beta\alpha(3) = 2, \quad \beta\alpha(4) = 3, \quad \beta\alpha(5) = 1.$$

(Recuérdese que, como siempre,  $\beta\alpha$  significa "primero  $\alpha$ , después  $\beta$ ".) En términos de reordenaciones tenemos

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 5 & 1 & 3 \\ \beta & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 4 & 2 & 3 & 1 \end{array}$$

La composición de permutaciones posee cuatro propiedades de la máxima importancia, que aparecen en el siguiente teorema. En la parte III del libro volveremos a estas propiedades en un contexto más general.

**Teorema 3.6.** *En el conjunto  $S_n$  de todas las permutaciones de  $\{1, 2, \dots, n\}$  se cumplen las siguientes propiedades.*

- (i) Si  $\pi$  y  $\sigma$  son de  $S_n$ , también lo es  $\pi\sigma$ .
- (ii) Para cualesquiera  $\pi$ ,  $\sigma$  y  $\tau$  de  $S_n$ ,

$$(\pi\sigma)\tau = \pi(\sigma\tau).$$

(iii) La función identidad, denotada por  $\text{id}$  y definida por  $\text{id}(r) = r$  para todo  $r$  de  $N_n$ , es una permutación y, para todo  $\sigma$  de  $S_n$ , tenemos que

$$\text{id}\sigma = \sigma\text{id} = \sigma.$$

(iv) Para toda permutación  $\sigma$  de  $S_n$  existe una permutación inversa  $\sigma^{-1}$  de  $S_n$  tal que

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = \text{id}.$$

**DEMOSTRACIÓN:** La afirmación (i) se desprende inmediatamente del hecho de que la composición de dos biyecciones es una biyección (teorema 2.2.1) y la (ii) es una propiedad estándar de la composición (ejercicio 2.1.4). La afirmación (iii) es evidente y la (iv) resulta del hecho de que toda biyección tiene una inversa (teorema 2.2.2).  $\square$

Es conveniente disponer de una notación más compacta para las permutaciones. Consideremos una vez más la permutación  $\alpha$  de  $\{1, 2, 3, 4, 5\}$  y notemos, en particular, que

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(4) = 1.$$

Así pues,  $\alpha$  envía el 1 al 2, el 2 al 4, y el 4 de vuelta al 1. Por esta razón decimos que los símbolos 1, 2 y 4 forman un *ciclo* de longitud 2 y escribimos

$$\alpha = (1\ 2\ 4)(3\ 5).$$

Esta es la notación de *ciclos* para  $\alpha$ . Cualquier permutación  $\pi$  de  $S_n$  puede escribirse en la notación de ciclos de la siguiente forma:

se empieza con un símbolo cualquiera (pongamos el 1) y se anota el efecto de  $\pi$  en él y en sus sucesores hasta llegar de nuevo al 1, de forma que tenemos un ciclo; se elige un símbolo que no haya aparecido todavía y construimos el ciclo que emana de él; se repite el proceso hasta que hayan aparecido todos los símbolos.

Por ejemplo, la notación en ciclos de la permutación  $\beta$  definida anteriormente es

$$\beta = (1\ 3)(2\ 5)(4),$$

donde hacemos notar que el símbolo 4 forma un ciclo en sí mismo “degenerado”, ya que  $\beta(4) = 4$ . En ciertas circunstancias, al escribir una permutación en la notación de ciclos, podemos omitir los ciclos de longitud 1, ya que corresponden a los símbolos que no se ven afectados por la permutación. Sin embargo, resulta útil *no* adoptar este convenio hasta que uno se haya familiarizado del todo con la notación.

Aunque la representación de una permutación en la notación de ciclos es esencialmente única, hay dos formas evidentes de cambiar la notación sin alterar la permutación. En primer lugar, cada ciclo puede empezar con uno cualquiera de sus símbolos —por ejemplo  $(7\ 8\ 2\ 1\ 3)$  y  $(1\ 3\ 7\ 8\ 2)$  describen el mismo ciclo. En segundo lugar, el orden de los ciclos no tiene importancia —por ejemplo  $(1\ 2\ 4)(3\ 5)$  es la misma permutación que  $(3\ 5)(1\ 2\ 4)$ . Lo importante es el número de ciclos, su longitud y la disposición de los símbolos dentro de los ciclos, y éstos están determinados de forma única. En consecuencia, la notación de ciclos nos da mucha información útil sobre una permutación.

**Ejemplo.** Se colocan doce cartas numeradas del 1 al 12 tal como se muestra abajo a la izquierda. Se van tomando en el orden de las filas y se vuelven a colocar, pero por columnas en lugar de por filas, de forma que aparecen como se muestra a la derecha.

1	2	3	1	5	9
4	5	6	2	6	10
7	8	9	3	7	11
10	11	12	4	8	12

¿Cuántas veces hay que repetir este proceso hasta que las cartas aparezcan en la posición inicial?

**SOLUCIÓN:** Sea  $\pi$  la permutación que lleva a cabo la reordenación; esto es,  $\pi(i) = j$  si la carta  $j$  aparece en la posición ocupada previamente por la carta  $i$ . Si utilizamos la notación en ciclos de  $\pi$ , obtenemos

$$\pi = (1\ 2\ 5\ 6\ 10\ 4)(3\ 9\ 11\ 8\ 7)(1\ 2).$$

Los ciclos degenerados  $(1)$  y  $(12)$  indican que las cartas 1 y 12 no cambian nunca de sitio. Los restantes ciclos tienen longitud 5, de forma que después de repetir el proceso 5 veces, todas las cartas volverán a estar en su sitio (compruébese). Otra manera de expresar el resultado es decir que  $\pi^5 = \text{id}$ , donde  $\pi^5$  significa efectuar cinco veces  $\pi$ .  $\square$

### Ejercicios 3.6

1 Escribir la notación de ciclos de la permutación que lleva a cabo la reordenación

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9 \end{array}$$

2 Sean  $\sigma$  y  $\tau$  dos permutaciones de  $\{1, 2, \dots, 8\}$  cuya representación en ciclos es

$$\sigma = (1\ 2\ 3)(4\ 5\ 6)(7\ 8), \quad \tau = (1\ 3\ 5\ 7)(2\ 6)(4\ 8).$$

Escribir los ciclos de  $\sigma\tau$ ,  $\tau\sigma$ ,  $\sigma^2$ ,  $\sigma^{-1}$ ,  $\tau^{-1}$ .

3 Resolver el problema planteado en el ejemplo cuando hay 20 cartas dispuestas en cinco filas de cuatro.

4 Demostrar que el número de elementos de  $S_4$  que tienen dos ciclos de longitud 2 es exactamente tres.

5 Sea  $K$  el subconjunto de  $S_4$  que contiene la permutación identidad  $\text{id}$  y las tres permutaciones  $\alpha_1$ ,  $\alpha_2$  y  $\alpha_3$  descritas en el ejercicio anterior. Escribir la “tabla de multiplicar” de  $K$ , donde la multiplicación se interpreta como la composición de permutaciones.

### 3.7 Ejercicios diversos

- 1 Una comisión de nueve personas ha de elegir un presidente, un secretario y un tesorero. ¿De cuántas maneras puede hacerlo? (Explicar con detalle qué se da por supuesto al formular la solución.)
- 2 En el juego del dominó, cada ficha puede representarse por el símbolo  $[x|y]$ , donde  $x$  e  $y$  son elementos del conjunto  $\{0, 1, 2, 3, 4, 5, 6\}$ . Los números  $x$  e  $y$  pueden ser iguales. Explicar por qué el total de fichas es 28 en lugar de 49.
- 3 ¿De cuántas maneras podemos elegir un cuadrado blanco y otro negro en un tablero de ajedrez de forma que los dos cuadrados no estén en la misma fila o en la misma columna?
- 4 ¿De cuántas formas podemos colocar ocho torres en un tablero de ajedrez de forma que ningún par de ellas estén en la misma fila o en la misma columna?
- 5 Supongamos que en una clase hay  $m$  chicas y  $n$  chicos. ¿De cuántas maneras podemos alinearlos de forma que todas las chicas estén juntas?
- 6 Si tenemos nueve subconjuntos distintos de  $N_{12}$ , cada uno con ocho elementos, y cada elemento de  $N_{12}$  pertenece al mismo número  $r$  de subconjuntos, ¿cuánto vale  $r$ ? ¿Es posible hallar nueve subconjuntos distintos de  $N_{12}$ , cada uno con siete elementos, de forma que cada elemento de  $N_{12}$  pertenezca al mismo número de subconjuntos?
- 7 ¿En cuántos números de teléfono de cinco cifras aparece alguna cifra más de una vez?
- 8 Calcular el número total de permutaciones  $\sigma$  de  $N_6$  que satisfacen  $\sigma^2 = \text{id}$ ,  $\sigma \neq \text{id}$ .

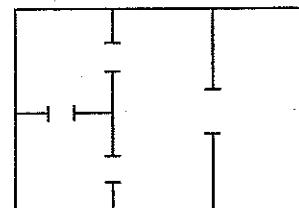


Fig. 3.1 Decoración de interiores.

- 9 Sean  $\alpha$  y  $\beta$  son permutaciones de  $N_9$  cuya representación en ciclos es

$$\alpha = (1\ 2\ 3\ 7)(4\ 9)(5\ 8)(6) \quad \beta = (1\ 3\ 5)(2\ 4\ 6)(7\ 8\ 9).$$

Escribir la notación en ciclos de  $\alpha\beta$ ,  $\beta\alpha$ ,  $\alpha^2$ ,  $\beta^2$ ,  $\alpha^{-1}$  y  $\beta^{-1}$ .

- 10 Se han de pintar las habitaciones de la casa que muestra la figura 3.1 de forma que las habitaciones que están conectadas por una puerta tengan colores distintos. ¿De cuántas maneras puede pintarse la casa si se dispone de  $n$  colores?
  - 11 Sea  $X_1 = \{0, 1\}$  y para  $i \geq 2$  defínase el conjunto  $X_i$  como el conjunto de subconjuntos de  $X_{i-1}$ . Hallar el menor valor de  $i$  para el cual  $|X_i| > 10^{100}$ .
  - 12 Supongamos que tenemos un conjunto de "dominó generalizado" en el que los números van de 0 a  $n$  y sea  $k$  un entero cualquiera entre 0 y  $n$ . Demostrar que el número de fichas  $[x|y]$  tales que  $x + y = n - k$  es igual al número para las cuales  $x + y = n + k$ .
  - 13 Para cada entero  $i$  con  $1 \leq i \leq n - 1$  se define  $\tau_i$  como la permutación de  $N_n$  que intercambia  $i$  y  $i + 1$  sin afectar a los restantes elementos de  $N_n$ . En concreto,
- $$\tau_i = (1)(2) \cdots (i-1)(i\ i+1)(i+2) \cdots (n).$$
- Demostrar que cualquier permutación de  $N_n$  puede expresarse en términos de  $\tau_1, \tau_2, \dots, \tau_{n-1}$ . (Ésta es la base de un antiguo pasatiempo inglés.)
- 14 Demostrar que para cualesquiera enteros positivos  $n$  y  $m$  se tiene
- $$\phi(n^m) = n^{m-1}\phi(n).$$
- 15 Calcular  $\phi(1000)$  y  $\phi(1001)$ .
- 16 Se dice que una permutación de  $N_n$  es *cíclica* si tiene un único ciclo (de longitud necesariamente igual a  $n$ ). Demostrar que existen  $(n-1)!$  permutaciones cíclicas de  $N_n$ .
- 17 Sea  $u_n$  el número de palabras de longitud  $n$  en el alfabeto  $\{0, 1\}$  con la propiedad de que no tienen dos ceros consecutivos. Demostrar que
- $$u_1 = 2, \quad u_2 = 3, \quad u_n = u_{n-1} + u_{n-2} \quad (n \geq 3).$$
- 18 Se divide una baraja de 52 cartas en dos partes iguales y se barajan de forma que si el orden original era  $1, 2, 3, 4, \dots$ , el nuevo orden es  $1, 27, 2, 28, \dots$ . ¿Cuántas veces hay que repetir el proceso para que las cartas vuelvan a la situación de partida?
- 19 Demostrar que en un conjunto de 20 personas existen cuatro mutuamente conocidas o mutuamente extrañas.
- 20 Si  $s$  y  $t$  son dos enteros mayores que 1, existe un entero mínimo  $r(s, t)$  con la propiedad de que si  $n \geq r(s, t)$ , entonces cualquier conjunto de  $n$  personas contiene un conjunto de  $s$  conocidos mutuos o un conjunto de  $t$  extraños mutuos. Demostrar que
- $$r(s, 2) = s, \quad r(2, t) = t, \quad r(s, t) \leq r(s-1, t) + r(s, t-1).$$

## 4 Subconjuntos y diseños

### 4.1 Números binomiales

Muchas cuestiones prácticas de la matemática discreta tienen la siguiente forma: ¿de cuántas maneras puede seleccionarse cierto número de objetos de un conjunto dado? La respuesta a una pregunta de este tipo dependerá de si se permiten o no *repeticiones*, y de si se tiene en cuenta el *orden* en la selección. Si importa el orden, tendremos que usar los modelos de selecciones ordenadas que discutimos en las secciones 3.4 y 3.5; pero en caso contrario, será apropiado utilizar otros modelos, tal como explicamos a continuación.

El modelo matemático de una *selección no ordenada sin repetición* es muy simple. Si tenemos un conjunto  $X$  con  $n$  elementos y seleccionamos  $r$  de ellos, el resultado es un subconjunto  $Y$  de  $X$  con  $|Y| = r$ . Hay que insistir en que lo importante en este modelo es el resultado de la selección (el subconjunto  $Y$ ), más que el proceso de selección. Por otra parte, no hay posibilidad de repetición, ya que cada elemento de  $X$  está en  $Y$  o no, y ningún elemento puede ser seleccionado dos veces.

Nos referiremos a un conjunto  $X$  de  $n$  elementos como un  $n$ -conjunto, y a un subconjunto  $Y$  de  $r$  elementos como un  $r$ -subconjunto de  $X$ . Así pues, el número de selecciones no ordenadas sin repetición de  $r$  objetos de un conjunto  $X$  de tamaño  $n$  es simplemente el número de  $r$ -subconjuntos del  $n$ -conjunto  $X$ . Por ejemplo, hay seis selecciones no ordenadas, sin repetición, de dos objetos del conjunto  $\{a, b, c, d\}$ ; corresponden a los subconjuntos

$$\{a, b\}, \quad \{a, c\}, \quad \{a, d\}, \quad \{b, c\}, \quad \{b, d\}, \quad \{c, d\}.$$

En general, el número de  $r$ -subconjuntos de un  $n$ -conjunto se denota

con el símbolo

$$\binom{n}{r}.$$

A menudo se pronuncia “ $n$  sobre  $r$ ”, y nos referiremos a él como un **número binomial**. Por ejemplo, hemos comprobado que un 4-conjunto tiene seis 2-subconjuntos, de forma que

$$\binom{4}{2} = 6.$$

Los ejercicios siguientes debieran demostrarse utilizando únicamente la definición de los números binomiales.

#### Ejercicios 4.1

1 Demostrar que

$$\binom{n}{r} = 0 \quad \text{si } r > n.$$

2 Hallar los valores de

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{n} \quad \text{para todo } n \geq 1.$$

3 Demostrar que

$$\binom{n}{r} = \binom{n}{n-r} \quad \text{para } 0 \leq r \leq n.$$

En general, el cálculo de los números binomiales depende del siguiente resultado fundamental.

**Teorema 4.1.1.** Si  $n$  y  $r$  son enteros positivos con  $1 \leq r \leq n$ , entonces

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

**DEMOSTRACIÓN:** Sea  $X$  un  $n$ -conjunto y supongamos que  $x$  es un cierto elemento de  $X$ . El conjunto de todos los  $r$ -subconjuntos de  $X$  puede dividirse en dos partes disjuntas  $U$  y  $V$  de la forma siguiente:

$U$  = los  $r$ -subconjuntos que contienen a  $x$ ;

$V$  = los  $r$ -subconjuntos que no contienen a  $x$ ;

Un  $r$ -subconjunto es de  $U$  si (y sólo si), al quitarle  $x$  se obtiene un  $(r-1)$ -subconjunto del  $(n-1)$ -conjunto  $X - \{x\}$ . Así pues,

$$|U| = \binom{n-1}{r-1}.$$

Por otra parte, un  $r$ -subconjunto es de  $V$  si (y sólo si) es un  $r$ -subconjunto del  $(n-1)$ -conjunto  $X - \{x\}$ . Por lo tanto,

$$|V| = \binom{n-1}{r}.$$

El principio de adición implica que el número total de  $r$ -subconjuntos es igual a  $|U| + |V|$  y, ya que este número es  $\binom{n}{r}$ , tenemos el resultado.  $\square$

El teorema 4.1.1 proporciona un método recursivo para calcular los números binomiales, ya que si conocemos los números  $\binom{n-1}{k}$  para  $0 \leq k \leq n-1$ , podemos calcular los  $\binom{n}{r}$ . Estos cálculos se suelen mostrar en forma de triángulo:

		1					
		1	1				
		1	2	1			
		1	3	3	1		
		1	4	6	4	1	
		1	5	10	10	5	1
		1	6	15	20	15	6
		1	7	21	35	35	21
		1					

También se conoce como *triángulo de Pascal*, en recuerdo de Blaise Pascal (1623-1662), a pesar de que era conocido mucho antes. Los números de la fila  $n+1$  son los números binomiales  $\binom{n}{r}$  para  $r = 0, 1, \dots, n$ . Los resultados

del ejercicio 4.1.2 implican que los bordes están enteramente constituidos por unos, y el teorema 4.1.1 nos dice que cada número es la suma de los dos números que tiene inmediatamente por encima. En consecuencia, podemos construir la tabla fila tras fila. Por ejemplo, el cuarto número de la fila siguiente es

$$\binom{8}{3} = \binom{7}{2} + \binom{7}{3} = 21 + 35 = 56.$$

En ocasiones es conveniente tener una fórmula explícita para los números binomiales.

**Teorema 4.1.2.** Si  $n$  y  $r$  son enteros positivos con  $1 \leq r \leq n$ , se tiene que

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}.$$

**DEMOSTRACIÓN:** Utilizaremos el principio de inducción. Para la base de la inducción, nótese que el resultado es cierto si  $n = 1$ , ya que  $\binom{1}{1} = 1$  y la fórmula se reduce también a  $1/1! = 1$ .

Por la hipótesis de inducción, supongamos que el resultado es cierto para  $n = k$ . Entonces, por el teorema 4.1.1 y la hipótesis de inducción,

$$\begin{aligned} \binom{k+1}{r} &= \binom{k}{r-1} + \binom{k}{r} \\ &= \frac{k(k-1)\cdots(k-r+2)}{(r-1)!} + \frac{k(k-1)\cdots(k-r+1)}{r!} \\ &= \frac{k(k-1)\cdots(k-r+2)}{(r-1)!} \left(1 + \frac{k-r+1}{r}\right) \\ &= \frac{(k+1)k(k-1)\cdots(k-r+2)}{r!}. \end{aligned}$$

(Si  $r = 1$  o  $r = k+1$ , tenemos que utilizar los valores  $\binom{k}{0} = 1$  y  $\binom{k}{k+1} = 0$  en lugar de la fórmula.) El resultado es, pues, cierto para  $n = k+1$  y, por el principio de inducción, es cierto para todos los enteros  $n$ .  $\square$

Existen muchas identidades útiles e interesantes en las que aparecen los números binomiales y, aunque en ocasiones pueden demostrarse utilizando la fórmula anterior, suele ser más conveniente basarse en la propia

definición o en la técnica recursiva dada en el teorema 4.1.1. Daremos ejemplos de ambos métodos.

**Ejemplo 1.** Demostrar que

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

**SOLUCIÓN:** La expresión de la izquierda es la suma del número de  $r$ -subconjuntos de un  $n$ -conjunto para todos los valores de  $r$ . Así pues, es igual al número total de subconjuntos de un  $n$ -conjunto y, según el ejemplo del apartado 3.4, este número es igual a  $2^n$ .  $\square$

**Ejemplo 2.** Demostrar que

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^{n-1} \binom{n}{n-1} + (-1)^n \binom{n}{n} = 0.$$

**SOLUCIÓN:** De acuerdo con el ejercicio 4.1.2. y el teorema 4.1.1, el término izquierdo es igual a

$$1 - \left\{ \binom{n-1}{0} + \binom{n-1}{1} \right\} + \left\{ \binom{n-1}{1} + \binom{n-1}{2} \right\} - \cdots \\ \cdots + (-1)^{n-1} \left\{ \binom{n-1}{n-2} + \binom{n-1}{n-1} \right\} + (-1)^n.$$

Cada término  $\binom{n-1}{k}$  con  $k$  entre 1 y  $n-2$  aparece con signo positivo y con signo negativo, de forma que estos términos se cancelan. Los términos restantes son

$$1 - \binom{n-1}{0} + (-1)^{n-1} \binom{n-1}{n-1} + (-1)^n = 1 - 1 + (-1)^{n-1} + (-1)^n,$$

lo cual es igual a 0.  $\square$

#### Ejercicios 4.1 (continuación)

- 4 Calcular las tres filas siguientes del triángulo de Pascal, empezando con la parte del triángulo dada en la página 72.

5 Evaluar  $\binom{16}{4}$  y  $\binom{17}{5}$ .

6 Demostrar que el número de palabras de longitud  $n$  en el alfabeto  $\{0, 1\}$  que contienen exactamente  $r$  ceros es igual a  $\binom{n}{r}$ .

7 Demostrar la identidad

$$\binom{s-1}{0} + \binom{s}{1} + \cdots + \binom{s+n-2}{n-1} + \binom{s+n-1}{n} = \binom{s+n}{n},$$

donde  $s$  y  $n$  son enteros positivos. [Indicación: si  $X$  es un  $(s+n)$ -conjunto e  $Y = \{y_1, y_2, \dots, y_n\}$  es un  $n$ -subconjunto específico de  $X$ , ¿cuál es el número de  $n$ -subconjuntos de  $X$  para los cuales  $y_r$  es el primer elemento de  $Y$  que no está en el subconjunto?]

8 Dar una demostración alternativa del ejercicio 7, partiendo de la fórmula

$$\binom{s+n}{n} = \binom{s+n-1}{n} + \binom{s+n-1}{n-1},$$

y aplicando repetidamente el teorema 4.1.1 para escindir el último término.

#### 4.2 Selecciones no ordenadas con repetición

El número binomial  $\binom{n}{r}$  se define como el número de  $r$ -subconjuntos de un  $n$ -conjunto, o como el número de selecciones no ordenadas *sin* repetición de  $r$  objetos de un conjunto de  $n$  objetos. Pasemos ahora a las selecciones no ordenadas *con* repetición. Cuando los números que intervienen son pequeños, es fácil dar una lista con todas las posibilidades. Por ejemplo, hay 15 selecciones no ordenadas de cuatro objetos del conjunto  $\{a, b, c\}$ , si se permiten repeticiones, y son:

aaaa	aaab	aaac	aabb	aabc
aacc	abbb	abbc	abcc	accc
bbbb	bbbc	bbcc	bccc	cccc

Demostraremos que es posible dar una fórmula general para el número de selecciones no ordenadas con repetición en términos de los números binomiales. En la demostración interviene la representación de las selecciones como palabras en el alfabeto  $\{0, 1\}$ ; por ejemplo, la selección

*abcc* se representará como la palabra 101011. Los ceros son marcas que separan el tipo de objetos, y los unos nos dicen cuántos objetos hay, según el esquema

<i>a</i>	<i>b</i>	<i>c</i>	<i>c</i>
1	0	1	0

1    0    1    0    1    1.

Dado que hay dos marcas, que pueden colocarse en cualquiera de las posiciones, el número total de selecciones en este caso es  $\binom{6}{2} = 15$ , lo cual coincide con la lista anterior. Demostraremos ahora este resultado de forma general.

**Teorema 4.2.** *El número de selecciones no ordenadas con repetición de  $r$  objetos de un conjunto de  $n$  objetos es*

$$\binom{n+r-1}{r}.$$

**DEMOSTRACIÓN:** Dado que las selecciones no son ordenadas, podemos arreglar las cosas de forma que, en cada selección, todos los objetos del mismo tipo estén juntos. Una vez hecho esto, podemos asignar a cada selección una palabra de longitud  $n + (r - 1)$  en el alfabeto  $\{0, 1\}$  según el método explicado arriba. Es decir, si hay  $k_i$  objetos de tipo  $i$  ( $1 \leq i \leq n$ ), entonces las primeras  $k_1$  letras de la palabra son unos, seguidos de un cero, seguidos de  $k_2$  unos, y así sucesivamente. La función definida por esta regla es una biyección entre el conjunto de selecciones y el conjunto de palabras de longitud  $n + r - 1$  que contienen exactamente  $n - 1$  ceros. Los ceros pueden ocupar cualesquiera de las  $n + r - 1$  posiciones, de forma que el número de palabras es

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r},$$

como queríamos demostrar.  $\square$

Podemos resumir en una tabla (tabla 4.2.1) nuestros resultados sobre los distintos tipos de selecciones —ordenadas y no ordenadas, con y sin repetición— de  $r$  objetos de un  $n$ -conjunto.

Tabla 4.2.1

	Ordenadas	No ordenadas
Sin repetición	$n(n-1)\cdots(n-r+1)$	$\binom{n}{r}$
Con repetición	$n^r$	$\binom{n+r-1}{r}$

### Ejercicios 4.2

1 Escribir los valores que proporciona la tabla anterior cuando  $r = 2$  y  $n = 3$ , y dar una lista de las selecciones pertinentes en cada caso tomando  $\{a, b, c\}$  como 3-conjunto.

2 Demostrar que al tirar tres dados indistinguibles pueden producirse 56 resultados distintos. ¿Cuántos resultados pueden darse al tirar  $n$  dados indistinguibles?

3 Supongamos que se desarrolla la expresión  $(x+y+z)^n$  y se agrupan los términos de acuerdo con las reglas elementales del álgebra; por ejemplo,

$$(x+y+z)^2 = x^2 + y^2 + z^2 + 2xy + 2yz + 2xz.$$

¿Cuántos términos se obtienen en la fórmula resultante?

4 Demostrar que el número de  $n$ -plas  $(x_1, x_2, \dots, x_n)$  de enteros no negativos que satisfacen la ecuación

$$x_1 + x_2 + \dots + x_n = r$$

es igual a  $\binom{n+r-1}{r}$ . [Indicación: supóngase que una selección no ordenada con repetición de  $r$  objetos de un conjunto de  $n$  objetos contiene  $x_i$  copias del  $i$ -ésimo objeto ( $1 \leq i \leq n$ ).]

### 4.3 El teorema del binomio

En álgebra elemental aprendemos las fórmulas

$$(a+b)^2 = a^2 + 2ab + b^2, \quad (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$

y se da el caso de tener que desarrollar la fórmula para  $(a+b)^4$  y potencias superiores de  $a+b$ . El resultado general que proporciona una fórmula para  $(a+b)^n$  se conoce como el **teorema del binomio**.

**Teorema 4.3.** Sea  $n$  un entero positivo. El coeficiente del término  $a^{n-r}b^r$  en la expansión de  $(a+b)^n$  es el número binomial  $\binom{n}{r}$ . En concreto, tenemos

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n.$$

**DEMOSTRACIÓN:** Veamos qué ocurre al multiplicar  $n$  factores

$$(a+b)(a+b) \cdots (a+b).$$

Los términos del producto se obtienen seleccionando  $a$  o bien  $b$  de cada factor. El número de términos  $a^{n-r}b^r$  es exactamente el número de maneras de seleccionar  $r$  veces  $b$  (y, en consecuencia,  $n-r$  veces  $a$ ), lo cual, por definición, es igual al número binomial  $\binom{n}{r}$ .  $\square$

Así pues, los coeficientes del desarrollo pueden calcularse utilizando la recurrencia de los números binomiales (triángulo de Pascal) o mediante la fórmula. Por ejemplo,

$$\begin{aligned} (a+b)^6 &= \binom{6}{0}a^6 + \binom{6}{1}a^5b + \binom{6}{2}a^4b^2 + \binom{6}{3}a^3b^3 \\ &\quad + \binom{6}{4}a^2b^4 + \binom{6}{5}ab^5 + \binom{6}{6}b^6 \\ &= a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6. \end{aligned}$$

Desde luego, podemos obtener otras fórmulas útiles sustituyendo  $a$  y  $b$  por expresiones convenientes. Algunos ejemplos típicos son:

$$(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4;$$

$$(1-x)^7 = 1 - 7x + 21x^2 - 35x^3 + 35x^4 - 21x^5 + 7x^6 - x^7;$$

$$(x+2y)^5 = x^5 + 10x^4y + 40x^3y^2 + 80x^2y^3 + 80xy^4 + 32y^5;$$

$$(x^2+y)^4 = x^8 + 4x^6y + 6x^4y^2 + 4x^2y^3 + y^4.$$

Se dice que la expresión  $a+b$  es una expresión *binomial*—porque tiene dos términos. Los números  $\binom{n}{r}$  ocurren como coeficientes en el desarrollo  $(a+b)^n$  y es frecuente referirse a ellos como *coeficientes binomiales*. Sin embargo, la demostración del teorema 4.3 nos hace ver que si ocurren en este contexto es porque representan el número de maneras de efectuar ciertas selecciones. Por este motivo seguiremos llamándolos *números binomiales*, lo cual corresponde con más exactitud al concepto que representan los símbolos.

Además de ser enormemente útiles en manipulaciones algebraicas, el teorema del binomio puede utilizarse para deducir igualdades en las que aparecen los números binomiales.

**Ejemplo.** Demostrar que

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

**SOLUCIÓN:** Usaremos la igualdad

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

Según el teorema del binomio, el término de la izquierda es el producto de dos factores, ambos iguales a

$$1 + \binom{n}{1}x + \cdots + \binom{n}{r}x^r + \cdots + x^n.$$

Al multiplicar los dos factores, el término  $x^n$  se obtiene tomando un término  $\binom{n}{r}x^r$  del primer factor y un término  $\binom{n}{n-r}x^{n-r}$  del segundo. Así pues, el coeficiente de  $x^n$  en el producto es

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \cdots + \binom{n}{n}\binom{n}{0}.$$

Puesto que  $\binom{n}{n-r} = \binom{n}{r}$ , vemos que se trata del miembro izquierdo de la igualdad del enunciado. Pero el miembro derecho es  $\binom{2n}{n}$ , que también es el coeficiente de  $x^n$  en el desarrollo de  $(1+x)^{2n}$ , de forma que la igualdad queda demostrada.  $\square$

En el capítulo 18 demostraremos una forma más general del teorema del binomio en la que aparecen exponentes negativos.

### Ejercicios 4.3

1. Escribir las fórmulas de  $(1+x)^8$  y  $(1-x)^8$ .

2. Calcular el coeficiente de

- (i)  $x^5$  en  $(1+x)^{11}$ ;
- (ii)  $a^2b^8$  en  $(a+b)^{10}$ ;
- (iii)  $a^6b^6$  en  $(a^2+b^3)^5$ ;
- (iv)  $x^3$  en  $(3+4x)^6$ .

3. Usar la igualdad  $(1+x)^m(1+x)^n = (1+x)^{m+n}$  para demostrar que

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r}\binom{n}{0}$$

donde  $m$ ,  $n$  y  $r$  son enteros positivos con  $m \geq r$  y  $n \geq r$ .

4. Dar demostraciones alternativas de los resultados de los ejemplos 1 y 2 del apartado 4.1 mediante sustituciones adecuadas en las fórmulas de  $(1+x)^n$  y  $(1-x)^n$ .

5. Demostrar que si  $r$  y  $s$  son enteros tales que  $s|r$  y  $p$  es un primo tal que  $p|r$  pero  $p\not|s$ , entonces  $p|r/s$ . [Indicación: hacer  $r = st$ .] Deducir que

- (i) el número binomial  $\binom{p}{i}$  es divisible por  $p$  para todos los  $i$  con  $1 \leq i \leq p-1$ ;
- (ii)  $(a+b)^p - a^p - b^p$  es divisible por  $p$  para enteros  $a$  y  $b$  cualesquiera.

### 4.4 El principio de la criba

El principio enumerativo básico (teorema 3.1) afirma que  $|A \cup B|$  es la suma de  $|A|$  y  $|B|$  si  $A$  y  $B$  son conjuntos disjuntos. Si  $A$  y  $B$  no son disjuntos, el resultado de sumar  $|A|$  y  $|B|$  es que los elementos de  $A \cap B$  se cuentan dos veces (figura 4.1a). De forma que para obtener la respuesta correcta, hemos de restar  $|A \cap B|$ :

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

Podemos aplicar un método similar en el caso de tres conjuntos (figura 4.1b). Al sumar  $|A|$ ,  $|B|$  y  $|C|$ , los elementos de  $A \cap B$ ,  $B \cap C$  y  $C \cap A$  se cuentan doble (si no están en los tres conjuntos al mismo tiempo). Para corregir esto, restamos  $|A \cap B|$ ,  $|B \cap C|$  y  $|C \cap A|$ . Pero ahora los elementos de  $A \cap B \cap C$ , que inicialmente habían sido contados tres veces, han sido restados tres veces. De forma que para obtener la respuesta correcta, hemos de *sumar*  $|A \cap B \cap C|$ . Resulta que

$$|A \cup B \cup C| = \alpha_1 - \alpha_2 + \alpha_3,$$

donde

$$\begin{aligned} \alpha_1 &= |A| + |B| + |C|, & \alpha_2 &= |A \cap B| + |B \cap C| + |C \cap A|, \\ & & \alpha_3 &= |A \cap B \cap C|. \end{aligned}$$

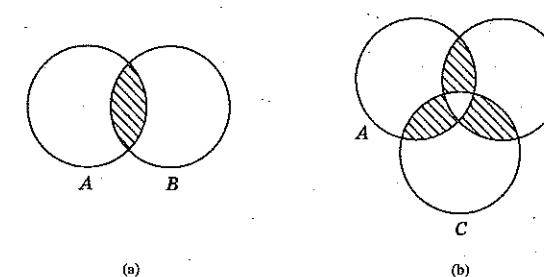


Fig. 4.1 Intersecciones de dos y tres conjuntos.

Este resultado es un caso sencillo de lo que solía llamarse, por razones evidentes, el principio de inclusión y exclusión. Actualmente se suele llamar el *principio de la criba*.

**Teorema 4.4.** Si  $A_1, A_2, \dots, A_n$  son conjuntos finitos, entonces

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \dots + (-1)^{n-1}\alpha_n,$$

donde  $\alpha_i$  es la suma de los cardinales de todas las intersecciones de  $i$  de los conjuntos ( $1 \leq i \leq n$ ).

**DEMOSTRACIÓN:** Demostraremos que cada elemento  $x$  de la unión contribuye exactamente en una unidad al término de la derecha. Supongamos que  $x$  pertenece precisamente a  $k$  de los conjuntos  $A_1, \dots, A_n$ . Entonces  $x$  contribuye con  $k$  a la suma  $\alpha_1 = |A_1| + \dots + |A_n|$ . En la suma  $\alpha_2$ ,  $x$  contribuye con 1 a  $|A_i \cap A_j|$  si tanto  $A_i$  como  $A_j$  están entre los  $k$  conjuntos que contienen a  $x$ . Hay  $\binom{k}{2}$  de estos pares, de forma que  $\binom{k}{2}$  es la contribución de  $x$  a  $\alpha_2$ . En general, la contribución de  $x$  a  $\alpha_i$  es  $\binom{k}{i}$ , y la contribución total de  $x$  al término derecho es

$$\binom{k}{1} - \binom{k}{2} + \dots + (-1)^{k-1} \binom{k}{k},$$

ya que los términos con  $i > k$  son nulos.

Pero la igualdad demostrada en el ejemplo 2 del apartado 4.1 implica que esta expresión es igual a  $\binom{k}{0}$ , que es igual a 1.  $\square$

Hay un corolario sencillo del teorema 4.4 que en la práctica suele ser muy útil. Supongamos que  $A_1, A_2, \dots, A_n$  son subconjuntos de un conjunto  $X$  con  $|X| = N$ . Entonces el número de elementos de  $X$  que no están en ninguno de estos subconjuntos es

$$\begin{aligned} |X \setminus (A_1 \cup A_2 \cup \dots \cup A_n)| &= |X| - |A_1 \cup A_2 \cup \dots \cup A_n| \\ &= N - \alpha_1 + \alpha_2 - \dots + (-1)^n \alpha_n. \end{aligned}$$

**Ejemplo 1.** En la asignatura de filosofía de primer curso de la Universidad de Folornia hay 73 estudiantes. De éstos, un total de 52 saben tocar el piano, 25 el violín y 20 la flauta; 17 saben tocar el piano y el violín, 12 el piano y la flauta, y 7 el violín y la flauta; pero sólo Osbert Smugg sabe tocar los tres instrumentos. ¿Cuántos estudiantes no saben tocar ninguno?

**SOLUCIÓN:** Sean  $P$ ,  $V$  y  $F$  los conjuntos de estudiantes que saben tocar el piano, el violín y la flauta, respectivamente. Con la información que nos dan tenemos que

$$\alpha_1 = |P| + |V| + |F| = 52 + 25 + 20 = 97,$$

$$\alpha_2 = |P \cap V| + |P \cap F| + |V \cap F| = 17 + 12 + 7 = 36,$$

$$\alpha_3 = |P \cap V \cap F| = 1.$$

Por lo tanto, el número de estudiantes que no pertenecen a ninguno de los conjuntos  $P$ ,  $V$  o  $F$  es

$$73 - 97 + 36 - 1 = 11.$$

$\square$

**Ejemplo 2.** Una secretaria poco eficiente tiene  $n$  cartas y  $n$  sobres con las direcciones correspondientes. ¿De cuántas maneras puede lograr la hazaña de poner cada carta en un sobre equivocado? (Esto se conoce a menudo como el *problema de los desarreglos*: existen otras versiones igualmente pintorescas.)

**SOLUCIÓN:** Podemos pensar en que cada letra y su correspondiente sobre tienen un entero  $i$  entre 1 y  $n$  como etiqueta. El hecho de poner las cartas en sobres se identifica con una permutación  $\pi$  de  $N_n$ :  $\pi(i) = j$  si la carta  $i$  se coloca en el sobre  $j$ . Lo que buscamos es el número de **desarreglos**, es decir, el número de permutaciones  $\pi$  tales que  $\pi(i) \neq i$  para todo  $i$  de  $N_n$ .

Sea  $A_i$  ( $1 \leq i \leq n$ ) el subconjunto de  $S_n$  (el conjunto de todas las permutaciones de  $N_n$ ) formado por las  $\pi$  tales que  $\pi(i) = i$ . Decimos que los elementos de  $A_i$  dejan *fijo* el elemento  $i$ . Por el principio de la criba, el número de desarreglos es

$$d_n = n! - \alpha_1 + \alpha_2 - \dots + (-1)^n \alpha_n,$$

donde  $\alpha_r$  es la suma de los cardinales de todas las intersecciones de  $r$  de los  $A_i$ . En otras palabras,  $\alpha_r$  es el número de permutaciones que fijan  $r$  símbolos elegidos de todas las formas posibles. Ahora bien, hay  $\binom{n}{r}$  formas de elegir  $r$  símbolos y el número de permutaciones que los dejan fijos es precisamente el número de permutaciones de los  $n - r$  símbolos restantes, es decir,  $(n - r)!$  Resulta finalmente que

$$\alpha_r = \binom{n}{r} \times (n - r)! = \frac{n!}{r!}, \quad d_n = n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right).$$

#### Ejercicios 4.4

- En una clase de matemáticas con 67 estudiantes, 47 saben leer francés, 35 saben leer alemán y 23 las dos lenguas. ¿Cuántos no saben leer ninguna

de las dos lenguas? Si, además, 20 saben leer ruso, de los cuales 12 saben también francés, 11 también alemán y 5 saben leer en las tres lenguas, ¿cuántos no saben leer ninguna lengua?

2 Hallar el número de maneras de ordenar las letras A, E, M, O, U, Y en una sucesión de forma que no aparezcan las palabras ME y YOU.

3 Calcular el número  $d_4$  de desarreglos de  $\{1, 2, 3, 4\}$  y escribir las permutaciones relevantes en la notación de ciclos.

4 Utilizar el principio de inducción para demostrar que la fórmula para  $d_n$  cumple la recurrencia

$$d_1 = 0, \quad d_2 = 1, \quad d_n = (n-1)(d_{n-1} + d_{n-2}) \quad (n \geq 3).$$

5 Demostrar que el número de desarreglos de  $\{1, 2, \dots, n\}$  en los que un objeto dado (pongamos 1) está en un 2-ciclo es  $(n-1)d_{n-2}$ . Construir de esta forma una demostración directa de la fórmula recurrente del ejercicio anterior.

## 4.5 Algunas aplicaciones aritméticas

Los matemáticos han estudiado los números primos y la factorización de números enteros durante siglos. La breve discusión de estos temas en capítulos anteriores debiera haber convencido al lector de que estos problemas son difíciles debido a que los primos están distribuidos irregularmente y a que no existe ningún método sencillo para hallar la factorización de un entero cualquiera.

Sin embargo, si conocemos la factorización de un entero, es relativamente fácil responder algunas preguntas sobre sus propiedades aritméticas. Supongamos, por ejemplo, que queremos hallar todos los divisores de un entero  $n$  y que conocemos su factorización

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Un entero  $d$  es divisor de  $n$  si, y sólo si, no tiene divisores primos distintos de los de  $n$ , y ningún primo lo divide más veces que a  $n$ . Por lo tanto, los divisores son exactamente los enteros que pueden escribirse como

$$d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

donde cada  $f_i$  cumple que  $0 \leq f_i \leq e_i$ . Por ejemplo, dado que  $60 = 2^2 \times 3 \times 5$ , podemos obtener rápidamente una lista con todos los divisores de 60: una buena manera de disponerlos se ilustra en la figura 4.2. (Técnicamente, la figura 4.2 es un diagrama del *retículo* de divisores de 60, aunque no necesitamos la descripción matemática precisa de este término.)

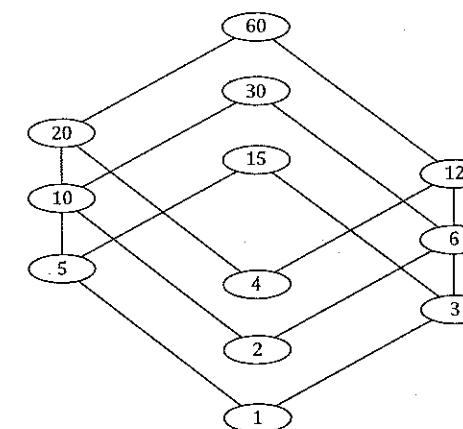


Fig. 4.2 Los divisores de 60.

Un problema similar es hallar el número de enteros  $x$  entre 1 y  $n$  que son primos con  $n$ . En el apartado 3.3 indicábamos este número con  $\phi(n)$ , el valor de la función  $\phi$  de Euler en  $n$ . Demostremos ahora que, conociendo la factorización de  $n$ , el principio de la criba nos permite calcular  $\phi(n)$ .

**Ejemplo.** ¿Cuánto vale  $\phi(60)$ ? En otras palabras, ¿cuántos enteros  $x$  entre 1 y 60 cumplen que  $\text{mcd}(x, 60) = 1$ ?

**SOLUCIÓN:** Puesto que  $60 = 2^2 \times 3 \times 5$ , hemos de contar los enteros entre 1 y 60 que *no* son divisibles por 2, 3 o 5. Sea  $A(2)$  el subconjunto de  $\mathbb{N}_{60}$  formado por los enteros que *son* divisibles por 2,  $A(2, 3)$  los que son divisibles por 2 y por 3, y así sucesivamente. Entonces tenemos, por el principio de la criba, que

$$\begin{aligned} \phi(60) &= 60 - |A(2) \cup A(3) \cup A(5)| \\ &= 60 - (|A(2)| + |A(3)| + |A(5)|) \\ &\quad + (|A(2, 3)| + |A(2, 5)| + |A(3, 5)|) - |A(2, 3, 5)|. \end{aligned}$$

Ahora bien,  $|A(2)|$  es el número de múltiplos de 2 en  $\mathbb{N}_{60}$ , que es igual a  $60/2 = 30$ . Igualmente,  $|A(2, 3)|$  es el número de múltiplos de  $2 \times 3$ , que es igual a  $60/(2 \times 3) = 10$ , y así sucesivamente. Por lo tanto,

$$\phi(60) = 60 - (30 + 20 + 12) + (10 + 6 + 4) - 2 = 16. \quad \square$$

Podemos utilizar el mismo método para dar una fórmula explícita de  $\phi(n)$  en el caso general.

**Teorema 4.5.1.** Sea  $n \geq 2$  un entero y sea  $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$  su factorización en números primos. Entonces

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

**DEMOSTRACIÓN:** Sea  $A_j$  el subconjunto de  $\mathbb{N}_n$  formado por los múltiplos de  $p_j$  ( $1 \leq j \leq r$ ). Entonces

$$\begin{aligned} \phi(n) &= n - |A_1 \cup A_2 \cup \cdots \cup A_r| \\ &= n - \alpha_1 + \alpha_2 - \cdots + (-1)^r \alpha_r, \end{aligned}$$

donde  $\alpha_i$  es la suma de los cardinales de todas las intersecciones de  $i$  de los  $A_j$ . Una intersección típica de la forma

$$A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_i}$$

contiene los múltiplos de  $P = p_{j_1} \times p_{j_2} \times \cdots \times p_{j_i}$  en  $\mathbb{N}_n$ , y éstos son precisamente los enteros

$$P, 2P, 3P, \dots, \left(\frac{n}{P}\right)P.$$

El cardinal de una intersección típica es por lo tanto  $n/P$ , y  $\alpha_i$  es la suma de todos los términos de la forma

$$\frac{n}{P} = n \left(\frac{1}{p_{j_1}}\right) \left(\frac{1}{p_{j_2}}\right) \cdots \left(\frac{1}{p_{j_i}}\right).$$

Resulta que

$$\begin{aligned} \phi(n) &= n - n \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}\right) + n \left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots\right) + \cdots \\ &\quad \cdots + (-1)^r n \left(\frac{1}{p_1 p_2 \cdots p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \quad \square \end{aligned}$$

La fórmula es fácil de usar siempre que conozcamos la factorización de  $n$ , por supuesto. Por ejemplo,

$$\phi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16.$$

El principio de la criba y la fórmula resultante para  $\phi(n)$  también tienen importantes consecuencias teóricas, como las que discutimos a continuación.

Suongamos que damos la vuelta al último paso de la demostración y multiplicamos los factores de la fórmula para  $\phi(n)$ . En el caso  $n = 60$  se obtiene

$$\phi(60) = \frac{60}{1} - \left(\frac{60}{2} + \frac{60}{3} + \frac{60}{5}\right) + \left(\frac{60}{6} + \frac{60}{10} + \frac{60}{15}\right) - \frac{60}{30}.$$

Tenemos un término  $60/d$  para cada divisor  $d$  de 60 que sea un producto de primos distintos, y su coeficiente es  $+1$  o  $-1$  según que el número de estos primos sea par o impar. Los divisores 4, 12 y 20, que tienen factores primos repetidos ( $2^2$  en este caso) no contribuyen, pero para conservar la uniformidad podemos decir que contribuyen con un término de coeficiente igual a 0. En general, podemos expresar  $\phi(n)$  como una suma de términos  $\mu(d) \times (n/d)$ , uno para cada divisor  $d$  de  $n$ , es decir,

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d},$$

donde los coeficientes  $\mu(d)$  vienen dados por

$$\mu(d) = \begin{cases} 1 & \text{si } d = 1, \\ (-1)^k & \text{si } d \text{ es un producto de } k \text{ primos distintos} \\ 0 & \text{si } d \text{ tiene un factor primo repetido.} \end{cases}$$

La función  $\mu$  se conoce como **función de Möbius**, en recuerdo de A. F. Möbius (1790-1868); jugará un papel vital en algunos de los teoremas algebraicos de la parte III del libro. Por el momento, demostraremos que posee algunas propiedades inesperadas.

Empezaremos por demostrar que para cualquier entero  $n \geq 2$ , la suma de  $\mu(d)$  para todos los divisores  $d$  de  $n$  es igual a cero; es decir,

$$\sum_{d|n} \mu(d) = 0.$$

Para demostrarlo, supongamos que  $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ . Cada divisor  $d$  es de la forma  $p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$  con  $0 \leq f_i \leq e_i$ , y  $\mu(d)$  es cero a menos que cada  $f_i$  sea 0 o 1. De esta forma, cada divisor  $d$  con  $\mu(d) \neq 0$  corresponde a un subconjunto de  $\{p_1, p_2, \dots, p_r\}$  formado por los  $p_i$  tales que  $f_i = 1$ . El número de tales subconjuntos de tamaño  $k$  es  $\binom{r}{k}$ , y  $\mu(d)$  es  $(-1)^k$ , de donde

$$\sum_{d|n} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \cdots + (-1)^r \binom{r}{r} = 0.$$

Hemos utilizado una vez más el resultado fundamental sobre la suma alternada de números binomiales (ejemplo 2, apartado 4.1).

Estamos a punto ya para demostrar la propiedad característica de la función de Möbius; se conoce con el nombre de **fórmula de inversión de Möbius**.

**Teorema 4.5.2.** Sea  $g$  una función definida en  $\mathbb{N}$  y supongamos que  $f$  es la función obtenida a partir de  $g$  mediante la regla

$$f(n) = \sum_{d|n} g(d).$$

Entonces  $g$  puede obtenerse a partir de  $f$  mediante la regla

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

**DEMOSTRACIÓN:** Si sustituimos  $f(n/d)$  en el miembro derecho de la segunda ecuación, obtenemos

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{c|n/d} g(c) \\ &= \sum_{(c,d) \in S} \mu(d) g(c). \end{aligned}$$

La doble suma se toma sobre el conjunto  $S$  de todos los pares  $(c, d)$  tales que  $c|n$  y  $d|n/c$  (ejemplo del apartado 1.6), y puede reagruparse de la manera siguiente:

$$\sum_{c|n} g(c) \left( \sum_{d|n/c} \mu(d) \right).$$

Por el resultado anterior, la suma entre paréntesis es igual a cero si  $n/c \geq 2$ . Así pues, sólo nos queda el término con  $n = c$ , que se reduce a

$$g(n) \sum_{d|1} \mu(d) = g(n)\mu(1) = g(n),$$

tal como queríamos demostrar.  $\square$

### Ejercicios 4.5

- 1 Calcular  $\phi(n)$  y  $\mu(n)$  para todos los enteros  $n$  con  $95 \leq n \leq 100$ .
- 2 Demostrar que si la factorización de  $n$  es  $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ , entonces el número de divisores de  $n$  es

$$(e_1 + 1)(e_2 + 1) \cdots (e_r + 1).$$

- 3 Utilizar el teorema 4.5.1 para demostrar que si  $\text{mcd}(m, n) = 1$ , entonces  $\phi(mn) = \phi(m)\phi(n)$ .

- 4 Demostrar que si  $1 \leq x \leq n$ , entonces

$$\text{mcd}(x, n) = \text{mcd}(n - x, n).$$

Como consecuencia, demostrar que la suma de todos los enteros  $x$  que cumplen  $1 \leq x \leq n$  y  $\text{mcd}(x, n) = 1$  es  $\frac{1}{2}n\phi(n)$ .

- 5 Demostrar que si la función  $f$  se obtiene a partir de  $g$  mediante

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right),$$

entonces  $g$  se obtiene de  $f$  mediante la regla

$$g(n) = \sum_{d|n} f(d).$$

(Este es el recíproco de la fórmula de inversión de Möbius.) Usar la fórmula

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

para dar otra demostración del teorema 3.3, es decir,

$$\sum_{d|n} \phi(d) = n.$$

## 4.6 Diseños

Supongamos que un fabricante ha desarrollado una gama de nuevos productos y pretende analizar un cierto número de modelos de la gama (digamos  $v$ ) pidiendo a algunos de sus clientes habituales que los prueben. Puede resultar impracticable que cada cliente pruebe todos los modelos, en cuyo caso parece razonable imponer las siguientes condiciones.

- (i) Cada cliente debería probar el mismo número ( $k$ ) de modelos
- (ii) Cada modelo debería ser probado por el mismo número ( $r$ ) de clientes.

Por ejemplo, si  $v = 8$ ,  $k = 4$  y  $r = 3$ , un posible esquema sería preguntar a seis personas que probaran los modelos

1234, 5678, 1357, 2468, 1247, 3568,

respectivamente (donde los modelos se representan por los números 1, 2, 3, 4, 5, 6, 7 y 8).

En general, sea  $X$  un  $v$ -conjunto. Decimos que un conjunto  $B$  de  $k$ -subconjuntos de  $X$  es un **diseño**, con parámetros  $(v, k, r)$ , si cada elemento de  $X$  pertenece exactamente a  $r$  de los subconjuntos de  $B$ . Es frecuente referirse a un conjunto  $B$  que pertenezca a  $B$  como un **bloque** del diseño. En el ejemplo anterior, los parámetros son  $(8, 4, 3)$  y los bloques son  $\{1, 2, 3, 4\}$ ,  $\{5, 6, 7, 8\}$ , etc.

Está claro que los parámetros de un diseño han de estar sujetos a ciertas restricciones; por ejemplo, no existe ningún diseño con parámetros  $(8, 3, 5)$ . (Esto se demostró en el ejercicio 3.2.3.) Veremos que las condiciones

necesarias más evidentes para la existencia de un diseño con parámetros  $(v, k, r)$  son también suficientes.

Supongamos que  $C$  es un conjunto cualquiera de  $k$ -subconjuntos de un  $v$ -conjunto  $X$ , no necesariamente un diseño. Podemos dibujar una tabla (en la línea de la tabla de McBrain, apartado 3.2) en la que las filas corresponden a los elementos  $x$  de  $X$ , las columnas a los subconjuntos  $C$  de  $C$ , y si  $x$  pertenece a  $C$ , se marca la fila  $x$ , columna  $C$ . En el ejemplo siguiente (tabla 4.6.1)  $X$  es el conjunto  $\{1, 2, 3, 4, 5, 6\}$  y hay cuatro subconjuntos  $C_1, C_2, C_3, C_4$ . En general, las marcas indican los pares  $(x, C)$  que pertenecen al conjunto

$$S = \{(x, C) \mid x \in C\}.$$

El “total por filas”  $r(x)$  nos da el número de veces que  $x$  ocurre como elemento de un subconjunto  $C$ : se le suele llamar el número de **replicaciones** de  $x$ . El “total por columnas” es  $k$  en cada caso, ya que hemos exigido que cada  $C$  sea un  $k$ -subconjunto de  $X$ . Así pues, los dos métodos para contar el conjunto  $S$  nos llevan a la ecuación

$$\sum_{x \in X} r(x) = |C| \times k.$$

Tabla 4.6.1

$x$	$C_1$	$C_2$	$C_3$	$C_4$	$r(x)$
1	✓	✓		✓	3
2	✓		✓		2
3		✓			1
4	✓		✓	✓	3
5			✓		1
6		✓		✓	2
$k$	3	3	3	3	

En el caso de un diseño  $B$ , el número de replicaciones  $r(x)$  es constante igual a  $r$ . Así que el miembro izquierdo de la ecuación se convierte en  $vr$ , y llegamos a

$$vr = bk,$$

donde  $b = |\mathbf{B}|$  es el número de bloques. Resulta que  $k$  ha de ser un divisor de  $vr$ . Aún más, puesto que el número total de  $k$ -subconjuntos de  $X$  es  $\binom{v}{k}$ , el número  $b$  de bloques no puede superar esta cantidad, es decir,

$$b = \frac{vr}{k} \leq \binom{v}{k}.$$

Es un hecho notable que estas sencillas condiciones sobre  $v$ ,  $k$  y  $r$  sean también suficientes para la existencia de un diseño.

**Teorema 4.6.** Existe un diseño con parámetros  $(v, k, r)$  si, y sólo si,

$$k|vr \quad \text{y} \quad \frac{vr}{k} \leq \binom{v}{k}.$$

**DEMOSTRACIÓN:** La necesidad de la condición ya ha sido demostrada. Recíprocamente, sean  $v$ ,  $k$  y  $r$  enteros positivos que satisfacen las condiciones, de forma que  $b = vr/k$  es un entero positivo menor o igual que  $\binom{v}{k}$ . Sea  $\mathbf{C}$  cualquier familia de  $b$   $k$ -subconjuntos distintos de un  $v$ -conjunto  $X$ . Los números de replicaciones  $r(x)$  de  $\mathbf{C}$  cumplen la ecuación

$$\sum_{x \in X} r(x) = bk = vr,$$

y si cada  $r(x)$  es igual a  $r$ , entonces  $\mathbf{C}$  ya es un diseño. En caso contrario, han de existir dos objetos  $x_1$  y  $x_2$  tales que  $r(x_1) > r > r(x_2)$ . (Véase la figura 4.3.)

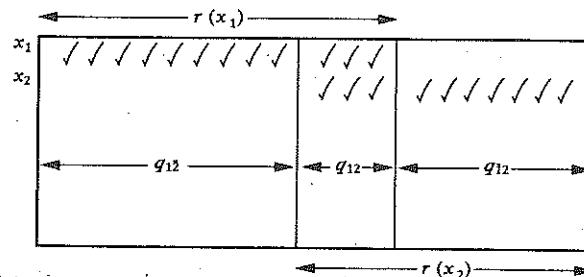


Fig. 4.3 Ilustración de la demostración del teorema 4.6.

Sea  $q_{1\bar{2}}$  el número de subconjuntos de  $C$  que contienen a  $x_1$  pero no a  $x_2$ , sea  $q_{\bar{1}2}$  el número de los que contienen a  $x_2$  pero no a  $x_1$ , y sea  $q_{12}$  el número de los que contienen a ambos. Entonces

$$q_{1\bar{2}} = r(x_1) - q_{12}, \quad q_{\bar{1}2} = r(x_2) - q_{12},$$

de forma que

$$q_{1\bar{2}} - q_{\bar{1}2} = r(x_1) - r(x_2) > 0.$$

Para cada uno de los  $q_{1\bar{2}}$  conjuntos  $C$  que contienen a  $x_1$  pero no a  $x_2$ , sea  $C^*$  el conjunto que se obtiene de  $C$  eliminando  $x_1$  e insertando  $x_2$ . Cada  $C^*$  contiene a  $x_2$  pero no a  $x_1$  y, puesto que  $q_{1\bar{2}} > q_{\bar{1}2}$ , ha de existir al menos un  $C^*$  que no pertenezca a la familia original  $\mathbf{C}$ . Sea  $C_0^*$  uno de estos conjuntos. Si eliminamos  $C_0$  de  $\mathbf{C}$  y lo sustituimos por  $C_0^*$ , obtenemos una nueva colección  $\mathbf{C}^*$  de  $k$ -subconjuntos distintos de  $X$ . Los números de replicaciones  $r^*(X)$  de  $\mathbf{C}^*$  son los mismos que para  $\mathbf{C}$ , salvo que

$$r^*(x_1) = r(x_1) - 1, \quad r^*(x_2) = r(x_2) + 1.$$

Si  $\mathbf{C}^*$  es un diseño, hemos acabado; si no, podemos repetir el proceso. En cada paso nos acercamos más a un diseño, ya que los números de replicaciones han de diferir en menos de la constante  $r$ . Por lo tanto, después de un número finito de pasos, tendremos que los números de replicaciones son todos iguales a  $r$  y habremos obtenido un diseño.  $\square$

Nótese que, utilizando la fórmula explícita de los números binomiales, la segunda condición puede reescribirse como

$$r \leq \binom{v-1}{k-1}.$$

Si nos fijamos en que cada vez que aparece un objeto  $x$  en un bloque, lo hace junto con  $k-1$  de los  $v-1$  objetos restantes, podemos ver que la condición es necesaria. En consecuencia,  $x$  no puede aparecer más de  $\binom{v-1}{k-1}$  veces.

#### Ejercicios 4.6

- Inalterable por el aparente fallo de su sistema para forzar a cada estudiante a seguir exactamente cuatro de las siete asignaturas de

matemáticas (apartado 3.2), el profesor McBrain prepara un plan para asegurarse de que, además, asista el mismo número de estudiantes a cada asignatura.

- (i) Si hay  $v$  estudiantes y a cada asignatura asisten  $k$  de ellos, ¿cuál es la relación entre  $v$  y  $k$ ?
- (ii) Si el número de estudiantes es 53, ¿cuántos ha de expulsar el profesor McBrain para que su plan sea factible?
- (iii) Mostrar diseños explícitos del plan del profesor McBrain en los casos  $v = 7$  y  $v = 14$ . (Recuérdese que en un diseño ningún bloque puede repetirse —es decir, no puede haber dos asignaturas con los mismos estudiantes.)

2 Para los siguientes valores de  $(v, k, r)$  construir un diseño que los tenga como parámetros o demostrar que no existe tal diseño.

- (i)  $(v, k, r) = (6, 3, 1)$ ; (ii)  $(v, k, r) = (5, 2, 1)$ ;
- (iii)  $(v, k, r) = (7, 3, 3)$ ; (iv)  $(v, k, r) = (9, 6, 4)$ .

3 ¿Qué valor tiene  $r$  en el diseño cuyos bloques son todos los  $k$ -subconjuntos de un  $v$ -conjunto?

4 Sea  $\mathbf{B}$  el conjunto de bloques de un diseño con parámetros  $(v, k, r)$  y sea  $\mathbf{B}'$  el conjunto de los complementarios  $\bar{B}$  de los bloques  $B$  de  $\mathbf{B}$ . Demostrar que  $\mathbf{B}'$  es también un diseño y calcular sus parámetros.

## 4.7 $t$ -diseños

La condición de que cada objeto o modelo pertenezca al mismo número de bloques puede reforzarse en varios sentidos. Podríamos exigir que cada *par* de objetos estuviera contenido en igual número de bloques, de forma que cada par fuese comparado en el mismo número de pruebas del experimento. Más en general, podríamos formular una condición similar para grupos de  $t$  objetos, donde  $t$  es un entero positivo.

**Definición.** Si  $X$  es un conjunto de cardinal  $v$ , se dice que un conjunto  $\mathbf{B}$  de  $k$ -subconjuntos de  $X$  es un  **$t$ -diseño** con parámetros  $(v, k, r_t)$  si, para

cada  $t$ -subconjunto  $T$  de  $X$ , el número de bloques que contienen a  $T$  es constante e igual a  $r_t$ .

Según la nueva definición, lo que inicialmente era un diseño, ahora es un  **$1$ -diseño**. El ejemplo que dimos de 1-diseño con  $v = 8$ ,  $k = 4$  y  $r_1 = 3$  era

$$1234, \quad 5678, \quad 1357, \quad 2468, \quad 1247, \quad 3568.$$

No se trata de un 2-diseño, ya que algunos 2-subconjuntos, como  $\{1, 2\}$ , ocurren dos veces, mientras que otros, como  $\{1, 5\}$ , ocurren sólo una vez; algunos, como  $\{1, 6\}$  no ocurren ninguna vez. Tampoco es un  $t$ -diseño para ningún otro valor superior de  $t$ . Sin embargo, existe un 3-diseño con  $v = 8$  y  $k = 4$ :

1235	4678
1346	2578
1457	2368
1568	2347
1267	3458
1378	2456
1248	3567.

Después de largas comprobaciones, podemos convencernos de que cada 3-subconjunto de  $\{1, 2, \dots, 8\}$  ocurre como un subconjunto de exactamente uno de los 14 bloques. Por ejemplo,  $\{2, 3, 8\}$  aparece en el bloque 2368 y en ningún otro. Por lo tanto, tenemos un 3-diseño con parámetros  $(v, k, r_3) = (8, 4, 1)$ . Es evidente que no se trata de un 4-diseño, ya que algunos 4-subconjuntos (como  $\{1, 2, 3, 6\}$ ) no aparecen, mientras que otros (como  $\{1, 2, 3, 5\}$ ) sí lo hacen. Se trata, sin embargo, tanto de un 2-diseño como de un 1-diseño, y el siguiente teorema demuestra que no se trata de ningún accidente.

**Teorema 4.7.1.** Si  $\mathbf{B}$  es un  $t$ -diseño, también es un  $s$ -diseño para  $s = 1, 2, \dots, t - 1$ .

**DEMOSTRACIÓN:** Basta demostrar que  $\mathbf{B}$  es un  $(t - 1)$ -diseño, ya que este resultado nos permitirá deducir, sustituyendo  $t$  por  $t - 1$ , que también es un  $(t - 2)$ -diseño, y así sucesivamente.

Sea  $X$  el conjunto de los objetos y supongamos que  $S$  es cualquier  $(t-1)$ -subconjunto de  $X$ . Vamos a contar los pares  $(x, B)$  tales que  $x$  es de  $B$  y  $B$  es un bloque que cumple

$$x \notin S \quad y \quad \{x\} \cup S \subseteq B.$$

Puesto que  $x$  no es del  $(t-1)$ -subconjunto  $S$ , hay  $v-(t-1)$  posibilidades para  $x$ ; para cada uno de estos  $x$ , el  $t$ -subconjunto  $\{x\} \cup S$  está contenido en  $r_t$  bloques, dado que  $\mathbf{B}$  es un  $t$ -diseño. Así pues, el número de pares es  $(v-(t-1)) \times r_t$ .

Por otra parte, supongamos que  $r_S$  es el número de bloques  $B$  que contienen a  $S$ ; para cada uno de estos  $B$ , cualquiera de los  $(k-(t-1))$  elementos de  $B \setminus S$  es un posible  $x$ . El número de pares es, por lo tanto,  $(k-(t-1)) \times r_S$ . Si igualamos las dos expresiones que dan el número de pares, tenemos que

$$(v-(t-1))r_t = (k-(t-1))r_S.$$

Esta ecuación muestra que  $r_S$  sólo depende de  $t, k, v$  y  $r_t$ , y por lo tanto es una constante, llamémosla  $r_{t-1}$ , para cada  $(t-1)$ -subconjunto de  $X$ . De aquí resulta que  $\mathbf{B}$  es una  $(t-1)$ -diseño.  $\square$

En la demostración del teorema 4.7.1 se ha hallado una fórmula útil para  $r_{t-1}$  en términos de  $r_t$ :

$$r_{t-1} = r_t \times \frac{v-t+1}{k-t+1}.$$

Por ejemplo, en nuestro 3-diseño con  $v=8, k=4$  y  $r_3=1$ , podemos calcular  $r_2$  y  $r_1$  de la siguiente forma:

$$r_2 = r_3 \times \frac{v-2}{k-2} = 3, \quad r_1 = r_2 \times \frac{v-1}{k-1} = 7.$$

Dedujimos que cada par ocurre 3 veces y que cada objeto ocurre 7 veces, lo cual puede comprobarse directamente.

Es interesante observar que el argumento usado en la demostración del teorema 4.7 es válido incluso si  $t=1$  y  $S$  es el conjunto vacío. En este caso, el número  $r_S$  (o  $r_0$ ) de bloques que contienen a  $S$  no es más que el número total de bloques,  $b=|\mathbf{B}|$ . En nuestro ejemplo,

$$b = r_0 = r_1 \times \frac{v}{k} = 14.$$

Estos cálculos no sólo nos permiten obtener los números  $r_s$  ( $0 \leq s \leq t-1$ ), sino que proporcionan al mismo tiempo condiciones necesarias para la existencia de un  $t$ -diseño.

**Teorema 4.7.2.** (i) Si  $\mathbf{B}$  es un  $t$ -diseño con parámetros  $(v, k, r_t)$ , entonces, al considerar  $\mathbf{B}$  como un  $s$ -diseño con  $1 \leq s \leq t-1$ , el parámetro  $r_s$  viene dado por

$$r_s = r_t \frac{(v-s)(v-s-1) \cdots (v-t+1)}{(k-s)(k-s-1) \cdots (k-t+1)}.$$

(ii) Si existe un  $t$ -diseño con parámetros  $(v, k, r_t)$ , entonces para cada  $s$  entre 0 y  $t-1$  se cumple que

$$(k-s)(k-s-1) \cdots (k-t+1) \mid r_t(v-s)(v-s-1) \cdots (v-t+1).$$

**DEMOSTRACIÓN:** (i) Esta fórmula se obtiene aplicando repetidamente la expresión de  $r_{t-1}$  en términos de  $r_t$ .

(ii) Dado que los números  $r_s$  han de ser enteros, el denominador ha de dividir al numerador.  $\square$

Las condiciones (ii) de divisibilidad excluyen muchos conjuntos de parámetros. Por ejemplo, si  $v=56, k=11$  y  $r_2=1$ , las condiciones son

$$(s=0) : 11 \times 20 \mid 56 \times 55,$$

$$(s=0) : 10 \mid 55.$$

La condición para  $s=1$  no se cumple y no puede existir ningún 2-diseño con estos parámetros.

Es importante observar que cuando  $t \geq 2$ , las condiciones de divisibilidad son necesarias pero no suficientes. (La demostración de este resultado forma parte de la teoría matemática más avanzada de los  $t$ -diseños.) Esta situación contrasta con el caso  $t=1$  en el que, según el teorema 4.6, las condiciones de divisibilidad son al mismo tiempo necesarias y suficientes.

### Ejercicios 4.7

- Partiendo del hecho de que existe un 5-diseño con parámetros  $v=12, k=6$  y  $r_5=1$ , hallar los valores de  $r_4, r_3, r_2, r_1$  y  $b$ .

2 ¿Es posible que existan diseños del tipo siguiente?

- (i) Un 3-diseño con  $v = 15$ ,  $k = 6$  y  $r_3 = 2$ .
- (ii) Un 4-diseño con  $v = 11$ ,  $k = 5$  y  $r_4 = 1$ .

3 Un *sistema de Steiner triple* (SST) es un 2-diseño con  $k = 3$  y  $r_2 = 1$ . Determinar para qué valores de  $v$  entre 3 y 12 puede existir un SST con  $v$  modelos y construir un SST en tales casos.

4 Demostrar que puede existir un SST con  $v$  modelos sólo si  $v$  es un entero positivo de la forma  $6n + 1$  o  $6n + 3$ .

5 En 1850, el Reverendo T.P. Kirkman propuso el siguiente problema. "Quince jovencitas de una escuela caminan en fila de a tres durante siete días consecutivos: ¿en qué orden hay que disponerlas cada día para que dos cualesquiera de ellas no caminen en la misma fila dos veces."

Resolver el problema de Kirkman y explicar cómo la solución está relacionada con un tipo especial de SST con quince modelos.

#### 4.8 Ejercicios diversos

1 Escribir las fórmulas para  $(x+y)^9$  y  $(x-y)^9$ .

2 Calcular el coeficiente de

- (i)  $x^6$  en  $(1+x)^{12}$ ;
- (ii)  $a^3b^7$  en  $(a+b)^{10}$ ;
- (iii)  $a^4b^6$  en  $(a^2+b)^8$ .

3 Demostrar que

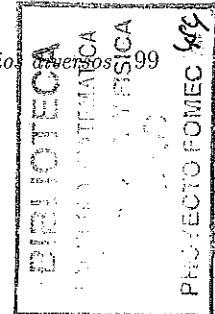
$$\binom{n}{r} \binom{r}{k} = \binom{n}{k} \binom{n-k}{r-k}.$$

4 Se trazan todas las diagonales que conectan un conjunto de  $n$  puntos de un círculo, de forma que tres de ellas no sean nunca concurrentes. ¿Cuántos puntos internos de intersección hay?

5 Demostrar que el número de maneras de distribuir  $n$  bolas idénticas en  $m$  cajas etiquetadas es

$$\binom{n+m-1}{n}.$$

#### 4.8 Ejercicio diverso



6 Demostrar que para  $n \geq m$

$$\binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{n}{m} = \binom{n+1}{m+1}.$$

7 Sea  $X$  un  $n$ -conjunto. Demostrar que

- (i) existe un conjunto de  $\binom{n-1}{k-1}$   $k$ -subconjuntos de  $X$  tales que cada par de ellos tiene intersección no vacía;
- (ii) existe un conjunto de  $\binom{n}{n^*}$  subconjuntos de  $X$  con la propiedad de que ninguno de ellos está contenido en otro, donde  $n^*$  es igual a  $\frac{1}{2}n$  si  $n$  es par y a  $\frac{1}{2}(n-1)$  si  $n$  es impar.

8 Dadas dos palabras  $u$  y  $v$  de longitud  $n$  en el alfabeto  $\{0,1\}$ , sea  $u+v$  la palabra que se obtiene al sumar los dígitos correspondientes de  $u$  y  $v$  según las reglas  $0+0=0$ ,  $0+1=1$ ,  $1+0=1$ ,  $1+1=0$ . Sea  $X$  el conjunto de estas palabras con la excepción de  $00\dots 0$ . Demostrar que el conjunto de todos los 3-subconjuntos de  $X$  de la forma

$$\{u, v, u+v\}$$

es un 2-diseño con parámetros  $(2^n - 1, 3, 1)$ . (En otras palabras, es un sistema de Steiner triple con  $2^n - 1$  modelos.)

9 Demostrar que los parámetros

$$v = q^3 + 1, \quad k = q + 1, \quad r_2 = 1$$

satisfacen las condiciones de divisibilidad de un 2-diseño. ¿Cuánto valen  $r_1$  y  $r_0$ ?

10 Supongamos que  $B$  es el conjunto de bloques de un  $t$ -diseño en un conjunto  $X$  con parámetros  $(v, k, r)$ , y elijamos un  $x$  de  $X$ . Sea  $B'$  el conjunto de bloques que se obtiene eliminando *todos* los bloques que no contienen a  $x$  y eliminando  $x$  de los que lo contienen. Demostrar que  $B'$  es un  $(t-1)$ -diseño en  $X - \{x\}$  con parámetros  $(v-1, k-1, r)$ .

11 Demostrar que puede existir un 2-diseño con parámetros  $(v, 4, 1)$  sólo si  $v$  es un entero positivo de la forma  $12n + 1$  o  $12n + 4$ .

12 Construir un 3-diseño con parámetros  $(10, 4, 1)$ .

13 ¿Cuántos enteros  $x$  ( $1 \leq x \leq 1000$ ) no son divisibles por 2, 3 o 5?

14 El profesor McBrain ha enseñado la misma asignatura durante los últimos doce años y cuenta tres bromas al año. Nunca ha dicho las mismas tres bromas dos veces (el orden en que se dicen las bromas no importa). ¿Cuántas bromas ha de saber?

- 15 Un grupo de hombres entra en un establecimiento de dudosa reputación y cada uno de ellos deja un abrigo y un paraguas en la puerta. Al recibir un mensaje avisando de una redada inminente de la policía, los hombres huyen rápidamente y cada uno coge un abrigo y un paraguas que no son suyos. Si hay  $n$  hombres, demostrar que el número de maneras en que esto puede ocurrir es

$$n! \left( n! - \frac{(n-1)!}{1!} + \frac{(n-2)!}{2!} - \cdots + (-1)^n \frac{1}{n!} \right).$$

- 16 Se dice que una función  $f$  definida en el conjunto de los enteros positivos es multiplicativa si

$$f(nm) = f(n)f(m) \text{ siempre que } \text{mcd}(n, m) = 1.$$

Demostrar que si  $f$  es multiplicativa, también lo es la función  $g$  definida por

$$g(n) = \sum_{d|n} f(d).$$

- 17 Obtener fórmulas para

$$(i) \quad \sum_{d|n} \mu(d)\phi(d), \quad (ii) \quad \sum_{d|n} \frac{\mu(d)}{\phi(d)}.$$

- 18 Sea  $\sigma_k(n)$  la suma de las potencias  $k$ -ésimas  $d^k$  de todos los divisores  $d$  de  $n$ . Demostrar que  $\sigma_k(n)$  es multiplicativa (ejercicio 16) y hallar una fórmula para ella.

- 19 Sea  $S_r(n)$  la suma de las potencias  $r$ -ésimas de los primeros  $n$  enteros positivos. Demostrar que, para  $r \geq 1$ ,

$$(n+1)^{r+1} - (n+1) = \sum_{i=1}^r \binom{r+1}{i} S_{r-i+1}(n).$$

- Deducir que existe una fórmula para  $S_r(n)$  que es un polinomio de grado  $r+1$  en  $n$ .

- 20 Dar una demostración alternativa del teorema del binomio basada en el principio de inducción y el teorema 4.1.1.

## 5 Particiones, clasificaciones y distribuciones

### 5.1 Particiones de un conjunto

En este capítulo estudiaremos tres tipos de problemas enumerativos asociados respectivamente a la partición de un conjunto en subconjuntos, la clasificación de un conjunto de objetos, y la distribución de un conjunto de objetos en un conjunto de cajas. Veremos que estos tres conceptos no son más que variaciones sobre un mismo tema.

Empezaremos por adoptar una notación conveniente. Sea  $I$  un conjunto no vacío, finito o infinito, y supongamos que para cada  $i$  de  $I$  tenemos un conjunto  $X_i$ . Decimos entonces que tenemos una familia de conjuntos y la escribimos

$$\mathcal{U} = \{X_i \mid i \in I\}.$$

Nos referiremos a  $I$  como al **conjunto de índices**. Nótese que los conjuntos no tienen por qué ser distintos, aunque en el caso que nos ocupará los conjuntos no sólo será distintos, sino disjuntos.

**Definición.** Una **partición** de un conjunto  $X$  es una familia  $\{X_i \mid i \in I\}$  de subconjuntos no vacíos de  $X$  tal que

- (i)  $X$  es la unión de los conjuntos  $X_i$  ( $i \in I$ ),
- (ii) cada par  $X_i, X_j$  ( $i \neq j$ ) es disjunto.

Se dice que los subconjuntos  $X_i$  son las **partes** de la partición.

Otra manera de enunciar la definición es decir que cada elemento de  $X$  ha de pertenecer a una, y sólo a una, parte. Por ejemplo, la figura 5.1 muestra una partición de  $\mathbb{N}_{16}$  con cinco partes  $X_1, X_2, X_3, X_4, X_5$ , donde

$$X_1 = \{1, 5, 9\}, \quad X_2 = \{2, 3, 4, 6, 7\}, \quad X_3 = \{8\}, \\ X_4 = \{10, 11, 13, 14\}, \quad X_5 = \{12, 15, 16\}.$$

En general, si  $X$  es un conjunto finito, una partición de  $X$  ha de tener un número finito  $k$  de partes, de forma que podemos usar el conjunto  $\mathbf{N}_k$  como conjunto de índices y dar las partes como una lista  $X_1, X_2, \dots, X_k$ . Pero hay que insistir en que el orden de las partes es irrelevante.

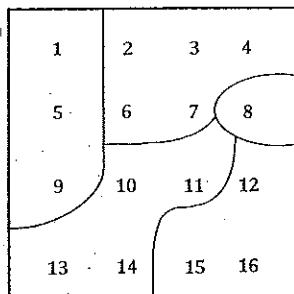


Fig. 5.1 Una partición de  $\mathbf{N}_{16}$ .

**Teorema 5.1.** Sea  $S(n,k)$  el número de particiones de un  $n$ -conjunto  $X$  en  $k$  partes, donde  $1 \leq k \leq n$ . Entonces

$$\begin{aligned} S(n, 1) &= 1, & S(n, n) &= 1, \\ S(n, k) &= S(n - 1, k - 1) + kS(n - 1, k) & (2 \leq k \leq n - 1). \end{aligned}$$

**DEMOSTRACIÓN:** Resulta claro que sólo hay una partición con una parte, el propio  $X$ , y que sólo hay una partición con  $n$  partes, los subconjuntos unitarios  $\{x\}$ .

Fijemos un elemento  $z$  de  $X$ . Una partición de  $X$  tiene que estar en una de las dos situaciones siguientes: (i) el subconjunto  $\{z\}$  es una de las partes, o (ii) la parte que contiene a  $z$  contiene además otros elementos. Al eliminar la parte  $\{z\}$  de una partición del tipo (i) obtenemos una partición del  $(n - 1)$ -conjunto  $X \setminus \{z\}$  en  $k - 1$  partes, y hay  $S(n - 1, k - 1)$  de ellas. Recíprocamente, dada una partición de éstas, podemos incorporar la parte  $\{z\}$ , de forma que la correspondencia es biyectiva.

Supongamos ahora que tenemos una partición  $\mathcal{U}$  del tipo (ii), con partes  $X_1, X_2, \dots, X_k$ . Esta situación determina un par de objetos  $(i, \mathcal{U}_0)$ , tal que  $z$  es de  $X_i$  y  $\mathcal{U}_0$  es la partición del  $(n - 1)$ -conjunto  $X \setminus \{z\}$  con partes  $X_1, X_2, \dots, X_i \setminus \{z\}, \dots, X_k$  (figura 5.2). Hay  $k$  posibles valores de  $i$  y

$S(n - 1, k)$  posibles particiones  $\mathcal{U}_0$ , de forma que tenemos  $kS(n - 1, k)$  pares. Además, dado uno de estos pares, podemos reincorporar  $z$  a la parte  $X_i$  y recuperar  $\mathcal{U}$ . Así pues, la correspondencia es biyectiva. Como cada partición es del tipo (i) o (ii), el resultado está demostrado.  $\square$

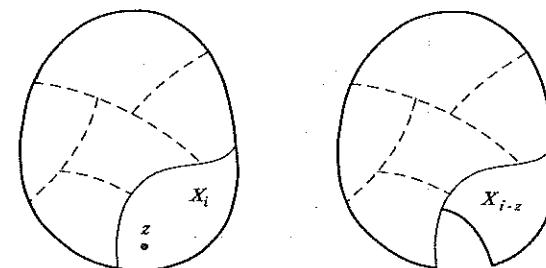


Fig. 5.2 Las particiones  $\mathcal{U}$  y  $\mathcal{U}_0$ .

A los números  $S(n, k)$  se les llama a veces **números de Stirling** (de segunda clase). El teorema 5.1 permite tabularlos (tabla 5.1.1) de forma parecida a los números binomiales en el triángulo de Pascal.

Tabla 5.1.1

			1			
		1	1	1		
	1	1	3	1		
1	1	7	6	1		
1	1	15	25	10	1	
1	1	31	90	65	15	1
1	63	301	350	140	21	1

La tabla puede construirse por filas utilizando la fórmula recursiva del teorema. Cada número se calcula a partir de los dos inmediatamente superiores; por ejemplo, el cuarto elemento de la fila inferior es

$$S(7, 4) = S(6, 3) + 4S(6, 4) = 90 + (4 \times 65) = 350.$$

**Ejercicios 5.1**

- 1 Calcular la siguiente fila de la tabla.
- 2 Dar una demostración directa de las igualdades

$$S(n, 2) = 2^{n-1} - 1, \quad S(n, n-1) = \binom{n}{2}.$$

3 Supongamos que se elimina la parte que contiene a un cierto elemento  $x$  de una partición de un  $n$ -conjunto en  $k$  partes. Se obtiene una partición de un subconjunto  $Y$  de  $X$  en  $k-1$  partes, donde  $r = |Y|$  está en el intervalo  $0 \leq r \leq n-1$ . Utilizar esta idea para demostrar que

$$S(n, k) = \sum_{r=0}^{n-1} \binom{n-1}{r} S(r, k-1).$$

**5.2 Clasificaciones y relaciones de equivalencia**

Hay otra forma de considerar una partición de un conjunto. Cuando un niño ordena un montón de ladrillos según su color, podemos decir que está construyendo una partición de un conjunto de ladrillos. También podemos decir que está *clasificando* los ladrillos usando el hecho de que ladrillos del mismo color están relacionados y han de ir a parar a la misma clase.

Más formalmente, sea  $\{X_i \mid i \in I\}$  una partición del conjunto  $X$ . Escribimos

$x R x'$  o  $x$  está relacionado con  $x'$ ,

si  $x$  y  $x'$  están en la misma parte  $X_i$ . La relación  $R$  definida de esta forma tiene tres propiedades que son una consecuencia trivial de la definición. Si  $x, y, z$  son elementos cualesquiera de  $X$ , no necesariamente distintos, entonces tenemos las siguientes afirmaciones (conocidas por los nombres que se indican):

- |                                  |                                   |
|----------------------------------|-----------------------------------|
| $x R x$                          | (la propiedad <i>reflexiva</i> )  |
| $x R y \Rightarrow y R x$        | (la propiedad <i>simétrica</i> )  |
| $x R y, y R z \Rightarrow x R z$ | (la propiedad <i>transitiva</i> ) |

Se dice que una relación  $R$  en un conjunto  $X$  es una **relación de equivalencia** si es reflexiva, simétrica y transitiva.

**Ejercicios 5.2**

- 1 Los símbolos de la columna izquierda de la tabla 5.2.1 denotan relaciones entre enteros. Contéstese sí o no a todas las preguntas sobre cada relación.

**Tabla 5.2.1**

$x R y$ es	¿Reflexiva?	¿Simétrica?	¿Transitiva?	¿Relación de equivalencia?
$x \leq y$				
$x   y$				
$3   (x-y)$				
$x + y = 7$				

Del mismo modo que una partición da lugar a una relación de equivalencia, recíprocamente, una relación de equivalencia  $R$  en un conjunto  $X$  determina una partición de  $X$ . Para ver que así es, definiremos la **clase de equivalencia** de  $x$  como

$$C_x = \{x' \in X \mid x' R x\}.$$

$C_x$  es el subconjunto de  $X$  formado por todos los  $x'$  relacionados con  $x$  mediante la relación  $R$ . Es importante darse cuenta de que, en general, el subconjunto  $C_x$  tendrá diferentes nombres. De hecho, si  $x$  y  $y$  cumplen que  $x R y$ , las clases de equivalencia  $C_x$  y  $C_y$  son iguales. Ya que si  $x R y$  y  $z$  es un elemento cualquiera de  $C_x$ , entonces

$$\begin{array}{ll} z R x & (\text{definición de } C_x) \\ y & x R y \quad (\text{por hipótesis}) \\ \text{de donde} & z R y \quad (\text{propiedad transitiva}). \end{array}$$

En otras palabras,  $z$  es de  $C_y$  y hemos demostrado que  $C_x \subseteq C_y$ . Un argumento idéntico demuestra que  $C_y \subseteq C_x$ , y tenemos  $C_x = C_y$  como afirmábamos.

Así pues, cada clase de equivalencia tiene varios alias; de hecho, utiliza el nombre  $C_x$  para cada  $x$  que pertenece a ella. Una vez se ha entendido este aspecto algo confuso, la demostración del siguiente teorema es casi evidente.

**Teorema 5.2.** Si  $R$  es una relación de equivalencia en un conjunto  $X$ , entonces las clases de equivalencia distintas de  $R$  forman una partición de  $X$ .

**DEMOSTRACIÓN:** La propiedad reflexiva nos dice que cada elemento  $x$  pertenece a su clase  $C_x$ , de manera que las clases no son vacías y su unión es todo  $X$ .

Queda por demostrar que dos clases distintas son disjuntas; o, equivalentemente, que si dos clases se cortan son idénticas. Supongamos que  $z$  pertenece tanto a  $C_x$  como a  $C_y$ . Tenemos que

	$z R x$	(definición de $C_x$ )
luego	$x R z$	(propiedad simétrica)
también	$x R y$	(definición de $C_y$ )
luego	$z R y$	(propiedad transitiva).

Ahora bien, de acuerdo con la discusión previa al teorema,  $x R y$  implica que  $C_x = C_y$ .  $\square$

Hemos demostrado que una partición  $X$  y una relación de equivalencia en  $X$  son esencialmente lo mismo. La idea de una partición es fácil de comprender, mientras que una relación de equivalencia es, a primera vista, un concepto más resbaladizo. Pero en matemáticas suele ser más conveniente empezar por definir una relación en un conjunto y demostrar las tres propiedades que caracterizan las relaciones de equivalencia. La partición resultante, o el conjunto de clases de equivalencia distintas, es a veces sorprendentemente familiar. Este es el caso del ejemplo siguiente, en el que nos adherimos a la práctica habitual de usar un símbolo parecido al de la igualdad, como  $\sim$ , para denotar una relación de equivalencia.

**Ejemplo.** Sea  $X$  el conjunto de los pares ordenados de enteros  $(a, b)$  con  $b \neq 0$ . Demostrar que la relación  $\sim$  definida en  $X$  por

$$(a, b) \sim (c, d) \iff ad = bc$$



es una relación de equivalencia.

**SOLUCIÓN:** Comprobaremos las tres propiedades.

Propiedad reflexiva: puesto que  $ab = ba$ , tenemos que  $(a, b) \sim (a, b)$ .

Propiedad simétrica: utilizando la definición de  $\sim$  tenemos las implicaciones

$$(a, b) \sim (c, d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c, d) \sim (a, b).$$

Propiedad transitiva: supóngamos que  $(a, b) \sim (c, d)$  y  $(c, d) \sim (e, f)$ , de forma que  $ad = bc$  y  $cf = de$ . Entonces

$$adf = adf = bc f = bde = bed,$$

y, puesto que  $d \neq 0$ , tenemos que  $af = be$ . Resulta que  $(a, b) \sim (e, f)$ , como queríamos demostrar.  $\square$

En este ejemplo las clases de equivalencia son, en efecto, objetos familiares, ya que podemos identificar la clase de  $(a, b)$  con la fracción  $a/b$ . La clase de  $(1, 2)$ , por ejemplo, contiene los pares  $(2, 4), (3, 6), (4, 8)$ , etc., al igual que la fracción  $\frac{1}{2}$  es equivalente a  $\frac{2}{4}, \frac{3}{6}, \frac{4}{8}$ , etc. Esto proporciona un método para construir las fracciones utilizando únicamente las propiedades de los enteros formuladas en el capítulo 1. El hecho de que una fracción sea, de hecho, una clase de equivalencia no es ningún problema, ya que todos hemos sido educados en la idea de que  $\frac{1}{2}$  y  $\frac{2}{4}$  habían de considerarse equivalentes.

El tipo de construcción anterior es muy frecuente en matemáticas; de hecho, el siguiente capítulo está dedicado precisamente a una construcción de este tipo.

### Ejercicios 5.2 (continuación)

2 Sea  $X = \{1, 2, 5, 6, 7, 9, 11\}$  y digamos que  $x \sim x'$  siempre que  $x - x'$  sea divisible por 5. Comprobar que  $\sim$  es una relación de equivalencia y describir la partición de  $X$  en clases de equivalencia.

3 Se disponen cuatro sillas con los números 1, 2, 3 y 4 alrededor de una mesa circular dejando el mismo espacio entre dos cualesquiera de ellas. Un

esquema para sentar a cuatro personas puede describirse como una tabla de la forma

1	2	3	4
$C$	$A$	$B$	$D$

que significa que  $C$  ocupa la silla 1,  $A$  la 2, etc. Dos esquemas están *relacionados* (en la relación  $R$ ) si puede obtenerse uno a partir del otro moviendo a todo el mundo el mismo número de posiciones hacia la derecha.

- (i) Demostrar que el número total de esquemas es 24.
- (ii) Demostrar que  $R$  es una relación de equivalencia.
- (iii) Hallar el número de clases de equivalencia y dar una representación de cada una de ellas.

4 Hallar el número de esquemas (véase ejercicio anterior) y el número de clases de equivalencia si hay  $n$  personas y  $n$  sillas.

5 Se define una relación  $\approx$  en  $\mathbb{Z}$  mediante la regla  $n \approx n'$  si  $nn' > 0$ . Demostrar que la relación es simétrica y transitiva, pero no reflexiva.

6 ¿Dónde está el error en el siguiente intento de demostrar que si una relación  $\sim$  es simétrica y transitiva, también es reflexiva?

Si  $a \sim b$ , entonces  $b \sim a$  (propiedad simétrica).

Pero  $a \sim b$  y  $b \sim a$  implican  $a \sim a$  (propiedad transitiva).

Así pues,  $a \sim a$  para todo  $a$ .

### 5.3 Distribuciones y números multinomiales

Otra forma más de considerar una partición  $\{X_i | i \in I\}$  de un conjunto  $X$  es considerar la función asociada  $p$  de  $X$  en  $I$ , definida por

$$p(x) = i \text{ si } x \in X_i.$$

Esta regla define  $p$  correctamente, ya que cada  $x$  pertenece exactamente a una parte  $X_i$ . Más concretamente, en lugar de partir el conjunto de objetos, llevamos a cabo una *distribución* de los objetos en cajas etiquetadas por los elementos del conjunto de índices. La figura 5.3 ilustra un ejemplo.

Por definición, las partes de una partición son no vacías, con lo que  $p$  es exhaustiva: cada caja recibe al menos un objeto. Recuérdese que

previamente ya utilizamos la imagen de "objetos en cajas" en nuestra discusión del principio de las cajas (apartado 2.4), pero allí se trataba de funciones inyectivas más que exhaustivas.

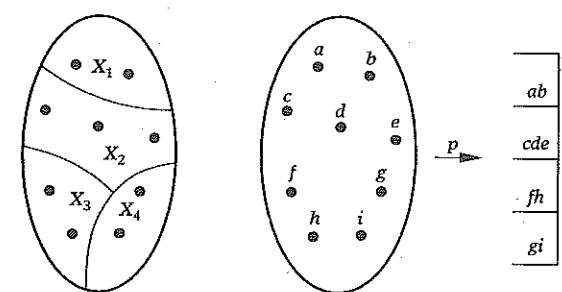


Fig. 5.3 Una partición y la correspondiente distribución.

La conexión entre particiones y distribuciones también funciona en la dirección opuesta. Dada una función exhaustiva  $p$  de un conjunto  $X$  en un conjunto  $Y$ , los subconjuntos de  $X$  definidos, para cada  $y$  de  $Y$ , por

$$X_y = \{x \in X | p(x) = y\}$$

forman una partición de  $X$ . Esta relación es la base de un sencillo método para contar funciones exhaustivas.

**Teorema 5.3.1.** Sea  $J$  el conjunto de funciones exhaustivas de un  $n$ -conjunto  $X$  en un  $k$ -conjunto  $Y$ . Entonces

$$|J| = k! S(n, k).$$

**DEMOSTRACIÓN:** Cada función exhaustiva  $p$  de  $X$  en  $Y$  induce una partición de  $X$  en  $k$  partes, tal como hemos visto. Recíprocamente, dada una partición de  $X$  en  $k$  partes, hay  $k!$  funciones exhaustivas que la inducen, ya que a cada una de las  $k$  partes puede asignársele uno de los  $k$  elementos de  $Y$  de forma biyectiva. Por lo tanto, el número de funciones exhaustivas es  $k!$  por el número de particiones  $S(n, k)$ .  $\square$

Muchos problemas prácticos pueden ser analizados en términos de "objetos en cajas". Por ejemplo, supongamos que hemos de contar de cuántas maneras podemos repartir las cartas en una partida de bridge. En este caso tenemos 52 objetos (las cartas) y cuatro cajas (los jugadores), y hemos de asignar 13 cartas a cada jugador. Uno de los jugadores (pongamos N) es el que da las cartas, y los otros tres (E, S, O) han de subastar por turno, con lo que es importante qué jugador recibe qué cartas. En otras palabras, no estamos preguntando por el número de particiones de un 52-conjunto  $X$  en cuatro 13-conjuntos, sino por el número de funciones exhaustivas de un 52-conjunto en un 4-conjunto  $Y = \{N, E, S, O\}$ , con la propiedad de que cada elemento de  $Y$  recibe 13 elementos de  $X$ .

Más en general, podemos preguntarnos por el número de funciones exhaustivas de un  $n$ -conjunto en un  $k$ -conjunto  $\{y_1, y_2, \dots, y_k\}$ , con la propiedad de que  $n_1$  objetos van a la primera caja  $y_1$ ,  $n_2$  van a  $y_2$ , etc. Indicamos este número por

$$\binom{n}{n_1, n_2, \dots, n_k},$$

y decimos que es un **número multinomial**. Desde luego, es necesario que  $n_1 + n_2 + \dots + n_k = n$ .

Los números multinomiales son una generalización de los números binomiales. Cuando  $k = 2$ , un número multinomial es igual a un número binomial; en concreto,

$$\binom{n}{n_1, n_2} = \binom{n}{n_1},$$

ya que ambos números cuentan las maneras de seleccionar los  $n_1$  objetos que van a la primera caja; los restantes  $n_2 = n - n_1$  objetos han de ir necesariamente a la segunda. Es fácil ver que podemos obtener fórmulas recurrentes para los números multinomiales parecidas a la recurrencia básica de los números binomiales (como la del ejercicio 5.3.4), pero como en estas fórmulas intervienen recursiones múltiples complicadas, demostraremos directamente una fórmula explícita.

**Teorema 5.3.2.** Dados enteros positivos  $n, n_1, n_2, \dots, n_k$  tales que  $n_1 + n_2 + \dots + n_k = n$ , se tiene que

$$\binom{n}{n_1, n_2, \dots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

**DEMOSTRACIÓN:** Sea  $X = \{x_1, x_2, \dots, x_n\}$ ,  $Y = \{y_1, y_2, \dots, y_k\}$ . Una permutación cualquiera  $\pi$  de  $N_n$  lleva a cabo una reordenación de  $X$  de la forma

$$x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}.$$

Definamos una función exhaustiva de  $X$  en  $Y$  que envíe los  $n_1$  primeros elementos de esta lista a  $y_1$ , los siguientes  $n_2$  a  $y_2$ , y así sucesivamente. Ésta es una función exhaustiva del tipo que cuenta el número multinomial.

Sin embargo, obtenemos la misma función si permutamos los primeros  $n_1$  objetos entre sí, los siguientes  $n_2$  entre sí, etc. Resulta que, de las  $n!$  permutaciones posibles, hay  $n_1! n_2! \cdots n_k!$  que inducen la misma función. Así pues, el número total es el que se afirma.  $\square$

**Ejemplo.** ¿Cuántas palabras de 11 letras pueden formarse con las letras de la palabra ABRACADABRA?

**SOLUCIÓN:** Cada palabra tiene 11 letras  $x_1, x_2, \dots, x_{11}$ , y cinco de estas letras son una  $A$ , dos son una  $B$ , dos son una  $R$ , una es una  $C$  y otra es una  $D$ . Cada palabra corresponde a una función exhaustiva del conjunto de 11 letras  $\{x_1, x_2, \dots, x_{11}\}$  en el conjunto de cinco cajas  $\{A, B, R, C, D\}$ , tal que cinco objetos van a la caja  $A$ , dos a la  $B$ , dos a la  $R$ , una a la  $C$  y una a la  $D$ . El número requerido es

$$\binom{11}{5, 2, 2, 1, 1},$$

y, por el teorema 5.3.2, su valor es

$$\frac{11!}{5! 2! 2! 1! 1!} = 11 \times 9 \times 7 \times 6 \times 5 \times 4 = 83\,160. \quad \square$$

Es conveniente extender esta definición de los números multinomiales al caso en que uno o más de los enteros  $n_i$  ( $1 \leq i \leq k$ ) son cero. Si  $n_1, n_2, \dots, n_k$  son enteros *no negativos*, definimos el símbolo

$$\binom{n}{n_1, n_2, \dots, n_k}$$

como el número de funciones de un  $n$ -conjunto en un conjunto de  $k$  cajas, con la propiedad de que  $n_1$  objetos van a la primera caja,  $n_2$  objetos

a la segunda, y así sucesivamente. En este caso las funciones no son necesariamente exhaustivas, ya que alguno de los  $n_i$  puede ser cero. Sin embargo, con la convención de que  $0! = 1$ , resulta claro que la fórmula

$$\binom{n}{n_1, n_2, \dots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

sigue siendo válida.

Puesto que los números multinomiales son una generalización de los binomiales, no es de extrañar que exista una generalización del teorema del binomio. Se conoce como **teorema multinomial**.

**Teorema 5.3.3.** Para cualesquiera enteros positivos  $n$  y  $k$  se tiene que

$$(x_1 + x_2 + \cdots + x_k)^n = \sum \binom{n}{n_1, n_2, \dots, n_k} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k},$$

donde la suma se toma sobre todas las  $k$ -plas de enteros no negativos  $(n_1, n_2, \dots, n_k)$  tales que  $n_1 + n_2 + \cdots + n_k = n$ .

**DEMOSTRACIÓN:** Al multiplicar los  $n$  factores  $x_1 + x_2 + \cdots + x_k$ , se obtienen productos de la forma  $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$  eligiendo el término  $x_1$  de  $n_1$  factores, el término  $x_2$  de  $n_2$  factores, etc. En otras palabras, un producto típico corresponde a una función del conjunto de los  $n$  factores en el conjunto  $\{x_1, x_2, \dots, x_k\}$  con la propiedad de que  $n_1$  de los factores van a parar a  $x_1$ ,  $n_2$  de ellos van a  $x_2$ , etc. Según la definición de los números multinomiales, hay

$$\binom{n}{n_1, n_2, \dots, n_k}$$

funciones de este tipo, y el teorema está demostrado.  $\square$

Debido a su ocurrencia como coeficientes en la expansión de  $(x_1 + x_2 + \cdots + x_k)^n$ , los números multinomiales se conocen también como *coeficientes multinomiales*. Sin embargo, la demostración del teorema multinomial nos permite ver que aparecen porque representan el número de funciones de un cierto tipo, y por este motivo preferimos utilizar un nombre que acentúa su carácter de números combinatorios básicos.

### Ejercicios 5.3

1 Formular y resolver el siguiente problema como una pregunta sobre funciones exhaustivas de un 11-conjunto en un 4-conjunto: "¿Cuántas palabras de 11 letras pueden formarse con las letras de la palabra MISSISSIPPI?"

2 Evaluar los números multinomiales

$$\binom{10}{4, 3, 2, 1} \text{ y } \binom{9}{5, 2, 2}.$$

3 Demostrar que el número de posiciones distintas posibles después de cuatro movimientos del juego de tres en raya es 756.

4 Demostrar que si  $a + b + c = n$ , entonces

$$\binom{n}{a, b, c} = \binom{n-1}{a-1, b, c} + \binom{n-1}{a, b-1, c} + \binom{n-1}{a, b, c-1}.$$

Obtener fórmulas análogas para un número multinomial general.

5 Calcular el coeficiente de

- (i)  $x^5 y^3 z^2$  en  $(x + y + z)^{10}$ ,
- (ii)  $x^3 y z^4 t$  en  $(x + y + z + t)^9$ .

6 Sea  $p$  un número primo. Demostrar que el número multinomial

$$\binom{p}{n_1, n_2, \dots, n_k}$$

es divisible por  $p$ , a menos de que uno de los  $n_i$  ( $1 \leq i \leq k$ ) sea igual a  $p$ .

### 5.4 Particiones de un entero positivo

Dada una partición de un  $n$ -conjunto  $X$

$$X = X_1 \cup X_2 \cup \cdots \cup X_k,$$

tenemos una ecuación correspondiente

$$n = n_1 + n_2 + \cdots + n_k,$$

donde  $n_i$  es el tamaño de  $X_i$  ( $1 \leq i \leq k$ ). Nos referimos a esta ecuación como una **partición del entero  $n$**  en  $k$  partes. Hay que insistir en que las partes no son cero (ya que los conjuntos  $X_i$  no son vacíos) y en que el orden de las partes es irrelevante. Las particiones del entero 6 son

$$\begin{array}{lll} 6, & 5+1, & 4+2, \\ 4+1+1, & 3+3, & 3+2+1, \\ 3+1+1+1, & 2+2+2, & 2+2+1+1, \\ 2+1+1+1+1, & 1+1+1+1+1+1. & \end{array}$$

La notación estándar para las particiones de un entero positivo  $n$  se obtiene contando el número de partes de cada tamaño. Si hay  $\alpha_i$  partes de tamaño  $i$ , la partición se escribe

$$[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}].$$

Con esta notación, y con algunas abreviaturas triviales, las particiones de 6 son

$$\begin{array}{ll} [6], & [3^2], \\ [15], & [2^3], \\ [1^2 4], & [24], \\ [1^3 3], & [123], \\ [1^4 2], & [1^2 2^2], \\ [1^6]. & \end{array}$$

Es poco afortunado que esta notación convencional para las particiones utilice un símbolo multiplicativo para una descomposición aditiva. Vale la pena recordar que cuando decimos, por ejemplo, que  $[2^3]$  es una partición de 6, queremos decir que 6 es la *suma* de 3 doses.

El problema de contar particiones de  $n$  es muy interesante, pero requiere técnicas que todavía no han sido tratadas en este libro. Volveremos a él en el capítulo 19.

#### Ejercicios 5.4

- 1 Escribir las particiones de 7 en notación estándar.
- 2 Sea  $p_k(n)$  el número de particiones de  $n$  en  $k$  partes. Demostrar que

$$p_k(n) = p_k(n-k) + p_{k-1}(n-k) + \dots + p_1(n-k).$$



3 Usar la fórmula del ejercicio 2 para construir una tabla de los números  $p_k(n)$  para  $1 \leq k \leq n \leq 7$ , y contrastar la respuesta con la del ejercicio 1.

#### 5.5 Clasificación de las permutaciones

En el apartado 3.6 mostramos cómo escribir una permutación cualquiera como producto de ciclos disjuntos. Por ejemplo, la permutación de  $N_9$  que se muestra en la figura 5.4 se escribe como  $(13624)(587)(9)$ ; resulta claro que sus ciclos son las partes de una partición de  $N_9$ , tal como se indica a la derecha. Esta observación puede utilizarse para dar una justificación formal a la notación en ciclos mediante una relación de equivalencia. Los detalles se indican en el ejercicio 5.7.18.

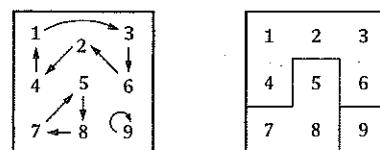


Fig. 5.4 Una permutación de  $N_9$  y la partición correspondiente.

En este apartado estudiamos la clasificación de las permutaciones según su estructura en ciclos. Recuérdese que  $S_n$  denota el conjunto de todas las permutaciones de  $N_n$ . Cada permutación  $\pi$  de  $S_n$  tiene asociada una partición de  $N_n$  cuyos ciclos son las partes de  $\pi$ , lo cual, a su vez, nos da una partición del entero  $n$ . Nos referiremos a esta última como al **tipo** de  $\pi$ . En otras palabras, si  $\pi$  tiene  $\alpha_i$  ciclos de longitud  $i$  ( $1 \leq i \leq n$ ), entonces el tipo de  $\pi$  es la partición  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$  de  $n$ . La permutación que muestra la figura 5.4 es de tipo  $[1^3 2^2 3^1]$ .

Es fácil contar el número de permutaciones de un tipo dado, siempre que recordemos las convenciones de la notación en ciclos. Supongamos, por ejemplo, que queremos contar el número de elementos de  $S_{14}$  de tipo  $[2^2 3^2 4]$ . Hemos de colocar los símbolos 1, 2, ..., 14 en el esquema de ciclos

$$(\cdot\cdot)(\cdot\cdot)(\cdot\cdot\cdot)(\cdot\cdot\cdot)(\cdot\cdot\cdot)$$

y tenemos  $14!$  maneras de hacerlo. Sin embargo, una permutación dada  $\pi$  proviene de este proceso por diferentes vías. Respecto a cada ciclo,

cualquier elemento del ciclo puede colocarse en primera posición y el orden de los restantes queda determinado por  $\pi$ . De forma que hay dos maneras de obtener cada 2-ciclo, tres maneras de obtener cada 3-ciclo y cuatro maneras de obtener el 4-ciclo. Así pues, los ciclos pueden reordenarse internamente de  $2^2 \times 3^2 \times 4$  maneras para cada  $\pi$ . En general, para una permutación de tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$  hay

$$1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}$$

maneras de reordenarla internamente.

Por otra parte, el orden de los ciclos de la misma longitud es arbitrario. En el ejemplo hay  $2!$  maneras de ordenar los dos 2-ciclos y  $2!$  maneras de ordenar los 3-ciclos. En general, el número a tener en cuenta es

$$\alpha_1! \alpha_2! \dots \alpha_n!$$

Por lo tanto, el número de permutaciones de tipo  $[2^2 3^2 4]$  es

$$\frac{14!}{2^2 \times 3^2 \times 4 \times 2! \times 2!},$$

y el número de tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$  es

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!}.$$

A menudo es más sencillo utilizar métodos de sentido común para contar permutaciones de un tipo dado, en lugar de utilizar esta fórmula aparatoso. Por ejemplo, los números en la clasificación de  $S_5$  que se muestran en la tabla 5.5.1 pueden obtenerse de varias maneras sencillas.

Tabla 5.5.1

Tipo	Ejemplo	Número
$[1^5]$	id	1
$[1^3 2]$	$(12)(3)(4)(5)$	10
$[1^2 3]$	$(123)(4)(5)$	20
$[1^2 2^2]$	$(12)(43)(5)$	15
$[1^4]$	$(1234)(5)$	30
$[2^3]$	$(123)(45)$	20
$[5]$	$(12345)$	24
		120

La clasificación de las permutaciones por su tipo es doblemente útil, dado que existe una descripción alternativa de las clases con interesantes aplicaciones a la teoría algebraica de las permutaciones (capítulos 14 y 20). Sean  $\alpha$  y  $\beta$  permutaciones de  $S_n$ . Si existe una permutación  $\sigma$  de  $S_n$  tal que

$$\sigma \alpha \sigma^{-1} = \beta,$$

decimos que  $\alpha$  y  $\beta$  son conjugadas.

**Teorema 5.5.** Dos permutaciones son conjugadas si, y sólo si, son del mismo tipo.

**DEMOSTRACIÓN:** Supongamos que  $\alpha$  y  $\beta$  son conjugadas, de forma que  $\sigma \alpha \sigma^{-1} = \beta$ . Si  $\alpha(x_1) = x_2$ , sea  $y_1 = \sigma(x_1)$ ,  $y_2 = \sigma(x_2)$ ; si  $\alpha(x_2) = x_3$ , sea  $y_3 = \sigma(x_3)$ ; y así sucesivamente (figura 5.5). Entonces

$$\beta(y_1) = \sigma \alpha \sigma^{-1}(\sigma(x_1)) = \sigma \alpha(x_1) = \sigma(x_2) = y_2.$$

De forma similar  $\beta(y_2) = y_3$ ,  $\beta(y_3) = y_4$ , etc. En consecuencia, para cada ciclo  $(x_1 x_2 \dots x_r)$  de  $\alpha$  tenemos un ciclo correspondiente  $(y_1 y_2 \dots y_r)$  de  $\beta$ , de donde resulta que  $\alpha$  y  $\beta$  tienen el mismo tipo.

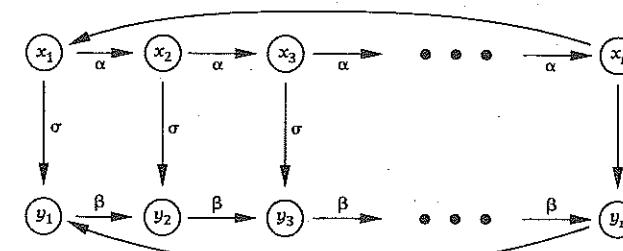


Fig. 5.5 Permutaciones conjugadas.

Recíprocamente, supongamos que  $\alpha$  y  $\beta$  son del mismo tipo. Puesto que tienen el mismo número de ciclos de cada longitud, podemos establecer una correspondencia biyectiva entre sus ciclos de forma que a un ciclo cualquiera  $(x_1 x_2 \dots x_r)$  de  $\alpha$  le corresponda un ciclo  $(z_1 z_2 \dots z_r)$  de  $\beta$ .

Definimos  $\sigma$  mediante la regla  $\sigma(x_i) = z_i$  ( $1 \leq i \leq r$ ), y de forma similar para los restantes ciclos. Entonces  $\sigma\alpha\sigma^{-1} = \beta$ , ya que

$$\sigma\alpha\sigma^{-1}(z_1) = \sigma\alpha(x_1) = \sigma(x_2) = z_2 = \beta(z_1),$$

y así sucesivamente. En consecuencia,  $\alpha$  y  $\beta$  son conjugadas.  $\square$

### Ejercicios 5.5

- 1 Escribir la clasificación de los elementos de  $S_6$  de forma análoga a la tabla 5.5.1 anterior para  $S_5$ .
- 2 Sean  $\alpha = (13624)(587)(9)$  y  $\beta = (15862)(394)(7)$ . Escribir una permutación  $\sigma$  de  $S_9$  tal que  $\sigma\alpha\sigma^{-1} = \beta$ .
- 3 Demostrar que si  $\pi$  y  $\tau$  son elementos de  $S_n$ , entonces  $\pi\tau$  y  $\tau\pi$  tienen el mismo tipo. [Indicación: usar el teorema 5.5].
- 4 Demostrar directamente a partir de la definición (sin utilizar el teorema 5.5) que la conjugación es una relación de equivalencia en  $S_n$ .
- 5 Usar la clasificación de  $S_6$  obtenida en el ejercicio 1 para hallar el número de desarreglos de  $S_6$  (véase la definición en el apartado 4.4).
- 6 Hallar el número de permutaciones  $\sigma$  que tienen la propiedad enunciada en el ejercicio 2.

### 5.6 Permutaciones pares e impares

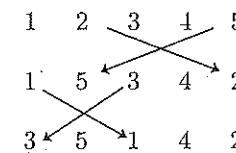
La clasificación de  $S_5$  obtenida en el apartado anterior tiene una propiedad notable que debiera ser evidente a partir de la siguiente tabulación de las clases:

Tipo	Número	Tipo	Número
$[1^5]$	1	$[1^32]$	10
$[1^23]$	20	$[14]$	30
$[12^2]$	15	$[23]$	20
$[5]$	24		
	60		60

Tenemos una partición de  $S_5$  en dos partes de 60 permutaciones cada una. En este apartado demostraremos que cada  $S_n$  con  $n \geq 2$  puede partirse

en dos partes iguales, y veremos que hay una forma sencilla para decidir a qué parte pertenece una permutación dada.

La observación clave es que cualquier permutación puede conseguirse permutando ciertos pares de objetos sucesivamente. Por ejemplo, para obtener 35142 a partir de 12345 necesitamos únicamente dos cambios:

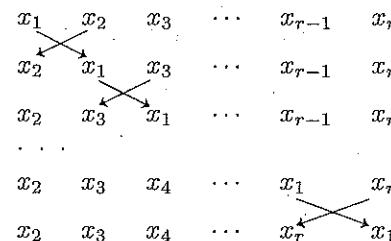


En términos de permutaciones, la permutación que efectúa la transformación de 12345 en 35142 es  $(13)(25)(4)$  y los dos 2-ciclos corresponden exactamente a los dos cambios anteriores. En general, no es evidente que toda permutación pueda expresarse en términos de 2-ciclos de esta forma y nuestra primera tarea es demostrar que, en efecto, así es.

El nombre técnico para una permutación que intercambia dos objetos y deja el resto sin mover es una **trasposición**. Así pues, un elemento de  $S_n$  es una trasposición si es del tipo  $[1^{n-2}2]$ : tiene  $(n-2)$  1-ciclos y un 2-ciclo. Ahora bien, un ciclo cualquiera como  $(x_1x_2\dots x_r)$  efectúa la reordenación

$$x_1x_2\dots x_{r-1}x_r \text{ a } x_2x_3\dots x_rx_1,$$

que puede obtenerse mediante trasposiciones sucesivas de la siguiente forma:



De modo que podemos escribir

$$(x_1x_2\dots x_{r-1}x_r) = (x_1x_r)\dots(x_1x_3)(x_1x_2).$$

Cada trasposición está representada por el correspondiente 2-ciclo, y hemos suprimido los 1-ciclos, ya que no tienen ningún efecto. Hay que recordar también que la trasposición escrita en último lugar es la primera que se efectúa, de acuerdo con la regla para combinar permutaciones. Puesto que cada permutación puede descomponerse en ciclos, también puede descomponerse en trasposiciones utilizando la regla anterior. Por ejemplo,

$$(136)(2457) = (16)(13)(27)(25)(24).$$

Insistimos en dos cuestiones sobre la descomposición en trasposiciones. En primer lugar, las trasposiciones no son disjuntas, de forma que un objeto puede moverse más de una vez. En segundo lugar, la descomposición no es única en absoluto, ya que no sólo puede modificarse el orden de las trasposiciones, sino que podemos usar un conjunto de trasposiciones totalmente diferente, por ejemplo

$$(136)(2457) = (15)(35)(36)(57)(14)(27)(12).$$

Queremos demostrar que, aunque existen varias descomposiciones de una permutación dada, todas ellas comparten una propiedad común.

Sea  $c(\pi)$  el número total de ciclos de una permutación  $\pi$ , de forma que si  $\pi$  es del tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ , entonces  $c(\pi) = \alpha_1 + \alpha_2 + \dots + \alpha_n$ . Supongamos que componemos  $\pi$  con una trasposición  $\tau$ , dando lugar a una nueva permutación  $\tau\pi$ . ¿Cuál es la relación entre  $c(\tau\pi)$  y  $c(\pi)$ ?

Supongamos que  $\tau$  intercambia  $a$  y  $b$ , de forma que  $\tau(a) = b$ ,  $\tau(b) = a$  y  $\tau(k) = k$  si  $k \neq a, b$ . Si  $a$  y  $b$  están en el mismo ciclo de  $\pi$ , tenemos que

$$\pi = (ax \dots yb \dots z) \dots \text{ y otros ciclos.}$$

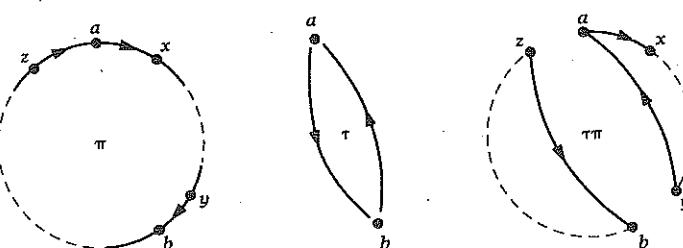


Fig. 5.6 Composición de  $\tau$  con un ciclo de  $\pi$  (primer caso).

La permutación compuesta  $\tau\pi$  (primero  $\pi$  y después  $\tau$ ) puede calcularse fácilmente; tal como ilustra la figura 5.6 es

$$\tau\pi = (ax \dots y)(b \dots z) \dots \text{ y los mismos otros ciclos.}$$

En este caso,  $c(\tau\pi) = c(\pi) + 1$ . Por otra parte, si  $a$  y  $b$  están en ciclos distintos de  $\pi$ , de forma que

$$\pi = (ax \dots y)(b \dots z) \dots \text{ y otros ciclos,}$$

entonces un cálculo parecido muestra que

$$\tau\pi = (ax \dots yb \dots z) \dots \text{ y los mismos otros ciclos.}$$

En este caso  $c(\tau\pi) = c(\pi) - 1$ . En ambos casos, la composición de  $\pi$  con una trasposición modifica el número de ciclos en uno, y este hecho sencillo nos lleva al siguiente teorema.

**Teorema 5.6.1.** Supongamos que una permutación  $\pi$  de  $S_n$  puede escribirse como la composición de  $r$  trasposiciones y al mismo tiempo como la composición de  $r'$  trasposiciones. Entonces, o bien  $r$  y  $r'$  son ambos pares, o bien son ambos impares.

**DEMOSTRACIÓN:** Sea  $\pi = \tau_r \tau_{r-1} \dots \tau_2 \tau_1$ , donde  $\tau_i$  ( $1 \leq i \leq r$ ) es una trasposición. Ya que  $\tau_1$  posee un 2-ciclo y  $(n-2)$  1-ciclos, tenemos que

$$c(\tau_1) = 1 + (n-2) = n-1.$$

Al componer  $\tau_2, \tau_3, \dots, \tau_r$  sucesivamente con  $\tau_1$ , el resultado final es  $\pi$ . En cada paso, el número de ciclos se modifica en 1: supongamos que crece en  $g$  ocasiones y decrece  $h$  veces. El número final de ciclos será

$$(n-1) + g - h = c(\pi).$$

Pero  $g + h$  es el número total de pasos,  $r-1$ . Así que

$$\begin{aligned} r &= 1 + g + h = 1 + g + (n-1 + g - c(\pi)) \\ &= n - c(\pi) + 2g. \end{aligned}$$

Por el mismo argumento, si  $\pi$  es igual a la composición de  $r'$  trasposiciones, existe un entero  $g'$  tal que  $r' = n - c(\pi) + 2g'$ . Así pues,

$$r - r' = 2(g - g'),$$

y dado que el término de la derecha es par, el resultado queda demostrado.

□

Como consecuencia del teorema podemos decir que una permutación es **par** o **impar** según que el número de trasposiciones en cualquier descomposición sea par o impar. También podemos definir el **signo** de una permutación  $\pi$ , y lo escribiremos  $\text{sgn } \pi$ , como  $+1$  si  $\pi$  es par, y  $-1$  si es impar. Por lo tanto,

$$\text{sgn } \pi = (-1)^r,$$

donde  $r$  es el número de trasposiciones en una descomposición de  $\pi$ . En particular,  $\text{sgn id} = (-1)^0 = +1$ . Si  $\pi$  y  $\sigma$  se descomponen, respectivamente, en  $r$  y  $s$  trasposiciones, está claro que la composición  $\pi\sigma$  puede descomponerse en  $r+s$  trasposiciones, de donde

$$\text{sgn } \pi\sigma = (-1)^{r+s} = (-1)^r(-1)^s = \text{sgn } \pi \text{ sgn } \sigma.$$

Esto implica, por ejemplo, que  $\text{sgn } \pi^{-1} = \text{sgn } \pi$ , ya que  $\pi^{-1}\pi$  es la identidad y

$$\text{sgn } \pi^{-1} \text{ sgn } \pi = \text{sgn } \pi^{-1}\pi = \text{sgn id} = +1.$$

Ahora podemos enunciar el resultado general sobre la partición de  $S_n$  que comentábamos al principio del apartado en el caso  $n = 5$ .

**Teorema 5.6.2.** Para todo entero  $n \geq 2$ , exactamente la mitad de las trasposiciones de  $S_n$  son pares y la mitad son impares.

**DEMOSTRACIÓN:** Sea  $\pi_1, \pi_2, \dots, \pi_k$  una lista con las permutaciones pares de  $S_n$ . (Desde luego existe alguna, ya que  $\text{id}$  es par.) Sea  $\tau$  una trasposición cualquiera de  $S_n$ , pongamos  $\tau = (12)(3)(4)\cdots(n)$ .

Las permutaciones  $\tau\pi_1, \tau\pi_2, \dots, \tau\pi_k$  son todas distintas, ya que si  $\tau\pi_i = \tau\pi_j$ , utilizando las reglas fundamentales dadas en el teorema 3.6, tendríamos que

$$\pi_i = (\tau^{-1}\tau)\pi_i = \tau^{-1}(\tau\pi_i) = \tau^{-1}(\tau\pi_j) = (\tau^{-1}\tau)\pi_j = \pi_j.$$

Más aún, estas permutaciones son todas impares, ya que

$$\text{sgn } \tau\pi_i = \text{sgn } \tau \text{ sgn } \pi_i = (-1) \times (+1) = -1.$$

Finalmente, demostraremos que *toda* permutación impar  $\rho$  es una de las  $\tau\pi_i$  ( $1 \leq i \leq n$ ). Por ser

$$\text{sgn } \tau^{-1}\rho = \text{sgn } \tau^{-1} \text{ sgn } \rho = (-1) \times (-1) = +1,$$

resulta que  $\tau^{-1}\rho$  es una de las permutaciones pares  $\pi_i$ . Así pues,

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

como afirmábamos. Hemos demostrado que hay tantas permutaciones pares como impares. □

La partición de  $S_n$  en dos partes iguales tiene varias consecuencias interesantes. El siguiente es un ejemplo de matemática “recreativa”.

**Ejemplo.** Se colocan ocho piezas con etiquetas A, E, I, O, U, Y, R, T en un marco cuadrado tal como muestra el primer diagrama de la figura 5.7. Un movimiento legal consiste en deslizar una pieza hacia el espacio libre. Demostrar que es imposible obtener la disposición que muestra el segundo diagrama mediante una sucesión de movimientos legales.

A	E	I
O	U	Y
R	T	

Y	O	U
A	R	E
I	T	

Fig. 5.7 ¿Puede hacerse?

**SOLUCIÓN:** Denotaremos el espacio en blanco por  $\square$ , de forma que la disposición inicial es AEIOUYRT $\square$  y la final es YOUAREIT $\square$ . Mover una letra  $X$  al espacio en blanco corresponde a un 2-ciclo ( $X\square$ ). Para

llegar a una disposición final con  $\square$  en su lugar original, tendremos que haber movido  $\square$  el mismo número de veces hacia arriba que hacia abajo, y el mismo número de veces hacia la izquierda que hacia la derecha. En consecuencia, el número total de movimientos es par y, dado que cada movimiento es una trasposición, la disposición final tiene que provenir de una permutación *par*. Sin embargo, la permutación que efectúa la reordenación de

$$\text{AEIOUYRT}\square$$

en

$$\text{YOUAREIT}\square$$

es igual a  $(\text{AYEO})(\text{IUR})(\text{T})(\square)$ . Ésta es una permutación *ímpar*, ya que el 4-ciclo es equivalente a tres trasposiciones y el 3-ciclo es equivalente a dos trasposiciones. Resulta que es imposible llegar a la situación requerida por una sucesión de movimientos legales.  $\square$

### Ejercicios 5.6

1 Expresar los siguientes elementos de  $S_8$  en términos de 2-ciclos y hallar el signo de cada uno de ellos:

$$\alpha = (1357)(2468),$$

$$\beta = (127)(356)(48),$$

$$\gamma = (135)(678)(2)(4).$$

2 Sin utilizar el teorema 5.5, demostrar que

$$\operatorname{sgn} \pi \sigma \pi^{-1} = \operatorname{sgn} \sigma \quad (\sigma, \pi \in S_n).$$

3 Demostrar que si  $\pi$  es del tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ , entonces

$$\operatorname{sgn} \pi = (-1)^{\alpha_2 + \alpha_4 + \alpha_6 + \dots}$$

4 ¿Cuáles de las siguientes posiciones pueden obtenerse mediante movimientos legales a partir de la disposición inicial que se muestra en el ejemplo?

$$(i) \begin{array}{ccc} \text{A} & \text{R} & \text{E} \\ \text{Y} & \text{O} & \text{U} \\ \text{I} & \text{T} & \end{array}$$

$$(ii) \begin{array}{ccc} \text{Y} & \text{E} & \text{A} \\ \text{T} & \text{O} & \text{U} \\ \text{U} & \text{R} & \text{I} \end{array}$$

5 Demostrar que todo ciclo de longitud impar puede escribirse como composición de 3-ciclos (no necesariamente disjuntos). Deducir que una permutación es par si, y sólo si, puede expresarse como composición de 3-ciclos.

### 5.7 Ejercicios diversos

1 ¿Cuántas palabras de 14 letras pueden formarse con las letras de la palabra CLASSIFICATION?

2 Calcular el coeficiente de

$$(i) x^3y^2z^4 \text{ en } (x+y+z)^9,$$

$$(ii) xy^3zt^2u \text{ en } (x+y+z+t+u)^8.$$

3 Calcular  $p(8)$ , el número total de particiones de 8, y comprobar que el número de las que tienen partes distintas es igual al número de aquellas cuyas partes son todas impares. ¿Puede explicar esta igualdad?

4 Sean  $\alpha$  y  $\beta$  los elementos de  $S_8$  que en la notación de ciclos se expresan por

$$\alpha = (123)(456)(78), \quad \beta = (1357)(26)(4)(8).$$

Hallar  $\operatorname{sgn} \alpha$  y  $\operatorname{sgn} \beta$  y expresar  $\alpha$  y  $\beta$  en términos de trasposiciones, utilizando el mínimo número de trasposiciones posibles en cada caso.

5 Demostrar que

$$S(n, 3) = \frac{1}{2}(3^{n-1} + 1) - 2^{n-1}.$$

6 Sea  $\sim$  la relación en  $\mathbb{Z}$  definida por

$$a \sim b \iff a - b \text{ es divisible por 11.}$$

Demostrar que  $\sim$  es una relación de equivalencia en  $\mathbb{Z}$ . ¿Cuál es el número de clases de equivalencia?

7 Se define una relación  $\approx$  en el conjunto  $\mathbb{N} \times \mathbb{N}$  de pares ordenados de enteros positivos mediante la regla

$$(a, b) \approx (c, d) \iff a + d = b + c.$$

Demostrar que  $\approx$  es una relación de equivalencia en  $\mathbb{N} \times \mathbb{N}$ . Explicar cómo puede usarse este resultado para construir  $\mathbb{Z}$  a partir de  $\mathbb{N}$ .

8 Demostrar que

$$\sum_{k=1}^m S(m, k) n(n-1) \cdots (n-k+1) = n^m.$$

9 La Asamblea General de las Naciones Unidas ha decretado que la bandera nacional de cada país debe consistir en  $m$  bandas verticales, cada una de ellas coloreada con uno de entre  $n$  colores, de forma que dos bandas adyacentes no tengan el mismo color. Demostrar que de esta forma pueden construirse  $n!S(m-1, n-1)$  banderas. Se supone que uno de los bordes de la bandera es distingüible por ser el del asta, de manera que  $ABC$  y  $CBA$  representan banderas distintas.

10 Sea  $q_n$  el número total de particiones de un conjunto con  $n$  elementos. Demostrar que

$$q_n = \sum_{k=1}^n \binom{n-1}{k-1} q_{n-k} = \sum_{k=0}^{n-1} \binom{n-1}{k} q_k.$$

11 Utilizar el principio de la criba para demostrar que el número de funciones exhaustivas de un  $n$ -conjunto en un  $k$ -conjunto es

$$\sum_{i=0}^n (-1)^i \binom{n}{i} (n-i)^k.$$

12 Demostrar que

$$S(n, k) = \frac{1}{k!} \sum \binom{n}{n_1, n_2, \dots, n_k},$$

donde la suma se toma sobre todas las  $k$ -plas  $(n_1, n_2, \dots, n_k)$  de enteros positivos que cumplen  $n_1 + n_2 + \dots + n_k = n$ .

13 Demostrar que si la suma del término derecho de la ecuación anterior se toma para todos los enteros *no negativos* que cumplen  $n_1 + n_2 + \dots + n_k = n$ , el resultado es  $k^n$ .

14 ¿De cuántas maneras pueden distribuirse  $mn$  objetos en  $m$  cajas de forma que cada caja contenga  $n$  objetos?

15 Utilizando los números multinomiales, demostrar que para todo entero positivo  $n$  se tiene

- (i)  $2^n$  divide a  $(2n)!$  y el cociente es par;
- (ii)  $(n!)^{n+1}$  divide a  $(n^2)!$ .

16 Demostrar que el número de permutaciones de  $S_6$  de tipo  $[1^4 2]$  es el mismo que el número de las de tipo  $[2^3]$ . Si  $\alpha$  es del primer tipo, hallar el número de permutaciones  $\beta$  del segundo tipo que cumplen  $\alpha\beta = \beta\alpha$ .

17 Dar una lista de los tipos de permutaciones de  $S_7$  que son desarreglos y comprobar así el valor de  $d_7$ .

18 Sea  $\pi$  una permutación de un conjunto finito  $X$ .

- (i) Demostrar que para cada  $x$  de  $X$  existe un entero no negativo  $k$  tal que  $\pi^k(x) = x$ , donde  $\pi^k$  denota la  $k$ -ésima iteración de  $\pi$  y  $\pi^0 = \text{id}$ .
- (ii) Se define una relación  $\sim$  en  $X$  mediante la regla

$$x \sim x' \quad \text{si} \quad x' = \pi^r(x) \quad \text{para algún } r \geq 0.$$

Demostrar que  $\sim$  es una relación de equivalencia en  $X$  y explicar cómo este resultado justifica la notación en ciclos para las permutaciones.

19 El "Puzzle de los quince" consiste en cuadrados numerados 1, 2, ..., 15 dispuestos en un marco  $4 \times 4$  con un espacio en blanco. Como en el ejemplo del apartado 5.6, un movimiento legal consiste en desplazar una pieza al espacio en blanco, creando así un nuevo espacio. Clasificar las posiciones siguientes, poniendo dos posiciones en la misma clase si, y sólo si, puede pasarse de una a otra mediante una sucesión de movimientos legales.

1	2	3	4		1	2	3	4
5	6	7	8		5	6	7	8
9	10	11	12		9	10	11	12
13	14	15			13	15	14	
1	8	9			1	2	3	4
2	7	10	15		12	13	14	5
3	6	11	14		11		15	6
4	5	12	13		10	9	8	7

20 Hallar el número de enteros positivos de diez cifras (en base 10) con la propiedad de que el número de cifras impares distintas es la mitad del número de cifras pares distintas.

## 6 Aritmética modular

### 6.1 Congruencias

Una de las particiones más usuales es la partición de  $\mathbb{Z}$  en números pares e impares. Según la teoría general discutida en el apartado 5.2, esta partición corresponde a una relación de equivalencia en  $\mathbb{Z}$  que (en este caso) puede definirse diciendo que  $x_1$  está relacionado con  $x_2$  si  $x_1 - x_2$  es divisible por 2. Es costumbre usar la notación

$$x_1 \equiv x_2 \pmod{2}$$

para esta relación y decir que  $x_1$  es *congruente* con  $x_2$  *módulo 2*. Así pues,  $x_1$  y  $x_2$  están en la misma parte de la partición si, y sólo si,  $x_1$  es congruente con  $x_2$  módulo 2.

Está claro que podemos usar cualquier entero positivo  $m$  en lugar de 2.

**Definición.** Sean  $x_1$  y  $x_2$  enteros y  $m$  un entero positivo. Decimos que  $x_1$  es *congruente* con  $x_2$  *módulo m*, y lo escribimos

$$x_1 \equiv x_2 \pmod{m},$$

si  $x_1 - x_2$  es divisible por  $m$ .

Es fácil comprobar que la congruencia módulo  $m$  es una relación de equivalencia. Es reflexiva, puesto que  $x - x$  es cero y es divisible por  $m$  para cualquier  $x$ . Es simétrica, ya que si  $x_1 - x_2 = km$ , entonces  $x_2 - x_1 = (-k)m$ . Es transitiva, puesto que si  $x_1 - x_2 = km$  y  $x_2 - x_3 = lm$ , entonces  $x_1 - x_3 = (k + l)m$ .

La utilidad de las relaciones de congruencias proviene principalmente del hecho de que son compatibles con las operaciones aritméticas. En concreto, tenemos el teorema siguiente.

**Teorema 6.1.** Sea  $m$  un entero positivo y  $x_1, x_2, y_1$  e  $y_2$  enteros tales que

$$x_1 \equiv x_2 \pmod{m}, \quad y_1 \equiv y_2 \pmod{m}.$$

Entonces

$$(i) x_1 + y_1 \equiv x_2 + y_2 \pmod{m}, \quad (ii) x_1 y_1 \equiv x_2 y_2 \pmod{m}.$$

**DEMOSTRACIÓN:** (i) Tenemos que  $x_1 - x_2 = mx$  y  $y_1 - y_2 = my$  para ciertos  $x$  e  $y$  de  $\mathbb{Z}$ . Resulta que

$$\begin{aligned} (x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= mx + my \\ &= m(x + y), \end{aligned}$$

de forma que el término izquierdo es divisible por  $m$ .

(ii) Ahora tenemos que

$$\begin{aligned} x_1 y_1 - x_2 y_2 &= (x_1 - x_2)y_1 + x_2(y_1 - y_2) \\ &= mxy_1 + x_2my \\ &= m(xy_1 + x_2y), \end{aligned}$$

y de nuevo el término izquierdo es divisible por  $m$ .  $\square$

**Ejemplo.** Sea  $(x_n x_{n-1} \cdots x_0)_{10}$  la representación en base 10 de un entero positivo  $x$ . Demostrar que

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$$

y utilizar este resultado para comprobar el cálculo

$$54\,321 \times 98\,765 = 5\,363\,013\,565.$$

**SOLUCIÓN:** Según la definición de la representación en base 10, tenemos que

$$\begin{aligned} x - (x_0 + \cdots + x_n) &= x_0 + 10x_1 + \cdots + 10^n x_n - (x_0 + \cdots + x_n) \\ &= (10^1 - 1)x_1 + \cdots + (10^n - 1)x_n. \end{aligned}$$

Ahora bien, para todo  $r \geq 1$ ,

$$\begin{aligned} 10^r - 1 &= (99\ldots9)_{10} \quad r \text{ nueves} \\ 9 \times (11\ldots1)_{10}. \end{aligned}$$

Por lo tanto, 9 divide a  $x - (x_0 + \cdots + x_n)$  como queríamos demostrar.

Por conveniencia, escribiremos  $\theta(x)$  en lugar de  $x_0 + \cdots + x_n$ . Hemos demostrado que  $\theta(x) \equiv x \pmod{9}$ . Por el apartado (ii) del teorema 6.1,

$$\theta(x)\theta(y) \equiv xy \pmod{9},$$

de forma que si  $xy = z$ , debe ser  $\theta(x)\theta(y) \equiv \theta(z) \pmod{9}$ . En el ejemplo,

$$\theta(54\,321) = 15, \quad \theta(98\,765) = 35, \quad \theta(5\,363\,013\,565) = 37$$

y

$$\theta(15) = 6, \quad \theta(35) = 8, \quad \theta(37) = 10.$$

Puesto que  $6 \times 8$  no es congruente con  $10 \pmod{9}$ , tampoco lo es  $15 \times 35$  con  $37$  y  $54\,321 \times 98\,765$  con  $5\,363\,013\,565$ . Si el cálculo fuera correcto, las expresiones serían iguales y, en consecuencia, congruentes módulo 9. El cálculo es, pues, erróneo.

Este método se conoce como el de "borrar nueves".  $\square$

### Ejercicios 6.1

1 Sin desarrollar las multiplicaciones, demostrar que

- (i)  $1\,234\,567 \times 90\,123 \equiv 1 \pmod{10}$ ,
- (ii)  $2\,468 \times 13\,579 \equiv -3 \pmod{25}$ ,

2 Utilizar el método de borrar nueves para demostrar que dos de las siguientes ecuaciones son falsas. ¿Qué puede decirse de la otra ecuación?

- (i)  $5\,783 \times 40\,162 = 233\,256\,846$ ,
- (ii)  $9\,787 \times 1\,258 = 12\,342\,046$ ,
- (iii)  $8\,901 \times 5\,743 = 52\,018\,443$ .

3 Sea  $m \geq 2$  y  $x$  un entero. El resto  $r$  de dividir  $x$  por  $m$  cumple

$$x \equiv r \pmod{m}, \quad 0 \leq r \leq m-1,$$

y a veces se le denomina el *mínimo residuo no negativo* de  $x \pmod{m}$ . Hallar el mínimo residuo no negativo de  $3^{15} \pmod{17}$  y  $15^{81} \pmod{13}$ .

4 Sea  $(x_n x_{n-1} \cdots x_0)_{10}$  la representación en base 10 de un entero positivo  $x$ . Demostrar que

$$x \equiv x_0 - x_1 + x_2 - \cdots + (-1)^n x_n \pmod{11},$$

y utilizar este resultado para comprobar si  $1\,213\,141\,516\,171\,819$  es divisible por 11.

### 6.2 $Z_m$ y su aritmética

En este apartado introduciremos un método más compacto para tratar con las propiedades de las congruencias en los enteros.

Para cada entero  $x$  y entero positivo  $m$ , utilizaremos la notación  $[x]_m$  para denotar la clase de equivalencia de  $x$  con respecto a la congruencia módulo  $m$ . En otras palabras,  $[x]_m$  consiste en todos los enteros  $x'$  para los que  $x' - x$  es un múltiplo de  $m$ . Por ejemplo,

$$\begin{aligned} [5]_3 &= \{\dots, -4, -1, 2, 5, 8, 11, \dots\}, \\ [6]_7 &= \{\dots, -8, -1, 6, 13, 20, \dots\}. \end{aligned}$$

Como es habitual, cada clase de equivalencia tiene varios sinónimos, según el representante que se use. Por ejemplo,

$$\dots = [-8]_7 = [-1]_7 = [6]_7 = [13]_7 = [20]_7 = \dots$$

La teoría general de las relaciones de equivalencia nos asegura que, para cada  $m$ , el conjunto  $\mathbf{Z}$  queda dividido en clases de equivalencia disjuntas por la relación de congruencia módulo  $m$ . Si  $m = 3$  tenemos

$$\mathbf{Z} = X_0 \cup X_1 \cup X_2,$$

donde

$$\begin{aligned} X_0 &= [0]_3 = \{\dots, -3, 0, 3, 6, \dots\}, \\ X_1 &= [1]_3 = \{\dots, -2, 1, 4, 7, \dots\}, \\ X_2 &= [2]_3 = \{\dots, -1, 2, 5, 8, \dots\}. \end{aligned}$$

En este ejemplo, y también para un  $m$  cualquiera, hay  $m$  clases de equivalencia distintas  $[0]_m, [1]_m, \dots, [m-1]_m$ . Esto se debe a que cualquier  $x$  de  $\mathbb{Z}$  puede expresarse de forma única como  $qm + r$  con  $0 \leq r \leq m-1$  (teorema 1.5), de forma que  $x$  está en  $[r]_m$  para un  $r$  exactamente.

**Definición.** El conjunto de enteros módulo  $m$ , que escribiremos  $\mathbb{Z}_m$ , es el conjunto de las clases de equivalencia distintas de la relación de congruencia módulo  $m$  en  $\mathbb{Z}$ .

De modo que  $\mathbb{Z}_m$  es el conjunto  $\{[0]_m, [1]_m, \dots, [m-1]_m\}$ . Insistimos en que los elementos de  $\mathbb{Z}_m$  se definen como *subconjuntos* de  $\mathbb{Z}$ ; sin embargo, suele ser conveniente pensar en ellos como los enteros  $0, 1, 2, \dots, m-1$  con una estructura aritmética modificada, y la manera de concretar esta idea es la siguiente.

Definimos nuevas operaciones de “suma” y “multiplicación” entre los elementos de  $\mathbb{Z}_m$ , que escribiremos  $\oplus$  y  $\otimes$ , mediante las reglas

$$[x]_m \oplus [y]_m = [x+y]_m, \quad [x]_m \otimes [y]_m = [xy]_m.$$

Como  $x$  e  $y$  son enteros, las expresiones  $x+y$  y  $xy$  de los términos derechos están definidas y tienen las propiedades enunciadas en el primer apartado de este libro. Las nuevas operaciones heredan sus propiedades de las mismas propiedades de las operaciones familiares. Pero antes de estudiarlas, hemos de resolver una dificultad relativa a las definiciones.

La dificultad proviene de que cada clase de equivalencia tiene varios nombres. Supongamos, por ejemplo, que  $[x]_m$  y  $[x']_m$  denotan la misma clase, y lo mismo para  $[y]_m$  e  $[y']_m$ . Entonces, para que la definición de  $\oplus$  sea razonable, hemos de asegurarnos de que  $[x]_m \oplus [y]_m$  y  $[x']_m \oplus [y']_m$  denotan la misma clase. El que esto sea así es una consecuencia sencilla del teorema 6.1. En efecto, tenemos que  $x \equiv x' \pmod{m}$  e  $y \equiv y' \pmod{m}$ , de donde  $x+x' \equiv y+y' \pmod{m}$  y  $[x+x']_m = [y+y']_m$  como queríamos demostrar. Una demostración análoga es válida para la multiplicación.

Podemos ahora dar una lista con las propiedades aritméticas de  $\mathbb{Z}_m$ . Las numeramos **M1-M6**, en correspondencia con la lista de axiomas de  $\mathbb{Z}$  del apartado 1.1.

**Teorema 6.2.** Las operaciones  $\oplus$  y  $\otimes$  cumplen las propiedades siguientes, donde  $a, b$  y  $c$  denotan elementos cualesquiera de  $\mathbb{Z}_m$  y  $0 = [0]_m, 1 = [1]_m$ .

**M1.**  $a \oplus b$  y  $a \otimes b$  son de  $\mathbb{Z}_m$ .

**M2.**  $a \oplus b = b \oplus a$ ,  $a \otimes b = b \otimes a$ .

**M3.**  $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ ,  $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ .

**M4.**  $a \oplus 0 = a$ ,  $a \otimes 1 = a$ .

**M5.**  $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ .

**M6.** Para cada  $a$  de  $\mathbb{Z}_m$  existe un único  $-a$  de  $\mathbb{Z}_m$  tal que  $a \oplus (-a) = 0$ .

**DEMOSTRACIÓN:** M1 es una consecuencia directa de las definiciones de  $\oplus$  y  $\otimes$ . En cuanto a la primera parte de M2, supongamos que  $a = [x]_m$  y  $b = [y]_m$ ; entonces

$$\begin{aligned} a \oplus b &= [x]_m \oplus [y]_m = [x+y]_m && \text{(definición de } \oplus\text{)} \\ &= [y+x]_m && \text{(axioma I2 de } \mathbb{Z}\text{)} \\ &= [y]_m \oplus [x]_m && \text{(definición de } \oplus\text{)} \\ &= b \oplus a. \end{aligned}$$

Demostraciones análogas prueban la segunda parte de M2 y M3, M4 y M5. Para M6, si  $a = [x]_m$ , pongamos  $-a = [-x]_m$  y comprobemos:

$$\begin{aligned} a \oplus (-a) &= [x]_m \oplus [-x]_m \\ &= [x + (-x)]_m \\ &= [0]_m \\ &= 0, \end{aligned}$$

como queríamos demostrar.  $\square$

En la práctica evitaremos la pesada notación  $[x]_m$  para los elementos de  $\mathbb{Z}_m$  y utilizaremos los enteros  $0, 1, \dots, m-1$  para referirnos a las clases  $[0]_m, [1]_m, \dots, [m-1]_m$ . El valor específico de  $m$  en cuestión deberá ser claro a partir del contexto o será enunciado explícitamente. También usaremos las notaciones habituales para la suma y el producto en lugar de  $\oplus$  y  $\otimes$ . Así pues, escribiremos

$$7 + 5 = 3 \text{ (en } \mathbb{Z}_9\text{)} \quad \text{en lugar de } [7]_9 \oplus [5]_9 = [3]_9,$$

y tendrá el mismo sentido que  $7 + 5 \equiv 3 \pmod{9}$ . Las propiedades establecidas en el teorema 6.2 justifican la mayoría de las manipulaciones aritméticas en  $\mathbb{Z}_m$ , tal como ocurría en  $\mathbb{Z}$ .

Sin embargo, hay algunas diferencias importantes entre  $\mathbf{Z}_m$  y  $\mathbf{Z}$ . Recordemos el axioma I7; según el cual  $ab = ac$  y  $a \neq 0$  implicaba que  $b = c$ . Esto no se cumple en  $\mathbf{Z}$ : por ejemplo, en  $\mathbf{Z}_6$  tenemos que

$$3 \times 1 = 3 \times 5 \quad y \quad 3 \neq 0, \quad \text{pero } 1 \neq 5.$$

Hay que tener cuidado con la "simplificación" en  $\mathbf{Z}_m$ , un tema que discutiremos con más detalle en el siguiente apartado.

Finalmente, nótese que no hay ninguna relación en  $\mathbf{Z}_m$  que se parezca la relación  $\leq$  en  $\mathbf{Z}$ . La imagen intuitiva de  $\mathbf{Z}$  como un conjunto de puntos en una recta igualmente espaciados que se extienden indefinidamente en ambas direcciones representa las propiedades de esta relación. En su lugar, en  $\mathbf{Z}_m$  tenemos una especie de orden *cíclico*, representado por un conjunto de puntos regularmente espaciados en un círculo (figura 6.1). Por este motivo, la aritmética en  $\mathbf{Z}_m$ , o la *aritmética modular*, se enseña a veces en la escuela como la "aritmética del reloj".

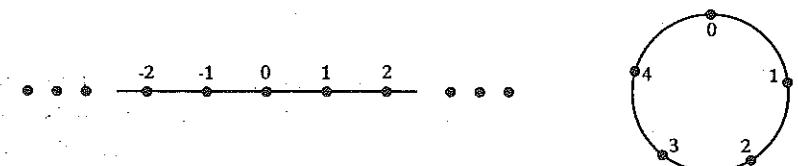


Fig. 6.1 Dibujos de  $\mathbf{Z}$  y  $\mathbf{Z}_m$ .

### Ejercicios 6.2

1 Completar las tablas 6.2.1 de suma y multiplicación en  $\mathbf{Z}_6$ .

Tabla 6.2.1

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2						
3						
4						
5						

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2						
3						
4						
5						



2 Deducir del axioma I7 de  $\mathbf{Z}$  que si  $x$  e  $y$  son enteros tales que  $xy = 0$  con  $x \neq 0$ , entonces  $y = 0$ . Demostrar mediante un contraejemplo que este axioma no se cumple en  $\mathbf{Z}_6$ ,  $\mathbf{Z}_8$  y  $\mathbf{Z}_{15}$ . ¿Existe algún contraejemplo en  $\mathbf{Z}_7$ ?

3 Resolver el sistema de ecuaciones

$$x + 2y = 4$$

$$4x + 3y = 4$$

en  $\mathbf{Z}_7$ . ¿Existe alguna solución en  $\mathbf{Z}_5$ ?

4 Resolver la ecuación cuadrática

$$x^2 + 3x + 4 = 0$$

en  $\mathbf{Z}_{11}$ .

### 6.3 Elementos inversibles de $\mathbf{Z}_m$

En el capítulo 1 insistíamos en el hecho de que el símbolo  $r/s$  no tiene por qué representar un entero aunque  $r$  y  $s$  sean enteros. En otras palabras, dados enteros  $r$  y  $s$ , la ecuación  $rx = s$  con  $x$  de  $\mathbf{Z}$  puede no tener solución. En este apartado investigamos el mismo problema en  $\mathbf{Z}_m$ .

**Definición.** Se dice que un elemento  $r$  de  $\mathbf{Z}_m$  es inversible si existe algún  $x$  de  $\mathbf{Z}_m$  tal que  $rx = 1$  en  $\mathbf{Z}_m$ . En tal caso, se dice que  $x$  es el inverso de  $r$  y escribimos  $x = r^{-1}$ .

Puesto que  $rx = xr$  en  $\mathbf{Z}_m$ , tenemos que  $xr = 1$  y, por lo tanto,  $r = x^{-1}$ .

### Ejercicios 6.3

1 Hallar los elementos inversibles de  $\mathbf{Z}_6$ ,  $\mathbf{Z}_7$  y  $\mathbf{Z}_8$ .

2 Demostrar que 0 no es inversible en ningún  $\mathbf{Z}_m$  y que 1 lo es siempre.

3 Demostrar que si  $x$  e  $y$  son inversibles en  $\mathbf{Z}_m$ , entonces  $xy$  y  $x^{-1}$  también lo son.

**Teorema 6.3.1.** El elemento  $r$  de  $\mathbf{Z}_m$  es inversible si, y sólo si,  $r$  y  $m$  son primos entre sí en  $\mathbf{Z}$ . En particular, si  $p$  es primo, todo elemento de  $\mathbf{Z}_p$  distinto de 0 es inversible.

**DEMOSTRACIÓN:** Supongamos que  $r$  es inversible, de forma que  $rx = 1$  en  $\mathbf{Z}_m$ . Resulta que en  $\mathbf{Z}$  tenemos  $rx - 1 = km$  para algún entero  $k$ , o bien

$$rx - km = 1.$$

Ahora bien, cualquier divisor común de  $r$  y  $m$  ha de dividir a  $rx - km$ , que es 1, de donde  $\text{mcd}(r, m) = 1$ .

Recíprocamente, supongamos que  $\text{mcd}(r, m) = 1$ . Por el teorema 1.7, existen enteros  $x$  e  $y$  tales que  $rx + my = 1$ , de donde  $rx \equiv 1 \pmod{m}$ ; es decir,  $rx = 1$  (en  $\mathbf{Z}_m$ ) como queríamos demostrar.  $\square$

Recuérdese que la función  $\phi(m)$  de Euler (apartado 3.3) es el número de enteros  $1 \leq r \leq m$  que son primos con  $m$ . Del teorema 6.3.1 se desprende que el número de elementos inversibles en  $\mathbf{Z}_m$  es igual a  $\phi(m)$ .

El siguiente teorema es un resultado clásico de la teoría elemental de números y tiene varias aplicaciones útiles. A modo de preparación, haremos una sencilla observación sobre el conjunto  $U_m$  de los elementos inversibles de  $\mathbf{Z}_m$ . Si  $y$  es de  $U_m$ , definimos  $yU_m$  como el conjunto obtenido al multiplicar cada elemento de  $U_m$  por  $y$ ; es decir,

$$yU_m = \{z \in \mathbf{Z}_m \mid z = yx \text{ para algún } x \text{ de } U_m\}.$$

Demostraremos que  $yU_m = U_m$ . Por ejemplo, tomando  $m = 9$  e  $y = 5$ , se tiene

$$U_9 = \{1, 2, 4, 5, 7, 8\}, \quad 5U_9 = \{5, 1, 2, 7, 8, 4\}.$$

En primer lugar, tenemos que  $yU_m \subseteq U_m$ , ya que si  $z = yx$  y tanto  $y$  como  $x$  son de  $U_m$ , también lo es  $z$  (ejercicio 6.3.3). Por otra parte,  $U_m \subseteq yU_m$ , ya que dado un  $x$  de  $U_m$  podemos escribir

$$x = y(y^{-1}x),$$

que claramente es un elemento de  $yU_m$  (nuevamente por el ejercicio 6.3.3). Así pues,  $yU_m = U_m$ , como afirmábamos.  $\square$

**Teorema 6.3.2.** Si  $y$  es inversible en  $\mathbf{Z}_m$ , entonces

$$y^{\phi(m)} = 1 \text{ en } \mathbf{Z}_m.$$

**DEMOSTRACIÓN:** Sea  $u$  el producto de todos los elementos de  $U_m$ , pongamos  $u = x_1 x_2 \cdots x_k$ , donde (de acuerdo con lo anterior)  $k = \phi(m)$ . Dado que  $yU_m = U_m$ , los elementos  $yx_1, yx_2, \dots, yx_k$  no son más que una reordenación de  $x_1, x_2, \dots, x_k$ . Resulta que

$$\begin{aligned} u &= x_1 x_2 \cdots x_k = (yx_1)(yx_2) \cdots (yx_k) \\ &= y^k u. \end{aligned}$$

Pero el propio  $u$  es inversible (su inverso es  $x_k^{-1} \cdots x_2^{-1} x_1^{-1}$ ), con lo que  $y^k = 1$ .  $\square$

El teorema 6.3.2 puede enunciarse también como un teorema sobre números enteros, de la siguiente forma:

$$\text{si } \text{mcd}(y, m) = 1, \text{ entonces } y^{\phi(m)} \equiv 1 \pmod{m}.$$

Se conoce como el **teorema de Euler**. El caso particular en que  $m$  es un primo  $p$  es el **teorema de Fermat**:

$$\text{si } p \nmid y, \text{ entonces } y^{p-1} \equiv 1 \pmod{p}.$$

**Ejempló.** Demostrar que para cada entero positivo  $m$  y cada primo  $p$ ,

$$n^p \equiv n \pmod{p}.$$

Deducir de ello que las últimas cifras de  $n$  y  $n^5$  en base 10 son iguales.

**SOLUCIÓN:** Supongamos que  $p \nmid n$ ; entonces, por el teorema de Fermat,  $n^{p-1} \equiv 1 \pmod{p}$ , y por lo tanto  $n^p \equiv n \pmod{p}$ . Por otra parte, si  $p \mid n$  tanto  $n$  como  $n^p$  son congruentes con 0 módulo  $p$ .

Si utilizamos este resultado para  $p = 5$ , tenemos que  $n^5 - n \equiv 0 \pmod{5}$ . Pero  $n^5 - n = n(n-1)(n^3 + n^2 + n + 1)$  y, como uno de los dos primeros factores es par,  $n^5 - n \equiv 0 \pmod{2}$ . Así pues,  $n^5 - n$  es divisible por 10, lo cual equivale al resultado enunciado.  $\square$

**Ejercicios 6.3 (continuación)**

4 Hallar los inversos de

- (i) 2 en  $\mathbf{Z}_{11}$ ,
- (ii) 7 en  $\mathbf{Z}_{15}$ ,
- (iii) 7 en  $\mathbf{Z}_{16}$ ,
- (iv) 5 en  $\mathbf{Z}_{13}$ .

5 Usar el teorema de Fermat para calcular el resto de dividir  $3^{47}$  entre 23.

6 Sean  $a$  y  $b$  enteros y  $p$  primo. Usar el teorema de Fermat para demostrar que

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

7 Demostrar que la ecuación  $x = x^{-1}$  en  $\mathbf{Z}_p$  implica que  $x^2 - 1 = 0$  en  $\mathbf{Z}_p$ , y deducir que 1 y  $-1$  son los únicos elementos de  $\mathbf{Z}_p$  que son iguales a su propio inverso.

8 Demostrar que

$$(p-1)! \equiv -1 \pmod{p}$$

considerando el producto de todos los elementos no nulos de  $\mathbf{Z}_p$ .

## 6.4 Construcciones cíclicas de diseños

En este apartado y en el siguiente estudiaremos algunas construcciones basadas en las propiedades cíclicas de la aritmética modular.

Si  $S$  es un subconjunto de  $\mathbf{Z}_m$  e  $i$  es un elemento de  $\mathbf{Z}_m$ , representaremos por  $S+i$  el subconjunto obtenido al añadir  $i$  a cada elemento de  $S$ . Por ejemplo, si  $m = 12$  y  $S = \{0, 1, 3, 11\}$ , entonces

$$S+1 = \{1, 2, 4, 0\}, \quad S+2 = \{2, 3, 5, 1\},$$

y así sucesivamente. Investigaremos la posibilidad de utilizar subconjuntos de la forma  $S+i$  ( $i \in \mathbf{Z}_m$ ) como bloques de un diseño.

La primera cuestión a tener en cuenta es que, a pesar de que hay  $m$  posibles valores de  $i$ , los subconjuntos  $S+i$  ( $i \in \mathbf{Z}_m$ ) no son necesariamente todos distintos. Para el subconjunto  $T = \{0, 3, 6, 9\}$  de  $\mathbf{Z}_{12}$  tenemos que

$$T+0 = T+3 = T+6 = T+9 = \{0, 3, 6, 9\},$$

$$T+1 = T+4 = T+7 = T+10 = \{1, 4, 7, 10\},$$

$$T+2 = T+5 = T+8 = T+11 = \{2, 5, 8, 11\},$$

y sólo se obtienen tres subconjuntos distintos. Sin embargo, el subconjunto  $S = \{0, 1, 3, 11\}$  de  $\mathbf{Z}_{12}$  da lugar a doce subconjuntos distintos:

0	1	3	11	6	7	9	5
1	2	4	0	7	8	10	6
2	3	5	1	8	9	11	7
3	4	6	2	9	10	0	8
4	5	7	3	10	11	1	9
5	6	8	4	11	0	2	10

En general, si  $K$  es un subconjunto de  $\mathbf{Z}_m$  tal que los subconjuntos  $K+i$  ( $i \in \mathbf{Z}_m$ ) son todos distintos, entonces estos subconjuntos son los bloques de un 1-diseño con parámetros

$$v = m, \quad k = |K|, \quad r = k.$$

Para demostrarlo, hacemos notar simplemente que el elemento  $\alpha$  de  $\mathbf{Z}_m$  pertenece a  $K+i$  si, y sólo si,

$$\alpha = x + i \quad \text{para algún } x \in K.$$

Esto es equivalente a

$$0 = x + (i - \alpha),$$

lo que significa que 0 está en el bloque  $K+(i-\alpha)$ . Así pues,  $\alpha$  está en los bloques

$$K+i_1, K+i_2, \dots, K+i_r$$

si, y sólo si, 0 está en los bloques

$$K+(i_1-\alpha), K+(i_2-\alpha), \dots, K+(i_r-\alpha).$$

Resulta que 0 y  $\alpha$  pertenecen al mismo número ( $r$ ) de bloques. Como esto se cumple para cualquier  $\alpha$  de  $\mathbf{Z}_m$ , tenemos un 1-diseño. Ahora bien, el número de objetos ( $v$ ) es igual a  $m$  y el número de bloques ( $b$ ) es también igual a  $m$ ; la ecuación  $bk = vr$  demuestra que el número de replicaciones  $r$  y el tamaño de los bloques  $k$  coinciden y que  $r = k = |K|$  como se afirmaba.

Si tomamos  $K = \{0, 1, 3, 11\}$  en  $\mathbf{Z}_{12}$  como antes, obtenemos un 1-diseño con parámetros  $(12, 4, 4)$ . En este caso no obtenemos un 2-diseño

ya que, por ejemplo, el par  $\{0, 1\}$  ocurre dos veces mientras que  $\{0, 6\}$  no ocurre ninguna. Sin embargo, con este método podemos obtener 2-diseños si insistimos en una propiedad adecuada de las *diferencias* en el conjunto básico  $K$ .

**Definición.** El subconjunto  $K$  de  $\mathbf{Z}_m$  es un **conjunto diferencia** si las diferencias  $x - y$  con  $x, y \in K$ ,  $x \neq y$ , toman cada valor no nulo de  $\mathbf{Z}_m$  el mismo número de veces.

El subconjunto  $\{0, 2, 3, 4, 8\}$  de  $\mathbf{Z}_{11}$  es un conjunto diferencia, como puede comprobarse construyendo la tabla de diferencias (tabla 6.4.1). En este ejemplo, cada valor no nulo ocurre dos veces como una diferencia. En general, si  $K$  es un  $k$ -subconjunto de  $\mathbf{Z}_m$ , hay  $k(k-1)$  diferencias y  $m-1$  valores no nulos, de forma que cada diferencia aparece  $k(k-1)/(m-1)$  veces. Resulta que este número es también el parámetro  $r_2$  del correspondiente 2-diseño.

Tabla 6.4.1

	0	2	3	4	8
0	—	9	8	7	3
2	2	—	10	9	5
3	3	1	—	10	6
4	4	2	1	—	7
8	8	6	5	4	—

**Teorema 6.4.** Si  $K$  es un conjunto diferencia en  $\mathbf{Z}_m$ , entonces los conjuntos  $K + i$  ( $i \in \mathbf{Z}_m$ ) son los bloques de un 2-diseño con parámetros

$$v = m, \quad k = |K|, \quad r_2 = k(k-1)/(m-1).$$

**DEMOSTRACIÓN:** Sean  $\alpha$  y  $\beta$  de  $\mathbf{Z}_m$ . Como  $K$  es un conjunto diferencia, la ecuación

$$x - y = \alpha - \beta$$

tiene  $k(k-1)/(m-1)$  soluciones con  $x$  e  $y$  de  $K$ . Para cada solución  $(x, y)$ , sea  $i = \alpha - x$ . Entonces

$$\alpha = x + i, \quad \beta = \alpha - (x - y) = y + i,$$

con lo que tanto  $\alpha$  como  $\beta$  pertenecen a  $K + i$ . Así pues, cada 2-subconjunto  $\{\alpha, \beta\}$  de  $\mathbf{Z}_m$  está contenido en  $r_2 = k(k-1)/(m-1)$  bloques  $K + i$ , y tenemos un 2-diseño con los parámetros enunciados.  $\square$

Dé acuerdo con el teorema 4.7.1, este diseño es también un 1-diseño, y los parámetros  $r_1$  y  $r_0 = b$  vienen dados por

$$r_1 = \frac{v-1}{k-1} \times r_2 = \frac{m-1}{k-1} \times \frac{k(k-1)}{m-1} = k, \quad r_0 = \frac{v}{k} \times k_1 = m.$$

En particular, el número de bloques es  $m$ , de forma que la condición de que  $K$  es un conjunto diferencia asegura automáticamente que los bloques  $K + i$  ( $i \in \mathbf{Z}_m$ ) son todos distintos.

A menudo es imposible hallar un conjunto diferencia con valores dados de  $m$  y  $k$ , incluso si se cumple la condición necesaria evidente de que  $m-1$  divide a  $k(k-1)$  para que  $r_2$  sea un entero. Sin embargo, existen métodos especiales para hallar conjuntos diferencia, muy útiles en la práctica para construir diseños.

**Ejemplo.** Sea  $K$  el subconjunto de  $\mathbf{Z}_{23}$  formado por los elementos no nulos que puede escribirse como cuadrados en  $\mathbf{Z}_{23}$ . Demostrar que  $K$  es un conjunto diferencia y hallar los parámetros del 2-diseño asociado.

**SOLUCIÓN:** Podemos calcular los cuadrados de  $\mathbf{Z}_{23}$  como sigue:

$$\begin{aligned} 1^2 &= 1, & 2^2 &= 4, & 3^2 &= 9, & 4^2 &= 16, & 5^2 &= 2, & 6^2 &= 13, \\ 7^2 &= 3, & 8^2 &= 18, & 9^2 &= 12, & 10^2 &= 8, & 11^2 &= 6, & \dots \end{aligned}$$

No es necesario calcular más, ya que  $12^2 = (-11)^2 = 6$ ,  $13^2 = (-10)^2 = 8$ , etc. Así pues, hemos hallado todos los cuadrados y

$$K = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\},$$

con lo que  $k = |K| = 11$ . Si calculamos las diferencias de  $K$ , se obtiene la tabla 6.4.2.

Tabla 6.4.2

	1	2	3	4	6	8	9	12	13	16	18
1	—	22	21	20	18	16	15	12	11	8	6
2	1	—	22	21	19	17	16	13	12	9	7
3	2	1	—	22	20	18	17	14	13	10	8
4	3	2	1	—	21	19	18	15	14	11	9
6	5	4	3	2	—	21	20	17	16	13	11
8	7	6	5	4	2	—	22	19	18	15	13
9	8	7	6	5	3	1	—	20	19	16	14
12	11	10	9	8	6	4	3	—	22	19	17
13	12	11	10	9	7	5	4	1	—	20	18
16	15	14	13	12	10	8	7	4	3	—	21
18	17	16	15	14	12	10	9	6	5	2	—

Después de inspeccionar la tabla, vemos que cada elemento no nulo de  $\mathbf{Z}_{23}$  aparece el mismo número de veces —cinco en concreto, en concordancia con la fórmula

$$\frac{k(k-1)}{m-1} = \frac{11 \times 10}{22} = 5.$$

Por lo tanto, los parámetros del 2-diseño asociado son  $v = 23$ ,  $k = 11$  y  $r_2 = 5$ .

#### Ejercicios 6.4

1. ¿Cuáles de los siguientes son conjuntos diferencia?
  - (i)  $\{2, 3, 5, 11\}$  en  $\mathbf{Z}_{13}$ ,
  - (ii)  $\{0, 1, 3, 5\}$  en  $\mathbf{Z}_{13}$ ,
  - (iii)  $\{3, 6, 7, 12, 14\}$  en  $\mathbf{Z}_{21}$ .
2. Repetir el ejemplo anterior sustituyendo 23 por 11 y después por 31. Formular una conjetura sobre los parámetros del diseño asociado si  $m$  es un primo de la forma  $4n + 3$ .
3. Demostrar que si  $K$  es un conjunto diferencia en  $\mathbf{Z}_m$ , también lo es  $K + i$  para cada  $i$  de  $\mathbf{Z}_m$ . Deducir que siempre se puede suponer, si se desea, que un conjunto diferencia contiene tanto al 0 como al 1.

4. Demostrar que con el método dado en el ejemplo puede construirse un sistema de Steiner triple (ejercicio 4.7.3) con siete objetos. Demostrar que esta es, esencialmente, la única manera de construir un SST con siete objetos. [Indicación: los tres bloques que contienen un objeto dado deben contener los siete objetos entre ellos.]

#### 6.5 Cuadrados latinos

Supongamos que hemos de planificar un experimento agrícola para probar cinco nuevos tipos de fertilizante en un campo de forma cuadrada. Podríamos dividir el campo en 25 cuadrados y aplicar los fertilizantes según el esquema

A	B	C	D	E
B	C	A	E	D
C	D	E	A	B
D	E	B	C	A
E	A	D	B	C

Hemos dispuesto cada fertilizante exactamente una vez en cada fila y cada columna, con la pretensión de que ciertos efectos (como la dirección dominante del viento) resulten minimizadas.

**Definición.** Un **cuadrado latino** de orden  $n$  es una tabla  $n \times n$  en que cada uno de  $n$  símbolos aparece una vez en cada fila y una vez en cada columna.

Si etiquetamos las filas y las columnas del cuadrado  $L$ , el símbolo en la fila  $i$  y columna  $j$  se indicará por  $L(i, j)$ . En la discusión que sigue, las etiquetas de las filas y columnas serán los elementos de  $\mathbf{Z}_m$ , y los símbolos serán también elementos de  $\mathbf{Z}_m$ .

**Teorema 6.5.1.** Para cada  $m \geq 2$ , la tabla  $m \times m$  definida por

$$L(i, j) = i + j \quad (i, j \in \mathbf{Z}_m)$$

es un cuadrado latino.

**DEMOSTRACIÓN:** Supongamos que los símbolos en las posiciones  $(i, j)$  e  $(i, j')$  son el mismo. Entonces

$$i + j = L(i, j) = L(i, j') = i + j'.$$

Ahora bien,  $\mathbf{Z}_m$  contiene el elemento  $-i$ , y al añadirlo a ambos lados de la ecuación se obtiene  $j = j'$ . Por lo tanto, cada símbolo aparece como máximo una vez en la fila  $i$ , y dado que hay  $m$  símbolos y  $m$  posiciones, cada símbolo aparece exactamente una vez. Un argumento análogo funciona para las columnas. En consecuencia,  $L$  es un cuadrado latino.  $\square$

El teorema demuestra que al menos existe un cuadrado latino de un orden dado. Por supuesto, el cuadrado latino que hemos construido en el teorema no es más que la “tabla de sumar” de  $\mathbf{Z}_m$  (véase ejercicio 6.2.1), y el hecho de que podamos hallar un cuadrado latino de esta manera no es especialmente excitante. De hecho, es fácil construir cuadrados latinos por tanteo.

Un problema algo más difícil es hallar pares de cuadrados latinos del mismo orden que sean, en un cierto sentido, tan diferentes como sea posible. Decimos que dos cuadrados latinos  $L_1$  y  $L_2$  del mismo orden son **ortogonales** si, para cada par ordenado de símbolos  $(k, k')$  existe exactamente una posición  $(i, j)$  para la cual

$$L_1(i, j) = k, \quad L_2(i, j) = k'.$$

Por ejemplo, en los cuadrados latinos

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
<i>B</i>	<i>A</i>	<i>D</i>	<i>C</i>
<i>C</i>	<i>D</i>	<i>A</i>	<i>B</i>
<i>D</i>	<i>C</i>	<i>B</i>	<i>A</i>

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
<i>C</i>	<i>D</i>	<i>A</i>	<i>B</i>
<i>D</i>	<i>C</i>	<i>B</i>	<i>A</i>
<i>B</i>	<i>A</i>	<i>D</i>	<i>C</i>

cada uno de los 16 pares  $(A, A), (A, B), \dots, (D, D)$  aparece en una de las 16 posiciones.

En 1871 Euler propuso el siguiente problema. Se tienen 36 oficiales de seis rangos diferentes en seis regimientos distintos: ¿pueden disponerse en

un cuadrado de forma que en cada fila y cada columna haya un oficial de cada rango y un oficial de cada regimiento? En lenguaje moderno, Euler buscaba un par de cuadrados latinos ortogonales de orden seis. No fue capaz de resolver el problema y ahora sabemos que no existe ningún par de este tipo.

Aunque el problema de Euler muestra que no es sencillo encontrar cuadrados latinos ortogonales, existe una construcción muy útil basada en las propiedades aritméticas de  $\mathbf{Z}_p$  si  $p$  es primo.

**Teorema 6.5.2.** Sea  $p$  un número primo y  $t$  un elemento no nulo de  $\mathbf{Z}_p$ . Entonces la regla

$$L_t(i, j) = ti + j \quad (i, j \in \mathbf{Z}_p)$$

define un cuadrado latino. Más aún, si  $t \neq u$ , los cuadrados latinos  $L_t$  y  $L_u$  son ortogonales.

**DEMOSTRACIÓN:** Para demostrar que  $L_t$  es un cuadrado latino podemos utilizar el mismo método que en el teorema anterior. Por ejemplo, si  $L_t(i, j) = L_t(i', j)$ , entonces  $ti + j = ti' + j$ , y al ser  $t$  invisible en  $\mathbf{Z}_p$ , se tiene que  $i = i'$ . Un argumento similar demuestra que  $j = j'$  si  $L_t(i, j) = L_t(i, j')$ .

Para demostrar que los cuadrados  $L_t$  y  $L_u$  son ortogonales si  $t \neq u$ , supongamos que existen dos posiciones distintas  $(i_1, j_1)$  y  $(i_2, j_2)$  tales que  $L_t$  y  $L_u$  tienen los símbolos  $k$  y  $k'$  respectivamente en cada posición. Es decir,

$$\begin{aligned} ti_1 + j_1 &= k, & ui_1 + j_1 &= k', \\ ti_2 + j_2 &= k, & ui_2 + j_2 &= k'. \end{aligned}$$

Resulta que

$$t(i_1 - i_2) = j_2 - j_1, \quad u(i_1 - i_2) = j_2 - j_1.$$

Si  $i_1 - i_2 = 0$  estas ecuaciones implican que  $j_2 - j_1 = 0$ , de forma que las posiciones  $(i_1, j_1)$  e  $(i_2, j_2)$  son la misma, contrariamente a la hipótesis. En consecuencia,  $i_1 - i_2 \neq 0$  e  $i_1 - i_2$  tiene un inverso en  $\mathbf{Z}_p$ . En este caso podemos resolver las ecuaciones en  $t$  y  $u$  y se llega a

$$t = u = (i_1 - i_2)^{-1}(j_2 - j_1).$$

En otras palabras, si insistimos en que  $t \neq u$ , los símbolos  $k$  y  $k'$  sólo pueden aparecer conjuntamente en una única posición y  $L_t$  y  $L_u$  son ortogonales.  $\square$

En general, decimos que el teorema proporciona un conjunto de  $p - 1$  cuadrados latinos de orden  $p$  mutuamente ortogonales para cada primo  $p$ . Por ejemplo, si  $p = 3$  se obtienen los cuadrados

$$L_1 = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}$$

$$L_2 = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

### Ejercicios 6.5

1 Una baraja de cartas (francesas) contiene cuatro jotas, cuatro reinas, cuatro reyes y cuatro ases, uno de cada color —corazones, tréboles, diamantes y picas—. Explíquese cómo disponer estas 16 cartas en un cuadrado  $4 \times 4$  de forma que cada fila contenga una carta de cada color y una carta de cada denominación. Interprétese el resultado en término de cuadrados latinos.

2 Utilizar la construcción del teorema 6.5.2 para obtener cuatro cuadrados latinos de orden 5 mutuamente ortogonales.

3 ¿Por qué no es posible usar el método del teorema 6.5.2 para hallar tres cuadrados latinos de orden 3 mutuamente ortogonales? Hallar tres cuadrados de este tipo por tanteo.

4 Sea

$$x_1 \ x_2 \ x_3 \ \dots \ x_{n-1} \ x_n$$

la primera fila de una tabla  $n \times n$  y supongamos que cada fila se obtiene a partir de la anterior por un desplazamiento cíclico de  $r$  posiciones, de forma que la segunda fila es

$$x_{r+1} \ x_{r+2} \ x_{r+3} \ \dots \ x_{r-1} \ x_r,$$

y así sucesivamente. Dado un  $n$  fijo, ¿para qué valores de  $r$  esta construcción da lugar a un cuadrado latino?

### Ejercicios diversos

1 Determinar todas las soluciones posibles de las congruencias

$$(i) \ 5x \equiv 1 \pmod{11}, \quad (ii) \ 5x \equiv 7 \pmod{15}.$$

2 Demostrar que 192 837 465 564 738 291 es divisible por 11 sin hacer la división.

3 Demostrar que la congruencia  $ax \equiv b \pmod{m}$  tiene solución en  $x$  si, y sólo si,  $b$  es un múltiplo de  $\text{mcd}(a, m)$ .

4 Resolver las ecuaciones

$$(i) \ 5x = 12 \text{ en } \mathbf{Z}_{13}, \quad (ii) \ x^2 - x - 1 = 0 \text{ en } \mathbf{Z}_{11}.$$

5 ¿Cuál es la última cifra de la representación en base 10 de  $7^{93}$ ?

6 Usar el hecho de que  $1001 = 7 \times 11 \times 13$  para construir una prueba de divisibilidad por 7, 11 o 13 parecida a la de “borrar nueves” y a la prueba de divisibilidad por 11 del ejercicio 6.14.

7 Hallar los inversos de

$$(i) \ 6 \text{ en } \mathbf{Z}_{11}, \quad (ii) \ 6 \text{ en } \mathbf{Z}_{17}, \\ (iii) \ 3 \text{ en } \mathbf{Z}_{10}, \quad (iv) \ 5 \text{ en } \mathbf{Z}_{12}.$$

8 Si  $\text{mcd}(r, m) = 1$ , utilizar la demostración del teorema 6.3.1 para formular un método práctico (basado en el algoritmo de Euclides) para hallar el inverso de  $r$  en  $\mathbf{Z}_m$ .

9 Demostrar que si  $\text{mcd}(m_1, m_2) = 1$ , entonces existe una solución en  $x$  de las congruencias

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}.$$

Demostrar que dos soluciones cualesquiera son congruentes módulo  $m_1 m_2$ .

10 Enunciar y demostrar una generalización del ejercicio anterior con  $n$  congruencias simultáneas (se conoce con el nombre del teorema chino del resto).

11 El teorema de Fermat implica que, para cada primo  $p > 2$ , se tiene  $2^{p-1} \equiv 1 \pmod{p}$ : Hallar el mínimo  $p$  para el cual

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

12 Sea  $F = \mathbf{Z}_3 \times \mathbf{Z}_3$ ; en otras palabras,  $F$  es el conjunto de los pares ordenados  $(x, y)$  con  $x$  e  $y$  de  $\mathbf{Z}_3$ . Se define una operación  $\otimes$  en  $F$  mediante la regla

$$(x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1),$$

donde las operaciones de la derecha tienen el significado habitual en  $\mathbf{Z}_3$ . Demostrar que todo elemento de  $F$  salvo el  $(0, 0)$  tiene un inverso respecto de la operación  $\otimes$ .

13 Determinar para qué valores de  $k$  en el intervalo  $2 \leq k \leq 6$  existe un conjunto diferencia de tamaño  $k$  en  $\mathbf{Z}_7$ .

14 Sea  $S$  el conjunto de los cuadrados no nulos de  $\mathbf{Z}_{13}$  y  $T$  el conjunto de los no cuadrados no nulos. Comprobar que el resultado de aplicar la construcción cíclica a  $S$  y al mismo tiempo a  $T$  es un 2-diseño con parámetros  $(13, 6, 5)$ .

15 Demostrar que si  $S$  es un conjunto diferencia en  $\mathbf{Z}_m$ , también lo es  $\mathbf{Z}_m - S$ . Calcular los parámetros del conjunto diferencia complementario en función de los del primero.

16 Determinar el valor de  $x$  para que el conjunto  $\{1, 5, 24, 25, 27, x\}$  sea un conjunto diferencia en  $\mathbf{Z}_{31}$ .

17 Sea  $B$  un 2-diseño con parámetros  $(v, k, r_2)$  que proviene de un conjunto diferencia en  $\mathbf{Z}_v$ . Demostrar que dos bloques cualesquiera de  $B$  tienen en común exactamente  $r_2$  elementos.

18 Construir un par de cuadrados latinos ortogonales de orden 8.

19 Se puede suponer (sin pérdida de generalidad) que la primera fila de un cuadrado latino de orden  $n$  es  $1, 2, 3, \dots, n$ . ¿De cuántas maneras puede llenarse la segunda fila?

20 Sea  $S$  el conjunto de los bloques de un sistema de Steiner triple en el conjunto  $\{1, 2, \dots, n\}$  (ejercicio 4.7.3). Demostrar que la siguiente regla define un cuadrado latino:

$$L(i, j) = \begin{cases} i & \text{si } i = j; \\ k & \text{si } i \neq j, \end{cases}$$

donde  $\{i, j, k\}$  es el único bloque de  $S$  que contiene a  $i$  y  $j$ .

## Parte II Grafos y algoritmos

---

En esta parte del libro discutiremos problemas que pueden resolverse paso a paso. Muchos de estos problemas pueden describirse en términos de un "grafo" o de una "red"; por este motivo, dedicaremos algún tiempo a estudiar propiedades de estas estructuras.

La Parte I cubre, esencialmente, los prerequisitos para leer esta parte. Casi todos los cálculos se hacen únicamente en el conjunto  $\mathbf{Z}$  de los enteros, pero en el capítulo 12 será conveniente conocer las propiedades aritméticas elementales de los conjuntos de los números reales y complejos que se denotan, respectivamente, por  $\mathbf{R}$  y  $\mathbf{C}$ . Aquí y allá se utilizan resultados muy sencillos sobre matrices.

En el apartado 7.2 se describen algunas notaciones del lenguaje de programación Pascal, aunque no se pretende dar los detalles necesarios para la construcción de un programa en Pascal efectivo. Para estas cuestiones, remitimos al lector al libro del autor *Introducción a la computación con Pascal*. El tratamiento que se da aquí es compatible con el de ese libro, pero independiente de él.

## 7 Algoritmos y su eficiencia

---

### 7.1 ¿Qué es un algoritmo?

Para dar una definición totalmente satisfactoria de lo que es un algoritmo, tendríamos que adentrarnos profundamente en el terreno de la lógica matemática. Pero la idea es tan sencilla y tan natural que un enfoque informal es suficiente para nuestros propósitos. En sus orígenes, la palabra “algoritmo” se utilizó para los procedimientos básicos de la aritmética elemental, como la suma y la multiplicación. Un niño que sepa sumar es capaz de calcular la suma de dos enteros positivos en base 10. El niño no tiene por qué entender la base lógica del procedimiento; todo lo que necesita es llevar a cabo los pasos correctos en el orden correcto.

Informalmente, podemos decir que un algoritmo es una sucesión de instrucciones. La persona o la máquina encargada de realizar el algoritmo tiene que efectuar cada una de las instrucciones en el orden exacto. Un algoritmo se basa siempre en ciertas consideraciones. Por ejemplo, los algoritmos básicos de la aritmética (tal como se enseñan a los niños) trabajan con enteros escritos en base 10. Dependen del hecho de que la suma y el producto de dos enteros de una cifra es un entero con dos cifras como máximo, de manera que los niños pueden aprender “de memoria” las tablas para las operaciones de una cifra.

Para estudiar estos algoritmos con más detalle es conveniente dar las siguientes definiciones: para cada entero  $m$  en el intervalo  $0 \leq m \leq 99$ , sea  $t(m)$  la cifra de la decena y  $u(m)$  la cifra de las unidades de  $m$ . Por ejemplo,  $t(73) = 7$  y  $u(73) = 3$ . Formalmente, si

$$m = 10t + u, \quad (0 \leq t \leq 9, 0 \leq u \leq 9),$$

entonces  $t(m) = t$  y  $u(m) = u$ . Utilizando esta notación, es posible dar una descripción precisa de algunos algoritmos elementales.

**Ejemplo.** Sean  $a$  y  $b$  dos enteros de  $n$  cifras en su representación en base 10 y sea  $s = a + b$ . El algoritmo para calcular la representación en base 10 de  $s$  suele llevarse a cabo como en el siguiente ejemplo.

$$\begin{array}{r} 7 \ 8 \ 1 \ 5 \ 3 \quad a \text{ (en base 10)} \\ + \ 3 \ 7 \ 4 \ 2 \ 9 \quad b \text{ (en base 10)} \\ \hline 1 \ 1 \ 0 \ 0 \ 1 \quad (\text{cifras de acarreo}) \\ 1 \ 1 \ 5 \ 5 \ 8 \ 2 \quad s \text{ (en base 10)} \end{array}$$

Obtener las fórmulas para calcular las cifras de  $s$  en el caso general utilizando las notaciones  $t$  y  $u$  introducidas anteriormente.

**SOLUCIÓN:** El método en el caso general es como sigue:

$$\begin{array}{r} a_{n-1} \ a_{n-2} \cdots \ a_2 \ a_1 \ a_0 \quad a \\ + \ b_{n-1} \ b_{n-2} \cdots \ b_2 \ b_1 \ b_0 \quad b \\ \hline c_n \ c_{n-1} \ \cdots \ c_2 \ c_1 \quad (\text{cifras de acarreo}) \\ s_n \ s_{n-1} \ s_{n-2} \cdots \ s_2 \ s_1 \ s_0 \quad s \end{array}$$

( Nótese que  $s_n$  puede ser cero.) En el primer paso sumamos  $a_0$  y  $b_0$ , definimos  $s_0$  como las unidades del resultado y “nos llevamos”  $c_1$ , las decenas de la respuesta. Es decir,

$$s_0 = u(a_0 + b_0), \quad c_1 = t(a_0 + b_0).$$

En el segundo paso calculamos  $a_1 + b_1 + c_1$  y le sumamos  $c_2$ ; las unidades del resultado dan  $s_1$  y las decenas  $c_2$ . Proseguimos de esta forma calculando para cada  $i$  en el intervalo  $1 \leq i \leq n - 1$  las cifras

$$s_i = u(a_i + b_i + c_i), \quad c_{i+1} = t(a_i + b_i + c_i).$$

Finalmente, hacemos  $s_n = c_n$ .  $\square$

El ejemplo ilustra el hecho de que un algoritmo debe considerarse en un contexto específico. En este caso, el contexto es una persona que conoce las tablas para sumar y multiplicar enteros pequeños. Este conocimiento podría residir en su memoria o en un manual de tablas.

### Ejercicios 7.1

1 El siguiente esquema describe el algoritmo habitual para multiplicar un entero  $x$  de  $n$  cifras por un entero de una cifra  $y$  en base 10.

$$\begin{array}{r} x_{n-1} \ x_{n-2} \cdots \ x_2 \ x_1 \ x_0 \quad x \\ \times \quad \quad \quad \quad \quad y \quad y \\ \hline c_n \ c_{n-1} \ \cdots \ c_2 \ c_1 \quad (\text{cifras de acarreo}) \\ p_n \ p_{n-1} \ p_{n-2} \cdots \ p_2 \ p_1 \ p_0 \quad xy \end{array}$$

Obtener las fórmulas que determinan las cifras de  $xy$  y las de acarreo.

2 Explicar con detalle cómo extender el algoritmo descrito en el ejercicio 1 para obtener el algoritmo de multiplicación entre un entero de  $n$  cifras y otro de  $m$  cifras ( $n \geq m \geq 1$ ).

3 Supongamos que una máquina puede realizar las siguientes tareas:

- (i) sumar 1 a un entero;
- (ii) restar 1 de un entero;
- (iii) decidir si un entero es cero.

Sea  $m$  un entero y  $n$  un entero no negativo. Escribir un algoritmo que indique a la máquina cómo calcular  $m + n$ . (Puede suponerse que la máquina es capaz de almacenar los cálculos intermedios y acceder a ellos en cualquier momento.)

### 7.2 El lenguaje de los programas

Con el desarrollo de los ordenadores, muchos de los algoritmos se diseñan para ser utilizados por una máquina y no por seres humanos. Por este motivo solemos describir los algoritmos en una especie de taquigrafía, mezclando lenguajes de programación, el lenguaje común y la notación matemática. El lenguaje de programación que usamos en este libro es Pascal, ya que su uso en la enseñanza está muy extendido y los lectores tendrán probablemente alguna familiaridad con él. De todas maneras, no necesitaremos más que algunas de las construcciones básicas de Pascal y éstas las describimos completamente.

Es útil pensar en un ordenador “modelo” que almacena los datos en una serie de “cajas”. Cada caja tiene el nombre de un identificador y

contiene un **valor**. En un cierto instante, los identificadores y los valores podrían ser los siguientes:

Identificador:	x	y	z	a	b	c
Valor:	17	5	45	67	8	-6

Los identificadores, los valores y las notaciones que sean parte del lenguaje Pascal se distinguirán por el uso de la letra "máquina de escribir" (como en el ejemplo anterior). En este ejemplo, el valor de cada identificador es un número, pero podría ser de otro tipo.

En el contexto de este modelo, las reglas para llevar a cabo cualquier algoritmo pueden expresarse en términos de un número notablemente reducido de instrucciones sencillas. La más importante de todas es la **instrucción de asignación** que, en Pascal, se denota por el símbolo `:=`. Por ejemplo, la instrucción

`x := 52`

asigna el valor 52 al identificador `x`, mientras que el valor previo (17 en el ejemplo anterior) se pierde. El objeto que va a continuación del símbolo `:=` no tiene por qué tener un valor concreto; puede ser cualquier expresión que tenga un valor bien definido en el momento de la asignación. Por ejemplo, las siguientes instrucciones de asignación son válidas:

`x:=y`    `x:=x+1`    `x:=y-z`

En el primer ejemplo se asigna a `x` el valor actual de `y` (mientras que `y` conserva su valor). En el segundo ejemplo, se toma el valor de `x`, se incrementa en 1 y este nuevo valor sustituye al antiguo. En el tercer ejemplo, se evalúa la expresión `y-z` y se asigna su valor a `x`.

Una sucesión de instrucciones puede imitar los pasos a seguir en el desarrollo de una fórmula matemática. Este es, quizás, el tipo de algoritmo más sencillo. Por ejemplo, el siguiente método calcula el número de 2-subconjuntos de un  $n$ -conjunto mediante la fórmula  $n(n - 1)/2$ . Suponemos que el valor de la "entrada" ha sido almacenado en el identificador `n` y que el valor de la "salida" se almacena en el identificador `b`.

`x:=n;`    `y:=x-1;`    `x:=x*y;`    `b:=x div 2`

Los punto y coma que separan las instrucciones de asignación nos dicen que una instrucción se efectúa después de haber completado la anterior. Podríamos pensar en el punto y coma como la instrucción "ir a la siguiente instrucción". El símbolo `*` en Pascal es la multiplicación y `x div 2` es el cociente de la división de `x` entre 2. Si nos fijamos en la secuencia de instrucciones, vemos que a `x` se le asigna el valor dado de `n` y que este valor menos 1 es asignado a `y`; el producto de estos dos valores se asigna a `x`, se divide por 2 y se asigna a `b`.

Para construir programas más interesantes hemos de permitir tipos de valores distintos de los enteros. Nos referimos a los **valores de verdad**, denotados por **cierto** y **falso** y conocidos también como **valores booleanos**. Para nosotros será suficiente suponer que la máquina puede asignar uno de estos valores a expresiones como `y=z` o `x>0`. El valor asignado será **cierto** o **falso** dependiendo de los valores de los identificadores `x`, `y` y `z` en este momento. Si `x` tiene el valor -35 la expresión `x>0` tendrá el valor **falso**, pero si `x` es 23, entonces `x>0` será **cierto**.

Con esta provisión podemos introducir dos tipos de instrucciones muy útiles. La primera es la **instrucción condicional**, que tiene la forma

`si B entonces C1 si no C2,`

donde `B` es una expresión que puede tomar cualquiera de los valores de verdad y `C1` y `C2` son instrucciones. La consecuencia es que si `B` es **cierto** se lleva a cabo `C1`, mientras que si `B` es **falso** se efectúa `C2`. Por ejemplo, otro método (más bien forzado) para calcular los números binomiales es el siguiente: la idea es usar el hecho de que  $n$ , ó bien  $n - 1$  es divisible por 2, de modo que en la fórmula  $n(n - 1)/2$  podemos hacer la división antes que la multiplicación. Utilizamos la notación `s mod m` de Pascal para indicar el resto de dividir `s` entre `m`. Así pues, en la ecuación  $s = qm + r$  ( $0 \leq r < m$ ), `q` corresponde a `s div m` y `r` a `s mod m`.

```

x:=n
si (x mod 2)=1
    entonces inicio y:=(x-1) div 2; z:=x fin
    si no inicio y:=x div 2; z:=x-1 fin;
    b:=y*z
  
```

Las palabras **inicio** y **fin** se utilizan como paréntesis. Significan que hemos de entender la sucesión de instrucciones que encierran como una

sola instrucción. A menudo las instrucciones alternativas  $C_1$  y  $C_2$  de una instrucción condicional son de este tipo. En muchos casos la instrucción  $C_2$  es vacía, es decir, no hay que hacer nada cuando la expresión  $B$  es falsa. En tales casos omitiremos también las palabras *si* y *no*.

El segundo tipo de instrucción que depende de si una expresión  $B$  es cierta o falsa es la **instrucción iterativa**

mientras  $B$  hacer  $C$ ,

que indica al ordenador que efectúe la instrucción  $C$  repetidamente mientras la expresión  $B$  sea cierta. La repetición cesa únicamente cuando  $B$  resulta falsa. Aquí tenemos, por ejemplo, otra manera de calcular el número de 2- subconjuntos de un  $n$ -conjunto utilizando el hecho de que es igual a la suma  $1 + 2 + \dots + (n - 1)$ .

```
x:=n; y:=0; z:=0;
mientras y<x-1 hacer
    inicio y:=y+1; z:=z+y fin;
b:=z
```

Una buena manera de seguir la acción de una instrucción iterativa es construir una tabla de los identificadores después de cada iteración. Supongamos que  $n$  tiene el valor 6; entonces los valores  $x$ ,  $y$  y  $z$  que resultan de las instrucciones anteriores son los siguientes (tabla 7.2.1):

Tabla 7.2.1

$x$	$y$	$z$
6	0	0
6	1	1
6	2	3
6	3	6
6	4	10
6	5	15

Llegados a este punto, el valor de verdad de la expresión  $y < x - 1$  es falso y la iteración acaba.

Hay una última notación de Pascal que usaremos frecuentemente. Es la instrucción

para  $y:=r$  hasta  $s$  hacer  $C$ ,

que tiene como consecuencia la ejecución de la instrucción  $C$  para cada valor de  $y$  entre  $r$  y  $s$ . Es más una abreviatura que una nueva instrucción, ya que podríamos conseguir el mismo efecto con la construcción iterativa *mientras-hacer*, tal como se muestra a continuación:

```
y:=r;
mientras y<s+1 hacer
    inicio C; y:=y+1 fin
```

### Ejercicios 7.2

1 Los valores de los identificadores  $x$ ,  $y$  y  $z$  son inicialmente 46, 23 y 78, respectivamente. Calcular los valores de los identificadores después de la ejecución de las instrucciones siguientes.

- (a)  $x:=y+z$     (b)  $x:=x+12$     (c)  $z:=z-17$

2 Si los valores iniciales son como en el ejercicio 1, usar una tabla como la 7.2.1 para obtener los valores de  $x$ ,  $y$  y  $z$  después de la ejecución de las siguientes instrucciones.

- (a) inicio  $x:=27$ ;  $y:=13$  fin  
 (b) inicio  $z:=25$ ;  $x:=y-12$ ;  $y:=z+6$  fin  
 (c) inicio  $x:=x+28$ ;  $y:=x$ ;  $x:=y-14$ ;  $y:=x+z$  fin

3 Los valores iniciales de  $x$ ,  $y$  y  $z$  son 3, 7 y 11, respectivamente. Hallar los valores de los identificadores después de efectuar las siguientes instrucciones.

- (a) si  $x>6$  entonces  $y:=z$  si no  $y:=x$   
 (b) si  $y=8$  entonces  $x:=9$   
 (c) mientras  $x<10$  hacer  $x:=x+3$   
 (d) mientras  $y<z$  hacer inicio  $y:=y+x$ ;  $x:=x+1$  fin  
 (e) mientras  $y>z$  hacer inicio  $y:=y+x$ ;  $x:=x+1$  fin

### 7.3 Algoritmos y programas

A partir de ahora, al formular un algoritmo emplearemos a menudo la notación de Pascal para las instrucciones de asignación, condicionales e iterativas. También será conveniente usar palabras comunes del español y notaciones matemáticas; ambas se escribirán en cursiva para indicar que no forman parte de Pascal. El lector que haya estudiado Pascal no tendrá ninguna dificultad en traducir estos "programas" en versiones que funcionen correctamente en un ordenador.

Como ejemplo, recordemos el algoritmo del apartado 1.5 para calcular la representación binaria  $r_k r_{k-1} \dots r_0$  de un entero positivo  $m$ . El procedimiento para obtener las sucesivas cifras binarias y el valor de  $k$  puede describirse de la siguiente forma.

```
i:=0; q:=m;
mientras q>0 hacer
    inicio
        ri es el resto de dividir q entre 2;
        el nuevo q es el cociente de dividir el antiguo q entre 2;
        i:=i+1
    fin;
    k:=i-1
```

Las líneas en cursiva pueden traducirse en Pascal efectivo utilizando los operadores mod y div descritos anteriormente y un método apropiado para representar la sucesión de restos. Los detalles de la codificación en Pascal (lo que habitualmente se conoce como una *realización* del algoritmo) no son relevantes en este caso, aunque naturalmente es bueno saber que existe una realización efectiva.

Es un hecho notable que cualquier algoritmo que pueda reducirse a una sucesión definida de operaciones lógicas y aritméticas es expresable en términos de instrucciones de asignación, condicionales e iterativas. La *programación estructurada* se basa en este hecho. Un algoritmo muy importante que ilustra la elegancia de la notación estructurada es el algoritmo de Euclides descrito en el apartado 1.7 para hallar el mcd de dos enteros positivos. Si almacenamos los dos enteros en los identificadores s y t, el algoritmo puede describirse así:

```
x:=s; y:=t;
mientras y>0 hacer
    sustituir (x, y) por (y, r) siendo r el resto
    de dividir x entre y;
    el mcd es el valor final de x
```

Esto podría realizarse en Pascal del siguiente modo:

```
x:=s; y:=t;
mientras y>0 hacer
    inicio z:=y; y:=x mod y; x:=z fin;
    d:=x
```

El identificador z se introduce para guardar temporalmente el valor antiguo de y mientras se calcula el nuevo. El método tabular introducido en el apartado anterior es una buena ilustración de cómo funciona. Supongamos, por ejemplo, que los valores de s y t son 2406 y 654; entonces los valores de x, y y z después de cada iteración son los que se muestran en la tabla 7.3.1.

Tabla 7.3.1

x	y	z
654	444	654
444	210	444
210	24	210
24	18	24
18	6	18
6	0	6

Llegados a este punto, y vale 0, la expresión y>0 resulta ser falsa y la iteración acaba. El valor final de x se asigna al identificador d, es decir 6, y este es el mcd de los valores iniciales.

#### Ejercicios 7.3

- 1 Tabular los valores de x, y y z en la realización del algoritmo de Euclides si los valores iniciales de s y t son 725 y 441.
- 2 ¿Cuál es el valor de resp calculado por el siguiente algoritmo?

```

suma:=0;
para i:=1 hasta 17 hacer
  sum:=sum+i;
resp:=suma

```

- 3 Sea  $S = \{x_1, x_2, \dots, x_n\}$  un conjunto de enteros. Explicar en lenguaje común cómo calcula el mínimo de  $S$  el siguiente algoritmo:

```

y:=x1
para j:=2 hasta n hacer
  si y es mayor que xj entonces y:=xj;
m:=y

```

- 4 Construir un algoritmo que, dado un conjunto  $S$  como en el ejercicio 3, asigne el valor 1 al identificador z si  $S$  posee dos elementos iguales y 0 en otro caso.

#### 7.4 Demostración de que un algoritmo es correcto

Los algoritmos son parte de las matemáticas y sería deseable poder dar demostraciones convincentes de su corrección, tal como hacemos con los teoremas. En este apartado discutimos algunos de los problemas que surgen y algunos de los argumentos que pueden utilizarse en casos muy sencillos.

El primer problema es que puede ser difícil decidir si un algoritmo produce un resultado razonable. Consideremos por ejemplo el siguiente algoritmo, que pretende asignar un valor a b si n tiene un valor positivo entero dado.

```

x:=n;
mientras x>1 hacer
  si x mod 2=0 entonces x:=x div 2
    si no x:=5*x+1;
b:=x

```

Si n es 3, los valores sucesivos de x calculados por el algoritmo son

3 16 8 4 2 1

Llegados a este punto la iteración acaba, ya que la expresión  $x>1$  es falsa, y se asigna el valor 1 a b. Pero si n es 5, la sucesión de valores empieza por

5 26 13 66 33 166 83 416 208 104 52

y el siguiente valor es 26 que ya ha aparecido antes. Así pues, la sucesión

26 13 66 33 166 83 416 208 104 52

se repite indefinidamente y b no recibirá nunca un valor. Tenemos un ejemplo de un procedimiento que no debiéramos considerar como un algoritmo, ya que es posible que nunca produzca un resultado.

El problema de demostrar que un algoritmo siempre acaba se conoce normalmente como el problema de la *terminación*. Si tratamos con números enteros, hay una propiedad fundamental que puede ayudarnos en este problema: el axioma de la buena ordenación, que puede formularse (apartado 1.2) como sigue.

*Todo subconjunto no vacío S de N posee un mínimo.*

Para ver cómo aplicar este resultado para demostrar que un algoritmo acaba, supongamos que tenemos un identificador y que toma valores enteros  $y_0, y_1, \dots$ , y tal que cada valor es estrictamente menor que el precedente. El axioma de la buena ordenación nos garantiza que existe un valor  $y_k$  que no es de N. En efecto, o bien  $y_0$  ya no es de N, o bien el conjunto  $S$  de valores que son positivos no es vacío. En este último caso,  $S$  tiene un mínimo  $y_t$ ; entonces  $y_{t+1}$  no es de  $S$ , ya que es estrictamente menor que  $y_t$ , y concluimos que  $y_{t+1}$  no es de N.

Este argumento prueba el hecho (intuitivamente evidente) de que si los valores de un identificador y forman una sucesión de enteros estrictamente decreciente, podemos estar seguros de que alguno de los valores será cero (o negativo) después de un número finito de pasos. Equivalentemente, la expresión  $y>0$  será eventualmente falso. Por ejemplo, en la versión que dimos del algoritmo de Euclides en el apartado anterior, cada nuevo valor de y es estrictamente menor que el valor anterior, ya que es el resto de dividir este último entre x. Por lo tanto, podemos estar seguros de que y será cero eventualmente y de que el algoritmo acaba necesariamente. Incluso si el algoritmo acaba, debemos aún demostrar que es "correcto", es decir, que produce la respuesta deseada. En el siguiente ejemplo se explica una técnica que funciona a menudo.

Al hablar de algoritmos es habitual utilizar el término **caso** para referirse a un ejemplo específico del problema. Si el problema es la multiplicación de dos enteros positivos, un caso típico es el par (7631, 205). Sería razonable utilizar el número de cifras del mayor de los números como una medida del tamaño de un caso, de forma que el tamaño del caso (7631, 205) sería 4.

Para medir el esfuerzo acostumbramos a contar el número de operaciones significativas que efectúa el algoritmo. Por ejemplo, si utilizamos el algoritmo de multiplicación ordinario, para un caso de tamaño  $n$  necesitamos como mucho  $n^2$  multiplicaciones de una sola cifra (y algunas sumas y acarreos), de modo que podemos decir que la eficiencia del algoritmo es  $n^2$ . Por otra parte, el algoritmo habitual para calcular la *suma* de dos enteros positivos necesita como mucho  $n$  operaciones de una sola cifra (y algún acarreo), así que podemos decir que su eficiencia es  $n$ .

En general, el análisis de un algoritmo comporta tres etapas:

- (A) describir el algoritmo con exactitud;
- (B) definir el tamaño de un caso, digamos  $n$ ;
- (C) calcular  $f(n)$ , el número de operaciones necesarias.

Este tipo de análisis lleva consigo una cierta subjetividad en varios puntos. ¿Cuál es la "mejor" medida del tamaño de un caso? ¿Cuáles de las operaciones que intervienen son más significativas, en oposición a aquellas que requieren relativamente poco esfuerzo? Para ilustrar los métodos que pueden usarse, discutiremos con detalle el algoritmo para hallar la representación binaria de un entero positivo dado en expresión decimal. Seguiremos las tres etapas que acabamos de exponer.

(A) El algoritmo se basa en la división por 2 reiterada. Para un entero positivo  $m$ , calculamos

$$m = 2q_0 + r_0$$

$$q_0 = 2q_1 + r_1$$

...

$$q_{k-1} = 2q_k + r_k.$$

Los restos  $r_i$  son todos 0 o 1 y nos detenemos cuando  $q_k = 0$ . La representación binaria buscada es la sucesión  $r_k r_{k-1} \dots r_1 r_0$ . El algoritmo se describe con exactitud en la página 168.

(B) Hay dos posibles medidas del tamaño de un caso. Podríamos usar el propio valor de  $m$ , pero sería más razonable usar el número  $n$  de cifras

de  $m$ . Esto se debe a que necesitamos teclear únicamente  $n$  veces para escribir el número  $m$ : si

$$m = (x_{n-1}x_{n-2} \dots x_1x_0)_{10},$$

entonces  $m$  está entre  $10^{n-1}$  y  $10^n - 1$ , con lo que  $n - 1$  es la parte entera de  $\log_{10} m$ , que escribiremos  $\lfloor \log_{10} m \rfloor$ . (Si  $x$  es un número real cualquiera, el símbolo  $\lfloor x \rfloor$  denota el mayor entero  $i$  tal que  $i \leq x$ .) Por lo tanto, el número  $n$  de cifras decimales de  $m$  viene dado por

$$n = \lfloor \log_{10} m \rfloor + 1.$$

(C) La operación más significativa es la división por 2 y el algoritmo la lleva a cabo  $k + 1$  veces. Este es también el número de cifras en la representación binaria de  $m$ , de modo que el mismo razonamiento nos da

$$k + 1 = \lfloor \log_{10} m \rfloor + 1.$$

La teoría elemental de los logaritmos nos dice que

$$\log_2 m = \frac{\log_{10} m}{\log_{10} 2} = (3.3219\dots) \times \log_{10} m,$$

de donde el número de operaciones,  $k + 1$ , es aproximadamente  $10n/3$  (como función de  $n$ ).

Consideraremos suficiente una fórmula aproximada para la eficiencia de un algoritmo ya que interesa más predecir su comportamiento en casos grandes que los detalles (que, en cualquier caso, dependerán de factores externos).

En este ejemplo particular, todos los casos con  $n$  cifras decimales requieren aproximadamente el mismo número de operaciones. En otros problemas, el esfuerzo necesario puede variar considerablemente para distintos casos del mismo tamaño. En tales circunstancias, acostumbramos a ser pesimistas y consideramos el **caso peor** de entre los casos de un tamaño dado.

**Ejercicios 7.5**

1 Supongamos que queremos calcular el mínimo de un conjunto finito de enteros  $\{x_1, x_2, \dots, x_n\}$  mediante el algoritmo descrito en el ejercicio 7.3.3.

- (i) Sugerir una buena medida del tamaño de un caso.
  - (ii) ¿Cuántas comparaciones son necesarias?
  - (iii) ¿Cuál es el caso peor respecto del número de instrucciones de asignación necesarias?
- 2 La regla para multiplicar dos números complejos es

$$(a + ib)(c + id) = x + iy,$$

donde  $x = ac - bd$  e  $y = ad + bc$ . Esto reduce el problema a cuatro multiplicaciones de números reales, una suma y una resta. Demostrar que es posible redefinir la regla de forma que sólo sean necesarios los tres productos  $a \times c$ ,  $b \times d$  y  $(a+b) \times (c+d)$ . ¿Cuántas sumas y cuántas restas son necesarias con este método?

3 La tabla 7.5.1 nos da el número de pasos necesarios para hallar  $\text{mcd}(a, b)$  mediante el algoritmo de Euclides para  $a \geq b \geq 1$  y  $a \leq 5$ .

- (i) Extender la tabla hasta  $a \leq 13$ .
- (ii) Para cada  $n$  entre 2 y 5, hallar el mínimo par  $(a_n, b_n)$  que requiere  $n$  pasos.
- (iii) Sugerir una regla para hallar el par  $(a_n, b_n)$  en general e intentar demostrarla.

**Tabla 7.5.1**

$b$	$a = 1$	$a = 2$	$a = 3$	$a = 4$	$a = 5$
1	1	1	1	1	1
2		1	2	1	2
3			1	2	3
4				1	2
5					1

**7.6 Órdenes de crecimiento: la notación  $O$ .**

La discusión del apartado anterior nos ha dado una idea bastante clara del significado de la palabra "eficiencia" en el contexto de los algoritmos. A partir de ahora, convendremos en que la eficiencia de un algoritmo es el número  $f(n)$  de operaciones (de un tipo determinado) que son necesarias para un caso de tamaño  $n$ , en el peor de los casos.

Es instructivo fijarse en los datos numéricos que relacionan la eficiencia de un algoritmo con el tiempo necesario para ejecutarlo. Supongamos que tenemos una máquina que efectúa un millón de operaciones por segundo y un algoritmo cuya eficiencia es  $f(n)$ . La tabla 7.6.1 nos indica el tiempo requerido para varias funciones usuales  $f$  y varios tamaños de  $n$ .

**Tabla 7.6.1**

$f(n)$	$n = 20$	$n = 40$	$n = 60$
$n$	0.00002 s	0.00004 s	0.00006 s
$n^2$	0.0004 s	0.0016 s	0.0036 s
$n^3$	0.008 s	0.064 s	0.216 s
$2^n$	1.0 s	12.7 días	366 siglos

Un ejemplo de un algoritmo que requiere  $2^n$  operaciones sería uno que debiera examinar todos los  $2^n$  subconjuntos de un conjunto de tamaño  $n$ . Es evidente que un tal algoritmo no es muy práctico y sería aconsejable buscar un algoritmo alternativo que necesitara únicamente un número de operaciones del orden de  $n^2$  o  $n^3$ . Se dice que un algoritmo es "polinómico en tiempo" si requiere  $n^c$  operaciones (donde  $c \geq 1$  es una constante), mientras que uno que requiera  $c^n$  operaciones ( $c > 1$ ) es un algoritmo "exponencial en tiempo".

Pasamos a introducir una notación matemática muy útil para estimar la eficiencia de un algoritmo. Al describir cómo el número de operaciones  $f(n)$  depende del tamaño  $n$ , podemos ignorar contribuciones relativamente pequeñas. También podemos pasar por alto características especiales que se producen si  $n$  es bastante pequeño. Lo que interesa es estimar el orden de crecimiento de  $f(n)$ , válido para todo  $n$  salvo quizás para un número finito de valores especiales. La siguiente definición resulta adecuada para tal propósito.

**Definición.** Sea  $f$  una función de  $\mathbf{N}$  en  $\mathbf{N}$ . Decimos que

$$f(n) \text{ es } O(g(n))$$

si existe una constante positiva  $k$  tal que  $f(n) \leq kg(n)$  para todo  $n$  de  $\mathbf{N}$  (con la posibilidad de un número finito de excepciones). El símbolo  $O(g(n))$  se pronuncia "o grande de  $g(n)$ ".

Supongamos que hemos hallado que el número de operaciones utilizadas por un cierto algoritmo es  $3n^3 + 20n^2 + 5n + 11$ . Como  $n \leq n^3$  y  $n^2 \leq n^3$ , tenemos la desigualdad

$$3n^3 + 20n^2 + 5n + 11 \leq (3 + 20 + 5 + 11)n^3.$$

Como el término de la derecha es un múltiplo constante de  $n^3$ , podemos decir que la eficiencia del algoritmo en este caso es  $O(n^3)$ . Simplificando, la notación  $O$  escoge el término más importante de una expresión e ignora los factores constantes. De esta forma se obtienen estimaciones como

$$n^2 + 17n + 3 \text{ es } O(n^2),$$

$$2^n + 3n^5 + 12n^4 \text{ es } O(2^n).$$

Hay un par de aspectos de la notación  $O$  que pueden causar dificultades. En primer lugar, no debiéramos escribir *ecuaciones* del tipo  $f(n) = O(g(n))$ , ya que puede conducir fácilmente a la conclusión (falsa) de que  $g(n)$  es  $O(f(n))$ . En segundo lugar, cuando decimos que  $f(n)$  es  $O(g(n))$ , se deduce a veces que  $g(n)$  es la "mejor" estimación de  $f(n)$ , aunque esto no forma parte estrictamente de la definición. Por ejemplo, es perfectamente correcto decir que la expresión  $n^2 + 17n + 3$  es  $O(n^3)$ , en lugar de  $O(n^2)$ . Por este motivo, a veces decimos que  $n^2 + 17n + 3$  es *como mínimo*  $O(n^2)$  y queda implícito que no existe una estimación mejor.

### Ejercicios 7.6

1 Hallar una función  $g(n)$  (de la forma  $A^B$ ) tal que  $f(n)$  sea  $O(g(n))$  en cada uno de los siguientes casos:

$$(i) \quad f(n) = \binom{n}{3};$$

$$(ii) \quad f(n) = \frac{5n^3 + 6}{n + 2};$$

$$(iii) \quad f(n) = \begin{cases} 3f(n-1) & (n > 1); \\ 2 & (n = 1); \end{cases}$$

$$(iv) \quad f(n) = n!$$

2 Demostrar que para cualesquiera constantes positivas  $C_0, C_1, \dots, C_k$ , la expresión

$$C_0 + C_1 n + C_2 n^2 + \dots + C_k n^k$$

es  $O(n^k)$ . Demostrar que la expresión *no* es  $O(n^{k-1})$ .

3 Supongamos que un algoritmo requiere  $n$  pasos en el peor de los casos de tamaño  $n$  y que en el  $i$ -ésimo paso ( $1 \leq i \leq n$ ) requiere  $i^2$  operaciones. Demostrar que la eficiencia del algoritmo es  $O(n^3)$ .

4 Cuando decimos que una expresión  $f(n)$  es  $O(n \log n)$ , ¿por qué es innecesario especificar la base de los logaritmos?

### 7.7 Comparación de algoritmos

Generalmente dispondremos de varios algoritmos para resolver un problema dado. A veces el algoritmo más directo es adecuado en la práctica, pero a menudo deberemos buscar algoritmos mejores para resolver casos de mayor tamaño. En este contexto, una eficiencia que sea  $O(\log n)$  será mejor que  $O(n)$  y  $O(n^a)$  es mejor que  $O(n^b)$  si  $a < b$ . Por ejemplo, el número de multiplicaciones de una cifra que intervienen en el algoritmo de multiplicación de dos enteros es  $O(n^2)$ , pero existe un algoritmo mejor cuya eficiencia es  $O(n^{1.59})$  (véanse los ejercicios 7.9.5 y 12.7.9). En este caso, el algoritmo más eficiente es también más complicado y no es necesario utilizarlo para cálculos de rutina. Pero si hemos de multiplicar un gran número de enteros grandes, el incremento en eficiencia puede compensar las complicaciones.

Ilustraremos estas ideas con el problema de calcular la potencia  $m$ -ésima de un número fijo  $u$ . Tomaremos como tamaño de un caso  $n = \lfloor \log_{10} m \rfloor$  (el número de cifras necesarias para representar  $m$ ) y como operaciones significativas las multiplicaciones. El método más sencillo (llamémosle *Algoritmo A*) para calcular  $u^m$  es calcular  $u^2, u^3, \dots, u^m$  sucesivamente, multiplicando cada término por  $u$ . Como esto supone  $m - 1$  multiplicaciones y  $m$  es aproximadamente  $10^n$ , la eficiencia del *Algoritmo A* es  $O(10^n)$ .

Es fácil ver, sin embargo, que hay algoritmos mejores. Por ejemplo, para calcular  $u^{23}$  podríamos calcular primero  $u^2, u^4, u^8, u^{16}$  multiplicando cada

término por sí mismo y entonces calcular

$$u \times u^2 = u^3, \quad u^3 \times u^4 = u^7, \quad u^7 \times u^{16} = u^{23}.$$

En este proceso se han hecho siete multiplicaciones en lugar de las 22 efectuadas por el *Algoritmo A*. La idea que se esconde tras el ejemplo puede deducirse de la ecuación

$$u^{23} = u^{16+4+2+1} = u^{16} \times u^4 \times u^2 \times u.$$

Esto explica por qué elegimos calcular  $u \times u^2 = u^3$ , después  $u^3 \times u^4 = u^7$  y finalmente  $u^7 \times u^{16} = u^{23}$ . Podemos hacer la regla más explícita si observamos que la representación binaria de 23 es 10111, de forma que

$$\begin{array}{rcl} 23 &= 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1 \\ &16 &+ 4 &+ 2 &+ 1 \end{array}$$

La figura 7.1 describe el proceso de cálculo. La línea superior presenta, de derecha a izquierda, el cálculo sucesivo de  $u^2, u^4, u^8, u^{16}$ , etc. En la línea inferior se multiplica el valor acumulado por el valor de la línea superior si la correspondiente cifra binaria es 1 y no se modifica si la cifra es 0.

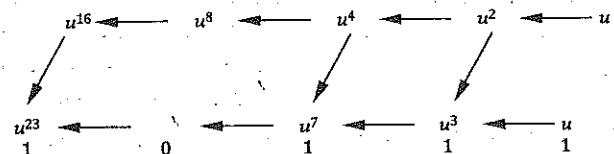


Fig. 7.1 Cálculo de  $u^{23}$ .

En la siguiente descripción del *Algoritmo B*, los identificadores *sup* e *inf* corresponden a las líneas superior e inferior de la figura 7.1. Obsérvese que calculamos la representación binaria de  $m$  a medida que procedemos. Nótese también que, en aras de una descripción uniforme, el programa hace dos multiplicaciones "innecesarias": en el caso  $m = 23$  son  $u \times 1 = u$  al principio y  $u^{16} \times u^{16} = u^{32}$  al final.

```
q:=m; inf:=1; sup:=u;
mientras q>0 hacer
```

```
    inicio
    si q mod 2=1 entonces inf:= sup*inf;
    sup:=sup*sup;
    q:=q div 2
    fin;
    potencia:=inf
```

Si el número de cifras binarias de  $m$  es  $L(m)$ , el *Algoritmo B* efectúa a lo sumo  $2m - 1$  multiplicaciones. Ahora bien,  $L(m)$  es aproximadamente  $\log_2 m$  y hemos acordado utilizar  $n = \lfloor \log_{10} m \rfloor$  como medida de un caso. Así pues,  $L(m)$  es un múltiplo constante de  $n$  y la eficiencia es  $O(n)$ . Esto es una mejora sustancial respecto del *Algoritmo A*; por ejemplo, para calcular  $n^{1000}$  son necesarias unas 20 multiplicaciones, en lugar de 999.

¿Podríamos encontrar un método aún mejor? Para valores concretos de  $m$ , podemos, en efecto, conseguir alguna mejora. Si  $m = 15$ , el *Algoritmo B* necesita seis multiplicaciones, mientras que cinco son suficientes:

$$\begin{aligned} u \times u &= u^2, & u \times u^2 &= u^3, & u^2 \times u^3 &= u^5, \\ u^5 \times u^5 &= u^{10}, & u^5 \times u^{10} &= u^{15}. \end{aligned}$$

Sin embargo, es fácil ver que el *Algoritmo B* no puede ser sustancialmente mejorado para todos los valores de  $m$ . Esto se debe a que una multiplicación no puede hacer más que doblar el mayor exponente obtenido hasta el momento, de modo que  $r$  multiplicaciones no pueden llevarnos más allá de  $u^{2^r}$ . Así pues, si  $m = 2^r + 1$ , el número de multiplicaciones necesarias para calcular  $u^m$  es al menos  $r + 1$ , que es aproximadamente  $\log_2 m$ . Deducimos que la eficiencia de cualquier algoritmo que resuelva este problema es como mínimo  $O(n)$ .

### Ejercicios 7.7

1 Estimar el tiempo necesario para calcular  $n^{100000}$  utilizando los *Algoritmos A* y *B*, suponiendo que podemos hacer una multiplicación por segundo.

2 ¿Cuántas multiplicaciones son necesarias para calcular  $m^{55}$  mediante los *Algoritmos A* y *B*? Hallar un método que requiera únicamente ocho multiplicaciones.

3 Utilizar las ideas del apartado 7.4 para obtener una demostración de la corrección del *Algoritmo B*. La demostración ha de justificar las siguientes afirmaciones:

- (i) el algoritmo termina;
- (ii) si  $b, t$  y  $q$  denotan los valores de los identificadores `inf`, `sup` y `q`, entonces  $bt^q$  es invariante en la instrucción iterativa;
- (iii) cuando el algoritmo termina, el valor calculado es  $u^m$ .

4 La regla para multiplicar matrices  $2 \times 2$  es

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix}.$$

Esto supone 8 multiplicaciones y 4 sumas. Demostrar que el cálculo puede hacerse con sólo 7 multiplicaciones:

$$\begin{aligned} m_1 &= (a+d) \times (x+t) & m_5 &= (a+b) \times t \\ m_2 &= (c+d) \times x & m_6 &= (c-a) \times (x+y) \\ m_3 &= a \times (y-t) & m_7 &= (b-d) \times (z+t). \\ m_4 &= d \times (z-x) \end{aligned}$$

(Hay que demostrar que cada elemento de la matriz producto puede expresarse como una suma de términos  $m_i$  ( $1 \leq i \leq 7$ ).) ¿Cuántas sumas y restas comporta este método?

## 7.8 Introducción a los algoritmos de ordenación

Supongamos que tenemos una lista de estudiantes en orden alfabético y queremos reordenarlos según los resultados obtenidos en un examen. Este es un ejemplo de un problema de *ordenación*. Para simplificar, supondremos que los resultados son todos distintos, ya que si algunos de ellos son iguales las modificaciones necesarias son sencillas.

Consideraremos el problema en toda su generalidad. Dada una sucesión de números enteros distintos  $\{x_1, x_2, \dots, x_n\}$  queremos ordenarla en orden creciente. En otras palabras, buscamos una permutación  $\pi$  del conjunto  $\{1, 2, \dots, n\}$  tal que

$$x_{\pi(1)} < x_{\pi(2)} < x_{\pi(3)} < \dots < x_{\pi(n)}.$$

En la práctica no se calcula  $\pi$  explícitamente; simplemente se ordenan los números en el orden pedido. Por ejemplo, la sucesión 7, 2, 9, 3, 5 se convierte en 2, 3, 5, 7, 9.

Uno de los algoritmos de ordenación más sencillos se conoce como la *ordenación de la burbuja*. La idea es comparar términos adyacentes de la lista e intercambiarlos si están en el orden erróneo. En la "primera pasada" del algoritmo se comparan el primer y el segundo elemento, después el segundo y el tercero, y así sucesivamente. Cada comparación se refiere a los elementos en el orden resultante de todas las comparaciones anteriores. Por ejemplo, la tabla 7.8.1 muestra el efecto de la primera pasada en el orden inicial 4, 7, 3, 1, 5, 8, 2, 6.

Tabla 7.8.1

Orden inicial	4	7	3	1	5	8	2	6
Después de la 1. <sup>a</sup> comparación:	4	7						
Después de la 2. <sup>a</sup> comparación:		3	7					
Después de la 3. <sup>a</sup> comparación:			1	7				
Después de la 4. <sup>a</sup> comparación:				5	7			
Después de la 5. <sup>a</sup> comparación:					7	8		
Después de la 6. <sup>a</sup> comparación:						2	8	
Después de la 7. <sup>a</sup> comparación:							6	8
Después de la primera pasada:	4	3	1	5	7	2	6	8

Al concluir la primera pasada, podemos estar seguros de que el máximo se encuentra en el último lugar. En la "segunda pasada" se comparan los primeros  $n - 1$  enteros de la misma forma y al concluir podemos asegurar que los dos enteros mayores están en sus posiciones correctas. Continuamos de esta forma hasta efectuar  $n - 1$  pasadas, después de las cuales se ha completado la ordenación.

Una de las mayores ventajas de la ordenación de la burbuja es que es fácil construir una versión explícita en un lenguaje de programación. Dado un conjunto de enteros  $\{x_1, x_2, \dots, x_n\}$ , el siguiente algoritmo los ordena en orden creciente:

```
para j:=1 hasta n-1 hacer
  para i:=1 hasta n-j hacer
    si  $x_i > x_{i+1}$  entonces intercambiar  $x_i$  y  $x_{i+1}$ 
```

Las operaciones que intervienen son comparaciones e intercambios. En el paso  $j$  se hacen  $n - j$  comparaciones, de forma que el número total de

comparaciones es

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

que es  $O(n^2)$ . El número de intercambios es también  $O(n^2)$ , ya que en el peor de los casos (cuando los enteros vienen dados en el orden inverso) cada comparación va seguida de un intercambio.

En el capítulo 9 demostraremos que el número de comparaciones necesarias en *cualquier* algoritmo de ordenación es como mínimo  $O(n \log n)$ . Si hallamos un algoritmo con eficiencia  $O(n \log n)$ , será mejor, en el sentido del apartado 7.7, que el de la burbuja, cuya eficiencia es  $O(n^2)$ . De hecho, se concen varios algoritmos  $O(n \log n)$  para el problema de la ordenación. Describiremos uno de los más sencillos, una versión de la ordenación por *inserción*.

La idea básica de la ordenación por inserción es empezar con la lista  $L = (x_1)$  e insertar  $x_i$  en el lugar correcto de la lista para  $i = 2, 3, \dots, n$ . Por ejemplo, si  $x_1, x_2, \dots, x_8$  son los enteros 47, 73, 21, 45, 28, 69, 19, 23, la tabla 7.8.2 muestra cómo se construye la lista.

Tabla 7.8.2

47
47    73
21    47    73
21    45    47    73
21    28    45    47    73
21    28    45    47    69    73
19    21    28    45    47    69    73
19    21    23    28    45    47    69    73

En la ordenación por inserción, el número de comparaciones necesarias para hallar el lugar correcto de  $x_i$  depende de cuál de varios métodos posibles se adopte. Si usamos el método secuencial, en el que se compara  $x_i$  sucesivamente con cada elemento de la lista parcial (empezando por la izquierda), entonces podríamos necesitar hasta  $i - 1$  comparaciones antes de hallar el lugar correcto. De este modo, el número total de comparaciones podría llegar a ser  $(n-1) + \dots + 1$ , que de nuevo es  $O(n^2)$ . Pero la inserción puede hacerse más hábilmente por “bisección”: hallar en qué mitad de la

lista está  $x_i$ , después en qué mitad de la mitad, etc. Si hay entre  $2^{r-1}$  y  $2^r$  términos, el método requiere  $r$  comparaciones (puesto que la lista parcial ya está ordenada). En otras palabras, para una lista de longitud  $i - 1$  se necesitan alrededor de  $\log_2 i$ . Así pues, el número total de comparaciones es aproximadamente

$$\log_2 2 + \log_2 3 + \dots + \log_2 n,$$

una expresión con  $n - 1$  términos, cada uno de ellos menor o igual que  $\log_2 n$ . Por lo tanto, el número de comparaciones es  $O(n \log n)$ .

Aunque la ordenación por inserción utilizando bisecciones alcanza el mejor orden de magnitud posible del número de comparaciones, es más difícil de programar que la ordenación de la burbuja. Por otra parte, el número de intercambios sigue siendo  $O(n^2)$ , ya que al insertar  $x_i$  hay que desplazar todos los  $i - 1$  elementos de la lista parcial. Sin embargo, existen algoritmos que consiguen  $O(n \log n)$  comparaciones y  $O(n \log n)$  intercambios; en el apartado 9.2 describiremos uno de ellos, el de *heapsort*.

### Ejercicios 7.8

- 1 Describir el resultado de cada una de las “pasadas” del algoritmo de la burbuja sobre la lista 4, 3, 9, 5, 1, 2, 7, 8, 6.
- 2 Utilizar la ordenación por inserción (a mano!) para ordenar la lista siguiente en orden creciente: 516, 207, 321, 581, 762, 163, 921, 105, 721, 813, 316, 188, 733, 909, 281, 312, 871, 950, 135, 888, 417.
- 3 Escribir un programa que, dada una sucesión  $z_1, z_2, \dots, z_n$  de enteros distintos en orden creciente, inserte un entero  $q$  en el lugar correcto y devuelva una lista  $w_1, w_2, \dots, w_{n+1}$  (puede suponerse que  $q$  no coincide con ninguno de los  $z_i$  y se observará que el método secuencial es mucho más sencillo de programar que el de la bisección).
- 4 Modificar el algoritmo de la burbuja incluyendo un identificador  $c$  con las siguientes propiedades.
  - (i) El valor de  $c$  es el número de intercambios en la pasada actual.
  - (ii) Al inicio de cada pasada se pone  $c$  a cero.
  - (iii) Si  $c$  es cero al final de una pasada, el programa no realizará más pasadas.

5 Calcular el número de comparaciones y el número de intercambios del programa de la burbuja modificado como en el ejercicio anterior, si la lista inicial está

- (i) en el orden correcto  $x_1 < x_2 < \dots < x_n$ ;
- (ii) en el orden inverso  $x_1 > x_2 > \dots > x_n$ .

6 La *ordenación por selección* es un algoritmo de ordenación alternativo. En este método, en el paso  $j$ -ésimo se selecciona el menor de  $x_j, x_{j+1}, \dots, x_n$  y (si no es  $x_j$ ) se intercambia con  $x_j$ . Describir cómo opera este método con la lista del ejercicio 1. ¿Cuántas comparaciones y cuántos intercambios se necesitan en general?

## 7.9 Ejercicios diversos

1 Demostrar formalmente que el algoritmo para sumar en base 10 dado en el ejemplo del apartado 7.1 es correcto. En otras palabras, demostrar que si

$$a = (a_{n-1}, a_{n-2}, \dots, a_1, a_0)_{10}, \quad b = (b_{n-1}, b_{n-2}, \dots, b_1, b_0)_{10}$$

y los dígitos  $s_i$  ( $0 \leq i \leq n$ ) se definen mediante las fórmulas dadas allí, entonces

$$a + b = (s_n, s_{n-1}, \dots, s_1, s_0)_{10}.$$

2 Igual que en el ejercicio anterior, pero para el algoritmo descrito en el ejercicio 7.1.1.

3 Describir (en lenguaje corriente) el método habitual para dividir; explicar por qué no es, en sentido estricto, un algoritmo.

4 Formular un algoritmo para restar en base 10 un número de  $n$  cifras de otro (mayor).

5 Sean  $x$  e  $y$  enteros de  $2n$  cifras en base 10 y sean

$$x = 10^n a + b, \quad y = 10^c + d,$$

donde  $a, b, c$  y  $d$  son enteros de  $n$  cifras. Comprobar la fórmula

$$xy = (10^{2n} + 10^n)ac + 10^n(a - b)(d - c) + (10^n + 1)bd$$

y explicar cómo podría usarse para mejorar el algoritmo elemental de multiplicación que calcula  $xy$ .

6 Determinar el valor de  $b$  calculado por el siguiente algoritmo.

```
x:=n; z:=1;
mientras x>1 hacer
    inicio
    z:=xz;
    x:=x-1;
    fin
    b:=z
```

7 Demuestre formalmente que su afirmación sobre el valor de  $b$  en el ejercicio anterior es correcta.

8 Sea  $n$  un entero positivo y  $p$  un primo. ¿Qué significado tiene el valor  $c$  que calcula el siguiente programa?

```
x:=n; y:=p; t:=p; z:=0;
mientras y sea divisible por x hacer
    inicio
    y:=ty;
    z:=z+1;
    fin;
    c:=z
```

9 Escribir el programa de multiplicación necesario para el cálculo de  $m^n$  en el *Algoritmo B* (apartado 7.7) cuando (i)  $n = 59$ , (ii)  $n = 77$ . Demostrar que en ambos casos el método requiere únicamente ocho multiplicaciones.

10 Escribir un programa que, dados dos enteros positivos  $a$  y  $b$  en base 10, asigne a  $q$  el valor 0, 1 o -1, según que  $a < b$ ,  $a = b$  o  $a > b$ .

11 ¿Cuántas sumas y multiplicaciones son necesarias para calcular el producto de dos matrices  $n \times n$  según el método estándar?

12 Hallar un método para multiplicar dos matrices  $4 \times 4$  que requiera menos de 64 multiplicaciones. [Indicación:  $2 + 2 = 4$ .]

13 Sea  $(f_r)$  la sucesión definida por

$$f_1 = 1, \quad f_2 = 2, \quad f_r = f_{r-1} + f_{r-2} \quad (r \geq 2).$$

Demostrar que si  $m \geq n$  y el algoritmo euclídeo necesita  $k$  pasos para calcular  $\text{mcd}(m, n)$ , entonces  $n \geq f_k$ . Deducir que el número de pasos necesario es  $O(\log n)$ .

14 Utilizar el principio de inducción para demostrar que después de  $k$  "pasadas" del algoritmo de la burbuja los últimos  $k$  enteros están en la posición correcta.

15 Escribir un programa para calcular el  $\text{mcd}$  de tres enteros positivos dados  $r, s$  y  $t$ .

## 8 Grafos

### 8.1 Los grafos y su representación

Los objetos conocidos como *grafos* son muy útiles en la matemática discreta. Su nombre proviene del hecho que admiten una notación gráfica (o pictórica) y corresponden a lo que en el lenguaje cotidiano se conoce como “redes”.

**Definición.** Un grafo  $G$  consiste en un conjunto finito  $V$ , cuyos elementos reciben el nombre de **vértices**, y un conjunto  $E$  de 2-subconjuntos de  $V$ , cuyos elementos se conocen como **aristas**. Habitualmente escribimos  $G = (V, E)$  y decimos que  $V$  es el **conjunto de vértices** y  $E$  el **conjunto de aristas**.

La restricción a conjuntos finitos no es esencial, pero en este libro no consideraremos “grafos” infinitos.

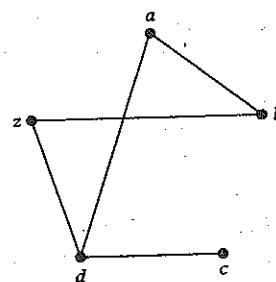


Fig. 8.1 Una representación pictórica de un grafo.

Un ejemplo típico de un grafo  $G = (V, E)$  viene dado por los conjuntos

$$V = \{a, b, c, d, z\}, \quad E = \{\{a, b\}, \{a, d\}, \{b, z\}, \{c, d\}, \{d, z\}\}.$$

Ni este ejemplo ni la propia definición nos dicen gran cosa, pero todo cambia si mostramos la *representación pictórica* de un grafo. Los vértices se representan por puntos y unimos dos puntos por una línea si el par correspondiente de vértices es una arista. Por ejemplo, la figura 8.1 es una representación pictórica del grafo dado en el ejemplo anterior. Esta representación es enormemente conveniente para estudiar “a mano” grafos no demasiado grandes. Además, su carácter intuitivo es de gran ayuda para formular y entender argumentos abstractos. Vamos a dar un ejemplo frívolo de todo esto.

**Ejemplo.** El profesor McBrain y su mujer April dan una fiesta en la que hay otros cuatro matrimonios. Algunas parejas se dan la mano al saludarse, pero naturalmente nadie da la mano a su pareja. Al acabar la fiesta, el profesor McBrain pregunta a los asistentes a cuánta gente han dado la mano y recibe nueve respuestas distintas. ¿A cuántas personas ha dado la mano April?

**SOLUCIÓN:** Construimos un grafo cuyos vértices son las personas de la fiesta; el par  $\{x, y\}$  es una arista si  $x$  e  $y$  se han dado la mano. Como hay nueve personas además del profesor McBrain y el número máximo de apretones de manos que puede dar una persona es ocho, resulta que las nueve respuestas distintas recibidas por el profesor McBrain deben ser 0, 1, 2, 3, 4, 5, 6, 7 y 8. Denotaremos los vértices por esos números y usaremos la  $M$  para el propio McBrain. Así que la representación pictórica es la de la figura 8.2

Ahora bien, el vértice 8 está unido a todos los demás vértices salvo uno, que necesariamente ha de representar a su esposa. Este vértice ha de ser 0, ya que ciertamente no está unido con 8 (ni con ningún otro, por lo demás). Por lo tanto, 8 y 0 son un matrimonio y 8 está unido a 1, 2, ..., 7 y  $M$ . En particular, 1 está unido a 8 y esta es la única arista desde 1. Luego, el vértice 7 no está unido (únicamente) a 0 y 1, de donde la esposa de 7 debe ser 1, ya que 0 está casada con 8. Razonando de esta forma, podemos ver que 6 y 2, y 5 y 3 son matrimonios, con lo que  $M$  y 4 han de

estar casados; April está representada por el vértice 4 y ha dado la mano a cuatro personas.  $\square$

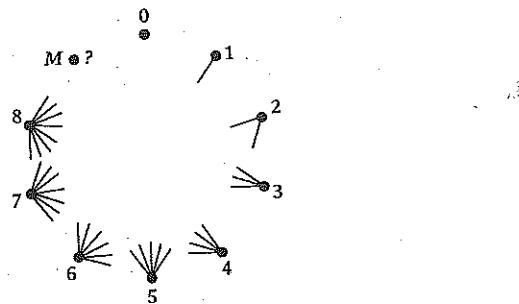


Fig. 8.2 La fiesta de April.

Aunque la representación pictórica de los grafos es conveniente para los seres humanos, es claramente inútil para comunicarnos con un ordenador. En este caso hemos de representar un grafo mediante algún tipo de lista o tabla. Diremos que dos vértices  $x$  e  $y$  de un grafo son **adyacentes** si  $\{x, y\}$  es una arista (también decimos que  $x$  e  $y$  son **vecinos**). Podemos representar un grafo  $G = (V, E)$  por su **lista de adyacencias**, en la que cada vértice  $v$  encabeza una lista de los vértices que le son adyacentes. El grafo de la figura 8.1 tiene la lista de adyacencias

$a$	$b$	$c$	$d$	$z$
$b$	$a$	$d$	$a$	$b$
$d$	$z$		$c$	$d$
			$z$	

### Ejercicios 8.1

- 1 Hay que conectar tres casas A, B y C a las redes de gas, agua y electricidad: G, W y E. Escribir la lista de adyacencia del grafo que representa este problema y construir una representación pictórica. ¿Puede

hallarse alguna figura en la que las líneas que representan la aristas no se corten?

- 2 Los caminos de un jardín están diseñados en forma de un **grafo rueda**  $W_n$ , que tiene por vértices  $V = \{0, 1, 2, \dots, n\}$  y por aristas

$$\begin{aligned} \{0, 1\}, \quad & \{0, 2\}, \dots, \{0, n\}, \\ \{1, 2\}, \quad & \{2, 3\}, \dots, \{n-1, n\}, \quad \{n, 1\}. \end{aligned}$$

Describir una ruta a través de los caminos que empiece y acabe en el vértice 0 y visite cada vértice exactamente una vez.

- 3 Para cada entero positivo  $n$  definimos el **grafo completo**  $K_n$  como el grafo de  $n$  vértices en el que cada par de vértices es adyacente. ¿Cuántas aristas tiene  $K_n$ ? ¿Para qué valores de  $n$  puede hallarse una representación pictórica de  $K_n$  con la propiedad de que las líneas que representan las aristas no se corten?

- 4 Un **3-ciclo** en un grafo es un conjunto de tres vértices mutuamente adyacentes. Construir un grafo con cinco vértices y seis aristas que no contenga 3-ciclos.

### 8.2 Isomorfismos de grafos

Llegados a este punto, hay que insistir en que un grafo se define como una entidad matemática abstracta; bajo este prisma discutiremos la importante cuestión de cuándo dos grafos son “el mismo”.

Es evidente que lo importante de un grafo no son los nombres de los vértices ni su representación pictórica, o cualquier otra representación. La propiedad característica de un grafo es la manera en que los vértices están unidos por las aristas. Esto motiva la siguiente definición.

**Definición.** Decimos que dos grafos  $G_1$  y  $G_2$  son **isomorfos** si existe una biyección  $\alpha$  entre el conjunto de vértices de  $G_1$  y el conjunto de vértices de  $G_2$ , de forma que  $\{\alpha(x), \alpha(y)\}$  es una arista de  $G_2$  si, y sólo si,  $\{x, y\}$  es una arista de  $G_1$ . Se dice que la biyección  $\alpha$  es un **isomorfismo**.

Por ejemplo, consideremos los dos grafos dibujados en la figura 8.3. En este caso existe una biyección entre el conjunto de vértices de  $G_1$  y el

conjunto de vértices de  $G_2$  con la propiedad exigida; viene dada por

$$\alpha(a) = t, \quad \alpha(b) = v, \quad \alpha(c) = w, \quad \alpha(d) = u.$$

Podemos comprobar que cada arista de  $G_1$  corresponde de forma única a una arista de  $G_2$ , y recíprocamente. Por ejemplo, la arista  $bc$  de  $G_1$  corresponde a la arista  $vw$  de  $G_2$ ; y así sucesivamente. (Acostumbraremos a usar la notación  $xy$  como una abreviatura de la arista  $\{x, y\}$ , aunque no debemos olvidar que una arista es un par no ordenado, de forma que  $xy$  e  $yx$  significan lo mismo.)

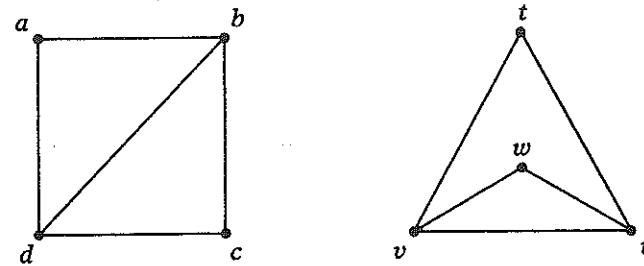


Fig. 8.3  $G_1$  y  $G_2$  son isomorfos.

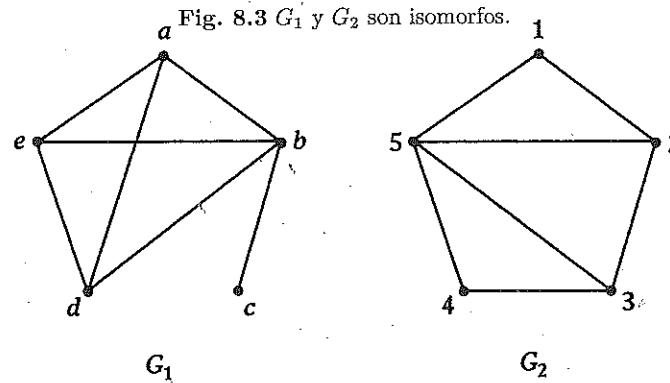


Fig. 8.4  $G_1$  y  $G_2$  no son isomorfos.

Cuando dos grafos  $G_1$  y  $G_2$  son isomorfos, como los de la figura 8.3, pensamos en ellos como si fueran "el mismo" grafo. Para demostrar que dos grafos *no* son isomorfos, hay que demostrar que no existe ninguna biyección entre el conjunto de vértices del uno y el del otro que transforma aristas en aristas. Si los dos grafos no tienen el mismo número de vértices, no hay

biyección posible. Si tienen el mismo número de vértices pero un número distinto de aristas, existen biyecciones pero ninguna de ellas puede ser un isomorfismo (ejercicio 8.8.10). Incluso si dos grafos tienen el mismo número de vértices y de aristas, no tienen por qué ser isomorfos. Por ejemplo, los dos grafos de la figura 8.4 tienen ambos cinco vértices y siete aristas, pero no son isomorfos. Una forma de demostrarlo es observando que los vértices  $a, b, d, e$  forman un subgrafo completo de  $G_1$  (cada par de ellos está unido por una arista). Cualquier isomorfismo debe transformar estos vértices en cuatro vértices de  $G_2$  con la misma propiedad, y como no existe ningún conjunto de vértices de este tipo en  $G_2$ , no pueden ser isomorfos.

### Ejercicios 8.2

- 1 Demostrar que los grafos que se muestran en la figura 8.5 no son isomorfos.

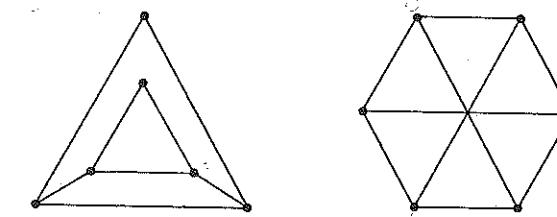


Fig. 8.5 Demostrar que estos grafos no son isomorfos.

- 2 Hallar un isomorfismo entre los grafos definidos por las siguientes listas de adyacencias (ambas listas corresponden a un conocido grafo, el grafo de Petersen. Véase también el ejercicio 8.8.3.)

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>	0	1	2	3	4	5	6	7	8	9
<i>b</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	1	2	3	4	5	0	1	0	2	6
<i>e</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>a</i>	<i>h</i>	<i>i</i>	<i>j</i>	<i>f</i>	<i>g</i>	5	0	1	2	3	4	4	3	5	7
<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>	<i>i</i>	<i>j</i>	<i>f</i>	<i>g</i>	<i>h</i>	7	6	8	7	6	8	9	9	9	8

- 3 Sea  $G = (V, E)$  el grafo definido de la siguiente forma. El conjunto de vértices  $V$  es el conjunto de las palabras de longitud 3 en el alfabeto

$\{0,1\}$  y el conjunto de aristas  $E$  contiene aquellos pares de palabras que difieren en una posición exactamente. Demostrar que  $G$  es isomorfo al grafo formado por las esquinas y las aristas de un cubo ordinario.

### 8.3 Grados

El grado de un vértice  $v$  en un grafo  $G = (V, E)$  es el número de aristas de  $G$  que contienen a  $v$ . Emplearemos la notación  $\delta(v)$  para el grado de  $v$ ; formalmente

$$\delta(v) = |D_v|, \quad \text{donde } D_v = \{e \in E \mid v \in e\}.$$

El grafo descrito en la figura 8.1 tiene  $\delta(a) = 2$ ,  $\delta(b) = 2$ ,  $\delta(c) = 1$ ,  $\delta(d) = 3$  y  $\delta(z) = 2$ . El primer teorema de la teoría de grafos afirma que la suma de estos números es dos veces el número de aristas; es una sencilla aplicación del método de contar conjuntos de pares expuesto en el apartado 3.2.

**Teorema 8.3.** *La suma de los grados  $\delta(v)$  para todos los vértices  $v$  de un grafo  $G = (V, E)$  es igual al doble del número de aristas:*

$$\sum_{v \in V} \delta(v) = 2|E|.$$

**DEMOSTRACIÓN:** Sea  $S$  el subconjunto de  $V \times E$  formado por los pares  $(v, e)$  tales que  $v$  pertenece a  $e$ . Para cada  $v$  de  $V$ , el “total por filas”  $r_v(S)$  es el número de aristas que contienen a  $v$ , es decir, igual a  $\delta(v)$ . Para cada  $e$  de  $E$ , el “total por columnas”  $c_e(S)$  es el número de vértices de  $e$ , que es 2. Así pues, según el teorema 3.2

$$\sum_{v \in V} \delta(v) = 2 + 2 + \cdots + 2 = 2|E|,$$

como queríamos demostrar.  $\square$

Este resultado tiene un corolario útil. Diremos que un vértice de  $G$  es **impar** si su grado es impar y **par** en caso contrario. Sean  $V_p$  y  $V_i$

los conjuntos de vértices pares e impares, respectivamente, de forma que  $V = V_p \cup V_i$  es una partición de  $V$ . Por el teorema 8.3, tenemos que

$$\sum_{v \in V_p} \delta(v) + \sum_{v \in V_i} \delta(v) = 2|E|.$$

Ahora bien, los términos de la segunda suma son pares y, en consecuencia, la suma es par. Como el término derecho es un número par, también lo es la primera suma. Pero una suma de números impares sólo puede ser par si hay un número par de ellos. En otras palabras:

*el número de vértices impares es par.*

Este resultado se conoce a veces como el lema de los apretones de manos: en cualquier grupo de gente, el número de personas que dan la mano a un número impar de personas es par.

Si todos los vértices de un grafo tienen el mismo grado  $r$ , se dice que el grafo es **regular** (de grado  $r$ ) o  **$r$ -regular**. En este caso, el resultado del teorema 8.3 se convierte en

$$r|V| = 2|E|.$$

De hecho, un grafo  $r$ -regular no es más que otro nombre para un 1-diseño con parámetros  $(|V|, 2, r)$ , con la terminología de el apartado 4.6. Pero este punto de vista no es especialmente útil en la práctica.

Muchos de los grafos que ocurren en las aplicaciones son regulares. Ya hemos visto los grafos completos  $K_n$  (ejercicio 8.1.3); son regulares de grado  $n - 1$ . En geometría elemental se estudian los polígonos de  $n$  lados, que en teoría de grafos corresponden a los grafos **ciclo**  $C_n$ . Formalmente, podemos decir que el conjunto de vértices de  $C_n$  es  $Z_n$ , y que los vértices  $i$  y  $j$  están unidos por una arista si  $j = i + 1$  o  $j = i - 1$  en  $Z_n$ . Es evidente que  $C_n$  es un grafo regular de grado 2, siempre que  $n \geq 3$ .

Una aplicación importante de la noción de grado se presenta en el problema de comprobar si dos grafos son o no isomorfos. Si  $\alpha : V_1 \rightarrow V_2$  es un isomorfismo entre  $G_1$  y  $G_2$  y  $\alpha(v) = w$ , entonces cada arista que contiene a  $v$  se transforma por  $\alpha$  en una arista que contiene a  $w$ . En consecuencia,  $\delta(v) = \delta(w)$ . Por otra parte, si  $G_1$  tiene un vértice  $x$  con  $\delta(x) = \delta_0$  y  $G_2$  no tiene ningún vértice con grado  $\delta_0$ , entonces  $G_1$  y  $G_2$

no pueden ser isomorfos. Esto proporciona otra forma de distinguir entre los dos grafos de la figura 8.4, ya que el primer grafo tiene un vértice de grado 1 y el segundo no.

En el ejercicio 8.3.4 se presenta una extensión de esta idea.

### Ejercicios 8.3

1 ¿Pueden ser las siguientes las listas de grados de todos los vértices de un grafo? En caso afirmativo, dar una representación pictórica de un grafo de estas características. (Recuérdese que cada par de vértices está unido por una arista como máximo.)

- (i) 2, 2, 2, 3.
- (ii) 1, 2, 2, 3, 4.
- (iii) 2, 2, 4, 4, 4.
- (iv) 1, 2, 3, 4.

2 Si  $G = (V, E)$  es un grafo, el complementario  $\bar{G}$  de  $G$  es el grafo cuyo conjunto de vértices es  $V$  y en el que dos vértices están unidos por una arista si no lo están en  $G$ . Si  $G$  tiene  $n$  vértices y sus grados son  $d_1, d_2, \dots, d_n$ , ¿cuáles son los grados de  $\bar{G}$ ?

3 Hallar tantos grafos (no isomorfos) 4-regulares con siete vértices como sea posible. [Indicación: considerar el grafo complementario.]

4 Sean  $G_1$  y  $G_2$  dos grafos isomorfos. Para cada  $k \geq 0$ , sea  $n_i(k)$  el número de vértices de  $G_i$  con grado  $k$  ( $i = 1, 2$ ). Demostrar que  $n_1(k) = n_2(k)$ .

5 Demostrar que si  $G$  es un grafo con al menos dos vértices,  $G$  tiene dos vértices con el mismo grado.

### 8.4 Caminos y ciclos

Con frecuencia se usan grafos como modelos de situaciones prácticas en las que intervienen rutas: los vértices representan ciudades o cruces y las aristas carreteras o algún otro tipo de vía de comunicación. Las definiciones de este apartado se comprenderán mejor teniendo en cuenta esta situación.

**Definición.** Un recorrido en un grafo  $G$  es una sucesión de vértices

$$v_1, v_2, \dots, v_k,$$

tal que  $v_i$  y  $v_{i+1}$  son adyacentes ( $1 \leq i \leq k-1$ ). Si todos los vértices son distintos, tenemos un **caminio**.

Así pues, un recorrido especifica una ruta en  $G$  que va de un vértice a otro adyacente, y así sucesivamente. Un recorrido puede visitar un vértice varias veces, y en particular puede cambiar de dirección yendo de  $x$  a  $y$  e inmediatamente de vuelta a  $x$ . En un camino, cada vértice se visita una vez como máximo.

Escribimos  $x \sim y$  si los vértices  $x$  e  $y$  de  $G$  pueden unirse por un camino en  $G$ : hablando con precisión, esto significa que existe un camino  $v_1, v_2, \dots, v_k$  en  $G$  tal que  $x = v_1$  e  $y = v_k$ . Es sencillo comprobar que  $\sim$  es una relación de equivalencia en el conjunto de vértices  $V$  de  $G$ , con lo que  $V$  queda dividido en clases de equivalencia disjuntas. Dos vértices están en la misma clase si pueden unirse por un camino y en clases distintas en caso contrario.

**Definición.** Sea  $G = (V, E)$  un grafo y

$$V = V_1 \cup V_2 \cup \dots \cup V_r$$

la partición de  $V$  correspondiente a la relación de equivalencia  $\sim$ . Sea  $E_i$  ( $1 \leq i \leq r$ ) el subconjunto de  $E$  formado por las aristas cuyos extremos están ambos en  $V_i$ . Los grafos  $G_i = (V_i, E_i)$  se conocen como los **componentes** de  $G$ . Se dice que  $G$  es **conexo** si tiene un único componente.

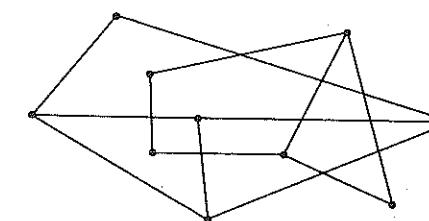


Fig. 8.6 Un grafo con dos componentes.

La terminología práctica se explica por sí misma. El grafo de la figura 8.6 tiene dos componentes y, por lo tanto, no es conexo. La descomposición de un grafo en sus componentes es muy útil, ya que

varias propiedades de los grafos pueden demostrarse considerando cada componente por separado. Por este motivo, los teoremas sobre grafos acostumbran a demostrarse únicamente para la clase de grafos conexos.

Es fácil ver si un grafo relativamente pequeño es conexo a partir de su representación pictórica. Sin embargo, si el grafo viene dado por una lista de adyacencias, necesitaremos un algoritmo eficiente para decidir si es conexo. Estudiaremos este problema en el siguiente capítulo.

Un **ciclo** es un recorrido  $v_1, v_2, \dots, v_{r+1}$  cuyos vértices son todos distintos salvo  $v_1 = v_{r+1}$ . Tiene  $r$  vértices distintos y  $r$  aristas; también se dice que es un  **$r$ -ciclo** o un ciclo de **longitud  $r$** .

**Ejemplo.** Dos catedráticos del Departamento de Matemáticas de la Universidad de Folornia tienen pensado ir de vacaciones a la isla de Wanda.

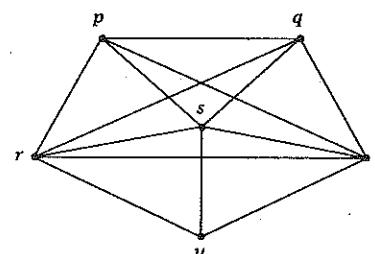


Fig. 8.7 El gran viaje.

La figura 8.7 representa los lugares interesantes de la isla y las carreteras que los unen. La Dra. Elsie Chunner es una turista nata y quisiera visitar cada lugar una sola vez y volver al punto de partida. El Dr. Bob Dodder es un explorador nato y prefiere atravesar cada carretera una vez en cualquier dirección; no le importa empezar y acabar en lugares distintos. ¿Pueden hallarse rutas convenientes para los doctores Chunner y Dodder?

**SOLUCIÓN:** La Dra. C puede escoger varias rutas: una posibilidad es el ciclo  $p, q, t, s, u, r, p$ .

Sin embargo, El Dr. D tiene un problema. Sea  $x$  el vértice de partida e  $y$  el de llegada, y supongamos por el momento que  $x \neq y$ . Al empezar utiliza una arista incidente en  $x$  y cada vez que pasa por  $x$  ha de llegar y volver por aristas nuevas. Por lo tanto, utiliza un número impar de aristas en  $x$ ,

con lo que  $x$  ha de ser un vértice impar. Igualmente,  $y$  ha de ser impar. Los restantes vértices han de ser pares, ya que cada vez que llega a un vértice intermedio ha de abandonarlo, usando de esta forma dos aristas.

Resumiendo, una ruta para el Dr. D que comience y acabe en vértices distintos  $x$  e  $y$  sólo es posible si ambos son impares y el resto son pares. Pero en el grafo en cuestión los grados son

$$\begin{aligned}v &: p \ q \ r \ s \ t \ u \\ \delta(v) &: 4 \ 4 \ 5 \ 5 \ 5 \ 3.\end{aligned}$$

Hay demasiados vértices impares y, en consecuencia, no existe ninguna ruta para el Dr. D. Si analizamos el caso en que  $x = y$  la situación es aún peor, ya que en este caso todos los vértices tendrían que ser pares.  $\square$

En general, la ruta de la Dra. C es un ciclo que contiene todos los vértices del grafo. Estos ciclos fueron estudiados por el matemático irlandés W.R. Hamilton (1805-1865); un ciclo con esta propiedad se conoce como un **ciclo hamiltoniano**. En nuestro ejemplo ha sido muy fácil hallar un ciclo hamiltoniano, pero esto no es absoluto frecuente. Para un grafo dado, decidir si existe o no un ciclo hamiltoniano puede ser un problema difícil.

Por otra parte, el problema del Dr. D se resuelve sin dificultad. Un recorrido que utilice cada arista de un grafo una sola vez se llama un **recorrido euleriano**, debido a que Euler fue el primero en estudiarlos. Encontró que si  $x \neq y$ , una condición para que un camino euleriano empiece en  $x$  y acabe en  $y$  es que  $x$  e  $y$  sean vértices impares y el resto pares, mientras que si  $x = y$  la condición es que todos los vértices sean pares. En consecuencia, una condición necesaria para la existencia de un recorrido euleriano en un grafo  $G$  es que  $G$  tenga como máximo dos vértices impares. Puede demostrarse que esta condición es también suficiente. Dado que calcular los grados de los vértices de un grafo es sencillo, el problema de decidir si un grafo dado tiene un recorrido euleriano es igualmente sencillo.

#### Ejercicios 8.4

- Hallar el número de componentes del grafo que tiene por lista de

adyacencias

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>f</i>	<i>c</i>	<i>b</i>	<i>h</i>	<i>c</i>	<i>a</i>	<i>b</i>	<i>d</i>	<i>a</i>	<i>a</i>
<i>i</i>	<i>g</i>	<i>e</i>		<i>g</i>	<i>i</i>	<i>c</i>		<i>f</i>	<i>f</i>
<i>j</i>		<i>g</i>		<i>j</i>	<i>e</i>				

2 ¿Cuántos componentes tiene el grafo de la fiesta de April (apartado 8.1)?

3 Hallar un ciclo hamiltoniano en el grafo formado por los vértices y las aristas de un cubo.

4 La Dra. Chunner y el Dr. Dodder tienen la intención de visitar el año próximo la isla de Meanda, en la que los lugares interesantes y las carreteras que los unen están representados por el grafo que tiene por lista de adyacencias

0	1	2	3	4	5	6	7	8
1	0	1	0	3	0	1	0	1
3	2	3	2	5	4	5	2	3
5	6	7	4		6	7	6	5
7	8		8	8		8	7	

¿Es posible hallar rutas para los dos que satisfagan los requisitos expuestos en el ejemplo?

5 Un ratón quiere comerse un cubo  $3 \times 3 \times 3$  de queso. Siendo de naturaleza metódica, empieza por morder una esquina y comerse un cubo  $1 \times 1 \times 1$  completo antes de proseguir con otro adyacente. ¿Puede el ratón terminar en el centro?

## 8.5 Árboles

**Definición.** Decimos que un grafo  $T$  es un *árbol* si tiene las dos propiedades siguientes:

- (T1)  $T$  es conexo;
- (T2) no existen ciclos en  $T$ .

Algunos ejemplos típicos de árboles se muestran en la figura 8.8. Debido a su estructura especial y a sus propiedades, los árboles ocurren en numerosas aplicaciones de las matemáticas, especialmente en la investigación operativa y en la informática. Empezaremos su estudio estableciendo algunas propiedades sencillas.

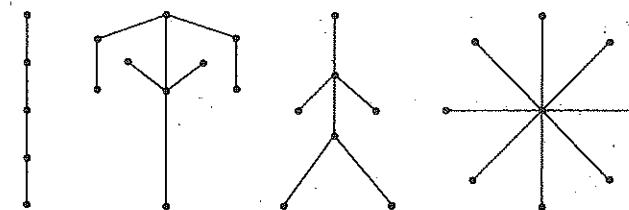


Fig. 8.8 Algunos árboles.

**Teorema 8.5.** Si  $T = (V, E)$  es un árbol con al menos dos vértices, entonces:

- (T3) para cada par de vértices  $x$  e  $y$ , existe un único camino de  $x$  a  $y$  en  $T$ ;
- (T4) el grafo que se obtiene de  $T$  al eliminar cualquier arista tiene dos componentes, cada uno de los cuales es un árbol;
- (T5)  $|E| = |V| - 1$ .

**DEMOSTRACIÓN:** (T3) Al ser  $T$  conexo, existe un camino de  $x$  a  $y$ , pongamos

$$x = v_0, v_1, \dots, v_r = y.$$

Si existiera otro camino distinto, digamos

$$x = u_0, u_1, \dots, u_s = y,$$

sea entonces  $i$  el menor índice para el cual  $u_{i+1} \neq v_{i+1}$  (figura 8.9).

Dado que ambos caminos acaban en  $y$ , han de encontrarse de nuevo y podemos definir  $j$  como el mínimo índice tal que

$$j > i \text{ y } v_j = u_k \text{ para algún } k.$$

Entonces  $v_i, v_{i+1}, \dots, v_j, u_{k-1}, u_{k-2}, \dots, u_{i+1}, v_i$  es un ciclo en  $T$ , contrariamente a la hipótesis.

(T4) Sea  $uv$  una arista de  $T$  y sea  $S = (V, E')$  el grafo que tiene los mismos vértices que  $T$  y aristas  $E' = E \setminus uv$ . Sea  $V_1$  el conjunto de vértices  $x$  de  $T$  para los cuales el único camino de  $x$  a  $v$  pasa por  $u$ ; es evidente que dicho camino ha de acabar en la arista  $uv$ , ya que de lo contrario  $T$  tendría un ciclo. Sea  $V_2$  el complementario de  $V_1$  en  $V$ .

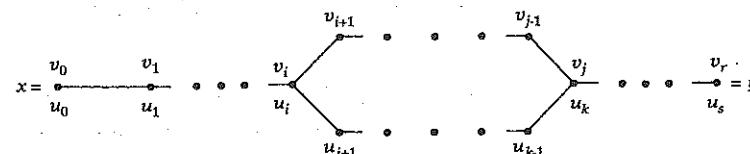


Fig. 8.9 Dos caminos distintos determinan un ciclo.

Cada vértice de  $V_1$  está unido a  $u$  por un camino en  $S$ , y cada vértice de  $V_2$  lo está a  $v$  también en  $S$ , pero en  $S$  no hay ningún camino de  $u$  a  $v$ . Resulta que  $V_1$  y  $V_2$  son los conjuntos de vértices de los dos componentes de  $S$ . Cada componente es conexo (por definición) y no contiene ciclos, ya que  $T$  no los contiene. Así pues, los dos componentes son árboles.

(T5) El resultado es cierto si  $|V| = 1$ , ya que el único árbol posible en este caso no tiene aristas. Supongámoslo cierto para todos los árboles con  $k$  o menos vértices. Sea  $T$  un árbol con  $|V| = k + 1$  y sea  $uv$  una arista de  $T$ . Si  $T_1 = (V_1, E_1)$  y  $T_2 = (V_2, E_2)$  son los árboles que se obtienen al eliminar  $uv$  de  $T$ , tenemos

$$|V_1| + |V_2| = |V|, \quad |E_1| + |E_2| = |E| - 1.$$

Aplicando la hipótesis de inducción a  $T_1$  y  $T_2$  tenemos

$$|E| = |E_1| + |E_2| + 1 = |V_1| - 1 + |V_2| - 1 + 1 = |V| - 1,$$

y el resultado es cierto para todo entero positivo  $k$ .  $\square$

Las propiedades (T1)–(T5) proporcionan varias formas alternativas de definir un árbol. Por ejemplo, la propiedad (T3) por sí sola puede tomarse como definición en lugar de (T1) y (T2). Ya hemos demostrado que (T3)

es consecuencia de (T1) y (T2), de modo que sólo queda demostrar el recíproco (ejercicio 8.5.3).

### Ejercicios 8.5

- 1 Existen seis árboles distintos (es decir, mutuamente no isomorfos) con seis vértices: dibujarlos.
- 2 Sea  $T = (V, E)$  un árbol con  $|V| \geq 2$ . Utilizando la propiedad (T5) y el teorema 8.3, demostrar que  $T$  tiene al menos dos vértices con grado 1.
- 3 Demostrar que la propiedad (T3) implica (T1) y (T2).
- 4 Un bosque es un grafo que satisface (T2) pero no necesariamente (T1). Demostrar que si  $F = (V, E)$  es un bosque con  $c$  componentes, entonces

$$|E| = |V| - c.$$

### 8.6 Colorear los vértices de un grafo

Un problema que aparece con frecuencia en la vida moderna es el de programar una serie de actos de manera que no entren en conflicto. Vamos a considerar un ejemplo muy sencillo de cómo la teoría de grafos puede ayudarnos a estudiar este problema.

Supongamos que hemos de programar seis conferencias de una hora  $v_1, v_2, v_3, v_4, v_5, v_6$ . Entre la posible audiencia hay quienes quieren escuchar  $v_1$  y  $v_2$ ,  $v_1$  y  $v_4$ ,  $v_3$  y  $v_5$ ,  $v_2$  y  $v_6$ ,  $v_4$  y  $v_5$ ,  $v_5$  y  $v_6$ , y  $v_1$  y  $v_6$ . ¿Cuántas horas son necesarias para poder dar las conferencias sin solaparse?

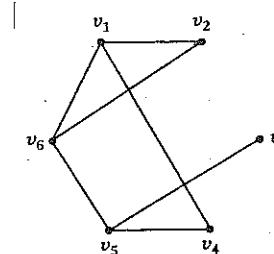


Fig. 8.10 El grafo de un problema de horarios.

Podemos representar la situación por un grafo (figura 8.10). Los vértices corresponden a las seis conferencias y las aristas a los posibles conflictos. Un horario que consigue el objetivo de no solaparse es el siguiente:

Hora 1	Hora 2	Hora 3	Hora 4
$v_1$ y $v_3$	$v_2$ y $v_4$	$v_5$	$v_6$

En términos matemáticos, tenemos una partición del conjunto de vértices en cuatro partes con la propiedad de que ninguna parte contiene un par de vértices adyacentes. Una descripción más gráfica se obtiene utilizando la función

$$c : \{v_1, v_2, v_3, v_4, v_5, v_6\} \rightarrow \{1, 2, 3, 4\}$$

que asigna a cada vértice (conferencia) la hora a que ha sido programada. En lugar de horas, se acostumbra a hablar de colores asignados a los vértices, pero es evidente que la naturaleza de los objetos 1, 2, 3 y 4 no es importante. Podemos usar nombres de colores como rojo, verde, azul y amarillo, o podemos hablar del color 1, color 2, etc. La cuestión importante es que vértices adyacentes del grafo deben tener colores diferentes.

**Definición.** Una **vértice-coloración** de un grafo  $G = (V, E)$  es una función  $c : V \rightarrow \mathbb{N}$  con la propiedad de que

$$c(x) \neq c(y) \text{ siempre que } \{x, y\} \in E.$$

El **número cromático** de  $G$ , que denotamos por  $\chi(G)$ , se define como el menor entero  $k$  tal que existe una vértice-coloración de  $G$  que usa  $k$  colores. En otras palabras,  $\chi(G) = k$  si, y sólo si, existe una función de coloración  $c$  de  $V$  en  $\mathbb{N}_k$  y  $k$  es el menor entero con esta propiedad.

Volviendo al ejemplo de la figura 8.10, podemos ver que nuestro primer intento de diseñar un horario es equivalente a una vértice-coloración con cuatro colores. El número mínimo de horas necesarias es el número cromático del grafo; nos preguntamos a continuación si este número es menor que 4. Un rápido intento con tres colores proporciona una solución:

Color 1	Color 2	Color 3
$v_1$	$v_2$ y $v_5$	$v_3, v_4$ y $v_6$

Más aún, son necesarios tres colores, ya que  $v_1, v_2$  y  $v_6$  son mutuamente adyacentes y deben tener colores distintos. Concluimos que el número cromático de este grafo es 3.

En general, para demostrar que el número cromático de un grafo es  $k$ , son necesarias dos cosas:

- (i) hallar una vértice-coloración con  $k$  colores;
- (ii) demostrar que ninguna coloración utiliza menos de  $k$  colores.

### Ejercicios 8.6

1 Hallar el número cromático de los siguientes grafos:

- (i) un grafo completo  $K_n$ ;
- (ii) un ciclo  $C_{2r}$  con un número par de vértices;
- (iii) un ciclo  $C_{2r+1}$  con un número impar de vértices.

2 Determinar el número cromático de los grafos que muestra la figura 8.11.

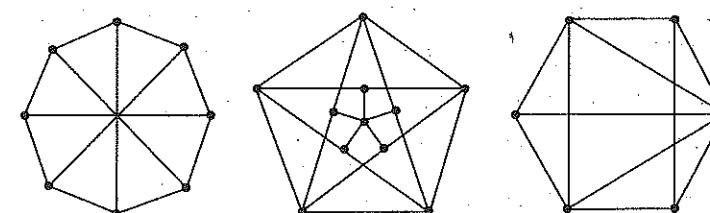


Fig. 8.11 Hallar el número cromático.

3 Describir todos los grafos  $G$  para los cuales  $\chi(G) = 1$ .

### 8.7 El algoritmo voraz para las vértice-coloraciones

Hallar el número cromático de un grafo es un problema difícil. En efecto, no se conoce ningún algoritmo que lo resuelva en "tiempo polinómico" y muchos creen que tal algoritmo no existe. Sin embargo, existe un método sencillo para construir una coloración que utiliza una cantidad "razonable" de colores.

El método consiste en asignar colores a los vértices ordenadamente, de forma que cada vértice reciba el primer color que no haya sido asignado

a ninguno de sus vecinos. En cada paso se toma la mejor opción, sin preocuparse de si esa opción creará complicaciones más adelante. Un algoritmo de este tipo se conoce como un **algoritmo voraz**.

El algoritmo voraz para colorear es fácil de programar. Se disponen los vértices en un cierto orden  $v_1, v_2, \dots, v_n$ . Se asigna el color 1 a  $v_1$ ; para cada  $v_i$  ( $2 \leq i \leq n$ ) formamos el conjunto  $S$  de los colores asignados a los vértices  $v_j$  ( $1 \leq j < i$ ) que son adyacentes a  $v_i$  y asignamos a  $v_i$  el primer color que no está en  $S$  (en la práctica pueden usarse métodos más sofisticados para gestionar los datos).

#### El algoritmo voraz para colorear vértices

```

asignar el color 1 a  $v_1$ ;
para  $i:=2$  hasta  $n$  hacer
    inicio
        sea  $S$  el conjunto de colores vacío;
        para  $j:=1$  hasta  $i-1$  hacer
            si  $v_j$  es adyacente a  $v_i$ 
                entonces añadir a  $S$  el color  $v_j$ ;
         $k:=1$ ;
        mientras el color  $k$  esté en  $S$  hacer  $k:=k+1$ ;
        asignar el color  $k$  a  $v_i$ 
    fin

```

Dado que la estrategia voraz es corta de vista, el número de colores que utiliza será normalmente mayor que el mínimo posible. Por ejemplo, el algoritmo voraz aplicado al grafo de la figura 8.10 proporciona precisamente la coloración con cuatro colores que se propuso inicialmente como "horario", mientras que más tarde hallamos una coloración con tres colores. Desde luego, todo depende del orden inicial en que se disponen los vértices. Es fácil ver que si acertamos con el orden correcto, el algoritmo voraz nos da una coloración óptima (ejercicio 8.7.2). Pero hay  $n!$  órdenes en total, y si tuviéramos que probarlos todos, el algoritmo necesitaría un "tiempo exponencial".

A pesar de no ser óptimo, el algoritmo voraz es útil tanto en la teoría como en la práctica. Demostraremos dos teoremas utilizando la estrategia voraz.

**Teorema 8.7.1.** Si  $G$  es un grafo con grado máximo  $k$ , entonces

- (i)  $\chi(G) \leq k + 1$ ,
- (ii) si  $G$  es conexo y no regular,  $\chi(G) \leq k$ .

**DEMOSTRACIÓN:** (i) Sea  $v_1, v_2, \dots, v_n$  una ordenación de los vértices de  $G$ . Cada vértice  $v_i$  tiene como máximo  $k$  vecinos, de forma que el conjunto  $S$  de colores que el algoritmo voraz asigna a los vértices  $v_j$  adyacentes a  $v_i$  ( $1 \leq j < i$ ) tiene como máximo  $k$  elementos. Por lo tanto, al menos uno de los colores  $1, 2, \dots, k+1$  no está en  $S$  y el algoritmo voraz asignará el primero de ellos a  $v_i$ . De esta forma, el algoritmo voraz proporciona una coloración de  $G$  que utiliza  $k+1$  colores como máximo, con lo que  $\chi(G) \leq k+1$ .

(ii) En esta ocasión disponemos los vértices en un orden especial. Como  $G$  tiene grado máximo  $k$  y no es regular, existe al menos un vértice de  $G$  cuyo grado es menor que  $k$ , llamémosle  $v_n$ . Sea  $v_{n-1}, v_{n-2}, \dots, v_1$  una lista con los vecinos de  $v_n$ ; hay  $k-1$  como máximo. A continuación formamos la lista con los vecinos de  $v_{n-1}$  (salvo  $v_n$ ), y hacemos notar que, como el grado de  $v_{n-1}$  es a lo sumo  $k$ , hay  $k-1$  de ellos como máximo. Seguimos con la lista de los vecinos de  $v_{n-2}$  que todavía no han aparecido, y así sucesivamente. Al ser  $G$  conexo, la lista contendrá eventualmente todos los vértices. El método de construcción asegura que, en el orden  $v_1, v_2, \dots, v_n$ , cada vértice es adyacente a  $k-1$  de sus predecesores como máximo.

El mismo argumento que en la parte (i) demuestra que el algoritmo voraz tiene bastante con  $k$  colores (para este orden particular). Así pues,  $\chi(G) \leq k$ .  $\square$

La parte (ii) del teorema no tiene por qué ser cierta si  $G$  es regular. El lector que haya resuelto correctamente el ejercicio 8.6.1 será capaz de mostrar dos ejemplos de este hecho: los grafos completos y los ciclos impares, que requieren  $k+1$  colores cada uno. Sin embargo, puede demostrarse que estos son los únicos contraejemplos.

Otra consecuencia útil del algoritmo voraz se refiere a los grafos  $G$  con  $\chi(G) = 2$ . Para uno de estos grafos, los conjuntos  $V_1$  y  $V_2$  de vértices que tienen asignado el color 1 y 2, respectivamente, forman una partición del conjunto de  $V$  con la propiedad de que cada arista de  $G$  tiene un vértice en  $V_1$  y otro en  $V_2$ . Por este motivo, si  $\chi(G) = 2$  se dice que  $G$  es **bipartido**.

La figura 8.12 ilustra una coloración del cubo con dos colores junto con una representación alternativa que acentúa el carácter bipartido del grafo. Este tipo de representación es frecuente al tratar con grafos bipartidos.

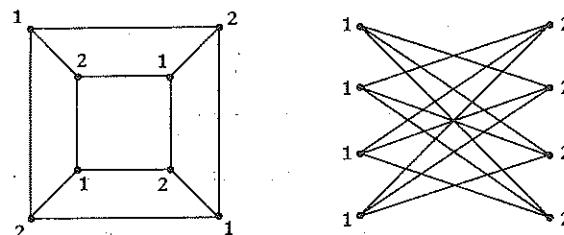


Fig. 8.12 El cubo como un grafo bipartido.

**Teorema 8.7.2.** Un grafo es bipartido si, y sólo si, no contiene ciclos de longitud impar.

**DEMOSTRACIÓN:** Si existe un ciclo con un número impar de vértices, entonces se necesitan tres colores para colorear el ciclo y el número cromático del grafo es al menos 3. Así pues, si el grafo es bipartido no puede tener ciclos impares.

Recíprocamente, supongamos que  $G$  no tiene ciclos impares. Construiremos una ordenación de  $G$  en la que el algoritmo voraz sólo requiera dos colores. Elijamos un vértice cualquiera y llamémoslo  $v_1$ ; decimos que  $v_1$  está en el *nivel 0*. A continuación, sean  $v_2, v_3, \dots, v_r$  los vecinos de  $v_1$ ; decimos que estos vértices están en el nivel 1. En el nivel 2 están los vecinos de los vértices del nivel 1 (salvo  $v_1$ ) y, prosiguiendo de esta forma, en el nivel  $l$  están aquellos que son vecinos de los vértices en el nivel  $l-1$  que no estuvieran ya en el nivel  $l-2$ . Cuando no podamos añadir nuevos vértices de esta forma, tenemos un componente  $G_0$  de  $G$  (si  $G$  es conexo,  $G_0 = G$ ).

La propiedad crucial de esta ordenación es que un vértice en el nivel  $l$  puede ser adyacente únicamente a vértices de los niveles  $l-1$  y  $l+1$ , y no a vértices del mismo nivel. Ya que si  $x$  e  $y$  son vértices en el mismo nivel, pueden unirse por caminos de igual longitud  $m$  a algún vértice  $z$  de un nivel previo, y los caminos pueden elegirse de manera que  $z$  sea el único

vértice común (figura 8.13). Si  $x$  e  $y$  fueran adyacentes, existiría un ciclo de longitud impar  $2m+1$  en  $G_0$ , contrariamente a la hipótesis.

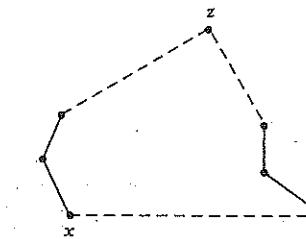


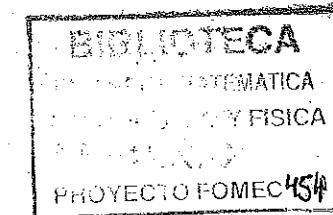
Fig. 8.13 Vértices adyacentes del mismo nivel dan lugar a un ciclo impar.

El algoritmo voraz asignará el color 1 a los vértices de los niveles  $0, 2, 4, \dots$  y el color 2 a los de los niveles  $1, 3, 5, \dots$  Así pues,  $\chi(G_0) = 2$ . Repitiendo el mismo procedimiento para cada componente de  $G$  se obtiene el resultado.  $\square$

### Ejercicios 8.7

- 1 Hallar ordenaciones de los vértices del cubo (figura 8.12) para las que el algoritmo voraz requiera 2, 3 y 4 colores respectivamente.
- 2 Demostrar que para cualquier grafo  $G$  existe una ordenación de los vértices para la que el algoritmo voraz requiere  $\chi(G)$  colores. [Indicación: usar una coloración de  $G$  con  $\chi(G)$  colores para definir la ordenación buscada.]
- 3 Sea  $e_i(G)$  el número de vértices de un grafo cuyo grado es estrictamente mayor que  $i$ . Utilizar el algoritmo voraz para demostrar que si  $e_i(G) \leq i+1$  para algún  $i$ , entonces  $\chi(G) \leq i+1$ .
- 4 El grafo  $M_r$  ( $r \geq 2$ ) se obtiene a partir del ciclo  $C_{2r}$  añadiendo aristas extra que unan cada par de vértices opuestos. Demostrar que

- (i)  $M_r$  es bipartido si  $r$  es impar,
- (ii)  $\chi(M_r) = 3$  si  $r$  es par y  $r \neq 2$ ,
- (iii)  $\chi(M_2) = 4$ .



## 8.8 Ejercicios diversos

1 ¿Para qué valores de  $n$  es cierto que el grafo completo  $K_n$  posee un recorrido euleriano?

2 Utilizar el principio de inducción para demostrar que si  $G = (V, E)$  es un grafo con  $|V| = 2m$  y  $G$  no tiene 3-ciclos, entonces  $|E| \leq m^2$ .

3 Sea  $X = \{1, 2, 3, 4, 5\}$  y sea  $V$  el conjunto de todos los 2-subconjuntos de  $X$ . Sea  $E$  el conjunto de pares de elementos de  $V$  que son disjuntos (como subconjuntos de  $X$ ). Demostrar que el grafo  $G = (V, E)$  es isomorfo al grafo que muestra la figura 8.14. Demostrar también que no es más que otra versión del grafo de Petersen introducido en el ejercicio 8.2.2.

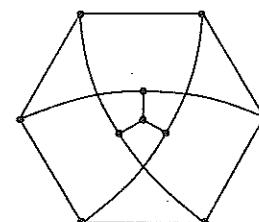


Fig. 8.14 El grafo de Petersen.

4 Sea  $G$  un grafo bipartido con un número impar de vértices. Demostrar que  $G$  no tiene ningún ciclo hamiltoniano.

5 El  $k$ -cubo  $Q_k$  es el grafo que tiene por vértices las palabras de longitud  $k$  en el alfabeto  $\{0, 1\}$  y cuyas aristas unen las palabras que difieren en una posición exactamente. Demostrar que

- (i)  $Q_k$  es un grafo regular de grado  $k$ ,
- (ii)  $Q_k$  es bipartido.

6 Demostrar que el grafo  $Q_k$  definido en el ejercicio 8.8.5 posee un ciclo hamiltoniano.

7 Demostrar que el grafo de Petersen no tiene ningún ciclo hamiltoniano.

8 En el juego del dominó (ejercicio 3.7.2), las fichas han de colocarse de manera que los números de fichas adyacentes sean iguales:  $[x|y]$  junto a  $[y|z]$ , etc. Considerando las fichas para las cuales  $x \neq y$  como las aristas del grafo completo  $K_7$ , demostrar que es posible colocar todas las fichas en una partida.

9 Calcular el número de recorridos eulerianos en  $K_7$  y el número de partidas completas de dominó.

10 Demostrar que si  $\alpha : V_1 \rightarrow V_2$  es un isomorfismo entre los grafos  $G_1 = (V_1, E_1)$  y  $G_2 = (V_2, E_2)$ , entonces la función  $\beta : E_1 \rightarrow E_2$  definida por

$$\beta\{x, y\} = \{\alpha(x), \alpha(y)\} \quad \text{para } \{x, y\} \in E_1$$

es una biyección.

11 Si  $G$  es un grafo  $k$ -regular con  $n$  vértices, demostrar que

$$\chi(G) \geq \frac{n}{n-k}.$$

12 Construir cinco grafos conexos regulares de grado 3 y ocho vértices mutuamente no isomorfos.

13 Demostrar que el grafo completo  $K_{2n+1}$  es la unión de  $n$  ciclos hamiltonianos, ninguno de los cuales tiene una arista en común.

14 ¿Puede un caballo visitar todas las casillas de un tablero de ajedrez exactamente una vez y regresar al punto de partida? Interpretar la respuesta en términos de ciclos hamiltonianos en un cierto grafo.

15 El grafo impar  $O_k$  se define como sigue (para  $k \geq 2$ ): los vértices son los  $(k-1)$ -subconjuntos de un  $(2k-1)$ -conjunto y las aristas unen subconjuntos disjuntos (por ejemplo,  $O_3$  es el grafo de Petersen). Demostrar que  $\chi(O_k) = 3$  para  $k \geq 2$ .

16 Demostrar que si  $G$  es un grafo con  $n$  vértices,  $m$  aristas y  $c$  componentes, entonces

$$n - c \leq m \leq \frac{1}{2}(n - c)(n - c + 1).$$

Construir ejemplos que demuestren que esta cota puede alcanzarse para todos los valores de  $n$  y  $c$  tales que  $n \geq c$ .

17 Una sucesión  $d_1, d_2, \dots, d_n$  es gráfica si existe un grafo con  $n$  vértices cuyos grados sean precisamente los  $d_i$ . Demostrar que si la sucesión  $d_1, d_2, \dots, d_n$  es gráfica y  $d_1 \geq d_2 \geq \dots \geq d_n$ , entonces

$$d_1 + d_2 + \dots + d_k \leq k(k-1) + \sum_{i=k+1}^n \min(k, d_i)$$

para  $1 \leq k \leq n$ .

18 La cintura de un grafo  $G$  es el mínimo valor  $g$  para el que  $G$  contiene un  $g$ -ciclo. Demostrar que un grafo regular de grado  $k$  y cintura  $2m+1$  ha de tener al menos

$$1 + k + k(k-1) + \dots + k(k-1)^{m-1}$$

vértices, y que un grafo regular de grado  $k$  y cintura  $2m$  ha de tener al menos

$$2[1 + (k - 1) + (k - 1)^2 + \dots + (k - 1)^{m-1}]$$

vértices.

19 Formar una tabla con las cotas inferiores que se obtienen en el ejercicio anterior cuando  $k = 3$  y la circunferencia es 3, 4, 5, 6 y 7. Demostrar que existe un grafo que alcanza la cota inferior en los cuatro primeros casos, pero no en el quinto.

20 Sea  $B$  el conjunto de los bloques de un 2-diseño en un conjunto  $X$  con parámetros  $(r^2 + r + 1, r + 1, 1)$ , y sea  $G$  el grafo que tiene por conjunto de vértices  $X \cup B$  y cuyas aristas unen los vértices  $x$  y  $B$  si el objeto  $x$  está en el bloque  $B$ . Demostrar que  $G$  es un grafo regular de circunferencia 6 que alcanza la cota inferior del ejercicio 18.

21 Sea  $G = (V, E)$  un grafo con al menos tres vértices y tal que

$$\delta(v) \geq \frac{1}{2}|V| \quad (v \in V).$$

Demostrar que  $G$  posee un ciclo hamiltoniano.

22 Demostrar que si  $\bar{G}$  es el complementario de un grafo  $G$  (tal como se definió en el ejercicio 8.3.2), entonces  $\chi(G)\chi(\bar{G}) \geq n$ , donde  $n$  es el número de vértices de  $G$ .

## 9 Árboles, ordenaciones y búsqueda

### 9.1 Contar las hojas de un árbol con raíz

Recuérdese que un *árbol* es un grafo conexo que no contiene ciclos. Los árboles aparecen en diversos contextos y con frecuencia uno de los vértices de un árbol queda señalado de alguna manera especial. Por ejemplo, en un “árbol genealógico” con todos los descendientes del rey Enrique VIII, podríamos acentuar la condición especial del Rey situándolo a la “cabeza” del árbol. En general, nos referiremos al vértice distinguido como la *raíz* y un árbol con una raíz señalada será un *árbol con raíz*. (Esta terminología, a pesar de ser estándar, tiene el defecto de que en una representación pictórica la raíz se suele colocar en la cima del árbol, de forma que el árbol parece crecer hacia abajo.)

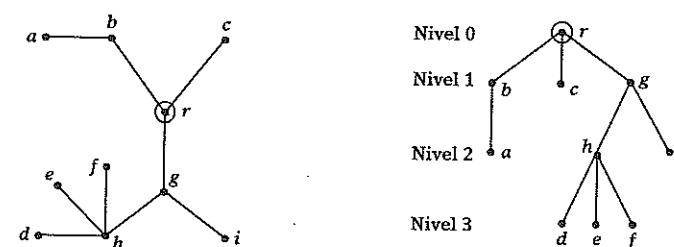


Fig. 9.1 Un árbol con raíz y sus niveles.

Para estudiar los árboles con raíz, es natural disponer los vértices por niveles, tal como hicimos con los grafos bipartidos en el apartado 8.7. Decimos que el vértice raíz  $r$  está en el *nivel 0* y que los vecinos de  $r$  están

en el *nivel 1*. Para cada  $k \geq 2$ , el *nivel k* contiene los vértices adyacentes a los vértices del nivel  $k - 1$ , salvo los que ya han sido asignados al nivel  $k - 2$ . El árbol con raíz que se muestra a la izquierda de la figura 9.1 puede redibujarse para hacer visible la posición de los vértices en los distintos niveles.

Un vértice de un árbol con raíz es una **hoja** si está en el nivel  $i$  y no es adyacente a ningún vértice del nivel  $i + 1$ . Un vértice que no es una hoja es un vértice **interno**. La **altura** de un árbol con raíz es el máximo valor de  $k$  para el cual el nivel  $k$  no es vacío. Por ejemplo, el árbol de la figura 9.1 tiene seis hojas, cuatro vértices internos y su altura es 3.

### Ejercicios 9.1

1 En la tabla siguiente,  $n_5(h)$  es el número de árboles *con raíz* no isomorfos con cinco vértices y altura  $h$ . (Se dice que dos árboles con raíz son isomorfos si existe un isomorfismo entre ellos —considerados como árboles sin raíz— que transforma la raíz del primero en la del segundo.) Comprobar los valores de la tabla dibujando el número de ejemplos necesarios en cada caso.

$h:$	1	2	3	4
$n_5(h):$	1	4	3	1

2 ¿Cuántos árboles (sin raíz) no isomorfos existen con cinco vértices? Dar una lista de las clases de isomorfismo y comprobar a partir de ella que la lista obtenida en el ejercicio anterior es completa.

3 Construir dos árboles con raíz no isomorfos con 12 vértices, 6 hojas y altura 4.

Las propiedades que utilizamos en el apartado 8.5 para definir un árbol tienen consecuencias evidentes al disponer los vértices en niveles. Como un árbol es un grafo conexo (propiedad T2), cada vértice  $v$  en el nivel  $i$  ( $i > 0$ ) es adyacente a exactamente un vértice  $u$  en el nivel  $i - 1$ . A veces se indica esta situación refiriéndonos a  $u$  como el “padre” de  $v$  y a  $v$  como el hijo de  $u$ . Cada vértice, salvo la raíz, tiene un único parente, pero un vértice

puede tener cualquier número de hijos (incluso cero). Naturalmente, un vértice es una hoja si, y sólo si, no tiene hijos.

En las aplicaciones suele ocurrir que cada parente (vértice interno) tenga el mismo número de hijos. Si cada parente tiene  $m$  hijos, tenemos un árbol con raíz  **$m$ -ario**; en particular, si  $m = 2$  utilizamos la palabra “binario” y si  $m = 3$ , la palabra “ternario”.

**Teorema 9.1.** *La altura de un árbol con raíz  $m$ -ario con  $l$  hojas es al menos  $\log_m l$ .*

**DEMOSTRACIÓN:** Dado que

$$h \geq \log_m l \iff m^h \geq l,$$

es suficiente demostrar la afirmación equivalente de que un árbol con raíz  $m$ -ario de altura  $h$  posee como máximo  $m^h$  hojas. La demostración es por inducción sobre  $h$ .

La afirmación es desde luego cierta para  $h = 0$ , ya que en este caso el árbol tiene sólo un vértice, la raíz, que es una hoja. Supongámosla cierta para  $0 \leq h \leq h_0$  y sea  $T$  un árbol con raíz  $m$ -ario de altura  $h_0 + 1$ . Si suprimimos de  $T$  la raíz y las aristas que la contienen, obtenemos  $m$  árboles  $T_1, \dots, T_m$ ; señalamos sus raíces como los vértices de  $T$  en el nivel 1. Cada  $T_i$  es un árbol con raíz de altura no superior a  $h_0$  y, por la hipótesis de inducción, tiene a lo sumo  $m^{h_0}$  hojas. Pero las hojas de  $T$  son precisamente las hojas de los árboles  $T_1, \dots, T_m$ , con lo que el número de hojas de  $T$  es menor o igual que  $m \times m^{h_0} = m^{h_0+1}$ .

La forma fuerte del principio de inducción asegura que el resultado es cierto para todo  $h \geq 0$ .  $\square$

Dado que  $\log_m l$  no acostumbra a ser un entero mientras que  $h$  sí lo es, podemos mejorar ligeramente el enunciado del teorema 9.1. Por ejemplo, si  $m = 3$  y  $l = 10$ , entonces la desigualdad

$$h \geq \log_m l = 2.0959\dots$$

implica que  $h \geq 3$ . En general, podemos decir que

$$h \geq \lceil \log_m l \rceil,$$

donde  $[x]$  es el menor entero  $z$  tal que  $z \geq x$  (compárese con la notación  $[x]$  introducida en el apartado 7.5).

Una aplicación frecuente del teorema 9.1 es al estudio de los *árboles de decisión*. Cada vértice interno de un árbol de decisión representa una decisión, y los posibles resultados de la decisión se representan por las aristas que conducen al siguiente nivel. El resultado final del proceso está representado por las hojas del árbol. Si el resultado de cada decisión es simplemente que una afirmación es cierta o falsa, entonces tenemos un árbol binario; esta situación, muy frecuente, se discutirá en el próximo apartado. El ejemplo siguiente se refiere a un árbol ternario.

**Ejemplo.** (El problema de la moneda falsa). Supongamos que tenemos una moneda auténtica, con la etiqueta 0, y otras  $r$  monedas, indistinguibles de 0 por su apariencia, salvo en que llevan las etiquetas 1, 2, ...,  $r$ . Se sospecha que una de las monedas puede ser falsa —demasiado ligera o demasiado pesada. Demostrar que se necesitan al menos  $\lceil \log_3(2r + 1) \rceil$  pesadas en una balanza para decidir qué moneda (si es que hay alguna) es falsa y si es más ligera o más pesada. Diseñar un procedimiento que utilice exactamente este número de pesadas en el caso  $r = 4$ .

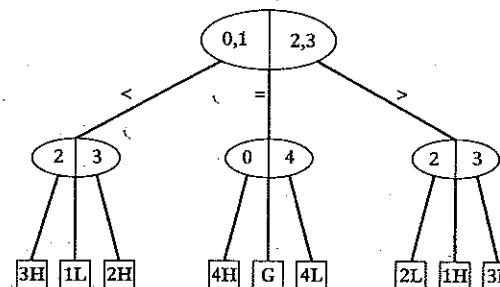


Fig. 9.2 Solución al problema de la moneda falsa cuando  $r = 4$ .

**SOLUCIÓN:** Hay  $2r + 1$  resultados posibles, u hojas en el árbol de decisión,

$$B, 1P, 1L, \dots, rP, rL,$$

que significan que todas las monedas son buenas, la moneda 1 es pesada, la moneda 1 es ligera, etc. El árbol de decisión es ternario, ya que para

cada pesada hay tres resultados posibles (al pesar un montón de monedas contra otro). Son los siguientes:

- < : el izquierdo es menos pesado;
- = : los dos pesan igual
- > : el izquierdo es más pesado.

Así pues, la altura del árbol de decisión es al menos  $\lceil \log_3(2r + 1) \rceil$ .

Si  $r = 4$ , entonces  $\lceil \log_3(2r + 1) \rceil = 2$  y una solución con dos pesadas se muestra en la figura 9.2.

### Ejercicios 9.1 (continuación)

4 En un torneo de fútbol de la Universidad de Folornia participan 20 equipos. El campeonato se organiza por “eliminatorias”, de manera que los ganadores de los partidos de la primera ronda pasan a la segunda ronda y así sucesivamente; los partidos no pueden quedar en empate. Diseñar un esquema del campeonato basado en un árbol con raíz y demostrar que son necesarias al menos cinco rondas. ¿Puede hacerse de forma que todos los que superan una eliminatoria directamente sin enfrentarse lo hagan en la primera ronda?

5 La Copa FA es un campeonato de fútbol por eliminatorias que representamos por un árbol con raíz. ¿Cuántas rondas necesita la competición si participan 4090 equipos y ninguno de ellos pasa directamente más de una ronda? ¿Cuántas rondas se necesitan si 90 equipos pasan directamente hasta la ronda 6?

6 ¿Cuántas pesadas son necesarias en el problema de la moneda falsa (tal como se enuncia en el ejemplo anterior) si hay seis monedas? Diseñar un procedimiento que utilice este número de pesadas.

7 Consideremos la siguiente variante del problema de la moneda falsa. Hay ocho monedas y sabemos que exactamente una es más ligera. Todas las demás son auténticas, pero no disponemos de ninguna moneda auténtica con la etiqueta 0. Dar una cota inferior teórica del número de pesadas necesarias para hallar la moneda ligera y demostrar que este número puede alcanzarse.

## 9.2 Árboles y algoritmos de ordenación

En el apartado 7.8 discutimos el problema de cómo disponer una lista  $x_1, x_2, \dots, x_n$  de enteros distintos en orden creciente. En el algoritmo que usamos para resolver este problema intervenían comparaciones entre números enteros y movimientos de los datos; este proceso puede representarse en forma de un árbol de decisión.

Cada vértice del árbol de decisión representa una comparación de dos enteros, por ejemplo los que en ese momento tienen las etiquetas  $x_i$  y  $x_j$ . Tenemos dos resultados posibles,  $x_i < x_j$  o  $x_i > x_j$ , con lo que el árbol de decisión es *binario*. En el algoritmo de la burbuja, en cada comparación intervienen enteros “adyacentes”  $x_i$  y  $x_{i+1}$ , y las reglas que nos indican qué par hay que comparar en cada paso no dependen del resultado de comparaciones previas (desde luego, los valores actuales de  $x_i$  y  $x_{i+1}$  sí dependen de las comparaciones previas). En la figura 9.3 se ilustra el árbol de decisión del algoritmo de la burbuja para  $n = 3$ . Hay  $3! = 6$  resultados posibles, que corresponden a las permutaciones del orden inicial  $\alpha\beta\gamma$ ; las hojas del árbol de decisión representan estos resultados, junto con algunas situaciones “imposibles”.

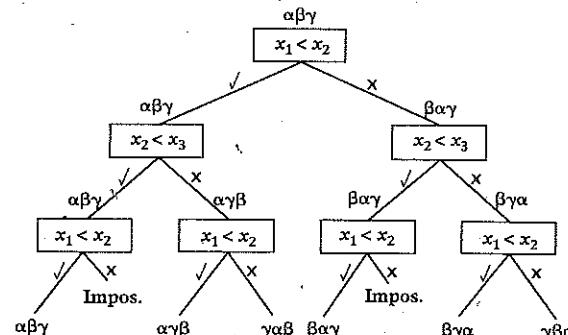


Fig. 9.3 El árbol de decisión del algoritmo de la burbuja (tres objetos).

Para un  $n$  cualquiera, el número de hojas del árbol de decisión es al menos  $n!$ , independientemente del algoritmo que se use. Por su parte, la altura del árbol de decisión es igual al número  $s(n)$  de comparaciones necesarias. Se sigue del teorema 9.1 que

$$s(n) \geq \log_2(n!).$$

Ahora bien,  $\log_2(n!)$  es  $O(n \log n)$ , ya que es la suma de  $n$  términos  $\log i$  ( $1 \leq i \leq n$ ) y ningún término es mayor que  $\log_2 n$ . De hecho, no es posible una aproximación mejor (ejercicio 9.2.5). Así pues, el número de comparaciones necesarias en cualquier algoritmo de ordenación es al menos  $O(n \log n)$ .

En el apartado 7.8 vimos que el algoritmo de la burbuja es  $O(n^2)$ , mientras que el método de bisección requiere  $O(n \log n)$  comparaciones pero  $O(n^2)$  movimientos de datos. Vamos a describir ahora un algoritmo donde el número de comparaciones y el de movimientos de datos son ambos  $O(n \log n)$ . Se conoce como *ordenación de Williams*.

El algoritmo de ordenación de Williams utiliza los árboles con raíz como ingrediente esencial, aunque no deben confundirse con los árboles de decisión que hemos utilizado al analizar un algoritmo de ordenación arbitrario. Empezaremos por asignar los elementos  $x_1, x_2, \dots, x_n$  a los vértices de un árbol con raíz de la siguiente forma (figura 9.4). Asignámos  $x_1$  a la raíz (nivel 0),  $x_2$  y  $x_3$  al nivel 1,  $x_4, x_5, x_6$  y  $x_7$  al nivel 2, etc. El vértice con la etiqueta  $x_r$  es el padre de  $x_{2r}$  y  $x_{2r+1}$ , siempre que  $2r+1 \leq n$ . El último nivel queda en general sin completar y cuando  $n$  es par, el vértice  $x_{n/2}$  tiene sólo  $x_n$  como hijo. Aparte de este hecho, se trata de un árbol binario con raíz, tal como ilustra la figura 9.4 en el caso  $n = 12$ .

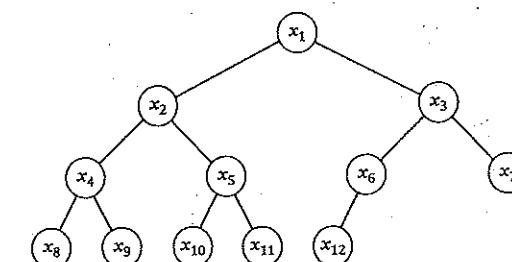


Fig. 9.4 Un árbol etiquetado para la ordenación de Williams.

El algoritmo de Williams tiene dos fases. En la primera se transforma la lista sin ordenar en un tipo especial de lista conocida como montículo (véase figura 9.5); en la segunda se transforma el montículo en una lista ordenada. La propiedad característica de un montículo es que cada padre

es menor que sus hijos; en otras palabras,

$$x_r < x_{2r} \text{ y } x_r < x_{2r+1}.$$

Por ejemplo, la lista sin ordenar

$$77, 23, 82, 47, 65, 17, 97, 85, 35, 91, 61, 73$$

se transforma primero en el montículo

$$17, 23, 73, 35, 61, 77, 97, 85, 47, 91, 65, 82$$

(como muestra la figura 9.5) y a continuación en la lista ordenada

$$17, 23, 35, 47, 61, 65, 73, 77, 82, 85, 91, 97.$$

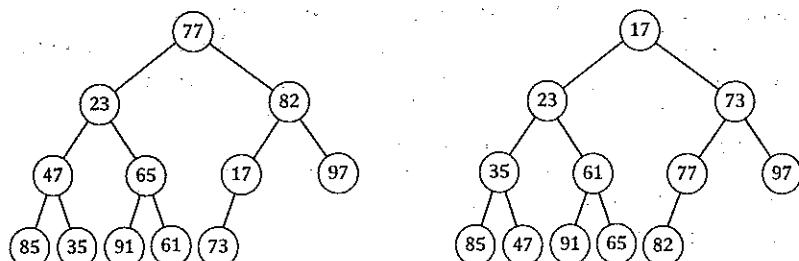


Fig. 9.5 Representación arbórea de una lista sin ordenar y el correspondiente montículo.

El método para transformar una lista en un montículo trata los padres (vértices internos) en orden inverso. Supongamos que al llegar a  $x_r$  los dos subárboles con raíces  $x_{2r}$  y  $x_{2r+1}$  ya han sido transformados en montículos. Si  $x_r$  es menor que  $x_{2r}$  y  $x_{2r+1}$  no es necesario hacer nada más, ya que en este caso el subárbol con raíz en  $x_r$  es un montículo. De lo contrario, guardamos  $x_r$  temporalmente y movemos el menor de  $x_{2r}$  y  $x_{2r+1}$  al vértice libre. Esto crea una nueva vacante; si  $x_r$  es menor que los hijos del vértice libre, o si éste no tiene hijos, llenamos la vacante con  $x_r$ ; en caso contrario, llenamos la vacante con el menor de los hijos y proseguimos. Al llegar a una hoja, si no antes, encontraremos un lugar para  $x_r$ .

Las reglas anteriores forman la base del procedimiento  $\text{montículo}(k, n)$  que, dado un vértice  $x_r$  con la propiedad de que los subárboles con raíces en  $x_{2r}$  y  $x_{2r+1}$  son montículos, transforma el subárbol con raíz en  $x_k$  en un montículo. Aplicando este proceso sucesivamente para  $k = \lfloor n/2 \rfloor, \lfloor n/2 \rfloor - 1, \dots, 2, 1$ , el árbol completo se transforma en un montículo. El lector debiera comprobar que el montículo que se muestra en la figura 9.5 es el resultado de aplicar esta técnica a la lista inicial.

El método de transformar un montículo en una lista ordenada puede expresarse también en términos del procedimiento  $\text{montículo}$ . En un montículo la raíz siempre tiene el valor mínimo, de forma que es el primer elemento  $y_1$  de la lista ordenada. El lugar que deja libre la raíz será ocupado por el último valor  $x_n$  y tenemos entonces un árbol con  $n - 1$  vértices; los subárboles con raíces en  $x_2$  y  $x_3$  son también montículos, de manera que el procedimiento  $\text{montículo}(1, n - 1)$  restablece la propiedad de montículo del árbol en su globalidad. La raíz tiene de nuevo el mínimo valor y la asignamos a  $y_2$ . El lugar libre es ocupado por  $x_{n-1}$ ,  $\text{montículo}(1, n - 2)$  restablece la propiedad de montículo, y así sucesivamente.

Podemos expresar el algoritmo de ordenación de Williams completo de manera muy concisa en términos del procedimiento  $\text{montículo}$ :

El algoritmo de ordenación de Williams

---

```

para j:=0 hasta  $\lfloor \frac{1}{2}n \rfloor - 1$  hacer  $\text{montículo}(\lfloor \frac{1}{2}n \rfloor - j)$ ;
para i:=0 hasta  $n-2$  hacer
  inicio asignar  $x_i$  a  $y_i$ ; sustituir  $x_1$  por  $x_{n-i+1}$ 
   $\text{montículo}(1, n - i)$ 
  fin;
asignar  $x_1$  y  $x_2$  a  $y_{n-1}$  e  $y_n$ 
```

---

¿Cuántas comparaciones son necesarias en el algoritmo de Williams? En el procedimiento  $\text{montículo}(k, n)$  hemos de hallar el mínimo entre  $x_{2k}$  y  $x_{2k+1}$ , y compararlo con  $x_k$ ; esto son dos comparaciones. Repetimos esta operación en cada nivel, posiblemente hasta llegar a una hoja. Como  $x_k$  está en el nivel  $\lfloor \log_2 k \rfloor$  y una hoja está en el nivel  $\lfloor \log_2 n \rfloor$  o  $\lfloor \log_2 n \rfloor - 1$ , el número de comparaciones necesarias en  $\text{montículo}(k, n)$  es aproximadamente

$$2(\log_2 n - \log_2 k) = 2\log_2(n/k).$$

En la primera fase del algoritmo, el procedimiento *montículo*( $k, n$ ) se ejecuta para todos los  $k$  en el intervalo  $1 \leq k \leq n/2$ , aproximadamente. En la segunda fase, el procedimiento *montículo*( $1, j$ ) se ejecuta para todos los  $j$  en el intervalo  $2 \leq j \leq n - 1$ . Así pues, el número total de comparaciones es, aproximadamente,

$$2 \sum_{k=1}^{n/2} \log_2(n/k) + 2 \sum_{j=2}^{n-1} \log_2 j.$$

Ambas sumas tienen menos de  $n$  términos y cada término es como máximo  $\log_2 n$ , de donde resulta que el número de comparaciones en el algoritmo de Williams es  $O(n \log n)$ . Más aún, el número de transferencias de datos es proporcional al número de comparaciones, con lo que también es  $O(n \log n)$ .

### Ejercicios 9.2

- 1 ¿Cuál es la mínima altura posible del árbol de decisión de un algoritmo que ordene cuatro elementos utilizando comparaciones binarias?
- 2 Calcular el número de comparaciones binarias necesarias (en el peor de los casos) si se ordenan cuatro objetos
  - (i) por el método de la burbuja;
  - (ii) por inserción (método secuencial);
  - (iii) por inserción (método de bisección).
- 3 Utilizar la ordenación de Williams para formar un montículo a partir de las siguientes listas no ordenadas. Ilustrar en cada caso el montículo resultante en forma de árbol y escribir la lista correspondiente.
  - (i) 63, 55, 33, 16, 81, 76.
  - (ii) 73, 21, 17, 28, 32, 56, 19, 84, 38, 49, 77, 51, 12.
- 4 El programa siguiente corresponde al procedimiento *montículo*( $k, n$ ) descrito en el texto. Explicar en lenguaje corriente el propósito de cada línea del programa (por ejemplo, en la línea 2 se comprueba que  $x_j$  no sea una hoja).

### El procedimiento *montículo*( $k, n$ )

---

```

1 j:=k;
2 mientras j no supere a [ $\frac{1}{2}n$ ] hacer
    inicio
    3 si  $2j < n$  y  $x_{2j} > x_{2j+1}$  entonces a:=2j+1
    4           si no a:=2j;
    5 si  $x_a < x_j$  entonces inicio intercambiar  $x_a$  y  $x_j$ ; j:=a fin
    6           si no j:=n
    fin

```

---

- 5 Demostrar que si  $i$  y  $n$  son enteros con  $1 \leq i \leq n$ , entonces

$$i(n - i + 1) \geq n.$$

Deducir que  $n! \geq n^{n/2}$  si  $n$  es par, y que por lo tanto

$$\frac{1}{2} \log_2 n \leq \log_2(n!) \leq n \log_2 n.$$

### 9.3 Árboles generadores y el problema AGM

Sea  $G = (V, E)$  un grafo conexo y  $T$  un subconjunto de  $E$  tal que

- (i) cada vértice de  $G$  pertenece a una arista de  $T$ ;
- (ii) las aristas de  $T$  forman un árbol;

En este caso decimos que  $T$  es un **árbol generador** de  $G$ . Por ejemplo, las líneas gruesas muestran un árbol generador en la figura 9.6

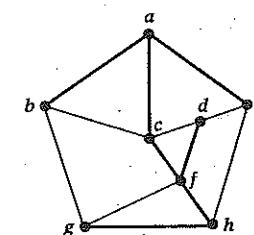


Fig. 9.6 Un grafo y uno de sus árboles generadores.

Es fácil "hacer crecer" un árbol generador: se toma un vértice  $v$  como "árbol parcial" inicial y se le añaden aristas una a una de forma que cada nueva arista añade un vértice al árbol parcial. El árbol generador de la figura 9.6 podría haber crecido a partir del vértice  $a$  y uniéndolo a los restantes vértices en el orden  $b, c, e, f, d, h, g$  mediante las aristas  $ab, ac, ae, cf, fd, fh$  y  $hg$ . En general, si hay  $n$  vértices necesitaremos  $n - 1$  pasos, después de los cuales tendremos  $1 + (n - 1) = n$  vértices y  $n - 1$  aristas (que es el número correcto según el teorema 8.5).

Para demostrar que el método siempre funciona, sea  $S$  el conjunto de los vértices en el árbol parcial en un estadio intermedio de forma que  $S$  no es vacío ni todo  $V$ . Si no hubiera ninguna arista con un vértice en  $S$  y otro en el conjunto complementario  $\bar{S}$ , no podría haber ningún camino entre  $S$  y  $\bar{S}$ ; entonces  $G$  no sería conexo, contrariamente a la hipótesis. Así pues, siempre hay alguna arista disponible en cada paso de la construcción.

### Ejercicios 9.3

- Hallar árboles generadores del grafo cubo (figura 8.12) y del grafo de Petersen (figura 8.14).
- Hacer un esquema de todos los árboles generadores del grafo completo  $K_4$  (hay 16 en total).

Los árboles generadores son útiles en varios contextos. Por ejemplo, supongamos que hemos de unir una serie de ciudades por pares mediante tuberías, de manera que formen una red conexa. Es posible que algunos pares de ciudades no puedan unirse por razones geográficas. Por otra parte, cada posible unión tiene asociado un coste. Formalmente tenemos un grafo  $(V, E)$  que tiene las ciudades como vértices y por aristas las posibles uniones, y una función  $w$  de  $E$  en  $\mathbb{N}$  de forma que  $w(e)$  representa el coste de construir la arista  $e$ . Decimos que  $G$  y  $w$  constituyen un **grafo ponderado** y que  $w$  es una **función de peso**.

En el problema de las tuberías, el objetivo práctico es obtener una red de interconexión de coste mínimo, que corresponde a un árbol generador  $T$  de  $G$  cuyo peso total

$$w(T) = \sum_{e \in T} w(e)$$

sea el menor posible. A esta situación la denominaremos el **problema AGM (problema del árbol generador minimal)** del grafo  $G$ .

Como los valores  $w$  son enteros positivos, es evidente que el problema tiene solución, ya que hay un número finito de árboles generadores  $T$  de  $G$  y cada uno de ellos proporciona un valor entero positivo de  $w(T)$ . En otras palabras, existe un árbol generador minimal  $T_0$  tal que

$$w(T_0) \leq w(T)$$

para todo árbol generador  $T$ . Hacemos notar, sin embargo, que pueden existir varios árboles distintos con la misma propiedad.

Hay un algoritmo sencillo para el problema AGM basado en el principio voraz aplicado al método de crecimiento anterior. En concreto, en cada paso se añade la arista *menos costosa* que une un nuevo vértice al árbol parcial (si hay varias aristas disponibles con el mismo peso se elige cualquiera de ellas). Por ejemplo, si en la figura 9.7 empezamos por  $u$ , podemos añadir las aristas en el orden  $uv, ux, uy, yz$ . Por otra parte, si empezamos por  $y$ , hemos de añadir las aristas en el orden  $yz, yu, uv, ux$ .

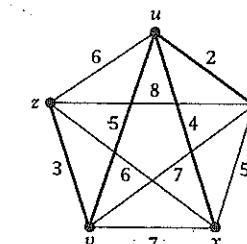


Fig. 9.7 Un árbol generador minimal.

A primera vista, es sorprendente que el algoritmo voraz en el problema AGM funcione, especialmente si recordamos que en el problema de la coloración de vértices el algoritmo voraz no siempre producía una coloración con el mínimo número posible de colores. Pero en el caso del problema AGM estamos de suerte.

**Teorema 9.3.** Sea  $G = (V, E)$  un grafo conexo con función de peso  $w : E \rightarrow \mathbb{N}$  y supongamos que  $T$  es un árbol generador de  $G$  construido mediante el algoritmo voraz. Entonces, para cualquier árbol generador  $U$  de  $G$  se tiene que

$$w(T) \leq w(U).$$

**DEMOSTRACIÓN:** Denotaremos las aristas de  $T$  por  $e_1, e_2, \dots, e_{n-1}$  en el orden de construcción del algoritmo. Si  $U = T$ , el resultado es evidentemente cierto. Si  $U \neq T$ , hay aristas de  $T$  que no son de  $U$ ; sea  $e_k$  la primera de ellas, en el orden que hemos establecido. Sea  $S$  el conjunto de vértices del árbol parcial inmediatamente anterior a la adjunción de  $e_k$ , y sea  $e_k = xy$ , donde  $x$  es de  $S$  e  $y$  no lo es.

Como  $U$  es un árbol generador, existe un camino en  $U$  de  $x$  a  $y$ ; al recorrer este camino encontraremos una arista  $e^*$  que tendrá un vértice en  $S$  y otro fuera de  $S$ . Cuando el algoritmo voraz selecciona  $e_k$  para  $T$ ,  $e^*$  es también un candidato pero no es seleccionado. Así pues, ha de ser  $w(e^*) \geq w(e_k)$ . Por otra parte, si  $e^*$  es de  $T$ , ha de ser seleccionada después de  $e_k$ , de modo que viene después de  $e_k$  en el orden establecido.

El resultado de eliminar  $e^*$  de  $U$  y sustituirlo por  $e_k$  es un árbol generador  $U_1$  para el cual

$$w(U_1) = w(U) - w(e^*) + w(e_k) \leq w(U).$$

Más aún, la primera arista de  $T$  que no es de  $U_1$  aparece después de  $e_k$ . Podemos repetir el proceso y obtenemos una sucesión de árboles generadores  $U_1, U_2, \dots$  con la propiedad de que cada uno tiene un segmento inicial de la sucesión  $e_1, e_2, \dots, e_{n-1}$  en común con  $T$  mayor que el anterior. El proceso acaba cuando llegamos a un árbol generador  $U_r$  igual a  $T$ , ya que entonces

$$w(T) = w(U_r) \leq w(U_{r-1}) \leq \dots \leq w(U_1) \leq w(U),$$

tal como se quería demostrar.  $\square$

Hay una forma clara de controlar el desarrollo del algoritmo mediante una tabla con tres columnas.

I	II	III
$x$	$y$	$w(x, y)$
$\vdots$	$\vdots$	$\vdots$

La columna I es una lista con los vértices que no están en  $S$ , el conjunto de vértices que ya han sido añadidos al árbol parcial. Para cada uno de

estos  $x$ , la entrada correspondiente  $y$  de la columna II es un vértice de  $S$  tal que la arista  $xy$  sea una de las aristas de menor coste que unen  $x$  a un vértice de  $S$ . La columna III contiene el valor de  $w(xy)$ .

En el paso  $i$ -ésimo de la construcción,  $|S| = i$  y hay  $n - i$  vértices en la columna I. Hemos de seleccionar la menor de las entradas de la columna III, pongamos  $w(x_0, y_0)$ , lo que conlleva  $n - i - 1$  comparaciones. Después hay que actualizar la tabla como resultado de añadir  $x_0$  a  $S$  mediante la arista  $x_0y_0$ . Esto significa eliminar la fila  $x_0$  y comprobar si  $x_0$  (que ahora es de  $S$ ) puede sustituir a alguna de las entradas anteriores en la columna II: es decir, comprobar si  $w(xx_0) < w(xy)$  para cualquiera de los restantes  $n - i - 1$  vértices  $x$ , lo que conlleva otras  $n - i - 1$  comparaciones. El número total de comparaciones necesarias es

$$\sum_{i=1}^{n-1} 2(n - i - 1) = (n - 1)(n - 2),$$

que es  $O(n^2)$ .

### Ejercicios 9.3 (continuación)

- 3 Utilizar el algoritmo voraz para hallar un árbol generador minimal para el grafo ponderado de la figura 9.8. En este caso, ¿es único el árbol generador minimal?

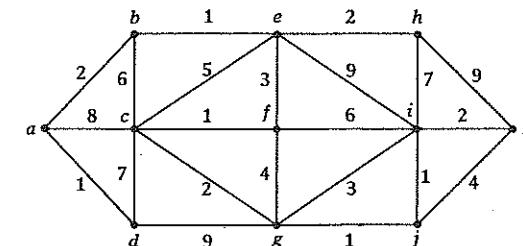


Fig. 9.8 Hallar el AGM.

- 4 Sea  $G$  el grafo ponderado que tiene por conjunto de vértices a  $\{x, a, b, c, d, e, f\}$  y cuyas aristas y pesos vienen dados por la siguiente tabla:

$xa$	$xb$	$xc$	$xd$	$xe$	$xf$	$ab$	$bc$	$cd$	$de$	$ef$	$fa$
6	3	2	4	3	7	6	2	3	1	8	6

Hallar todos los árboles generadores minimales de  $G$ .

5 Sea  $T$  un árbol generador minimal de un grafo ponderado  $K$  y sea  $e^*$  una arista de  $K$  que no es de  $T$ . Sea  $e$  una de las aristas de  $T$  pertenecientes al único camino en  $T$  que une los vértices de  $e^*$ . Demostrar que  $w(e) \leq w(e^*)$ .

6 Escribir un "programa" para el algoritmo voraz basado en el método tabular esbozado anteriormente.

#### 9.4 Búsqueda en profundidad

Supongamos que hemos de llevar a cabo una búsqueda de los vértices de un grafo, empezando por un vértice concreto. Esencialmente, podemos emplear dos estrategias distintas. Podríamos "profundizar"; moviéndonos a un nuevo vértice siempre que fuera posible, o podríamos "desplegarnos", comprobando todos los vértices en un "nivel" antes de pasar al siguiente. En este apartado consideraremos la primera estrategia, conocida técnicamente con el nombre de **búsqueda en profundidad** (BEP).

El diagrama de la figura 9.9a representa el juego del escondite. El que busca está inicialmente en  $a$  y ha de comprobar los escondites  $b, c, d$  y  $e$  utilizando las rutas disponibles. Es claro que el grafo de la figura 9.9b contiene los elementos esenciales del problema.

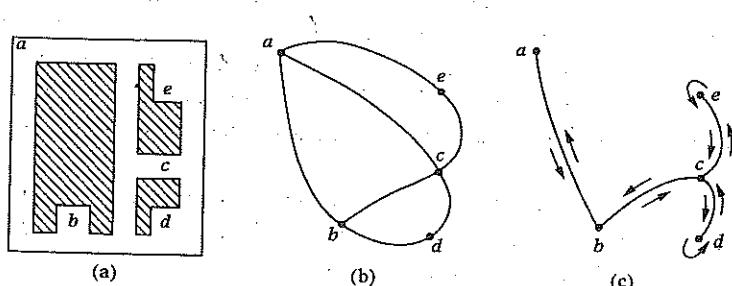


Fig. 9.9 El juego del escondite.

En la estrategia BEP, el que busca se comporta como un niño excitado. Va de  $a$  a cualquier vértice adyacente, pongamos  $b$ , e inmediatamente a un nuevo vértice  $c$ . De  $c$  va a  $d$ , pero allí se encuentra clavado, puesto que

ya ha visitado a los dos vértices adyacentes. De forma que "retrocede" de  $d$  a  $c$  y descubre un nuevo vértice  $e$  disponible al cual se dirige.

Aunque el que busca no puede saberlo, ya no hay más escondites que comprobar. En la estrategia BEP podemos imaginar que la excitación infantil ha sido sustituida por una comprobación sistemática que revelará si todavía queda algún vértice por visitar. Como los dos vecinos  $a$  y  $c$  de  $e$  ya han sido visitados, el buscador retrocede a  $c$  (de donde fue primero a  $e$ ). Nuevamente, todos los vecinos de  $c$  han sido visitados, de modo que retrocede a  $b$  (de donde, en primera instancia, fue a  $c$ ). Análogamente, de  $b$  retrocede hasta  $a$ . En  $a$  no hay nuevos vecinos y reconoce el punto de partida. La búsqueda ha terminado: si se ha seguido el procedimiento correctamente, todos los vértices accesibles desde  $a$  han sido explorados.

El procedimiento BEP puede considerarse como un caso particular del método de crecimiento de árboles introducido al principio del apartado anterior. Al visitar un nuevo vértice, añadimos al árbol parcial la arista que conduce a él; en el ejemplo anterior, las aristas se añadirían en el orden  $ab, bc, cd$  y  $ce$  (fig. 9.9c). La característica especial del método BEP es que el nuevo vértice siempre se elige adyacente al último de los posibles vértices anteriores.

Una descripción más formal del método BEP es la siguiente. Empezamos en un vértice  $v$  y construimos un árbol parcial  $W$  de la siguiente manera. Siempre que el vértice activo  $x$  tenga nuevos vecinos, elegimos uno de ellos  $y$ , añadimos  $xy$  a  $W$ , AVANZAMOS hasta  $y$  y sustituimos  $x$  por  $y$  como nuevo vértice activo. Cuando no hay nuevos vértices adyacentes a  $x$ , RETROCEDEMOS al vértice que originalmente nos condujo a  $x$ . Eventualmente, nos hallaremos de nuevo en  $v$  sin ningún lugar a dónde ir, y entonces  $W = T$  y acabamos. En este proceso, hemos usado cada arista de  $T$  dos veces, una para avanzar y otra para retroceder (fig. 9.9c).

Hay una diferencia importante entre los problemas de crecimiento de árboles del apartado anterior y el procedimiento de búsqueda BEP. En el apartado 9.3 sabíamos de antemano que el grafo  $G$  era conexo, con lo que la lista de vértices contendría finalmente todos los vértices del grafo y el árbol era un árbol generador de  $G$  (por este motivo podíamos acabar después de  $n - 1$  pasos sin tener que comprobar que no había más vértices accesibles). Pero en un problema de búsqueda no sabemos si  $G$  es conexo: de hecho, el objetivo de la búsqueda puede ser dilucidar precisamente esta

cuestión. Lo que sabemos es que BEP hallará todos los vértices que pueden ser alcanzados desde el vértice inicial  $v$ .

**Teorema 9.4.** Sea  $v$  un vértice del grafo  $G$  y  $T$  el conjunto de aristas construido mediante el método BEP. Entonces  $T$  es un árbol generador del componente de  $G$  que contiene a  $v$ .

**DEMOSTRACIÓN:** Que  $T$  es un árbol es consecuencia directa de las reglas de la construcción. Sea  $z$  un vértice en el mismo componente que  $v$ , de forma que existe un camino en  $G$

$$v = v_0, v_1, \dots, v_k = z.$$

Si  $z$  no es de  $T$ , entonces (ya que  $v$  es de  $T$ ) ha de existir un par  $v_i, v_{i+1}$  tal que  $v_i$  sea vértice de  $T$  y  $v_{i+1}$  no lo sea. Al ser  $v_i$  de  $T$ , será el vértice activo  $x$  al menos una vez. Siempre que avancemos de  $v_i$  hacia un nuevo vértice debemos volver eventualmente a  $v_i$ , ya que se puede retroceder a través de las aristas del árbol. No podemos abandonar  $v_i$  hasta que todos sus vecinos hayan sido visitados; en particular, si  $v_{i+1}$  no es de  $T$ , no puede ser vecino de  $v_i$ , contrariamente a la hipótesis. Así pues,  $z$  debe estar en  $T$ .  $\square$

Tabla 9.4.1

Pila	Añadir	Quitar
$a$	$a$	—
$ab$	$b$	—
$abc$	$c$	—
$abcd$	$d$	—
$abc$	—	$d$
$abce$	$e$	—
$abc$	—	$e$
$ab$	—	$c$
$a$	—	$b$
$\emptyset$	—	$a$

Una buena manera de describir BEP es haciendo una lista de los vértices. Cuando alcanzamos un vértice por primera vez en la búsqueda,

se añade a la lista, y se elimina cuando lo abandonamos definitivamente. La lista de vértices se conoce con el nombre de pila, ya que se comporta como una pila de platos para ser usados en un restaurante: sólo se pueden añadir o quitar vértices (platos) en la cima de la pila. Si el final de la lista representa la cima de la pila, la tabla 9.4.1 describe BEP para el grafo de la figura 9.9c empezando por el vértice  $a$ .

En general, BEP en un grafo se describe mediante el siguiente algoritmo, donde  $v$  es el vértice inicial y  $cima(pila)$  es el vértice activo al final de la lista.

```

sea pila=(v);
mientras pila no vacía hacer
    inicio
        x:= cima(pila);
        si x es adyacente a un nuevo vértice y
            entonces añadir y a la cima de la pila
            si no quitar x de la pila
        fin
    
```

#### Ejercicios 9.4

- 1 Sea  $G$  el grafo definido mediante la lista de adyacencias de la tabla 9.4.2.

Tabla 9.4.2

$a$	$b$	$c$	$d$	$e$	$f$	$g$	$h$
$b$	$a$	$b$	$a$	$b$	$g$	$c$	$a$
$d$	$c$	$d$	$b$		$f$	$g$	
$h$	$d$	$g$	$c$		$h$		
				$e$			

Calcular el árbol BEP de  $G$ , empezando por  $g$  (cuando haya más de un vértice, elegir el primero por orden alfabético). ¿Es  $G$  conexo?

- 2 Usar el método BEP de forma sistemática para hallar los componentes del grafo que tiene por lista de adyacencias la que muestra la tabla 9.4.3.

Tabla 9.4.3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	0	1	11	0	11	0	1	10	9	4	1	2	4
5	8	5	12	14	2	14	5	12	12	6	3	5	6	
7	13				7	13			14	9	7	11		
										10				
											13			

3 El diagrama de la figura 9.10 representa un laberinto, donde las líneas son paredes y los espacios pasillos.

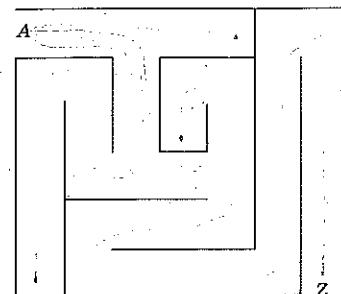


Fig. 9.10 Un laberinto que no es famoso.

- Poner etiquetas a los cruces y a las calles sin salida (la entrada es A y la salida Z).
- Obtener la lista de adyacencias del grafo correspondiente.
- Utilizar BEP para hallar un camino de A a Z en el grafo.
- Dibujar el camino correspondiente en el laberinto.

4 Construir una tabla que muestre cómo se comporta la pila al aplicar BEP al grafo de la tabla 9.4.2 (empezar por a y utilizar el orden alfabético si hay más de una opción).

## 9.5 Búsqueda en anchura

La principal alternativa a BEP es la **búsqueda en anchura** (BEA). Mientras que en BEP avanzamos de un vértice a otro nuevo siempre que

sea posible, en BEA visitamos todos los vecinos del vértice activo antes de ir al siguiente. En consecuencia, no hay necesidad de retroceder.

Al igual que BEP, BEA puede considerarse como un método de crecimiento de árboles, aunque también como una pura técnica de búsqueda, sin más que fabricar una lista con los vértices en su orden de aparición. El lector debiera comparar y contrastar la siguiente descripción con la de BEP.

Empezamos en un vértice  $v$  y construimos un árbol parcial  $W$ . Mientras el vértice activo  $x$  tenga vecinos nuevos, elegimos uno de ellos  $y$  y ADJUNTAMOS  $xy$  a  $W$  (*no sustituimos*  $x$  por  $y$ ). Cuando ya no quedan vecinos nuevos de  $x$ , pasamos al SIGUIENTE vértice después de  $x$  en el orden original de aparición. Finalmente llegaremos a un vértice que no tiene nuevos vecinos y para el que no existe vértice siguiente; entonces hacemos  $T = W$  y acabamos. Por ejemplo, el procedimiento BEA aplicado al grafo del escondite (fig. 9.9) empezando por  $a$ , añadiría las aristas en el orden  $ab, ac, ae, bd$ .

La demostración del siguiente teorema es muy parecida a la del teorema 9.4 y la dejamos como ejercicio (ejercicio 9.7.16).

**Teorema 9.5.** Sea  $v$  un vértice del grafo  $G$  y  $T$  el conjunto de aristas construido mediante el método BEA. Entonces  $T$  es un árbol generador del componente de  $G$  que contiene a  $v$ .  $\square$

Es instructivo comparar el desarrollo de BEP y BEA en términos de la lista de vértices en el orden de búsqueda. Mientras que en BEP la lista se comporta como una pila, en BEA es una cola, ya que recuerda a la progresión ordenada de gente esperando en una tienda a ser atendidos. Los nuevos vértices se añaden al final de la cola y los antiguos se eliminan del principio. El algoritmo es el siguiente, donde  $v$  es el vértice inicial.

```

sea cola = (v);
mientras cola no vacía hacer
  inicio
    x := principio(cola);
    si x es adyacente a un nuevo vértice y
      entonces añadir y al final de la cola
    si no quitar x de la cola
fin
  
```

Por ejemplo, el desarrollo del método BEA para el grafo del escondite es el de la tabla 9.5.1

En ciertos contextos, la cola BEA se conoce como el modo *primero en entrar, primero en salir* (en inglés *FIFO*), mientras que la pila BEP es el modo *último en entrar, primero en salir* (en inglés *LIFO*).

Tabla 9.5.1

Cola	Añadir	Quitar
<i>a</i>	<i>a</i>	—
<i>ab</i>	<i>b</i>	—
<i>abc</i>	<i>c</i>	—
<i>abce</i>	<i>e</i>	—
<i>bce</i>	—	<i>a</i>
<i>bced</i>	<i>d</i>	—
<i>ced</i>	—	<i>b</i>
<i>ed</i>	—	<i>c</i>
<i>d</i>	—	<i>e</i>
$\emptyset$	—	<i>d</i>

### Ejercicios 9.5

- Construir el árbol BEA con raíz en *c* para el grafo *G* definido en el ejercicio 9.4.1.
- Utilizar BEA para comprobar si el grafo definido en la tabla 9.5.2 es conexo.

Tabla 9.5.2

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>
<i>e</i>	<i>d</i>	<i>e</i>	<i>b</i>	<i>a</i>	<i>c</i>	<i>b</i>	<i>b</i>	<i>a</i>
<i>i</i>	<i>g</i>	<i>f</i>	<i>g</i>	<i>c</i>	<i>e</i>	<i>d</i>	<i>d</i>	<i>c</i>
<i>h</i>	<i>i</i>	<i>h</i>	<i>f</i>	<i>i</i>	—	—	—	<i>f</i>

- Sea *v* un vértice del grafo completo  $K_n$ . Calcular la altura de los árboles BEP y BEA en  $K_n$  con raíz en *v*. ¿Cuáles son las alturas respectivas si el grafo es ahora el ciclo  $C_n$ ?

4 Construir tablas que muestren cómo se forma la cola al aplicar BEA al grafo del ejercicio 9.4.1 (empezar con el vértice *a* y usar el orden alfabético si hay que elegir).

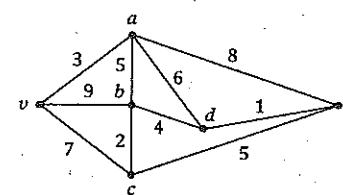
5 Sea *G* un grafo conexo regular de grado *k* y sea *d* la altura del árbol BEA con raíz en un vértice de *G*. Demostrar que el número de vértices de *G* es, a lo sumo,

$$1 + k + k(k - 1) + k(k - 1)^2 + \cdots + k(k - 1)^{d-1}.$$

### 9.6 El problema del camino más corto

Muchos de los algoritmos que se usan en la informática y la investigación operativa están basados en BEP o BEA. Puede ser difícil decidir, en un problema particular, qué técnica es la apropiada; la decisión puede depender de un análisis teórico, de la experiencia práctica, o de ambos. En términos generales, BEP es preferible si el problema requiere hallar sólo una solución entre varias posibles: por ejemplo, si hemos de hallar un camino cualquiera que una dos vértices de un grafo. Por su parte, BEA es más adecuado para problemas que requieren algún tipo de optimización, tales como hallar un camino con el menor número de aristas. En este apartado estudiaremos una generalización de este último problema.

Supongamos que tenemos un grafo ponderado, por ejemplo el que muestra la figura 9.11, y pensemos en los pesos como en las "distancias" de las aristas en alguna interpretación práctica. Queremos hallar el camino más corto de un vértice *v* a otro vértice *w*, donde la longitud de un camino se mide sumando las longitudes de sus aristas.

Fig. 9.11 Hallar el camino más corto de *v* a *e*.

Supongamos que hemos comprobado que el camino más corto de  $v$  a un vértice  $p$  tiene longitud  $l(p)$ . Supónganos también que  $y$  es un vecino de  $p$  para el que sólo tenemos una estimación  $l(y)$  de la longitud del camino más corto de  $v$  a  $y$  (fig. 9.12). La ruta más corta de  $v$  a  $y$  vía  $p$  tiene longitud  $l(p) + w(py)$  y, si ésta es menor que  $l(y)$ , podemos mejorar nuestra estimación. Es decir, asignamos a  $l(y)$  un nuevo valor, igual a

$$\min\{l(y), l(p) + w(py)\}.$$

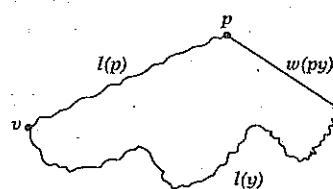


Fig. 9.12  $l(y) \leftarrow \min\{l(y), l(p) + w(py)\}$ .

La idea que subyace en el algoritmo para el problema del camino más corto es usar una versión del procedimiento BEA para construir un árbol, con raíz en  $v$ , cuyas aristas definen el camino más corto de  $v$  a cualquier otro vértice. En cada paso, un vértice  $x$  tiene una etiqueta  $l(x)$ , que puede ser temporal o permanente. Cuando estamos seguros de que  $l(x)$  es la longitud del camino más corto de  $v$  a  $x$ , la etiqueta  $l(x)$  se vuelve permanente y añadimos  $x$  al árbol.

Empezamos con  $l(v) = 0$ , que ya es permanente, y para cualquier otro vértice  $x$  hacemos  $l(x)$  igual a algún número grande  $L$ . Sea  $p$  el último vértice que ha recibido una etiqueta permanente (inicialmente es  $p = v$ ). Para cada vértice  $y$  adyacente a  $p$  que tenga una etiqueta temporal, calculamos el nuevo valor de  $l(y)$  tal como se ha indicado anteriormente. Después hallamos el vértice  $q$  que tiene la etiqueta temporal mínima: hacemos su etiqueta permanente y lo añadimos al árbol mediante la arista  $zq$ , donde  $z$  es el vértice utilizado para obtener el valor  $l(q)$ . Luego sustituimos  $p$  por  $q$  y proseguimos hasta que todos los vértices tengan una etiqueta permanente.

La tabla 9.6.1 muestra el proceso de etiquetaje y la formación del árbol para el grafo de la figura 9.11.

Tabla 9.6.1

$p$	$v$	$a$	$b$	$c$	$d$	$e$	$q$	$zq$
	0	$L$	$L$	$L$	$L$	$L$		
$v$	3	9	7	$L$	$L$	$a$	$va$	
$a$		8	7	9	11	$c$	$vc$	
$c$			8	9	11	$b$	$ab$	
$b$				9	11	$d$	$ad$	
$d$					10	$e$	$de$	

Un valor adecuado para  $L$  en este caso sería 50, la suma de todos los pesos; es evidente que ningún camino puede tener una longitud mayor. El camino más corto de  $v$  a cualquier otro vértice es el único camino en el árbol que va de  $v$  a dicho vértice; por ejemplo, el camino más corto de  $v$  a  $e$  es  $v, a, d, e$ . Si sólo necesitamos el camino más corto hasta un vértice en particular, nos detendremos en cuanto dicho vértice reciba una etiqueta permanente.

### Ejercicios 9.6

- 1 Usar el método tabular descrito más arriba para hallar el camino más corto de  $v$  a  $w$  en el grafo ponderado de la figura 9.13.

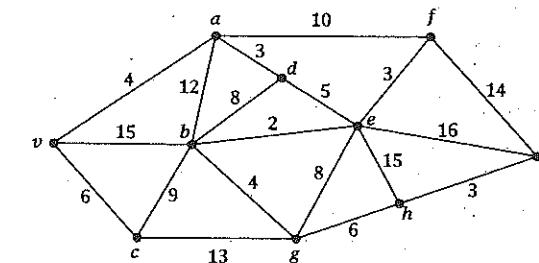


Fig. 9.13 Hallar el camino más corto de  $v$  a  $w$ .

- 2 Hallar la ruta más corta de  $A$  a  $F$  en el grafo ponderado que especifica la tabla 9.6.2.

Tabla 9.6.2

	A	B	C	D	E	F
A	—	5	8	3	4	9
B	—	—	6	1	5	4
C	—	—	—	3	9	2
D	—	—	—	—	4	6
E	—	—	—	—	—	3

3 Partimos de un grafo ponderado con  $n$  vértices. Definimos el *Estado i* del algoritmo como la fase en la que  $i$  de los vértices han recibido etiquetas permanentes ( $1 \leq i \leq n-1$ ). ¿Cuál es el número mínimo de comparaciones necesarias para calcular las nuevas etiquetas en el Estado  $i$ ? ¿Cuál es el número máximo de comparaciones necesarias para decidir qué vértice será el siguiente en recibir una etiqueta permanente? Deducir que el número total de comparaciones que requiere el algoritmo es  $O(n^2)$ .

## 9.7 Ejercicios diversos

1 Sea  $T$  un árbol  $m$ -ario con raíz y  $n$  vértices,  $l$  hojas e  $i$  vértices internos. Demostrar que

$$n = mi + 1$$

y deducir una expresión de  $l$  en términos de  $m$  y  $n$ .

2 Para cada uno de los seis árboles diferentes (sin raíz) con seis vértices (ejercicio 8.5.1) hallar el número de maneras esencialmente distintas de elegir un vértice como raíz. Calcular el número de árboles con raíz y seis vértices distintos.

3 Utilizar la ordenación de Williams para construir un montículo a partir de la lista

$$29, 38, 71, 15, 32, 61, 83, 35, 47, 67, 78, 63, 91.$$

4 Supongamos que etiquetamos  $x_1, x_2, \dots, x_n$  los vértices de un árbol "quasi-binario" como el de la figura 9.4 y sea  $r_i$  el número de vértices del subárbol con raíz en  $x_i$ . Demostrar que el número de maneras de asignar  $n$  enteros distintos a los vértices de modo que formen un montículo es

$$\frac{n!}{r_1 r_2 \cdots r_n}.$$

5 Demostrar que el grafo completo  $K_5$  tiene 125 árboles generadores distintos (no hacer una lista de todos ellos).

6 Hallar todos los árboles generadores minimales del grafo ponderado de la figura 9.14.

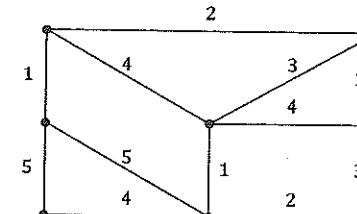


Fig. 9.14 Hallar todos los AGM.

7 Hallar el camino más corto de  $a$  a  $k$  en la figura 9.8.

8 La versión de Kruskal del algoritmo voraz es la siguiente: elegir las aristas en orden de peso creciente, rechazando aquellas que al incluirlas completarían un ciclo. Mostrar mediante un ejemplo que, en el método de Kruskal, el conjunto de aristas construido en un paso intermedio no tiene por qué formar un grafo conexo.

9 Demostrar la versión del teorema 9.3 correspondiente al método de Kruskal (en otras palabras, demostrar que el método de Kruskal funciona).

10 Diseñar un laberinto con una única "puerta" y un único "centro" usando una representación similar a la de la figura 9.11. Describir cómo utilizar BEP para encontrar un modo de salir del centro a la puerta.

11 En 1895 G. Tarry dio la siguiente regla para salir de un laberinto. *No volver a pasar por el lugar que condujo a una bifurcación por primera vez, a menos que no haya otra alternativa.* Explicar la conexión entre la regla de Tarry y el algoritmo de búsqueda en profundidad.

12 Sea  $T$  un árbol generador de un grafo  $G$  y  $r$  un vértice de  $G$ . Si consideramos  $T$  como un grafo dirigido (dirigiendo cada arista desde  $r$ ) podemos decir que los vértices  $x$  e  $y$  están  $T$ -relacionados si existe un camino dirigido en  $T$  de  $x$  a  $y$  o de  $y$  a  $x$ .

Demostrar que si  $T$  es un árbol BEP con raíz en  $r$  y  $xy$  es una arista de  $G$  que no está en  $T$ , entonces  $x$  e  $y$  están  $T$ -relacionados.

13 Demostrar con un ejemplo que la conclusión del ejercicio anterior es falsa si  $T$  es un árbol BEA con raíz en  $r$ .

14 Un vértice de un grafo conexo es un vértice de articulación si su supresión (junto con las aristas que contiene) desconecta el grafo. Utilizar la idea contenida

en el ejercicio 1.3 para formular un algoritmo, basado en BEP, para hallar los vértices de articulación de un grafo conexo dado.

15 Demostrar el teorema 9.5.

16 Denotemos por  $1, 2, \dots, n$  los vértices del grafo completo  $K_n$  y definamos, para cada árbol generador  $T$  de  $K_n$ , el símbolo de Prüfer  $(p_1, p_2, \dots, p_{n-2})$  como sigue. El símbolo de Prüfer de un árbol con dos vértices es nulo. Si  $n > 2$ , el símbolo de Prüfer de un árbol  $T$  con  $n$  vértices es  $(j, q_1, \dots, q_{n-3})$ , donde

- (i)  $j$  es el único vértice de  $T$  adyacente al primer vértice  $i$  de grado uno en orden alfabético,
- (ii)  $(q_1, \dots, q_{n-3})$  es el símbolo de Prüfer del árbol que se obtiene al suprimir de  $T$  la arista  $ij$ .

Demostrar que el símbolo de Prüfer define una biyección entre el conjunto de árboles generadores de  $K_n$  y el conjunto de  $(n - 2)$ -plas ordenadas del conjunto  $\{1, 2, \dots, n\}$  y deducir que  $K_n$  posee  $n^{n-2}$  árboles generadores.

17 Tenemos cuatro monedas y como máximo una de ellas es falsa (más liviana o más pesada). Demostrar que para determinar la moneda falsa, si hay alguna, se requieren, en teoría, al menos dos pesadas, pero que este número no puede alcanzarse (en este problema no se dispone de una moneda verdadera).

## 10 Grafos bipartidos y problemas de emparejamientos

### 10.1 Relaciones y grafos bipartidos

En el apartado 3.2 introdujimos una amplia clase de problemas que pueden expresarse en términos de contar un cierto subconjunto de un conjunto producto  $X \times Y$ . Una manera de describir tal subconjunto, es decir que un elemento  $x$  de  $X$  y un elemento  $y$  de  $Y$  están “relacionados” si el par  $(x, y)$  pertenece al subconjunto. Por ejemplo, si  $X$  es un conjunto de estudiantes e  $Y$  un conjunto de asignaturas, podríamos decir que  $x$  e  $y$  están relacionados si el estudiante  $x$  cursa la asignatura  $y$ .

Estos comentarios nos llevan a definir una relación  $R$  entre dos conjuntos  $X$  e  $Y$  simplemente como un subconjunto de  $X \times Y$ , de modo que los enunciados

$x$  e  $y$  están relacionados (por  $R$ ),  
el par  $(x, y)$  es de  $R$ ,

significan exactamente lo mismo. Es posible que  $X = Y$ ; es el caso, por ejemplo, si consideramos relaciones de equivalencia definidas en  $X$ . Sin embargo, en este capítulo estudiaremos relaciones entre conjuntos  $X$  e  $Y$  disjuntos. A continuación mostraremos cómo representar una relación de este tipo mediante un grafo bipartido.

Si  $R$  es una relación entre conjuntos disjuntos  $X$  e  $Y$  (es decir,  $R$  es un subconjunto de  $X \times Y$ ), definimos un grafo bipartido  $G$  que representa a  $R$  como sigue. El conjunto de vértices de  $G$  es la unión de  $X$  e  $Y$  y el conjunto de aristas  $E$  contiene las aristas  $xy$  tales que  $(x, y)$  es de  $R$ . Como cada arista tiene un vértice en  $X$  y otro en  $Y$ , está claro que  $G$  es bipartido. Es conveniente pensar en un dibujo de  $G$ , por ejemplo el

de la figura 10.1. Si queremos insistir en que  $G$  es bipartido, usaremos la notación  $G = (X \cup Y, E)$ :

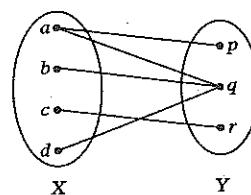


Fig. 10.1 El grafo bipartido que representa la relación  
 $R = \{(a, p), (a, q), (b, q), (c, r), (d, q)\}$ .

El teorema básico para contar conjuntos de pares tiene una interpretación sencilla en términos de grafos.

**Teorema 10.1.** Sea  $G = (X \cup Y, E)$  un grafo bipartido y sea  $\delta(v)$  el grado de un vértice  $v$  de  $G$ . Entonces

$$\sum_{x \in X} \delta(x) = \sum_{y \in Y} \delta(y) = |E|.$$

**DEMOSTRACIÓN:** Como cada arista tiene exactamente un vértice en  $X$ , el número total de aristas es la suma de los grados de los vértices de  $X$ . Igualmente para la suma de los grados de los vértices de  $Y$  y de aquí se sigue el resultado.  $\square$

En lo que resta de capítulo enunciaremos los resultados en términos de grafos bipartidos, más que de relaciones. Sin embargo, todos los resultados podrían interpretarse como resultados sobre relaciones si quisieramos.

**Ejemplo.** Tenemos un conjunto de personas y un conjunto de trabajos, de tal forma que cada persona está cualificada para hacer exactamente  $k$  trabajos y para cada trabajo hay exactamente  $k$  personas cualificadas para hacerlo. Demostrar que

- (i) el número de personas es igual al número de trabajos;
- (ii) dado un  $n$ -subconjunto  $A$  de las personas, hay al menos  $n$  trabajos para las cuales algún miembro de  $A$  está cualificado.

**SOLUCIÓN:** Sea  $X$  el conjunto de personas e  $Y$  el de trabajos. Diremos que  $x$  y  $y$  están relacionados si la persona  $x$  está cualificada para el trabajo  $y$ . La condición del enunciado nos dice que el grafo bipartido  $G = (X \cup Y, E)$  que representa esta relación es un grafo regular de grado  $k$ . Según el teorema 10.1 tenemos que

$$|X|k = |Y|k = |E|,$$

con lo que  $|X| = |Y|$ , tal como se afirmaba en (i).

Para la parte (ii), sea  $A$  un  $n$ -subconjunto de  $X$  y definamos  $T(A)$  como el conjunto de trabajos para las que al menos un miembro de  $A$  está cualificado; es decir,

$$T(A) = \{y \in Y \mid xy \in E \text{ para algún } x \in A\}.$$

Como cada vértice pertenece exactamente a  $k$  aristas de  $G$ , el conjunto  $E_A$  de aristas que tienen un vértice en  $A$  tiene cardinal  $k|A| = kn$ . Por definición de  $T(A)$ , cada una de estas aristas tiene un vértice en  $T(A)$ , y la condición enunciada nos dice que el número total de aristas con un vértice en  $T(A)$  es  $k|T(A)|$ . Por lo tanto,

$$|E_A| = kn \leq k|T(A)|$$

y  $|T(A)| \geq n$  como afirmábamos.  $\square$

### Ejercicios 10.1

- 1 Sea  $X = \{2, 3, 5, 7, 11\}$ ,  $Y = \{99, 100, 101, 102, 103\}$  y digamos que  $x$  e  $y$  están relacionados si  $x$  es un divisor de  $y$ . Dibujar el grafo bipartido que representa a esta relación y comprobar que se satisface el teorema 10.1.
- 2 El **grafo bipartido completo**  $K_{r,s}$  es el grafo bipartido  $(X \cup Y, E)$  donde  $|X| = r$ ,  $|Y| = s$ , y cada par  $xy$  con  $x \in X$  e  $y \in Y$  es una arista.

- (i) ¿Cuál es el grado de los vértices de  $X$ ?
- (ii) ¿Cuál es el grado de los vértices de  $Y$ ?
- (iii) ¿Cuántas aristas hay en  $K_{r,s}$ ?
- (iv) Describir en lenguaje coloquial la relación que representa  $K_{r,s}$ .
- (v) Demostrar que  $K_{1,s}$  es un árbol para  $s \geq 1$ .
- (vi) Demostrar que  $K_{r,s}$  no es un árbol si  $r \geq s \geq 2$ .

3 ¿Es bipartido el grafo de la figura 10.2?

## 10.2 Arista-coloraciones de grafos

Hay muchos problemas que pueden interpretarse en términos de una partición del conjunto de aristas  $E$  de un grafo, es decir, una descomposición de la forma

$$E = E_1 \cup E_2 \cup \dots \cup E_r,$$

donde  $E_1, E_2, \dots, E_r$  son disjuntos y no vacíos. Es útil describir, de manera intuitiva, una partición de este tipo en términos de una "coloración" de las aristas: las aristas de  $E_1$  reciben un color, las de  $E_2$  un color distinto, y así sucesivamente. Para denotar los colores utilizaremos letras griegas minúsculas. Habitualmente impondremos una condición a la coloración, análoga a la que imponíamos a las coloraciones de vértices.

**Definición.** Sea  $G$  un grafo y  $E$  el conjunto de aristas. Se dice que una coloración de  $E$  es una **arista-coloración** de  $G$  si dos aristas cualesquiera que comparten un vértice reciben colores distintos.

El diagrama de la figura 10.2 muestra dos coloraciones de las aristas de un mismo grafo. Una es una arista-coloración pero la otra no lo es.

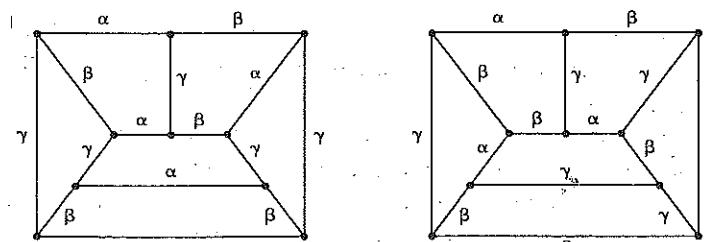


Fig. 10.2 ¿Cuál de las dos es una arista-coloración?

### Ejercicios 10.2

1 ¿Cuál es el número mínimo de colores necesario para una arista-coloración de:

- (i) el grafo completo  $K_4$ ;
- (ii) el grafo completo  $K_5$ ;
- (iii) el grafo cubo (fig. 8.12).

2 Supongamos que tenemos una arista-coloración del grafo de Petersen (fig. 8.14) que sólo utiliza tres colores. Demóstrar que cada color debe usarse dos veces en las aristas del "hexágono exterior" de la figura y que, esencialmente, sólo hay dos maneras de hacerlo. Deducir que el grafo de Petersen no admite una arista-coloración de este tipo.

3 Para cada entero positivo  $n$ , demostrar que el grafo bipartido completo  $K_{n,n}$  admite una arista-coloración con  $n$  colores.

Si  $v$  es un vértice de grado  $k$ , tenemos  $k$  aristas que contienen a  $v$ . Para que estas aristas reciban colores distintos, es evidente que hemos de disponer de al menos  $k$  colores. Por lo tanto, si  $\hat{k}$  es el grado máximo de  $G$ , se necesitan al menos  $\hat{k}$  colores para una arista-coloración de  $G$ . En general,  $\hat{k}$  no serán suficientes (ejercicio 10.2.2); sin embargo, podemos demostrar que  $\hat{k}$  colores son suficientes si  $G$  es *bipartido*.

**Teorema 10.2.** Si  $G = (X \cup Y, E)$  es un grafo bipartido, entonces el número mínimo de colores necesarios para una arista-coloración de  $G$  es igual al grado máximo de  $G$ .

**DEMOSTRACIÓN:** Lo demostraremos por inducción sobre  $m$ , el número de aristas. Si  $m = 1$ , entonces  $G$  tiene grado máximo 1 y un color es suficiente para colorear la única arista.

Supongamos el resultado cierto para un grafo con  $m$  aristas y sea  $G$  con  $m + 1$  aristas y grado máximo  $\hat{k}$ . Quitemos una arista cualquiera  $xy$  de  $G$  para obtener un grafo bipartido  $G'$  con  $m$  aristas. Como el grado máximo de  $G'$  es  $\hat{k}$  o  $\hat{k} - 1$ , la hipótesis de inducción implica que  $G'$  admite una arista-coloración con  $\hat{k}$  colores  $\alpha, \beta, \dots$  como máximo.

El grado de  $x$  en  $G'$  es  $\hat{k} - 1$  como máximo (ya que hemos eliminado  $xy$ ), con lo que debe existir un color, pongamos  $\alpha$ , que no se utiliza en

las aristas incidentes con  $x$ . Igualmente, debe existir un color  $\beta$  que no se usa en  $y$ . Si podemos elegir  $\alpha$  y  $\beta$  iguales, podemos dar este color a  $xy$  y obtener la arista-coloración de  $G$  exigida. Diremos que este es el *caso fácil*. Por lo tanto, sólo debemos considerar el caso en que  $\alpha \neq \beta$  y demostraremos que, en esta situación, podemos modificar la coloración de  $G'$  de manera que pueda aplicarse el caso fácil.

Supongamos que  $\alpha \neq \beta$  y definamos un camino  $x, y_1, x_1, y_2, x_2, \dots$  como sigue:

- (1)  $xy_1$  es la arista en  $x$  de color  $\beta$ ;
- (2) si hay una arista en  $y_1$  de color  $\alpha$ , llamémosla  $y_1x_1$ : en otro caso, acabamos;
- (3) si hay una arista en  $x_1$  de color  $\beta$ , llamémosla  $x_1y_2$ : en otro caso, acabamos;
- (4) prosigamos con aristas de colores  $\alpha$  y  $\beta$  alternativamente hasta que nos veamos forzados a acabar.

La figura 10.3 muestra el camino en cuestión. Como el grafo es finito, tarde o temprano habremos de acabar. Por otra parte, el camino no contiene el vértice  $y$ , ya que siempre llega a  $Y$  a través de aristas de color  $\beta$  y se ha definido  $\beta$  como el color que no se utilizaba en  $y$ .

A continuación modificamos la coloración de  $G'$  intercambiando los colores  $\alpha$  y  $\beta$  en el camino así construido y manteniendo los colores de las aristas restantes (figura 10.3). El resultado es el caso fácil de una arista-coloración de  $G'$ : ninguna arista en  $x$  tiene el color  $\beta$ . Para obtener la arista-coloración de  $G$ , asignamos a  $xy$  el color  $\beta$ . El principio de inducción asegura que el resultado es válido para todos los grafos.  $\square$

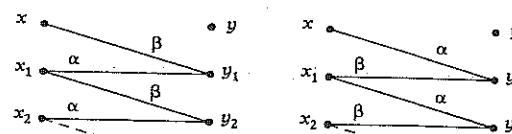


Fig. 10.3 Un camino alternado y su re-coloración.

La parte crucial de la demostración es la construcción del “camino alternado”  $x, y_1, x_1, y_2, \dots$ , que depende críticamente del carácter bipartido de  $G$ . Volveremos a utilizar esta construcción en los siguientes apartados.

### Ejercicios 10.2 (continuación)

- 4 Demostrar que el grafo de la figura 10.4 es bipartido y construir una arista-coloración con tres colores únicamente.

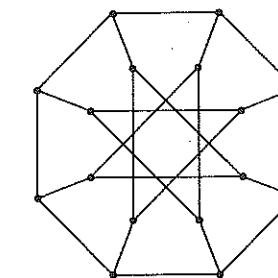


Fig. 10.4 Un grafo bipartido.

- 5 Según el ejercicio 8.2.3, el grafo  $Q_3$  formado por las esquinas y las aristas de un cubo puede representarse de la siguiente manera: los vértices son las palabras de longitud 3 en el alfabeto  $\{0, 1\}$  y las aristas unen palabras que difieren en una sola letra. Utilizar esta representación para demostrar que  $Q_3$  es bipartido y construir una arista-coloración de  $Q_3$  con sólo tres colores.

- 6 Generalizar los resultados del ejercicio 5 al grafo  $Q_k$  sustituyendo 3 por  $k$  en todas partes.

### 10.3 Arista-coloraciones y cuadrados latinos

Existe una relación sencilla entre cuadrados latinos y arista-coloraciones de grafos bipartidos. Podemos describir un cuadrado latino  $n \times n$  en términos de las filas  $f_1, f_2, \dots, f_n$ , las columnas  $c_1, c_2, \dots, c_n$  y los símbolos  $s_1, s_2, \dots, s_n$  dispuestos de tal forma que cada símbolo aparece una única vez en cada fila y cada columna. Por supuesto, en la práctica solemos usar las mismas etiquetas para las filas, las columnas y los símbolos, pero la notación anterior más general ayudará a clarificar la discusión siguiente.

Dado un cuadrado latino, por ejemplo el de la figura 10.5a, podemos usarlo para asignar colores a las aristas de un grafo bipartido completo, tal como muestra la figura 10.5b. Los vértices del grafo son las filas y columnas del cuadrado latino y a la arista  $f_i c_j$  se le asigna el "color"  $s_k$ , siendo  $s_k$  el símbolo en la fila  $f_i$  y columna  $c_j$  del cuadrado. La propiedad que define a los cuadrados latinos asegura que esta asignación de colores es, efectivamente, una arista-coloración; de esta forma, todo cuadrado latino de orden  $n$  define una arista-coloración del grafo bipartido completo  $K_{n,n}$ .

En matemáticas, a veces es provechoso adoptar un punto de vista retorcido, y esto resulta cierto en nuestro caso. En lugar de construir una coloración de  $K_{n,n}$  según el método evidente que acabamos de describir, usaremos el cuadrado latino de otro modo. Los vértices serán los símbolos  $s_1, s_2, \dots, s_n$  y las columnas  $c_1, c_2, \dots, c_n$ , y a la arista  $s_i c_j$  le asignaremos el "color"  $f_k$ , donde  $f_k$  es tal que  $s_i$  aparece en la fila  $f_k$  y columna  $c_j$  del cuadrado (figura 10.5c). De nuevo, la propiedad que define a los cuadrados latinos asegura que se trata de una arista-coloración de  $K_{n,n}$ .

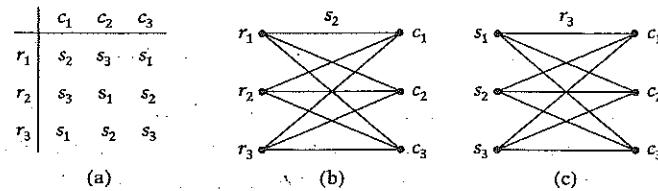


Fig. 10.5 Un cuadrado latino  $3 \times 3$  y dos arista-coloraciones de  $K_{3,3}$ .

Adoptaremos esta modificación para investigar la construcción de cuadrados latinos. Supongamos que queremos construir un cuadrado latino  $n \times n$  llenando una fila detrás de otra. Naturalmente, nos aseguramos de que cada fila contiene todos los símbolos una sola vez y de que un símbolo no aparece más de una vez en una columna. El resultado de llenar filas de este modo es un **rectángulo latino**  $m \times n$  ( $1 \leq m < n$ ). En la figura 10.6 tenemos un ejemplo de rectángulo latino  $3 \times 5$ .

Dado un rectángulo latino  $m \times n$ , ¿podremos llenar las restantes  $n - m$  filas y obtener un cuadrado latino  $n \times n$ ? Curiosamente, la respuesta es que sí, sin ninguna condición adicional sobre el rectángulo latino. En otras palabras, si construimos un cuadrado latino fila a fila entonces, siempre que

respetemos las restricciones obvias en cada paso, nunca nos quedaremos bloqueados.

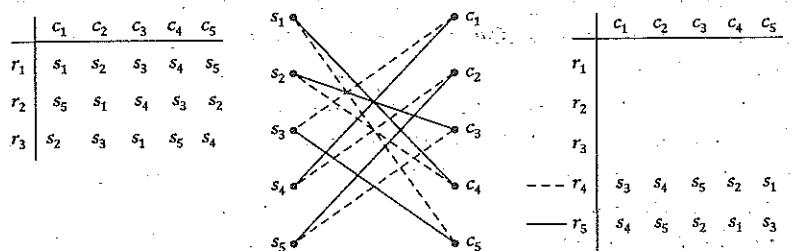


Fig. 10.6 Un rectángulo latino y cómo completarlo.

**Teorema 10.3.1.** Un rectángulo latino  $m \times n$  con  $1 \leq m < n$  siempre puede completarse hasta formar un cuadrado latino.

**DEMOSTRACIÓN:** Las  $m$  filas del rectángulo latino nos permiten, mediante la regla modificada, colorear algunas de las aristas de  $K_{n,n}$ . Sea  $E$  el conjunto de aristas que quedan por colorear; es decir,

$$E = \{s_i c_j \mid \text{el símbolo } s_i \text{ no aparece en la columna } c_j\}.$$

El grafo formado por las aristas sin colorear es  $G = (S \cup C, E)$ , donde  $S$  y  $C$  denotan, respectivamente, los conjuntos de símbolos y de columnas. El grafo  $G$  es regular de grado  $n - m$  y, por el teorema 10.2, admite una arista-coloración con  $n - m$  colores: llamémoslos  $f_{m+1}, f_{m+2}, \dots, f_n$ .

Ahora no hay más que llenar las restantes filas del cuadrado poniendo  $s_i$  en la fila  $f_k$  y columna  $c_j$  siempre que la arista  $s_i c_j$  tenga el color  $f_k$  ( $m + 1 \leq k \leq n$ ).  $\square$

En la figura 10.6 se ilustra el procedimiento para el rectángulo  $3 \times 5$ . El grafo formado por las aristas "sin colorear" tiene grado  $5 - 3 = 2$  y puede colorearse con dos colores, tal como se muestra. Entonces ya pueden llenarse las dos últimas filas.

Pasamos a investigar otro problema relativo a la construcción paso a paso de cuadrados latinos. Queremos construir un cuadrado latino  $n \times n$  utilizando los símbolos  $s_1, s_2, \dots, s_n$  y hemos llenado ya un rectángulo de tamaño  $k \times l$ , donde  $k$  y  $l$  son menores estrictamente que  $n$ . En este caso,

tanto las filas como las columnas están incompletas y, aunque hayamos llenado el rectángulo sin que ningún símbolo aparezca más de una vez en alguna fila o columna, puede resultar imposible completar el cuadrado latino. Por ejemplo, el rectángulo latino parcial  $3 \times 4$

A	C	D	E
C	E	A	B
E	A	C	D

no puede completarse en un cuadrado latino de orden 5. Para verlo, nótese que  $B$  sólo aparece una vez en el rectángulo y sólo puede aparecer tres veces más en el cuadrado (una en la última columna y dos más en las dos últimas filas); de modo que sólo hay cuatro posibles ocurrencias de  $B$  y son necesarias cinco. El siguiente teorema demuestra que la condición de que cada símbolo aparezca el suficiente número de veces en el rectángulo es una condición tanto necesaria como suficiente para poder completar.

**Teorema 10.3.2.** Sea  $R$  un rectángulo latino parcial  $m \times p$  que utiliza los símbolos  $\{s_1, s_2, \dots, s_n\}$  y sea  $n_R(s_i)$  el número de veces que aparece  $s_i$  en  $R$  ( $1 \leq i \leq n$ ). Entonces  $R$  puede completarse a un cuadrado latino  $n \times n$  si, y sólo si,

$$n_R(s_i) \geq m + p - n \quad (1 \leq i \leq n).$$

**DEMOSTRACIÓN:** Supongamos que  $R$  puede completarse. Como quedan  $n - m$  filas y  $n - p$  columnas por llenar, hay como mucho  $(n - m) + (n - p)$  ocurrencias adicionales de cada símbolo. Esto implica que

$$n_R(s_i) + (n - m) + (n - p) \geq n$$

y se obtiene la condición enunciada.

Recíprocamente, supongamos que se cumple la condición. Construimos un grafo bipartido que tenga por vértices las filas  $\{f_1, \dots, f_m\}$  y los símbolos  $\{s_1, \dots, s_n\}$ , y por aristas el conjunto

$$E = \{f_i s_j \mid \text{el símbolo } s_j \text{ no aparece en la fila } f_j\}.$$

Como cada fila de  $R$  contiene  $p$  símbolos distintos, el grado de cada vértice  $f_i$  es

$$\delta(r_i) = n - p \quad (1 \leq i \leq n).$$

Como cada símbolo  $s_j$  aparece al menos  $m + p - n$  veces en  $R$  y cada ocurrencia es en una fila distinta,  $s_j$  deja de estar en  $m - (m + p - n)$  filas como mucho. Luego,

$$\delta(s_j) \leq n - p.$$

Puesto que el grafo bipartido tiene grado máximo  $n - p$ , se sigue del teorema 10.2 que admite una arista-coloración con  $n - p$  colores, a los que llamaremos  $c_{p+1}, c_{p+2}, \dots, c_n$ .

Con esta coloración podemos completar las  $m$  filas de  $R$  poniendo  $s_j$  en la fila  $f_i$  y columna  $c_k$  si la arista  $f_i s_j$  recibe el color  $c_k$ . Tenemos ahora un rectángulo latino  $m \times n$  con las filas completas, y podemos usar el teorema 10.3.1 para completarlo hasta formar un cuadrado latino  $n \times n$ .  $\square$

### Ejercicios 10.3

- 1 Utilizar el método de las arista-coloraciones para extender el siguiente rectángulo latino a un cuadrado latino  $5 \times 5$ .

A	B	C	D	E
C	D	B	E	A
B	C	E	A	D

- 2 Hallar todos los valores de  $Q$  para los que el rectángulo  $R_1$  puede extenderse a un cuadrado latino  $6 \times 6$ . Demostrar que  $R_2$  no puede extenderse, sea cual sea el valor de  $Q$ .

$R_1 :$ <table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td>A</td><td>B</td><td>C</td><td>D</td></tr> <tr><td>F</td><td>E</td><td>A</td><td>B</td></tr> <tr><td>C</td><td>D</td><td>F</td><td>A</td></tr> <tr><td>D</td><td>A</td><td>B</td><td>Q</td></tr> </table>	A	B	C	D	F	E	A	B	C	D	F	A	D	A	B	Q	$R_2 :$ <table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td>A</td><td>B</td><td>C</td><td>D</td></tr> <tr><td>F</td><td>E</td><td>A</td><td>B</td></tr> <tr><td>B</td><td>D</td><td>F</td><td>A</td></tr> <tr><td>D</td><td>A</td><td>B</td><td>Q</td></tr> </table>	A	B	C	D	F	E	A	B	B	D	F	A	D	A	B	Q
A	B	C	D																														
F	E	A	B																														
C	D	F	A																														
D	A	B	Q																														
A	B	C	D																														
F	E	A	B																														
B	D	F	A																														
D	A	B	Q																														

- 3 Demostrar que cualquier cuadrado latino  $n \times n$  puede usarse como "esquina superior izquierda" de un cuadrado latino  $2n \times 2n$ .

## 10.4 Emparejamientos

En el ejemplo del apartado 10.1 discutimos un caso especial de la situación donde tenemos un conjunto  $X$  de personas y un conjunto  $Y$  de trabajos, y cada persona está cualificada para algunos de los trabajos. Una pregunta con evidentes implicaciones prácticas es la siguiente: ¿cómo asignar personas a los trabajos de forma que el máximo número de personas consigan trabajos para los que están cualificados?

Traduciremos la pregunta en el lenguaje de los grafos bipartidos. La relación de "estar cualificado" nos permite construir un grafo bipartido  $G = (X \cup Y, E)$  como de costumbre:  $xy$  es una arista si, y sólo si,  $x$  está cualificado para el trabajo  $y$ . Una asignación de personas a trabajos para los que están cualificados corresponde a un "emparejamiento" en  $G$ , en el sentido técnico que definimos a continuación.

**Definición.** Un **emparejamiento** en un grafo bipartido  $G = (X \cup Y, E)$  es un subconjunto  $M$  de  $E$  con la propiedad de que dos aristas de  $M$  nunca tienen un vértice en común.

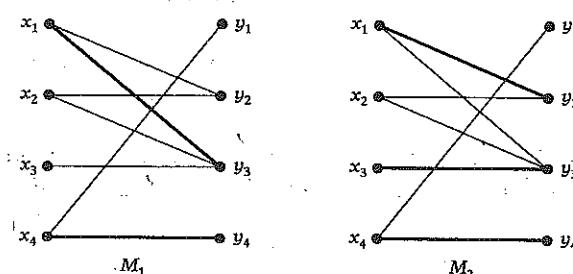


Fig. 10.7 Un emparejamiento  $M_1$  y un emparejamiento máximo  $M_2$ .

En la figura 10.7 tenemos dos emparejamientos  $M_1$  y  $M_2$  de un mismo grafo; las aristas que pertenecen a los emparejamientos se indican con trazo grueso. En la terminología de las personas y los trabajos,  $M_1$  nos da una asignación de trabajos a dos personas  $x_1$  y  $x_4$ , y  $M_2$  a las tres personas  $x_1, x_2$  y  $x_3$ . De hecho,  $M_2$  no puede mejorarse, ya que las cuatro personas en conjunto no pueden obtener trabajos para los que están cualificados. Para verlo, señalemos simplemente que las tres personas  $\{x_1, x_2, x_3\}$  están

cualificadas colectivamente sólo para los trabajos  $y_2$  e  $y_3$ , de modo que alguna de las tres ha de quedar excluida cuando se asignen los trabajos.

Daremos que un emparejamiento  $M$  es un **emparejamiento máximo** de  $G = (X \cup Y, E)$  si ningún otro emparejamiento tiene un cardinal mayor. Si  $|M| = |X|$  (todas las personas consiguen un trabajo), diremos que  $M$  es un **emparejamiento completo**. En el ejemplo anterior,  $M_2$  es máximo pero no completo.

El primer paso en el estudio de los emparejamientos es decidir cuándo es posible un emparejamiento completo. En la discusión de la figura 10.7, al observar que tres personas estaban cualificadas colectivamente sólo para dos trabajos, hemos hallado una condición necesaria. Más en general, si  $G = (X \cup Y, E)$  y  $A$  es un subconjunto de  $X$ , sea

$$T(A) = \{y \in Y \mid xy \in E \text{ para algún } x \in A\},$$

de modo que  $T(A)$  es el conjunto de trabajos para los que las personas de  $A$  están cualificadas colectivamente. La observación sobre la figura 10.7 significa que si  $|T(A)| < |A|$ , entonces alguien de  $A$  quedará excluido. Si existe un emparejamiento completo, entonces debe cumplirse que  $|T(A)| \geq |A|$  para todo  $A \subseteq X$ . Esta es la **condición de Hall**, en honor del matemático Philip Hall que estudió un problema similar en 1935 (véase apartado 10.6).

El teorema fundamental sobre emparejamientos perfectos afirma que la condición de Hall es suficiente, además de necesaria.

**Teorema 10.4.** El grafo bipartido  $G = (X \cup Y, E)$  admite un emparejamiento completo si, y sólo si, se cumple la condición de Hall, es decir,

$$|T(A)| \geq |A| \quad \text{para todo } A \subseteq X.$$

**DEMOSTRACIÓN:** Supongamos que existe un emparejamiento perfecto. Para todo  $A \subseteq X$  los vértices de  $Y$  emparejados con los de  $A$  forman un subconjunto  $T(A)$  de tamaño  $|A|$ . Así pues,  $|T(A)| \geq |A|$ .

Recíprocamente, supongamos que se cumple la condición de Hall. Dado un emparejamiento  $M$  con  $|M| < |X|$ , mostraremos cómo construir un emparejamiento  $M'$  con  $|M'| = |M| + 1$ .

Sea  $x_0$  un vértice cualquiera no emparejado por  $M$ . Como  $|T\{x_0\}| \geq |\{x_0\}| = 1$ , existe al menos una arista  $x_0y_1$ . Si  $y_1$  no está emparejado, podemos añadir  $x_0y_1$  a  $M$  y obtenemos el  $M'$  buscado.

Si  $y_1$  está emparejado, pongamos con  $x_1$ , entonces

$$|T\{x_0, x_1\}| \geq |\{x_0, x_1\}| = 2$$

y ha de existir otro vértice  $y_2$  además de  $y_1$  adyacente a  $x_0$  o  $x_1$ . Si  $y_2$  no está emparejado, acabamos; si  $y_2$  está emparejado, pongamos con  $x_2$ , repetimos el argumento y seleccionamos un nuevo vértice  $y_3$  adyacente a alguno de entre  $x_0, x_1$  y  $x_2$ . Si proseguimos de este modo, al ser  $G$  finito, eventualmente acabaremos en un vértice  $y_r$  no emparejado.

Cada vértice  $y_i$  ( $1 \leq i \leq r$ ) es adyacente al menos a alguno de los  $x_0, x_1, \dots, x_{i-1}$ . Si deshacemos los pasos, tendremos un camino

$$y_r, x_s, y_t, x_u, \dots, y_w, x_0$$

en el que las aristas  $x_i y_i$  son de  $M$  y las aristas alternadas no lo son. Construimos un nuevo emparejamiento  $M'$  tal que las aristas  $x_i y_i$  del camino no estén en  $M'$ , pero sí las aristas alternadas. Como las aristas de los extremos  $y_r x_s$  e  $y_w x_0$  son ambas de  $M'$ , tenemos que  $|M'| = |M| + 1$ , tal como queríamos.  $\square$

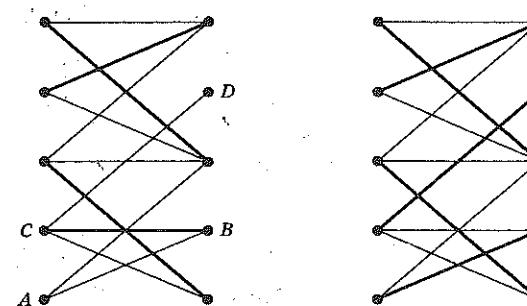


Fig. 10.8 Un camino alternado  $ABCD$  y el resultado del cambio.

La idea clave en la demostración es la construcción de un camino cuyas aristas estén, alternativamente, en  $M$  y fuera de  $M$ . En general, sea  $G = (X \cup Y, E)$  un grafo bipartido y  $M$  un emparejamiento de  $G$ . Diremos que el camino

$$x_0, y_1, x_1, y_2, x_2, \dots, x_{k-1}, y_k$$

es un **camino alternado** (para  $M$ ) si las aristas  $y_i x_i$  son de  $M$ , las aristas  $x_{i-1} y_i$  no son de  $M$  ( $1 \leq i \leq k$ ), y  $x_0$  e  $y_k$  no pertenecen a ninguna arista de  $M$ . Nótese que la primera y última aristas no son de  $M$ , con lo que el camino tiene una arista menos en  $M$  que en el complementario de  $M$ . La demostración del teorema nos hace ver que si se satisface la condición de Hall y  $M$  es un emparejamiento incompleto, entonces existe un camino alternado para  $M$ . Modificando el estado de las aristas de este camino se obtiene un nuevo emparejamiento  $M'$  con una arista más.

La idea no es útil únicamente para la demostración, sino que es un instrumento práctico para la construcción de emparejamientos. En la figura 10.8, el camino  $ABCD$  es alternado y, cambiando las aristas de este camino, puede verse que se obtiene un emparejamiento completo.

En el apartado 10.5 explicaremos cómo este enfoque proporciona un algoritmo para hallar un emparejamiento máximo en un grafo bipartido cualquiera.

#### Ejercicios 10.4

- 1 Utilizar la condición de Hall para demostrar que el grafo de la figura 10.9 no admite ningún emparejamiento completo.
- 2 Sea  $M$  el emparejamiento indicado en trazo grueso en la figura 10.9
  - (i) Hallar un camino alternado para  $M$  que empiece en  $x_2$ .
  - (ii) Utilizarlo para construir un emparejamiento  $M'$  con  $|M'| = 4$ .
  - (iii) Comprobar que no hay ningún camino alternado para  $M'$ .
  - (iv) ¿Es  $M'$  un emparejamiento máximo?

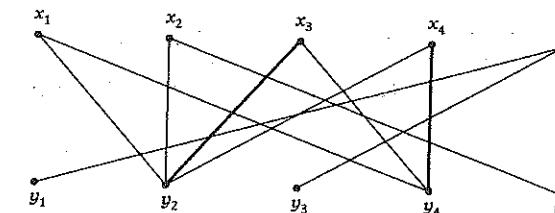


Fig. 10.9 Ilustración del ejercicio 10.4.2.

- 3 Supongamos que cada elemento de un conjunto de personas tiene una lista de  $k$  libros que desea tomar prestados de la biblioteca. Supongamos

también que cada libro aparece en  $k$  listas exactamente. Demostrar que todos ellos pueden tomar prestado un libro de su lista al mismo tiempo. [Indicación: utilizar el resultado establecido en el ejemplo del apartado 10.1.]

## 10.5 Emparejamientos máximos

En general, un grafo bipartido no tendrá un emparejamiento completo. Esta observación nos lleva a nuestra pregunta original de hallar el tamaño máximo de un emparejamiento. En la terminología personas-trabajos, intentamos hallar la asignación en la que el máximo número de personas obtiene trabajos adecuados. La solución a este problema es, de hecho, una deducción bastante sencilla del resultado sobre emparejamientos completos, el teorema 10.4.

El punto crucial es la observación de que, si un conjunto de personas  $A$  están cualificadas colectivamente para un conjunto  $T(A)$  de trabajos y  $|A| > |T(A)|$ , alguien no obtendrá un trabajo adecuado. De hecho, al menos  $|A| - |T(A)|$  personas no lo obtendrán.

**Definición.** La deficiencia  $d$  de un grafo bipartido  $G = (X \cup Y, E)$  se define como

$$d = \max_{A \subseteq X} \{|A| - |T(A)|\}.$$

Nótese que el conjunto vacío  $\emptyset$  es un subconjunto de  $X$  y  $|\emptyset| = |T(\emptyset)| = 0$ , de modo que  $d \geq 0$  en cualquier caso. El teorema 10.4 afirma que  $G$  admite un emparejamiento completo si, y sólo si,  $d = 0$ ; el siguiente teorema trata del tamaño de un emparejamiento máximo en el caso general.

**Teorema 10.5.1.** El tamaño de un emparejamiento máximo  $M$  en un grafo bipartido  $G = (X \cup Y, E)$  es

$$|M| = |X| - d,$$

donde  $d$  es la deficiencia de  $G$ .

**DEMOSTRACIÓN:** Por definición de  $d$ , existe un conjunto  $A_0 \subseteq X$  tal que  $|A_0| - |T(A_0)| = d$ . En cualquier emparejamiento, al menos  $d$  elementos

de  $A_0$  no se emparejan; con lo que  $|M| \leq |X| - d$ . Hemos de demostrar que existe un emparejamiento de tamaño  $|X| - d$ .

Sea  $D$  un nuevo conjunto de tamaño  $d$  y sea  $G^*$  el grafo  $(X^* \cup Y^*, E^*)$  definido por

$$X^* = X, \quad Y^* = Y \cup D, \quad E^* = E \cup K,$$

donde  $K$  es el conjunto de todas las posibles aristas que unen  $X$  con  $D$ . El conjunto de los vértices  $T^*(A)$  adyacentes a un subconjunto  $A$  de  $X$  en  $G^*$  es  $D \cup T(A)$  y, por definición de  $d$ , tenemos que

$$|T^*(A)| - |A| = d + |T(A)| - |A| \geq 0.$$

Por lo tanto,  $G^*$  cumple la condición de Hall y admite un emparejamiento completo  $M^*$ . Si eliminamos de  $M^*$  las  $d$  aristas que tienen un vértice en  $D$ , se obtiene el emparejamiento buscado de  $G$ .  $\square$

El teorema 10.5.1 no nos dice cómo hallar un emparejamiento-máximo. De hecho, no es ni siquiera la base de un buen método práctico para hallar el tamaño de un emparejamiento máximo, ya que para calcular  $d$  deberíamos examinar todos los  $2^{|X|}$  subconjuntos de  $X$ .

Un enfoque más práctico se basa en el hecho de que si tenemos un camino alternado para un emparejamiento  $M$ , podemos construir un emparejamiento  $M'$  mejor. Para que esta idea funcione, necesitamos el siguiente resultado.

**Teorema 10.5.2.** Si un emparejamiento  $M$  del grafo bipartido  $G$  no es máximo, entonces  $G$  contiene un camino alternado para  $M$ .

**DEMOSTRACIÓN:** Sea  $M^*$  un emparejamiento máximo y  $F$  el conjunto de las aristas que están en  $M$  o en  $M^*$ , pero no en ambos ( $F$  es la “diferencia simétrica” de  $M$  y  $M^*$ ). Las aristas de  $F$  y los vértices que contienen forman un grafo en el que cada vértice tiene grado 1 o 2, con lo que los componentes de este grafo son caminos y ciclos. En cada camino o ciclo, las aristas de  $M$  alternan con las que no son de  $M$  y, por lo tanto, en cada ciclo el número de aristas en  $M$  es igual al número de las que no son de  $M$ . Al ser  $|M^*| > |M|$ , debe existir al menos un componente que sea un camino: este es el camino alternado para  $M$ .  $\square$

Basándonos en el teorema 10.5.2, podemos delinear una estrategia para hallar un emparejamiento máximo.

- (1) Empezar con un emparejamiento cualquiera (una sola arista basta).
- (2) Buscar un camino alternado para  $M$ .
- (3) Si se ha hallado un camino alternado, construir un emparejamiento  $M'$  mejor en la forma habitual y volver a (2) con  $M'$  en lugar de  $M$ .
- (4) Si no se ha hallado un camino alternado, acabar:  $M$  es un emparejamiento máximo.

Para la búsqueda de un camino alternado puede utilizarse un procedimiento BEA modificado. Elegimos un vértice  $x_0$  no emparejado y construimos un árbol de caminos alternados "parciales" empezando en  $x_0$  de la manera siguiente.

- (1) En el nivel 1 ponemos todos los vértices  $y_1, y_2, \dots, y_k$  adyacentes a  $x_0$ . Si alguno de estos vértices  $y_i$  no tiene pareja, acabamos:  $x_0y_i$  es un camino alternado.
  - (2) Si todos los vértices en el nivel 1 están emparejados, se ponen en el nivel 2 los vértices  $x_1, x_2, \dots, x_k$  con los que hacen pareja.
  - (3) En el nivel 3 ponemos todos los nuevos vértices adyacentes a los vértices del nivel 2. Si alguno de ellos no está emparejado, acabamos: el camino que lleva de este vértice a  $x_0$  es un camino alternado.
  - (4) Si todos los vértices en el nivel 3 están emparejados, se ponen en el nivel 4 los vértices con los que hacen pareja.
- ... y así sucesivamente.

Sólo queda señalar que esta construcción puede detenerse por no haber nuevos vértices que poner en un nivel impar. Cuando esto ocurre no hay ningún camino alternado que empiece en el vértice elegido  $x_0$ . Sin embargo, para asegurarnos de que en  $G$  no existe ningún camino alternado en absoluto, hay que repetir el proceso para todos los vértices sin pareja de  $X$ .

**Ejemplo.** Sea  $G = (X \cup Y, E)$  el grafo bipartido con  $X = \{x_1, x_2, x_3, x_4, x_5\}$ ,  $Y = \{y_1, y_2, y_3, y_4, y_5\}$  y  $E$  especificado en la tabla 10.5.1. Sea  $M$  el emparejamiento  $\{x_1y_3, x_2y_1, x_3y_5, x_4y_4\}$ . Construir el árbol de caminos alternados parciales con raíz en  $x_5$  y hallar un emparejamiento completo a partir de él.

$x_1$	$x_2$	$x_3$	$x_4$	$x_5$
$y_1$	$y_1$	$y_1$	$y_2$	$y_3$
$y_3$	$y_3$	$y_3$	$y_4$	$y_4$
		$y_5$	$y_5$	

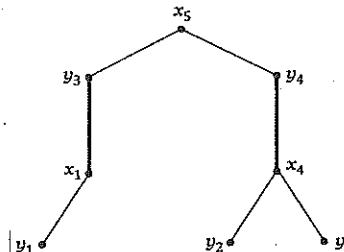


Fig. 10.10 El árbol de caminos alternados parciales con raíz en  $x_5$ .

**SOLUCIÓN:** El árbol es el que muestra la figura 10.10. En el nivel 3 vemos que  $y_2$  no está emparejado, con lo que  $x_5y_4x_4y_2$  es un camino alternado. Cambiando el estado de las aristas obtenemos un emparejamiento completo  $\{x_1y_3, x_2y_1, x_3y_5, x_4y_2, x_5y_4\}$ .

### Ejercicios 10.5

1 Sea  $G = (X \cup Y, E)$  el grafo bipartido con  $X = \{a, b, c, d, e\}$ ,  $Y = \{v, w, x, y, z\}$  y  $E = \{av, ax, bv, bz, cw, cy, cz, dy, dz, ez\}$ . Utilizar el método algorítmico para hallar un emparejamiento completo en  $G$ , empezando con  $M = \{av, bz, cy\}$ .

2 Supongamos que  $G = (X \cup Y, E)$  el grafo descrito en la figura 10.7. ¿Para qué 3-subconjuntos de  $X$  es posible hallar un emparejamiento completo de  $G$  tal que los tres vértices dados tengan pareja?

3 Sea que  $G = (X \cup Y, E)$  es un grafo bipartido con  $|X| = |Y| = n$ . Demostrar que si  $\delta$  es el grado mínimo de  $G$ , entonces

$$|A| - |T(A)| \leq n - \delta, \quad \text{para todo } A \subseteq X.$$

Deducir que si  $|E| > (m - 1)n$ , entonces  $G$  admite un emparejamiento con al menos  $m$  aristas.

## 10.6 Transversales de familias de conjuntos finitos

El Departamento de Matemáticas de la Universidad de Folornia funciona por comisiones. El Departamento sólo tiene seis miembros (Profesor McBrain, Dr. Angst, Dr. Blott, Dr. Chunner, Dr. Dodder y Dr. Elder) y se han organizado en cuatro comisiones:

- Docencia: {McBrain, Angst},
- Administración {McBrain, Blott},
- Investigación: {McBrain, Angst, Blott},
- Aparcamiento: {Chunner, Dodder, Elder}.

Se ha decidido que cada comisión nombre un representante para la nueva Comisión de Comisiones del Departamento. Nadie puede representar más de una comisión. ¿Puede hacerse?

Dada la composición de las comisiones, hay varias maneras de seleccionar representantes distintos: una manera es seleccionar a Angst, Blott, McBrain y Chunner como representantes de las respectivas comisiones en el orden dado anteriormente. Sin embargo, si la comisión de Aparcamiento contuviera sólo a Angst y Blott, entonces la selección sería imposible (¿por qué?).

La versión general de este problema se expresa mejor con la notación de familias de conjuntos del apartado 5.1. Tenemos una familia

$$\mathcal{F} = \{S_i \mid i \in I\}$$

de conjuntos, no necesariamente distintos, y hemos de elegir representantes  $s_i$  ( $i \in I$ ) tales que

$$s_i \in S_i \quad \text{e} \quad i \neq j \Rightarrow s_i \neq s_j.$$

Un conjunto de representantes distintos de esta forma se conoce habitualmente como un **transversal** de  $\mathcal{F}$ . El problema básico es hallar condiciones que aseguren que una familia dada  $\mathcal{F}$  tiene un transversal.

De hecho, el problema no es más que una forma disfrazada del problema de hallar una condición suficiente para la existencia de un emparejamiento completo en un grafo bipartido. Para ver que es así, construyamos el grafo bipartido que tiene por partes los nombres de los conjuntos y los elementos de los conjuntos, respectivamente, y cuyas aristas indican qué

elementos pertenecen a qué conjuntos (la figura 10.11 ilustra la situación en la Universidad de Folornia).

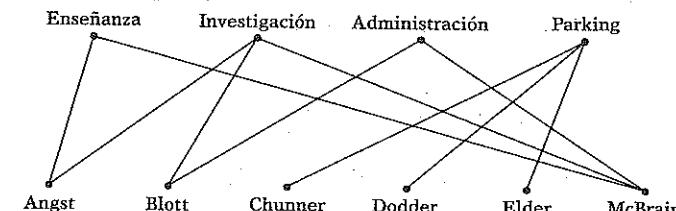


Fig. 10.11 Democracia en la Universidad de Folornia.

En general, definimos  $G = (X \cup Y, E)$  como sigue:

$$\begin{aligned} X &= I && (\text{los nombres de los conjuntos}), \\ Y &= \bigcup_{i \in I} S_i && (\text{la unión de los conjuntos}), \end{aligned}$$

y ponemos la arista  $iy$  en  $E$  siempre que  $y$  sea un elemento de  $S_i$ . Entonces un transversal de  $\mathcal{F}$  es simplemente un emparejamiento completo de  $G$ ; si  $y_i$  representa a  $S_i$ , la arista que une  $i$  con  $y_i$  está en el emparejamiento. Ahora podemos expresar fácilmente la condición de Hall en la terminología de transversales. Un subconjunto  $H$  de  $I$  no es más que una subfamilia de conjuntos de  $\mathcal{F}$  y  $T(H)$  la reunión de todos estos subconjuntos, es decir,

$$\bigcup_{i \in H} S_i.$$

Si traducimos la condición de Hall a este lenguaje obtenemos la siguiente versión del teorema 10.4.

**Teorema 10.6.** *La familia finita de conjuntos finitos*

$$\mathcal{F} = \{S_i \mid i \in I\}$$

tiene un transversal si, y sólo si,

$$\left| \bigcup_{i \in H} S_i \right| \geq |H| \quad \text{para todo } H \subseteq I. \quad \square$$

Una forma útil de expresar la condición, es decir que cualesquiera  $k$  de los conjuntos han de tener al menos  $k$  elementos colectivamente ( $k \geq 1$ ).

### Ejercicios 10.6

- 1 Sea  $\mathcal{F}$  la familia de los conjuntos  $\{a, b, l, e\}$ ,  $\{l, e, s, t\}$ ,  $\{s, t, a, b\}$ ,  $\{s, a, l, e\}$ ,  $\{t, a, l, e\}$  y  $\{s, a, l, t\}$ . Hallar un transversal de  $\mathcal{F}$ .
- 2 Demostrar que la familia del ejercicio 1 no tiene ningún transversal en el que los tres primeros conjuntos estén representados por  $e, l$  y  $s$ , respectivamente.
- 3 Demostrar que la familia de conjuntos  $\{a, m\}$ ,  $\{a, r, e\}$ ,  $\{m, a, r, e\}$ ,  $\{m, a, s, t, e, r\}$ ,  $\{m, e\}$  y  $\{r, a, m\}$  no tiene ningún transversal, demostrando explícitamente que no se cumple la condición de Hall.
- 4 Sea  $\{X_1, X_2, \dots, X_n\}$  una familia de conjuntos y sea  $X$  la unión de todos ellos. Demostrar que si la familia tiene un transversal entonces, dado un  $x$  de  $X$  cualquiera, existe un transversal que contiene a  $x$ .

### 10.7 Ejercicios diversos

- 1 Demostrar que si un grafo regular de grado 3 tiene un ciclo hamiltoniano, entonces admite una arista-coloración con tres colores.
- 2 En una fiesta hay  $n$  matrimonios. Dos personas conversan sólo si son de sexo opuesto y no están casadas. Representar esta situación mediante un grafo bipartido y demostrar explícitamente que el grafo admite una arista-coloración que utiliza  $n - 1$  colores.
- 3 Sea  $S = \{a, d, i, m, o, r, s, t\}$  y sea  $\mathcal{F}$  la familia de los subconjuntos  $\{r, o, a, d\}$ ,  $\{r, i, o, t\}$ ,  $\{r, i, d, s\}$ ,  $\{s, t, a, r\}$ ,  $\{m, o, a, t\}$ ,  $\{d, a, m, s\}$  y  $\{m, i, s, t\}$ . Demostrar que cualquier 7-subconjunto de  $S$  es un transversal de  $\mathcal{F}$ .
- 4 Sea  $X$  la unión de la familia de conjuntos  $\{X_1, X_2, \dots, X_n\}$ , y sean  $x$  e  $y$  elementos de  $X$ . Demostrar mediante un ejemplo que la familia puede tener un transversal, pero no un transversal que contenga a  $x$  y a  $y$ .
- 5 Representemos los vértices del grafo ciclo  $C_{14}$  mediante los elementos de  $\mathbb{Z}_{14}$  y sea  $G$  el grafo que se obtiene de  $C_{14}$  añadiendo las aristas  $\{i, i + 5\}$  para  $i = 0, 2, 4, 6, 8, 10, 12$  ( $G$  se conoce como el grafo de Heawood). Demostrar que  $G$  es bipartido y construir una arista-coloración de  $G$  que use el mínimo número de colores posible.

6 Se tienen cinco comisiones:  $C_1 = \{a, c, e\}$ ,  $C_2 = \{b, c\}$ ,  $C_3 = \{a, b, d\}$ ,  $C_4 = \{d, e, f\}$  y  $C_5 = \{e, f\}$ . Cada comisión ha de enviar un representante al Congreso Anual de Comisiones;  $C_1$  quiere nombrar a  $e$ ,  $C_2$  quiere nombrar a  $b$ ,  $C_3$  quiere nombrar a  $a$  y  $C_4$  quiere nombrar a  $f$ .

- (i) Demostrar que no es posible respetar los deseos de  $C_1, C_2, C_3$  y  $C_4$ .
- (ii) Usar el método del camino alternado y el grafo asociado para hallar un sistema completo de representantes distintos.
- (iii) ¿Es posible construir un sistema completo de representantes distintos si la comisión  $C_1$  se niega a cambiar su nominación?

7 Un grafo bipartido  $G = (V \cup W, E)$  puede representarse mediante una matriz  $B = (b_{ij})$  de tamaño  $m \times n$ , donde  $m = |V|, n = |W|$  y

$$b_{ij} = \begin{cases} 1 & \text{si } \{v_i, w_j\} \in E; \\ 0 & \text{en otro caso.} \end{cases}$$

Describir, en términos de operaciones sobre  $B$ , el algoritmo del camino alternado para hallar un emparejamiento máximo.

8 Decimos que un *paso* del algoritmo del camino alternado para hallar un emparejamiento máximo comprende las operaciones necesarias para aumentar el emparejamiento parcial en una arista. Demostrar que si  $G = (V \cup W, E)$  es tal que  $\max(|V|, |W|) = n$ , el número de operaciones necesarias en cada paso es  $O(n^2)$ . Deducir que la eficiencia del algoritmo es  $O(n^3)$ .

9 Demostrar que el grafo completo  $K_{2m}$  admite una arista-coloración que utiliza  $2m - 1$  colores.

10 En “geometría proyectiva”, se dice que dos triángulos  $A_1B_1C_1$  y  $A_2B_2C_2$  están en perspectiva si  $A_1A_2, B_1B_2$  y  $C_1C_2$  tienen un punto común  $X$ . El teorema de Desargues afirma que si los triángulos están en perspectiva, los puntos  $P$  (intersección de  $A_1B_1$  y  $A_2B_2$ ),  $Q$  (intersección de  $B_1C_1$  y  $B_2C_2$ ) y  $R$  (intersección de  $A_1C_1$  y  $A_2C_2$ ) son colineales.

Sea  $G$  el grafo bipartido cuyos vértices representan los diez puntos y las diez rectas que intervienen en el teorema y en el que dos vértices son adyacentes si, y sólo si, representan un punto y una recta que contiene el punto. Demostrar que  $G$  es hamiltoniano y construir una arista-coloración de  $G$  con sólo tres colores.

11 Sea  $B$  el grafo utilizado en la demostración del teorema 10.3.1 para demostrar que todo rectángulo latino  $r \times n$  puede completarse. Demostrar que si  $r = n - 2$ , el rectángulo puede completarse de una manera esencialmente única si, y sólo si,  $B$  es conexo.

12 Sean  $p, q$  y  $n$  enteros tales que  $1 \leq p \leq n$  y  $1 \leq q \leq n$ , y sean  $s_1, s_2, \dots, s_n$  símbolos. Sea  $M$  una tabla  $n \times n$  de celdas tal que en cada una de las  $p$  primeras filas  $q$  celdas están ocupadas por un símbolo y las restantes  $n^2 - pq$  celdas están

vacías. Supongamos también que ningún símbolo aparece más de una vez en una fila o columna. Demostrar lo siguiente: podemos completar un cuadrado latino asignando símbolos a las restantes celdas si, y sólo si, el número  $N(i)$  de celdas ocupadas en la columna  $i$  satisface

$$N(i) \geq p + q - n \quad (1 \leq i \leq n).$$

13 Demostrar que la siguiente familia infinita de conjuntos cumple la condición de Hall pero no tiene ningún transversal.

$$\begin{aligned} X_0 &= \{1, 2, 3, \dots\}, \quad X_1 = \{1\}, \quad X_2 = \{1, 2\}, \dots \\ &\dots \quad X_i = \{1, 2, \dots, i\}, \dots \end{aligned}$$

14 Sea  $X$  la unión de la familia de conjuntos  $\{X_1, X_2, \dots, X_n\}$  y supongamos que la familia tiene un transversal. Demostrar que el transversal es único si, y sólo si,  $|X| = n$ .

15 Se tienen dos particiones de un conjunto  $X$ :

$$X = A_1 \cup A_2 \cup \dots \cup A_n = B_1 \cup B_2 \cup \dots \cup B_n.$$

Un **transversal simultáneo** es un conjunto  $\{x_1, x_2, \dots, x_n\}$  de elementos de  $X$  distintos tal que cada parte de las dos particiones contiene algún  $x_i$ . Demostrar que existe un transversal simultáneo si, y sólo si,  $k$  de las partes  $A_i$  nunca están contenidas en menos de  $k$  de las partes  $B_j$  ( $1 \leq k \leq n-1$ ).

16 Sean  $m$  y  $n$  enteros con  $m \geq n$ . Construir una arista-coloración explícita de  $K_{m,n}$  con  $m$  colores.

17 Demostrar que si un grafo regular de grado  $k$  tiene un número impar de vértices, no admite una arista-coloración con  $k$  colores.

18 Sea  $G$  un grafo con  $n$  vértices,  $m$  aristas y grado máximo  $\hat{k}$ . Demostrar que si  $m > \hat{k}\lfloor n/2 \rfloor$ , entonces  $G$  no admite una arista-coloración con  $\hat{k}$  colores.

19 Un **recubrimiento por vértices** de un grafo  $G$  es un conjunto de vértices  $R$  tal que cada arista de  $G$  contiene al menos un vértice de  $R$ . Demostrar que si  $G$  es bipartido, el tamaño de un emparejamiento máximo es igual al tamaño de un recubrimiento por vértices mínimo.

20 Demostrar que existen al menos  $(n-r)!$  maneras de añadir una nueva fila a un rectángulo latino  $r \times n$  de manera que se mantenga la propiedad latina ( $1 \leq r \leq n-1$ ).

## 11 Digrafos, redes y flujos

### 11.1 Digrafos

Un **digrafo** (o bien **grafo dirigido**) consta de un conjunto finito  $V$ , a cuyos elementos llamaremos **vértices**, y un subconjunto  $A$  de  $V \times V$ , a cuyos elementos llamaremos **arcos**. Utilizaremos la notación  $D = (V, A)$  para el digrafo  $D$  definido de este modo. Al igual que sucedía con los grafos, los digrafos pueden representarse mediante figuras: la única diferencia es que un arco es un par ordenado  $(v, w)$ , mientras que una arista es un par no ordenado  $\{v, w\}$ . Al dibujar un digrafo, indicaremos el orden de los vértices  $v$  y  $w$  mediante una flecha que apunte de  $v$  a  $w$  en la línea que representa el arco  $(v, w)$  (ver figura 11.1). Si  $(v, v)$  es un arco, lo indicaremos dibujando un lazo en  $v$  (la dirección de la flecha es irrelevante). Si tanto  $(v, w)$  como  $(w, v)$  son arcos, dibujaremos dos líneas que unan  $v$  y  $w$  con flechas en las direcciones adecuadas.

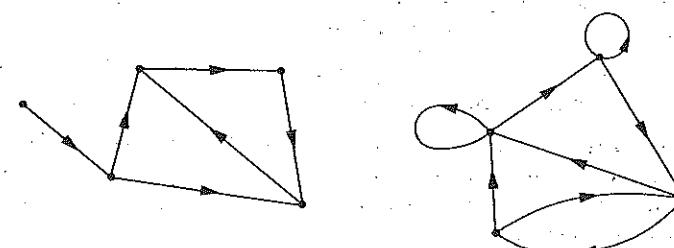


Fig. 11.1 Dos digrafos.

Formalmente, un digrafo no es más que otra manera de describir una relación  $R$  entre elementos de un *mismo* conjunto. En lugar de decir que

$v$  está relacionado con  $w$  en la relación  $R$ , decimos que  $(v, w)$  es un arco del digrafo que tienen  $R$  por conjunto de arcos (hay que distinguir esto último de la representación bipartida introducida en el apartado 10.1, que es relevante sólo si  $R$  es una relación entre conjuntos *disjuntos*). Las propiedades de las relaciones pueden traducirse fácilmente en propiedades de digrafos. Por ejemplo, si una relación es simétrica, el digrafo correspondiente tiene la propiedad de que los arcos (salvo los lazos) ocurren en pares: o bien tanto  $(v, w)$  como  $(w, v)$  son arcos, o bien ninguno de ellos lo es.

Las definiciones de recorrido, camino y ciclo se trasladan de grafos a digrafos sin dificultad. Así, un **recorrido dirigido** en un digrafo  $D = (V, A)$  es una sucesión de vértices  $v_1, v_2, \dots, v_k$  con la propiedad de que  $(v_i, v_{i+1})$  es de  $A$  para  $1 \leq i \leq k - 1$ . Un recorrido dirigido es un **camino dirigido** si los vértices son distintos, y es un **ciclo dirigido** si los vértices son distintos salvo que  $v_1 = v_k$ .

Un ejemplo sencillo que ilustra estas ideas es el análisis de un campeonato de liga, una competición en la que cada equipo juega contra todos los demás (una sola vez) y en la que cada partido tiene un resultado definido:  $x$  gana a  $y$ , o  $y$  gana a  $x$ . En el digrafo correspondiente, los vértices representan a los equipos y, para cada par de vértices distintos  $x$  e  $y$ , hay exactamente uno de los arcos  $(x, y)$  o  $(y, x)$ , según que  $x$  gane a  $y$  o que  $y$  gane a  $x$ . Este digrafo puede pensarse como un grafo completo, en el que cada arista ha sido transformada en un arco introduciendo una flecha en alguno de los dos sentidos. Debido a la interpretación en términos de campeonatos de liga, un digrafo de este tipo se dice que es un **campeonato**.

Un campeonato de liga es muy divertido, pero no es particularmente útil para decidir los méritos relativos de cada equipo (estamos suponiendo que no hay ningún tipo de asignación de puntos por ganar un partido). Ocurre con frecuencia que  $x$  gana a  $y$ ,  $y$  gana a  $z$ , pero  $z$  gana a  $x$ . De este modo tenemos un ciclo dirigido  $(x, y, z)$  de los tres equipos en el que cada uno gana y es ganado por alguno de los restantes.

En vista de esto, el siguiente resultado puede parecer sorprendente a primera vista.

**Teorema 11.1.** *En cualquier campeonato existe un camino dirigido que contiene todos los vértices.*

**DEMOSTRACIÓN:** Veremos que cualquier camino dirigido  $y_1, y_2, \dots, y_l$  que no contenga todos los vértices puede extenderse con la adjunción de un nuevo vértice. De esta forma, podemos empezar por un arco cualquiera  $(y_1, y_2)$  y extender sucesivamente hasta llegar a un camino dirigido que contiene todos los vértices.

Sea  $z$  un vértice que no está en camino dirigido  $y_1, y_2, \dots, y_l$ . Si  $(z, y_1)$  es un arco, insertamos  $z$  al principio. Si no lo es, al tratarse de un campeonato,  $(y_1, z)$  ha de ser un arco. Sea  $r$  el mayor entero tal que  $(y_1, z), (y_2, z), \dots, (y_r, z)$  son arcos. Si  $r < l$ , tenemos los arcos  $(y_r, z)$  y  $(z, y_{r+1})$ , y podemos insertar  $z$  entre  $y_r$  e  $y_{r+1}$ . Si  $r = l$ , añadimos  $z$  al final.  $\square$

El camino dirigido que asegura el teorema 11.1 tiene la deseable propiedad de que ordena los “competidores” en una sucesión tal que  $y_1$  gana a  $y_2$ ,  $y_2$  gana a  $y_3$ , etc. De todas maneras, esto no significa que cada equipo gane a todos los que le siguen en la sucesión, ya que (por ejemplo)  $y_1$  puede perder ante  $y_3$ .

### Ejercicios 11.1

- 1 En la lista de adyacencias de un *digrafo* ponemos  $y$  en la columna  $x$  siempre que  $(x, y)$  sea un arco. Dibujar el digrafo que tiene por lista de adyacencias

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>
<i>d</i>	<i>a</i>	<i>b</i>	<i>b</i>	<i>f</i>	<i>a</i>
<i>e</i>			<i>c</i>		
			<i>e</i>		

Hallar un camino dirigido de  $c$  a  $f$  y un ciclo dirigido que empiece y acabe en  $d$ .

- 2 En la tabla 11.1.1 hay un  $+$  en la fila  $i$  y columna  $j$  si  $i$  gana a  $j$ , y un  $-$  si  $j$  gana a  $i$ . Hallar un camino dirigido que contenga todos los vértices del campeonato.

Tabla 11.1.1

	<i>j</i>								
<i>i</i>	1	2	3	4	5	6	7	8	9
1	+	+	-	-	+	-	+	-	-
2	-	+	+	-	+	+	-	-	-
3	+	-	-	-	+	-	-	+	-
4	-	-	+	-	-	+	-	-	-
5	-	-	-	-	+	-	-	-	-
6	-	-	-	-	+	-	-	-	-
7	-	-	-	-	-	+	+	-	-
8	-	-	-	-	-	-	-	-	-

3 Escribir un programa para hallar un camino dirigido que pase por todos los vértices de un campeonato, utilizando la demostración del teorema 11.1.

4 El **grado de salida**  $\delta^+(v)$  de un vértice en un dígrafo es el número de arcos de la forma  $(v, w)$  y el **grado de entrada**  $\delta^-(v)$  es el número de arcos de la forma  $(x, v)$ . Demostrar que, en general,

$$\sum_{v \in V} \delta^-(v) = \sum_{v \in V} \delta^+(v)$$

y, si el dígrafo es un campeonato,

$$\sum_{v \in V} (\delta^-(v))^2 = \sum_{v \in V} (\delta^+(v))^2.$$

## 11.2 Redes y caminos críticos

En muchas situaciones prácticas, es más adecuado usar un dígrafo como modelo que un grafo. Por ejemplo, si un arco representa una calle de dirección única o alguna otra clase de unión en la que el movimiento sólo es posible en una dirección. A menudo, el modelo obliga a que los arcos tengan números que representen costes o distancias. Teniendo presentes

estas ideas, usaremos el término **red** para un dígrafo  $D = (V, A)$  junto con una función de peso  $w : A \rightarrow \mathbb{N}$ . El motivo de restringir los valores de  $w$  a enteros positivos es evitar complicaciones respecto a la existencia de soluciones óptimas. En la práctica es sencillo salvar las dificultades que esta restricción pueda causar.

Un ejemplo típico de red que se presenta en la práctica es la llamada *red de actividades*. Un proyecto de construcción grande se suele dividir en varias actividades menores; estas actividades están relacionadas, en el sentido de que algunas de ellas no pueden comenzar hasta que otras hayan finalizado. Por ejemplo, para la construcción de una casa son necesarios cimientos, muros, carpintería, tejados, instalación eléctrica, etc. Una actividad como la instalación eléctrica, por ejemplo, no puede empezar hasta haber completado otras actividades. Para planificar un proyecto de esta clase, se acostumbra a utilizar una red en la que los arcos representan actividades y los vértices representan "sucesos"; cada suceso es la finalización de varias actividades. El peso de un arco representa el tiempo necesario para la actividad y el problema es planificar las actividades de forma que el tiempo total para realizar el proyecto completo sea el menor posible.

**Ejemplo.** La tabla siguiente es una lista de las actividades  $\alpha_1, \alpha_2, \dots, \alpha_8$  de un proyecto y, para cada una de ellas, el tiempo (en días) necesario y las actividades que deben completarse antes de poder iniciarse. ¿Cuál es el mínimo número de días en que puede completarse el proyecto?

Actividad	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\alpha_5$	$\alpha_6$	$\alpha_7$	$\alpha_8$
Tiempo necesario	4	3	7	4	6	5	2	5
Prerrequisitos	-	-	$\alpha_1$	$\alpha_1$	$\alpha_2$	$\alpha_4$	$\alpha_3$	$\alpha_4$

**SOLUCIÓN:** El primer paso es construir la red de actividades, como en la figura 11.2. El vértice  $s$  representa el inicio del proyecto y  $t$  su finalización, mientras que  $q$  representa la finalización de las actividades  $\alpha_4$  y  $\alpha_5$ , y así sucesivamente. La lista completa de actividades y los arcos que las representan es la siguiente:

Actividad:	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\alpha_5$	$\alpha_6$	$\alpha_7$	$\alpha_8$
Arco:	$(s, r)$	$(s, p)$	$(r, z)$	$(r, q)$	$(p, q)$	$(q, z)$	$(z, t)$	$(q, t)$

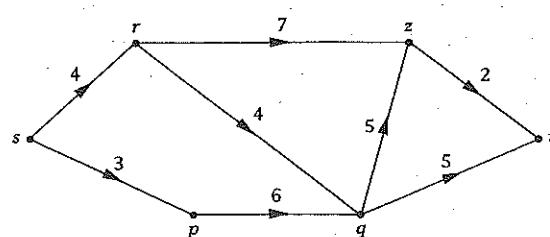


Fig. 11.2 Una red de actividades.

Para cada vértice  $v$  calculamos  $E(v)$ , el menor tiempo para el suceso correspondiente, es decir,  $E(v)$  es el menor tiempo necesario para completar todas las actividades representadas por arcos dirigidos hacia  $v$ . Al principio tenemos  $E(s) = 0$ . Es evidente que  $E(p) = 3$ , ya que sólo interviene la actividad  $\alpha_2 = (p, q)$  que requiere 3 días. Igualmente,  $E(q) = 4$ . En  $q$  han de haberse completado las actividades  $(p, q)$  y  $(r, q)$ . Ahora bien,  $E(p) = 3$  y  $(p, q)$  lleva 6 días, mientras que  $E(q) = 4$  y  $(r, q)$  lleva 4 días: así pues,

$$E(q) = \max(3 + 6, 4 + 4) = 9.$$

(Recuérdese que *ambas* actividades han de completarse, de modo que hemos de permitir el *mayor* número de días.) Prosiguiendo de esta forma, obtenemos los siguientes valores de  $E$ :

$$\begin{array}{c} v: s \quad p \quad q \quad r \quad z \quad t \\ E(v): 0 \quad 3 \quad 9 \quad 4 \quad 14 \quad 16. \end{array}$$

Por lo tanto, el tiempo total necesario para el proyecto es de al menos 16 días.  $\square$

El ejemplo anterior es un caso especial del problema de hallar el camino *más largo* en una red. En general, utilizaremos una versión de la estrategia BEA (convenientemente adaptada a los dígrafos), junto con un cálculo recursivo de la función "menor tiempo" de acuerdo con las reglas

$$E(s) = 0, \quad E(v) = \max_u \{E(u) + w(u, v)\},$$

donde el máximo se toma sobre los vértices  $u$  tales que  $(u, v)$  es un arco.

Este método para estudiar una red de actividades es parte de una técnica llamada **análisis del camino crítico**. El resto de la técnica consiste en lo siguiente. Para cada vértice  $v$  calculamos  $L(v)$ , el tiempo límite en que todas las actividades  $(v, x)$  deben empezar para completar el proyecto a tiempo. Esto se calcula mediante una recursión "hacia atrás":

$$L(t) = E(t), \quad L(v) = \min_x \{L(x) - w(v, x)\},$$

donde el mínimo se toma sobre los vértices  $x$  tales que  $(v, x)$  es un arco. Consideremos ahora lo que sabemos acerca de una actividad cualquiera  $(y, z)$ :

- (i) no puede empezar antes del instante  $E(y)$ ;
- (ii) ha de acabar antes del instante  $L(z)$ ;
- (iii) lleva un tiempo  $w(y, z)$ .

Si ahora definimos la función **tiempo flotante**  $F(y, z)$  como

$$F(y, z) = L(z) - E(y) - w(y, z),$$

entonces  $(y, z)$  puede empezar a partir del instante  $E(y)$  y antes del instante  $E(y) + F(y, z)$  sin retrasar el proyecto. Una actividad  $(y, z)$  es **crítica** si el tiempo flotante es cero: si el proyecto ha de acabar a tiempo, ha de empezar en  $E(y)$ , lo más temprano posible. En una red de actividades existirá al menos un camino dirigido formado únicamente por actividades críticas y este será un **camino crítico**.

### Ejercicios 11.2

1 Calcular los tiempos límite  $L(v)$  y los tiempos flotantes  $F(u, v)$  del proyecto descrito en el ejemplo anterior. Hallar un camino crítico y hacer un calendario del proyecto que muestre los tiempos de inicio alternativos para las actividades que no son críticas.

2 Efectuar el análisis completo de caminos críticos del proyecto siguiente:

Actividad	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\alpha_5$	$\alpha_6$	$\alpha_7$	$\alpha_8$	$\alpha_9$	$\alpha_{10}$	$\alpha_{11}$
Tiempo necesario	6	2	10	1	4	2	7	7	9	2	4
Prerrequisitos	—	—	$\alpha_1$	$\alpha_1$	$\alpha_1$	$\alpha_5$	$\alpha_2$	$\alpha_3$	$\alpha_2$	$\alpha_7$	$\alpha_8$

### 11.3. Flujos y cortes

En los tres apartados siguientes imaginaremos los arcos de una red como "tuberías" a través de las cuales fluye cierto suministro. Los pesos numéricos asignados a los arcos se interpretarán como capacidades que en la práctica limitan las cantidades que pueden fluir a través de los arcos. Además, siempre habrá un vértice  $s$  con la propiedad de que todos los arcos que lo contienen están dirigidos desde  $s$  y un vértice  $t$  con la propiedad de que todos los arcos que lo contienen están dirigidos hacia  $t$ . Los vértices  $s$  y  $t$  se conocen como **fuente** y **sumidero**, respectivamente. En resumen, nos ocuparemos de redes con

- (i) un digrafo  $D = (V, A)$ ;
- (ii) una función de capacidad  $c : A \rightarrow \mathbb{N}$ ;
- (iii) una fuente  $s$  y un sumidero  $t$ .

En la figura 11.3 se muestra un ejemplo.

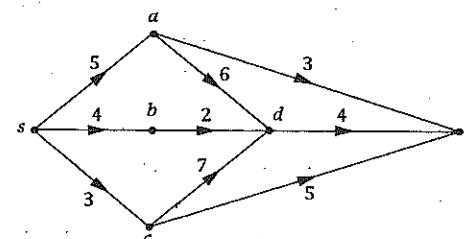


Fig. 11.3 Una red con la capacidad de cada arco.

Supongamos que un suministro fluye a través de los arcos de la red y sea  $f(x, y)$  la cantidad que fluye a lo largo del arco  $(x, y)$ . Insistiremos en que, salvo para  $s$  y  $t$ , la cantidad de flujo que llega a un vértice  $v$  ha de ser igual a la cantidad que sale de  $v$ . En consecuencia, definimos la **entrada** y la **salida** en  $v$  como

$$\text{entrada}(v) = \sum_{(x, v) \in A} f(x, v), \quad \text{salida}(v) = \sum_{(v, y) \in A} f(v, y)$$

y exigimos que las dos cantidades sean iguales excepto cuando  $v = s$  o  $v = t$ . Esta es la "regla de la conservación" para los flujos en redes. También impondremos la "regla de la viabilidad", según la cual ningún arco puede

transportar más allá de su capacidad. Es conveniente incorporar estas dos reglas en nuestra definición de flujo.

**Definición.** Un **flujo** de una fuente  $s$  a un sumidero  $t$  en una red es una función que asigna un número no negativo  $f(x, y)$  a cada arco  $(x, y)$ , sujeta a las reglas

$$\begin{aligned} \text{conservación: } & \text{entrada}(v) = \text{salida}(v) \quad (v \neq s, t); \\ \text{viabilidad: } & f(x, y) \leq c(x, y) \quad ((x, y) \in A). \end{aligned}$$

El lector debiera comprobar que la función definida en la siguiente tabla es un flujo en la red de la figura 11.3.

$(x, y)$ :	$(s, a)$	$(s, b)$	$(s, c)$	$(a, d)$	$(b, d)$	$(c, d)$	$(a, t)$	$(c, t)$	$(d, t)$
$f(x, y)$ :	3	2	3	1	2	1	2	2	4

Como no se permite acumular nada en los vértices intermedios, la cantidad total que fluye de  $s$  ha de ser igual a la cantidad total que fluye hacia  $t$  (en el ejercicio 11.3.3 se esboza una demostración). En otras palabras, para cualquier flujo de  $s$  a  $t$

$$\text{salida}(s) = \text{entrada}(t).$$

El valor común de estas cantidades, llamada **valor** del flujo, mide la cantidad total de flujo a través de la red y se escribe  $\text{val}(f)$ . En el ejemplo anterior,

$$\begin{aligned} \text{salida}(f) &= f(s, a) + f(s, b) + f(s, c) = 3 + 2 + 3 = 8 \\ \text{entrada}(f) &= f(a, t) + f(d, t) + f(c, t) = 2 + 4 + 2 = 8, \end{aligned}$$

de modo que  $\text{val}(f) = 8$ .

Nuestro problema es calcular el valor máximo de un flujo para una red dada. Empezaremos por hallar una cota superior para este valor en función de las capacidades. En la figura 11.3 observamos que la capacidad total de los arcos que salen de  $s$  es  $5 + 4 + 3 = 12$ ; es evidente que ningún flujo puede tener un valor superior a 12. Más en general, supongamos que partimos el conjunto de vértices en dos partes; una parte  $S$  que contiene a  $s$  y otra  $T$  que contiene a  $t$ . Entonces el flujo neto de  $S$  a  $T$  será, por la

regla de conservación, el mismo que el flujo de  $s$  a  $t$ , que es el valor de  $f$ . Es decir,

$$\text{val}(f) = \sum_{\substack{x \in S \\ y \in T}} f(x, y) - \sum_{\substack{u \in T \\ v \in S}} f(u, v).$$

La primera suma mide el flujo total de  $S$  a  $T$  y la segunda mide el flujo total en la dirección contraria. Como los términos de la segunda suma no son negativos, tenemos que

$$\text{val}(f) \leq \sum_{\substack{x \in S \\ y \in T}} f(x, y).$$

Además, como  $f(x, y) \leq c(x, y)$  para cada arco, podemos concluir que la suma

$$\sum_{\substack{x \in S \\ y \in T}} c(x, y)$$

es una cota superior del valor de cualquier flujo. Por ejemplo, si en la figura 11.3 tomamos  $S = \{d, b\}$  y  $T = \{a, c, d, t\}$ , los arcos dirigidos de  $S$  a  $T$  son  $(s, a), (s, c)$  y  $(b, d)$ , con una capacidad total de 10; deducimos que  $\text{val}(f) \leq 10$  para cualquier flujo en esa red.

Formalmente, diremos que  $(S, T)$  es un **corte** (que separa  $s$  y  $t$ ) si  $S \cup T$  es una partición del conjunto de vértices tal que  $s$  es de  $S$  y  $t$  es de  $T$ . La **capacidad del corte** es

$$\text{cap}(S, T) = \sum_{\substack{x \in S \\ y \in T}} c(x, y)$$

y, con esta terminología, hemos establecido el siguiente resultado.

**Teorema 11.3.** Sean  $s$  y  $t$  la fuente y sumidero de una red. Si  $f$  es un flujo de  $s$  a  $t$  y  $(S, T)$  es un corte, entonces

$$\text{val}(f) \leq \text{cap}(S, T). \quad \square$$

Sea  $f_0$  un flujo que tiene valor máximo y  $(S_0, T_0)$  un corte con la mínima capacidad posible. El teorema 11.3 nos dice que  $\text{val}(f_0) \leq \text{cap}(S_0, T_0)$  o, más expresivamente,

$$\text{flujo-máximo} \leq \text{corte-mínimo}.$$

En el siguiente apartado demostraremos el fundamental “teorema del flujo-máximo y corte-mínimo”, que afirma que las dos expresiones son, de hecho, iguales.

### Ejercicios 11.3

- 1 Hallar un flujo  $f^*$  en la figura 11.3 tal que  $\text{val}(f^*) = 10$ . ¿Por qué es este el máximo valor posible?
- 2 Dibujar una red que tenga por vértices  $s, a, b, c, d, t$ , y arcos y capacidades

$$\begin{array}{cccccccccc} (x, y) : & (s, a) & (s, b) & (a, b) & (a, c) & (b, d) & (d, c) & (c, t) & (d, t) \\ c(x, y) : & 5 & 3 & 3 & 3 & 5 & 2 & 6 & 2 \end{array}$$

Hallar un flujo con valor 7 y un corte con capacidad 7. ¿Cuál es el valor máximo de un flujo y por qué?

- 3 Sea  $D = (V, A)$  un digrafo y supongamos que  $\phi : A \rightarrow \mathbb{N}$  es una función, no necesariamente un flujo. Si definimos la entrada y la salida para  $\phi$  como antes, demostrar que

$$\sum_{v \in V} \text{salida}(v) = \sum_{v \in V} \text{entrada}(v).$$

Deducir que  $s$  y  $t$  son la fuente y sumidero de una red y  $\phi$  es un flujo, entonces

$$\text{salida}(s) = \text{entrada}(t).$$

### 11.4 El teorema del flujo máximo y el corte mínimo

En este apartado describiremos un método para incrementar el valor de un flujo dado, siempre que su valor no sea el máximo posible. El método es, además de la base para un algoritmo práctico (apartado 11.5), la clave para

demostrar el teorema fundamental del flujo máximo y el corte mínimo.

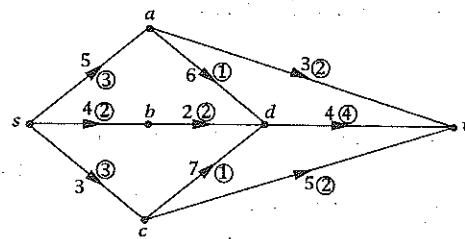


Fig. 11.4 Un flujo con valor 8.

Estudiemos de nuevo la red de la figura 11.3 y el flujo  $f$  con valor 8 descrito en el apartado anterior. Consideremos el camino dirigido  $s, a, t$ . Ninguno de los arcos  $(s, a)$  y  $(a, t)$  transporta flujo al máximo de su capacidad, de modo que podemos aumentar el flujo en ambos arcos hasta alcanzar la capacidad máxima de uno de ellos. Si definimos  $f_1(s, a) = 4$  y  $f_1(a, t) = 3$ , el arco  $(a, t)$  se satura; más aún, como hemos incrementado el flujo en ambos arcos en la misma cantidad, en el vértice  $a$  se sigue cumpliendo la regla de conservación. Si definimos  $f_1(x, y) = f(x, y)$  en los arcos restantes, tenemos un nuevo flujo

$$\begin{array}{llllllll} (x, y) : & (s, a) & (s, b) & (s, c) & (a, d) & (b, d) & (c, d) & (a, t) & (c, t) & (d, t) \\ f_1(x, y) : & 4 & 2 & 3 & 1 & 2 & 1 & 3 & 2 & 4 \end{array}$$

con valor  $\text{val}(f_1) = \text{val}(f) + 1 = 9$ .

Para mejorar el valor todavía más necesitamos algo más ingenioso, un "camino" como  $s, a, d, c, t$ . El problema es que no hemos definido "caminos" en una red, sólo caminos dirigidos, y este último claramente no es un camino dirigido, ya que el arco  $(c, d)$  no está en la dirección correcta. Hablando con precisión, deberíamos referirnos a  $s, a, d, c, t$  como a un camino en el grafo que se obtiene al ignorar las direcciones de los arcos del digrafo y tratarlos como aristas. Sin embargo, utilizaremos simplemente la palabra "camino". Las capacidades y los  $f_1$ -valores en el camino son

$$s \xrightarrow[4]{ } a \xrightarrow[1]{ } d \xleftarrow[1]{ } c \xrightarrow[2]{ } t.$$

Como el flujo  $(c, d)$  es contrario a la dirección del camino, podemos reducir en 1 el flujo en  $(c, d)$  e incrementar en la misma cantidad el flujo en los arcos

restantes, sin violar la ley de la conservación. De esta forma obtenemos un nuevo flujo  $f_2$  cuyos valores en el camino son

$$s \xrightarrow[5]{ } a \xrightarrow[2]{ } d \xleftarrow[0]{ } c \xrightarrow[3]{ } t,$$

e iguales a  $f_1$  en los restantes arcos. Nótese que ya no podemos hacer ninguna mejora en este camino, puesto que  $(s, a)$  ya está saturado y el flujo en  $(c, d)$  no puede ser negativo.

Ahora tenemos que  $\text{val}(f_2) = \text{val}(f_1) + 1 = 10$ . En el apartado anterior hallamos un corte con capacidad 10 y, por el teorema 11.3, sabemos que ningún flujo puede tener un valor mayor que éste. Así pues,  $f_2$  es un flujo máximo.

Los caminos  $s, a, t$  y  $s, a, d, c, t$  que utilizamos para incrementar los flujos  $f_1$  y  $f_2$ , respectivamente, son ejemplos de lo que se conoce como un "camino aumentante de flujo". En general, dado un flujo  $f$ , un camino

$$s = x_1, x_2, \dots, x_{k-1}, x_k = t$$

es un **camino f-aumentante** si

$$f(x_i, x_{i+1}) < c(x_i, x_{i+1}) \quad \text{y} \quad (x_i, x_{i+1}) \in A,$$

o bien

$$f(x_{i+1}, x_i) > 0 \quad \text{y} \quad (x_{i+1}, x_i) \in A,$$

para  $1 \leq i \leq k - 1$ . En otras palabras, los arcos "directos" no se usan al máximo de su capacidad, mientras que los arcos "inversos" llevan algún "contra-flujo". Dado un camino de estas características, podemos aumentar el flujo en los arcos directos y disminuirlo en los arcos inversos en la misma cantidad sin violar la ley de conservación. El mayor que puede obtenerse de este modo, sin sobrecargar los arcos directos o hacer negativo el flujo en los inversos, es el mínimo de las cantidades

$$\begin{aligned} c(x_i, x_{i+1}) - f(x_i, x_{i+1}) &\quad \text{si } (x_i, x_{i+1}) \in A, \\ f(x_{i+1}, x_i) &\quad \text{si } (x_{i+1}, x_i) \in A \end{aligned}$$

en el rango  $1 \leq i \leq k - 1$ . Si denotamos esta cantidad por  $\alpha$  entonces, al añadir  $\alpha$  al flujo en los arcos directos y sustraerla de los inversos, obtenemos un nuevo flujo  $f^*$  con  $\text{val}(f^*) = \text{val}(f) + \alpha$ .

La existencia de un camino  $f$ -aumentante de  $s$  a  $t$  nos permite hallar un nuevo flujo  $f^*$  con  $\text{val}(f^*) > \text{val}(f)$ . Por otra parte, el teorema 11.3 asegura que el valor de un flujo cualquiera no puede exceder la capacidad de un corte cualquiera. En el siguiente teorema se combinan ambas ideas; en la demostración se introducen los caminos  $f$ -aumentantes *incompletos*, que satisfacen las condiciones de un camino  $f$ -aumentante, salvo que el vértice final no es  $t$ .

**Teorema 11.4.** *El valor máximo de un flujo de  $s$  a  $t$  en una red es igual a la capacidad mínima de un corte que separe  $s$  de  $t$ .*

**DEMOSTRACIÓN:** Sea  $f$  un flujo máximo. Sea  $S$  el conjunto de vértices  $x$  para los que existe un camino  $f$ -aumentante incompleto de  $s$  a  $x$  y sea  $T$  el conjunto de vértices complementario. El sumidero  $t$  ha de estar en  $T$ , ya que de otro modo tendríamos un camino  $f$ -aumentante de  $s$  a  $t$  y podríamos aumentar  $f$ , contrariamente a la hipótesis de que es un flujo máximo. Así pues,  $(S, T)$  es un corte que separa  $s$  de  $t$ .

Demostremos que  $\text{cap}(S, T) = \text{val}(f)$ . Sea  $(x, y)$  un arco cualquiera con  $x \in S$  e  $y \in T$ . Por definición de  $S$ , existe un camino  $f$ -aumentante incompleto de  $s$  a  $x$ ; si  $f(x, y) < c(x, y)$ , podríamos extenderlo a  $y$ , contradiciendo el hecho de que  $y$  es de  $T$ . Por lo tanto,  $f(x, y) = c(x, y)$ . Análogamente, dado un arco  $(u, v)$  con  $u$  de  $T$  y  $v$  de  $V$ , existe un camino  $f$ -aumentante incompleto de  $s$  a  $v$ , y si  $f(u, v) > 0$  podríamos extenderlo hasta  $u$ , contradiciendo el hecho de que  $u$  es de  $T$ . Así pues,  $f(u, v) = 0$  y tenemos que

$$\begin{aligned} \text{val}(f) &= \sum_{\substack{x \in S \\ y \in T}} f(x, y) - \sum_{\substack{u \in T \\ v \in S}} f(u, v) = \sum_{\substack{x \in S \\ y \in T}} c(x, y) \\ &= \text{cap}(S, T). \end{aligned}$$

Si  $(S', T')$  es otro corte, por el teorema 11.3 y el resultado que acabamos de demostrar, tenemos que

$$\text{cap}(S', T') \geq \text{val}(f) = \text{cap}(S, T).$$

Resulta que  $(S, T)$  es un corte mínimo, como queríamos demostrar.  $\square$

#### Ejercicios 11.4

1 El diagrama de la figura 11.5 representa una red y los números en los arcos, sus capacidades. Se define un flujo de la siguiente manera:

$$\begin{array}{ll} (x, y) : & (s, a) \quad (s, b) \quad (s, c) \quad (a, b) \quad (a, d) \quad (b, c) \quad (b, d) \quad (b, e) \quad (c, e) \quad (d, t) \quad (e, t) \\ f(x, y) : & 5 \quad 6 \quad 0 \quad 0 \quad 5 \quad 1 \quad 2 \quad 3 \quad 1 \quad 7 \quad 4 \end{array}$$

- (i) ¿Cuál es el valor de  $f$ ?
- (ii) Hallar un camino  $f$ -aumentante y calcular el valor del flujo aumentado.
- (iii) Hallar un corte de capacidad 12.
- (iv) ¿Qué puede deducirse?

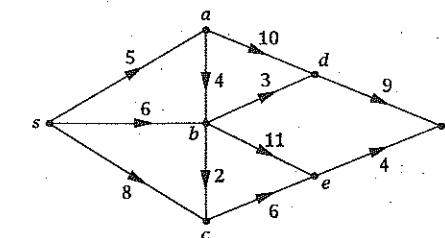


Fig. 11.5 Una red junto con la capacidad de cada arco.

2 El conjunto de vértices de una red es  $\{s, a, b, c, d, e, t\}$  y la capacidad de un arco  $(x, y)$ , si existe, es la que indica la tabla 11.4.1 en la fila  $x$ , columna  $y$ . Hallar un flujo máximo en la red de  $s$  a  $t$  y explicar por qué es máximo.

Tabla 11.4.1

	$s$	$a$	$b$	$c$	$d$	$e$	$t$
$s$	—	14	—	14	—	12	—
$a$	—	—	8	14	—	3	—
$b$	—	—	—	—	—	2	15
$c$	—	—	—	—	19	—	—
$d$	—	—	6	—	—	1	10
$e$	—	—	—	—	—	—	14

### 11.5 El algoritmo de etiquetaje para flujos en redes

Los resultados anteriores sugieren un algoritmo práctico para el problema del máximo flujo. En líneas generales, la estrategia es la siguiente.

- Empezar con un flujo cualquiera (por ejemplo, asignar un cero a cada arco).
- Utilizar BEA para construir un árbol de caminos  $f$ -aumentantes incompletos con raíz en  $s$ .
- Si el árbol llega a  $t$ , aumentar  $f$  como corresponde y volver a (B) con el nuevo flujo.
- Si el árbol no llega a  $t$ , sea  $S$  el conjunto de vértices que se alcanzan y  $T$  su complementario. El flujo  $f$  es máximo y  $(S, T)$  es un corte mínimo.

**Ejemplo.** Hallar un flujo máximo para la red de la figura 11.6, empezando con el flujo  $f_1$  que es igual 4 en  $(s, b)$  y  $(b, y)$ , y cero en los demás arcos.

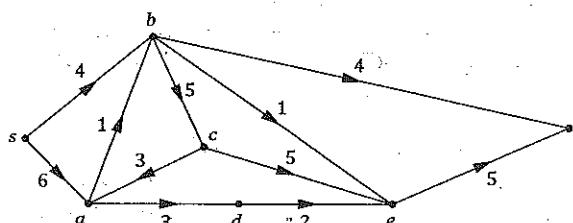


Fig. 11.6 La red discutida en el ejemplo.

**SOLUCIÓN:** Ignorando la dirección de los arcos, consideramos la red como un grafo y utilizamos BEA para construir un árbol con raíz en  $s$ . Las aristas del árbol han de formar caminos  $f_1$ -aumentantes (incompletos); al añadir una arista  $xy$  al árbol, el nuevo vértice  $y$  recibe una etiqueta  $l(y)$  igual al máximo aumento posible en el camino de  $s$  a  $y$ .

Por motivos didácticos, anotaremos el proceso (tabla 11.5.1) en términos de la cola  $Q$  de vértices formada según las reglas de BEA (apartado 9.5). En cada paso “exploramos”  $x$ , el primer vértice de  $Q$ , para ver si existen aristas  $xy$  que extiendan el camino  $f_1$ -aumentante de  $s$  a  $x$ ; si hay más de uno, usaremos el orden alfabético para decidir qué arista se añade primero.

Tabla 11.5.1

Paso	Cola $Q$	Examinar $x$	Llegada $y$	Etiqueta $l(y)$	Salida
1	$s$	$s$	$a$	6	—
2	$sa$	$s$	—	—	$s$
3	$a$	$a$	$b$	1	—
4	$ab$	$a$	$d$	3	—
5	$abd$	$a$	—	—	$a$
6	$bd$	$b$	$c$	1	—
7	$bdc$	$b$	$e$	1	—
8	$bdce$	$b$	—	—	$b$
9	$dce$	$d$	—	—	$d$
10	$ce$	$c$	—	—	$c$
11	$e$	$e$	$t$	1	—

#### Comentarios

Paso 2: no puede añadirse  $sb$  porque el arco  $(s, b)$  está saturado.

Paso 3: puede añadirse  $ab$ ,  $l(b) = c(a, b) - f_1(a, b) = 1$ .

Paso 4: no puede añadirse  $ac$  como arco inverso  $(c, a)$  ya que  $f_1(c, a) = 0$ .

Paso 9: no puede añadirse  $de$ , puesto que  $e$  ya está en el árbol.

Paso 11: hemos llegado a  $t$  y acabamos.

Como  $f(t) = 1$ , podemos aumentar  $f_1$  en 1 en los arcos  $(s, a), (a, b), (b, e)$  y  $(e, t)$ . En ejemplos como éste, es fácil marcar las aristas del árbol y las etiquetas en el diagrama de la red. Véase la figura 11.7 y el flujo  $f_2$  que le sigue.

$$(x, y) : (s, a) \quad (s, b) \quad (a, b) \quad (a, d) \quad (b, c) \quad (b, e) \quad (b, t) \quad (c, a) \quad (c, e) \quad (d, e) \quad (e, t)$$

$$f_2(x, y) : 1 \quad 4 \quad 1 \quad 0 \quad 0 \quad 1 \quad 4 \quad 0 \quad 0 \quad 0 \quad 1$$

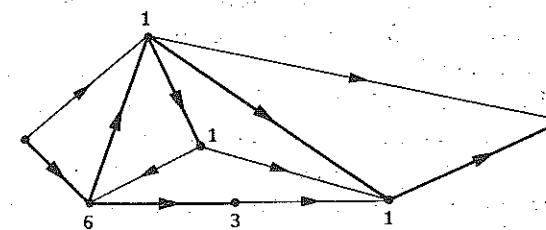


Fig. 11.7 Primera iteración del algoritmo.

Si empezamos con  $f_2$  y repetimos el proceso, obtenemos el árbol y las etiquetas que muestra la figura 11.8 y el flujo aumentado  $f_3$ .

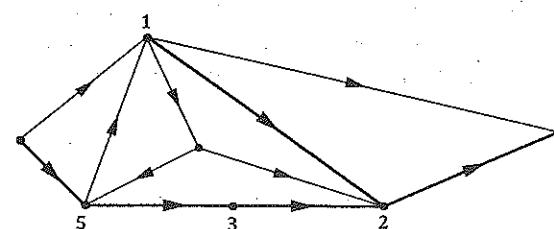


Fig. 11.8 Segunda iteración del algoritmo.

$$(x, y) : \begin{matrix} (s, a) & (s, b) & (a, b) & (a, d) & (b, c) & (b, e) & (c, a) & (c, e) & (d, e) & (e, t) \\ f_2(x, y) : & 3 & 4 & 1 & 2 & 0 & 1 & 4 & 0 & 0 & 2 & 3 \end{matrix}$$

Finalmente, empezando con  $f_3$  y repitiendo el proceso llegamos a un árbol que no contiene  $t$  (figura 11.9).

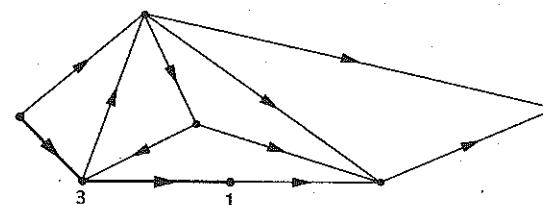


Fig. 11.9 Tercera iteración del algoritmo.

Podemos concluir que  $f_3$  es un flujo máximo. Su valor es 7 y el hecho de que es maximal puede comprobarse con el corte  $(S, T)$ , donde  $S$  es el conjunto de vértices que se alcanzan en el árbol final. En este caso,  $S = \{s, a, d\}$  y

$$\text{cap}(S, T) = c(s, b) + c(a, b) + c(d, e) = 4 + 1 + 2 = 7,$$

con lo que  $(S, T)$  es un corte mínimo y  $f_3$  un flujo máximo.  $\square$

La descripción formal del algoritmo de etiquetaje sigue las líneas del procedimiento indicado más adelante, pero son necesarios algunos ajustes para adaptarse a los ordenadores poco inteligentes.

Sea  $F(x, y)$  el enunciado “ $(x, y)$  es un arco directo y  $f(x, y) < c(x, y)$ ”, y sea  $B(x, y)$  el enunciado “ $(y, x)$  es un arco inverso y  $f(y, x) > 0$ ”. Al añadir

la arista  $xy$  al árbol, el vértice  $y$  recibe una doble etiqueta  $(l_1(y), l_2(y))$ . La primera etiqueta indica cómo ha sido alcanzado  $y$  y la segunda es la  $l(y)$  del ejemplo anterior. En concreto, si se cumple  $F(x, y)$  definimos

$$l_1(y) = x^+, \quad l_2(y) = \min\{l_2(x), c(x, y) - f(x, y)\},$$

mientras que si  $B(x, y)$  es el que se cumple, definimos

$$l_1(y) = x^-, \quad l_2(y) = \min\{l_2(x), f(y, x)\}.$$

Inicialmente tomamos  $f$  como el flujo que es cero en todos los arcos y la etiqueta  $l_2(s)$  como  $l_{\text{big}}$  (que, en la práctica, puede ser la suma de las capacidades de todos los arcos). El programa que se expone a continuación indica cómo injertar el algoritmo de etiquetaje en un procedimiento BEA (en recuadro); acabará cuando  $f_{\text{max}}$  sea igual al valor de un flujo máximo.

#### Algoritmo de etiquetaje para el flujo máximo

```

asignar a  $f$  el flujo cero y a  $f_{\text{max}}$  una cantidad grande;
mientras  $\text{val}(f) \neq f_{\text{max}}$  hacer
    inicio
        sea  $\text{cola} = (s)$ ; asignar a  $l_2(s)$  una cantidad grande;
        mientras  $\text{cola}$  es no vacía hacer
            inicio
                 $x := \text{principio}(\text{cola})$ ;
                si  $x$  es adyacente a un nuevo vértice  $y$ 
                    entonces inicio si  $F(x, y)$  o  $B(x, y)$  entonces etiqueta  $y$ 
                        añadir  $y$  al final de la cola;
                    si  $y = t$  entonces aumentar  $f$  y  $\text{val}(f)$ 
                        y vaciar la cola
                    fin
                si no
                    inicio
                        borrar  $x$  de la cola;
                    si  $\text{cola}$  está vacía entonces asignar  $f_{\text{max}} = \text{val}(f)$ 
                    fin
                fin
            fin
        fin
    fin
fin

```

**Ejercicios 11.5**

- 1 Empezando con el flujo cero; utilizar el algoritmo de etiquetaje (ja mano!) para hallar el flujo máximo en la red que muestra la figura 11.10.

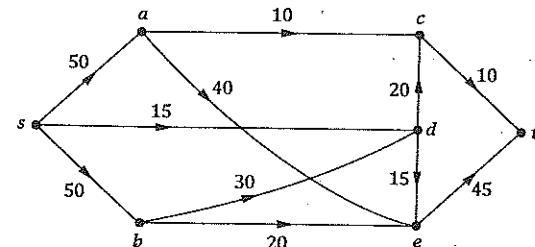


Fig. 11.10 Hallar el flujo máximo.

- 2 En  $s_1$  y  $s_2$  se fabrica un producto que se transporta a través de la red que muestra la figura 11.11 a los mercados en  $t_1, t_2$  y  $t_3$ .

- (i) Añadir una nueva "superfuente" y un nuevo "supersumidero" para que la red sea estándar.
- (ii) Hallar un "buen" flujo inicial por tanteo.
- (iii) Utilizar el algoritmo de etiquetaje para hallar un flujo máximo.

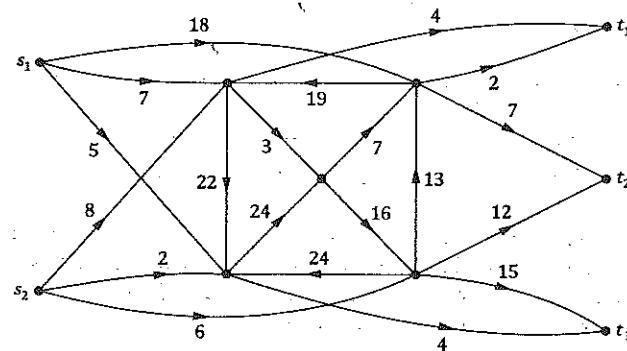


Fig. 11.11 Ilustración para el ejercicio 11.5.2.

**11.6 Ejercicios diversos**

- 1 Hallar un camino dirigido que contenga todos los vértices del campeonato descrito en la tabla 11.6.1 (la notación es como en el ejercicio 11.1.2).

Tabla 11.6.1

i	j							
	1	2	3	4	5	6	7	8
1	+	-	+	-	-	-	-	+
2	+	-	-	+	-	-	+	
3	-	-	+	+	+	+		
4		+	+	+	+	+		
5			-	-	-			
6				+	-			
7					+			

- 2 Definimos la **puntuación** de un vértice en un campeonato como si grado de salida y la **sucesión de puntuaciones** como la secuencia de puntuaciones ordenadas en orden no creciente. Comprobar que la sucesión de puntuaciones del campeonato descrito en el ejercicio 11.1.2 es  $(6, 5, 4, 4, 4, 3, 3, 3)$  y demostrar que, en general, si la sucesión de puntuaciones es  $(s_1, s_2, \dots, s_n)$ , entonces

$$\sum_{i=1}^n s_i = \frac{1}{2}n(n-1).$$

- 3 Demostrar qué la sucesión de puntuaciones de un campeonato con  $n$  vértices cumple

- (i)  $s_1 + s_2 + \dots + s_n \geq \frac{1}{2}k(k-1)$  ( $1 \leq k \leq n-1$ );
- (ii)  $\frac{1}{2}(k-1) \leq s_k \leq \frac{1}{2}(n+k-2)$  ( $1 \leq k \leq n$ ).

- 4 Se dice que un campeonato es **transitivo** si representa una relación transitiva, es decir, si la existencia de los arcos  $(x, y)$  e  $(y, z)$  implica la existencia del arco  $(x, z)$ . Demostrar que un campeonato es transitivo si, y sólo si, el término  $k$ -ésimo de la sucesión de puntuaciones es igual a  $k-1$ .

- 5 ¿Cuántos campeonatos hay con  $n$  vértices? ¿Cuántos de ellos son transitivos?

- 6 Demostrar que en cualquier campeonato existe un vértice  $s$  tal que todo vértice  $x$  puede alcanzarse desde  $s$  mediante un camino dirigido de longitud 0, 1 o 2.

7 Efectuar el análisis del camino crítico completo para el proyecto descrito a continuación.

Actividad	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\alpha_5$	$\alpha_6$	$\alpha_7$	$\alpha_8$	$\alpha_9$
Tiempo necesario	3	5	4	4	4	4	2	4	7
Prerrequisitos	—	—	—	$\alpha_1$	$\alpha_3$	$\alpha_1$	$\alpha_2$	$\alpha_6$	$\alpha_3$

 $\alpha_4$  $\alpha_7$ 

8 Modificar los valores de los tiempos necesarios para las actividades del ejercicio 7 de modo que exista más de un camino crítico. Demostrar que, en general, toda actividad que tenga un tiempo flotante igual a cero está en algún camino crítico.

9 Considerar la red que tiene por vértices  $\{s, a, b, c, t\}$  y arcos y capacidades dados por la siguiente tabla.

$(s, a)$	$(s, b)$	$(a, b)$	$(a, c)$	$(a, t)$	$(b, c)$	$(c, t)$
5	2	3	1	3	3	4

Calcular las capacidades de todos los cortes que separan  $s$  de  $t$  y hallar un flujo máximo de  $s$  a  $t$ .

10 Utilizar el algoritmo de etiquetaje para comprobar que si las capacidades de los arcos de una red son enteros, existe un flujo máximo tal que el flujo en cada arco es un entero.

11 Demostrar que el flujo máximo de la figura 11.11 no está únicamente determinado; como consecuencia, dar un ejemplo de un flujo máximo en el que el flujo en cada arco no es un entero.

12 Sean  $(S_1, \bar{S}_1)$  y  $(S_2, \bar{S}_2)$  cortes que separan  $s$  de  $t$  en una red, ambos mínimos. Demostrar que  $(S_1 \cap S_2, \bar{S}_1 \cap \bar{S}_2)$  es también un corte mínimo.

13 Escribir un procedimiento general para introducir una "superfuente" y un "supersumidero" en una red que tiene varias fuentes y sumideros, como en el ejercicio 11.5.2. Enunciar y demostrar la versión correspondiente del teorema del flujo máximo y corte mínimo.

14 Considérese la red con conjunto de vértices  $\{s, a, b, c, d, e, f, t\}$  y arcos y capacidades dados por la tabla siguiente.

Arco:	$(s, a)$	$(s, d)$	$(a, b)$	$(b, c)$	$(b, e)$	$(c, t)$	$(d, e)$	$(e, f)$	$(f, t)$
Capacidad:	$n$	$n$	$n$	$n$	1	$n$	$n$	$n$	$n$

Si en el algoritmo de etiquetaje empezamos con el flujo cero y hacemos las elecciones pertinentes, demostrar que pueden llegar a ser necesarias  $O(n)$

iteraciones del algoritmo para construir un flujo máximo. ¿Qué nos dice esto acerca del algoritmo de etiquetaje?

15 Sea  $G = (V \cup W, E)$  un grafo bipartido. Construir un dígrafo asociado a  $G$  añadiendo dos nuevos vértices  $s$  y  $t$ , junto con los arcos  $(s, v)$  para todo  $v$  de  $V$  y  $(w, t)$  para todo  $w$  de  $W$ , y considerando cada arista  $vw$  de  $G$  como un arco  $(v, w)$ . Asignar capacidades a los arcos de forma que los arcos  $(s, v)$  y  $(w, t)$  tengan capacidades grandes y los arcos  $(v, w)$  tengan capacidad unidad.

Sea  $(S, \bar{S})$  un corte mínimo de esta red y definamos  $A = S \cap V, B = S \cap W$ . Demostrar que la capacidad de  $(S, \bar{S})$  es  $|V| - |A| + |B|$  y deducir que el tamaño de un emparejamiento máximo en  $G$  es  $|V| - d$ , donde  $d$  es la deficiencia.

16 Demostrar la siguiente generalización del teorema 11.1. Sea  $D$  un dígrafo y  $\chi$  el número cromático del grafo que se obtiene de  $D$  ignorando las direcciones de los arcos. Demostrar que  $D$  contiene un camino dirigido de longitud  $\chi - 1$ .

17 Un "triple malo" en un campeonato es un conjunto de tres vértices  $\{a, b, c\}$  tales que  $a$  gana a  $b$ ,  $b$  gana a  $c$  y  $c$  gana a  $a$ . Demostrar que el número de triples malos es igual a

$$\binom{n}{3} - \sum_{i=1}^n \binom{s_i}{2},$$

donde  $(s_i)$  es la secuencia de puntuaciones. Deducir que el número máximo de triples malos es  $\frac{1}{4} \binom{n+1}{3}$ .

## 12 Técnicas recursivas

### 12.1 Generalidades sobre la recursividad

En capítulos anteriores hemos visto varios problemas cuya solución puede expresarse como una función  $u$  de un entero positivo  $n$ . Los valores de  $u$  pueden escribirse como valores de una función  $u(n)$  o en términos de una sucesión  $(u_n)$ . Algunos ejemplos típicos son

$\phi(n)$ : el número de enteros  $k$  tales que  $1 \leq k \leq n$  y  $\text{mcd}(k, n) = 1$ .

$d_n$ : el número de desarreglos de  $\{1, 2, \dots, n\}$ .

$q_n$ : el número de particiones de un  $n$ -conjunto

A menudo podemos obtener una ecuación que nos dé el valor de  $u_n$  en términos de otros valores  $u_r$ , con  $r < n$ : esta es la esencia del método recursivo. Por ejemplo, en el ejercicio 4.4.4 demostramos que

$$d_n = (n-1)(d_{n-1} + d_{n-2}) \quad (n \geq 3).$$

Esta ecuación, junto con el conocimiento de que  $d_1 = 0$  y  $d_2 = 1$ , implica que podemos calcular  $d_3, d_4, d_5, \dots$ , del siguiente modo:

$$d_3 = 2(1+0) = 2, \quad d_4 = 3(2+1) = 9, \quad d_5 = 4(9+2) = 44,$$

y así sucesivamente. La existencia de una ecuación recurrente adecuada nos permite calcular el valor de  $d_n$  para cualquier entero positivo  $n$ .

Por varios motivos, es útil tener una fórmula explícita para  $u_n$ . De hecho, convenimos en decir que hemos “resuelto” la recurrencia cuando disponemos de una tal fórmula. En este sentido, la fórmula explícita

$$d_n = n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!} \right)$$

obtenida en el apartado 4.4 puede considerarse como la solución de la recurrencia  $d_n = (n-1)(d_{n-1} + d_{n-2})$  ( $n \geq 3$ ), con condiciones iniciales  $d_1 = 0$  y  $d_2 = 1$ . Aunque hemos de insistir en que la fórmula es, con frecuencia, menos útil que la propia ecuación. Si queremos calcular  $d_{10}$  (por ejemplo), por lo general será más eficiente utilizar la ecuación que sustituir valores en la fórmula (ejercicio 12.1.1).

Una razón por la que una fórmula puede ser útil es para describir el comportamiento de una sucesión para valores grandes de  $n$ . El lector que conozca el resultado

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^r \frac{1}{r!} + \cdots$$

podrá deducir de la fórmula que  $d_n$  es aproximadamente igual a  $n!/e$ . En otras palabras, la proporción de las  $n!$  permutaciones que son desarreglos es más o menos  $e^{-1} = 0.367 \dots$

#### Ejercicios 12.1

1 Demostrar que la fórmula para  $d_n$  puede escribirse así:

$$d_n = 3 \times 4 \times \cdots \times (n-1) \times n - 4 \times \cdots \times (n-1) \times n + \cdots + (-1)^{n-1} n + (-1)^n.$$

Demostrar que para calcular  $d_n$  mediante esta fórmula son necesarias  $O(n^2)$  multiplicaciones. ¿Cuántas multiplicaciones son necesarias utilizando la recurrencia?

2 (i) Escribir un programa que calcule  $d_n$  a partir de la recurrencia.

(ii) Modificar el programa para hallar el mínimo valor de  $n$  tal que  $d_n > 10^{10}$ .

3 Demostrar que el número de desarreglos  $d_n$  también satisface la recurrencia

$$d_1 = 0, \quad d_n = nd_{n-1} + (-1)^n \quad (n \geq 2).$$

¿Es ventajoso utilizar esta recurrencia (en lugar de la habitual) para calcular  $d_n$ ?

4 Sean  $c_0, c_1, \dots, c_{k-1}$  constantes y  $f_k, f_{k+1}, \dots$ , funciones dadas. Demostrar que existe una única función  $u$  que cumple la recurrencia

$$\begin{aligned} u(0) &= c_0, & u(1) &= c_1, \dots, & u(k-1) &= c_{k-1}, \\ u(n+k) &= f_{n+k}[u(0), u(1), \dots, u(n+k-1)] & (n \geq 0). \end{aligned}$$

[Indicación: suponer que existen dos funciones  $u$  y  $u'$  y sea  $X$  el conjunto de los  $n$  tales que  $u(n) \neq u'(n)$ ; utilizar el axioma de la buena ordenación tal como se hizo en el apartado 1.3.]

## 12.2 Recurrencias lineales

Una forma particular de la recurrencia general presentada en el ejercicio 12.1.4 se produce cuando  $u(n+k)$  viene dado por una combinación lineal constante de los valores  $u(n), u(n+1), \dots, u(n+k-1)$ . Usaremos la notación de las sucesiones en lugar de la notación funcional y reescribiremos las ecuaciones de forma que el caso típico sea de la forma

$$\begin{aligned} u(0) &= c_0, & u(1) &= c_1, \dots, & u(k-1) &= c_{k-1}, \\ u_{n+k} + a_1 u_{n+k-1} + a_2 u_{n+k-2} + \dots + a_k u_n &= 0 & (n \geq 0), \end{aligned}$$

donde  $c_0, c_1, \dots, c_{k-1}$  y  $a_1, a_2, \dots, a_k$  son constantes. Se conoce con el nombre de **recurrencia lineal** de grado  $k$ . Veremos que para los términos de una sucesión dada por una recurrencia lineal siempre existe una fórmula explícita, aunque no siempre será factible (o sensato) utilizarla. Aquí nos limitaremos al caso  $k = 2$ ; el caso general se discutirá en el capítulo 18.

**Teorema 12.2.** Sea  $(u_n)$  una sucesión que satisface la recurrencia lineal

$$\begin{aligned} u_0 &= c_0, & u_1 &= c_1, \\ u_{n+2} + a_1 u_{n+1} + a_2 u_n &= 0 & (n \geq 0), \end{aligned}$$

y sean  $\alpha$  y  $\beta$  las raíces de la ecuación auxiliar

$$t^2 + a_1 t + a_2 = 0.$$

Si  $\alpha \neq \beta$ , entonces existen constantes  $A$  y  $B$  tales que

$$u_n = A\alpha^n + B\beta^n \quad (n \geq 0),$$

mientras que si  $\alpha = \beta$ , existen constantes  $C$  y  $D$  tales que

$$u_n = (Cn + D)\alpha^n \quad (n \geq 0).$$

Las constantes  $A$  y  $B$  (o bien  $C$  y  $D$ ) están determinadas por  $c_0$  y  $c_1$ .

**DEMOSTRACIÓN:** Si  $\alpha \neq \beta$ , las ecuaciones

$$A + B = c_0, \quad A\alpha + B\beta = c_1,$$

determinan  $A$  y  $B$ :

$$A = \frac{c_1 - c_0\beta}{\beta - \alpha}, \quad B = \frac{c_1 - c_0\alpha}{\alpha - \beta}.$$

Por lo tanto, si asignamos a  $A$  y  $B$  estos valores, el resultado se cumple para  $u_0$  y  $u_1$  y tenemos la base para una demostración mediante el principio fuerte de inducción.

Para la hipótesis de inducción, supongamos que el resultado se cumple para todos los  $u_r$  con  $0 \leq r \leq n+1$  (donde  $n \geq 0$ ). Utilizando la ecuación recurrente para  $u_{n+2}$  y la hipótesis de inducción, tenemos que

$$\begin{aligned} u_{n+2} &= -(a_1 u_{n+1} + a_2 u_n) \\ &= -[a_1(A\alpha^{n+1} + B\beta^{n+1}) + a_2(A\alpha^n + B\beta^n)] \\ &= -A\alpha^n(a_1\alpha + a_2) - B\beta^n(a_1\beta + a_2) \\ &= A\alpha^{n+2} + B\beta^{n+2}. \end{aligned}$$

El último paso es utilizar el hecho de que  $\alpha$  y  $\beta$  son raíces de la ecuación cuadrática y concluir que el resultado se cumple para  $u_{n+2}$ ; por el principio fuerte de inducción, se cumple para todo  $u_n$  con  $n \geq 0$ .

Si  $\alpha = \beta$  aplicamos el mismo método con la fórmula alternativa.  $\square$

El teorema proporciona un método simple para hallar una fórmula para los términos de una sucesión  $(u_n)$  que satisface una recurrencia lineal con  $k = 2$ . No tenemos más que resolver la ecuación cuadrática y determinar las constantes  $A$  y  $B$  (o bien  $C$  y  $D$ ) que cuadren con los valores especificados de  $u_0$  y  $u_1$ .

**Ejemplo.** Hallar una fórmula explícita para  $u_n$  si

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+2} - 5u_{n+1} + 6u_n = 0 \quad (n \geq 0).$$

SOLUCIÓN: La ecuación auxiliar es

$$t^2 - 5t + 6 = 0.$$

Sus raíces son  $\alpha = 2$  y  $\beta = 3$ , de modo que la fórmula para  $u_n$  es de la forma  $A(2^n) + B(3^n)$ . Los valores indicados de  $u_0$  y  $u_1$  dan lugar a las ecuaciones

$$A + B = 0, \quad 2A + 3B = 1,$$

que tienen por solución  $A = -1$  y  $B = 1$ . La fórmula para  $u_n$  es, pues,

$$u_n = 3^n - 2^n. \quad \square$$

Nótese que las raíces  $\alpha$  y  $\beta$  pueden ser números reales o complejos en lugar de enteros. Si los valores iniciales  $c_0$  y  $c_1$  y los coeficientes  $a_1$  y  $a_2$  son enteros, es evidente por la forma de la propia recurrencia que cada  $u_n$  ha de ser entero. Sin embargo en la fórmula para  $u_n$  pueden intervenir potencias de números no enteros. Este es el caso del ejercicio 12.2.2, por ejemplo, donde las raíces de  $\alpha$  y  $\beta$  son  $\frac{1}{2}(1+\sqrt{5})$  y  $\frac{1}{2}(1-\sqrt{5})$ . Cuando  $\alpha$  y  $\beta$  son números complejos, el teorema de De Moivre nos permite a menudo simplificar la solución. Por ejemplo, si tenemos

$$u_0 = 2, \quad u_1 = 0, \quad u_{n+2} + u_n = 0 \quad (n \geq 0),$$

la ecuación auxiliar es  $t^2 + 1 = 0$  y sus raíces  $i$  y  $-i$ . Con los valores de  $u_0$  y  $u_1$  se obtiene la fórmula

$$u_n = i^n + (-i)^n,$$

que puede expresarse en la forma

$$u_n = 2 \cos \frac{1}{2}n\pi.$$

Esto no es más que una manera complicada de decir que los términos de la sucesión son  $2, 0, -2, 0, 2, 0, -2, 0, \dots$ , lo que, por otra parte, es una consecuencia directa evidente de la ecuación recurrente. Tenemos un nuevo ejemplo de la regla de que en muchas ocasiones es más útil la propia ecuación que una fórmula.

### Ejercicios 12.2

1 Hallar una fórmula explícita para  $u_n$  si

- (i)  $u_0 = 1, \quad u_1 = 1, \quad u_{n+2} - 3u_{n+1} - 4u_n = 0 \quad (n \geq 0);$
- (ii)  $u_0 = -2, \quad u_1 = 1, \quad u_{n+2} - 2u_{n+1} + u_n = 0 \quad (n \geq 0).$

2 Los números de Fibonacci  $F_n$  se definen por la recurrencia

$$F_0 = 1, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n \quad (n \geq 0).$$

Demostrar que

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left( \frac{1 - \sqrt{5}}{2} \right)^{n+1} \right].$$

3 Sea  $q_n$  el número de palabras de longitud  $n$  en el alfabeto  $\{0, 1\}$  con la propiedad de que no hay dos ceros consecutivos. Demostrar que

$$q_1 = 2, \quad q_2 = 3, \quad q_{n+2} = q_{n+1} + q_n \quad (n \geq 0).$$

4 ¿Qué relación hay entre los números de Fibonacci y los números  $q_n$  definidos en el ejercicio anterior? Usar esta relación para dar una fórmula explícita para  $q_n$ .

5 Sin usar la fórmula de los números de Fibonacci, demostrar que

- (i)  $F_{n+2} = F_n + F_{n-1} + \dots + F_1 + 2,$
- (ii)  $F_n F_{n+2} = F_{n+1}^2 + (-1)^n.$

### 12.3 Bisección recursiva

Al discutir la ordenación por inserción (apartado 7.8), mencionamos el método de la bisección reiterada. En numerosos algoritmos se usa un método similar, que nos lleva a estudiar recurrencias de la forma general

$$u_{2n} = P u_n + Q(n),$$

donde  $P$  es una constante y  $Q$  una función de  $n$ . Por supuesto, una recurrencia de este tipo no determina  $u_n$  para todos los valores de  $n$ , pero dado

$u_2$  (por ejemplo), podemos calcular  $u_4, u_8, u_{16}$ , etc. El comportamiento de estos términos puede ser suficiente para indicar el comportamiento de la sucesión  $(u_n)$ . El método también se conoce con el nombre de "divide y vencerás".

**Ejemplo.** Sea  $S$  un conjunto de  $n = 2^k$  enteros distintos ( $k \geq 1$ ). Demostrar que el máximo y el mínimo de  $S$  pueden hallarse con

$$f_n = \frac{3}{2}n - 2$$

comparaciones binarias. ¿Qué puede afirmarse si  $n$  no es una potencia de 2?

**SOLUCIÓN:** Antes que nada, es interesante observar que para hallar el máximo de un conjunto de  $n$  enteros necesitamos hacer  $n-1$  comparaciones (ya que el máximo puede ser el último entero examinado). Igualmente, son necesarias  $n-1$  comparaciones para hallar el mínimo. Así pues, si las dos búsquedas se hacen independientemente, necesitaremos  $2n-2$  comparaciones.

Para obtener la mejora enunciada hemos de proceder del siguiente modo. Partimos el conjunto  $S$  en dos subconjuntos  $S_1$  y  $S_2$  de tamaño  $n/2 = 2^{k-1}$ ; supongamos que el máximo y el mínimo de  $S_i$  son  $\sigma_i$  y  $\tau_i$  ( $i = 1, 2$ ). El máximo de  $S$  es el mayor de  $\sigma_1$  y  $\sigma_2$ , y el mínimo de  $S$  es el menor de  $\tau_1$  y  $\tau_2$ . Si  $f_{n/2}$  es el número de comparaciones necesarias para hallar el máximo y el mínimo de un conjunto de tamaño  $n/2$  (como  $S_1$  y  $S_2$ ), hemos demostrado que

$$f_n = f_{n/2} + 2.$$

Con esta recurrencia podemos demostrar que

$$f_{2^k} = 3 \cdot 2^{k-1} - 2 \quad (k \geq 1).$$

Es evidente que es necesaria una comparación si  $|S| = 2$ , de modo que  $f_2 = 1$  y la fórmula se cumple para  $k = 1$ . Si suponemos que se cumple para  $f_{2^{k-1}}$  y utilizamos la recurrencia, entonces

$$f_{2^k} = 2(3 \cdot 2^{k-2} - 2) + 2 = 3 \cdot 2^{k-1} - 2,$$

con lo que se cumple la fórmula para  $f_{2^k}$ . En consecuencia, la fórmula se cumple para todo  $n$  potencia de 2 y con la sustitución  $n = 2^k$  obtenemos la forma original.

El caso en que  $n$  no es una potencia de 2 se trata del siguiente modo. En primer lugar partimos  $S$  en un conjunto  $S_1$  de tamaño  $2^m$  y un conjunto  $S_2$  de tamaño  $n - 2^m$ , donde  $2^m$  es la mayor potencia de 2 menor que  $n$ . Ahora no hay más que repetir el proceso para  $S_2$ , y así sucesivamente. Por ejemplo, si  $n = 26$ , tenemos que  $26 = 16 + 10$  y  $10 = 8 + 2$  y, por el argumento básico anterior,

$$f_{26} = f_{16} + f_{10} + 2, \quad f_{10} = f_8 + f_2 + 2.$$

Sustituyendo las fórmulas conocidas para  $f_2, f_8$  y  $f_{16}$ , hallamos que

$$\begin{aligned} f_{10} &= (\frac{3}{2} \cdot 8 - 2) + (\frac{3}{2} \cdot 2 - 2) + 2 = \frac{3}{2} \cdot 10 - 2, \\ f_{26} &= (\frac{3}{2} \cdot 16 - 2) + (\frac{3}{2} \cdot 10 - 2) + 2 = \frac{3}{2} \cdot 26 - 2. \end{aligned}$$

De esta forma se puede demostrar que  $f_n = \frac{3}{2}n - 2$  si  $n$  es par (si  $n$  es impar, una modificación trivial nos permite tratar el que "sobra").  $\square$

### Ejercicios 12.3

1 Demostrar que si

$$u_2 = 5, \quad u_{2r} = 2u_r + 3 \quad (r = 2^k, k \geq 1),$$

entonces  $u_n = 4n - 3$  para todo  $n$  que sea una potencia de 2.

2 Demostrar que si

$$u_2 = 5, \quad u_{r+s} = u_r + u_s + 3 \quad (r \geq s \geq 2),$$

entonces  $u_n = 4n - 3$  siempre que  $n$  sea par. [Indicación: escribir  $n$  como suma de potencias 2 y utilizar el ejercicio 1.]

3 Hallar una fórmula explícita para  $a_n$  cuando  $n$  es una potencia de 4 y

$$a_1 = 2, \quad a_{4n} = 2a_n + 4n \quad (n = 4^k, k \geq 0).$$

4 Una versión del algoritmo de *ordenación por fusión* procede del siguiente modo: si la lista es  $x_1, x_2, \dots, x_n$ , donde  $n$  es una potencia de 2, se

comparan  $x_1$  y  $x_2$  y se ordenan, se repite con  $x_3$  y  $x_4$ ,  $x_5$  y  $x_6$ , etc. Luego se fusionan los pares ordenados  $(x_1, x_2)$  y  $(x_3, x_4)$  en una sola lista ordenada, y así sucesivamente. Demostrar que el número de comparaciones binarias necesarias satisface

$$u_2 = 1, \quad u_{2n} = 2u_n + 2n - 1.$$

Deducir que  $u_n$  es  $O(n \log n)$ .

## 12.4 Optimización recursiva

En este apartado mostraremos cómo usar un método recursivo para hallar el valor máximo de una función de varias variables. La idea viene a ser resolver el problema por etapas, de modo que cada etapa suponga un problema de optimización relativamente simple.

**Ejemplo.** Un especulador tiene 5 millones de libras y piensa invertir su capital en tres compañías  $C_1$ ,  $C_2$  y  $C_3$  (en unidades de 1 millón de libras). Al invertir  $x$  unidades ( $0 \leq x \leq 5$ ) en las compañías respectivas hace la siguiente previsión de beneficios:

$x = 5$	$x = 4$	$x = 3$	$x = 2$	$x = 1$	$x = 0$
$C_1$	8	7	6	4	1
$C_2$	11	10	8	5	3
$C_3$	11	11	10	2	0

¿Cómo ha de invertir su dinero para obtener el máximo beneficio?

**SOLUCIÓN:** Atacaremos el problema por etapas: la etapa  $i$  será la inversión en  $C_i$  ( $i = 1, 2, 3$ ).

*Etapa 1* Si se invierten  $x_1$  unidades en  $C_1$ , el beneficio  $r_1(x_1)$  viene dado directamente por la tabla. Para uniformizar la notación, definimos

$$y_1 = \text{inversión total hasta el momento} (= x_1),$$

$$f_1(y_1) = \text{beneficio máximo de este total} (= r_1(x_1)).$$

Con esta notación, tenemos los valores

$y_1$	5	4	3	2	1	0
$f_1(y_1)$	8	7	6	4	1	0

*Etapa 2* Supongamos que se invierten  $x_2$  unidades adicionales en  $C_2$ , con un beneficio  $r_2(x_2)$  como en la tabla inicial. Sea

$$y_2 = \text{inversión total hasta el momento} (= y_1 + x_2),$$

$$f_2(y_2) = \text{beneficio máximo de este total.}$$

El cálculo de  $f_2(y_2)$  puede hacerse en forma tabular (tabla 12.4.1), tal como se explica a continuación.

Como la cantidad total disponible es de 5 unidades, sólo hay que calcular los beneficios máximos para  $0 \leq y_2 \leq 5$ . Cada valor  $y_2$  de éstos proviene de varios pares de valores  $x_2$  e  $y_1$ , indicados en las diagonales de la tabla. El valor de  $f_2(y_2)$  es el máximo de la diagonal correspondiente, es decir,

$$f_2(y_2) = \max\{f_1(y_1) + r_2(x_2)\},$$

donde el máximo se toma sobre los valores de  $x_2$  e  $y_1$  tales que  $y_1 + x_2 = y_2$ .

Tabla 12.4.1

$x_2$	$r_2(x_2)$	5	4	3	2	1	0	$y_1$	$f_1(y_1)$
5	11								11
4	10								10
3	8								8
2	5								5
1	3								3
0	0	8	7	6	4	1	0		
		5	4	3	2	1	0	$y_2$	
		12	10	8	5	3	0		$f_2(y_2)$

*Etapa 3* Supongamos que se invierten  $x_3$  unidades adicionales en  $C_3$ , con un beneficio  $r_3(x_3)$  como en la tabla inicial. Sea

$$y_3 = \text{inversión total hasta el momento} (= y_2 + x_3),$$

$$f_3(y_3) = \text{beneficio máximo de este total.}$$

Como esta es la etapa final y hay 5 unidades disponibles, sólo hemos de considerar el caso  $y_3 = 5$ . Manteniendo la uniformidad con la etapa 2, presentamos los cálculos en la tabla 12.4.2.

Tabla 12.4.2

$x_3$	$r_3(x_3)$	5	4	3	2	1	0	$y_2$	$f_2(y_2)$
5	11								
4	11								
3	10								
2	2								
1	0								
0	0	12	10	15	14	11			
		5					$y_3$		
		15					$f_3(y_3)$		

Vemos que  $f_3(5) = 15$ , donde

$$f_3(y_3) = \max\{f_2(y_2) + r_3(x_3)\}$$

y el máximo se toma sobre los valores de  $x_3$  e  $y_2$  para los que  $y_2 + x_3 = y_3$ .

La conclusión es que el beneficio máximo es de 15 unidades. Si miramos de nuevo las tablas, vemos que  $f_3(5) = 15$  se obtiene cuando  $x_3 = 3$  e  $y_2 = 2$ , y que el valor  $f_2(2) = 5$  se obtiene cuando  $x_2 = 2$  e  $y_1 = x_1 = 0$ . El especulador no debe invertir nada en  $C_1$ , 2 unidades en  $C_2$  y 3 unidades en  $C_3$ .  $\square$

En la solución del ejemplo hemos invocado implícitamente un principio muy útil. En cada etapa sólo hemos calculado el máximo beneficio  $f_i(y_i)$  para cada valor factible de  $y_i$ ; la razón de que esto funcione es la siguiente: *si en la mejor política global interviene un valor particular de  $y_i$ , entonces la política en la etapa  $i$  ha de ser necesariamente la mejor para este valor de  $y_i$ .*

Tal como indica el ejemplo, este “principio de optimidad” es fundamental en la técnica de la optimización recursiva. El siguiente símil puede ayudar a comprenderlo. Si la mejor ruta de Londres a París es a través de Dover, hay que utilizar necesariamente la mejor ruta de Londres a Dover; si, por otra parte, la mejor ruta es a través de Newhaven, hay que usar necesariamente la mejor ruta entre Londres y Newhaven.

### Ejercicios 12.4

- 1 Un gerente tiene 6 unidades para invertir en cuatro compañías  $C_1, C_2, C_3$  y  $C_4$ , pero las compañías  $C_1$  y  $C_2$  sólo permiten inversiones en múltiplos de dos unidades. Si los beneficios previstos son los de la tabla 12.4.3, hallar el máximo beneficio posible. ¿Es única la mejor política de inversión?

Tabla 12.4.3

Inversión	Compañía			
	$C_1$	$C_2$	$C_3$	$C_4$
0	0	0	0	0
1	—	—	0	2
2	0	3	1	3
3	—	—	3	4
4	4	6	5	4
5	—	—	7	4
6	8	9	9	4

- 2 El propietario de tres tiendas ha comprado cinco cajas de fresas frescas. Las tiendas están en diferentes áreas y el comportamiento de las ventas varía; por ejemplo, en la tienda  $B$  los clientes pagan precios altos pero el volumen de ventas es pequeño, por lo que las fresas pueden estropearse antes de poder venderse. Por este motivo, el propietario estima el beneficio de adjudicar  $x$  cajas a las tiendas tal como muestra la tabla 12.4.4. Hallar la distribución que da el máximo beneficio (es posible que algunas tiendas se queden sin fresas).

Tabla 12.4.4

$x$	Tienda		
	$A$	$B$	$C$
1	3	5	4
2	7	10	6
3	9	11	11
4	12	11	12
5	13	11	12

## 12.5 El marco de la programación dinámica

El método utilizado para resolver el problema del especulador es típico de una técnica general conocida como **programación dinámica**, o simplemente **PD**. El nombre es, de hecho, algo confuso y es bueno recordar que se trata simplemente de una forma de optimización recursiva.

En general, el método de la programación dinámica se basa en la descomposición de un problema en un cierto número finito  $N$  de etapas. Una *etapa  $i$*  prototípico puede representarse con un diagrama como en la figura 12.1.

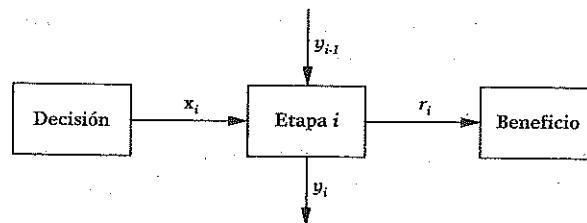


Fig. 12.1 Una etapa prototípica en la programación dinámica.

Los símbolos  $y_{i-1}$  e  $y_i$  representan lo que se conoce como *variables de estado*. El valor de  $y_{i-1}$  depende del valor inicial  $y_0$  y de las decisiones que se han tomado en las etapas  $1, 2, \dots, i-1$ . En la etapa  $i$  se toma una nueva decisión, representada por el valor asignado a la *variable de decisión*  $x_i$  y ésta, junto con  $y_{i-1}$ , determina el valor de  $y_i$ . Expresamos el hecho de que  $y_i$  depende de  $x_i$  e  $y_{i-1}$  utilizando la notación funcional:

$$y_i = y_i(x_i, y_{i-1}).$$

La regla que nos permite determinar  $y_i$  a partir de  $x_i$  e  $y_{i-1}$  se llama la *transformación de etapa*. Finalmente, cada etapa produce un *beneficio de etapa*  $r_i$ , que también depende de la decisión  $x_i$  y de la entrada  $y_{i-1}$ , de modo que escribimos

$$r_i = r_i(x_i, y_{i-1}).$$

Volviendo al ejemplo del apartado 12.4, podemos dar ejemplos concretos de este aluvión de terminología. Tenemos  $N = 3$  etapas, que corresponden

a la inversión en las tres compañías. La variable de estado  $y_i$  representa la inversión total en las compañías  $C_1$  hasta  $C_i$ , mientras que la variable de decisión  $x_i$  representa la cantidad invertida en  $C_i$ . Está claro que la transformación de etapa viene dada por la ecuación

$$y_i = x_i + y_{i-1}.$$

Finalmente, el beneficio de etapa  $r_i$  sólo depende (en este caso) de  $x_i$  y viene dado explícitamente por la tabla al inicio del ejemplo.

El objetivo del especulador es maximizar la suma de los beneficios de etapa, partiendo de que la inversión inicial  $y_0$  es cero y de que  $y_N$ , el número total de unidades compradas, es 5. Por lo general, un problema PD puede consistir en la maximización o minimización de una función más complicada de los beneficios de etapa, pero para nosotros será suficiente considerar la siguiente forma estándar.

Dado el valor inicial  $y_0 = y_0^*$ , maximizar (o minimizar) el beneficio total  $r_1 + r_2 + \dots + r_N$ , entre todos los valores de  $x_1, x_2, \dots, x_N$  que dan lugar a un valor final  $y_N = y_N^*$ .

La esencia del método PD es que nos permite optimizar por etapas, en lugar de hacerlo para todas las variables al mismo tiempo. A menudo esto supone una enorme mejora en la eficiencia (ver ejercicio 12.7.16).

Podemos justificar el método recursivo para tratar la forma estándar del problema DP de la siguiente manera. El problema es hallar

$$\max\{r_1(x_1, y_0^*) + r_2(x_2, y_1) + \dots + r_N(x_N, y_{N-1})\}$$

entre todos los valores  $(x_1, x_2, \dots, x_N)$  que dan  $y_N = y_N^*$ . Lo que es equivalente al problema de hallar

$$\max\{\dots \max\limits_{N} \max\limits_2 \max\limits_1 \{r_1(x_1, y_0^*)\} + r_2(x_2, y_1)\} + \dots + r_N(x_N, y_{N-1})\},$$

donde los máximos sucesivos se toman sobre valores apropiados de las variables. La primera maximización es entre los valores de  $x_1$  que dan un valor determinado de  $y_1$  y el resultado es una función de  $y_1$ :

$$f_1(y_1) = \max\limits_1 \{r_1(x_1, y_0^*)\}.$$

(Recuérdese que  $y_1$  es una función conocida de  $x_1$  e  $y_0$ , y que  $y_0$  ha de tener el valor inicial  $y_0^*$ .) La segunda maximización es entre los valores de  $x_2$  e  $y_1$  que dan un valor determinado de  $y_2$  y el resultado es una función de  $y_2$ :

$$f_2(y_2) = \max_2 \{f_1(y_1) + r_2(x_2, y_1)\}.$$

Prosiguiendo de este modo, vemos que el cálculo en la etapa  $i$  viene dado por

$$f_i(y_i) = \max_i \{f_{i-1}(y_{i-1}) + r_i(x_i, y_{i-1})\},$$

donde el máximo es entre los valores de  $x_i$  e  $y_{i-1}$  que dan el valor de  $y_i$  de acuerdo con la transformación de etapa. En cada etapa intermedia hay que calcular  $f_i(y_i)$  para todos los posibles valores de  $y_i$ , pero en la etapa final sólo es necesario hallar el valor de  $f_N(y_N^*)$ .

En resumen, la solución al problema PD con  $N$  etapas, en la forma estándar anterior, puede hallarse por una recurrencia que consiste en  $N$  problemas de optimización del siguiente tipo:

$$f_1(y_1) = \max \{r_1(x_1, y_0^*)\},$$

$$f_i(y_i) = \max \{f_{i-1}(y_{i-1}) + r_i(x_i, y_{i-1})\} \quad (2 \leq i \leq N).$$

La solución buscada es  $f_N(y_N^*)$ .

### Ejercicios 12.5

- 1 Se define un *problema de inversión* como un problema DP en forma estándar que puede descomponerse en etapas de la siguiente manera: el beneficio de etapa  $r_i$  sólo depende de  $x_i$ , siendo  $x_i$  la variable de decisión que representa una cantidad "invertida" en la etapa  $i$ ; y la variable de estado  $y_i$  representa la cantidad total invertida hasta la etapa  $i$ , inclusive.

Escribir las transformaciones de etapa de un problema de inversión y demostrar que si  $y_0 = 0$ , la recurrencia puede escribirse en la forma

$$f_1(y_1) = r_1(y_1), \quad f_i(y_i) = \max_{y_{i-1}} \{f_{i-1}(y_{i-1}) + r_i(y_i - y_{i-1})\}.$$

- 2 La Compañía Eléctrica Ecléctica tiene seis vendedores que venden sus productos en Berkshire, Hampshire y Surrey. El director gerente estima

que el beneficio mensual (en miles de libras) obtenido al asignar vendedores a los diferentes condados es el que indica la tabla 12.5.1

Tabla 12.5.1

Condado	Número de vendedores						
	0	1	2	3	4	5	6
Berkshire	38	42	48	58	66	72	83
Hampshire	40	42	50	60	66	75	82
Surrey	60	64	68	78	87	102	104

El problema es hallar la asignación de los seis vendedores que proporciona el máximo beneficio.

Formularlo como un problema de inversión e identificar las variables de estado, las variables de decisión y los beneficios de etapa. Resolver el problema.

Si suponemos que dos vendedores se despiden para montar su propio negocio, ¿cuál es la mejor asignación de los vendedores restantes?

### 12.6 Ejemplos del método de la programación dinámica

En este apartado se discuten dos ejemplos del amplio espectro de aplicación del método PD. En los ejercicios al final del capítulo pueden encontrarse más ejemplos.

**Ejemplo.** Un excursionista ha de llenar su mochila con latas, paquetes de galletas, guías, etc.; cada objeto tiene un peso conocido y una cierta "utilidad" para el viaje. Sea  $W$  el peso total que puede llevar,  $P_1, P_2, \dots, P_n$  las diferentes clases de objetos y sean  $w_i$  el peso y  $u_i$  la utilidad de cada objeto  $P_i$ . Sea finalmente  $x_i$  el número de objetos  $P_i$  seleccionados. El *problema de la mochila* es hallar  $x_1, x_2, \dots, x_n$  de forma que la utilidad

$$u_1x_1 + u_2x_2 + \dots + u_nx_n$$

sea máxima, dado que el peso total está limitado por la ecuación

$$w_1x_1 + w_2x_2 + \dots + w_nx_n \leq W.$$

(Debería resultar claro que este problema se presenta en muchas situaciones prácticas, generalmente más serias que el excursionismo.)

Formular el problema general en la terminología PD y utilizar el método PD para resolver el problema cuando  $n = 3$ ,  $W = 10$ , y  $w_i$  y  $u_i$  vienen dados por la tabla

$i$	1	2	3
$w_i$	4	3	1
$u_i$	5	2	1

**SOLUCIÓN:** Tomamos como etapa  $i$ -ésima la asignación de  $P_i$  ( $1 \leq i \leq n$ ). Las variables de decisión no son más que las  $x_i$  definidas antes, mientras que las variables de estado y los beneficios de etapa son

$$y_i = \text{peso de la asignación de } P_1, P_2, \dots, P_i,$$

$$r_i = \text{utilidad de la asignación de } P_i (= u_i x_i).$$

En consecuencia, las transformaciones de etapa son

$$y_i = y_{i-1} + w_i x_i \quad (1 \leq i \leq n),$$

con condiciones iniciales  $y_0 = 0$  e  $y_n = W$ . La recurrencia es

$$f_1(y_1) = u_1 x_1, \quad f_i(y_i) = \max\{f_{i-1}(y_{i-1}) + u_i x_i\} \quad (2 \leq i \leq n),$$

donde  $y_1 = w_1 x_1$  y el máximo es sobre los valores de  $x_i$  e  $y_{i-1}$  tales que  $y_{i-1} + w_i x_i = y_i$ .

En el ejemplo numérico, nótese en primer lugar que los valores de  $W$  y  $w_i$  implican que  $0 \leq x_1 \leq 2$ ,  $0 \leq x_2 \leq 3$ . Los cálculos en las dos primeras etapas son los siguientes:

Etapa 1	$x_1$	0	1	2
	$y_1$	0	4	8
	$f_1(y_1)$	0	5	10.

Etapa 2	$x_2$	0	0	0	1	1	2	2	3
	$y_1$	0	4	8	0	4	0	4	0
	$y_2$	0	4	8	3	7	6	10	9

$$f_2(y_2) = f_1(y_1) + u_2 x_2 \quad 0 \quad 5 \quad 10 \quad 2 \quad 7 \quad 4 \quad 9 \quad 6.$$

Por fortuna, cada valor de  $y_i$  sólo proviene de un par  $(x_2, y_1)$ , de modo que en el cálculo de  $f_2(y_2)$  no hay que maximizar. En la tercera etapa solamente hay que considerar los pares  $(x_3, y_2)$  tales que  $y_2 + x_3 = y_3 = 10$ .

Etapa 3	$x_3$	0	1	2	3	4	5	6	7	8	9	10
	$y_2$	10	9	8	7	6	—	4	3	—	—	0
	$y_3$	10	10	10	10	10		10	10			10
	$f_3(y_3) = f_2(y_2) + u_3 x_3$	9	7	12	10	8		11	9			10.

Vemos que  $f_3(10)$  es el máximo de los valores de la última fila, es decir,  $f_3(10) = 12$ . Deshaciendo los cálculos, vemos que proviene de la asignación  $x_1 = 2$ ,  $x_2 = 0$  y  $x_3 = 2$ .  $\square$

**Ejemplo.** Hallar el camino dirigido más corto de  $s$  a  $t$  en la red de la figura 12.2

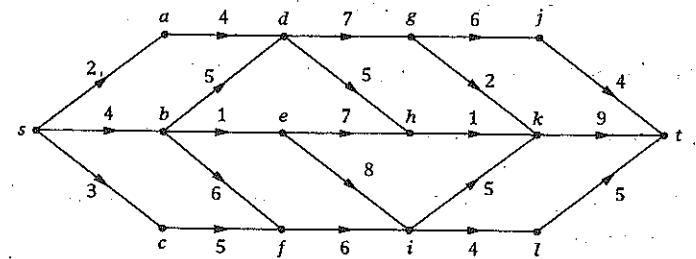


Fig. 12.2 Hallar el camino más corto de  $s$  a  $t$ .

**SOLUCIÓN:** El diagrama de la red sugiere que dispongamos los vértices en seis "líneas";  $s$  en la línea 0,  $a, b, c$  en la línea 1, etc. Así podemos considerar el proceso de ir de la línea  $i - 1$  a la línea  $i$  como la etapa  $i$  de un programa dinámico. Las variables de decisión y de estado son

$$x_i = \text{arco elegido para ir de la línea } i - 1 \text{ a la } i,$$

$$y_i = \text{vértice en la línea } i.$$

El beneficio de etapa  $r_i$  es  $l(x_i)$ , la longitud de  $x_i$ , según indica el diagrama y la transformación de etapa es la regla que, dado un vértice  $y_{i-1}$  en la línea  $i-1$  y un arco  $x_i = (y_{i-1}, y_i)$ , define el vértice  $y_i$  en la línea  $i$ . Las condiciones de contorno son  $y_0 = s$  e  $y_5 = t$ .

La recurrencia es:

$$f_1(y_1) = l(x_1), \quad \text{donde } x_1 = (s, y_1),$$

$$f_i(y_i) = \min\{f_{i-1}(y_{i-1}) + l(x_i)\} \quad (2 \leq i \leq 5),$$

donde el mínimo es entre los pares  $x_i$  e  $y_{i-1}$  para los que  $x_i$  es un arco de  $y_{i-1}$  a  $y_i$ .

Los cálculos son los siguientes:

<i>Etapa 1</i>	$y_1$	$a$	$b$	$c$
	$f_1(y_1)$	2	4	3
<i>Etapa 2</i>	$y_2$	$d$	$e$	$f$
	$f_2(y_2)$	6	5	8
<i>Etapa 3</i>	$y_3$	$g$	$h$	$i$
	$f_3(y_3)$	13	11	13
<i>Etapa 4</i>	$y_4$	$j$	$k$	$l$
	$f_4(y_4)$	19	12	17
<i>Etapa 5</i>	$y_5$	$t$		
	$f_5(y_5)$	21		

El camino más corto tiene, pues, longitud 21 y es  $s, a, d, h, k, t$ . ( Nótese que los valores  $f_i(y_i)$  asignados a los vértices se obtienen exactamente de la misma manera que las etiquetas del algoritmo más general del apartado 9.6.)  $\square$

### Ejercicios 12.6

1 Hallar la longitud del camino dirigido más corto de  $s$  a  $t$  en la red de la figura 12.3. ¿Cuántos caminos hay de longitud mínima?

2 Resolver el problema de la mochila para  $n = 3$  y  $W = 19$ , si  $w_i$  y  $u_i$  vienen dados por la tabla

$i$	1	2	3
$w_i$	6	4	3
$u_i$	11	7	5.

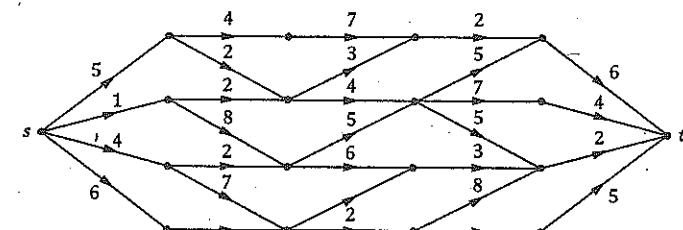


Fig. 12.3 Hallar el camino dirigido mínimo de  $s$  a  $t$ .

### 12.7 Ejercicios diversos

1 Hallar una fórmula explícita para los términos de las sucesiones definidas por

$$(i) u_0 = 0, \quad u_1 = 1, \quad u_{n+2} + u_{n+1} - 2u_n = 0 \quad (n \geq 0);$$

$$(ii) u_0 = 1, \quad u_1 = 0, \quad u_{n+2} - 6u_{n+1} + 8u_n = 0 \quad (n \geq 0).$$

2 Demostrar que  $u_n = n$  satisface la ecuación

$$n(n+1)u_{n+2} - 5n(n+2)u_{n+1} + 4(n+1)(n+2)u_n = 0.$$

Mediante la sustitución  $u_n = nv_n$ , demostrar que la solución para la cual  $u_1 = 12$  y  $u_2 = 60$  es

$$u_n = 3n2^{2n-1} + 6n.$$

3 Hallar una fórmula explícita para el término de la sucesión  $(u_n)$  definida por

$$u_0 = X, \quad u_1 = Y, \quad u_{n+2} = u_n + n \quad (n \geq 0).$$

4 Se dice que una terna  $(a, b, c)$  de enteros es lineal si  $a < b < c$  y  $b - a = c - b$ . Sea  $L_n$  el número de ternas lineales cuyos elementos pertenecen a  $\mathbb{N}_n$ . Demostrar que

$$L_{2n+1} = L_{2n} + n$$

y obtener una ecuación similar para  $L_{2n}$ . Deducir que  $L_n$  cumple la recurrencia del ejercicio 3 y hallar una fórmula para  $L_n$ .

5 Sea  $C_n$  el grafo ciclo con  $n$  vértices, tal como se definió en el apartado 8.3, y sea  $f_n(k)$  el número de vértice-coloraciones de  $C_n$  con  $k$  colores. Dividir el conjunto de coloraciones en dos partes, según que 0 y 2 reciban o no el mismo color, y demostrar que

$$f_n(k) = (k-1)f_{n-2}(k) + (k-2)f_{n-1}(k) \quad (n \geq 5).$$

Deducir que

$$f_n(k) = (k-1)[(k-1)^{n-1} + (-1)^n] \quad (n \geq 3).$$

6 Demostrar que el número de vértice-coloraciones con  $k$  colores de un árbol de  $n$  vértices es  $k(k-1)^{n-1}$ .

7 Decimos que una permutación  $\pi$  de  $\mathbb{N}_n$  es *uniforme* si

$$\pi(i) \leq \pi(i-2) + 2 \quad \text{o bien} \quad \pi(i) \leq \pi(i+1) + 2 \quad (2 \leq i \leq n-1)$$

y

$$\pi(1) \leq \pi(2) + 2 \quad \pi(n) \leq \pi(n-1) + 2.$$

Sea  $x_n$  el número de permutaciones uniformes con  $n = \pi(k)$  y  $n-1 = \pi(k-1)$  o  $\pi(k+1)$  para algún  $k$  de  $\mathbb{N}_n$ , y sea  $y_n$  el número de permutaciones uniformes que no tienen esta propiedad. Demostrar que

$$x_{n+1} = 2x_n + 2y_n,$$

$$y_{n+1} = x_n + 2y_n$$

y hallar una fórmula explícita del número total de permutaciones uniformes.

8 Demostrar que si  $a_n$  satisface la recurrencia de divide y vencerás de la forma

$$a_{2n} = Aa_n + Bn,$$

entonces  $a_n$  es  $O(n \log n)$  si  $A = 2$  y es  $O(n^{\log_2 A})$  si  $A > 2$ .

9 Sea  $t(n)$  el tiempo necesario para multiplicar dos enteros de  $n$  cifras mediante el método de "divide y vencerás" indicado en el ejercicio 7.9.5. Suponiendo que todas las operaciones, salvo las multiplicaciones de una cifra, pueden hacerse en tiempo  $cn$  (donde  $c$  es una constante), demostrar que

$$t(2n) = 3t(n) + 2cn$$

y deducir que  $t(n)$  es  $O(n^{\log_2 3})$ .

10 Sea  $(F_n)$  la sucesión de los números de Fibonacci definida en el ejercicio 12.2.2. Demostrar que

- (i)  $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$ ,
- (ii)  $F_{n+1}^3 + F_n^3 + F_{n-1}^3 = F_{3n}$ .

11 Sea  $\lambda(n, k)$  el número de  $k$ -sunconjuntos de  $\mathbb{N}_n$  que no contienen dos enteros consecutivos. Demostrar que

$$\lambda(n, k) = \lambda(n-2, k-1) + \lambda(n-1, k)$$

y deducir que

$$\lambda(n, k) = \binom{n-k+1}{k}.$$

12 Sea  $\mu(n, k)$  el número de maneras de seleccionar  $k$  objetos entre  $n$  objetos dispuestos en círculo, de forma que no haya dos adyacentes. Demostrar que si  $\lambda(n, k)$  es como en el ejercicio anterior, entonces

$$\mu(n, k) = \lambda(n-1, k) + \lambda(n-3, k-1)$$

y deducir que

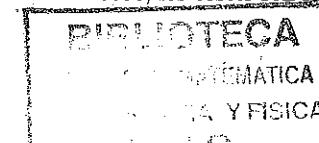
$$\mu(n, k) = \frac{n}{n-k} \binom{n-k}{k}.$$

13 Hallar la solución al problema del director de inversiones (como en el apartado 12.4) si la cantidad disponible es de 6 millones de libras y hay tres compañías que dan los siguientes beneficios.

	$x=6$	$x=5$	$x=4$	$x=3$	$x=2$	$x=1$	$x=0$
$C_1$	9	8	8	6	4	2	0
$C_2$	12	12	12	9	7	3	0
$C_3$	11	10	10	7	2	0	0

14 La producción de Agendas de Mesa para Profesores Despistados se lleva a cabo a lo largo del año y las agendas se almacenan en la fábrica para ser entregadas a finales de septiembre. El número total de agendas a producir es de 19000 y la producción máxima por trimestre es de 6000; los costes son los de la tabla 12.7.1.

Tabla 12.7.1



Número (1000)	Coste (£100)			
	Oct-Dic	Ene-Mar	Abr-Jun	Jul-Sep
0	2	6	5	4
1	4	7	8	5
2	8	9	11	9
3	9	11	15	13
4	11	15	16	15
5	12	19	17	17
6	14	20	20	20

El coste de almacenar las agendas durante un trimestre completo (el coste es nulo para una fracción de trimestre) es de 100 libras por mil unidades. Hacer una tabla que dé el coste total de producción y almacenaje y hallar el calendario de producción de menor coste.

- 15 Un contrabandista opera en un área donde tres países  $X, Y$  y  $Z$  tienen fronteras comunes dos a dos. Cada noche pasa de un país ( $i$ ) a otro ( $j$ ) y obtiene un beneficio  $r_{ij}$  como el que indica la tabla 12.7.2.

Tabla 12.7.2

$i$	$j$		
	$X$	$Y$	$Z$
$X$	—	10	7
$Y$	1	—	4
$Z$	8	2	—

Hoy está en  $X$ . Demostrar que sus máximo beneficio durante las siguientes diez noches es 77 y determinar la ruta óptima.

- 16 Supongamos que un problema de inversión puede expresarse en el esquema PD con  $N$  etapas, de forma que cada variable de decisión  $x_i$  ( $1 \leq i \leq N$ ) puede tomar  $n$  valores enteros. Demostrar que, considerando  $N$  fijo,

- (i) el número de comparaciones necesarias para hallar la solución óptima con el método PD es  $O(n^2)$ ;
- (ii) el número de comparaciones necesarias para hallar la solución óptima evaluando todas las soluciones posibles explícitamente es  $O(n^N)$ .

- 17 Formular el siguiente problema como un programa dinámico con  $N$  etapas. Hallar enteros positivos  $x_1, x_2, \dots, x_k$  que tengan por suma  $N$  y tales que el producto  $x_1 x_2 \cdots x_k$  sea lo mayor posible.

- 18 Resolver los siguientes casos especiales del problema enunciado en el ejercicio anterior:  $N = 13$ ,  $k = 3$  y  $N = 15$ ,  $k = 4$ .

- 19 Un ladrón no puede transportar más de 100kg de objetos robados. Tiene la oportunidad de robar seis objetos que tienen los pesos y valores indicados en la tabla. ¿Qué objetos debe robar? (Este es un problema de la mochila *cero-uno*, ya que las variables de decisión sólo toman los valores 0 y 1.)

Objeto	1	2	3	4	5	6
Peso (kg)	20	50	10	35	48	21
Valor (£K)	2	8	2	3	5	4

### **Parte III   Métodos algebraicos**

---

La tercera parte del libro es la última y la más extensa. Estudiaremos la aplicación de las técnicas algebraicas a problemas de la Matemática Discreta. Aunque para ello deberemos estudiar partes de lo que comúnmente se conoce como álgebra “abstracta”, seguiremos pisando tierra firme.

En las Partes I y II se han cubierto los prerrequisitos para esta parte, excepto que en los capítulos 13, 15 y 17 suponemos un conocimiento del álgebra matricial básica.

## 13 Grupos

---

### 13.1 Los axiomas de grupo

Para un estudio serio de la matemática discreta, es esencial un conocimiento de las técnicas algebraicas modernas. El estudio de las permutaciones, diseños y cuadrados latinos (por ejemplo) está unido inextricablemente a varios aspectos de la teoría algebraica de los grupos, anillos y cuerpos. En este libro estudiaremos estas teorías de manera utilitarista, con la esperanza de que el lector se sienta animado a estudiar el álgebra por sí misma.

La idea básica que subyace en la definición de cualquier estructura algebraica es la de un conjunto con una “operación binaria”. Sea  $X$  un conjunto de objetos con la propiedad de que dos cualesquiera de ellos,  $x$  e  $y$ , pueden combinarse de alguna forma para producir un objeto  $z$ . Esta regla de combinación puede expresarse mediante la ecuación

$$x * y = z,$$

donde el símbolo  $*$  indica una **operación binaria**; la palabra “binario” significa que intervienen dos objetos. Los ejemplos más conocidos son las operaciones aritméticas como  $+$  y  $\times$  definidas en el conjunto  $\mathbf{Z}$  de los enteros. Otro ejemplo importante es la regla para componer permutaciones de  $\{1, 2, \dots, n\}$  en el conjunto  $S_n$ .

Toda operación binaria cumple ciertas propiedades algebraicas. En las primeras páginas de este libro enunciamos las propiedades de las operaciones aritméticas en  $\mathbf{Z}$ , propiedades que evidentemente tienen una importancia fundamental. En el teorema 3.6 obtuvimos cuatro propiedades de la operación de composición en  $S_n$  e hicimos notar que el verdadero significado de esas propiedades aparecería más tarde. El momento ha

llegado: veremos que esas cuatro propiedades son compartidas por muchos otros sistemas y que tienen consecuencias de largo alcance. Por este motivo, los matemáticos utilizan la palabra especial *grupo* para describir uno de tales sistemas.

**Definición.** Un **grupo** consiste en un conjunto  $G$ , junto con una operación binaria  $*$  definida en  $G$  que satisface los siguientes axiomas:

**G1 (Clausura).** Para todos  $x$  e  $y$  de  $G$

$$x * y \text{ está en } G.$$

**G2 (Asociatividad).** Para todos  $x, y, z$  de  $G$

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

**G3 (Neutro).** Existe un elemento  $e$  de  $G$  tal que

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

para todo  $x$  de  $G$ .

**G4 (Inverso).** Para todo  $x$  de  $G$ , existe un  $x'$  de  $G$  tal que

$$x * x' = x' * x = e.$$

Estos axiomas se conocen con los nombres que se indican. Un elemento  $e$  con la propiedad enunciada en **G3** se dice que es un elemento **neutro** de la operación  $*$  en  $G$  y un elemento  $x'$  en **G4** se dice que es un elemento **inverso** de  $x$ .

Si  $G$  es un grupo y  $|G|$  es finito, se dice que  $|G|$  es el **orden** de  $G$ ; un grupo con infinitos elementos se dice que es un grupo de **orden infinito**.

### Ejercicios 13.1

1 Sea  $G = \mathbb{Z}$ . Completar la siguiente tabla, donde  $+$ ,  $-$  y  $\times$  representan las operaciones aritméticas habituales.

$*$	Cerrada	Asociativa	Identidad	Inverso
$+$	✓			
$-$	✓			
$\times$	✓			

2 Repetir el ejercicio 1 con las mismas operaciones, pero tomando  $G = \mathbb{N}$ .

### 13.2 Ejemplos de grupos

Hemos encontrado ya dos ejemplos de grupos. El conjunto de las permutaciones de  $\{1, 2, \dots, n\}$  es un grupo respecto de la composición. Se conoce como el **grupo simétrico** (lo cual explica la notación  $S_n$ ) y su orden es  $n!$  El conjunto  $\mathbb{Z}$  de los enteros es un grupo respecto de la operación suma y tiene orden infinito. Aunque estos fueran los únicos ejemplos, ya valdría la pena estudiar los grupos. Pero la realidad es que el concepto tiene una aplicación tan amplia que penetra toda la matemática moderna. Daremos dos ejemplos más en favor de esta afirmación.

El primer ejemplo será geométrico. Sea  $\Delta$  un triángulo equilátero; puede ser conveniente pensar en  $\Delta$  como en una carta con las esquinas etiquetadas  $A$ ,  $B$  y  $C$ . Existen seis transformaciones distintas de  $\Delta$  con la propiedad de que  $\Delta$  ocupa la misma posición en el espacio antes y después de la transformación. Se conocen cómo simetrías de  $\Delta$  y en la figura 13.1 se indica su efecto sobre la posición de  $\Delta$ .

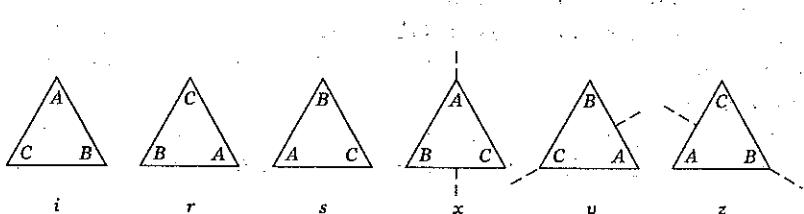


Fig. 13.1 Simetrías de un triángulo equilátero.

En la figura anterior,  $i$  es la simetría trivial que no tiene ningún efecto;  $r$  y  $s$  son rotaciones de  $120^\circ$  y  $240^\circ$  alrededor del baricentro de  $\Delta$  y  $x$ ,  $y$  y  $z$  son reflexiones sobre los ejes que se indican. También podemos pensar en  $x$ ,  $y$  y  $z$  como operaciones que hacen girar  $\Delta$  sobre el eje correspondiente (nótese que los ejes son fijos en el espacio y no se mueven al transformar  $\Delta$ ).

**Ejemplo 1.** Demostrar que  $G_\Delta = \{i, r, s, x, y, z\}$  es un grupo respecto a la operación \* que representa la acción sucesiva de dos simetrías.

**SOLUCIÓN:** Se deduce de consideraciones geométricas generales que la acción de dos simetrías sucesivas es otra simetría. Así pues, si consideramos por ejemplo  $y$  y  $s$ , el resultado de efectuar primero  $s$  y después  $y$  se denota por  $y * s$  (nótese el orden), y para hallar el valor de  $y * s$  podemos estudiar el efecto de las transformaciones como en la figura 13.2. Si comparamos el efecto final de  $y * s$  con la figura 13.1, vemos que  $y * s = z$ .

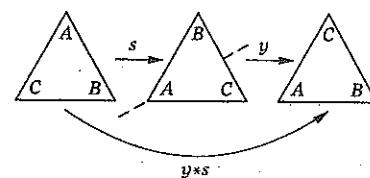


Fig. 13.2  $y * s$  tiene el mismo efecto que  $z$ .

El resultado de estos cálculos puede disponerse convenientemente en la tabla de grupo de  $G_\Delta$  (tabla 13.2.1).

Tabla 13.2.1

	$i$	$r$	$s$	$x$	$y$	$z$
$i$	$i$	$r$	$s$	$x$	$y$	$z$
$r$	$r$	$s$	$i$	$y$	$z$	$x$
$s$	$s$	$i$	$r$	$z$	$x$	$y$
$x$	$x$	$z$	$y$	$i$	$s$	$r$
$y$	$y$	$x$	$z$	$r$	$i$	$s$
$z$	$z$	$y$	$x$	$s$	$r$	$i$

En la tabla, el símbolo de la fila  $y$  y la columna  $s$  es  $z$ , que corresponde al hecho de que  $y * s = z$ . Las otras entradas de la tabla se obtienen análogamente.

Ahora es sencillo comprobar que se cumplen todos los axiomas de grupo. Las propiedades de clausura y asociatividad son consecuencia inmediata de la naturaleza de las simetrías. Resulta claro que el neutro de  $G_\Delta$  es

la simetría trivial  $i$  y que el inverso de cada elemento puede obtenerse a partir de la tabla 13.2.1 de la siguiente forma:

$$\text{Elemento: } i \ r \ s \ x \ y \ z$$

$$\text{Inverso: } i \ s \ r \ x \ y \ z$$

Por lo tanto,  $G_\Delta$  es un grupo.

**Ejemplo 2.** Sea  $G_M$  el conjunto de matrices  $2 \times 2$  de la forma

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix},$$

donde  $\alpha$  y  $\beta$  son elementos de  $\mathbb{Z}_3$  y  $\alpha \neq 0$ . Demostrar que  $G_M$  es un grupo respecto de la multiplicación usual de matrices.

**SOLUCIÓN:** Comprobaremos sucesivamente los axiomas G1-G4.

(G1) El producto de dos matrices de  $G_M$  es

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \alpha\delta + \beta \\ 0 & 1 \end{pmatrix},$$

con lo que el producto tiene la forma necesaria para ser un elemento de  $G_M$  (nótese que, al ser  $\alpha \neq 0$  y  $\gamma \neq 0$ ,  $\alpha\gamma$  no puede ser cero).

(G2) El producto de matrices es siempre asociativo (en el ejemplo actual podría comprobarse explícitamente si fuera necesario).

(G3) Tomando  $\alpha = 1$  y  $\beta = 0$  se obtiene la matriz identidad, que es el neutro de  $G_M$ .

(G4) Para hallar el inverso de un elemento cualquiera de  $G_M$ , observemos que

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

si, y sólo si,

$$\alpha\gamma = 1 \quad \text{y} \quad \alpha\delta + \beta = 0.$$

Dados  $\alpha$  y  $\beta$ , podemos resolver estas ecuaciones en  $\gamma$  y  $\delta$  (recuérdese que al ser  $\alpha \neq 0$ , existe  $\alpha^{-1}$  en  $\mathbb{Z}_3$ ). En concreto,

$$\gamma = \alpha^{-1} \quad \text{y} \quad \delta = -(\alpha^{-1}\beta).$$

Así pues, cada elemento de  $G_M$  tiene un inverso determinado por estas ecuaciones.

### Ejercicios 13.2

- 1 Escribir todas las matrices que pertenecen al grupo del ejemplo 2 (son exactamente seis). Hallar el inverso de cada una de ellas.
- 2 Un cuadrado tiene ocho simetrías. Hacer una lista con todas ellas y calcular la tabla de grupo como en el ejemplo 1.
- 3 ¿Para qué valores de  $n \geq 2$  es cierto que los siguientes son grupos?
  - (i)  $\mathbb{Z}_n$  con la operación  $+$ .
  - (ii)  $\mathbb{Z}_n$  con la operación  $\times$ .
  - (iii)  $\mathbb{Z}_n \setminus \{0\}$  con la operación  $\times$ .
- 4 Calcular la tabla de grupo del conjunto de los números complejos  $\{1, -1, i, -i\}$  respecto del producto y comprobar que es efectivamente un grupo.

### 13.3 Álgebra básica en grupos

En este apartado empezaremos a estudiar las consecuencias de los cuatro axiomas de grupo. Los símbolos que manipularemos serán arbitrarios y no formularemos ninguna hipótesis, salvo el hecho de que satisfacen los axiomas de grupo. Los estudiantes han recibido varios años de entrenamiento algebraico y han aprendido muchas reglas, pero sólo algunas de ellas se aplican en esta situación. Es por eso por lo que el estudio del álgebra abstracta, en la que los símbolos no tienen más propiedades que las enunciadas en los axiomas, puede resultarles difícil en ocasiones.

Empezaremos por librarnos de la molesta notación  $*$  para la operación de grupo y utilizaremos lo que a veces se conoce como notación *multiplicativa*, en la que

$x * y$  se transforma en  $xy$ ,

$e$  se transforma en  $1$ ,

$x'$  se transforma en  $x^{-1}$ .

Esta notación tiene la ventaja de ser económica, pero también el inconveniente de que puede confundirse con la multiplicación usual de números. Hemos de insistir en que las únicas propiedades que podemos suponer son las propiedades de grupo, es decir,

$$x(yz) = (xy)z, \quad xl = l x = x, \quad xx^{-1} = x^{-1}x = 1.$$

En particular, *no* podemos suponer que  $xy = yx$ . Si un par de elementos satisfacen  $xy = yx$ , diremos que  $x$  e  $y$  **comutan**; un grupo es **comutativo** si cada par de elementos comuta (un término alternativo es **abeliano**, en recuerdo del matemático N.H. Abel (1802-1829)).

**Teorema 13.3.1.** Sean  $x, y, z, a$  y  $b$  elementos de un grupo  $G$ . Entonces

$$xy = xz \Rightarrow y = z \quad (\text{simplificación por la izquierda}),$$

y

$$ax = bx \Rightarrow a = b \quad (\text{simplificación por la derecha}).$$

**DEMOSTRACIÓN:** Como  $G$  es un grupo,  $x$  tiene un inverso  $x^{-1}$ . Si multiplicamos la ecuación  $xy = xz$  a la izquierda por  $x^{-1}$  y utilizamos los axiomas como se indica, llegamos a

$$\begin{aligned} x^{-1}(xy) &= x^{-1}(xz) \\ (x^{-1}x)y &= (x^{-1}x)z \quad \text{por (G2)} \\ 1y &= 1z \quad \text{por (G4)} \\ y &= z. \quad \text{por (G3)} \end{aligned}$$

La simplificación por la derecha se demuestra de manera análoga.  $\square$

Sean  $\{g_1, g_2, \dots, g_n\}$  los elementos de un grupo finito. La fila de la tabla de grupo correspondiente al elemento  $g_i$  está formada por los elementos

$$g_1g_i, g_2g_i, \dots, g_ng_i.$$

Son todos distintos, ya que si  $g_ig_r = g_ig_s$ , entonces podemos simplificar por la izquierda para obtener  $g_r = g_s$ . Igualmente, la simplificación por

la derecha implica que los elementos de cualquier columna son todos distintos. En otras palabras,

*la tabla de un grupo es un cuadrado latino.*

El ejemplo más sencillo de cuadrado latino de orden  $m$  es la tabla de grupo de  $\mathbf{Z}_m$  respecto de la operación suma. Ahora sabemos que *cualquier* grupo finito da lugar a un cuadrado latino pero, como cabría esperar, no todo cuadrado latino es la tabla de algún grupo (véase el ejercicio 13.3.5).

**Teorema 13.3.2.** Si  $a$  y  $b$  son elementos de un grupo  $G$ , la ecuación

$$ax = b$$

tiene una solución única en  $G$ .

**SOLUCIÓN:** Si  $x$  y  $\bar{x}$  son soluciones de la ecuación, entonces

$$ax = a\bar{x} \quad (= b),$$

con lo que, por la regla de simplificación,  $x = \bar{x}$ . Esto demuestra que sólo puede existir una solución. Por otra parte,  $x = a^{-1}b$  es una solución, ya que

$$a(a^{-1}b) = (aa^{-1})b = 1b = b.$$

□

En el caso  $a = b$ , el teorema implica que la ecuación  $ax = a$  tiene una única solución. Como un elemento neutro de  $G$  satisface dicha ecuación, deducimos que

*G tiene un único elemento neutro.*

De forma análoga, en el caso  $b = 1$  el teorema implica que la ecuación  $ax = 1$  tiene solución única, y como el inverso de  $a$  la cumple, deducimos que

*cada elemento de G tiene un único inverso.*

Estas observaciones nos permiten hablar *del* neutro de  $G$  y *del* inverso de  $a$  en  $G$ .

### Ejercicios 13.3

- 1 Demostrar que el inverso de  $ab$  es  $b^{-1}a^{-1}$ .
- 2 Demostrar las siguientes implicaciones, donde  $x$  e  $y$  son elementos de un grupo:
  - (i)  $xy = 1 \Rightarrow yx = 1;$
  - (ii)  $(xy)^2 = x^2y^2 \Rightarrow xy = yx.$  ( $x^2$  significa  $xx$ )
- 3 Sea  $G$  un grupo con la propiedad de que  $g^2 = 1$  para todo  $g$  de  $G$ . Demostrar que  $G$  es un grupo commutativo.
- 4 (i) Sea  $G = \{1, a, b, c\}$  un grupo, donde  $1$  es el elemento neutro y  $a^2 = b^2 = c^2 = 1$ . Utilizar la propiedad de cuadrado latino para escribir la tabla completa de  $G$ .
  - (ii) Justificar que el cuadrado latino obtenido a partir de la tabla de grupo de  $\mathbf{Z}_4$  (con respecto a la suma) es esencialmente distinto del obtenido en el apartado (i).
- 5 Demostrar que el siguiente cuadrado latino de orden 5 no es la tabla de ningún grupo.

1	$a$	$b$	$c$	$d$
$a$	$b$	1	$d$	$c$
$b$	$c$	$d$	$a$	1
$c$	$d$	$a$	1	$b$
$d$	1	$c$	$b$	$a$

### 13.4 El orden de un elemento en un grupo

Dado un elemento  $x$  de un grupo  $G$ , podemos definir las potencias negativas y positivas de  $x$  recursivamente:

$$\begin{aligned} x^1 &= x, & x^r &= xx^{r-1} & (r \geq 2), \\ x^{-1} &= x^{-1}, & x^{-s} &= x^{-1}x^{-(s-1)} & (s \geq 2). \end{aligned}$$

Si convenimos en que  $x^0 = 1$  (el neutro), entonces  $x^n$  está definido para todos los enteros  $n$  y se cumplen las reglas conocidas para manipular potencias. Es decir,

$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn} \quad (m, n \in \mathbf{Z}).$$

Al ser  $G$  un grupo,  $x^n$  es un elemento de  $G$  para cada  $n$ , aunque esto no significa que todas las potencias  $x^n$  representen elementos distintos de  $G$ . De hecho, si  $G$  es un grupo *finito*, algunas de las potencias han de ser iguales, ya que son infinitas en número y  $G$  sólo tiene un número finito de elementos. Supongamos que  $x^a = x^b$  con  $a > b$ . Multiplicando a ambos lados de la ecuación por  $x^{-b}$ , se obtiene que  $x^{a-b} = 1$ , donde  $a - b > 0$ . En consecuencia, podemos asegurar que  $x^n = 1$  para algún entero positivo  $n$  y, por el axioma del buen orden, que existe un entero mínimo con esta propiedad.

**Definición.** Si  $x$  es un elemento de un grupo finito  $G$ , llamaremos **orden** de  $x$  al menor entero positivo  $m$  tal que  $x^m = 1$ . Si  $G$  es un grupo infinito, el orden de  $x$  se define de la misma forma, siempre que exista; en caso contrario, se dice que  $x$  tiene **orden infinito**.

En la práctica, obtendremos el orden de un elemento calculando sus potencias positivas hasta llegar al neutro. Por ejemplo, en el grupo  $G_\Delta$  del triángulo, las potencias del elemento  $r$  son

$$r^1 = r, \quad r^2 = s, \quad r^3 = rs = i.$$

Como  $i$  es el elemento neutro, el orden de  $r$  en  $G_\Delta$  es igual a 3.

El resultado más útil sobre el orden de un elemento está contenido en el siguiente teorema.

**Teorema 13.4.** Sea  $x$  un elemento de orden  $m$  en un grupo finito  $G$ . Entonces

$$x^s = 1 \text{ en } G$$

si, y sólo si,  $s$  es un múltiplo de  $m$ .

**DEMOSTRACIÓN:** Si  $s$  es un múltiplo de  $m$ , digamos  $s = mk$ , entonces

$$x^s = x^{mk} = (x^m)^k = 1^k = 1,$$

donde hemos utilizado las reglas usuales para manipular potencias y el hecho de que  $x^m = 1$ .

Recíprocamente, supongamos que  $x^s = 1$ . Según el teorema 1.5 podemos escribir

$$s = mq + r, \quad 0 \leq r < m.$$

Entonces

$$1 = x^s = x^{mq+r} = (x^m)^q x^r = x^r,$$

ya que  $x^m = 1$ . Ahora bien, si  $r > 0$  la ecuación  $x^r = 1$  contradice el hecho de que  $m$  sea el mínimo entero positivo tal que  $x^m = 1$ . En consecuencia, debe ser  $r = 0$  y  $s = mq$ , tal como se afirmaba.  $\square$

### Ejercicios 13.4

1 Sean  $\alpha$  y  $\beta$  las permutaciones de  $N_7$  que en su representación en ciclos son

$$\alpha = (15)(27436), \quad \beta = (1372)(46)(5).$$

Calcular los órdenes de  $\alpha$  y  $\beta$  considerados como elementos del grupo simétrico  $S_7$ . ¿Qué órdenes tienen  $\alpha\beta$  y  $\beta\alpha$ ?

2 Sean  $x$  e  $y$  elementos de un grupo finito  $G$ . Demostrar que  $x$  e  $yxy^{-1}$  tienen el mismo orden.

3 Sea  $M$  el conjunto de las matrices de la forma

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

a coeficientes en  $Z_7$  y tales que  $a \neq 0$ . Demostrar que  $M$  es un grupo con respecto al producto de matrices. Hallar el orden de los elementos

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}.$$

4 Sea  $G$  el grupo definido en el ejercicio 3, salvo que los coeficientes de las matrices son ahora números reales. Demostrar que  $G$  contiene infinitos elementos de orden 2.

5 Sean  $u$  y  $v$  elementos de un grupo commutativo y supongamos que tienen órdenes  $r$  y  $s$ , respectivamente. Demostrar que si  $r$  y  $s$  son primos entre sí, entonces el orden de  $uv$  es  $rs$ .

### 13.5 Isomorfismo de grupos

Recordemos los dos ejemplos considerados en el apartado 13.2. En el primero discutimos el grupo  $G_\Delta$  cuyos elementos son las seis simetrías de un triángulo equilátero,  $G_\Delta = \{i, r, s, x, y, z\}$ . En el segundo ejemplo discutimos otro grupo  $G_M$  que también tenía seis elementos; son las matrices que denotaremos por

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

$$X = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix},$$

donde los símbolos 0, 1 y 2 son elementos de  $\mathbb{Z}_3$ . Por el momento nos olvidaremos de las definiciones de  $G_\Delta$  y  $G_M$  y nos concentraremos en sus tablas respectivas (tablas 13.5.1).

Tabla 13.5.1

	<i>i</i>	<i>r</i>	<i>s</i>	<i>x</i>	<i>y</i>	<i>z</i>		<i>I</i>	<i>R</i>	<i>S</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
<i>i</i>	<i>i</i>	<i>r</i>	<i>s</i>	<i>x</i>	<i>y</i>	<i>z</i>	<i>I</i>	<i>I</i>	<i>R</i>	<i>S</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
<i>r</i>	<i>r</i>	<i>s</i>	<i>i</i>	<i>y</i>	<i>z</i>	<i>x</i>	<i>R</i>	<i>R</i>	<i>S</i>	<i>I</i>	<i>Y</i>	<i>Z</i>	<i>X</i>
<i>s</i>	<i>s</i>	<i>i</i>	<i>r</i>	<i>z</i>	<i>x</i>	<i>y</i>	<i>S</i>	<i>S</i>	<i>I</i>	<i>R</i>	<i>Z</i>	<i>X</i>	<i>Y</i>
<i>x</i>	<i>x</i>	<i>z</i>	<i>y</i>	<i>i</i>	<i>s</i>	<i>r</i>	<i>X</i>	<i>X</i>	<i>Z</i>	<i>Y</i>	<i>I</i>	<i>S</i>	<i>R</i>
<i>y</i>	<i>y</i>	<i>x</i>	<i>z</i>	<i>r</i>	<i>i</i>	<i>s</i>	<i>Y</i>	<i>Y</i>	<i>X</i>	<i>Z</i>	<i>R</i>	<i>I</i>	<i>S</i>
<i>z</i>	<i>z</i>	<i>y</i>	<i>x</i>	<i>s</i>	<i>r</i>	<i>i</i>	<i>Z</i>	<i>Z</i>	<i>Y</i>	<i>X</i>	<i>S</i>	<i>R</i>	<i>I</i>

Resulta claro que ambas tablas son esencialmente la misma —la notación ha sido elegida cuidadosamente para que esto fuera evidente. En lo que se refiere a las propiedades de grupo,  $G_\Delta$  y  $G_M$  son idénticos; sólo difieren en los nombres que damos a sus elementos. Más formalmente, tenemos una biyección  $\beta : G_\Delta \rightarrow G_M$  que lleva *i* a *I*, *r* a *R*, etc. y que conserva la operación de grupo. Por ejemplo,  $rx = y$  en  $G_\Delta$  y  $RX = Y$  en  $G_M$ , lo cual implica que

$$\beta(rx) = \beta(y) = Y = RX = \beta(r)\beta(x).$$

**Definición.** Si  $G_1$  y  $G_2$  son grupos (ambos escritos en notación multiplicativa), una biyección  $\beta : G_1 \rightarrow G_2$  se dice que es un **isomorfismo**

si, para todos  $g$  y  $g'$  de  $G_1$

$$\beta(gg') = \beta(g)\beta(g').$$

Si existe un tal isomorfismo, decimos que  $G_1$  y  $G_2$  son isomorfos y escribimos  $G_1 \approx G_2$ .

### Ejercicios 13.5

1 Describir las cuatro simetrías de un rectángulo y construir la tabla del grupo correspondiente. Mediante una biyección adecuada, demostrar que es isomorfo al grupo que tiene por tabla la 13.5.2.

Tabla 13.5.2

	1	<i>a</i>	<i>b</i>	<i>c</i>
1	1	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	1	<i>c</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>c</i>	1	<i>a</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>a</i>	1

2 Analizando las posibles tablas de grupo, y considerando iguales dos grupos isomorfos, demostrar que

- (i) existe un solo grupo de orden 2;
- (ii) existe un solo grupo de orden 3;
- (iii) existen exactamente dos grupos de orden 4.

3 Demostrar que la relación  $\approx$  de isomorfismo es de equivalencia.

4 Sean  $G_1$  y  $G_2$  dos grupos finitos y  $\beta : G_1 \rightarrow G_2$  un isomorfismo. Si  $x_2 = \beta(x_1)$  para un  $x_1$  de  $G_1$ , demostrar que  $x_1$  y  $x_2$  tienen el mismo orden.

### 13.6 Grupos cíclicos

Desde un punto de vista abstracto, dos grupos isomorfos son el mismo. La noción de isomorfismo nos permite, pues, clasificar los grupos sin

ambigüedades. En la práctica, si hallamos un grupo  $G$  en un contexto particular, por lo general intentaremos demostrar que es isomorfo a un "ejemplo estándar"  $H$  cuyas propiedades son conocidas. Las propiedades de grupo de  $G$  son precisamente las de  $H$  y no es necesario estudiarlas de nuevo.

Para que el programa que acabamos de esbozar tenga sentido, necesitamos naturalmente una provisión de ejemplos estándar.

**Definición.** Se dice que un grupo  $G$  es **cíclico** si posee un elemento  $x$  tal que cada elemento de  $G$  es una potencia de  $x$ . Decimos que el elemento  $x$  **genera**  $G$  y lo denotamos por  $G = \langle x \rangle$ .

Si  $x$  genera  $G$  y todas las potencias de  $x$  son *distintas*, entonces

$$G = \{\dots, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, \dots\}.$$

En este caso, decimos que  $G$  es un **grupo cíclico infinito** y utilizamos el símbolo  $C_\infty$  para un grupo de este tipo. Los grupos isomorfos a  $C_\infty$  son muy frecuentes y aparecen bajo distintas apariencias.

**Ejemplo.** Demostrar que el conjunto  $\mathbf{Z}$  de los enteros con la operación suma es un grupo cíclico infinito.

**SOLUCIÓN:** Tenemos que construir una biyección  $\beta$  entre  $\mathbf{Z}$  y  $C_\infty$  tal que  $\beta(n_1 + n_2) = \beta(n_1)\beta(n_2)$ . Nótese que el signo  $+$  aparece en el lado izquierdo debido a que la operación definida para  $\mathbf{Z}$  es la suma. Si  $x$  es un generador de  $C_\infty$ , definimos  $\beta$  mediante

$$\beta(n) = x^n \quad (n \in \mathbf{Z}).$$

Para cada  $n$  de  $\mathbf{Z}$  existe una potencia  $x^n$  en  $C_\infty$  y son todas distintas, de forma que  $\beta$  es una biyección. Además,

$$\beta(n_1 + n_2) = x^{n_1 + n_2} = x^{n_1}x^{n_2} = \beta(n_1)\beta(n_2),$$

con lo que  $\beta$  es un isomorfismo.  $\square$

Pasamos ahora al caso de un grupo cíclico  $G$  con un generador  $x$  tal que las potencias de  $x$  no son todas distintas. En este caso,  $x$  es un elemento de orden finito  $m$  y

$$G = \{1, x, x^2, \dots, x^{m-1}\},$$

ya que si  $k$  es un entero cualquiera, tenemos  $k = mq + r$  con  $0 \leq r < m$  y

$$x^k = x^{mq+r} = (x^m)^q x^r = 1^q x^r = x^r.$$

En consecuencia, cualquier potencia de  $x$  es igual a uno de los  $m$  elementos de la lista anterior. Estos elementos son distintos, ya que si  $x^i = x^j$  ( $0 \leq i < j \leq m - 1$ ), entonces  $x^{j-i} = 1$ , contradiciendo la definición de  $m$ . En este caso diremos que  $G$  es un **grupo cíclico de orden  $m$**  y lo denotaremos por  $C_m$ . El ejemplo más conocido de un grupo isomorfo a  $C_m$  es el conjunto  $\mathbf{Z}_m$  de los enteros módulo  $m$  con la operación  $+$ . Como en el caso infinito, es fácil demostrar que la función  $\beta : \mathbf{Z}_m \rightarrow C_m$  definida por  $\beta(n) = x^n$  es un isomorfismo.

Una manera de ampliar la lista de ejemplos estándar de grupos es combinar grupos conocidos de alguna forma. Por ejemplo, si tenemos dos grupos  $A$  y  $B$  (ambos escritos en notación multiplicativa) podemos formar su **producto directo**  $A \times B$  de la siguiente forma. Los elementos de  $A \times B$  son los pares ordenados

$$(a, b) \quad (a \in A, b \in B),$$

que se combinan según la operación definida por

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Nótese que en el miembro derecho,  $a_1 a_2$  indica el resultado de combinar  $a_1$  y  $a_2$  según la operación de grupo de  $A$  y  $b_1 b_2$  el de combinar  $b_1$  y  $b_2$  según la de  $B$ .

Es fácil comprobar que  $A \times B$  es efectivamente un grupo con la operación que acabamos de definir (ejercicio 13.6.3).

**Ejemplo.** Hacer una lista con los elementos de  $C_2 \times C_3$  y  $C_2 \times C_4$ . Demostrar que  $C_2 \times C_3$  es isomorfo a  $C_6$ , pero que  $C_2 \times C_4$  no es isomorfo a  $C_8$ .

**SOLUCIÓN:** Supongamos que  $C_2$  y  $C_3$  vienen generados por  $x$  e  $y$  respectivamente, de manera que

$$C_2 = \langle x \rangle = \{1, x\}, \quad C_3 = \langle y \rangle = \{1, y, y^2\}.$$

Según la definición del producto directo, los elementos de  $C_2 \times C_3$  son

$$(1, 1), (1, y), (1, y^2), (x, 1), (x, y), (x, y^2).$$

Pongamos  $z = (x, y)$  y calculemos según la regla anterior; tendremos que

$$\begin{aligned} z^2 &= (1, y^2), & z^3 &= (x, 1), & z^4 &= (1, y), \\ z^5 &= (x, y^2), & z^6 &= (1, 1). \end{aligned}$$

Como  $(1, 1)$  es el neutro de  $C_2 \times C_3$ , hemos demostrado que los elementos de  $C_2 \times C_3$  pueden escribirse como  $1, z, z^2, z^3, z^4, z^5$  y, en consecuencia, se trata de un grupo cíclico de orden 6.

Sea  $u$  un generador de  $C_4$ , de forma que

$$C_4 = \langle u \rangle = \{1, u, u^2, u^3\}.$$

Los elementos de  $C_2 \times C_4$  son

$$(1, 1), (1, u), (1, u^2), (1, u^3), (x, 1), (x, u), (x, u^2), (x, u^3)$$

y sus órdenes son, respectivamente,

$$1, \quad 4, \quad 2, \quad 4, \quad 2, \quad 4, \quad 2, \quad 4.$$

Vemos que no existe ningún elemento de orden 8 en  $C_2 \times C_4$  y, en consecuencia, que  $C_2 \times C_4$  no puede ser isomorfo a  $C_8$ .  $\square$

El hecho de que  $C_2 \times C_3 \approx C_6$  es un caso especial del teorema siguiente.

**Teorema 13.6.** Si  $m$  y  $n$  enteros positivos primos entre sí, entonces

$$C_m \times C_n \approx C_{mn}.$$

**DEMOSTRACIÓN:** Sean  $x$  e  $y$  generadores de  $C_m$  y  $C_n$ , respectivamente,  $z$  el elemento  $(x, y)$  de  $C_m \times C_n$  y  $r$  el orden de  $z$  en  $C_m \times C_n$ . Demostraremos que  $r = mn$ .

Puesto que  $z^r = (x^r, y^r)$  y  $(1, 1)$  es el neutro de  $C_m \times C_n$ , la ecuación  $z^r = 1$  implica que  $x^r = 1$  en  $C_m$  y que  $y^r = 1$  en  $C_n$ . Se deduce del teorema 13.4 que  $r$  es un múltiplo de  $m$  y también un múltiplo de  $n$ . Como  $r$  es el mínimo entero para el cual  $z^r = 1$ , debe ser el mínimo

común múltiplo de  $m$  y  $n$ . Según el ejercicio 1.9.8, y al ser  $m$  y  $n$  primos entre sí,

$$r = \text{mcm}(m, n) = \frac{mn}{\text{mcd}(m, n)} = mn.$$

Pero  $C_m \times C_n$  tiene  $mn$  elementos y contiene un elemento  $z$  de orden  $mn$ ; es, pues, un grupo cíclico.  $\square$

### Ejercicios 13.6

1 Sea  $U$  el subconjunto de  $\mathbb{Z}_7$  formado por los elementos no nulos. Demostrar que la multiplicación en  $\mathbb{Z}_7$  define una operación de grupo en  $U$  y que  $U \approx C_6$ .

2 Sea  $M$  el conjunto de matrices  $2 \times 2$  de la forma

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

con coeficientes enteros. Demostrar que con la multiplicación de matrices  $M$  es un grupo cíclico infinito.

3 Escribir los detalles de la demostración de que el producto directo  $A \times B$  de dos grupos es un grupo.

4 Demostrar que los dos grupos distintos de orden 4 obtenidos en el ejercicio 13.5.2 son isomorfos a  $C_4$  y a  $C_2 \times C_2$ .

### 13.7 Subgrupos

Se dice que un subconjunto  $H$  de un grupo  $G$  es un **subgrupo** de  $G$  si los elementos de  $H$  forman un grupo respecto de la operación de grupo de  $G$ .

**Ejemplo.** Sea  $G_\Delta = \{i, r, s, x, y, z\}$  el grupo de las simetrías del triángulo (ejemplo 1, apartado 13.2). ¿Cuáles de los siguientes subconjuntos de  $G_\Delta$  son subgrupos?

$$H_1 = \{r, s, z\}, \quad H_2 = \{i, r, s\}, \quad H_3 = \{i, r, s, x\}.$$

**SOLUCIÓN:** Hay varios motivos por los que  $H_1$  no es un subgrupo. No es cerrado, ya que  $r$  y  $s$  son de  $H_1$  pero no lo es su producto  $x = rs$ . Además,  $H_1$  no posee elemento neutro.

Por otra parte,  $H_2$  es un subgrupo de  $G_\Delta$ . La "tabla de multiplicar" de  $H_2$  es

	$i$	$r$	$s$
$i$	$i$	$r$	$s$
$r$	$r$	$s$	$i$
$s$	$s$	$i$	$r$

lo cual demuestra que  $H_2$  es cerrado. La propiedad asociativa se cumple en  $H_2$  por cumplirse en  $G_\Delta$  y, claramente,  $i$  es el neutro de  $H_2$  al igual que en  $G_\Delta$ . Finalmente,  $i^{-1} = i$ ,  $r^{-1} = s$  y  $s^{-1} = r$ .

Al no ser cerrado, el subconjunto  $H_3$  no es un subgrupo; por ejemplo,  $rx = y$ , mientras que  $y$  no es de  $H_3$ .  $\square$

Aunque siempre podemos comprobar la propiedad de subgrupo a partir de la tabla de grupo, por lo general no se trata de un método muy práctico. De hecho, podríamos decir que el principal objetivo de la teoría de grupos es estudiar los grupos sin recurrir a las tablas. Teniendo esto en cuenta, formulamos un teorema que da condiciones suficientes para que un subconjunto sea un subgrupo.

**Teorema 13.7.** Sea  $G$  un grupo y  $H$  un subconjunto no vacío de  $G$  que cumple las siguientes condiciones:

- S1.  $x, y \in H \Rightarrow xy \in H;$
- S2.  $x \in H \Rightarrow x^{-1} \in H.$

Entonces  $H$  es un subgrupo de  $G$ . Si  $G$  es finito, la propiedad S1 es suficiente por sí misma para asegurar que  $H$  es un subgrupo.

**DEMOSTRACIÓN:** Las condiciones afirman que  $H$  es cerrado y que cada elemento de  $H$  tiene un inverso. La propiedad asociativa se desprende de la correspondiente propiedad de  $G$ , ya que los elementos de  $H$  son también de  $G$ . Para demostrar que el neutro de  $G$  está en  $H$ , partimos de un elemento  $x$  cualquiera de  $H$ ; por S2,  $x^{-1}$  es de  $H$ , y por S1 el producto  $xx^{-1}$  también. Pero  $xx^{-1} = 1$ , de forma que  $1 \in H$ .

Nos queda por demostrar que, en el caso finito, S1 implica S2. Si  $H$  sólo contiene al neutro, se trata evidentemente de un subgrupo. Si no, sea  $x$  un elemento de  $H$  distinto de 1 y sea  $m$  su orden. Multiplicando la ecuación  $x^n = 1$  por  $x^{-1}$  obtenemos que  $x^{m-1} = x^{-1}$  y, dado que  $m > 1$ ,  $x^{-1}$  es igual a una potencia positiva de  $x$ . Usando S1 repetidamente vemos que cualquier potencia positiva de  $x$  está en  $H$ , con lo que  $x^{-1}$  está en  $H$ .  $\square$

**Ejemplo.** Sea  $G$  un grupo y  $Z(G)$  el subconjunto formado por aquellos elementos que commutan con cualquier elemento de  $G$ , es decir,

$$Z(G) = \{z \in G \mid zg = gz \text{ para todo } g \text{ de } G\}.$$

Demostrar que  $Z(G)$  es un subgrupo de  $G$  (se conoce como el centro de  $G$ ).

**SOLUCIÓN:** Comprobaremos las condiciones S1 y S2. Tomemos  $x$  e  $y$  de  $Z(G)$ , de forma que

$$xg = gx, \quad yg = gy$$

para cualquier  $g$  de  $G$ . Tenemos que

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

con lo que  $xy$  está en  $Z(G)$  y se cumple S1. Por otra parte, si multiplicamos la ecuación  $xg = gx$  por  $x^{-1}$  a ambos lados, tenemos

$$x^{-1}(xg)x^{-1} = x^{-1}(gx)x^{-1}$$

y, utilizando la propiedad asociativa,  $gx^{-1} = x^{-1}g$ . Así pues,  $x^{-1}$  es de  $Z(G)$  y se cumple S2.  $\square$

Si  $x$  es un elemento de orden  $m$  de un grupo  $G$ , los elementos

$$1, x, x^2, \dots, x^{m-1}$$

forman el subgrupo cíclico  $\langle x \rangle$  generado por  $x$ . Es fácil comprobar que  $\langle x \rangle$  es efectivamente un subgrupo (ejercicio 13.7.6) y, evidentemente,

el orden de  $x$  es igual al orden del subgrupo  $\langle x \rangle$ .

Sea, por ejemplo,  $U$  el grupo de los elementos no nulos de  $\mathbb{Z}_7$  respecto del producto (ejercicio 13.6.1). Si calculamos las potencias de 2 en  $U$ , resulta

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1,$$

de forma que 2 tiene orden 3 y el subgrupo cíclico  $\langle 2 \rangle$  contiene los elementos 1, 2 y 4. El subgrupo cíclico  $\langle 3 \rangle$ , por su parte, es todo  $U$ , ya que

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

### Ejercicios 13.7

1 ¿Cuáles de los siguientes son subgrupos de  $G_\Delta$ ?

$$K_1 = \{i, x\}, \quad K_2 = \{i, x, y\}, \quad K_3 = \{i, r, s, x, y\}.$$

2 Utilizar el grupo  $G_\Delta$  para dar un ejemplo de dos subgrupos  $H$  y  $K$  tales que  $H \cup K$  no sea un subgrupo.

3 Demostrar que si  $H$  y  $K$  son subgrupos de  $G$ , también lo es  $H \cap K$ .

4 Sea  $g$  un elemento de un grupo  $G$  y denotemos por  $C(g)$  los elementos de  $G$  que comutan con  $g$ , es decir,

$$C(g) = \{x \in G \mid xg = gx\}.$$

Demostrar que  $C(g)$  es un subgrupo de  $G$ . ¿Cuál es la relación entre estos subgrupos y el centro  $Z(G)$ ?

5 Si  $G$  es el grupo del cuadrado (ejercicio 13.2.2), hallar  $C(g)$  para cada  $g$  de  $G$  y, en consecuencia, hallar  $Z(G)$ .

6 Usar el teorema 13.7 para comprobar que si  $x$  es un elemento de orden  $m$  de un grupo  $G$ , entonces  $\langle x \rangle = \{1, x, \dots, x^{m-1}\}$  es un subgrupo de  $G$ .

### 13.8 Clases laterales y el teorema de Lagrange

En este apartado demostraremos el primer teorema de grupos realmente interesante. Quien comprenda el significado de este teorema, no tendrá dificultad en creer que la teoría de grupos es un tema que abunda en resultados elegantes y fascinantes.

El teorema afirma que si  $H$  es un subgrupo de un grupo finito  $G$ , entonces  $|H|$  es un divisor de  $|G|$ . Por ejemplo, un grupo de orden 20 sólo puede tener subgrupos de órdenes 1, 2, 4, 5, 10 y 20. La idea de la demostración es construir una partición de  $G$  en la que todas las partes tengan el mismo tamaño que  $H$ . Si hay  $k$  partes, entonces deberá ser  $|G| = k|H|$  y tendremos el resultado. Tales partes se conocen como clases laterales.

**Definición.** Sea  $H$  un subgrupo de un grupo  $G$  (no necesariamente finito). Se define la **clase lateral por la izquierda**  $gH$  de  $H$  respecto de un elemento  $g$  de  $G$  como el conjunto que se obtiene al multiplicar cada elemento de  $H$  por la izquierda por  $g$ , es decir,

$$gH = \{x \in G \mid x = gh \text{ para algún } h \in H\}.$$

La **clase lateral por la derecha** de  $H$  respecto  $g$  se define análogamente:

$$Hg = \{x \in G \mid x = hg \text{ para algún } h \in H\}.$$

Si  $H$  es un subgrupo finito, pongamos  $H = \{h_1, h_2, \dots, h_m\}$ , los elementos de la clase lateral por la izquierda  $gH$  son

$$gh_1, gh_2, \dots, gh_m.$$

Es claro que son todos distintos, ya que si  $gh_i = gh_j$  podemos simplificar y tenemos que  $h_i = h_j$ . Tenemos, pues, una propiedad fundamental de las clases laterales:

$$|gH| = |H| \quad (g \in G).$$

Por ejemplo, sea  $G_\Delta = \{i, r, s, x, y, z\}$  el grupo del triángulo y  $H$  el subgrupo  $\{i, x\}$ . Las clases laterales de  $H$  en  $G_\Delta$  son

$$\begin{array}{ll} iH = \{ii, ix\} = \{i, x\}, & rH = \{ri, rx\} = \{r, y\}, \\ sH = \{si, sx\} = \{s, z\}, & xH = \{xi, xx\} = \{x, i\}, \\ yH = \{yi, yx\} = \{y, r\}, & zH = \{zi, zx\} = \{z, s\}. \end{array}$$

Nótese que sólo se obtienen tres subconjuntos distintos como clases laterales de  $G_\Delta$  y que son disjuntas. Así pues, tenemos la partición

$$G_\Delta = \{i, x\} \cup \{r, y\} \cup \{s, z\},$$

tal como muestra la figura 13.3 (en la que cada parte es una clase lateral por la izquierda de  $H$ ).

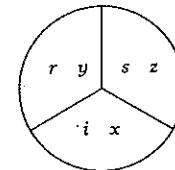


Fig. 13.3 Las clases laterales de  $\{i, x\}$  en  $G_\Delta$ .

La cuestión que a menudo confunde a los principiantes es que, vistas como clases laterales, las partes pueden tener nombres alternativos; por ejemplo,  $\{r, y\}$  puede escribirse como  $rH$  o como  $yH$ . Por lo tanto, hay diferentes maneras de escribir  $G_\Delta$  como unión disjunta de clases laterales, tales como

$$G_\Delta = iH \cup rH \cup sH \quad \text{o} \quad G_\Delta = xH \cup yH \cup zH,$$

aunque las partes son las mismas en cada caso. El siguiente teorema establece la propiedad general que hemos observado en el ejemplo.

**Teorema 13.8.1.** *Sea  $H$  un subgrupo de un grupo  $G$ . Si  $g_1$  y  $g_2$  son elementos de  $G$ , las clases laterales  $g_1H$  y  $g_2H$  son, o bien idénticas, o bien no tienen ningún elemento en común.*

**DEMOSTRACIÓN:** Demostraremos que si  $g_1H$  y  $g_2H$  tienen un elemento en común, entonces son idénticas. Supongamos que  $x$  pertenece a  $g_1H$  y  $g_2H$ , es decir

$$x = g_1h_1 \text{ para algún } h_1 \text{ de } H, \quad x = g_2h_2 \text{ para algún } h_2 \text{ de } H.$$

Para demostrar que  $g_1H \subseteq g_2H$ , sea  $y$  un elemento cualquiera de  $g_1H$ , es decir,  $y = g_1h$  para algún  $h$  de  $H$ . Entonces

$$\begin{aligned} y &= g_1h = (xh_1^{-1})h = x(h_1^{-1}h) \\ &= (g_2h_2)h_1^{-1}h \\ &= g_2(h_2h_1^{-1}h). \end{aligned}$$

Al ser  $H$  un subgrupo,  $h_2h_1^{-1}h$  está en  $H$  y resulta que  $y$  está en  $g_2H$ . Un argumento análogo intercambiando  $g_1$  y  $g_2$  demuestra que  $g_2H \subseteq g_1H$  y con ello la igualdad.  $\square$

Otra manera de demostrar el teorema 13.8.1 es utilizar la teoría de las relaciones de equivalencia. Si definimos una relación  $\sim$  en  $G$  mediante

$$x \sim y \quad \text{si} \quad x^{-1}y \in H,$$

entonces  $\sim$  es una relación de equivalencia y las clases de equivalencia son las clases laterales por la izquierda (ejercicio 13.8.1). La propiedad básica de las relaciones de equivalencia (teorema 5.2) implica que las clases laterales distintas forman una partición de  $G$ . Esta observación fundamental nos lleva inmediatamente a nuestro teorema principal, conocido como **teorema de Lagrange**, en honor de L. Lagrange (1736-1813).

**Teorema 13.8.2.** *Si  $G$  es un grupo finito de orden  $n$  y  $H$  es un subgrupo de orden  $m$ , entonces  $m$  es un divisor de  $n$ .*

**DEMOSTRACIÓN:** Ya hemos visto que todas las clases laterales tienen el mismo cardinal que  $H$  y que las clases distintas forman una partición de  $G$ . Así pues, si hay  $k$  clase laterales distintas, tenemos  $n = km$ .  $\square$

El número de clases laterales distintas es el índice de  $H$  en  $G$  y se escribe  $|G : H|$ , esto es,

$$|G : H| = \frac{|G|}{|H|}.$$

Desde luego, podríamos trabajar con clases laterales por la derecha en lugar de por la izquierda y obtendríamos los mismos resultados. Sin embargo, hacemos notar que no es cierto que las clases laterales por la

izquierda y por la derecha den lugar a la misma partición de  $G$ , a pesar de que su número es el mismo (véase el ejercicio 13.8.2).

Muchos teoremas útiles sobre grupos son consecuencia del teorema de Lagrange. Daremos dos ejemplos.

**Teorema 13.8.3.** *Sea  $g$  un elemento de un grupo finito  $G$  y sea  $|G| = n$ . Entonces*

- (i) *el orden de  $g$  divide a  $n$ ,*      (ii)  $g^n = 1$ .

**DEMOSTRACIÓN:** (i) El orden de  $g$  es el mismo que el orden del subgrupo cíclico  $\langle g \rangle$  y, por el teorema de Lagrange, es un divisor  $d$  de  $n$ .

(ii) Si  $dk = n$ , entonces, dado que  $x^d = 1$ ,

$$x^n = (x^d)^k = 1^k = 1.$$

□

**Teorema 13.8.4.** *Si  $G$  es un grupo de orden primo  $p$ , entonces  $G$  es isomorfo al grupo cíclico  $C_p$ .*

**DEMOSTRACIÓN:** Como  $p > 1$ , el grupo  $G$  posee un elemento  $x \neq 1$ . El orden del subgrupo cíclico  $\langle x \rangle$  es mayor que 1 y, según el teorema de Lagrange, ha de ser un divisor de  $p$ . Al ser  $p$  primo, el orden de  $\langle x \rangle$  es  $p$  y  $\langle x \rangle$  es todo  $G$ . Por lo tanto,  $G$  es un grupo cíclico de orden  $p$ .

En la práctica, el teorema de Lagrange es importante porque restringe el posible orden de los subgrupos (y de los elementos) drásticamente. Sin embargo, no proporciona información sobre el número de subgrupos. Veremos en el siguiente apartado que si  $G$  es cíclico existe exactamente un subgrupo para cada divisor  $d$  de  $|G|$ , pero en general el número de subgrupos podrá ser cualquiera, incluso ninguno. El siguiente ejemplo muestra algunas de las complicaciones que puede presentar el conjunto de los subgrupos en el caso general.

**Ejemplo.** Demostrar que el conjunto  $A_4$  de las permutaciones pares de  $\{1, 2, 3, 4\}$  es un grupo de orden 12 y hallar todos sus subgrupos.

**SOLUCIÓN:** En el apartado 5.6 demostramos que la composición de dos permutaciones pares es par con lo que, según el teorema 13.7,  $A_4$  es

un grupo (de hecho, un subgrupo del grupo simétrico  $S_4$ ). Su orden es  $4!/2 = 12$  (teorema 5.6.2); la siguiente es una lista de las permutaciones que pertenecen a  $A_4$ .

La permutación identidad: id.

Las de orden 2:  $(12)(34)$ ,  $(13)(24)$ ,  $(14)(23)$ .

Las de orden 3:  $(123)$ ,  $(132)$ ,  $(124)$ ,  $(142)$ ,  $(134)$ ,  $(143)$ ,  $(234)$ ,  $(243)$ .

Por el teorema de Lagrange, los posibles órdenes de los subgrupos de  $A_4$  son 1, 2, 3, 4, 6 y 12. Examinaremos estas posibilidades correlativamente.

*Orden 1.* La única posibilidad es el subgrupo trivial  $\{\text{id}\}$ .

*Orden 2.* Por el teorema 13.8.4 (o por el método ingenuo del ejercicio 13.5.2) un subgrupo de orden 2 ha de ser cíclico. Como  $A_4$  tiene tres elementos de orden 2, hay exactamente tres subgrupos de orden 2; por ejemplo,  $\{\text{id}, (12)(34)\}$ .

*Orden 3.* Un argumento parecido nos muestra que hay cuatro (¿por qué no ocho?) subgrupos de orden 3, como  $\{\text{id}, (123), (132)\}$ .

*Orden 4.* Un subgrupo de orden 4 es isomorfo a  $C_4$  o a  $C_2 \times C_2$  (ejercicio 13.6.4). Como no hay elementos de orden 4, no puede ser  $C_4$ . Los tres elementos de orden 2, a saber,  $(12)(34)$ ,  $(13)(24)$  y  $(14)(23)$ , junto con el neutro, sí forman un subgrupo isomorfo a  $C_2 \times C_2$ . Ésta es la única posibilidad, ya que los elementos de orden 3 no pueden pertenecer a un subgrupo de orden 4 (¿por qué?).

*Orden 6.* Supongamos que  $K$  es un subgrupo de orden 6. Como sólo hay cuatro elementos de  $A_4$  que no tienen orden 3,  $K$  debe contener al menos un elemento de orden 3, digamos  $x = (123)$ , y su inverso  $x^{-1} = (132)$ . Los elementos de  $K$  de orden 3 ocurren por parejas, como  $x$  y  $x^{-1}$ , de manera que hay un número par de ellos. Pero  $K$  contiene también el neutro, así que si el número total de elementos ha de ser par,  $K$  debe contener al menos uno de los elementos de orden 2. Ahora bien, si uno de estos elementos  $y$  está en  $K$ , también lo están  $xyx^{-1}$  y  $x^{-1}yx$  (por la propiedad de subgrupo). Estos elementos, por ser conjugados de  $y$ , tienen su mismo tipo y además son distintos. Así pues, los elementos  $y$ ,  $xyx^{-1}$  y  $x^{-1}yx$  son los tres elementos de orden 2,  $(12)(34)$ ,  $(13)(24)$  y  $(14)(23)$ , en algún orden.

Pero hemos demostrado que estos tres elementos, junto con el neutro, forman un subgrupo de orden 4, que ha de ser un subgrupo de  $K$ . Por el

teorema de Lagrange, el orden de  $K$  es un múltiplo de 4, lo cual contradice la hipótesis de que  $|K| = 6$ . Así pues, no existen subgrupos de orden 6.

*Orden 12.* La única posibilidad es el propio  $A_4$ .  $\square$

Es conveniente disponer los subgrupos en un *retículo* (figura 13.4). En general, el retículo de subgrupos puede ser enormemente complicado, pero en el próximo apartado veremos que para un grupo cíclico puede describirse en términos aritméticos sencillos.

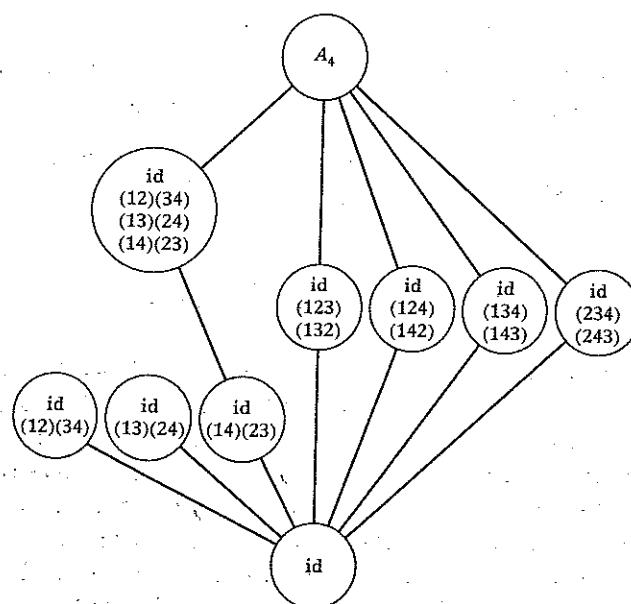


Fig. 13.4 El retículo de subgrupos de  $A_4$ .

### Ejercicios 13.8

- Sea  $H$  un subgrupo de  $G$  y definamos una relación  $\sim$  en  $G$  mediante la regla  $x \sim y \iff x^{-1}y \in H$ . Demostrar que  $\sim$  es una relación de equivalencia y que sus clases de equivalencia son las clases laterales por la izquierda de  $H$ .

- Describir explícitamente la partición del grupo del triángulo mediante las clases laterales por la derecha del subgrupo  $H = \{i, x\}$ . Comprobar que la partición no es la misma que la que proporcionan las clases por la izquierda.
- El grupo de simetría de un pentágono regular es un grupo de orden 10. Demostrar que tiene subgrupos de todos los órdenes permitidos por el teorema de Lagrange y dar un esquema de su retículo de subgrupos.
- Sea  $G$  un grupo finito y  $p$  un número primo, y supongamos que  $G$  tiene exactamente  $m$  subgrupos de orden  $p$ . Demostrar que el número de elementos de orden  $p$  en  $G$  es  $m(p - 1)$ .
- Utilizar el ejercicio 4 para demostrar que un grupo cíclico de orden 55 tiene al menos un subgrupo de orden 5 y uno de orden 11.
- Dar un esquema del retículo de subgrupos del grupo simétrico  $S_4$ . [Indicación: necesitará una hoja de papel grande.]

### 13.9 Caracterización de los grupos cíclicos

En el teorema de Lagrange partimos de una hipótesis algebraica ( $H$  es un subgrupo de  $G$ ) y llegamos a una conclusión aritmética ( $|H|$  divide a  $|G|$ ). Los resultados de este tipo son enormemente útiles, ya que reducen problemas algebraicos difíciles a otros aritméticos más sencillos. En este apartado discutiremos las propiedades aritméticas de los grupos cíclicos y demostraremos que estos grupos pueden caracterizarse mediante propiedades numéricas. Utilizaremos algunas de las técnicas combinatorias desarrolladas en los capítulos 3 y 4, en particular el método de inversión de Möbius y su relación con la función  $\phi$  de Euler.

**Teorema 13.9.** Si  $G$  es un grupo finito de orden  $n \geq 2$ , las siguientes afirmaciones son equivalentes:

- $G$  es cíclico.
- Para cada divisor  $d$  de  $n$ , el número de elementos  $x$  de  $G$  que cumplen  $x^d = 1$  es igual a  $d$ .
- Para cada divisor  $d$  de  $n$ , el número de elementos  $x$  de  $G$  que tienen orden  $d$  es igual a  $\phi(d)$ .

**DEMOSTRACIÓN:** Demostraremos que (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iii)  $\Rightarrow$  (i), de donde se seguirá que las afirmaciones son equivalentes.

(i)  $\Rightarrow$  (ii) Sea  $G$  un grupo cíclico de orden  $n$  generado por  $g$ . Dado un divisor  $d$  de  $n$ , sea  $dk = n$ . Los elementos

$$1, g^k, g^{2k}, \dots, g^{(d-1)k}$$

son distintos y cada uno de ellos satisface la ecuación  $x^d = 1$ , ya que

$$(g^{ik})^d = (g^{kd})^i = (g^n)^i = 1^i = 1.$$

Así pues, tenemos  $d$  elementos de  $G$  que cumplen  $x^d = 1$ . Hemos de demostrar que no hay otras soluciones. Sea  $y$  un elemento de  $G$  tal que  $x^d = 1$ ; como  $G$  está generado por  $g$ , tenemos que  $y = g^e$  para algún  $e \geq 0$  y, por lo tanto,

$$g^{ed} = (g^e)^d = y^d = 1.$$

El orden de  $g$  es  $n$  y, según el teorema 13.4,  $ed$  es un múltiplo de  $n$ , pongamos  $ln$ . Entonces

$$ed = ln = l(dk),$$

con lo que  $e = lk$ ,  $y = g^e = g^{lk}$ , que es uno de los elementos que ya hemos hallado como solución.

(ii)  $\Rightarrow$  (iii) Supongamos (ii) cierto. Por el teorema 13.4, un elemento  $x$  satisface  $x^d = 1$  si, y sólo si, el orden de  $x$  es un divisor  $c$  de  $d$ . Si hay  $\alpha(c)$  elementos de orden  $c$ , debe ser

$$d = \sum_{c|d} \alpha(c).$$

Por la fórmula de inversión de Möbius,

$$\alpha(d) = \sum_{c|d} \mu(c) \frac{d}{c}.$$

Pero la relación entre  $\mu$  y  $\phi$  (página 87) demuestra que el término derecho es igual a  $\phi(d)$ ; esto demuestra (iii).

(iii)  $\Rightarrow$  (i) Si se cumple (iii), sabemos en particular que el número de elementos de orden  $n$  es  $\phi(n)$ , que es mayor que 1. Así pues,  $G$  contiene

al menos un elemento de orden  $n$ . Como  $|G| = n$ , este elemento genera  $G$  y  $G$  es cíclico.  $\square$

En el capítulo 16 utilizaremos esta caracterización numérica para demostrar que una importante clase de grupos, que aparecen en un contexto algebraico más amplio, son grupos cíclicos.

Por el momento, nos contentaremos con usar el teorema para hallar todos los subgrupos  $H$  de un grupo cíclico  $G$  de orden  $n$ . El teorema de Lagrange nos dice que  $|H| = d$  para algún divisor  $d$  de  $n$ , y el teorema 13.8.3 (ii) que cada uno de los  $d$  elementos de  $H$  cumple  $x^d = 1$ . Pero hemos demostrado que  $G$  contiene *exactamente*  $d$  elementos que cumplen  $x^d = 1$ , de forma que  $H$  debe contener precisamente estos elementos. En resumen, hemos demostrado que

*un grupo cíclico de orden  $n$  posee exactamente un subgrupo de cada orden  $d$  que divide a  $n$ , y estos subgrupos son cíclicos.*

Tomemos, por ejemplo, el grupo cíclico  $C_{12}$  generado por el elemento  $z$ . Cada uno de los elementos  $1, z, \dots, z^{11}$  de  $C_{12}$  genera un subgrupo cíclico de  $C_{12}$ ; sabemos además que estos son los únicos subgrupos y que dos subgrupos del mismo orden son iguales. Podemos comprobarlo explícitamente mediante cálculos sencillos como los de la tabla 13.9.1. Otra manera de ilustrar este resultado es decir que el retículo de subgrupos de  $C_{12}$  es igual al retículo de divisores de 12 (figura 13.5).

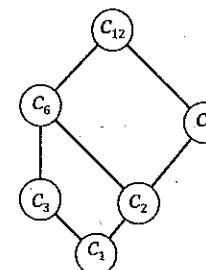


Fig. 13.5 El retículo de subgrupos de  $C_{12}$ .

Tabla 13.9.1

Subgrupo	Elementos	Clase de isomorfismo
$\langle z^6 \rangle$	1, $z^6$	$C_1$
$\langle z^4 \rangle$	1, $z^4$	$C_2$
$\langle z^8 \rangle$	1, $z^4, z^8$	$C_3$
$\langle z^3 \rangle$	1, $z^3$	$C_4$
$\langle z^9 \rangle$	1, $z^3, z^6, z^9$	$C_4$
$\langle z^2 \rangle$	1, $z^2, z^4, z^6, z^8, z^{10}$	$C_6$
$\langle z^{10} \rangle$	1, $z^2, z^4, z^6, z^8, z^{10}$	$C_6$
$\langle z \rangle$	1, $z, z^2, \dots, z^{11}$	$C_{12}$
$\langle z^5 \rangle$	1, $z, z^2, \dots, z^{11}$	$C_{12}$
$\langle z^7 \rangle$	1, $z, z^2, \dots, z^{11}$	$C_{12}$
$\langle z^{11} \rangle$	1, $z, z^2, \dots, z^{11}$	$C_{12}$

## Ejercicios 13.9

- 1 Dar un esquema del retículo de subgrupos del grupo cíclico  $C_{24}$ . Si  $z$  es un generador de  $C_{24}$ , identificar los subgrupos generados por  $z^7, z^8$  y  $z^9$ .
- 2 ¿Cuántos elementos de  $C_{60}$  generan todo el grupo?
- 3 Sean  $r$  y  $s$  divisores de  $n$  y sea  $x$  un generador del grupo cíclico  $C_n$ . Obtener generadores de los subgrupos cíclicos  $C_r$  y  $C_s$  de  $C_n$ . Hallar el orden de  $C_r \cap C_s$  y hallar un generador.
- 4 Explicar cómo deducir el teorema 13.8.4 del teorema 13.9.

## 13.10 Ejercicios diversos

- 1 Sean  $x, y$  y  $z$  elementos de un grupo  $G$ . Simplificar las siguientes expresiones en  $G$ :

$$(i) (x^{-1}z^{-1})(y^{-1}x)^{-1}y, \quad (ii) (xzy)^{-1}x(xyz^{-1})^{-1}.$$

- 2 Si  $x$  e  $y$  son elementos de un grupo  $G$ , el conjugado de  $x$  respecto de  $y$  es  $xyx^{-1}$ , que escribimos  $x^y$ , y el comutador de  $x$  e  $y$  es  $xyx^{-1}y^{-1}$ , que escribimos  $[x, y]$ . Demostrar que, para elementos cualesquiera  $a, b, c$  de  $G$ ,

$$(i) [ab, c] = [b, c]^a [a, c], \quad (ii) [a, bc] = [a, b][a, c]^b.$$

- 3 Sea  $t_{a,b}$  la fución del conjunto de los números reales  $\mathbf{R}$  en sí mismo definida por

$$t_{a,b}(x) = ax + b,$$

donde  $a$  y  $b$  son números reales y  $a \neq 0$ . Demostrar que el conjunto de todas las funciones de este tipo forman un grupo con la composición de funciones.

- 4 Demostrar que el grupo definido en el ejercicio anterior contiene infinitos elementos de orden 2.

- 5 Demostrar que si  $H$  es un subgrupo de índice 2 en un grupo  $G$ , entonces la clase lateral por la izquierda  $gH$  es igual a la clase por la derecha  $Hg$  para todo  $g$  de  $G$ .

- 6 Se define una operación binaria  $*$  en el conjunto  $\mathbf{R}$  de los números reales mediante  $x * y = xy + x + y$ , donde el término de la derecha consiste en las operaciones usuales entre números reales. Demostrar que  $\mathbf{R}$  cumple tres de los axiomas de grupo respecto de  $*$ , pero que no todo elemento tiene un inverso.

- 7 Sean  $\alpha$  y  $\beta$  las funciones definidas (en un subconjunto apropiado de los números reales) por

$$\alpha(x) = 1/x, \quad \beta(x) = 1/(1-x).$$

Sea  $K$  el grupo obtenido mediante la composición de  $\alpha$  y  $\beta$  y sus potencias de todas las formas posibles. Demostrar que  $K$  es isomorfo al grupo del triángulo  $G_\Delta$  definido en el apartado 13.2.

- 8 Sea  $J_m$  el conjunto de los números complejos  $z$  tales que  $z^m = 1$ , donde  $m$  es un entero positivo. Demostrar que  $J_m$  es un grupo cíclico de orden  $m$  con respecto al producto de números complejos.

- 9 Demostrar que el conjunto de las matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (a, b, c, d \in \mathbf{R}),$$

tales que  $ad \neq bc$  es un grupo respecto del producto de matrices.

- 10 Sean  $K$  y  $L$  subgrupos finitos de un grupo  $G$  y sea

$$KL = \{g \in G \mid g = kl \text{ para algún } k \in K \text{ y } l \in L\}.$$

Demostrar que  $|K||L| = |KL||K \cap L|$ .

- 11 Demostrar que el subconjunto  $KL$  definido en el ejercicio anterior es un subgrupo de  $G$  si, y sólo si,  $KL = LK$ .

- 12 Demostrar que todo grupo de orden 6 es isomorfo a  $C_6$  o a  $S_3$ .

13 Sean  $H$  y  $K$  subgrupos finitos de un grupo  $G$  tales que  $\text{mcd}(|H|, |K|) = 1$ . Demostrar que  $|H \cap K| = 1$ .

14 Sea  $X$  el conjunto de pares ordenados  $(n, f)$ , donde  $n$  es un número entero y  $f$  uno racional (una fracción). Se define una operación binaria  $\circ$  en  $X$  mediante la regla

$$(n_1, f_1) \circ (n_2, f_2) = (n_1 + n_2, 2^{n_2} f_1 + f_2).$$

Demostrar que  $X$  es un grupo respecto a la operación  $\circ$ . ¿Cuáles de los siguientes son subgrupos de  $X$ ?

- (i) El subconjunto de los elementos de la forma  $(n, 0)$ ;
- (ii) El subconjunto de los elementos de la forma  $(0, f)$ .

15 Sea  $M$  el grupo obtenido mediante la construcción del ejercicio 3 al sustituir el conjunto  $\mathbf{R}$  por  $\mathbf{Z}_5$ , los enteros módulo 5. Demostrar que

- (i)  $|M| = 20$ ;
- (ii)  $M$  contiene subgrupos de cada uno de los órdenes permitidos por el teorema de Lagrange.

Dar un esquema del retículo de subgrupos de este grupo (puede ser útil considerar los elementos de  $M$  como permutaciones de  $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ ).

16 Escribir la partición de  $A_4$  (ejemplo del apartado 13.8) formada por las clases laterales por la izquierda del subgrupo cíclico generado por  $(123)$  y comprobar que la partición formada por las clases por la derecha del mismo subgrupo es una partición distinta.

17 Demostrar que  $S_5$  no tiene ningún subgrupo de orden 15.

18 Sea  $p$  un número primo. Se define el grupo  $GL_2(\mathbf{Z}_p)$  como el grupo de las matrices  $2 \times 2$  a coeficientes en  $\mathbf{Z}_p$  que tienen inversa respecto del producto. Demostrar que

- (i)  $GL_2(\mathbf{Z}_2)$  es isomorfo al grupo simétrico  $S_3$ .
- (ii) El orden de  $GL_2(\mathbf{Z}_p)$  es  $p(p^2 - 1)$ .
- (iii) El centro de  $GL_2(\mathbf{Z}_p)$  consiste en las matrices  $\alpha I$ , donde  $I$  es la matriz identidad y  $\alpha \neq 0$  en  $\mathbf{Z}_p$ .

19 Sea  $F$  el conjunto de las funciones  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  y sea  $V$  el conjunto de los pares ordenados  $(n, f)$  con  $n$  de  $\mathbf{Z}$  y  $f$  de  $F$ . Definimos una operación binaria  $*$  en  $V$  mediante la regla

$$(n_1, f_1) * (n_2, f_2) = (n_1 + n_2, f_3),$$

donde  $f_3(m) = f_1(m - n_1) + f_2(m)$ . Demostrar que  $V$  es un grupo respecto de la operación  $*$ .

20 Sean  $V$  y  $F$  como en el ejercicio anterior y sea  $E$  el subconjunto de  $F$  formado por las funciones  $f$  tales que  $f(n) = n$  salvo para un número finito de enteros  $n$ .

Demostrar que el subconjunto de los elementos de la forma  $(0, f)$  con  $f$  de  $E$  es un subgrupo de  $V$ .

21 Demostrar que existen cinco grupos distintos (es decir, mutuamente no isomorfos) de orden ocho.

22 Sea  $x$  un elemento de orden  $m$  de un grupo finito  $G$ . Demostrar que el orden de  $x^t$  en  $G$  es  $m/d$ , donde  $d = \text{mcd}(m, t)$ .

23 Sea  $G$  un grupo finito y  $H$  un subgrupo de índice  $k$  en  $G$ . Demostrar que existe un conjunto  $\{g_1, g_2, \dots, g_k\}$  de elementos de  $G$  que es, al mismo tiempo, un sistema de representantes de las clases laterales por la izquierda y por la derecha de  $H$  en  $G$ . En otras palabras,

$$G = g_1 H \cup \dots \cup g_k H = H g_1 \cup \dots \cup H g_k.$$

[Indicación: ejercicio 10.7.15.]

## 14 Grupos de permutaciones

### 14.1 Definiciones y ejemplos

Al empezar nuestro estudio de las permutaciones, señalamos que la regla de composición del grupo simétrico  $S_n$  posee cuatro propiedades fundamentales. En el capítulo anterior, estas propiedades sirvieron para definir los axiomas de un grupo. Volvemos ahora al estudio de las permutaciones, utilizando para ello la terminología de la teoría de grupos como guía en nuestras investigaciones.

Sea  $G$  un conjunto de permutaciones de un grupo finito. Si  $G$  es un grupo (respecto de la regla para combinar permutaciones) diremos que  $G$  es un **grupo de permutaciones de  $X$** . A menudo se dice que  $G$  actúa sobre  $X$ , pero hay que indicar que este último término cubre también una situación más general (apartado 14.5).

Si tomamos  $X = \{1, 2, \dots, n\}$ , entonces un grupo de permutaciones de  $X$  no es más que un subgrupo de  $S_n$ . Por ejemplo, aquí tenemos una lista de todos los subgrupos de  $S_3$ , cada uno de los cuales es también un grupo de permutaciones de  $\{1, 2, 3\}$ :

$$\begin{aligned} H_1 &= \{\text{id}\}, & H_2 &= \{\text{id}, (12)\}, & H_3 &= \{\text{id}, (13)\}, \\ H_4 &= \{\text{id}, (23)\}, & H_5 &= \{\text{id}, (123), (132)\}, & H_6 &= S_3. \end{aligned}$$

Para comprobar si un subconjunto dado de  $S_n$  es un subgrupo, es conveniente utilizar el teorema 13.7, el cual nos dice que (dado que  $S_n$  es finito) sólo es necesario comprobar la propiedad de clausura.

#### Ejercicios 14.1

- Cuáles de los siguientes son grupos de permutaciones del conjunto  $\{1, 2, 3, 4, 5\}$ , es decir, cuáles son subgrupos de  $S_5$ .

- (i)  $\{(12345), (124)(35)\}$ .
- (ii)  $\{\text{id}, (12345), (13524), (14253), (15432)\}$ .
- (iii)  $\{\text{id}, (12)(34), (13)(24), (14)(23)\}$ .
- (iv)  $\{\text{id}, (12)(345), (135)(24), (15324), (12)(45), (134)(25), (143)(25)\}$ .

Un subgrupo importante de  $S_n$  es el compuesto por todas las permutaciones pares, al que se conoce como **grupo alternado  $A_n$** . Los resultados del apartado 5.6 nos dicen que la composición de dos permutaciones pares es par (así que  $A_n$  es efectivamente un subgrupo de  $S_n$ ) y que el orden de  $A_n$  es  $\frac{1}{2}n!$ .

Muchos ejemplos de grupos de permutaciones ocurren como grupos de simetría de objetos geométricos. Por ejemplo, si marcamos las esquinas de un cuadrado en el sentido horario con 1, 2, 3, 4, entonces cada simetría del cuadrado induce una permutación del conjunto  $\{1, 2, 3, 4\}$ , y resultan las 8 permutaciones de la tabla 14.1.1.

Tabla 14.1.1

Identidad	$\text{id}$
Rotación de $90^\circ$ en sentido horario	$(1234)$
Rotación de $180^\circ$ en sentido horario	$(13)(24)$
Rotación de $270^\circ$ en sentido horario	$(1432)$
Reflexión sobre la diagonal 13	$(24)$
Reflexión sobre la diagonal 24	$(13)$
Reflexión sobre el bisector perpendicular a 12	$(12)(34)$
Reflexión sobre el bisector perpendicular a 14	$(14)(23)$

De la interpretación geométrica se desprende que estas ocho permutaciones forman un grupo; en concreto, se trata de un subgrupo de  $S_4$ .

Algo parecido ocurre al estudiar grafos en lugar de objetos geométricos. En este caso las “simetrías” son las permutaciones de los vértices que transforman aristas en aristas. Una permutación de este tipo se dice que es un **automorfismo** del grafo. La permutación  $(15)(24)$  es un automorfismo del grafo que se muestra en la figura 14.1, mientras que  $(12345)$  no lo es, ya que la arista  $\{2, 4\}$  se transforma en  $\{3, 5\}$ , que no es una arista. Es claro que el conjunto de automorfismos de un grafo forma un grupo, llamado el

grupo de automorfismos del grafo.

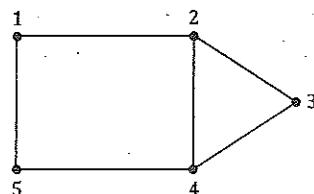


Fig. 14.1 Un grafo con dos automorfismos.

Lo más importante sobre los automorfismos es que si  $v$  y  $w$  son vértices de un grafo  $\Gamma$  y existe un automorfismo  $\alpha$  tal que  $\alpha(v) = w$ , entonces  $v$  y  $w$  tienen las mismas propiedades respecto de  $\Gamma$ . Por ejemplo, cualquier arista que contenga a  $v$  se transforma por  $\alpha$  en una arista que contiene a  $w$ , de forma que el grado de  $w$  es la misma que la de  $v$  (véase fig. 14.2).

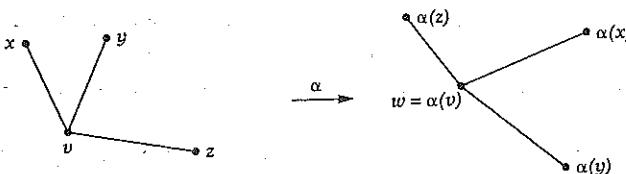


Fig. 14.2 Los automorfismos conservan el grado.

Igualmente, cada ciclo que pasa por  $v$  se transforma en un ciclo de la misma longitud a través de  $w$ . En algunos casos sencillos, esto puede utilizarse para determinar completamente el grupo de automorfismos de  $G$ .

**Ejemplo.** Encontrar el grupo de automorfismos del grafo de la figura 14.3.

**SOLUCIÓN:** Nótese en primer lugar que los vértices se distribuyen de forma natural en dos conjuntos: el conjunto  $\{1, 3, 5\}$  de grado cuatro y el conjunto  $\{2, 4, 6\}$  de grado dos. Por las razones que hemos expuesto antes, ningún automorfismo puede transformar un elemento del primer conjunto en un elemento del segundo. Por otra parte, es fácil ver que podemos tomar *cualquier* permutación de  $\{1, 3, 5\}$  y extenderla a un automorfismo del grafo. Por ejemplo, si la permutación  $(135)$  es parte de un automorfismo  $\alpha$ , entonces  $\alpha$  debe transformar  $4$  en  $2$ , ya que  $2$  es el único vértice adyacente

a  $1$  y a  $3$ , y  $4$  es el único vértice adyacente a  $3$  y a  $5$ . Igualmente,  $\alpha$  debe transformar  $4$  en  $6$  y  $6$  en  $2$ , de forma que ha de ser  $\alpha = (135)(246)$ . Del mismo modo, cada una de las seis permutaciones de  $\{1, 3, 5\}$  se extiende de forma única a un automorfismo del grafo:

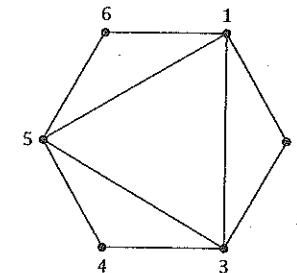


Fig. 14.3 ¿Cuántos automorfismos?

id	se extiende a id,	(13) se extiende a (13)(46),
(135)	se extiende a (135)(246),	(15) se extiende a (15)(24),
(153)	se extiende a (153)(264),	(35) se extiende a (35)(26).

Resulta que el grafo tiene exactamente seis automorfismos, y que éstos son las seis permutaciones extendidas que se muestran más arriba.  $\square$

### Ejercicios 14.1 (continuación)

1 Hallar el orden de las siguientes permutaciones, consideradas como elementos del grupo simétrico  $S_8$ :

$$(i) (1235)(48)(67); \quad (ii) (12)(35)(48)(67); \quad (iii) (13672)(458).$$

2 Segundo el teorema 13.8.3, el orden de un elemento de  $S_8$  es un divisor de  $|S_8| = 8!$ . Teniendo en cuenta la estructura en ciclos de las permutaciones de  $S_8$ , escribir los órdenes de los elementos de  $S_8$  y dar un ejemplo de un divisor de  $8!$  que no sea el orden de un elemento de  $S_8$ .

3 Dar una lista con todas las simetrías de un pentágono regular, consideradas como permutaciones de los vértices  $1, 2, 3, 4$  y  $5$  en orden cíclico.

4 Hallar el grupo de automorfismos del grafo dado por la siguiente matriz de adyacencia (un dibujo puede ser útil).

1	2	3	4	5	6	7	8
2	1	1	1	2	3	4	4
3	3	2	7	7	7	5	5
4	5	6	8	8	8	6	6

## 14.2 Órbitas y estabilizadores

Sea  $G$  un grupo de permutaciones de un conjunto  $X$ . Demostraremos que la estructura de grupo de  $G$  proporciona una partición de  $X$  de forma natural.

Definimos la relación  $\sim$  en  $X$  mediante la regla

$$x \sim y \iff g(x) = y \text{ para algún } g \in G.$$

Comprobaremos que  $\sim$  es una relación de equivalencia.

(Reflexividad) Como  $\text{id}$  pertenece a cualquier grupo e  $\text{id}(x) = x$  para todo  $x$  de  $X$ , tenemos que  $x \sim x$ .

(Simetría) Supongamos que  $x \sim y$ , de forma que  $g(x) = y$  para algún  $g$  de  $G$ . Como  $G$  es un grupo,  $g^{-1}$  pertenece a  $G$ , y como  $g^{-1}(y) = x$ , tenemos que  $y \sim x$ .

(Transitividad) Si  $x \sim y$  e  $y \sim z$ , tenemos que  $y = g(x)$  y  $z = h(y)$  para ciertos  $g$  y  $h$  de  $G$ . Al ser  $G$  un grupo,  $gh$  es de  $G$ , y  $h(g(x)) = z$  implica que  $x \sim z$ .

Las clases de equivalencia forman una partición de  $X$ , en la que  $x$  e  $y$  están en la misma parte si, y sólo si, existe una permutación de  $G$  que transforma  $x$  en  $y$ . Estas partes (clases de equivalencia) son las órbitas de  $G$  en  $X$ . La órbita de  $x$  contiene todos los elementos de  $X$  que son de la forma  $g(x)$  para algún  $g$  de  $G$  y se acostumbra a denotar por  $Gx$ . En concreto,

$$Gx = \{y \in X \mid y = g(x) \text{ para algún } g \text{ de } G\}.$$

Intuitivamente, la órbita  $Gx$  contiene todos los objetos que son indistinguibles de  $x$  bajo la acción de  $G$ . Por ejemplo, si  $G$  es el grupo de automorfismos del grafo de la figura 14.3, el conjunto de vértices queda dividido en dos órbitas  $\{1, 3, 5\}$  y  $\{2, 4, 6\}$ ; tenemos que

$$G1 = G3 = G5 = \{1, 3, 5\}, \quad G2 = G4 = G6 = \{2, 4, 6\}.$$

### Ejercicios 14.2

- Hallar todos los automorfismos del grafo que muestra la figura 14.1 (sólo hay 2). Demostrar que el grupo de automorfismos induce una partición del conjunto de vértices en tres órbitas.
- Sea  $G$  el grupo de automorfismos del árbol de la figura 14.4a. Determinar las órbitas de la acción de  $G$  sobre el conjunto de vértices  $X$ .

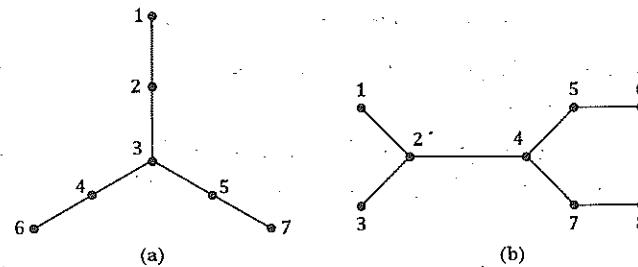


Fig. 14.4 Hallar las órbitas.

- Repetir el ejercicio 2 para el árbol de la figura 14.4b.

Se plantean dos problemas evidentes respecto de las órbitas: cómo hallar el tamaño de cada órbita y cómo hallar el número de órbitas. La solución a estos problemas introduce una combinación de ideas de teoría de grupos por una parte, y por otra algunas técnicas enumerativas elementales.

Si  $G$  es un grupo de permutaciones de un conjunto  $X$ , denotaremos por  $G(x \rightarrow y)$  el conjunto de los elementos de  $G$  que transforman  $x$  en  $y$ ; es decir,

$$G(x \rightarrow y) = \{g \in G \mid g(x) = y\}.$$

En particular, si  $x = y$ ,  $G(x \rightarrow x)$  consta de las permutaciones  $\gamma$  de  $G$  que dejan fijo  $x$ ; es decir, las permutaciones tales que  $\gamma(x) = x$ . El conjunto  $G(x \rightarrow x)$  se conoce como el **estabilizador** de  $x$  y se denota por  $G_x$ . Notemos que si  $\gamma_1$  y  $\gamma_2$  son de  $G_x$ , entonces

$$\gamma_1\gamma_2(x) = \gamma_1(x) = x,$$

con lo que  $\gamma_1\gamma_2$  también pertenece a  $G_x$ . Vemos que  $G_x$  es de hecho un **subgrupo** de  $G$ .

**Teorema 14.2.** Sea  $G$  un grupo de permutaciones de  $X$  y supongamos que  $h$  pertenece a  $G(x \rightarrow y)$ . Entonces

$$G(x \rightarrow y) = hG_x,$$

la clase lateral por la izquierda de  $G_x$  con respecto a  $h$ .

**DEMOSTRACIÓN:** Si  $\alpha$  es de la clase lateral  $hG_x$ , entonces  $\alpha = h\beta$  para algún  $\beta$  de  $G_x$ . Así pues,

$$\alpha(x) = h\beta(x) = h(x) = y,$$

de manera que  $\alpha$  pertenece a  $G(x \rightarrow y)$ . Recíprocamente, si  $\gamma$  es de  $G(x \rightarrow y)$ , entonces

$$h^{-1}\gamma(x) = h^{-1}(y) = x$$

y  $h^{-1}\gamma$  es del estabilizador  $G_x$ . Esto demuestra que  $\gamma$  pertenece a  $hG_x$  y que los dos conjuntos son el mismo.  $\square$

El teorema 14.2 nos permite hallar el tamaño del conjunto  $G(x \rightarrow y)$ . Recordemos que una clase lateral de un subgrupo tiene el mismo tamaño que el propio subgrupo, así que  $|hG_x| = |G_x|$ . Si tenemos un elemento  $h$  de  $G$  que transforma  $x$  en  $y$  (en otras palabras, si  $y$  está en la órbita  $Gx$ ) tenemos la ecuación

$$|G(x \rightarrow y)| = |G_x| \quad (y \in Gx).$$

Esto se cumple para cualquier  $y$  de  $Gx$ . Por otra parte, si  $y$  no está en la órbita  $Gx$  entonces, por definición, no hay ninguna permutación que transforme  $x$  en  $y$ , de forma que

$$G(x \rightarrow y) = 0 \quad (y \notin Gx).$$

### Ejercicios 14.2 (continuación)

4 Comprobar que en el ejemplo del apartado 14.1

$$(i) |G(2 \rightarrow 6)| = |G_2|, \quad (ii) |G(3 \rightarrow 1)| = |G_3|.$$

5 Sea  $G$  un grupo de permutaciones de un conjunto  $X$  y sea  $k$  un elemento de  $G(x \rightarrow y)$ . Demostrar que  $G(x \rightarrow y)$  es igual a la clase por la derecha  $G_y k$  y deducir que si  $u$  y  $v$  son dos elementos de la misma órbita de  $G$ , entonces  $|G_u| = |G_v|$ .

6 Sea  $X = \mathbb{Z}_5$  y  $G$  el grupo cíclico de permutaciones de  $X$  generado por la permutación  $\pi$  definida mediante  $\pi(x) = 2x$ . Dar una lista de los elementos de  $G$  en la notación de ciclos y determinar las órbitas de  $G$  en  $X$ .

### 14.3 El tamaño de una órbita

En este apartado estableceremos una relación fundamental entre el tamaño de una órbita  $Gx$  y el del estabilizador  $G_x$ . Necesitaremos los resultados del apartado anterior, además de las técnicas enumerativas para contar conjuntos de pares desarrolladas en el apartado 3.2.

Sea  $G$  un grupo de permutaciones de un conjunto  $X$  y sea  $x$  un elemento cualquiera de  $X$ . El conjunto  $S$  de pares  $(g, y)$  tales que  $g(x) = y$  puede describirse mediante una tabla como en el apartado 3.2.

$\cdots y \cdots$	
$\vdots$	
$g$	$\checkmark$ significa que $(g, y)$ está en $S$
$\vdots$	
	$r_g(S)$
	$c_y(S)$

Los dos métodos para contar  $S$ , el de los totales por filas  $r_g(S)$  y el de los totales por columnas  $c_y(S)$  forman la base de la demostración de nuestro teorema principal.

**Teorema 14.3.** Sea  $G$  un grupo de permutaciones de un conjunto  $X$  y sea  $x$  un elemento de  $X$ . Se tiene la ecuación

$$|Gx| \times |G_x| = |G|.$$

**DEMOSTRACIÓN:** Sea  $S$  el conjunto de los pares que ilustra la tabla anterior, es decir,

$$S = \{(g, y) \mid g(x) = y\}.$$

Al ser  $g$  una permutación, existe exactamente un  $y$  tal que  $g(x) = y$  para cada  $g$ . En otras palabras, cada total por filas  $r_g(S)$  es igual a 1.

El total por columnas  $c_y(S)$  es igual al número de  $g$  tales que  $g(x) = y$ , es decir,  $|G(x \rightarrow y)|$ . Si  $y$  es de la órbita de  $x$  tenemos que

$$c_y(S) = |G(x \rightarrow y)| = |G_x|.$$

Por otra parte, si  $y$  no es de  $Gx$ , entonces  $c_y(S) = 0$ .

Los dos métodos para contar  $S$  nos dan la ecuación

$$\sum_{y \in X} c_y(S) = \sum_{g \in G} r_g(S).$$

En el término izquierdo hay  $|Gx|$  sumandos iguales a  $|G_x|$  y el resto cero, mientras que en el derecho hay  $|G|$  sumandos iguales a 1. De aquí se desprende el resultado.  $\square$

Por ejemplo, es fácil comprobar el resultado si  $G$  es el grupo de las simetrías de un cuadrado, consideradas como permutaciones de los cuatro vértices (como en el apartado 14.1). Para determinar la órbita del vértice 1 (pongamos por caso) observemos que  $G$  contiene permutaciones que transforman

$$1 \text{ en } 1: \text{id} \quad 1 \text{ en } 2: (1234)$$

$$1 \text{ en } 3: (13)(24), \quad 1 \text{ en } 4: (1432).$$

Por lo tanto, la órbita  $G1$  es todo el conjunto y  $|G1| = 4$ . El estabilizador de 1 es

$$G_1 = \{\text{id}, (24)\},$$

y esto nos da

$$|G1| \times |G_1| = 4 \times 2 = 8$$

como era de esperar, ya que hay ocho simetrías en total.

También podemos usar este resultado para calcular el orden de un grupo de permutaciones, siempre que podamos calcular el tamaño de una órbita y del correspondiente estabilizador.

**Ejemplo.** Sea  $T$  un tetraedro regular en el espacio tridimensional (figura 14.5). Hallar el orden del grupo de simetrías rotacionales de  $T$ .

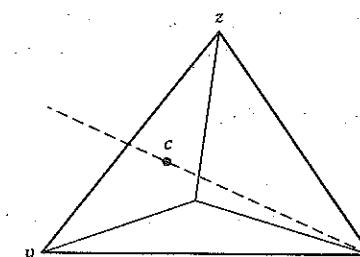


Fig. 14.5 Un tetraedro regular.

**SOLUCIÓN:** Sea  $G$  el grupo de permutaciones de los vértices que corresponde al grupo de las simetrías rotacionales y sea  $z$  un vértice cualquiera de  $T$ . Dado cualquier otro vértice  $y$  existe una arista  $yz$  de  $T$  y dos caras de  $T$  limitadas por  $yz$ . Sea  $c$  el baricentro de una de ellas y  $v$  el vértice opuesto (figura 14.5). Una rotación de  $120^\circ$  sobre el eje  $cv$  (en el sentido apropiado) envía  $z$  a  $y$ . La órbita  $Gz$  contiene, pues, los cuatro vértices y tenemos que  $|Gz| = 4$ .

Las únicas simetrías que dejan fijo  $z$  son las rotaciones de  $0^\circ$ ,  $120^\circ$  y  $240^\circ$  alrededor del eje que pasa por  $z$ , de manera que el estabilizador  $G_z$  tiene orden 3. Por lo tanto,

$$|G| = |Gz| \times |G_z| = 4 \times 3 = 12. \quad \square$$

**Ejercicios 14.3**

- 1 Se numeran los vértices de un tetraedro  $T$  como 1, 2, 3, 4. Escribir las permutaciones que corresponden a las doce simetrías de  $T$  y comprobar que el grupo que se obtiene es el grupo alternado  $A_4$ .
- 2 Sea  $X$  el conjunto de vértices de un cubo y  $G$  el grupo de permutaciones de  $X$  correspondiente a las rotaciones del cubo. Demostrar que

- (i)  $G$  tiene una sola órbita en  $X$ ;
- (ii) si  $z$  es un vértice cualquiera, entonces  $|G_z| = 3$ ;
- (iii)  $|G| = 24$ .

- 3 Sea  $V$  el conjunto de vértices del grafo  $\Gamma$  de la figura 14.6 y sea  $G$  el grupo de automorfismos de  $\Gamma$ . Hallar las órbitas de  $G$  en  $V$  y calcular los órdenes de  $G_a$ ,  $G_b$  y  $G$ .

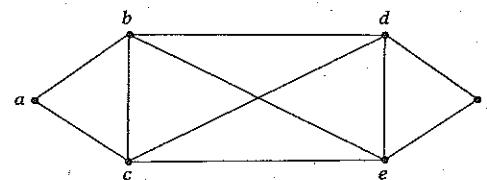


Fig. 14.6 Ilustración del ejercicio 14.3.3.

**14.4 El número de órbitas**

Pasamos ahora al problema de contar el número de órbitas de un grupo de permutaciones  $G$  en un conjunto  $X$ . Cada órbita es un subconjunto de  $X$  cuyos elementos son indistinguibles bajo la acción de  $G$ , de manera que el número de órbitas nos indica el número de clases de objetos indistinguibles de  $X$ .

Supongamos, por ejemplo, que hay que fabricar tarjetas de identificación sobre cuadrados de plástico marcados con una cuadrícula  $3 \times 3$  en ambas caras y perforadas en dos de los cuadrados (figura 14.7).

Como hay 9 posiciones y dos agujeros, las tarjetas se pueden perforar de  $\binom{9}{2} = 36$  maneras. Nos referiremos a ellas como a las *configuraciones*.

Ahora bien, no todas las configuraciones son indistinguibles, ya que las tarjetas pueden girarse y se les puede dar la vuelta. Las dos primeras configuraciones que muestra la figura 14.7 son indistinguibles, pero la tercera es esencialmente distinta de las otras dos.

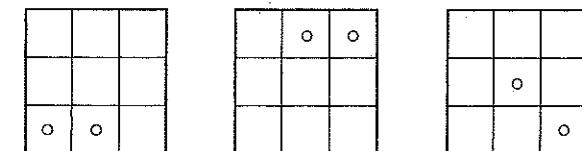


Fig. 14.7 Tarjetas de identificación.

Es evidente que el grupo que actúa en esta situación es el grupo de las ocho simetrías de un cuadrado, aunque debemos considerar su acción en el conjunto  $X$  de las 36 configuraciones, en lugar de los cuatro vértices de un cuadrado. El número de órbitas de  $G$  en  $X$  es precisamente el número de tarjetas indistinguibles distintas.

Podríamos hallar el número de órbitas numerando los 36 elementos de  $X$  de alguna forma y escribiendo explícitamente las ocho permutaciones de las 36 configuraciones. Esto sería bastante laborioso y, afortunadamente, hay una manera mejor de proceder. Dado un grupo  $G$  de permutaciones de un conjunto  $X$ , para cada  $g$  de  $G$  definimos el conjunto

$$F(g) = \{x \in X \mid g(x) = x\}.$$

Así pues,  $F(g)$  es el conjunto de objetos que quedan *fijos* por  $g$ . El siguiente teorema nos dice que el número de órbitas es igual al tamaño medio de los conjuntos  $F(g)$ .

**Teorema 14.4.** *El número de órbitas de  $G$  en  $X$  es*

$$\frac{1}{|G|} \sum_{g \in G} |F(g)|.$$

**DEMOSTRACIÓN:** Una vez más, utilizaremos el método de contar pares. Sea

$$E = \{(g, x) \mid g(x) = x\}.$$

El total por filas  $r_g(E)$  es igual al número de  $x$  que quedan fijos por  $g$ , es decir,  $|F(g)|$ . Por otra parte, el total por columnas  $c_x(E)$  es igual al número de  $g$  que dejan fijo  $x$ , es decir,  $|G_x|$ . Los dos métodos de contar dan lugar a la igualdad

$$\sum_{g \in G} |F(g)| = \sum_{x \in X} |G_x|.$$

Supongamos que hay  $t$  órbitas y sea  $z$  un cierto elemento de  $X$ . El ejercicio 14.2.5 nos dice que si  $x$  pertenece a la órbita  $Gz$ , entonces  $|G_x| = |G_z|$ . Vemos que en el término derecho de la ecuación anterior hay  $|G_z|$  términos iguales a  $|G_z|$ , uno para cada  $x$  de  $Gz$ . La contribución total de estos términos es, según el teorema 14.3,

$$|Gz| \times |G_z| = |G|.$$

En otras palabras, la contribución de los elementos de una órbita cualquiera es  $|G|$ . Como hay  $t$  órbitas en total, el término derecho es igual a  $t|G|$ , lo cual nos lleva a

$$t = \frac{1}{|G|} \sum_{g \in G} |F(g)|. \quad \square$$

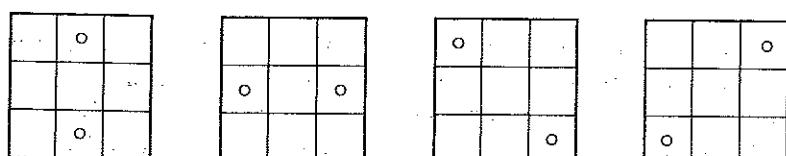


Fig. 14.8 Configuraciones invariantes por una rotación de  $180^\circ$ .

Podemos ahora resolver el problema de las tarjetas de identificación. No tenemos más que calcular  $|F(g)|$  para cada una de las ocho simetrías  $g$ . Por ejemplo, si  $g$  es una rotación de  $180^\circ$ , hay cuatro configuraciones fijas, tal como muestra la figura 14.8. De la misma manera, podemos comprobar

que el número de configuraciones fijadas por cada una de las ocho simetrías es el que indica la tabla 14.4.1. Finalmente, el número de órbitas es

$$\frac{1}{8}(36 + 0 + 4 + 0 + 6 + 6 + 6 + 6) = 8.$$

Podemos concluir que de esta forma pueden producirse exactamente ocho tarjetas distintas.

Tabla 14.4.1

Identidad	36
Rotación de $90^\circ$ en sentido horario	0
Rotación de $180^\circ$ en sentido horario	4
Rotación de $270^\circ$ en sentido horario	0
Reflexión sobre la diagonal 13	6
Reflexión sobre la diagonal 24	6
Reflexión sobre el bisector perpendicular a 12	6
Reflexión sobre el bisector perpendicular a 14	6

Desde luego, en este caso particular no sería difícil obtener las ocho configuraciones distintas por tanteo, pero el resultado del teorema 14.4 tiene una aplicación mucho más amplia y es útil en la solución de muchos otros problemas en los que interviene la simetría.

**Ejemplo.** Se fabrican collares colocando 13 sartas blancas y 3 negras en un cordel. ¿Cuántos collares diferentes pueden fabricarse de esta manera? (podemos ignorar la posición del nudo.)

**SOLUCIÓN:** Podemos pensar en que las 16 sartas se colocan en los vértices de un polígono regular de 16 lados. Para especificar una configuración se eligen tres vértices que serán ocupados por las sartas negras, de forma que hay  $\binom{16}{3} = 560$  configuraciones en total. Dos configuraciones dan lugar al mismo collar si una puede obtenerse a partir de la otra mediante una simetría del polígono: una rotación o una reflexión (esta última supone darle la vuelta al polígono). Hay 32 simetrías en total:

- (a) El neutro deja fijas las 560 configuraciones.
- (b) Hay 15 rotaciones de ángulos  $2\pi n/16$  ( $n = 1, 2, \dots, 15$ ) y ninguna de ellas tiene configuraciones fijas (¿por qué?).

- (c) Hay ocho reflexiones sobre los ejes que unen los puntos medios de lados opuestos y ninguna de ellas posee configuraciones fijas.
- (d) Hay ocho reflexiones sobre los ejes que unen vértices de lados opuestos. Una de estas reflexiones deja fijas las posiciones de las tres sartas negras sólo si una de ellas ocupa uno de los vértices del eje y las otras dos uno de los siete pares de vértices simétricos respecto del eje. Hay, pues,  $2 \times 7 = 14$  configuraciones fijas para cada una de ellas.

El número de collares distintos resulta ser

$$\frac{1}{32}(560 + 8 \cdot 14) = 21.$$

□

#### Ejercicios 14.4

- 1 Demostrar que con cinco sartas blancas y tres negras pueden construirse exactamente cinco collares distintos. Hacer un esquema de ellos.
- 2 Se fabrican tarjetas de identificación cuadradas con dos agujeros sobre una cuadrícula  $4 \times 4$ . ¿Cuántas tarjetas distintas pueden fabricarse?
- 3 Sea  $V$  el conjunto de vértices del árbol binario que muestra la figura 14.9 y sea  $G$  el grupo de automorfismos del árbol. Escribir los elementos de  $G$  (como permutaciones de  $V$ ) y comprobar que se cumple el teorema 14.4 en este caso.
- 4 Sea  $X$  el conjunto de “árboles coloreados” que resulta de asignar a cada vértice del árbol de la figura 14.9 uno de los colores rojo o azul. ¿Cuántos árboles coloreados distintos se obtienen?

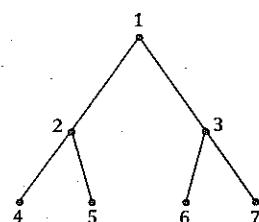


Fig. 14.9 Ilustración de los ejercicios 14.4.3 y 14.4.4.

- 5 Sea  $G$  un grupo de permutaciones de  $X$  y sea  $I(x)$  una expresión constante sobre cada órbita de  $G$ , es decir,

$$I(g(x)) = I(x) \quad \text{para todos } g \in G, x \in X.$$

Sea  $D$  un conjunto de representantes de las órbitas y sea  $E = \{(g, x) \mid g(x) = x\}$  como en la demostración del teorema 14.4. Evaluando la suma

$$\sum_{(g,x) \in E} I(x)$$

de dos maneras distintas, demostrar que

$$\sum_{x \in D} I(x) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in F(g)} I(x).$$

(Esta es una versión “ponderada” del teorema 14.4, teorema que se obtiene tomando  $I(x) = 1$  para todo  $x \in X$ . Se utilizará en el capítulo 20.)

#### 14.5 Representación de grupos mediante permutaciones

Sea  $G$  un grupo, no necesariamente un grupo de permutaciones, y  $X$  un conjunto. Una representación de  $G$  mediante permutaciones de  $X$  asigna a cada elemento  $g$  de  $G$  una permutación  $\hat{g}$  de  $X$  de manera compatible con las operaciones. En otras palabras,

$$\widehat{g_1 g_2} = \hat{g}_1 \hat{g}_2 \quad \text{para todo } g_1 \text{ y } g_2 \text{ de } G.$$

La condición de compatibilidad significa que el conjunto de todas las permutaciones  $\hat{g}$  es un grupo  $\hat{G}$  de permutaciones de  $X$ . Sin embargo, es importante señalar que  $G$  y  $\hat{G}$  no son necesariamente grupos isomorfos, ya que no hemos impuesto que elementos distintos sean representados por permutaciones distintas. Si, en efecto, se cumple la propiedad de que

$$\hat{g}_1 = \hat{g}_2 \iff g_1 = g_2 \quad (g_1, g_2 \in G),$$

entonces decimos que la representación es **fiel**; en otro caso, decimos que **no es fiel**. En el caso fiel, la función que envía  $g$  a  $\hat{g}$  es una biyección y la condición de compatibilidad implica que es un isomorfismo de  $G$  en  $\hat{G}$ .

**Ejemplo.** Sea  $G$  el grupo de simetrías del cuadrado. Demostrar que la representación en la que cada simetría está representada por la permutación correspondiente de los vértices del cuadrado es fiel, mientras que aquella en la que cada simetría está representada por la permutación correspondiente de las diagonales (consideradas como rectas sin dirección) no lo es.

**SOLUCIÓN:** Numeramos los vértices 1, 2, 3 y 4 en orden cíclico y denotamos los elementos de  $G$  por  $\hat{1}$  (la simetría trivial),  $\hat{\rho}_1, \hat{\rho}_2, \hat{\rho}_3$  (rotaciones de  $90^\circ, 180^\circ, 270^\circ$ ),  $\hat{\mu}_1, \hat{\mu}_2$  (reflexiones sobre las diagonales) y  $\hat{\mu}_3, \hat{\mu}_4$  (reflexiones sobre las bisectrices perpendiculares de los lados). Las permutaciones de los vértices correspondientes a las simetrías son, como en el apartado 14.1:

$$\begin{aligned}\hat{1} &= \text{id}, & \hat{\rho}_1 &= (1234), & \hat{\rho}_2 &= (13)(24), & \hat{\rho}_3 &= (1432), \\ \hat{\mu}_1 &= (24), & \hat{\mu}_2 &= (13), & \hat{\mu}_3 &= (12)(34), & \hat{\mu}_4 &= (14)(23).\end{aligned}$$

Como las permutaciones son todas distintas, tenemos una representación fiel (de hecho, en algunos de los ejemplos anteriores, se trataba de una suposición tácita).

Sean  $a$  y  $b$  las diagonales 13 y 24 respectivamente. Las permutaciones de  $\{a, b\}$  que corresponden a las simetrías son:

$$\begin{aligned}\hat{1} &= \text{id}, & \hat{\rho}_1 &= (ab), & \hat{\rho}_2 &= \text{id}, & \hat{\rho}_3 &= (ab), \\ \hat{\mu}_1 &= \text{id}, & \hat{\mu}_2 &= \text{id}, & \hat{\mu}_3 &= (ab), & \hat{\mu}_4 &= (ab),\end{aligned}$$

con lo que en este caso la representación no es fiel.  $\square$

Siempre que tengamos una representación de  $G$  mediante permutaciones de  $X$  diremos que  $G$  actúa sobre  $X$ . Esta terminología ya ha sido utilizada para representaciones fieles, pero también se aplica si la representación no es fiel.

La técnica de representar un grupo mediante permutaciones es útil porque es más fácil calcular con permutaciones que con elementos de un grupo abstracto. Naturalmente, la técnica adquiere el máximo interés cuando la representación es fiel. El siguiente teorema muestra que todo grupo finito admite una representación fiel.

**Teorema 14.5.** Sea  $G$  un grupo finito y  $X$  el conjunto de los elementos de  $G$  (es decir,  $X$  es lo mismo que  $G$ , pero sin tener en cuenta la estructura de grupo). Definimos para  $g$  de  $G$  una permutación  $\hat{g}$  de  $X$  como

$$\hat{g}(h) = gh \quad (h \in X),$$

donde el símbolo  $gh$  no es más que el producto de  $g$  y  $h$  en  $G$ . Esta construcción define una representación fiel de  $G$  por permutaciones de  $X$ .

**DEMOSTRACIÓN:** Dados  $g_1$  y  $g_2$  de  $G$  y  $h$  de  $X$ , tenemos que

$$\widehat{g_1 g_2}(h) = (g_1 g_2)h = g_1(g_2 h) = \hat{g}_1(\hat{g}_2(h)),$$

de donde  $\widehat{g_1 g_2} = \hat{g}_1 \hat{g}_2$  y se trata, en efecto, de una representación. Además,

$$\begin{aligned}\hat{g}_1 = \hat{g}_2 &\iff g_1(h) = g_2(h) \quad (h \in X) \\ &\iff g_1 h = g_2 h \\ &\iff g_1 = g_2.\end{aligned}$$

Así pues, la representación es fiel.  $\square$

Resulta del teorema que todo grupo finito es isomorfo a un grupo de permutaciones, aunque en general el número de objetos permutados, al ser igual al orden del grupo, es excesivamente grande. En la práctica intentaremos hallar representaciones fieles sobre un conjunto relativamente pequeño, con la intención de que los cálculos sean factibles. En el ejercicio 14.5.4 damos un ejemplo.

### Ejercicios 14.5

1. Sea  $G = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}$  el grupo que tiene por tabla la 14.5.1. Escribir las permutaciones  $\hat{g}_i$  ( $1 \leq i \leq 8$ ) como en el teorema 14.5 y determinar así el orden de cada elemento de  $G$  (para escribir las permutaciones, es conveniente usar el índice  $i$  en lugar de  $g_i$ : por ejemplo,  $\hat{g}_2 = (1234)(5678)$ ).

Tabla 14.5.1

	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$	$g_7$	$g_8$
$g_1$	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$	$g_7$	$g_8$
$g_2$	$g_2$	$g_3$	$g_4$	$g_1$	$g_6$	$g_7$	$g_8$	$g_5$
$g_3$	$g_3$	$g_4$	$g_1$	$g_2$	$g_7$	$g_8$	$g_5$	$g_6$
$g_4$	$g_4$	$g_1$	$g_2$	$g_3$	$g_8$	$g_5$	$g_6$	$g_7$
$g_5$	$g_5$	$g_8$	$g_7$	$g_6$	$g_3$	$g_2$	$g_1$	$g_4$
$g_6$	$g_6$	$g_5$	$g_8$	$g_7$	$g_4$	$g_3$	$g_2$	$g_1$
$g_7$	$g_7$	$g_6$	$g_5$	$g_8$	$g_1$	$g_4$	$g_3$	$g_2$
$g_8$	$g_8$	$g_7$	$g_6$	$g_5$	$g_2$	$g_1$	$g_4$	$g_3$

2 Sea  $G$  el grupo de simetrías de un hexágono regular. Decir, en cada uno de los casos siguientes, si la representación de  $G$  mediante permutaciones del conjunto  $X$  dado es fiel.

- (i)  $X =$  vértices;
- (ii)  $X =$  lados (considerados como pares no ordenados de vértices);
- (iii)  $X =$  diagonales;
- (iv)  $X =$  bisectrices perpendiculares de los lados.

3 Demostrar que si tenemos una representación no fiel de un grupo  $G$ , existe un elemento  $g \neq 1$  de  $G$  tal que  $\hat{g} = \text{id}$ .

4 Sea  $G$  el grupo de simetrías de un cubo (ejercicio 14.3.2) y sea  $D$  el conjunto de las cuatro diagonales espaciales del cubo (una diagonal espacial une vértices opuestos y pasa por el centro del cubo). Examinando los distintos tipos de simetrías, demostrar que la representación que asigna a cada rotación la correspondiente permutación de  $D$  es fiel. Deducir que  $G \approx S_4$ .

## 14.6 Aplicaciones a la teoría de grupos

En este apartado estudiaremos una representación *no fiel* de un grupo finito mediante permutaciones de sí mismo y obtendremos algunos resultados importantes de la teoría de grupos. Empezaremos por demostrar que la relación entre el tamaño de una órbita y el del estabilizador

que obtuvimos en el teorema 14.3 también se cumple si  $G$  posee una representación no fiel en  $X$ .

Dada una representación de  $G$  mediante permutaciones de  $X$  (fiel o no), podemos definir la órbita  $Gx$  como el conjunto

$$Gx = \{y \in X \mid y = \hat{g}(x) \text{ para algún } g \text{ de } G\}.$$

Es evidente que esto es lo mismo que  $\hat{G}x$ . Por otra parte, se define el estabilizador  $G_x$  como el subgrupo

$$G_x = \{g \in G \mid \hat{g}(x) = x\},$$

que no es lo mismo que  $C_x$ , ya que varios elementos  $g$  pueden inducir la misma permutación  $\hat{g}$ . Sin embargo, si repetimos la demostración del teorema 14.3 con el conjunto  $\{(g, y) \mid \hat{g}(x) = y\}$ , obtendremos la relación esperada entre  $|Gx|$ ,  $|G_x|$  y  $|G|$ , es decir,

$$|Gx| \times |G_x| = |G|.$$

Sea  $A$  un grupo finito y definamos para cada elemento  $a$  de  $A$  una permutación  $\hat{a}$  de  $A$  como

$$\hat{a}(x) = axa^{-1} \quad (x \in A).$$

El elemento  $axa^{-1}$  se conoce como el **conjugado** de  $x$  por  $a$ . Esta asignación satisface la condición de compatibilidad, ya que

$$\begin{aligned} \hat{a}_1 a_2(x) &= (a_1 a_2)x(a_1 a_2)^{-1} \\ &= a_1(a_2 x a_2^{-1})a_1^{-1} \\ &= \hat{a}_1 \hat{a}_2(x), \end{aligned}$$

y tenemos una representación de  $A$  mediante permutaciones de sí mismo. Sin embargo, la representación no es necesariamente fiel, debido a que si  $a$  commuta con  $x$  tenemos que

$$\hat{a}(x) = axa^{-1} = xaa^{-1} = x.$$

En el apartado 13.7 definimos el *centro*  $Z(A)$  como el conjunto formado por los elementos de  $A$  que comutan con cualquier otro elemento. Se

desprende de la ecuación anterior que si  $\alpha$  pertenece a  $Z(A)$ , entonces  $\hat{\alpha} = \text{id}$  y, por lo tanto, si el centro contiene elementos distintos del neutro la representación es infiel. En particular, si  $A$  es un grupo commutativo,  $Z(A) = A$  y la representación es la representación trivial en la que cada elemento de  $A$  se transforma en la identidad.

En el caso general, el estabilizador de  $x$  en esta representación es el subgrupo formado por los elementos  $a$  tales que  $\hat{a}(x) = x$ , es decir,  $axa^{-1} = x$  o, equivalentemente,  $ax = xa$ . En otras palabras, es el subgrupo  $C(x)$  formado por los elementos que comutan con  $x$  y que normalmente se conoce como el **centralizador** de  $x$ . La órbita de  $x$  es el conjunto de todos los conjugados de  $x$ ; la versión ampliada del teorema 14.3 nos da la ecuación

$$|C(x)| \times (\text{número de conjugados de } x) = |A|.$$

Esto implica en particular que el tamaño de una clase de conjugación es un divisor de  $|A|$ . Si  $A$  es el grupo simétrico  $S_n$ , recordemos que (teorema 5.5) la clase de conjugación de  $x$  consiste en las permutaciones que tienen el mismo tipo que  $x$ . Si  $x$  tiene  $\alpha_i$  ciclos de longitud  $i$ , el número total de permutaciones de este tipo es

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!}.$$

Como  $|S_n| = n!$  podemos deducir que el número de permutaciones de  $S_n$  que comutan con  $x$  es

$$|C(x)| = 1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!$$

En un grupo finito  $A$ , las órbitas de la representación definida por  $\hat{a}(x) = axa^{-1}$  corresponden a las clases de conjugación y forman una partición de  $A$ . De este hecho puede deducirse una fórmula útil en la que interviene el centro de  $A$ . Como cada elemento de  $Z(A)$ , incluido el neutro, es conjugado únicamente de sí mismo, hay  $|Z(A)|$  clases de conjugación de tamaño 1. Supongamos que las demás clases tienen tamaños  $n_1, n_2, \dots, n_c$  donde, como hemos indicado antes, cada  $n_i$  es un divisor de  $|A|$ . El número total de elementos de  $A$  será

$$|A| = |Z(A)| + n_1 + n_2 + \dots + n_c.$$

Esta ecuación se conoce como la **ecuación de clases** de  $A$ . El hecho de que cada término  $n_i$  sea un divisor de  $|A|$  tiene una consecuencia notable si el orden de  $A$  es un número primo.

**Teorema 14.6.** Si  $A$  es un grupo de orden  $p^r$ , donde  $p$  es un primo y  $r \geq 1$ , el centro  $Z(A)$  contiene algún elemento distinto del neutro.

**DEMOSTRACIÓN:** En la ecuación de clases de  $A$  tenemos que  $|A| = p^r$  y cada  $n_i$  es un divisor de  $p^r$ . Como  $n_i \neq 1$ , ha de ser  $n_i = p^{e_i}$  para algún  $e_i \geq 1$ . Tenemos que  $p$  es un divisor de  $|A|$  y de cada  $n_i$ , con lo que también lo es de  $|Z(A)|$ ; en consecuencia,  $|Z(A)| > 1$ .  $\square$

El teorema 14.6 nos muestra cómo argumentos enumerativos sencillos pueden tener profundas consecuencias. Partimos de un grupo abstracto con un cierto número de elementos y concluimos que uno de ellos que no es el neutro commuta con todos los demás. Estos resultados inesperados quizá expliquen por qué tantos matemáticos se sienten fascinados por la teoría abstracta de grupos.

### Ejercicios 14.6

- 1 ¿Cuántas permutaciones de  $S_8$  comutan con  $(135)(24)(67)(8)$ ?
- 2 Sea  $\pi$  una permutación de  $S_n$  con un único ciclo de longitud  $n$ . Demostrar que el centralizador  $C(\pi)$  es el subgrupo cíclico de  $S_n$  generado por  $\pi$ .
- 3 Según el teorema 14.6, todo grupo de orden  $8 (= 2^3)$  tiene un centro no trivial. Comprobar este resultado para el grupo del cuadrado hallando un elemento distinto del neutro que commute con cualquier otro; hacer lo mismo para el grupo discutido en el ejercicio 14.5.1.
- 4 Hallar las clases de conjugación del grupo dado en el ejercicio 14.5.1 y comprobar la ecuación de clases en este caso.
- 5 Demostrar que el orden del centralizador de  $\pi = (123)(45)$  en  $S_7$  es 12. Demostrar que es isomorfo a  $C_6 \times C_2$ , donde  $C_6$  está generado por  $\pi$  y  $C_2$  por una permutación  $\sigma$  que habrá que hallar.

### 14.7 Ejercicios diversos

- 1 Sea  $G$  un subgrupo de  $S_n$ . Demostrar que, o bien todas las permutaciones de  $G$  son pares, o bien la mitad exactamente de ellas son pares.
  - 2 Demostrar que  $A_n$  es el único subgrupo de índice 2 de  $S_n$ .
  - 3 Sea  $\pi$  una permutación cuyos ciclos son de longitud  $n_1, n_2, \dots, n_r$ . Demostrar que el orden de  $\pi$  es el mínimo común múltiplo de los  $n_i$ .
  - 4 Construir subgrupos de  $S_5$  de órdenes 1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24, 60 y 120.
  - 5 Estudiar la posibilidad de que existan subgrupos de  $S_5$  cuyos órdenes no sean de la lista del ejercicio anterior.
  - 6 Sea  $G$  el grupo de automorfismos del grafo  $K_{3,3}$  (definido en el ejercicio 10.1.2) y sea  $v$  un vértice cualquiera. Calcular  $|G_v|$  y  $|G|$ .
  - 7 Demostrar que el grupo de automorfismos del grafo de Petersen tiene orden 120.
  - 8 Se asigna uno de los colores rojo, blanco o azul a cada uno de los vértices de un tetraedro regular: hallar el número de tetraedros indistinguibles.
  - 9 Demostrar que pueden construirse 57 cubos distintos si pintamos cada una de las caras del cubo roja, blanca o azul.
  - 10 Sea  $Y$  el conjunto de las particiones de un 8-conjunto en dos partes de tamaño 4. Supongamos que  $A_8$  actúa sobre  $Y$  tal como corresponde a su acción sobre el 8-conjunto. Demostrar que esta acción sólo tiene una órbita y calcular el orden de un estabilizador.
  - 11 Sea  $G$  un grupo de permutaciones de un conjunto  $X$  que sea abeliano y tenga una única órbita en  $X$ . Demostrar que  $|G| = |X|$ .
  - 12 Demostrar que el número de tarjetas de identidad sobre una retícula cuadrada  $n \times n$  con dos agujeros (como en el apartado 14.4) es
- $$\begin{cases} \frac{1}{16}(n^4 + 6n^2 - 4n) & \text{si } n \text{ es par,} \\ \frac{1}{16}(n^4 + 8n^2 - 8n - 1) & \text{si } n \text{ es impar.} \end{cases}$$
- 13 Se fabrican tarjetas de identidad en forma de triángulo equilátero con  $n$  líneas equidistantes paralelas a cada uno de los lados (en ambas caras de la tarjeta) y un agujero perforado en alguno de los pequeños triángulos que resultan. Si  $n$  es un número impar de la forma  $6m+1$  o  $6m+3$ , demostrar que el número de tarjetas que pueden construirse es  $\frac{1}{6}(n+2)(n+3)$ . ¿Cuál es el resultado si  $n = 6m+5$ ?
  - 14 ¿Cuántos collares pueden hacerse con siete cuentas negras y tres blancas?

15 Se divide un disco circular en ocho sectores iguales, cinco de los cuales se pintan de azul y tres de rojo. ¿De cuántas maneras puede pintarse?

16 Sea  $p$  un número primo y definamos  $T_p$  como el conjunto de las permutaciones de  $Z_p$  dadas por funciones de la forma

$$t(x) = ax + b \quad (x \in Z_p),$$

con  $a$  y  $b$  son de  $Z_p$  y  $a \neq 0$ . Demostrar que  $T_p$  es un grupo de orden  $p(p-1)$ . Demostrar también que, dados dos pares ordenados  $(x_1, y_1)$  y  $(x_2, y_2)$  de elementos distintos de  $Z_p$ , existe una única permutación  $t$  de  $T_p$  tal que  $t(x_1) = x_2$  y  $t(y_1) = y_2$ .

17 Sea  $X$  un conjunto de trasposiciones de  $S_n$  y definamos un grafo  $\Gamma(X)$  como sigue. Los vértices son los enteros  $1, 2, \dots, n$  y  $jk$  es una arista si existe una transposición de  $X$  que intercambia  $j$  y  $k$ . Demostrar que  $\Gamma(X)$  es conexo si, y sólo si, todo elemento de  $S_n$  puede expresarse como producto de trasposiciones de  $X$ .

18 Una inversión en una permutación  $\pi$  de  $N_n$  es un par  $(i, j)$  tal que  $i < j$  y  $\pi(i) > \pi(j)$ . Demostrar que si  $q(\pi)$  es el número total de inversiones de  $\pi$ , entonces  $\text{sgn}(\pi) = (-1)^{q(\pi)}$ .

*En los tres ejercicios siguientes consideraremos un grupo  $G$  de rotaciones en el espacio tridimensional de forma que el eje de cada rotación pase por el origen.*

19 Sea  $S$  una esfera con centro en el origen y supongamos que  $\rho$  es de  $G$ . El eje de  $\rho$  corta a  $S$  en dos puntos llamados los *polos* de  $\rho$ . Demostrar que si  $x$  es un polo de  $\rho$  e  $y = \theta(x)$  para algún  $\theta$  de  $G$ , entonces  $y$  es un polo de  $\theta\rho\theta^{-1}$ . Deducir que  $G$  actúa en el conjunto  $P$  de los polos.

20 Se dice que un polo tiene orden  $m$  si es el polo de una rotación de orden  $m$ . Demostrar que si  $x$  tiene orden  $m_x$ , entonces el tamaño de la órbita de  $x$  es  $|G|/m_x$ . Deducir que

$$2(|G| - 1) = \sum \frac{|G|}{m_x} (m_x - 1),$$

donde la suma se toma sobre las órbitas de  $G$  en  $P$ .

21 Demostrar que la fórmula obtenida en el ejercicio anterior puede reescribirse como

$$2\left(1 - \frac{1}{|G|}\right) = \sum \left(1 - \frac{1}{m_x}\right).$$

Deducir que el número de órbitas es dos o bien tres, y que las distintas posibilidades vienen dadas por la tabla siguiente.

$ G  :$	$n$	$2n$	12	24	60
Órdenes de los polos:	$n, n$	$2, 2, n$	$2, 3, 3$	$2, 3, 4$	$2, 3, 5$

## 15 Anillos, cuerpos y polinomios

### 15.1 Anillos

Aunque el concepto de grupo es muy útil, un grupo es un objeto algebraico bastante restringido, ya que sólo posee una operación. Estamos acostumbrados a tratar con estructuras en las que hay dos operaciones básicas, como la suma y el producto en  $\mathbb{Z}$ .

El objeto más básico de este tipo es un *anillo*, cuyos axiomas son bastante parecidos a los axiomas aritméticos **I1-I6** de los enteros, pero ligeramente más débiles (y más generales, por supuesto). Presentaremos los axiomas de una manera compacta, utilizando el concepto de grupo para unir varios axiomas en uno solo.

**Definición.** Un anillo es un conjunto  $R$  en el que hay definidas dos operaciones binarias  $+$  y  $\times$ , que cumplen los siguientes axiomas.

**R1**  $R$  es un grupo comunitativo con la operación  $+$ .

**R2** La operación  $\times$  tiene las propiedades de clausura, asociativa y elemento neutro.

**R3** (La propiedad distributiva.) Para todos  $a, b$  y  $c$  de  $R$ ,

$$a \times (b + c) = (a \times b) + (a \times c)$$

$$(a + b) \times c = (a \times c) + (b \times c).$$

Por lo general, suprimiremos el símbolo  $\times$  y escribiremos  $ab$  en lugar de  $a \times b$ .

Repasemos las consecuencias de la definición con detalle. Según **R1**, la

operación  $+$  tiene las propiedades siguientes:

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

$$a + 0 = 0 + a = a,$$

$$a + (-a) = (-a) + a = 0,$$

$$a + b = b + a,$$

donde la existencia del neutro  $0$  y del inverso aditivo  $-a$  es parte de la definición. Igualmente, la operación  $\times$  cumple

$$(ab)c = a(bc),$$

$$a1 = 1a = a,$$

donde también se supone la existencia del elemento  $1$ . Sin embargo, hemos de insistir en que *no* supondremos la existencia de un inverso multiplicativo  $a^{-1}$  para cada elemento  $a$ . *No* supondremos tampoco que la operación  $\times$  es comunitativa. Finalmente, el axioma **R3** nos proporciona la regla para tratar con los “paréntesis”, tan habituales en el álgebra elemental.

El prototipo de anillo es, evidentemente, el conjunto  $\mathbb{Z}$  de los enteros con la suma y el producto corrientes. Los enteros poseen dos propiedades adicionales no incluidas en la definición general de anillo: la multiplicación es comunitativa (axioma **I2**, parte (ii)) y el hecho de poder simplificar un entero no nulo a ambos lados de una ecuación (axioma **I7**).

Otro ejemplo conocido de anillo es el conjunto  $\mathbb{Z}_m$  de los enteros módulo  $m$  con las operaciones definidas en el apartado 6.2. El producto en  $\mathbb{Z}_m$  es comunitativo, pero la simplificación no siempre es posible, por ejemplo en  $\mathbb{Z}_6$ , donde tenemos que  $3 \times 1 = 3 \times 5$ , pero no podemos deducir que  $1 = 5$ .

Como ejemplo de anillo en el que no se cumple la propiedad comunitativa podemos tomar el conjunto de las matrices  $2 \times 2$  a coeficientes enteros y las operaciones usuales de suma y producto de matrices. Es fácil comprobar que se cumplen los axiomas **R1**, **R2** y **R3**, pero el producto no es comunitativo. Por ejemplo, si

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix},$$

entonces

$$AB = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}, \quad BA = \begin{pmatrix} 2 & 1 \\ 4 & 4 \end{pmatrix}.$$

**Ejercicios 15.1**

1 Si  $R$  es un anillo, entonces el conjunto  $M_2(R)$  de las matrices  $2 \times 2$  sobre  $R$  es también un anillo (no es necesario comprobarlo).

- (i) ¿Cuál es el neutro aditivo de  $M_2(R)$ ?
- (ii) ¿Cuál es el inverso aditivo  $-A$  de una matriz  $A$  en  $M_2(R)$ ?
- (iii) ¿Cuál es el neutro multiplicativo de  $M_2(R)$ ?
- (iv) ¿Cuál es el cardinal de  $M_2(\mathbf{Z}_m)$ ?
- (v) Demostrar que la multiplicación en  $M_2(\mathbf{Z}_2)$  no es commutativa.
- (vi) ¿Qué elementos de  $M_2(\mathbf{Z}_2)$  tienen inverso multiplicativo?

2 Utilizar el axioma I7 de  $\mathbf{Z}$  para demostrar que, si  $x$  e  $y$  son enteros tales que  $xy = 0$ , entonces  $x = 0$  o  $y = 0$ . Hallar ejemplos que demuestren que no ocurre lo mismo en  $\mathbf{Z}_6$  o en  $M_2(\mathbf{Z})$ .

3 Demostrar que si  $x$  e  $y$  son de un anillo  $R$ , entonces  $(-x)y = -xy$  y  $(-x)(-y) = xy$  (explicar qué propiedad de  $R$  se utiliza en cada paso de la demostración).

**15.2 Elementos inversibles de un anillo**

Se dice que un elemento  $x$  de un anillo  $R$  es **inversible** si  $x$  posee un inverso multiplicativo, es decir, si existe un elemento  $u$  de  $R$  tal que

$$ux = xu = 1.$$

Un argumento sencillo (ejercicio 15.2.2) demuestra que si  $x$  es inversible, el elemento  $u$  es único, de manera que podemos utilizar el símbolo  $x^{-1}$  para denotar  $u$  sin ambigüedades. El elemento  $x^{-1}$  es el **inverso** de  $x$ ; denotamos por  $U(R)$  el conjunto de los elementos inversibles de  $R$ .

Los únicos inversibles de  $\mathbf{Z}$  son 1 y  $-1$ , y cada uno es su propio inverso. En el apartado 6.3 se estudiaron los inversibles de  $\mathbf{Z}_m$ ; según los resultados allá obtenidos, tenemos por ejemplo que  $U(\mathbf{Z}_8) = \{1, 3, 5, 7\}$ .

**Teorema 15.2.** *El conjunto  $U(R)$  de los elementos inversibles de un anillo  $R$  es un grupo con respecto al producto.*

**DEMOSTRACIÓN:** Si  $x$  e  $y$  son inversibles, entonces

$$(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = 1,$$

de manera que  $y^{-1}x^{-1}$  es el inverso de  $xy$ . Así pues,  $U(R)$  es cerrado respecto del producto de  $R$ . El producto es asociativo y 1 pertenece a  $U(R)$  por ser su propio inverso. Finalmente, si  $x$  es de  $U(R)$ , su inverso  $x^{-1}$  es inversible (su inverso es  $x$ ) y también pertenece a  $U(R)$ .  $\square$

Vimos en el apartado 6.3 que el elemento  $r$  era inversible en  $\mathbf{Z}_m$  si, y sólo si,  $\text{mcd}(r, m) = 1$ , de donde se desprende que  $U(\mathbf{Z}_m)$  es un grupo de orden  $\phi(m)$ . Por ejemplo,  $U(\mathbf{Z}_8) = \{1, 3, 5, 7\}$  es un grupo de orden  $\phi(8) = 4$ ; su tabla de grupo es la 15.2.1.

Tabla 15.2.1

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

En este caso, se trata del grupo  $C_2 \times C_2$  de orden 4 no cíclico. Por otra parte,

$$U(\mathbf{Z}_7) = \{1, 2, 3, 4, 5, 6\}$$

es el grupo cíclico  $C_6$  con 3 como generador, ya que

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

En el siguiente capítulo demostraremos que  $U(\mathbf{Z}_p)$  es un grupo cíclico de orden  $\phi(p) = p - 1$  siempre que  $p$  sea primo.

**Ejercicios 15.2**

- 1 Hallar los órdenes de los grupos  $U(\mathbf{Z}_{10})$ ,  $U(\mathbf{Z}_{11})$  y  $U(\mathbf{Z}_{12})$  y describir su estructura.
- 2 Demostrar que si  $x$  es un elemento de un anillo  $R$  y  $u$  y  $v$  son elementos de  $R$  tales que

$$ux = xu = 1, \quad vx = xv = 1,$$

entonces  $u = v$ .

3 Un entero gaussiano es un número complejo de la forma  $m+ni$  donde  $m$  y  $n$  son enteros. Comprobar que el conjunto  $\Gamma$  de los enteros gaussianos es un anillo respecto a la suma y producto ordinarios de los números complejos (no es necesario comprobar explícitamente las propiedades estándar de los números complejos). Hallar los elementos inversibles de  $\Gamma$  y describir la estructura de grupo de  $U(\Gamma)$ .

### 15.3 Cuerpos

Un **cuerpo** es un anillo en el que el producto es commutativo y cada elemento salvo el 0 tiene un inverso multiplicativo. Así pues, en un cuerpo  $F$  se tiene

$$U(F) = F \setminus \{0\}.$$

Para evitar dificultades con los casos triviales, imponemos que un cuerpo tenga al menos dos elementos.

Podemos redefinir un cuerpo como un conjunto que, respecto de las operaciones  $+$  y  $\times$ , cumple

- (i)  $F$  es un grupo commutativo con respecto a  $+$ ,
- (ii)  $F \setminus \{0\}$  es un grupo commutativo con respecto a  $\times$ ,
- (iii) se cumple la propiedad distributiva **R3**.

Nos referiremos a los grupos de (i) y (ii) como al **grupo aditivo** y al **grupo multiplicativo** del cuerpo, respectivamente.

Es evidente que  $\mathbf{Z}$  no es un cuerpo, ya que sólo 1 y  $-1$  tienen inverso en  $\mathbf{Z}$ . Igualmente, el anillo  $\mathbf{Z}_m$  no es un anillo en general, pero el teorema 6.3.1 nos dice que

$\mathbf{Z}_p$  es un cuerpo si  $p$  es primo.

Desde luego, el más conocido de los cuerpos es el cuerpo **R** de los números reales pero, a pesar de ser la base de la mayor parte de la matemática elemental y del análisis, su definición y sus propiedades no son en absoluto elementales. Afortunadamente, los cuerpos más sencillos como  $\mathbf{Z}_p$  son tan importantes para la matemática discreta como pueda serlo **R** para el análisis.

De hecho, existen otros cuerpos finitos además de los cuerpos  $\mathbf{Z}_p$  ( $p$  primo) y en el siguiente capítulo estudiaremos su construcción y propiedades. El ejemplo siguiente contiene la construcción de uno de tales cuerpos.

**Ejemplo.** Sea  $F$  un cuerpo y  $S_2(F)$  el conjunto de las matrices  $2 \times 2$  antisimétricas sobre  $F$ , es decir, matrices de la forma

$$M = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}, \quad (x, y \in F).$$

Demostrar que

- (i)  $S_2(F)$  es un anillo respecto de las operaciones matriciales usuales,
- (ii) la multiplicación en  $S_2(F)$  es commutativa,
- (iii)  $S_2(F)$  es un cuerpo si  $F = \mathbf{Z}_3$  pero no si  $F = \mathbf{Z}_5$ .

**SOLUCIÓN:** (i) El hecho crucial es que  $S_2(F)$  es cerrado respecto de la suma y el producto. Para demostrarlo, no hay más que calcular

$$\begin{aligned} \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} &= \begin{pmatrix} x_1 + x_2 & y_1 + y_2 \\ -(y_1 + y_2) & x_1 + x_2 \end{pmatrix}, \\ \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \times \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} &= \begin{pmatrix} x_1 x_2 - y_1 y_2 & x_1 y_2 + x_2 y_1 \\ -(x_1 y_2 + x_2 y_1) & x_1 x_2 - y_1 y_2 \end{pmatrix}, \end{aligned}$$

y hacer notar que las matrices de la derecha son antisimétricas. También hay que señalar que los neutros de la suma y del producto

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

son ambas antisimétricas, y que si  $M$  es antisimétrica también lo es  $-M$ . Los restantes axiomas de anillo son consecuencia de las propiedades estándar del álgebra de matrices.

(ii) El producto de matrices no es, en general, commutativo, pero sí en el caso que nos ocupa. Ya hemos calculado el producto de dos matrices antisimétricas en un orden; en el orden inverso se obtiene

$$\begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} \times \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_2 x_1 - y_2 y_1 & x_2 y_1 + x_1 y_2 \\ -(x_2 y_1 + x_1 y_2) & x_2 x_1 - y_2 y_1 \end{pmatrix}$$

lo cual, en virtud de los axiomas de cuerpo de  $F$ , es lo mismo.

(iii) Supongamos que

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \text{ tiene por inversa } \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Entonces

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \times \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

de forma que  $ax - by = 1$  y  $ay + bx = 0$ . Despejando formalmente  $a$  y  $b$  se obtiene

$$a = x(x^2 + y^2)^{-1}, \quad b = -y(x^2 + y^2)^{-1}.$$

Como  $F$  es un cuerpo, el elemento  $x^2 + y^2$  tendrá un inverso multiplicativo a menos que sea cero. Si  $x$  e  $y$  son ambos cero, tenemos la matriz cero y no es necesario que tenga inversa. Hemos de preguntarnos por el caso  $x^2 + y^2 = 0$  sin que ambos  $x$  e  $y$  sean cero.

En  $\mathbf{Z}_3$  podemos comprobar explícitamente que  $x^2 + y^2 \neq 0$  siempre que  $(x, y) \neq (0, 0)$ :

$$\begin{array}{ccccccccc} x & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ y & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ x^2 + y^2 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \end{array}$$

Podemos concluir que toda matriz no nula de  $S_2(\mathbf{Z}_3)$  tiene inversa y, por lo tanto, que  $S_2(\mathbf{Z}_3)$  es un cuerpo.

Por otra parte, en  $\mathbf{Z}_5$  tenemos que

$$1^2 + 2^2 = 0,$$

de forma que la matriz con  $x = 1$  e  $y = 2$  no tiene inversa en  $S_2(\mathbf{Z}_5)$  y no tenemos un cuerpo.  $\square$

### Ejercicios 15.3

1 Hemos visto en el ejemplo que  $S_2(\mathbf{Z}_3)$  es un cuerpo; tiene nueve elementos.

- (i) Denotemos los elementos de  $S_2(\mathbf{Z}_3)$  por  $O, I, A_1, A_2, \dots, A_7$ , donde  $O$  e  $I$  son la matriz nula e identidad y  $A_1, A_2, \dots, A_7$  son los elementos restantes.

- (ii) Escribir la tabla del grupo aditivo.
- (iii) Demostrar que el grupo aditivo no es cíclico.
- (iv) Escribir la tabla del grupo multiplicativo.
- (v) Demostrar que el grupo multiplicativo es cíclico.

2 Demostrar que el grupo multiplicativo de  $\mathbf{Z}_{23}$  es cíclico mostrando un generador.

3 Sean  $x$  e  $y$  elementos de un cuerpo tales que  $xy = 0$ . Demostrar que  $x = 0$  o  $y = 0$ .

### 15.4 Polinomios

La palabra *polinomio* en álgebra elemental se utiliza para describir expresiones como

$$x^2 + 4x + 3, \quad 7x^4 + 2x^2 + 3x + 1.$$

Por lo general, no nos preocupamos sobre el significado del símbolo  $x$ , ya que el contexto nos muestra el significado. Por ejemplo, si nos piden resolver la *ecuación*

$$x^2 + 4x + 3 = 0,$$

se supone que  $x$  ha de sustituirse por un número conveniente para que resulte una igualdad válida entre números.

Al calcular con polinomios, los símbolos  $x, x^2, x^3, \dots$  no indican más que las posiciones de los coeficientes. Para sumar dos polinomios, sumamos los coeficientes correspondientes a cada  $x^i$ . Para hallar el coeficiente de  $x^i$  en el producto de dos polinomios, multiplicamos el coeficiente de  $x^j$  en el primero y el de  $x^{i-j}$  en el segundo, y sumamos estos productos para  $j = 0, 1, \dots, i$ . Estas consideraciones nos llevan a la conclusión de que lo importante en un polinomio es la sucesión de sus coeficientes.

Es conveniente basarse en las observaciones anteriores al formular definiciones formales sobre polinomios. Sea  $R$  un anillo conmutativo; diremos que una sucesión finita

$$(a_0, a_1, a_2, \dots, a_n)$$

de elementos de  $R$  es un **polinomio** con coeficientes en  $R$ . Generalmente representaremos este polinomio en la forma tradicional, es decir,

$$a(x) = a_0 + a_1x + \cdots + a_nx^n.$$

No es necesario ser más explícito sobre la  $x$ , ya que se introduce como parte de la notación, más que de la definición. El conjunto de los polinomios con coeficientes en  $R$  se denota por  $R[x]$ . Los polinomios de la forma  $(a_0)$  son los polinomios **constantes** y se identifican de manera evidente con los elementos del anillo  $R$ .

Supongamos que tenemos dos polinomios

$$a(x) = a_0 + a_1x + \cdots + a_nx^n, \quad b(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Podemos suponer, sin pérdida de generalidad, que  $n \geq m$ , y si  $n > m$  ponemos  $b_{m+1} = b_{m+2} = \cdots = b_n = 0$ . Definimos la **suma**  $a(x) + b(x)$  y el **producto**  $a(x)b(x)$  de los polinomios de la siguiente forma:

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \\ a(x)b(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x \\ &\quad + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_mx^{n+m}. \end{aligned}$$

Más formalmente,  $s(x) = a(x) + b(x)$  es el polinomio  $(s_0, s_1, \dots, s_n)$  dado por

$$s_i = a_i + b_i \quad (0 \leq i \leq n),$$

y  $p(x) = a(x)b(x)$  es el polinomio  $(p_0, p_1, \dots, p_{n+m})$  dado por

$$p_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 \quad (0 \leq i \leq n+m).$$

Se desprende de las definiciones que si los coeficientes de  $a(x)$  y  $b(x)$  pertenecen a un anillo  $R$ , los coeficientes de la suma y del producto pertenecen al mismo anillo. Por ejemplo, si  $a(x)$  y  $b(x)$  son los elementos de  $\mathbf{Z}_3[x]$  dados por

$$a(x) = 1 + 2x + 2x^2, \quad b(x) = 2 + x,$$

entonces

$$\begin{aligned} a(x) + b(x) &= (1 + 2) + (2 + 1)x + (2 + 0)x^2 \\ &= 2x^2; \end{aligned}$$

$$\begin{aligned} 63a(x)b(x) &= (1 \times 2) + (1 \times 1 + 2 \times 2)x + (2 \times 2 + 2 \times 1)x^2 + (2 \times 1)x^3 \\ &= 2 + 2x + 2x^3. \end{aligned}$$

En general,  $R[x]$  es cerrado respecto de la suma y del producto. Largas y tediosas comprobaciones nos permitirían demostrar que, de hecho,  $R[x]$  es un anillo conmutativo si lo es  $R$ . Aceptaremos este hecho sin justificación explícita.

También utilizaremos las convenciones de notación estándar para con los polinomios. Suprimiremos el coeficiente 1, de forma que, por ejemplo, escribiremos  $2 + x$  en lugar de  $2 + 1x$ . Si un coeficiente es cero, suprimiremos tanto el coeficiente como la potencia de  $x$  correspondiente (por ejemplo, el coeficiente de  $x^2$  en el producto  $a(x)b(x)$  anterior). Finalmente, acostumbramos a escribir un polinomio con el **coeficiente dominante** en primer lugar, es decir, en la forma

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

donde  $a_n \neq 0$ . Si  $a_n = 1$ , diremos que el polinomio es **mónico**.

### Ejercicios 15.4

1 Calcular la suma y el producto de los siguientes polinomios en  $\mathbf{Z}_5[x]$ :

- (i)  $x^3 + 3x^2 + 2x + 1$  y  $x^2 + 4x + 2$ ;
- (ii)  $x^4 + x^2 + 2$  y  $x^3 + 4x + 1$ .

2 Demostrar que, para calcular el producto de los polinomios

$$a_nx^n + \cdots + a_0 \quad \text{y} \quad b_nx^n + \cdots + b_0$$

usando directamente la definición, son necesarias  $O(n^2)$  multiplicaciones (es notable que este no sea el método más eficiente).

3 Sean

$$a(x) = a_0 + \cdots + a_nx^n$$

y

$$b(x) = b_0 + \cdots + b_mx^m$$

polinomios de  $\mathbf{Z}[x]$ . Escribir un programa que calcule los coeficientes  $c_i$  ( $0 \leq i \leq n+m$ ) del producto  $a(x)b(x)$ .

4 Demostrar que en  $\mathbf{Z}_7[x]$  se cumple

$$(x + 1)^7 = x^7 + 1.$$

¿Para qué valores de  $m$  es cierto que  $(x+1)^m = x^m + 1$  en  $\mathbf{Z}_m[x]$ ?

5 Sea

$$f(x) = f_0 + f_1x + \cdots + f_kx^k$$

un elemento del anillo  $\mathbf{Z}_p[x]$ , donde  $p$  es primo. Sea  $f(x)^n$  el producto de  $n$  factores  $f(x)$  y  $f(x^n)$  el resultado de sustituir  $x$  por  $x^n$  en  $f(x)$ . Demostrar que

- (i)  $f(x)^p = f(x^p)$ ,
- (ii)  $f(x)^r = f(x^{p^r})$  para  $r \geq 1$ .

[Indicación: para la parte (i) usar el teorema multinomial y el ejercicio 5.3.6; para la parte (ii) el principio de inducción.]

## 15.5 El algoritmo de división para polinomios

En álgebra elemental aprendemos cómo hallar el cociente y el resto al "dividir" un polinomio por otro. Las operaciones se suelen disponer como en el siguiente ejemplo:

$$\begin{array}{r} x^4 + 4x^3 + x^2 + 3x + 4 \\ \underline{-} x^4 + 3x^3 + 2x^2 \\ \hline x^3 - x^2 + 3x \\ \underline{-} x^3 + 3x^2 + 2x \\ \hline -4x^2 + x + 4 \\ \underline{-} -4x^2 - 12x - 8 \\ \hline 13x + 12 \end{array}$$

En este caso, la división de  $x^4 + 4x^3 + x^2 + 3x + 4$  entre  $x^2 + 3x + 2$  da  $x^2 + x - 4$  como cociente y  $13x + 12$  como resto. Explícitamente, tenemos que

$$x^4 + 4x^3 + x^2 + 3x + 4 = (x^2 + 3x + 2)(x^2 + x - 4) + (13x + 12).$$

Ésta es una igualdad en  $\mathbf{Z}[x]$ , el anillo de polinomios con coeficientes en  $\mathbf{Z}$ . Resulta claro que el método puede generalizarse; investigaremos ahora los detalles del caso general.

El grado de un polinomio es el máximo valor de  $d$  para el cual el coeficiente de  $x^d$  no es nulo. Por ejemplo, el grado de  $x^2 + 3x + 2$  es 2. Denotaremos el grado del polinomio  $f(x)$  por  $\text{gr } f(x)$ ; nótese que, según nuestra definición, el grado de 0 no está definido (0 denota el polinomio cero). Razones técnicas aconsejan tratar el polinomio cero como un caso especial, de modo que nos conformaremos dejando su grado indefinido.

Si el anillo  $R$  de coeficientes es un anillo como  $\mathbf{Z}_m$ , el grado no siempre tiene las propiedades que nuestra familiaridad con polinomios sobre  $\mathbf{Z}$  o  $\mathbf{R}$  nos haría esperar. Por ejemplo, el grado de la suma de dos polinomios puede ser estrictamente menor que el grado de cualquiera de los sumandos. En  $\mathbf{Z}_3[x]$  tenemos el ejemplo

$$\begin{aligned} a(x) &= x^2 + x + 1, & b(x) &= 2x^2 + x + 1, \\ a(x) + b(x) &= 2x + 2, \end{aligned}$$

con lo que el grado de  $a(x) + b(x)$  es 1, mientras que tanto  $a(x)$  como  $b(x)$  tienen grado 2.

También puede darse el caso de que el grado del producto de dos polinomios sea estrictamente menor que la suma de sus grados. Ya que si

$$\begin{aligned} f(x) &= f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0, \\ g(x) &= g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0, \end{aligned}$$

entonces el coeficiente de  $x^{n+m}$  en  $f(x)g(x)$  es  $f_n g_m$ , que puede ser cero aunque  $f_n \neq 0$  y  $g_m \neq 0$ . Por ejemplo,  $2 \times 3 = 0$  en  $\mathbf{Z}_6$ , con lo que

$$(2x^2 + x + 4)(3x + 1) = 5x^2 + x + 4$$

en  $\mathbf{Z}_6[x]$ . Sin embargo, si los coeficientes están en un cuerpo  $F$ , tenemos la importante propiedad (ejercicio 15.3.3) de que

$$uv = 0 \Rightarrow u = 0 \text{ o } v = 0.$$

Es evidente que esto implica que en  $F[x]$

$$\text{gr } f(x)g(x) = \text{gr } f(x) + \text{gr } g(x).$$

El siguiente teorema es el análogo en  $F[x]$  del teorema de la división para los enteros (teorema 1.5). El hecho de que el grado en  $F[x]$  cumple la ecuación anterior es una parte vital de la demostración.

**Teorema 15.5.** Sea  $F$  un cuerpo y sean  $a(x)$  y  $b(x)$  polinomios de  $F[x]$  con  $b(x) \neq 0$ . Entonces existen polinomios únicos  $q(x)$  y  $r(x)$  tales que

$$a(x) = b(x)q(x) + r(x),$$

siendo  $\text{gr } r(x) < \text{gr } b(x)$ , o bien  $r(x)$  igual a cero.

**DEMOSTRACIÓN:** Supondremos  $b(x)$  fijo y procederemos por inducción sobre el grado de  $a(x)$ . Si  $\text{gr } a(x) < \text{gr } b(x)$ ; podemos satisfacer las condiciones tomando  $q(x) = 0$  y  $r(x) = a(x)$ , ya que

$$a(x) = b(x) \times 0 + a(x).$$

Si  $\text{gr } a(x) \geq \text{gr } b(x)$ , supondremos por inducción que el resultado es cierto para todos los polinomios de grado estrictamente menor que el de  $a(x)$ . Sean

$$a(x) = a_{d+k}x^{d+k} + \cdots + a_0, \quad b(x) = b_dx^d + \cdots + b_0,$$

donde  $a_{d+k} \neq 0$ ,  $b_d \neq 0$  y  $k \geq 0$ . Sea también

$$\bar{a}(x) = a(x) - a_{d+k}b_d^{-1}x^k b(x).$$

El coeficiente de  $x^{d+k}$  en  $\bar{a}(x)$  es

$$a_{d+k} - (a_{d+k}b_d^{-1})b_d = 0,$$

de forma que  $\text{gr } \bar{a}(x) < \text{gr } a(x)$ . Según la hipótesis de inducción, existen polinomios  $\bar{q}(x)$  y  $r(x)$  tales que

$$\bar{a}(x) = b(x)\bar{q}(x) + r(x),$$

donde  $\text{gr } r(x) < \text{gr } b(x)$ , o bien  $r(x) = 0$ . Así pues, tomando

$$q(x) = \bar{q}(x) + a_{d+k}b_d^{-1}x^k$$

tenemos que

$$a(x) = b(x)q(x) + r(x),$$

como queríamos demostrar. Esto completa la inducción y el resultado es cierto para todos los valores de  $\text{gr } a(x)$ .

Para demostrar que  $q(x)$  y  $r(x)$  son únicos, supongamos que

$$a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x),$$

donde  $\text{gr } r_1(x) < \text{gr } b(x)$ , o bien  $r_1(x) = 0$ , y análogamente para  $r_2(x)$ . Entonces

$$b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

Si  $q_1(x) \neq q_2(x)$ , el grado del término izquierdo es como mínimo el de  $b(x)$ . Por otra parte, si el término derecho no es nulo su grado es estrictamente menor que el de  $b(x)$ . Concluimos que ambos términos han de ser cero y que  $q_1(x) = q_2(x)$  y  $r_1(x) = r_2(x)$ .  $\square$

Vale la pena señalar que la construcción de  $\bar{a}(x)$  en la demostración coincide precisamente con la manera de dividir dos polinomios. En el ejemplo al principio del apartado, empezamos con

$$a(x) = x^4 + 4x^3 + x^2 + 3x + 4, \quad b(x) = x^2 + 3x + 2$$

y en el primer paso obtuvimos

$$\bar{a}(x) = x^5 - x^2 + (3x + 4).$$

Desde luego, al disponer los cálculos según el procedimiento usual no "bajamos" los términos  $3x$  y  $4$  hasta que es necesario.

### Ejercicios 15.5

- Hallar el cociente y el resto de dividir  $x^3 + x^2 + 1$  entre  $x^2 + x + 1$  en  $\mathbb{Z}_2[x]$ .
- Hallar el cociente y el resto de dividir  $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$  entre  $x^2 + 2x + 3$  en  $\mathbb{Z}_5[x]$ .
- Repetir el ejercicio 2 considerando los polinomios como elementos de  $\mathbb{Z}[x]$  y comentar la relación entre los dos resultados.
- Sin efectuar más divisiones, hallar el cociente y el resto de dividir  $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$  entre  $x^2 + 2x + 3$  en  $\mathbb{Z}_7[x]$  y en  $\mathbb{Z}_{73}[x]$ .
- Sea  $F$  un cuerpo. Demostrar que el polinomio  $p(x)$  tiene un inverso en el anillo  $F[x]$  si, y sólo si,  $p(x)$  es una constante no nula.

## 15.6 El algoritmo de Euclides para polinomios

Ahora que tenemos un algoritmo de división en  $F[x]$ , análogo al bien conocido de  $\mathbf{Z}$ , continuaremos con algunas definiciones y teoremas sobre divisibilidad y factorización de polinomios.

Diremos que  $g(x)$  es un divisor (o factor) de  $f(x)$  en  $F[x]$  si existe un polinomio  $h(x)$  de  $F[x]$  tal que  $f(x) = g(x)h(x)$ . Dados dos polinomios  $a(x)$  y  $b(x)$  de  $F[x]$ , decimos que  $d(x)$  es un **máximo común divisor (mcd)** de  $a(x)$  y  $b(x)$  si

- (i)  $d(x)$  es un divisor de  $a(x)$  y  $b(x)$  y
- (ii) todo divisor de  $a(x)$  y  $b(x)$  es también divisor de  $d(x)$ .

Según la definición, en general no existe un único mcd de dos polinomios. Si  $d_1(x)$  y  $d_2(x)$  son dos mcds, entonces  $d_1(x) = \alpha d_2(x)$  para algún polinomio constante  $\alpha$  (ejercicio 15.6.4). De esta forma, existirá un único mcd mónico (es decir, con coeficiente dominante igual a 1) y, si se desea, puede definirse como el mcd; en general, sin embargo, no será conveniente introducir esta restricción.

Para calcular el mcd de  $a(x)$  y  $b(x)$  en  $F[x]$  imitaremos el método utilizado en  $\mathbf{Z}$  de dividir repetidamente; este es el *algoritmo de Euclides* para  $F[x]$ . El método sigue el esquema ya conocido:

$$a(x) = b(x)q_0(x) + r_0(x)$$

$$b(x) = r_0(x)q_1(x) + r_1(x)$$

$$r_0(x) = r_1(x)q_2(x) + r_2(x)$$

...

$$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$$

$$r_{n-1}(x) = r_n(x)q_{n+1}(x).$$

La última ecuación nos dice que  $r_n(x)$  es un divisor de  $r_{n-1}(x)$ ; la penúltima muestra que también lo es de  $r_{n-2}(x)$  y, utilizando las ecuaciones en orden inverso, llegamos a la conclusión de que  $r_n(x)$  es un divisor de  $b(x)$  y de  $a(x)$ . Por otra parte, la primera ecuación nos dice que cualquier divisor  $c(x)$  de  $a(x)$  y de  $b(x)$  es también un divisor de  $r_0(x)$ . Utilizando las ecuaciones en el orden en que están dispuestas, vemos que  $c(x)$  divide también a  $r_1(x), r_2(x), \dots, r_{n-1}(x)$  y  $r_n(x)$ . Resulta, pues, que  $r_n(x)$  es un mcd de  $a(x)$  y  $b(x)$ .

Por sustituciones sucesivas en las ecuaciones, podemos expresar  $r_n(x)$  en la forma

$$\lambda(x)a(x) + \mu(x)b(x),$$

donde  $\lambda(x)$  y  $\mu(x)$  son polinomios de  $F[x]$ . Además, si  $d(x)$  es cualquier mcd de  $a(x)$  y  $b(x)$ , entonces  $d(x)$  es un múltiplo constante de  $r_n(x)$  (de nuevo el ejercicio 15.6.4). Hemos demostrado el siguiente resultado importante.

**Teorema 15.6.** Sea  $F$  un cuerpo y  $d(x)$  el mcd de los polinomios  $a(x)$  y  $b(x)$  en  $F[x]$ . Entonces existen polinomios  $\lambda(x)$  y  $\mu(x)$  en  $F[x]$  tales que

$$d(x) = \lambda(x)a(x) + \mu(x)b(x).$$

□

**Ejemplo.** Hallar el mcd de

$$a(x) = x^3 + x^2 + x + 1$$

y

$$b(x) = x^2 + 5$$

en  $\mathbf{Z}_7[x]$  y expresarlo en la forma  $\lambda(x)a(x) + \mu(x)b(x)$  con  $\lambda(x)$  y  $\mu(x)$  de  $\mathbf{Z}_7[x]$ .

**SOLUCIÓN:** Si recordamos que los coeficientes están en  $\mathbf{Z}_7$ , el primer paso es

$$\begin{array}{r} x^3 + 2x^2 + x + 1 \\ \underline{-} x^3 - 5x \\ \hline 2x^2 + 3x + 1 \\ \underline{-} 2x^2 - 3 \\ \hline 3x + 5 \end{array}$$

Es decir,

$$x^3 + 2x^2 + x + 1 = (x^2 + 5)(x + 2) + (3x + 5).$$

El siguiente paso es dividir  $x^2 + 5$  entre  $3x + 5$ :

$$\begin{array}{r} x^2 + 5 \\ \hline x^2 + 4x & | 3x + 5 \\ \hline 3x + 5 \\ 3x + 5 \\ \hline 0 \end{array}$$

El resto es cero y tenemos que

$$x^2 + 5 = (3x + 5)(5x + 1),$$

de manera que  $3x + 5$  es un mcd. De la primera ecuación obtenemos

$$\begin{aligned} 3x + 5 &= (x^3 + 2x^2 + x + 1) - (x + 2)(x^2 + 5) \\ &= (x^3 + 2x^2 + x + 1) + (6x + 5)(x^2 + 5), \end{aligned}$$

que tiene la forma requerida con  $\lambda(x) = 1$  y  $\mu(x) = 6x + 5$ .  $\square$

### Ejercicios 15.6

1 Hallar el mcd mónico de  $x^3 + x^2 + x + 1$  y  $x^2 + 2$  en  $\mathbb{Z}_3[x]$  y expresar el resultado en la forma

$$\lambda(x)(x^3 + x^2 + x + 1) + \mu(x)(x^2 + 2).$$

2 Hallar el mcd mónico de  $x^4 + 2x^3 + x^2 + 4x + 2$  y  $x^2 + 3x + 1$  en  $\mathbb{Z}_5[x]$ .

3 Hallar el mcd mónico en  $\mathbb{Z}_2[x]$  de

- (i)  $x^4 + 1$  y  $x^2 + 1$ ,
- (ii)  $x^5 + 1$  y  $x^2 + 1$ ,
- (iii)  $x^9 + 1$  y  $x^6 + 1$ .

¿Es posible hallar una fórmula para el mcd mónico de  $x^n + 1$  y  $x^m + 1$  en  $\mathbb{Z}_2[x]$ ?

4 Sean  $d_1(x)$  y  $d_2(x)$  dos mcds de  $a(x)$  y  $b(x)$  en  $F[x]$ , donde  $F$  es un cuerpo. Demostrar que

- (i)  $d_1(x)$  es un divisor de  $d_2(x)$  y  $d_2(x)$  lo es de  $d_1(x)$ ;
- (ii) si  $d_1(x) = \alpha(x)d_2(x)$  y  $d_2(x) = \beta(x)d_1(x)$ , entonces  $\text{gr } \alpha(x) = \text{gr } \beta(x) = 0$ , con lo que  $\alpha(x)$  y  $\beta(x)$  son polinomios constantes.

### 15.7 Factorización teórica de polinomios

El estudio de la divisibilidad y factorización de enteros en el capítulo 1 culminaba con el teorema según el cual todo entero  $\geq 2$  factoriza en primos de forma única. En este apartado veremos resultados análogos para  $F[x]$ .

En primer lugar, nótese que la existencia de polinomios constantes no nulos permite factorizar trivialmente cualquier polinomio. Esto es debido a que una constante no nula  $\alpha$  tiene un inverso  $\beta$  en  $F$ , que también es su inverso en  $F[x]$ ; de manera que

$$f(x) = \alpha(\beta f(x))$$

es una factorización de  $f(x)$  en  $F[x]$ . Es evidente que tales factorizaciones deben ser ignoradas en nuestro estudio. Por este motivo, decimos que un polinomio  $f(x)$  de  $F[x]$  es **irreducible** si no es un polinomio constante y si, siempre que

$$f(x) = g(x)h(x) \quad \text{en } F[x],$$

algunos de los polinomios  $g(x)$  o  $h(x)$  sea constante. Los polinomios irreducibles juegan el mismo papel en  $F[x]$  que los números primos en  $\mathbb{Z}$ .

El siguiente teorema se demuestra de forma similar al teorema 1.8.2, de manera que su demostración se presenta como una serie de ejercicios.

**Teorema 15.7.** *Todo polinomio no constante  $f(x)$  de  $F[x]$  puede expresarse como producto de polinomios irreducibles. Si tenemos dos factorizaciones*

$$f(x) = g_1(x)g_2(x) \cdots g_r(x) = h_1(x)h_2(x) \cdots h_s(x),$$

*entonces  $r = s$  y podemos reordenar los factores de forma que  $g_i(x)$  sea un múltiplo constante de  $h_i(x)$  ( $1 \leq i \leq r$ ); es decir,  $g_i(x) = \alpha_i h_i(x)$  para alguna constante  $\alpha_i$  no nula.*  $\square$

**Ejercicios 15.7**

(Todos los polinomios en los ejercicios 1–5 pertenecen a  $F[x]$ , donde  $F$  es un cuerpo.)

1 Demostrar que si  $r(x)$  es un polinomio no constante, entonces

$$\text{gr } r(x)s(x) > \text{gr } s(x).$$

2 (Existencia de factorizaciones.) Demostrar que si  $f(x)$  es un polinomio no constante, entonces  $f(x)$  es irreducible, o bien  $f(x) = g(x)h(x)$ , donde  $g(x)$  y  $h(x)$  son polinomios no constantes cuyos grados son menores que el de  $f(x)$ .

3 Demostrar que si 1 es un mcd de  $r(x)$  y  $s(x)$ , y  $r(x)$  es un divisor de  $s(x)t(x)$ , entonces  $r(x)$  es un divisor de  $t(x)$ .

4 Demostrar que si  $r(x)$  es irreducible y  $r(x)$  es un divisor de  $s_1(x)s_2(x)\cdots s_k(x)$ , entonces  $r(x)$  es un divisor de  $s_i(x)$  para algún  $i$  con  $1 \leq i \leq k$ .

5 (Unicidad de la factorización.) Demostrar la unicidad que se afirma en el teorema 15.7.

6 Comprobar que en  $\mathbf{Z}_{15}[x]$

$$(x+1)(x+14) = (x+4)(x+11).$$

¿Qué significa este resultado en relación a la teoría anterior?

**15.8 Factorización práctica de polinomios**

La existencia de un teorema altamente satisfactorio sobre factorización no significa que sea fácil hallar los factores en un caso concreto. El problema general es difícil, pero existe un test sencillo para hallar los factores de un tipo particular que pasamos a describir.

Un polinomio de la forma  $a_1x + a_0$  con  $a_1 \neq 0$  tiene grado 1; decimos que es un **polinomio lineal**. Si multiplicamos por la constante  $a_1^{-1}$ , el polinomio se transforma en uno de la forma  $x - \alpha$ , con  $\alpha = a_1^{-1}a_0$ . Ésta

será la forma estándar que consideraremos, debido a que existe un test sencillo que nos dice cuándo  $x - \alpha$  es un factor de  $f(x)$  en  $F[x]$ .

Sea

$$f(x) = f_nx^n + f_{n-1}x^{n-1} + \cdots + f_0$$

y, para cada  $\alpha$  de  $F$ , sea

$$f(\alpha) = f_n\alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_0.$$

Por ser  $F$  un cuerpo, la expresión  $f(\alpha)$  es de  $F$ , y decimos que se ha obtenido evaluando  $f(x)$  en  $\alpha$ . La regla que transforma  $\alpha$  en  $f(\alpha)$  es una función de  $F$  en  $F$ ; en rigor debiera llamarse la **función polinómica** correspondiente al polinomio  $f(x)$ . Aunque no es necesario insistir en esta cuestión ahora, existen buenas razones para distinguir entre la función y el polinomio (que no es más que una sucesión de coeficientes): una de tales razones es que polinomios distintos pueden dar lugar a la misma función (ejercicios 15.9.8 y 15.9.16).

**Teorema 15.8.1.** Sea  $F$  un cuerpo y  $f(x)$  un polinomio de  $F[x]$ . Entonces  $x - \alpha$  es un divisor de  $f(x)$  en  $F[x]$  si, y sólo si,  $f(\alpha) = 0$  en  $F$ .

**DEMOSTRACIÓN:** Supongamos que  $x - \alpha$  divide a  $f(x)$ , de forma que

$$f(x) = (x - \alpha)g(x) \quad \text{en } F[x].$$

Si evaluamos ambos lados en  $\alpha$  se obtiene que

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0.$$

Recíprocamente, supongamos que  $f(\alpha) = 0$ . El teorema 15.5 asegura que existen polinomios  $q(x)$  y  $r(x)$  de  $F[x]$  tales que

$$f(x) = (x - \alpha)q(x) + r(x),$$

donde  $\text{gr } r(x) < \text{gr}(x - \alpha)$ , o bien  $r(x) = 0$ . Si evaluamos ambos miembros en  $\alpha$ , teniendo en cuenta que  $f(\alpha) = 0$ ,

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Ahora bien, si  $\text{gr } r(x) < \text{gr}(x - \alpha)$ , entonces el grado de  $r(x)$  ha de ser cero y  $r(x)$  debe ser un polinomio constante no nulo, en cuyo caso  $r(\alpha)$  no

puede ser cero. En consecuencia, debe ser  $r(x) = 0$  y  $x - \alpha$  divide a  $f(x)$ .  $\square$

El teorema anterior se conoce como el **teorema del factor**. Antes de mostrar cómo usarlo en la práctica, mencionaremos una importante consecuencia teórica que nos será útil más adelante. Si  $f(x)$  es un polinomio de  $F[x]$  y  $\alpha$  un elemento de  $F$ , decimos que  $\alpha$  es una **raíz** de la ecuación  $f(x) = 0$  si  $f(\alpha) = 0$ .

**Teorema 15.8.2.** Si  $F$  es un cuerpo y  $f(x)$  un polinomio de grado  $n \geq 1$ , entonces la ecuación  $f(x) = 0$  tiene a lo sumo  $n$  raíces en  $F$ .

**DEMOSTRACIÓN:** Supongamos que la ecuación tiene  $m$  raíces distintas  $\alpha_1, \alpha_2, \dots, \alpha_m$  en  $F$ . Por el teorema del factor,  $x - \alpha_1, x - \alpha_2, \dots, x - \alpha_m$  son divisores de  $f(x)$ . Al ser todos irreducibles, la factorización de  $f(x)$  es de la forma

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)g(x)$$

para algún  $g(x)$  de  $F[x]$ . Como los coeficientes pertenecen a un cuerpo  $F$ , el grado de un producto es igual a la suma de los grados de los factores, de donde se deduce que el grado de  $f(x)$  es al menos  $m$ . O lo que es lo mismo, que el número de raíces de  $f(x) = 0$  es como máximo  $n$ .  $\square$

Volvemos ahora al problema práctico de hallar los factores irreducibles de un polinomio dado. Los casos más interesantes y útiles desde nuestro punto de vista son aquéllos en que los polinomios pertenecen a  $\mathbf{Z}_p[x]$ , donde  $\mathbf{Z}_p$  es el cuerpo de los enteros módulo un primo  $p$ . En este caso podemos hallar todos los factores lineales en un número finito de pasos, ya que el teorema del factor nos dice que no hay más que evaluar el polinomio en cada uno de los elementos de  $\mathbf{Z}_p$ . Por otra parte, no hay ninguna razón para suponer que los factores de un polinomio vayan a ser lineales. Si el grado del polinomio es bajo, podremos hacer algo con métodos rudimentarios, métodos que discutiremos a continuación. Podemos suponer sin pérdida de generalidad que el polinomio es mónico, ya que podemos transformar un polinomio dado en uno mónico del mismo grado multiplicándolo por una constante.

Por definición, un polinomio lineal es irreducible en  $\mathbf{Z}_p[x]$ , de forma que hay  $p$  polinomios lineales monicos irreducibles  $x + a_0$ . Si el polinomio

cuadrático  $x^2 + a_1x + a_0$  es reducible en  $\mathbf{Z}_p[x]$ , entonces posee dos factores lineales que pueden hallarse mediante el teorema del factor. Como hay  $p$  factores lineales posibles, habrá  $p(p-1)/2$  polinomios cuadráticos monicos irreducibles de la forma  $(x - \alpha)(x - \beta)$  con  $\alpha \neq \beta$ , y  $p$  de la forma  $(x - \alpha)^2$ . Hay  $p^2$  cuadráticos monicos en total, así que el número de irreducibles es

$$p^2 - (p(p-1)/2 + p) = p(p-1)/2.$$

En particular, nótese que siempre existe al menos un polinomio cuadrático mónico irreducible en  $\mathbf{Z}_p[x]$ . Si  $p = 2$ , tenemos que

$$x^2 = (x + 0)^2, \quad x^2 + 1 = (x + 1)^2, \quad x^2 + x = (x + 0)(x + 1),$$

pero  $x^2 + x + 1$  es irreducible.

Si un polinomio *cúbico*  $x^3 + a_2x^2 + a_1x + a_0$  es reducible, debe tener tres factores lineales o uno lineal y otro cuadrático. En cualquier caso hay un factor lineal y podemos utilizar de nuevo el teorema del factor para comprobar la reducibilidad. Sin embargo, cuando el grado sea igual o superior a cuatro serán necesarios otros métodos.

**Ejemplo.** Hallar los factores irreducibles de  $x^4 + 1$  en  $\mathbf{Z}_3[x]$ .

**SOLUCIÓN:** En primer lugar utilizaremos el teorema del factor para hallar los factores lineales. Sea  $f(x) = x^4 + 1$ ; entonces

$$f(0) = 0^4 + 1 = 1, \quad f(1) = 1^4 + 1 = 2, \quad f(2) = 2^4 + 1 = 2.$$

Así que no hay factores lineales. La única posibilidad que resta es una factorización en dos polinomios cuadráticos:

$$x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D),$$

con  $A, B, C$ , y  $D$  de  $\mathbf{Z}_3$ . Si igualamos los coeficientes de las potencias correspondientes de  $x$ , obtenemos las ecuaciones

- (i)  $A + C = 0$ ,
- (ii)  $B + D + AC = 0$ ,
- (iii)  $AD + BC = 0$ ,
- (iv)  $BD = 1$ .

De (i) resulta que  $A = -C$  y de (iv) que  $B = D$  (¿por qué?). Tomando  $B = D = 1$  se obtiene  $AC = 1$  en (ii), lo cual contradice (i). Si tomamos

$B = D = 2$  obtenemos  $AC = 2$ , de donde una solución es  $A = 1, C = 2$ . Por lo tanto, la factorización buscada es

$$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2). \quad \square$$

El método que acabamos de exponer es, desde luego, muy poco eficiente en la mayoría de los casos. Se ha invertido mucho esfuerzo en el desarrollo de algoritmos eficientes para hallar factores irreducibles de polinomios, pero muchos de los mejores métodos van más allá del nivel de este libro.

### Ejercicios 15.8

1 Hallar los factores irreducibles de

- (i)  $x^2 + 1$  en  $\mathbf{Z}_5[x]$ ;
- (ii)  $x^3 + 5x^2 + 5$  en  $\mathbf{Z}_{11}[x]$ ;
- (iii)  $x^4 + 3x^3 + x + 1$  en  $\mathbf{Z}_5[x]$ .

2 Hallar todos los polinomios cuadráticos mónicos e irreducibles de  $\mathbf{Z}_3[x]$ .

3 Demostrar que el número de polinomios cúbicos mónicos e irreducibles de  $\mathbf{Z}_p[x]$  es igual a  $p(p^2 - 1)/3$  y dar una lista con todos ellos para  $p = 2$ .

4 Sea  $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_0$  un polinomio de grado  $n$  en  $F[x]$  y sea  $\alpha \in F$ . Explicar cómo evaluar  $f(\alpha)$  mediante la recursión

$$f_0(\alpha) = f_n, \quad f_i(\alpha) = \alpha f_{i-1}(\alpha) + f_{n-i} \quad (1 \leq i \leq n).$$

¿Cuántas multiplicaciones se requieren con este método? (A veces se conoce como *método de Horner*.)

5 Sean  $f(x)$  y  $\alpha$  como en el ejercicio 4. Ahora evaluamos  $f(\alpha)$  calculando cada término  $f_i \alpha^i$  individualmente ( $0 \leq i \leq n$ ). Hallar el número aproximado de multiplicaciones necesarias usando los métodos para calcular  $\alpha^i$  expuestos en el apartado 7.7.

### 15.9 Ejercicios diversos

1 Investigar las estructuras de los grupos de elementos inversibles de  $\mathbf{Z}_{15}$  y de  $\mathbf{Z}_{16}$ .

2 Factorizar los siguientes polinomios de  $\mathbf{Z}_5[x]$  en irreducibles:

- (i)  $x^4 + 4$ ,
- (ii)  $x^4 + 3x^3 + 2x + 4$ .

3 Hallar un polinomio irreducible de grado 4 en  $\mathbf{Z}_5[x]$ .

4 Demostrar que si un entero  $r$  es raíz de la ecuación  $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$  en  $\mathbf{Z}[x]$ , entonces  $r$  es un divisor de  $a_0$ .

5 Hallar el *mcd* mónico de los polinomios  $x^3 + 1$  y  $x^4 + x^2 + 1$  en  $\mathbf{Z}_3[x]$  y en  $\mathbf{Z}_7[x]$ .

6 Demostrar que la multiplicación en un anillo  $R$  es conmutativa si, y sólo si,

$$(a+b)^2 = a^2 + 2ab + b^2$$

para todos  $a$  y  $b$  de  $R$ .

7 Demostrar mediante un ejemplo que si  $m$  no es primo, entonces una ecuación cuadrática en  $\mathbf{Z}_m[x]$  puede tener más de dos raíces en  $\mathbf{Z}_m$ .

8 Sea  $p$  un número primo. Demostrar que los polinomios  $f(x) = x^p$  y  $g(x) = x$  definen la misma función de  $\mathbf{Z}_p$  en sí mismo.

9 Sea  $\phi$  el conjunto de las funciones  $f$  de  $\mathbf{Z}$  en sí mismo y definamos la suma y el producto de dos funciones mediante las reglas  $(f+g)(x) = f(x) + g(x)$ ,  $(fg)(x) = f(x)g(x)$ . ¿Cuáles de los siguientes subconjuntos de  $\phi$  son anillos?

- (i) Las funciones que cumplen  $f(0) = 0$ .
- (ii) Las funciones que cumplen  $f(0) \neq 0$ .
- (iii) Las funciones que cumplen  $f(0) = f(1)$ .
- (iv) Las funciones que cumplen  $f(x) = f(x+1)$  para todo  $x$  de  $\mathbf{Z}$ .

10 Demostrar que si  $a \neq 0$ , el polinomio  $ax^2 + bx + c$  es irreducible en  $\mathbf{Z}_p[x]$  (siendo  $p$  primo) si, y sólo si,  $b^2 - 4ac$  no es cuadrado en  $\mathbf{Z}_p$ .

11 Hallar el *mcd* mónico en  $\mathbf{Z}[x]$  de

$$x^6 + 6x^5 + 8x^4 + x^3 + 4x^2 + 2x + 8 \quad y \quad x^4 + 5x^3 + 6x^2 + 9x + 4.$$

12 Sea  $\omega$  el número complejo  $e^{2\pi i/3}$ . Demostrar que  $1 + \omega + \omega^2 = 0$  y deducir que el conjunto de los números complejos de la forma  $m + nw$  ( $m, n \in \mathbf{Z}$ ) es un anillo. (No es necesario comprobar las propiedades que se desprenden directamente de las propiedades estándar de los números complejos.)

13 Describir el grupo de los elementos inversibles del anillo construido en el ejercicio anterior.

14 Sea  $F$  un cuerpo con un número infinito de elementos. Demostrar que si  $f(x)$  y  $g(x)$  son polinomios de  $F[x]$  que inducen la misma función de  $F$  en sí mismo, entonces  $f(x) = g(x)$ .

15 Sea  $f(x) = f_0 + f_1x + \dots + f_nx^n$  un polinomio con coeficientes en un cuerpo  $F$ . Se define la derivada de  $f(x)$  como el polinomio

$$f'(x) = f_1 + 2f_2x + \dots + nf_nx^{n-1}.$$

Demostrar que (i)  $(f + g)'(x) = f'(x) + g'(x)$ ; (ii)  $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$ .

16 Hallar todos los primos  $p$  para los cuales los polinomios  $x^2 + 3x + 1$  y  $x^6 + 2x^5 + x + 1$  definen la misma función en  $\mathbf{Z}_p$ .

17 Demostrar que el conjunto de los números reales de la forma  $m + n\sqrt{2}$ , donde  $m$  y  $n$  son enteros, es un anillo respecto de las operaciones de suma y producto. Demostrar también que  $m + n\sqrt{2}$  es inversible en este anillo si, y sólo si,  $m^2 - 2n^2 = \pm 1$ .

18 Sean  $i, j$  y  $k$  símbolos que satisfacen las ecuaciones

$$\begin{aligned} i^2 &= j^2 = k^2 = -1, & ij &= -ji = k, \\ jk &= -kj = i, & ki &= -ik = j. \end{aligned}$$

Demostrar que el conjunto  $Q$  de las expresiones de la forma  $a + bi + cj + dk$ , donde  $a, b, c$  y  $d$  son números reales, cumple los axiomas de un cuerpo salvo la propiedad conmutativa del producto ( $Q$  es un ejemplo de **cuerpo no conmutativo** y sus elementos se conocen como **cuaterniones**).

19 Se dice que un elemento  $x$  de un anillo  $R$  es **nilpotente** si  $x^n = 0$  en  $R$  para algún entero positivo  $n$ . Demostrar que si  $x$  e  $y$  son elementos nilpotentes de un anillo  $R$  con un producto conmutativo, entonces  $x + y$  es también nilpotente.

20 Hallar los elementos nilpotentes de los anillos  $\mathbf{Z}_7$ ,  $\mathbf{Z}_8$  y  $\mathbf{Z}_9$ .

21 Demostrar que toda función  $f$  de  $\mathbf{Z}_2$  en sí mismo puede representarse mediante un polinomio  $f(x)$ . ¿Es cierto el resultado para los cuerpos  $\mathbf{Z}_p$  con  $p$  primo?

## 16 Cuerpos finitos y aplicaciones

### 16.1 Un cuerpo con nueve elementos

En el apartado 6.5 vimos cómo usar las propiedades aritméticas de  $\mathbf{Z}_p$  cuando  $p$  es primo para construir un conjunto de  $p - 1$  cuadrados latinos mutuamente ortogonales. Si observamos con cuidado la construcción, veremos que la clave es el hecho de que  $\mathbf{Z}_p$  es un cuerpo. Dado un cuerpo con  $n$  elementos, podríamos utilizar el mismo método para construir  $n - 1$  cuadrados latinos mutuamente ortogonales. Este solo hecho justifica que nos preguntemos si es posible construir otros cuerpos finitos además de los  $\mathbf{Z}_p$ .

De hecho, ya hemos dado un ejemplo de un cuerpo que no tiene un número primo de elementos: el cuerpo formado por las nueve matrices  $2 \times 2$  antisimétricas sobre  $\mathbf{Z}_3$  estudiado en el ejemplo del apartado 15.3. Empezaremos nuestra discusión dando otra construcción de un cuerpo de orden nueve, que denominaremos por  $F_9$ .

Representaremos los elementos de  $F_9$  mediante el 0 y los ocho polinomios de grados 0 y 1 con coeficientes en el cuerpo  $\mathbf{Z}_3$ , es decir,

$$F_9 = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.$$

Este conjunto es cerrado respecto de la suma de polinomios; se tiene, por ejemplo,

$$(x + 1) + (2x + 1) = 2 \quad \text{en } \mathbf{Z}_3[x].$$

Sin embargo, el conjunto no es cerrado para el producto, ya que

$$(x + 1) \times (2x + 1) = 2x^2 + 1 \quad \text{en } \mathbf{Z}_3[x]$$

y  $2x^2 + 1$  no es ninguno de los elementos de  $F_9$ . Esto nos lleva a definir un producto modificado, a saber, calcular primero el producto ordinario

en  $\mathbb{Z}_3[x]$  y después reducir módulo  $x^2 + 1$ . Por ejemplo,

$$\begin{aligned}(x+1) \times (2x+1) &= 2x^2 + 1 && (\text{en } \mathbb{Z}_3[x]) \\ &= 2 + 2(x^2 + 1) \\ &= 2. && (\text{en } F_9).\end{aligned}$$

De forma análoga,

$$\begin{aligned}(2x+1) \times (x) &= 2x^2 + x \\ &= (x+1) + 2(x^2 + 1) \\ &= x + 1.\end{aligned}$$

Es evidente que las operaciones  $+$  y  $\times$  hacen de  $F_9$  un anillo. Los polinomios constantes 0 y 1 son de hecho el 0 y el 1 del anillo, y los restantes axiomas pueden comprobarse con facilidad. Lo que no es tan evidente es que  $F_9$  sea efectivamente un cuerpo; esto es así porque todo elemento no nulo tiene un inverso multiplicativo. El lector escéptico puede comprobar por sí mismo la siguiente tabla.

Elemento:	1	2	$x$	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
Inverso:	1	2	$2x$	$x+2$	$x+1$	$x$	$2x+2$	$2x+1$

En el apartado 16.3 explicaremos la construcción general de la cual  $F_9$  es un caso particular. Por el momento, mencionaremos otra propiedad de  $F_9$  relativa a su grupo multiplicativo. Si calculamos las potencias del polinomio  $2x + 1$  en  $F_9$  se obtienen los siguientes resultados:

$$\begin{aligned}(2x+1)^1 &= 2x+1, & (2x+1)^2 &= x, & (2x+1)^3 &= x+1, \\ (2x+1)^4 &= 2, & (2x+1)^5 &= x+2, & (2x+1)^6 &= 2x, \\ (2x+1)^7 &= 2x+2, & (2x+1)^8 &= 1.\end{aligned}$$

Vemos que todos los elementos no nulos de  $F_9$  pueden expresarse como potencias de  $2x + 1$ . En otras palabras, el grupo multiplicativo de  $F_9$  es el grupo cíclico  $C_8$  generado por  $2x + 1$ :

$$F_9 \setminus \{0\} = U(F_9) = \langle 2x + 1 \rangle \approx C_8.$$

En el apartado 16.4 demostraremos el sorprendente resultado de que el grupo multiplicativo de *cualquier* cuerpo finito es cíclico.

### Ejercicios 16.1

- 1 ¿Qué elementos de  $F_9$  pueden tomarse como generadores de su grupo multiplicativo?
- 2 ¿Qué elementos de  $F_9$  admiten raíz cuadrada en  $F_9$ ?
- 3 Demostrar, sin hacer cálculos explícitos, que el producto de todos los elementos no nulos de  $F_9$  es igual a 2.
- 4 Demostrar que el grupo aditivo de  $F_9$  no es cíclico.

### 16.2 El orden de un cuerpo finito

Sea  $F$  un cuerpo, finito o infinito. Como  $F$  es cerrado para la suma y contiene el neutro del producto 1, los elementos

$$2 = 1 + 1, \quad 3 = 1 + 1 + 1, \quad 4 = 1 + 1 + 1 + 1, \quad \dots$$

pertenecen todos a  $F$  (no afirmamos que sean todos distintos). Para cualquier entero positivo  $n$ , la suma de  $n$  unos es un elemento de  $F$ ; en un lenguaje más formal podemos decir que son los elementos del subgrupo cíclico  $\langle 1 \rangle$  del grupo aditivo de  $F$ .

Si  $F$  es finito, el teorema de Lagrange nos dice que el orden de  $\langle 1 \rangle$  es un divisor de  $|F|$ ; este número se conoce como la **características** de  $F$ . Por ejemplo, en el cuerpo  $\mathbb{Z}_p$  el subgrupo  $\langle 1 \rangle$  comprende todos los elementos, de manera que la característica de  $\mathbb{Z}_p$  es igual a  $p$ . En general, la característica de  $F$  es el menor entero positivo  $m$  tal que  $m = 0$  en  $F$ , donde la última  $m$  denota la suma de  $m$  unos en  $F$  (si  $F$  es infinito la característica puede no estar definida).

Es fácil ver que la característica de un cuerpo finito ha de ser un número primo. En efecto, si  $m$  no fuera primo podría escribirse como un producto  $m_1m_2$ , y si en un cuerpo tenemos  $m_1m_2 = 0$ , entonces  $m_1 = 0$  o  $m_2 = 0$ . Así pues, si un número no es primo no puede ser el mínimo para el cual  $m = 0$ . En el siguiente teorema usaremos el hecho de que la característica es prima para determinar la estructura del grupo aditivo de un cuerpo finito y para demostrar que el orden de un cuerpo finito ha de ser de una forma muy especial.

**Teorema 16.2.** Si  $F$  es un cuerpo finito de característica  $p$ , entonces el grupo aditivo de  $F$  es isomorfo a  $(C_p)^r$ , producto directo de  $r$  copias de  $C_p$ . En consecuencia,  $|F| = p^r$  para algún  $r \geq 1$ .

**DEMOSTRACIÓN:** Dado un elemento  $f \neq 0$  de  $F$  y un entero positivo  $n$ , podemos definir el elemento

$$nf = (1 + 1 + \cdots + 1)f = f + f + \cdots + f$$

de  $F$ , donde en la suma hay  $n$  términos. Estos elementos forman el subgrupo cíclico  $\langle f \rangle$  del grupo aditivo de  $F$ . Al ser  $p = 0$  en  $F$ , los únicos valores relevantes de  $n$  son  $0, 1, \dots, p - 1$ , y podemos considerar  $n$  como un elemento de  $Z_p$ .

Diremos que el subconjunto  $\{f_1, f_2, \dots, f_k\}$  genera  $F$  si todo elemento  $f$  de  $F$  puede escribirse como

$$f = n_1 f_1 + n_2 f_2 + \cdots + n_k f_k \quad (n_1, n_2, \dots, n_k \in Z_p).$$

Tales conjuntos existen:  $F$ , por ejemplo, es uno de ellos. Supongamos que  $\{f_1, f_2, \dots, f_k\}$  genera  $F$  pero no ningún subconjunto propio. Entonces cada una de las expresiones

$$n_1 f_1 + n_2 f_2 + \cdots + n_k f_k \quad (n_1, n_2, \dots, n_k \in Z_p).$$

es un elemento de  $F$ . Si dos expresiones representan el mismo elemento de  $F$ , pongamos

$$n_1 f_1 + n_2 f_2 + \cdots + n_r f_r = m_1 f_1 + m_2 f_2 + \cdots + m_r f_r,$$

tomamos el primer índice  $i$  tal que  $n_i \neq m_i$  y reescribimos la igualdad como

$$(n_i - m_i) f_i = (m_{i+1} - n_{i+1}) f_{i+1} + \cdots + (m_r - n_r) f_r.$$

Al ser  $n_i - m_i \neq 0$ , tiene un inverso en  $Z_p$ . Si multiplicamos la ecuación por  $(n_i - m_i)^{-1}$ , obtendremos una expresión de  $f_i$  en términos de  $f_{i+1}, \dots, f_r$ . De esta forma podríamos eliminar  $f_i$  del conjunto generador, contrariamente a la suposición de que ningún subconjunto propio de  $\{f_1, f_2, \dots, f_r\}$  generaba  $F$ .

Se deduce que existe una biyección entre los elementos de  $F$  y la  $r$ -plas  $(n_1, n_2, \dots, n_r)$  de elementos de  $Z_p$ . Como la suma en  $F$  corresponde a la

suma de las  $r$ -plas, la biyección es un isomorfismo entre el grupo aditivo de  $F$  y el producto directo de  $r$  copias de  $Z_p$  (considerado como grupo cíclico), es decir,  $(C_p)^r$ .  $\square$

La consecuencia más inmediata del teorema es que el orden de un cuerpo finito ha de ser una potencia de un número primo. Conocemos los cuerpos  $Z_p$  (de orden  $p$ ) y hemos encontrado dos ejemplos de cuerpos de orden 9 (es decir,  $3^2$ ). Nuestro siguiente objetivo será demostrar que existen cuerpos de orden  $p^r$  para todo primo y todo  $r \geq 1$ .

### Ejercicios 16.2

- 1 Las tablas 16.2.1 definen las operaciones  $+$  y  $\times$  en el conjunto  $\{w, y, z, t\}$ ; la estructura resultante es un cuerpo  $F_4$ .

Tabla 16.2.1

$+$	$w$	$y$	$z$	$t$	$\times$	$w$	$y$	$z$	$t$
$w$	$w$	$y$	$z$	$t$	$w$	$w$	$w$	$w$	$w$
$y$	$y$	$w$	$t$	$z$	$y$	$w$	$y$	$z$	$t$
$z$	$z$	$t$	$w$	$y$	$z$	$w$	$z$	$t$	$y$
$t$	$t$	$z$	$y$	$w$	$t$	$w$	$t$	$y$	$z$

- (i) Identificar los elementos 0 y 1 de  $F_4$ .  
(ii) Demostrar que los grupos aditivo y multiplicativo de  $F_4$  son isomorfos a  $C_2 \times C_2$  y  $C_3$ , respectivamente.  
(iii) ¿Cuál es la característica de  $F_4$ ?

2 Demostrar que el subconjunto de un cuerpo  $F$  formado por los elementos de la forma  $1 + 1 + \cdots + 1$  es a su vez un cuerpo  $F_0$  (conocido como el **cuerpo primo** de  $F$ ).

3 Sea  $F$  un cuerpo de característica 3. Demostrar las siguientes identidades en  $F$ :

- (i)  $x^3 + y^3 = (x + y)^3$ ,  
(ii)  $(x + y)^4 + x^4 + (x - y)^4 + y^4 = 0$ .

4 Demostrar que un cuerpo de característica  $p$  se tiene

$$(x+y)^p = x^p + y^p.$$

[Indicación: ejercicio 4.3.5.]

### 16.3 Construcción de cuerpos finitos

El cuerpo de orden nueve que construimos en el apartado 16.1 puede considerarse de una forma algo más abstracta. La relación  $\sim$  definida en  $\mathbb{Z}_3[x]$  mediante

$$a(x) \sim b(x) \iff a(x) - b(x) \text{ es divisible por } x^2 + 1$$

es una relación de equivalencia. Los polinomios

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$$

forman un sistema completo de representantes de las clases de equivalencia y podemos tomar estas clases, en lugar de sus representantes, como elementos de  $F_9$ . Si denotamos la clase de equivalencia de  $a(x)$  mediante  $[a(x)]$ , podemos definir la suma y el producto de clases de equivalencia de forma natural como

$$[a(x)] + [b(x)] = [a(x) + b(x)], \quad [a(x)][b(x)] = [a(x)b(x)],$$

definiciones que corresponden exactamente a los cálculos elementales del apartado 16.1.

Este punto de vista más abstracto abre la vía a una construcción general de los cuerpos finitos. El punto crítico es que el polinomio que define las clases de equivalencia ha de ser *irreducible*.

**Teorema 16.3.** Sea  $k(x)$  un polinomio irreducible de grado  $r$  en  $\mathbb{Z}_p[x]$  y sea  $\sim$  la relación de equivalencia definida en  $\mathbb{Z}_p[x]$  mediante

$$a(x) \sim b(x) \iff a(x) - b(x) \text{ es divisible por } k(x).$$

En estas condiciones, el conjunto de las clases de equivalencia de  $\sim$  es un cuerpo de orden  $p^r$ .

**DEMOSTRACIÓN:** Es evidente que los polinomios de grados  $0, 1, \dots, r-1$  forman un conjunto completo de representantes de las clases de equivalencia, de manera que hay  $p^r$  clases en total. Por otra parte, es un ejercicio rutinario comprobar que las clases (al igual que los propios polinomios) forman un anillo y que el producto es conmutativo.

Lo importante es demostrar que cualquier clase salvo  $[0]$  tiene un inverso multiplicativo, y es ahí donde la irreducibilidad de  $k(x)$  es vital. Dado un polinomio  $a(x)$  de  $\mathbb{Z}_p[x]$  de grado  $< r$ , el hecho de que  $k(x)$  sea irreducible significa que el mcd monóico de  $a(x)$  y  $k(x)$  es igual a 1. El teorema 15.6 asegura entonces que existen polinomios  $f(x)$  y  $g(x)$  de  $\mathbb{Z}_p[x]$  tales que

$$a(x)f(x) + k(x)g(x) = 1.$$

Pasando a clases de equivalencia, y recordando que  $[k(x)] = [0]$ , se llega a

$$[a(x)][f(x)] = [1].$$

En otras palabras,  $[a(x)]$  tiene como inverso  $[f(x)]$ .  $\square$

El teorema nos dice que basta con hallar un polinomio irreducible de grado  $r$  en  $\mathbb{Z}_p[x]$  para construir un cuerpo de orden  $p^r$ . Esto parece fácil, y lo es en un sentido muy elemental, pues existen tablas de polinomios irreducibles que cubren todos los valores de  $p$  y  $r$  que verosímilmente puedan darse en la práctica. Pero desgraciadamente la demostración general de que existe al menos un polinomio irreducible para cada valor de  $p$  y  $r$  es más bien difícil. Por esta razón pasamos a deducir algunas propiedades generales de los cuerpos finitos e indicar algunas de sus aplicaciones, y aplazamos la demostración de su existencia hasta el apartado 16.9.

### Ejercicios 16.3

- Demostrar que  $x^3 + x^2 + 1$  es irreducible en  $\mathbb{Z}_2[x]$  y construir un cuerpo de orden 8. ¿Cuál es el orden del grupo multiplicativo? Describir el grupo explícitamente.
- Demostrar que el cuerpo de orden 4 construido mediante el polinomio irreducible  $x^2 + x + 1$  en  $\mathbb{Z}_2[x]$  es esencialmente el mismo que el cuerpo  $F_4$  construido en el ejercicio 16.2.1.

3: ¿Para cuáles de los siguientes primos  $p$  podemos construir un cuerpo de orden  $p^2$  utilizando el polinomio  $x^2 + 1$ ?

$$p = 3, 5, 7, 11, 13, 19, 23.$$

Describir el grupo multiplicativo en los dos primeros casos en que la construcción es posible.

4 Demostrar que para cada primo  $p$  existen cuerpos de orden  $p^2$  y  $p^3$ . [Indicación: véase el apartado 15.8.]

#### 16.4 El teorema del elemento primitivo

En el apartado 16.2 demostramos que el grupo *aditivo* de un cuerpo finito de orden  $q = p^r$  es isomorfo a  $(C_p)^r$ , el producto directo de  $r$  grupos cíclicos  $C_p$ . El grupo *multiplicativo* es de orden  $q - 1$  (ya que excluimos el 0); su estructura es sorprendentemente sencilla.

**Teorema 16.4.** *El grupo multiplicativo de un cuerpo finito es cíclico.*

**DEMOSTRACIÓN:** Sea  $F$  un cuerpo de orden  $q$  y sea  $F^*$  su grupo multiplicativo  $F \setminus \{0\}$ . Si  $f$  pertenece a  $F^*$ , el teorema 13.8.3 implica que  $f^{q-1} = 1$ . En otras palabras, la ecuación  $x^{q-1} - 1 = 0$  tiene  $q - 1$  raíces en  $F$ .

Demostraremos que  $F^*$  cumple la caracterización numérica de los grupos cíclicos obtenida en el teorema 13.9. En concreto, demostraremos que para cada divisor  $d$  de  $q - 1$  existen  $d$  elementos  $f$  de  $F^*$  tales que  $f^d = 1$ .

Sea  $dk = q - 1$ ; la ecuación

$$x^{q-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1)$$

en  $F[x]$  es un resultado de álgebra elemental. Denotaremos el segundo factor mediante  $g(x)$ . Al ser  $g(x)$  un polinomio de grado  $d(k - 1)$ , la ecuación  $g(x) = 0$  tiene como máximo  $d(k - 1)$  raíces en  $F$  (teorema 15.8.2). Análogamente, la ecuación  $x^d - 1 = 0$  tiene a lo sumo  $d$  raíces en  $F$ . Pero como  $x^{q-1} - 1 = 0$  tiene exactamente  $q - 1$  raíces en  $F$  y como

$d(k - 1) + d = q - 1$ , resulta que cada una de las otras ecuaciones ha de tener el máximo número posible de raíces. En particular,  $x^d - 1 = 0$  tiene  $d$  raíces y  $F^*$  posee  $d$  elementos tales que  $f^d = 1$ . El resultado se sigue del teorema 13.9.  $\square$

Recordemos que un grupo es cíclico si todos sus elementos pueden expresarse como potencias de uno dado, al que llamaremos generador del grupo. Así pues, si  $z$  es un generador de  $F^*$  tenemos que

$$F^* = \{1, z, z^2, \dots, z^{q-2}\}, \quad \text{donde } z^{q-1} = 1.$$

Por ejemplo, el grupo multiplicativo del cuerpo  $\mathbf{Z}_{23}$  es un grupo cíclico de orden 22 con 5 como generador, ya que las potencias de 5 nos dan todos los elementos no nulos del cuerpo:

$$\begin{aligned} 5^1 &= 5, & 5^2 &= 2, & 5^3 &= 10, & 5^4 &= 4, \\ &\dots &&&&& \\ 5^{19} &= 75, & 5^{20} &= 12, & 5^{21} &= 14, & 5^{22} &= 1. \end{aligned}$$

Un generador del grupo multiplicativo  $F^*$  se denomina un **elemento primitivo** del cuerpo  $F$ . Con esta terminología, el teorema 16.4 puede enunciarse en la forma siguiente:

*todo cuerpo finito posee un elemento primitivo.*

A pesar de su elegancia y simplicidad, el teorema padece un defecto inevitable: no nos dice cómo hallar un elemento primitivo en cada caso. Como el número de elementos de orden  $q - 1$  en  $C_{q-1}$  es  $\phi(q - 1)$ , un cuerpo finito de orden  $q$  tiene  $\phi(q - 1)$  elementos primitivos. Para hallar uno de ellos "a mano", el mejor método es una versión refinada del "ir probando".

**Ejemplo.** Hallar un elemento primitivo de  $\mathbf{Z}_{41}$ .

**SOLUCIÓN:** El menor entero positivo que podría representar a un elemento primitivo de  $\mathbf{Z}_{41}$  es 2. Si 2 es un elemento primitivo, obtendremos todos los elementos no nulos; si no, habremos obtenido información útil. Tenemos

la siguiente tabla:

$n :$	1	2	3	4	5	6	7	8	9	10
$2^n :$	2	4	8	16	32	23	5	10	20	40
$n :$	11	12	13	14	15	16	17	18	19	20
$2^n :$	39	37	33	25	9	18	36	31	21	1

Así pues, el orden de 2 es 20, y no 40, de donde deducimos que 2 no es un elemento primitivo. Podríamos intentarlo con 3, pero la tabla nos indica que 9 (es decir,  $3^2$ ) es igual a  $2^{15}$ , de manera que

$$3^8 = 9^4 = 2^{60} = (2^{30})^3 = 1,$$

y el orden de 3 es sólo 8. Tanto 4 como 5 son potencias de 2, con lo que sus órdenes han de ser divisores de 20. Pero 6 no es una potencia de 2 y

$$6^2 = 36 = 2^{17}.$$

El orden de  $2^{17}$  es 20 (¿por qué?), de manera que el orden de 6 es 40 y 6 es el elemento primitivo que buscábamos.  $\square$

En la práctica podemos recurrir a tablas que proporcionan el menor entero positivo que es un elemento primitivo de  $\mathbb{Z}_p$ . Estas tablas están disponibles en varios sistemas informáticos y cubren un amplio rango de valores de  $p$ . También hay tablas para el caso en que el orden del cuerpo no es un número primo, sino una potencia  $q$  de un primo; a continuación discutiremos algunos aspectos de este caso.

El cuerpo  $F$  de orden  $q = p^r$  se construye eligiendo un polinomio irreducible  $k(x)$  de grado  $r$  en  $\mathbb{Z}_p[x]$ . Con algo de suerte, puede resultar que el propio polinomio  $x$  sea un elemento primitivo, y en este caso diremos que  $k(x)$  es un polinomio irreducible primitivo.

**Ejemplo.** Demostrar que  $x^2 + 2x + 2$  es un polinomio irreducible primitivo de  $\mathbb{Z}_3[x]$ .

**SOLUCIÓN:** Demostremos en primer lugar que  $x^2 + 2x + 2$  es irreducible. Al ser cuadrático sólo puede tener factores lineales y podemos utilizar el teorema del factor para comprobar si existen. Tenemos que

$$0^2 + (2 \times 0) + 2 = 2, \quad 1^2 + (2 \times 1) + 2 = 2, \quad 2^2 + (2 \times 2) + 2 = 1,$$

con lo que no hay factores lineales y el polinomio es irreducible. Por lo tanto, los polinomios

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$$

representan los elementos de un cuerpo con respecto a la suma y la multiplicación módulo  $x^2 + 2x + 2$ . Si calculamos las potencias de  $x$  en este cuerpo obtenemos

$$\begin{aligned} x^1 &= x, & x^2 &= x+1, & x^3 &= 2x+1, & x^4 &= 2, \\ x^5 &= 2x, & x^6 &= 2x+2, & x^7 &= x+2, & x^8 &= 1. \end{aligned}$$

Así pues,  $x$  genera el grupo multiplicativo del cuerpo y  $x^2 + 2x + 2$  es un polinomio irreducible primitivo.  $\square$

Si usamos el polinomio  $x^2 + 2x + 2$  para construir un cuerpo de orden 9, el hecho de que sea primitivo tiene sus ventajas. Por ejemplo, podemos usar la tabla de las potencias de  $x$  para facilitar la multiplicación, de forma muy similar a cómo se utilizaban las tablas de logaritmos en la aritmética elemental. Si queremos multiplicar  $x+1$  y  $2x+1$  lo haremos de la siguiente forma:

$$(x+1) \cdot (x^2+1) = x^2 \cdot x^3 = x^5 = 2x.$$

Por su parte, el polinomio  $x^2 + 1$  de  $\mathbb{Z}_3[x]$  que usamos en el apartado 16.1 para construir  $F_9$  no es una buena elección, ya que no es primitivo. Si calculamos las potencias de  $x$  en  $F_9$  hallamos que  $x^4 = 1$  y, en consecuencia,  $x$  no es un elemento primitivo de  $F_9$ .

Estas observaciones conducen de forma natural a nuestra última cuestión teórica sobre los cuerpos finitos. Sabemos que dada una potencia  $q = p^r$  de un número primo podemos utilizar cualquier polinomio irreducible de  $\mathbb{Z}_p[x]$  de grado  $r$  para construir un cuerpo de orden  $q$ . ¿Qué conexión existe entre los cuerpos construidos mediante distintos polinomios?

Llegados a este punto, el lector que crea en la belleza de las matemáticas probablemente pensará: son todos iguales. Y, en efecto, lo son. Hemos demostrado que dos cuerpos cualesquiera de orden  $q$  tienen grupos aditivos y multiplicativos isomorfos, de manera que difícilmente podrá sorprender que los cuerpos sean también isomorfos, en el sentido de que existe una

biyección entre ellos que es, al mismo tiempo, un isomorfismo de los grupos aditivo y multiplicativo. Desde luego, desde un punto de vista constructivo, es más importante saber que existe un cuerpo con  $q$  elementos que no que éste es único. Por este motivo nos contentaremos con dar una demostración formal únicamente de la existencia (en el apartado 16.9).

Resumiendo, la teoría de los cuerpos finitos resulta ser notablemente simple:

*Un cuerpo finito tiene orden igual a la potencia de un primo  $q = p^r$ .*

*En esencia, hay un solo cuerpo finito de orden  $q$ .*

*El grupo aditivo del cuerpo es  $(C_p)^r$ .*

*El grupo multiplicativo del cuerpo es  $C_{q-1}$ .*

Utilizaremos la notación  $\mathbf{F}_q$  para el único cuerpo de orden  $q$ . Los cuerpos finitos se conocen también con el nombre de *cuerpos de Galois*, en honor de Évariste Galois (1811-1832), y en ocasiones se denotan también por el símbolo  $GF(q)$ . Por supuesto, si  $q$  es igual a un primo  $p$ , el cuerpo  $\mathbf{F}_p$  (o  $GF(p)$ ) no es más que el cuerpo  $\mathbf{Z}_p$  de los enteros módulo  $p$ .

#### Ejercicios 16.4

1. Hallar el menor entero positivo que representa a un elemento primitivo

$$(i) \text{ en } \mathbf{Z}_7, \quad (ii) \text{ en } \mathbf{Z}_{11}, \quad (iii) \text{ en } \mathbf{Z}_{47}.$$

2. Demostrar que si construimos  $\mathbf{F}_8$  usando el polinomio irreducible  $x^3 + x^2 + 1$  (como en el ejercicio 16.3.1), el polinomio  $x$  es un elemento primitivo.

3. ¿Cuáles de los siguientes polinomios de  $\mathbf{Z}_2[x]$  son irreducibles y cuáles de los irreducibles son primitivos?

$$(i) x^4 + 1, \quad (ii) x^4 + x + 1, \quad (iii) x^4 + x^2 + 1.$$

4. ¿Cuántos elementos primitivos hay en el cuerpo  $\mathbf{F}_{32}$ ? Deducir de la respuesta que el polinomio  $x^5 + x + 1$  es un polinomio irreducible primitivo de  $\mathbf{Z}_2[x]$ .

5. Hallar los valores de  $m$  para los cuales  $x^2 + mx + 2$  es un polinomio irreducible primitivo de  $\mathbf{Z}_{11}[x]$ .

#### 16.5 Cuerpos finitos y cuadrados latinos

En este apartado y en los tres siguientes describiremos algunas de las aplicaciones constructivas de los cuerpos finitos.

Hemos comenzado este capítulo recordando el problema de construir conjuntos de cuadrados latinos mutuamente ortogonales; resulta natural preguntarse cuál es el tamaño máximo de tales conjuntos. Sabemos que para cada primo  $p$  existe un conjunto de  $p - 1$  cuadrados latinos mutuamente ortogonales, y de aquí poco demostraremos que lo mismo se cumple al sustituir  $p$  por una potencia  $q = p^r$ . Pero antes demostraremos que  $n - 1$  es el número máximo de cuadrados latinos mutuamente ortogonales de orden  $n$ , para cualquier  $n$ .

Observemos en primer lugar que los símbolos de cada cuadrado pueden reenumerarse independientemente de forma que la primera fila de cada uno de ellos sea la misma, digamos

$$1 \ 2 \ 3 \ \dots \ n.$$

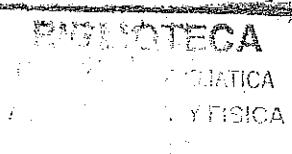
La reenumeración no afecta a la ortogonalidad del conjunto. Consideremos las distintas posibilidades del símbolo en la posición  $(2,1)$ , es decir, segunda fila y primera columna. Este símbolo no puede ser 1, ya que el 1 aparece en la primera columna de cada cuadrado, así que quedan como máximo  $n - 1$  posibilidades. Si dos cuadrados distintos tienen el mismo símbolo en la posición  $(2,1)$ , pongamos  $k$ , al tener también el mismo símbolo  $k$  en la posición  $(1, k)$ , se contradice la hipótesis de ortogonalidad. Por lo tanto, el número máximo de cuadrados latinos de orden  $n$  mutuamente ortogonales es  $n - 1$ .

Las observaciones anteriores indican que el siguiente teorema es el mejor resultado posible sobre conjuntos de cuadrados latinos mutuamente ortogonales. La demostración es una simple transcripción de la del teorema 6.5.2, utilizando el cuerpo finito  $\mathbf{F}_q$  en lugar de  $\mathbf{Z}_p$ .

**Teorema 16.5.** Si  $q$  es una potencia de un número primo, es posible construir  $q - 1$  cuadrados latinos de orden  $q$  mutuamente ortogonales.

**DEMOSTRACIÓN:** Para cada uno de los  $q - 1$  elementos no nulos  $t$  de  $\mathbf{F}_q$  definimos una tabla  $q \times q$  mediante

$$L_t(i, j) = ti + j \quad (i, j \in \mathbf{F}_q).$$



$L_t$  es un cuadrado latino, ya que  $L_t(i, j) = L_t(i, j')$  implica que  $ti + j = ti + j'$ , y esto a su vez implica que  $j = j'$ . De forma análoga, si  $L_t(i, j) = L_t(i', j)$ , como  $\mathbf{F}_q$  es un cuerpo y  $t \neq 0$ , se deduce que  $i = i'$ .

Consideremos ahora los cuadrados latinos  $L_t$  y  $L_u$  y supongamos que tienen el mismo par de símbolos  $(k, k')$  en las posiciones  $(i_1, j_1)$  e  $(i_2, j_2)$ . Entonces

$$\begin{aligned} ti_1 + j_1 &= k, & ui_1 + j_1 &= k', \\ ti_2 + j_2 &= k, & ui_2 + j_2 &= k'. \end{aligned}$$

De aquí resulta que

$$t(i_1 - i_2) = j_2 - j_1, \quad u(i_1 - i_2) = j_2 - j_1.$$

Si  $i_1 - i_2 = 0$  entonces  $j_2 - j_1 = 0$  y las dos posiciones son la misma. En caso contrario,  $i_1 - i_2$  tiene un inverso en  $\mathbf{F}_q$  y

$$t = u = (i_1 - i_2)^{-1}(j_2 - j_1),$$

de manera que  $L_t = L_u$ . Hemos demostrado que si  $t \neq u$  los cuadrados  $L_t$  y  $L_u$  son ortogonales y de esta forma tenemos  $q - 1$  cuadrados latinos de orden  $q$  mutuamente ortogonales.  $\square$

¿Es posible construir  $n - 1$  cuadrados latinos de orden  $n$  mutuamente ortogonales si  $n$  no es una potencia de un primo? Este es uno de los problemas no resueltos más famosos de la matemática discreta y su solución supondría un paso adelante importante en muchas aplicaciones. Sabemos que no es posible si  $n = 6$ ; de hecho, no existen ni siquiera dos cuadrados latinos ortogonales de orden 6 (lo cual significa que el problema de Euler de los 36 oficiales mencionado en el apartado 6.5 no tiene solución). Durante años los matemáticos pensaron que no existía ningún par ortogonal en el caso  $n = 10$ , pero esta conjectura fue refutada en 1960 cuando Bose, Parker y Shrikhande consiguieron construir un par de cuadrados latinos ortogonales de orden 10. Hasta el momento nadie ha sido capaz de construir un conjunto con más de dos cuadrados pero, por otra parte, nadie ha sido capaz de demostrar que es imposible.

### Ejercicios 16.5

- 1 Se han de disponer los números del 0 al 99 en un cuadrado  $10 \times 10$  de manera que no haya dos en la misma fila o columna con el primer o

segundo dígito iguales (para conservar la uniformidad, los enteros del 0 al 9 se representan por 00 hasta 09). Completar la siguiente disposición parcial dada en la tabla 16.5.1 y explicar su relevancia en relación a los comentarios del párrafo anterior.

Tabla 16.5.1

00	47	18	76	29	93	85	34	61	52
86	11	57	28	70	39	94	45	02	63
95	80	22	67	38	71	49	56	13	04
59	96	81	33	07	48	72	60	24	15
73	69	90	82	44	17	58	01	35	26
68	74	09	91	83	55	27	12	46	30
37	08	75	19	92	84				
14	25	36	40	51	62				
21	32	43	54	65	06				
42	53	64	05	16	20				

- Construir una representación explícita de  $\mathbf{F}_4$  y utilizarla para construir un sistema de tres cuadrados latinos mutuamente ortogonales de orden cuatro.
- Renumeral los símbolos de los cuadrados del ejercicio anterior de manera que la primera fila de cada uno de ellos sea 1 2 3 4.
- ¿Cómo pueden construirse 63 cuadrados latinos de orden 64 mutuamente ortogonales? (no se valorarán las respuestas frívolas).

## 16.6 Geometrías finitas y diseños

Otra aplicación importante de los cuerpos finitos es la construcción de diseños. La forma más sencilla de introducir esta aplicación es mediante la geometría analítica elemental.

El lector está familiarizado con la representación de los puntos del plano mediante pares de coordenadas  $(x, y)$ , donde  $x$  e  $y$  pertenecen al cuerpo  $\mathbf{R}$  de los números reales. Si tomamos  $x$  e  $y$  como elementos de un cuerpo *finito*  $\mathbf{F}_q$ , todas las manipulaciones algebraicas de la geometría analítica elemental siguen siendo válidas. Obtenemos un “plano” con un número finito de “puntos” y “rectas”, y las rectas resultan ser los bloques de un 2-diseño en el conjunto de puntos.

Empezaremos por definir un *punto* como un par ordenado  $(x, y)$ , donde  $x$  e  $y$  son elementos de  $\mathbf{F}_q$ . Una *recta* será un conjunto de puntos  $(x, y)$  que satisfacen una ecuación de la forma

$$ax + by = c,$$

donde  $a$ ,  $b$  y  $c$  son a su vez elementos de  $\mathbf{F}_q$ , y  $a$  y  $b$  no son ambos iguales a cero. Hacemos notar que si  $\alpha \neq 0$  en  $\mathbf{F}_q$ , la recta determinada por  $\alpha a$ ,  $\alpha b$  y  $\alpha c$  es la misma que la determinada por  $a$ ,  $b$  y  $c$ .

**Teorema 16.6.** Sea  $\mathbf{F}_q$  un cuerpo finito dado y definamos los puntos y las rectas como se ha indicado. Entonces las rectas son los bloques de un 2-diseño en el conjunto de puntos con parámetros

$$v = q^2, \quad k = q, \quad r_2 = 1.$$

**DEMOSTRACIÓN:** Es evidente que el número de puntos es  $q^2$ ; ya que tanto  $x$  como  $y$  pueden ser elementos cualesquiera de  $\mathbf{F}_q$ . Hemos de demostrar que cada recta tiene exactamente  $q$  puntos y que dos puntos pertenecen a una recta exactamente.

Sea una recta de ecuación  $ax + by = c$ . Si  $b \neq 0$ , cada uno de los  $q$  valores posibles de  $x$  determina un único valor  $y = b^{-1}(c - ax)$  tal que  $(x, y)$  está sobre la recta, de manera que la recta tiene  $q$  puntos. Si  $b = 0$  entonces  $a \neq 0$  (por hipótesis) y la ecuación se convierte en  $ax = c$ , es decir,

$$x = a^{-1}c.$$

En este caso, los  $q$  valores posibles de  $y$  en  $\mathbf{F}_q$  nos dan  $q$  puntos de la forma  $(a^{-1}c, y)$  y todos estos puntos están sobre la recta.

Sean ahora  $(x_1, y_1)$  y  $(x_2, y_2)$  dos puntos distintos. Como  $x_2 - x_1$  e  $y_1 - y_2$  no son ambos cero, la ecuación

$$(y_1 - y_2)x + (x_2 - x_1)y = x_2y_1 - x_1y_2$$

es la ecuación de una recta que contiene a ambos puntos. Si  $ax + by = c$  es la ecuación de otra recta que también los contiene, entonces

$$ax_1 + by_1 = c, \quad ax_2 + by_2 = c.$$

Por lo tanto,

$$a(x_2 - x_1) = b(y_1 - y_2).$$

Si  $x_1 \neq x_2$ , entonces  $(x_2 - x_1)^{-1}$  existe en  $\mathbf{F}_q$  y podemos escribir

$$a = \alpha(y_1 - y_2), \quad \text{donde } \alpha = b(x_2 - x_1)^{-1}.$$

Así pues,  $b = \alpha(x_2 - x_1)$ ; despejando  $c$  tenemos que

$$c = ax_1 + by_2 = \alpha(x_2y_1 - x_1y_2)$$

y la recta es la misma que la anterior. (Si  $x_1 = x_2$  entonces  $y_1 \neq y_2$  y se razona análogamente.) En conclusión, por cada dos puntos pasa una y sólo una recta.  $\square$

El 2-diseño construido en el teorema 16.6 se conoce generalmente como el **plano afín** sobre  $\mathbf{F}_q$ . Podemos calcular los parámetros  $r_1$  (número de rectas que contienen a un punto dado) y  $r_0$  ( $= b$ , número total de rectas) mediante la teoría general desarrollada en el apartado 4.6 y obtenemos

$$r_1 = \left( \frac{v-1}{k-1} \right) r_2 = \frac{q^2-1}{q-1} = q+1,$$

$$b = r_0 = \left( \frac{v}{k} \right) r_1 = \frac{q^2}{q} (q+1) = q^2 + q.$$

Désde luego, los argumentos que usamos para demostrar el teorema son igualmente válidos en el caso del plano ordinario y funcionan debido a que las coordenadas pertenecen a un cuerpo. Podríamos pensar en el

plano ordinario como en un 2-diseño con  $q$  infinito y, en ocasiones, las propiedades conocidas del plano nos ayudan a visualizar propiedades de los planos afines finitos. Por ejemplo, sea  $q = 3$  y consideremos el plano afín sobre  $F_3$ , es decir, sobre  $Z_3$ . Hay nueve puntos

$$\begin{aligned} A &= (0,0), \quad B = (0,1), \quad C = (0,2), \\ D &= (1,0), \quad E = (1,1), \quad F = (1,2), \\ G &= (2,0), \quad H = (2,1), \quad I = (2,2), \end{aligned}$$

y doce rectas, tal como muestra la tabla 16.6.1.

Tabla 16.6.1

Recta	Ecuación	Puntos
$L_1$	$x = 0$	$A B C$
$L_2$	$x = 1$	$D E F$
$L_3$	$x = 2$	$G H I$
$L_4$	$y = 0$	$A D G$
$L_5$	$y = 1$	$B E H$
$L_6$	$y = 2$	$C F I$
$L_7$	$x + y = 0$	$A F H$
$L_8$	$x + y = 1$	$B D I$
$L_9$	$x + y = 2$	$C E G$
$L_{10}$	$2x + y = 0$	$A E I$
$L_{11}$	$2x + y = 1$	$B F G$
$L_{12}$	$2x + y = 2$	$C D H$

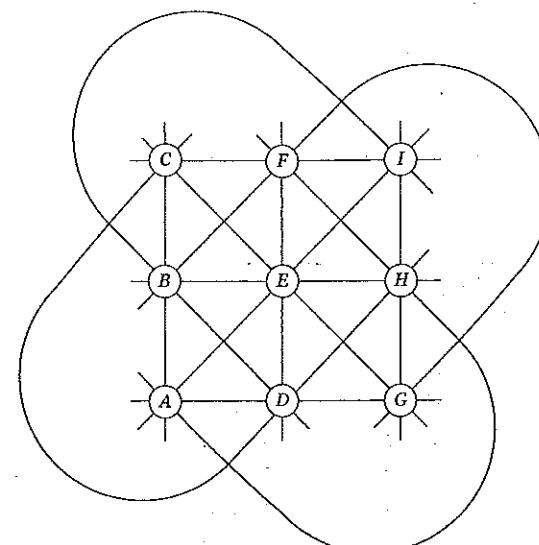
Al igual que en el plano ordinario, las rectas se dividen de forma natural en clases de rectas paralelas; en nuestro caso hay cuatro clases con tres rectas cada una:

$$\{L_1, L_2, L_3\}, \{L_4, L_5, L_6\}, \{L_7, L_8, L_9\}, \{L_{10}, L_{11}, L_{12}\}.$$

Aún más, las propiedades habituales de las rectas paralelas siguen siendo válidas en el plano finito. Cada clase de rectas paralelas contiene exactamente una recta por cada punto y, mientras que dos rectas paralelas

no tienen ningún punto en común, dos rectas no paralelas se cortan en un punto exactamente.

Es instructivo intentar “dibujar” el plano afín sobre  $F_3$  para ilustrar la noción de paralelismo. Sin embargo, esto sólo es posible si dobramos algunas de las rectas (figura 16.1).

Fig. 16.1 El plano afín sobre  $F_3$ .

### Ejercicios 16.6

1 Hacer una tabla con los puntos y las rectas del plano afín sobre  $F_2$  y dibujar el diagrama correspondiente. Explicar por qué este plano en particular no es muy interesante considerado como un 2-diseño.

2 Cuando  $q$  es impar, podemos definir el “punto medio” de  $(x_1, y_1)$  y  $(x_2, y_2)$  como el punto que tiene por coordenadas  $(\frac{1}{2}(x_1 + x_2), \frac{1}{2}(y_1 + y_2))$ , donde  $\frac{1}{2}$  denota el inverso de 2 en el cuerpo  $F_q$ . Sea  $q = 5$  y sean  $A, B$  y  $C$  los puntos  $(1, 2)$ ,  $(3, 1)$  y  $(4, 2)$ , respectivamente.

- (i) Hallar los puntos medios de los lados del triángulo  $ABC$ .
- (ii) Hallar las ecuaciones de las “medianas” del triángulo  $ABC$ .

(iii) Demostrar que las medianas tienen un punto en común  $G$  y hallar sus coordenadas.

3. ¿Cuántos puntos contienen las siguientes "cónicas" del plano afín sobre  $\mathbf{F}_3$ ?

$$\begin{array}{ll} \text{(i)} & y = x^2, \\ & \text{(ii)} xy = 1, \\ \text{(iii)} & x^2 + y^2 = 1, \\ & \text{(iv)} x^2 + 2y^2 = 1. \end{array}$$

4. Igual que en el ejercicio 3, pero con el cuerpo  $\mathbf{F}_5$ ; generalizar los resultados en el caso del cuerpo  $\mathbf{F}_p$  ( $p$  primo). [Indicación: consultar el apartado 16.8 antes de atacar la última parte.]

## 16.7 Planos proyectivos

Desde un punto de vista geométrico, el plano afín carece de una cierta uniformidad. Dos rectas no paralelas tienen un punto en común, mientras que dos rectas paralelas no se cortan. En geometría elemental nos enseñan a aceptar esta situación como correcta, pero los matemáticos estudian desde hace tiempo sistemas alternativos en los que *cada* par de rectas tienen exactamente un punto en común. Esta clase de geometría se conoce con el nombre de *geometría proyectiva*. Estudiaremos la versión finita de la geometría proyectiva y su relación con la teoría de los diseños.

Consideremos de nuevo el plano afín sobre  $\mathbf{F}_3$ . Para conseguir que las rectas paralelas se corten introducimos cuatro nuevos puntos  $W, X, Y$  y  $Z$ , conocidos como *puntos del infinito*. El punto  $W$  se añade a las rectas  $L_1, L_2, L_3$ ;  $X$  se añade a  $L_4, L_5, L_6$ ;  $Y$  se añade a  $L_7, L_8, L_9$ ; y  $Z$  se añade a  $L_{10}, L_{11}, L_{12}$ . Introducimos también una nueva recta  $L_\infty$ , la *recta del infinito*, que contiene a los puntos  $W, X, Y, Z$ . Tenemos pues

13 puntos (los nueve originales y cuatro en el infinito),

y

13 rectas (las doce originales y una en el infinito).

En concreto, las rectas y los puntos que contienen son los siguientes:

$L_1 : ABCW$     $L_2 : DEFW$     $L_3 : GHIW$     $L_4 : ADGX$     $L_5 : BEHX$   
 $L_6 : CFIY$     $L_7 : AFHY$     $L_8 : BDY$     $L_9 : CEGY$     $L_{10} : AEIZ$   
 $L_{11} : BFGZ$     $L_{12} : CDHZ$     $L_\infty : WXYZ$

Notemos en particular que cada recta contiene cuatro puntos y cada par de puntos pertenece a una recta exactamente. Tenemos, por lo tanto, un 2-diseño de parámetros  $(13, 4, 1)$ .

El siguiente teorema muestra cómo realizar una construcción análoga sobre un cuerpo finito cualquiera  $\mathbf{F}_q$  y, de esta manera, obtener un 2-diseño de parámetros  $(q^2 + q + 1, q + 1, 1)$ . El diseño resultante se conoce con el nombre de *plano proyectivo* sobre  $\mathbf{F}_q$ .

**Teorema 16.7.** Si  $q$  es una potencia de un primo, existe un 2-diseño de parámetros

$$v = q^2 + q + 1, \quad k = q + 1, \quad r_2 = 1.$$

Este diseño tiene la propiedad adicional de que dos bloques cualesquiera tienen exactamente un elemento en común.

**DEMOSTRACIÓN:** Definimos en primer lugar la noción general de paralelismo en el plano afín sobre  $\mathbf{F}_q$ , diciendo que las rectas

$$ax + by = c \quad y \quad a'x + b'y = c'$$

son *paralelas* si  $ab' - a'b = 0$  en  $\mathbf{F}_q$ . Está claro que esta definición es independiente de las ecuaciones elegidas para representar las rectas y que define una relación de equivalencia en el conjunto de rectas. Hay  $q + 1$  clases de equivalencia de rectas paralelas, representadas por las  $q$  rectas

$$x + fy = 0 \quad (f \in \mathbf{F}_q),$$

y la recta  $y = 0$ . Cada punto del plano afín pertenece a una, y sólo a una, recta de cada clase.

Introducimos  $q + 1$  nuevos puntos  $\Omega_f$  ( $f \in \mathbf{F}_q$ ) y  $\Omega_\infty$ , y añadimos  $\Omega_f$  a cada recta paralela a  $x + fy = 0$  y  $\Omega_\infty$  a cada recta paralela a  $y = 0$ . Introducimos también una nueva recta  $L_\infty$  que contiene a todos los nuevos puntos.

Comprobemos ahora que las rectas son los bloques de un diseño con los parámetros deseados. Claramente hay  $q^2 + q + 1$  puntos y cada recta contiene  $q + 1$  puntos, de manera que sólo queda por demostrar que dos puntos distintos pertenecen a una única recta. Sean  $P$  y  $Q$  dos puntos; hay tres casos a tener en cuenta.

(i) Si  $P$  y  $Q$  son ambos puntos antiguos (es decir, del plano afín), entonces pertenecen a una única recta del plano, que corresponde a una única recta en el plano extendido.

(ii) Si  $P$  es un punto antiguo y  $Q$  uno nuevo, sea  $Q = \Omega_f$ . Entonces  $P$  pertenece a una única recta antigua en la clase de paralelismo representada por  $\Omega_f$  y esta es la única recta que contiene a  $P$  y  $Q$ . Lo mismo ocurre si  $Q = \Omega_\infty$ .

(iii) Si  $P$  y  $Q$  son los dos antiguos,  $L_\infty$  es la única recta que los contiene a ambos.

En resumen, dos puntos pertenecen a una única recta. El hecho de que dos rectas se corten en un único punto es una consecuencia inmediata de la construcción.  $\square$

Podemos calcular los parámetros  $r_1$  y  $r_0$  ( $= b$ ) del plano proyectivo siguiendo el procedimiento usual:

$$r = \left( \frac{v-1}{k-1} \right) r_2 = \left( \frac{q^2+q}{q} \right) = q+1,$$

$$v = r_0 = \left( \frac{v}{k} \right) r_1 = \left( \frac{q^2+q+1}{q+1} \right) (q+1) = q^2+q+1.$$

( Nótese que el hecho de que  $b = q^2 + q + 1$  es evidente a partir de la construcción, ya que a las  $q^2 + q$  rectas del plano afín se les añade una nueva.) Resumiendo nuestros resultados, podemos ver que hay una reciprocidad entre los puntos y las rectas del plano proyectivo, puesta de manifiesto por los hechos siguientes:

hay  $q^2 + q + 1$  puntos;

hay  $q^2 + q + 1$  rectas;

cada recta contiene  $q + 1$  puntos;

cada punto pertenece a  $q + 1$  rectas;

cada dos puntos pertenecen a una recta común;

cada dos rectas tienen un punto en común.

**Ejemplo.** Construir el plano proyectivo sobre  $F_2$  usando el método dado en el teorema 16.7.

**SOLUCIÓN:** Denotemos los puntos del plano afín sobre  $F_2$  mediante  $A = (0, 0)$ ,  $B = (1, 0)$ ,  $C = (0, 1)$  y  $D = (1, 1)$ . Las seis rectas del plano y sus ecuaciones son las siguientes:

$$\begin{array}{ll} AC : x = 0, & BD : x = 1, \\ AD : x + y = 0, & BC : x + y = 1, \\ AB : y = 0, & CD : y = 1. \end{array}$$

(Nótese que hay tres clases y cada una contiene dos rectas paralelas.) Los nuevos puntos  $\Omega_0$ ,  $\Omega_1$  y  $\Omega_\infty$  forman la recta del infinito y se añaden a las rectas de las respectivas clases en el orden dado. Así pues, las siete rectas del plano proyectivo son

$$AC\Omega_0, BD\Omega_0, AD\Omega_1, BC\Omega_1, AB\Omega_\infty, CD\Omega_\infty, \Omega_0\Omega_1\Omega_\infty.$$

La figura 16.2 contiene un esquema del plano con la recta del infinito en la "base".

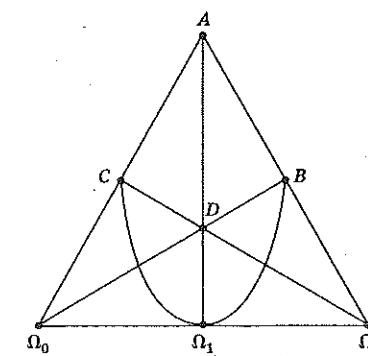


Fig. 16.2 El plano proyectivo sobre  $F_2$ .

**Ejercicios 16.7**

1 Los trece miembros de los Ritos Satánicos y del Club de Bridge de la Universidad de Folornia quieren organizar un programa de manera que cada semana cuatro de ellos puedan encontrarse con el demonio, o jugar al bridge caso de no tener éxito. Debido a que son personas temperamentales, no puede haber dos de ellos en más de uno de estos encuentros de a cuatro. ¿Durante cuántas semanas puede prolongarse el programa? Obtener un programa adecuado al número máximo de semanas.

2 Un *cuadrángulo* en un plano proyectivo es un conjunto de cuatro puntos tales que tres cualesquiera de ellos no sean colineales. Demostrar que hay exactamente siete cuadrángulos en el plano proyectivo sobre  $\mathbf{F}_2$ . ¿Cuál es la relación entre los siete cuadrángulos y las siete rectas?

3 Si  $X, Y, Z$  y  $T$  son los puntos de un cuadrángulo en un plano proyectivo, se definen los puntos  $A, B$  y  $C$  como las intersecciones de  $XY$  con  $ZT$ ,  $XZ$  con  $YT$  y  $XT$  con  $YZ$ , respectivamente. Los puntos  $ABC$  se conocen como los *puntos diagonales* del cuadrángulo. Demostrar que los puntos diagonales de cualquier cuadrángulo del plano proyectivo sobre  $\mathbf{F}_2$  son colineales.

4 Dar un ejemplo que demuestre que el enunciado del ejercicio 3 no es cierto en el plano proyectivo sobre  $\mathbf{F}_3$ .

5 Un *óvalo* en el plano proyectivo sobre  $\mathbf{F}_q$  es un conjunto de  $q + 2$  puntos tales que tres cualesquiera de ellos no son colineales. Demostrar que el número de puntos comunes a una recta y a un óvalo es o bien cero, o bien dos.

**16.8 Cuadrados en cuerpos finitos**

En este apartado utilizaremos el teorema del elemento primitivo para determinar qué elementos de  $\mathbf{F}_q$  tienen raíz cuadrada. Esto proporciona una interesante familia de conjuntos diferencia y una familia asociada de diseños.

Si  $\alpha$  es un elemento primitivo de  $\mathbf{F}_q$ , entonces los elementos no nulos del cuerpo son

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^{q-1} = 1.$$

Es evidente que las potencias pares tienen raíz cuadrada, ya que  $\alpha^{2m} = (\alpha^m)^2$ . La naturaleza de las potencias impares depende de si  $q$  es par (en este caso una potencia de 2) o impar.

Supongamos que una potencia impar de  $\alpha$  tiene raíz cuadrada, pongamos  $\alpha^{2m+1} = \beta^2$ . Como  $\beta$  es también una potencia de  $\alpha$ , tenemos que  $\beta = \alpha^k$  y

$$\alpha^{2(m+k)+1} = \alpha^{2m+1}\alpha^{-2k} = \alpha^{2m+1}(\beta^2)^{-1} = 1.$$

El orden de  $\alpha$  en el grupo multiplicativo de  $\mathbf{F}_q$  es  $q - 1$  y, según el teorema 13.4.2, el entero  $2(m + k) + 1$  ha de ser un múltiplo de  $q - 1$ . Pero si  $q$  es impar,  $q - 1$  es par y  $2(m + k) + 1$  no puede ser múltiplo de  $q - 1$ . Tenemos que si  $q$  es impar, un elemento no nulo de  $\mathbf{F}_q$  tiene raíz cuadrada si, y sólo si, es una potencia par de un elemento primitivo. (Si  $q$  es una potencia de 2, cada elemento de  $\mathbf{F}_q$  tiene raíz cuadrada —véase el ejercicio 16.8.3.)

En lo que sigue nos ocuparemos únicamente del caso en que  $q$  es impar. Denotaremos el conjunto de los cuadrados no nulos de  $\mathbf{F}_q$  mediante  $\square$ ; equivalentemente,  $\square$  es el conjunto de los elementos no nulos que poseen raíz cuadrada, o el conjunto de las potencias pares de un elemento primitivo  $\alpha$ :

$$\square = \{\alpha^2, \alpha^4, \dots, \alpha^{q-1}\}.$$

Por lo tanto,  $|\square| = \frac{1}{2}(q - 1)$ .

En un curso de matemática elemental es frecuente dedicar algún tiempo a discutir la raíz cuadrada de  $-1$ . La cuestión de la raíz cuadrada de  $-1$  en  $\mathbf{F}_q$  también es importante, y el teorema siguiente nos da la respuesta.

**Teorema 16.8.1.** Sea  $q$  una potencia de un primo impar. Si  $q \equiv 1 \pmod{4}$ , entonces  $-1$  tiene raíz cuadrada en  $\mathbf{F}_q$ , pero si  $q \equiv 3 \pmod{4}$ ,  $-1$  no tiene raíz cuadrada.

**DEMOSTRACIÓN:** Demostraremos en primer lugar que

$$\alpha^{(q-1)/2} = -1,$$

donde  $\alpha$  es un elemento primitivo de  $\mathbf{F}_q$ . En efecto, la ecuación  $x^2 = 1$  tiene dos soluciones en  $\mathbf{F}_q$ , ya que el grupo multiplicativo es cíclico y tiene orden par (esto resulta de la caracterización de los grupos cíclicos dada en el teorema 13.9). Es evidente que las dos soluciones son 1 y  $-1$ . Por

otra parte, como  $\alpha$  tiene orden  $q - 1$ , tanto  $\alpha^{q-1}$  como  $\alpha^{(q-1)/2}$  satisfacen  $x^2 = 1$  y han de ser iguales a 1 y -1, respectivamente.

De acuerdo con las consideraciones previas al teorema,  $\alpha^{\frac{1}{2}(q-1)}$  es un cuadrado si, y sólo si,  $\frac{1}{2}(q-1)$  es par; es decir,

$$\frac{1}{2}(q-1) = 2m,$$

o bien  $q = 4m + 1$ . Éste es el resultado enunciado.  $\square$

En el siguiente teorema demostraremos que si  $q \equiv 3 \pmod{4}$ , en cuyo caso -1 no es un cuadrado, el conjunto  $\square$  de los cuadrados de  $\mathbf{F}_q$  es un conjunto diferencia: es decir, la diferencia  $x - y$  ( $x, y \in \square$ ) toma cada valor no nulo el mismo número de veces.

**Teorema 16.8.2.** Si  $q$  es una potencia de un primo de la forma  $4n + 3$ , el conjunto  $\square$  de cuadrados no nulos de  $\mathbf{F}_q$  es un conjunto diferencia con parámetros  $(4n + 3, 2n + 1, n)$ . En otras palabras, cada elemento no nulo de  $\mathbf{F}_q$  puede expresarse como una diferencia de dos cuadrados de  $n$  formas distintas.

**DEMOSTRACIÓN:** Sea  $z$  un cuadrado de  $\mathbf{F}_q$ , digamos  $z = \zeta^2$  con  $\zeta \neq 0$ . Habrá un cierto número de maneras  $\mu$  de expresar  $z$  como diferencia de cuadrados y una expresión típica será

$$z = u^2 - v^2.$$

Demostraremos qué cualquier otro elemento no nulo  $w$  de  $\mathbf{F}_q$  puede expresarse como diferencia de cuadrados del mismo número de maneras. Si  $w$  es un cuadrado,  $w = \omega^2$ , entonces

$$w = (\omega\zeta^{-1})^2\zeta^2 = \beta^2 z \quad (\beta = \omega\zeta^{-1} \in \mathbf{F}_q).$$

Para cada expresión de  $z$  como diferencia de cuadrados existe una expresión correspondiente para  $w$ :

$$w = (\beta u)^2 - (\beta v)^2.$$

Por otra parte, si  $w$  no es un cuadrado, es una potencia impar de un elemento primitivo. Como -1 no es un cuadrado, es también una potencia

impar del mismo elemento primitivo y  $-w = (-1)w$  es una potencia par de dicho elemento. De aquí se deduce que  $-w$  es un cuadrado,  $-w = \theta^2$ , y que

$$w = -\theta^2 = -(\theta\zeta^{-1})^2\zeta^2 = \gamma^2(-z) \quad (\gamma = \theta\zeta^{-1} \in \mathbf{F}_q).$$

De nuevo, para cada expresión de  $z$  como diferencia de cuadrados existe una expresión correspondiente para  $w$ :

$$w = (\gamma u)^2 - (\gamma v)^2.$$

Hemos demostrado que cada elemento no nulo de  $\mathbf{F}_q$  posee el mismo número  $\mu$  de representaciones como diferencia de cuadrados.

Ahora bien,  $|\square| = \frac{1}{2}(q-1) = 2n+1$ , de donde el número total de diferencias de cuadrados distintos es  $2n(2n+1)$ . Como hay  $q-1 = 4n+2$  valores no nulos y cada uno de ellos ocurre  $\mu$  veces, tenemos que

$$2n(2n+1) = \mu(4n+2)$$

y  $\mu = n$  como queríamos demostrar.  $\square$

Si  $p$  es un primo de la forma  $4n+3$ , el teorema nos dice que el conjunto  $\square$  de cuadrados no nulos de  $\mathbf{Z}_p$  es un conjunto diferencia de parámetros  $(4n+3, 2n+1, n)$ , lo cual generaliza el resultado demostrado para  $p = 23$  en el apartado 6.4. Del teorema 6.4 se desprende que los conjuntos  $\square + i$  ( $i \in \mathbf{Z}_p$ ) son los bloques de un 2-diseño con los mismos parámetros.

Puede usarse el mismo método con los conjuntos  $\square + i$  en cualquier cuerpo finito  $\mathbf{F}_q$  si  $q$  es congruente con 3 módulo 4. Observemos que en el caso general no tenemos una construcción cíclica en el sentido del apartado 6.4, ya que el grupo aditivo de  $\mathbf{F}_q$  no es un grupo cíclico. Sin embargo, lo importante es que si  $q$  es una potencia de un primo y congruente con 3 módulo 4, siempre podemos construir un 2-diseño con parámetros  $(q, \frac{1}{4}(q-1), \frac{1}{4}(q-3))$ .

Una propiedad especialmente útil de tales diseños es que pueden extenderse fácilmente a un 3-diseño. Veamos el caso  $q = 7$ , en el que el 2-diseño proviene de  $\square = \{1, 2, 4\}$  en  $\mathbf{Z}_7$ . Los bloques del 2-diseño son

$$124, \quad 235, \quad 346, \quad 450, \quad 561, \quad 602, \quad 013.$$

El diseño extendido tiene dos tipos de bloques. El primero se obtiene añadiendo un nuevo objeto  $\infty$  a cada uno de los bloques iniciales y el

segundo tomando el complementario (en  $\mathbf{Z}_7$ ) de cada uno de los bloques iniciales. De esta forma se obtienen 14 bloques:

$$\begin{array}{ccccccc} \infty 124, & \infty 235, & \infty 346, & \infty 450, & \infty 561, & \infty 602, & \infty 013, \\ 0356, & 0146, & 0125, & 1236, & 0234, & 1345, & 2456. \end{array}$$

Una comprobación cuidadosa demuestra que tenemos un 3-diseño con parámetros  $(8, 4, 1)$ .

No deja de ser sorprendente que el mismo procedimiento funcione para cualquier 2-diseño con parámetros  $(4n+3, 2n+1, n)$ , pero así es y, en consecuencia, tenemos una familia infinita de 3-diseños con parámetros  $(4n+4, 2n+2, n)$ .

### Ejercicios 16.8

- 1 Calcular el conjunto  $\square$  de cuadrados no nulos de  $\mathbf{Z}_{19}$  y construir con él un diseño de parámetros  $(19, 9, 4)$ .
- 2 Construir un 3-diseño con parámetros  $(20, 10, 4)$ .
- 3 Demostrar que si  $q$  es una potencia de 2, entonces todo elemento de  $\mathbf{F}_q$  tiene raíz cuadrada. [Indicación: un entero  $i$  con  $1 \leq i \leq q-1$  es impar si, y sólo si,  $(q-1)+i$  es par.]
- 4 Sea  $F^*$  el grupo multiplicativo del cuerpo finito  $\mathbf{F}_q$ . Demostrar que  $\square$  es un subgrupo de  $F^*$  y que su índice es 2 si  $q$  es impar y 1 si  $q$  es par.
- 5 Explicar cómo construir un 3-diseño con parámetros  $(28, 14, 6)$ .

### 16.9 Existencia de cuerpos finitos

En este apartado demostraremos que para cada primo  $p$  y cada entero  $n \geq 1$  existe un polinomio irreducible de grado  $n$  de  $\mathbf{Z}_p[x]$ . De aquí deduciremos (teorema 16.3) que existe un cuerpo finito de orden  $p^n$ .

El método de la demostración es conceptualmente muy sencillo: obtendremos una fórmula general para el número  $N_n(p)$  de polinomios monicos irreducibles de grado  $n$  de  $\mathbf{Z}_p[x]$  y demostraremos que  $N_n(p)$  no es cero. De todas formas, el trabajo necesario para establecer la fórmula es considerable y la mayor parte tiene que ver con la demostración del siguiente resultado algebraico:

En  $\mathbf{Z}_p[x]$  cada polinomio mónico irreducible cuyo grado divide a  $n$  ocurre una, y sólo una, vez en la factorización del polinomio  $x^{p^n} - x$  y no hay otros factores.

Antes de demostrarlo, veamos cómo conduce al resultado principal.

**Teorema 16.9.** Para cada primo  $p$  y cada entero  $n \geq 1$ , existe un polinomio mónico irreducible de grado  $n$  de  $\mathbf{Z}_p[x]$ .

**DEMOSTRACIÓN:** Sea  $N_n(p)$  el número de polinomios monicos irreducibles de grado  $n$  de  $\mathbf{Z}_p[x]$ . Según la afirmación anterior, la factorización de  $x^{p^n} - x$  en  $\mathbf{Z}_p[x]$  contiene  $N_d(p)$  factores de grado  $d$  para cada divisor  $d$  de  $n$ . Estos factores contribuyen en  $dN_d(p)$  al grado total, que es  $p^n$ ; de aquí se deduce la ecuación

$$p^n = \sum_{d|n} dN_d(p).$$

Aplicando la fórmula de inversión de Möbius (teorema 4.5.2) con  $f(n) = p^n$  y  $g(d) = dN_d(p)$  se obtiene

$$nN_n(p) = \sum_{d|n} \mu(d)p^{n/d},$$

es decir,

$$N_n(p) = \frac{1}{n} \sum_{d|n} \mu(d)p^{n/d}.$$

En la suma del miembro derecho el término con  $d = 1$  es  $p^n$  y los otros términos tienen la forma  $\pm p^i$ , con  $i < n$ . Por lo tanto, una cota inferior de  $N_n(p)$  viene dada por

$$\begin{aligned} N_n(p) &\geq \frac{1}{n}(p^n - (p^{n-1} + p^{n-2} + \cdots + p + 1)) \\ &= \frac{1}{n} \left( p^n - \frac{p^n - 1}{p - 1} \right). \end{aligned}$$

que es estrictamente mayor que cero. Al ser  $N_n(p)$  un número entero, se tiene  $N_n(p) \geq 1$ , tal como se afirmaba.  $\square$

Nótese que para  $n = 1$  la fórmula nos da  $N_1(p) = p$ , en concordancia con el hecho de que todo polinomio mónico  $x - \alpha$  con  $\alpha$  de  $\mathbf{Z}_p$  es irreducible. La fórmula confirma también los resultados que obtuvimos para  $N_2(p)$  y  $N_3(p)$  por razonamiento directo en el apartado 15.8, es decir,

$$\begin{aligned} N_2(p) &= \frac{1}{2}(\mu(1)p^2 + \mu(2)p) = \frac{1}{2}(p^2 - p), \\ N_3(p) &= \frac{1}{3}(\mu(1)p^3 + \mu(3)p) = \frac{1}{3}(p^3 - p). \end{aligned}$$

A continuación nos embarcamos en la demostración del resultado sobre la factorización de  $x^{p^n} - x$  en  $\mathbf{Z}_p[x]$ . Descompondremos la demostración en tres pasos.

- (I) Si  $d$  es un divisor de  $n$ , todo polinomio mónico irreducible de grado  $d$  es un factor de  $x^{p^n} - x$ .
- (II) El grado de cualquier factor mónico irreducible de  $x^{p^n} - x$  es un divisor de  $n$ .
- (III) Los factores irreducibles de  $x^{p^n} - x$  son todos simples.

Si  $n = mk$  tenemos la fórmula

$$z^n - 1 = (z^m - 1)(z^{(k-1)m} + z^{(k-2)m} + \dots + z^m + 1).$$

Si tomamos  $z$  igual a un primo  $p$ , deducimos que

$$m|n \Rightarrow p^m - 1 | p^n - 1,$$

mientras que si  $z$  es una variable polinómica, deducimos que

$$m|n \Rightarrow x^m - 1 | x^n - 1.$$

Los dos resultados conjuntamente nos dan

$$m|n \Rightarrow x^{p^m - 1} - 1 | x^{p^n - 1} - 1.$$

Consideraremos esta última como una propiedad del anillo de polinomios  $\mathbf{Z}_p[x]$ , donde el primo  $p$  se mantendrá fijo en lo que sigue.

**DEMOSTRACIÓN DE (I).** Es evidente que el polinomio  $x$  es un factor de  $x^{p^n} - x$ , ya que

$$x^{p^n} - x = x(x^{p^n - 1} - 1).$$

Vamos a demostrar que cualquier otro polinomio mónico irreducible cuyo grado divida a  $n$  es un factor de  $x^{p^n - 1} - 1$ . Consideremos en primer lugar un polinomio lineal  $x - \alpha$  con  $\alpha \neq 0$ . Segundo el teorema de Fermat,  $\alpha^{p^n} = 1$ , lo cual implica que  $x - \alpha$  es un factor de  $x^{p^n - 1} - 1$ , que a su vez es un factor de  $x^{p^n - 1} - 1$ . Así pues,  $x - \alpha$  es también un factor de  $x^{p^n - 1} - 1$ .

Sea  $f(x)$  un polinomio mónico irreducible de grado  $d \geq 2$ . Sabemos que las clases de equivalencia  $[h(x)]$  de polinomios con respecto a la suma y producto módulo  $f(x)$  forman un cuerpo de orden  $p^d$ . Denotemos los elementos de este cuerpo por  $[0]$  y

$$[h_1(x)], [h_2(x)], \dots, [h_t(x)] \quad (t = p^d - 1).$$

Las clases

$$[xh_1(x)], [xh_2(x)], \dots, [xh_t(x)]$$

son también, en un cierto orden, representantes de los elementos no nulos del cuerpo, de forma que

$$[xh_1(x)][xh_2(x)] \cdots [xh_t(x)] = [h_1(x)][h_2(x)] \cdots [h_t(x)].$$

Si reordenamos la ecuación obtenemos

$$[x^t][h_1(x) \cdots h_t(x)] = [h_1(x) \cdots h_t(x)],$$

con lo que  $[x^t] = [1]$ , o bien

$$[x^{p^d - 1} - 1] = [0].$$

Esto significa que  $x^{p^d - 1} - 1$  es un múltiplo de  $f(x)$ , ya que la clase  $[0]$  está formada por los múltiplos de  $f(x)$ . Como  $d|n$ ,  $x^{p^n - 1} - 1$  es un múltiplo de  $x^{p^d - 1} - 1$ , y también de  $f(x)$ .

**DEMOSTRACIÓN DE (II).** Sea  $g(x)$  un factor mónico irreducible de  $x^{p^n} - x$  y de grado  $m \geq 2$ . Sea  $n = ms + r$ , donde  $0 \leq r < m$ . Demostraremos que el caso  $r > 0$  no puede darse.

Sea  $F$  el cuerpo de orden  $p^m$  formado por las clases de polinomios módulo  $g(x)$ . Por el apartado (I),  $x^{p^m} - x$  es un múltiplo de  $g(x)$ , con lo que  $x^{p^m}$  y  $x$  pertenecen a la misma clase en  $F$ . La igualdad

$$x^{p^n} = x^{p^{ms+r}} = (x^{p^m})^{p^{m-r}}$$

implica que  $x^{p^r}$  está en la misma clase que  $x^{p^n}$ . Como suponemos que  $x^{p^n} - x$  es un múltiplo de  $g(x)$ , también  $x$  pertenece a la misma clase que  $x^{p^n}$ . En consecuencia,  $x$  y  $x^{p^r}$  pertenecen a la misma clase en  $F$ .

El razonamiento anterior indica que, dado un polinomio  $h(x)$ , el polinomio  $h(x^{p^r})$  que se obtiene sustituyendo  $x$  por  $x^{p^r}$  está en la misma clase que  $h(x)$ . Pero según el ejercicio 15.4.5 tenemos que  $h(x^{p^r}) = h(x)^{p^r}$ , de donde

$$[h(x)] = [h(x^{p^r})] = [h(x)^{p^r}] = [h(x)]^{p^r}.$$

En otras palabras, cada uno de los  $p^m$  elementos de  $F$  es raíz de la ecuación  $x^{p^r} - x = 0$ . Si  $r > 0$ , la ecuación tiene grado  $p^r$  y no puede tener  $p^m$  raíces, ya que  $m > r$ . La única posibilidad es  $r = 0$  y  $m$  resulta ser un divisor de  $n$  como afirmábamos.

**DEMOSTRACIÓN DE (III).** Sólo nos queda demostrar que un polinomio irreducible  $k(x)$  no puede ser un factor múltiple de  $x^{p^n} - x$ . Si

$$k(x) = k_0 + k_1 x + \cdots + k_u x^u,$$

podemos definir su *derivada formal*  $k'(x)$  como el polinomio

$$k'(x) = k_1 + 2k_2 x + \cdots + u k_u x^{u-1}.$$

Esta definición es independiente de cualquier razonamiento de paso al límite, pero concuerda con las reglas del cálculo infinitesimal. En particular, la regla de la derivada del producto es la usual y puede demostrarse mediante un cálculo directo (ejercicio 15.9.15).

Supongamos que  $k(x)$  es un factor múltiple de  $x^{p^n} - x$ , de forma que

$$x^{p^n} - x = k(x)^2 l(x)$$

para algún  $l(x)$  de  $\mathbb{Z}_p[x]$ . Si derivamos formalmente la ecuación y recordamos que  $p^n = 0$  en  $\mathbb{Z}_p$ , se obtiene que

$$-1 = 2k(x)k'(x)l(x) + k(x)^2 l'(x).$$

Pero esto implica que  $k(x)$  es un factor de  $-1$ , lo cual es imposible a menos que  $k(x)$  sea constante. Hemos demostrado finalmente el resultado.  $\square$

### Ejercicios 16.9

- 1 Obtener las fórmulas para  $N_4(p)$ ,  $N_5(p)$  y  $N_6(p)$ .
- 2 ¿Cuántos polinomios monómicos irreducibles hay de grado 4 en  $\mathbb{Z}_2[x]$ ? Hallarlos todos.
- 3 Hallar los factores irreducibles de  $x^{16} - x$  en  $\mathbb{Z}_3[x]$ .
- 4 Formar una tabla con los valores de  $N_n(2)$  para  $1 \leq n \leq 10$ . Para cada  $n$  calcular el porcentaje aproximado del número total de polinomios monómicos de grado  $n$  de  $\mathbb{Z}_2[x]$  que son irreducibles.
- 5 Sea  $F$  un cuerpo finito. Se dice que un subconjunto  $S$  de  $F$  es un *subcuerpo* si los elementos de  $S$  forman un cuerpo con las operaciones de  $F$ .
  - (i) Demostrar que la característica de  $S$  es igual a la de  $F$ .
  - (ii) Demostrar que si  $|S| = p^s$  y  $|F| = p^r$ , entonces  $s$  es un divisor de  $r$ . [Indicación: el grupo multiplicativo de  $S$  es un subgrupo del grupo multiplicativo de  $F$ .]
  - (iii) Obtener los posibles órdenes de los subcuerpos de  $\mathbb{F}_{64}$ .

### 16.10 Ejercicios diversos

- 1 Hallar el menor entero positivo que representa a un elemento primitivo de  $\mathbb{Z}_{31}$ .
- 2 Demostrar que  $x^4 + x^3 + x^2 + x + 1$  es irreducible en  $\mathbb{Z}_2[x]$  pero no es primitivo.
- 3 Hallar todos los valores de  $b$  para los cuales  $x^2 + x + b$  es un polinomio primitivo de  $\mathbb{Z}_{17}[x]$ .
- 4 ¿Cuántos puntos contienen las "curvas" siguientes del plano afín sobre  $\mathbb{F}_3$ ?
  - (i)  $x^3 + y^3 = 1$ ;
  - (ii)  $x^2 + xy + y^2 = 0$ .
- 5 Un *triángulo* en un plano proyectivo es un conjunto de tres puntos que no pertenecen a una recta común. Demostrar que el número de triángulos del plano proyectivo sobre  $\mathbb{F}_q$  es  $\frac{1}{6}q^3(q+1)(q^2+q+1)$ .
- 6 Demostrar que  $x^2 + 1$  es irreducible en  $\mathbb{Z}_p[x]$  si, y sólo si,  $p \equiv 3 \pmod{4}$ .
- 7 Sea  $X$  el conjunto de las palabras de longitud  $n$  en el alfabeto  $\mathbb{Z}_2$ , salvo la palabra nula  $00\dots 0$ . Se define la suma  $x + y$  de dos palabras  $x$  e  $y$  como la

palabra cuyo dígito  $i$ -ésimo es la suma (en  $\mathbf{Z}_2$ ) de los dígitos  $i$ -ésimos de  $x$  y de  $y$ . Demostrar que el conjunto  $B$  de los 3-subconjuntos de  $X$  de la forma  $\{x, y, x+y\}$  es un 2-diseño de parámetros  $(2^n - 1, 3, 1)$ .

8 Sea  $b$  un elemento primitivo de  $\mathbf{F}_q$  y, para cada entero positivo  $n$  tal que  $b^n \neq -1$ , defínase  $J(n)$  mediante la ecuación  $b^n + 1 = b^{J(n)}$ . Construir una tabla de  $J(n)$  para los cuerpos  $\mathbf{F}_9$  y  $\mathbf{F}_{13}$  (respecto de elementos primitivos adecuados).

9 Demostrar que si  $J(n)$  es como en el ejercicio anterior, siempre que  $J(n-m)$  esté definido se tiene

$$b^m + b^n = b^{m+J(n-m)}.$$

( $J(n)$  es el logaritmo de Jacobi. Es un instrumento útil para calcular en cuerpos finitos.)

10 El grafo de incidencia de un plano proyectivo es el grafo bipartito  $G = (V \cup W, E)$ , donde  $V$  es el conjunto de puntos,  $W$  el de rectas y  $vw$  es una arista siempre que el punto  $v$  pertenezca a la recta  $w$ . Demostrar que el grafo de incidencia es un grafo regular de cintura 6 que tiene el mínimo número de vértices compatible con estas propiedades (comparar con el ejercicio 8.8.20.)

11 Sean  $p_1, p_2, \dots, p_k$  primos congruentes con 1 módulo 4 y sea  $q$  un divisor primo de  $4(p_1 p_2 \cdots p_k)^2 + 1$ . Demostrar que  $-1$  es un cuadrado en  $\mathbf{Z}_q$  y deducir que existen infinitos primos congruentes con 1 módulo 4.

12 Se dice que un polinomio  $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  de grado par es recíproco si  $a_i = a_{n-i}$  ( $0 \leq i \leq \frac{1}{2}n$ ). Demostrar que un polinomio recíproco no puede ser primitivo.

13 Demostrar que si 10 es un elemento primitivo del cuerpo  $\mathbf{Z}_p$ , las representaciones decimales de las fracciones  $r/p$  ( $1 \leq r \leq p-1$ ) son periódicas de periodo  $p-1$  y difieren únicamente en permutaciones cíclicas.

14 Para cada potencia  $q$  de un primo, sea  $\square$  el complementario de  $\square$  en  $\mathbf{F}_q$ . Demostrar que si  $q = 4n+3$ , entonces  $\square$  es un conjunto diferencia con parámetros  $(4n+3, 2n+2, n+1)$ .

15 Utilizando el método esbozado al final del apartado 16.8, demostrar que un 2-diseño con parámetros  $(4n+3, 2n+1, n)$  puede extenderse a un 3-diseño con parámetros  $(4n+4, 2n+2, n)$ .

16 R.A. Fisher, pionero en el uso de diseños y cuadrados latinos en la investigación agrícola, propuso el siguiente problema.

En un grupo de dieciséis personas, cuatro son inglesas, cuatro escocesas, cuatro irlandesas y cuatro galesas. Hay cuatro de 35 años, cuatro de 45, cuatro de 55 y cuatro de 65. Cuatro son abogados, cuatro doctores, cuatro soldados y cuatro clérigos. Cuatro son solteros, cuatro casados, cuatro viudos y cuatro divorciados. Finalmente, cuatro son conservadores, cuatro socialistas, cuatro liberales y cuatro

fascistas. No hay del mismo tipo en una categoría que sean iguales en otra categoría. Tres de los fascistas son: un abogado inglés soltero de 65 años, un soldado escocés casado de 55 y un doctor irlandés viudo de 45. Además, el socialista irlandés tiene 35 años, el escocés conservador 45 y el clérigo inglés 55. ¿Qué puede decirse del abogado galés?

17 Supongamos dado un 3-diseño con parámetros  $(10, 4, 1)$ . Demostrar que si quitamos los bloques que no contienen un objeto dado  $x$  y eliminamos  $x$  de los bloques restantes, el resultado es un 2-diseño con parámetros  $(9, 3, 1)$ . Utilizar esta construcción a la inversa para obtener un 3-diseño a partir del plano afín sobre  $\mathbf{F}_3$ .

18 Demostrar que si  $F$  es un cuerpo cuyo grupo multiplicativo es cíclico, entonces  $|F|$  ha de ser finito.

19 Demostrar que todo polinomio cuadrático de  $\mathbf{Z}_p[x]$  puede escribirse como el producto de dos polinomios lineales a coeficientes en  $\mathbf{F}_{p^2}$ .

20 Construir una representación explícita de  $\mathbf{F}_{16}$  y determinar todos sus subcuerpos.

## 17 Códigos correctores de errores

### 17.1 Palabras, códigos y errores

Al enviar un mensaje télex a gran distancia, puede haber alguna interferencia y el mensaje puede no recibirse exactamente tal como fue enviado. En estas circunstancias hemos de ser capaces de detectar errores y, si es posible, corregirlos. El lenguaje corriente proporciona facilidades para esto, ya que algunas secuencias de letras no tienen sentido. Así pues, si recibimos el mensaje TE QUIERP, podemos estar seguros de que se ha producido un error y no será difícil corregirlo. Pero las propiedades de detección y corrección de errores del lenguaje corriente no son uniformes: si el mensaje recibido es TE QUIERO, no podemos saber con certeza si el mensaje es correcto.

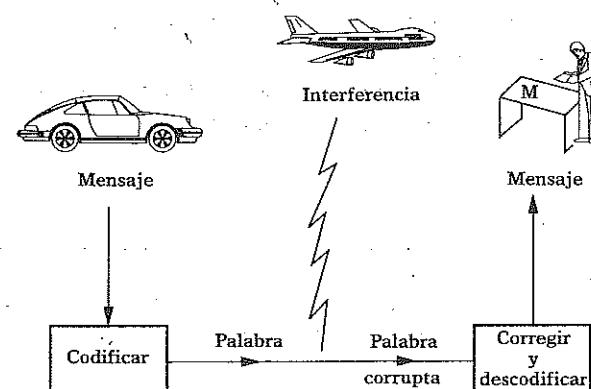


Fig. 17.1 El proceso de codificación ideal.

Un enfoque más sistemático es representar los mensajes mediante palabras escogidas del alfabeto binario  $\{0, 1\}$ , ya que de este modo un error no es más que la confusión entre un 0 y un 1. Las palabras binarias escogidas corresponden a los mensajes reales según un conjunto de reglas preestablecido que conocen tanto el emisor como el receptor. En una situación ideal, el proceso funcionaría como en la figura 17.1.

El emisor codifica el mensaje seleccionando la palabra binaria que le ha sido asignada; después se transmite a través del canal y, debido a las interferencias, el mensaje se corrompe. Una vez recibido, se corrigen los errores del mensaje corrupto y el receptor descodifica la versión correcta utilizando las mismas reglas que se utilizaron en la traducción del mensaje original. Nótese que este tipo de proceso de codificación no pretende la confidencialidad; al contrario, el objetivo es reconstruir exactamente el mensaje recibido, aunque haya sido alterado en la transmisión.

Es conveniente utilizar palabras de la misma longitud en todos los casos. Hay  $2^n$  palabras binarias de longitud  $n$  y denotaremos el conjunto de todas ellas por  $V^n$ . Por ejemplo,

$$V^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}.$$

Cada uno de los símbolos de una palabra es un bit (una contracción, en inglés, de "binary digit", dígito binario). Un código binario de longitud  $n$  no es más que un subconjunto  $C$  de  $V^n$  y los elementos de  $C$  son las palabras del código. Cualquier subconjunto vale, pero en la práctica elegiremos aquellos  $C$  que tengan propiedades adecuadas para la detección, y si es posible corrección, de errores.

Supongamos, por ejemplo, que los mensajes que queremos ser capaces de enviar son *arriba*, *abajo*, *izquierda*, *derecha*. Podríamos usar cualquiera de los siguientes códigos.

Código	Longitud	arriba	abajo	izquierda	derecha
$C_1$	2	00	10	01	11
$C_2$	3	000	110	011	101
$C_3$	6	000000	111000	001110	110011

El código  $C_1$  es muy económico, pero no tiene ninguna capacidad de corregir errores. Si se envía la palabra 00 y ocurre un error en el primer bit

de la transmisión, la palabra recibida será 10. Esta es también una palabra del código, con lo que el receptor será incapaz de detectar el error.

El código  $C_2$  es mejor, ya que es capaz de *detectar* un error individual. Si se altera un bit de una palabra cualquiera (el 0 se transforma en 1, o el 1 en 0), la palabra resultante ya no es del código y el receptor sabrá que se ha producido un error. Pero no hay forma razonable de *corregir* el error. Ya que si enviamos 000 y se produce un error en el primer bit, la palabra recibida 100 también podría igualmente ser el resultado de un error en el segundo bit de la palabra 101 (figura 17.2). En términos prácticos, la detección de errores sin posibilidad de corrección es útil sólo si el receptor puede solicitar la repetición de un mensaje en el que se haya detectado algún error.

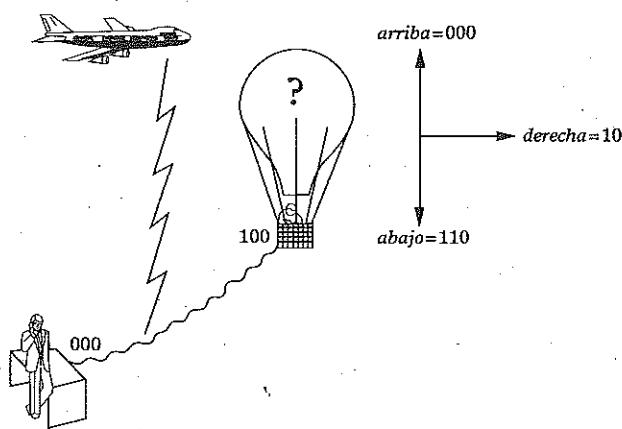


Fig. 17.2 La detección de errores no es suficiente.

Es evidente que el código  $C_3$  requiere más esfuerzo que los demás, pero puede detectar y corregir algunos errores. En concreto, si suponemos que se ha producido un único error en la transmisión de alguna palabra, es posible decidir qué palabra se ha emitido. Por ejemplo, si recibimos 110000, la única palabra del código que puede obtenerse modificando un solo bit es 111000. Por supuesto, es posible que haya errores en dos o más bits, pero la probabilidad de que esto ocurra en la práctica es mucho menor que la de un solo error.

Ha llegado el momento de formalizar las ideas introducidas hasta ahora. Usaremos símbolos vectoriales  $a, b, c, \dots$ , para las palabras de  $V^n$  y

definiremos la **distancia**  $\delta(a, b)$  como el número de bits en que difieren  $a$  y  $b$ . Por ejemplo,

$$\begin{aligned}\delta(1101, 1000) &= 2, \\ \delta(\overline{1}01\overline{0}101, \overline{1}10\overline{0}100) &= 3.\end{aligned}$$

La distancia  $\delta$  posee tres propiedades sencillas:

- (i)  $\delta(x, y) = 0 \iff x = y$ ,
- (ii)  $\delta(x, y) = \delta(y, x)$ ,
- (iii)  $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$ .

Sólo la tercera requiere algún esfuerzo (ejercicio 17.1.4).

Dado un código  $C$ , denotaremos por  $\delta$  la **distancia mínima** entre pares de palabras distintas de  $C$ :

$$\delta = \min\{\delta(a, b) \mid a, b \in C, a \neq b\}.$$

Para los códigos  $C_1$ ,  $C_2$  y  $C_3$  anteriores,  $\delta$  es 1, 2 y 3, respectivamente.

La distancia entre dos palabras mide el número de errores que han de ocurrir para que una se transforme en otra. Así pues, si la distancia mínima de un código es  $\delta$  y no se producen más de  $\delta - 1$  errores en la transmisión, el receptor será capaz de reconocer que la palabra recibida no es del código. Si se producen  $\delta$  errores, la palabra emitida puede convertirse en otra palabra del código. En consecuencia, podemos decir que un código de distancia mínima  $\delta$  puede detectar con seguridad hasta  $\delta - 1$  errores (y en algunos casos más).

En el contexto actual, estamos más interesados en la corrección de errores. Las ideas esbozadas en la discusión del código  $C_3$  sugieren que, si se recibe una palabra errónea, debiéramos suponer que la palabra del código enviada es la más cercana (en el sentido de la distancia  $\delta$ ). Esto se conoce como el principio de descodificación del **vecino más próximo**: se resume diciendo que si  $r < s$ , es más probable que se hayan producido  $r$  errores que  $s$  errores. El siguiente teorema establece la relación entre  $\delta$  y el número de errores que pueden corregirse utilizando este principio.

**Teorema 17.1.** *Un código  $C$  puede corregir  $e$  errores con el principio del vecino más próximo si la distancia mínima cumple*

$$\delta \geq 2e + 1.$$

**DEMOSTRACIÓN:** Supongamos que se envía una palabra  $c$  del código  $y$ , habiéndose producido  $e$  errores en la transmisión, se recibe la palabra  $z$ . Por definición de  $\delta$ , tenemos que  $\delta(c, z) = e$ .

Sea  $c'$  otra palabra del código. Entonces, por la propiedad (iii) de  $\delta$ , la definición de  $\delta$  y la hipótesis,

$$\begin{aligned}\delta(c, z) + \delta(z, c') &\geq \delta(c, c') \\ &\geq \delta \\ &\geq 2e + 1.\end{aligned}$$

Resulta que  $e + \delta(z, c') \geq 2e + 1$ , es decir,

$$\delta(z, c') \geq e + 1.$$

Vemos que  $c$  es la única palabra del código a distancia  $e$  de  $z$  y el principio del vecino más próximo da la solución correcta.  $\square$

### Ejercicios 17.1

1 Hallar la distancia mínima  $\delta$  de cada uno de los siguientes códigos.

- (i)  $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$  en  $V^4$ ;
- (ii)  $\{10000, 01010, 00001\}$  en  $V^5$ ;
- (iii)  $\{000000, 101010, 010101\}$  en  $V^6$ .

Determinar en cada caso el número de errores que pueden ser detectados y corregidos.

2 ¿Cuál de los códigos del ejercicio 1 puede extenderse mediante la inclusión de una palabra adicional sin modificar  $\delta$ ?

3 Construir un código  $C$  en  $V^6$  que codifique cinco mensajes y corrija un error.

4 Demostrar la "desigualdad triangular"

$$\delta(x, y) \leq \delta(x, z) + \delta(z, y),$$

donde  $x, y$  y  $z$  son palabras de  $V^n$ .

### 17.2 Códigos lineales

El conjunto  $V^n$  de todas las palabras binarias de longitud  $n$  puede equiparse con una estructura algebraica de varias maneras. La más sencilla es hacer de  $V^n$  un grupo definiendo  $x + y$  como la palabra que se obtiene sumando los correspondientes bits de  $x$  e  $y$  módulo 2. Por ejemplo,

$$1011001 + 1000111 = 0011110.$$

Es fácil comprobar que con esta definición de la suma,  $V^n$  se convierte en un grupo. Como grupo no es más que  $(Z_2)^n$ , el producto directo de  $n$  copias de  $Z_2$ .

**Definición.** Un código  $C$  en  $V^n$  es **lineal** si  $a + b$  es de  $C$  siempre que lo sean  $a$  y  $b$ . Equivalentemente,  $C$  es lineal si, y sólo si, es un subgrupo de  $V^n$ .

Los códigos  $C_1$  y  $C_2$  discutidos en el apartado anterior son lineales; pero el código  $C_3$  no lo es, ya que 111000 y 110011 son de  $C_3$  pero

$$111000 + 110011 = 001011$$

no lo es.

Del teorema de Lagrange se desprende que, al ser un subgrupo de  $V^n$ , el tamaño  $|C|$  de un código lineal es un divisor de  $|V^n| = 2^n$ . Así pues,  $|C|$  es un entero de la forma  $2^k$  con  $0 \leq k \leq n$ : el entero  $k$  es la **dimensión** de  $C$ .

Hasta el momento hemos definido tres parámetros (véase la tabla 17.2.1) que determinan la utilidad práctica de un código lineal.

Tabla 17.2.1

Nombre	Símbolo	Significado
Longitud	$n$	Las palabras son de $n$ bits.
Dimensión	$k$	Hay $2^k$ palabras disponibles.
Distancia mínima	$\delta$	Pueden corregirse hasta $e$ errores, siempre que $\delta \geq 2e + 1$ .

La relación entre estos parámetros es lo que hace de la teoría de la codificación un reto para los matemáticos. Para poder enviar un buen

número de mensajes sin demasiado esfuerzo, quisiéramos que  $k$  fuese razonablemente grande en relación a  $n$ . Pero si el código contiene muchas palabras, la distancia entre ellas será pequeña y podrán corregirse pocos errores.

**Ejemplo.** Sea  $C$  un código lineal de longitud  $n$  y dimensión  $k$ . Demostrar que si  $e$  es el máximo número de errores que puede corregir  $C$ , entonces

$$2^{n-k} \geq 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}.$$

Deducir que ningún código lineal de longitud 17 y dimensión 10 puede corregir más de un error.

**SOLUCIÓN:** Si  $c$  es una palabra de longitud  $n$ , el número de palabras que pueden obtenerse modificando  $r$  bits de  $c$  es  $\binom{n}{r}$ , ya que podemos elegir  $r$  entre  $n$  bits. Sea  $S_e(c)$  el conjunto de las palabras que pueden obtenerse modificando como máximo  $e$  bits de  $c$ , de forma que

$$|S_e(c)| = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}.$$

Si  $C$  corrige  $e$  errores, los conjuntos  $S_e(c)$  y  $S_e(c')$  han de ser disjuntos para cualesquiera palabras distintas  $c$  y  $c'$  de  $C$ . Por lo tanto,  $V^n$  contiene  $|C| = 2^k$  subconjuntos mutuamente disjuntos de tamaño  $|S_e(c)|$ , con lo que

$$2^n \geq 2^k \times |S_e(c)|$$

y ya tenemos el resultado.

Si  $n = 17$  y  $k = 10$ , tenemos que

$$1 + \binom{17}{1} + \binom{17}{2} = 1 + 17 + 136 = 154,$$

que es mayor que  $2^{17-10} = 128$  y, en consecuencia, no es posible corregir dos (o más) errores.  $\square$

Una ventaja importante de los códigos lineales es que la distancia mínima puede calcularse de un modo relativamente simple. Esto es debido

a que la distancia entre dos palabras no cambia si añadimos la misma palabra a ambas:

$$\partial(x + a, y + a) = \partial(x, y) \quad (x, y, a \in V^n).$$

En particular, si definimos el peso  $w(z)$  de una palabra  $z$  como el número de unos en  $z$ , tenemos que  $w(z) = \partial(z, 0)$  y

$$\begin{aligned} \partial(x, y) &= \partial(x - y, y - y) = \partial(x - y, 0) \\ &= w(x - y). \end{aligned}$$

Nótese que, al ser la suma módulo 2,  $x - y$  es lo mismo que  $x + y$ .

**Teorema 17.2.** Sea  $C$  un código lineal y sea  $w_{\min}$  el peso mínimo de las palabras de  $C$ , exceptuando 0. Entonces la distancia mínima de  $C$  viene dada por

$$\delta = w_{\min}.$$

**DEMOSTRACIÓN:** Sea  $c^*$  una palabra de  $C$  tal que  $w(c^*) = w_{\min}$ . Como  $c^*$  y 0 son palabras del código, tenemos que

$$\delta \leq \partial(c^*, 0) = w(c^*) = w_{\min}.$$

Por otra parte, si  $c^1$  y  $c^2$  son dos palabras a distancia mínima,  $c^1 - c^2$  también es de  $C$  (por ser lineal) y

$$\delta = \partial(c^1, c^2) = w(c^1 - c^2) \geq w_{\min}. \quad \square$$

El cálculo directo de  $\delta$  a partir de la definición requiere que hallemos las distancias entre cada par de palabras del código, mientras que el teorema 17.2 nos dice que es suficiente calcular el peso de cada palabra—una mejora considerable (ejercicio 17.2.5).

### Ejercicios 17.2

- Para cada  $n \geq 1$ , el código que contiene únicamente las dos palabras  $000\dots 0$  y  $111\dots 1$  de longitud  $n$  es lineal. ¿Qué valores toman  $k$  y  $\delta$ ?

- 2 Dada una palabra  $x$  de  $V^n$ , sea  $S_2(2)$  el conjunto de palabras que pueden obtenerse a partir de  $x$  cometiendo dos errores como máximo. Demostrar que

$$|S_2(x)| = \frac{1}{2}(n^2 + n + 2).$$

Deducir que si  $E$  es un código cualquiera (no necesariamente lineal) de longitud 8 que corrige dos errores, entonces  $|E| \leq 6$ .

- 3 ¿Cuál es la dimensión máxima de un código *lineal* de longitud 8 que corrija dos errores? Construir uno de ellos.

- 4 Sea  $C$  un código lineal. Demostrar que el subconjunto de  $C$  que contiene las palabras de peso par es también un código lineal. Deducir que las palabras de peso par son, o bien todas las de  $C$ , o la mitad exactamente de ellas.

- 5 Sea  $C$  un código con  $m$  palabras y definamos una "operación" como el cálculo del peso de una palabra. Demostrar que el número de operaciones necesarias para hallar la distancia entre cada par de palabras de  $C$  es  $O(m^2)$ . Si  $C$  es lineal, explicar cómo hallar la distancia mínima de  $C$  mediante un método que requiera  $O(m)$  operaciones únicamente.

### 17.3 Construcción de códigos lineales

Sea  $H$  una matriz binaria de  $n$  columnas y sea  $x'$  la palabra  $x$  de  $V^n$  considerada como vector columna. En particular,  $0'$  denota el vector columna formado por ceros. Si  $a$  y  $b$  son palabras tales que

$$Ha' = Hb' = 0',$$

entonces  $a + b$  tiene la misma propiedad, ya que

$$H(a + b)' = Ha' + Hb' = 0'.$$

En otras palabras, el conjunto  $C$  definido por

$$C = \{x \in V^n \mid Hx' = 0'\}$$

es un código lineal. La matriz  $H$  se conoce habitualmente como una **matriz de comprobación de la paridad**, aunque nosotros abreviaremos y la llamaremos **matriz de paridad**.

**Ejemplo.** Hallar las palabras del código determinado por la matriz de paridad

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

**SOLUCIÓN:** El código contiene todas las palabras binarias  $x_1x_2x_3x_4$  que cumplen

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

es decir,

$$x_1 + x_3 = 0, \quad x_2 + x_3 + x_4 = 0.$$

Si recordamos que la aritmética se lleva a cabo en  $\mathbb{Z}_2$ , podemos reescribir las ecuaciones como

$$x_1 = x_3, \quad x_2 = x_3 + x_4.$$

Si asignamos valores a  $x_3$  y  $x_4$ , entonces  $x_1$  y  $x_2$  quedan determinados. Hay cuatro maneras de elegir  $x_3$  y  $x_4$  (00, 10, 01 y 11), que dan lugar a las palabras

$$0000, \quad 1110, \quad 0101, \quad 1011. \quad \square$$

El método descrito en el ejemplo nos permite construir códigos en  $V^n$  de cualquier dimensión. Tomamos una matriz binaria  $H$  de la forma

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & b_{11} & b_{12} & \cdots & b_{1,n-r} \\ 0 & 1 & 0 & \cdots & b_{21} & b_{22} & \cdots & b_{2,n-r} \\ \vdots & & & & & & & \\ 0 & 0 & \cdots & 1 & b_{r1} & b_{r2} & \cdots & b_{r,n-r} \end{pmatrix},$$

en la que hay  $r$  filas y  $n$  columnas. Una palabra  $x_1x_2\dots x_n$  definida por la matriz de paridad  $H$  satisface las ecuaciones

$$x_1 = b_{11}x_{r+1} + b_{12}x_{r+2} + \cdots + b_{1,n-r}x_n$$

$$x_2 = b_{21}x_{r+1} + b_{22}x_{r+2} + \cdots + b_{2,n-r}x_n$$

$$\vdots$$

$$x_r = b_{r1}x_{r+1} + b_{r2}x_{r+2} + \cdots + b_{r,n-r}x_n$$

y estas ecuaciones determinan  $x_1, x_2, \dots, x_r$  si damos valores a  $x_{r+1}, x_{r+2}, \dots, x_n$ . Hay  $2^{n-r}$  maneras de elegir estos últimos valores, de modo que obtenemos un código de dimensión  $k = n - r$ .

Desde un punto de vista teórico, el orden de las columnas de  $H$  no es importante, ya que una reordenación de las columnas corresponde a una reordenación de los bits de las palabras del código. Por lo tanto, podemos tomar  $H$  en la forma descrita anteriormente y diremos que  $H$  está en *forma estándar*.

### Ejercicios 17.3

- 1 Hallar todas las palabras del código lineal asociado a la matriz de paridad

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

- 2 ¿Qué valor tienen los parámetros  $n$ ,  $k$  y  $\delta$  del código construido en el ejercicio 1?

- 3 Queremos ser capaces de enviar 128 mensajes diferentes y cada mensaje ha de representarse como una palabra binaria de longitud 11. Explicar cómo construir un código lineal para este propósito. ¿Es posible construirlo con la propiedad adicional de que  $\delta \geq 3$ , de modo que pueda corregirse un error?

- 4 El profesor McBrain ha decidido que se le asigne un "número de identidad" en forma de palabra binaria a cada estudiante de matemáticas de la Universidad de Folornia.

(i) Si hay 53 estudiantes, hallar la dimensión mínima de un código *lineal* para este propósito (se supone que algunas palabras quedarán sin asignar).

(ii) Si el código ha de permitir la detección de un error, hallar la mínima longitud posible.

(iii) Hallar una matriz de paridad de un código que cumpla las condiciones enunciadas en (i) y (ii). ¿Tiene el código resultante la propiedad de corrección de errores exigida?

### 17.4 Corrección de errores en códigos lineales

Hay una manera muy sencilla de comprobar si el código lineal definido por una matriz de paridad corregirá al menos un error.

**Teorema 17.4.** Si  $H$  no contiene ninguna columna de ceros y no hay dos columnas iguales, el código  $C$  definido por la matriz  $H$  es capaz de corregir un error.

**DEMOSTRACIÓN:** Segundo el teorema 17.1 hemos de demostrar que  $\delta \geq 3$  y, por el teorema 17.2, esto es equivalente a  $w_{\min} \geq 3$ .

Supongamos que  $C$  contiene una palabra  $a$  con  $w(a) = 1$ . Entonces  $a$  tiene un único bit igual a 1: supongamos que es el bit en la posición  $i$ . Como los bits restantes son todos 0,  $Ha'$  es igual a la  $i$ -ésima columna  $h^{(i)}$  de  $H$  y la condición  $Ha' = 0'$  significa que  $h^{(i)}$  está formada enteramente por ceros, contrariamente a la hipótesis. Por lo tanto,  $C$  no contiene palabras de peso 1.

Supongamos que  $C$  contiene una palabra  $b$  con  $w(b) = 2$ , de forma que  $b$  tiene unos en las posiciones  $i$  y  $j$ . Entonces

$$Hb' = h^{(i)} + h^{(j)},$$

con lo que  $Hb' = 0'$  implica que  $h^{(i)} = h^{(j)}$ , contrariamente a la hipótesis. Hemos demostrado que  $C$  no contiene palabras de peso 2 y que  $w_{\min} \geq 3$ .  $\square$

**Ejemplo.** (i) Sea  $r$  un entero positivo. ¿Cuál es el máximo número posible de columnas en una matriz binaria con  $r$  filas que satisface las condiciones del teorema 17.4?

(ii) Calcular una matriz de este tipo si  $r = 3$  y hallar el código correspondiente.

(iii) Hallar los parámetros  $n$ ,  $k$  y  $\delta$  del código para cualquier valor de  $r$ .

**SOLUCIÓN:** (i) cada columna de la matriz tiene  $r$  elementos y cada uno de ellos es 0 o 1. El número de columnas distintas es  $2^r$  y, como una de ellas no está permitida (la columna 0), el número máximo es  $2^r - 1$ .

(ii) Una forma natural de hallar la matriz es hacer que las columnas correspondan a las representaciones binarias de los enteros  $1, 2, \dots, 7$  en

orden, es decir,

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

De esta forma aseguramos que cada una de las 7 posibles columnas aparezca sólo una vez. Nótese que si reordenamos las columnas de forma que las 4, 2 y 1 queden colocadas en las tres primeras posiciones, tenemos la *forma estándar* discutida en el apartado anterior. Sin embargo, es perfectamente posible trabajar con la matriz anterior y nos proponemos hacerlo.

Las ecuaciones que resultan de  $Hx' = 0'$  son

$$\begin{aligned} x_4 &= x_5 + x_6 + x_7, \\ x_2 &= x_3 + x_6 + x_7, \\ x_1 &= x_3 + x_5 + x_7. \end{aligned}$$

Dados  $x_3, x_5, x_6, x_7$ , los restantes  $x_1, x_2, x_4$  quedan determinados. El código contiene  $2^4 = 16$  palabras, que pueden obtenerse como en la tabla 17.4.1

Tabla 17.4.1

$x_3$	$x_5$	$x_6$	$x_7$	$x_1$	$x_2$	$x_4$	$\mathbf{x}$	$w(\mathbf{x})$
0	0	0	0	0	0	0	00000000	0
0	0	0	1	1	1	1	11000001	4
0	0	1	0	0	1	1	01100010	3
0	0	1	1	1	0	0	10100011	3
0	1	0	0	1	0	1	01001100	3
0	1	0	1	0	1	0	01101101	3
0	1	1	0	1	1	0	00101110	4
0	1	1	1	0	0	1	11001111	4
1	0	0	0	1	1	0	11100000	3
1	0	0	1	0	0	1	00110010	3
1	0	1	0	1	0	1	10110010	4
1	0	1	1	0	1	0	01110011	4
1	1	0	0	0	1	1	11110000	4
1	1	0	1	1	0	0	10110001	4
1	1	1	0	0	0	0	00110011	3
1	1	1	1	1	1	1	11111111	7

(iii) En la parte (i) demostramos que  $n = 2^r - 1$ . Para cada palabra del código, los  $r$  bits  $x_1, x_2, x_4, \dots, x_{2^r-1}$  están determinados por los restantes  $2^r - 1 - r$  bits, tal como vimos en (ii). La dimensión es, pues,  $k = 2^r - 1 - r$ .

El teorema 17.4 nos dice que  $\delta \geq 3$ . De hecho, la palabra 11100...0 es del código para todo  $r \geq 2$  (¿por qué?) y tiene peso 3, de modo que  $\delta = 3$ .

□

Los códigos del ejemplo anterior se conocen como **códigos de Hamming** (en honor de R.W. Hamming). Tienen como parámetros

$$n = 2^r - 1, \quad k = 2^r - 1 - r, \quad \delta = 3$$

y, puesto que  $\delta = 3$ , pueden corregir un error. De hecho, los códigos de Hamming son los mejores códigos con esta propiedad, en el sentido de que tienen el máximo número de palabras. Para demostrarlo, sea  $C$  un código de longitud  $n$  con  $\delta = 3$ . El conjunto de palabras que pueden obtenerse a partir de una palabra  $c$  con un sólo error es  $S_1(c)$  —siguiendo la notación del apartado 17.2— y tenemos que  $|S_1(c)| = n + 1$ . Como  $\delta = 3$ , los conjuntos  $S_1(c)$  no se solapan y, como el número total de palabras es  $2^n$ , debe ser

$$|C| \times (n + 1) \leq 2^n.$$

Si  $C$  es un código de Hamming, entonces  $|C| = 2^k$ , donde  $k = 2^r - 1 - r$ , y  $n + 1 = 2^r$ , de modo que se tiene una igualdad y  $|C|$  alcanza el máximo.

El razonamiento del párrafo anterior es un caso especial del estudiado en el ejemplo del apartado 17.2. Si fijamos el número de errores corregidos, un argumento de carácter general proporciona una cota similar para  $|C|$ . Los códigos que alcanzan esta cota se dice que son **perfectos**; desgraciadamente, son muy escasos.

El teorema 17.4 es un resultado teórico. Nos dice que si  $H$  cumple ciertas condiciones sencillas, el código asociado  $|C|$  será capaz de corregir un error usando el principio del vecino más próximo. En la práctica nos gustaría saber cómo corregir el error sin tener que comparar la palabra recibida con todas las palabras del código. Por fortuna, es posible hacerlo de manera sencilla.

Supongamos que se envía una palabra del código  $c$  y que se comete un error en el bit  $i$ -ésimo. La palabra recibida es

$$\mathbf{z} = \mathbf{c} + \mathbf{e}_i$$

donde  $\mathbf{e}$  es la palabra que tiene todos los bits a 0, salvo el  $i$ -ésimo que es 1. Por lo tanto,

$$H\mathbf{z}' = H(\mathbf{c} + \mathbf{e})' = H\mathbf{c}' + H\mathbf{e}'.$$

Como  $\mathbf{c}$  es del código, tenemos que  $H\mathbf{c}' = \mathbf{0}'$  y  $H\mathbf{e}'$  es igual a  $\mathbf{h}^{(i)}$ , la columna  $i$ -ésima de  $H$ . Resumiendo, el siguiente procedimiento detecta y corrige errores aislados del código  $C$ .

- (i) Si  $\mathbf{z}$  es la palabra recibida, calcular  $H\mathbf{z}'$ .
- (ii) Si  $H\mathbf{z}' = \mathbf{0}'$ , entonces  $\mathbf{z}$  es del código.
- (iii) Si  $H\mathbf{z}' \neq \mathbf{0}'$ , hallar la columna  $\mathbf{h}^{(i)}$  de  $H$  tal que  $H\mathbf{z}' = \mathbf{h}^{(i)}$  y cambiar el  $i$ -ésimo bit de  $\mathbf{z}$ .

Supongamos, por ejemplo, que usamos el código que tiene la matriz de paridad dada en el ejercicio 17.3.1 y que recibimos la palabra  $\mathbf{z} = 1110111$ . Calculamos

$$H\mathbf{z}' = [1010]',$$

vemos que es la primera columna de  $H$  y deducimos que se ha producido un error en el primer bit y que la palabra enviada es 0110111.

Los códigos de Hamming proporcionan una aplicación especialmente pulida del principio de corrección de errores que acabamos de describir. Si la matriz de paridad de un código de Hamming viene dada en la forma estándar, la columna  $\mathbf{h}^{(i)}$  no es más que la representación binaria de  $i$ . De modo que si la palabra recibida  $\mathbf{z}$  contiene un error, entonces  $H\mathbf{z}'$  es la representación binaria de la posición  $i$  donde se ha producido el error. Por ejemplo, supongamos que recibimos la palabra  $\mathbf{z} = 0111010$  en el código de Hamming de longitud 7 descrito en el ejemplo. Entonces

$$H\mathbf{z}' = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

y como 011 es la representación binaria de 3, tendremos que corregir el tercer bit. La palabra correcta es, pues, 0101010.

### Ejercicios 17.4

- 1 Sea  $C$  el código lineal definido por la matriz de paridad

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Si recibimos la palabra 110110 y sólo se ha producido un error, ¿qué palabra se ha enviado en realidad?

- 2 Calcular una matriz de comprobación para el código de Hamming de longitud 15. ¿Cuántas palabras tiene el código? Si suponemos que las columnas de la matriz se han escrito en el orden natural, como en la parte (ii) del ejemplo, ¿cuáles de las siguientes son palabras del código?

011010110111000

1000000000000011

110110110111111

Corregir aquellas palabras que no son del código suponiendo que se ha cometido sólo un error.

- 3 Queremos ser capaces de enviar 256 mensajes mediante un código lineal que corrija un error.

- (i) ¿Cuál es la mínima longitud posible del código?
- (ii) Obtener una matriz de paridad adecuada.
- (iii) Si han de corregirse dos errores, hallar una cota inferior para la longitud del código.

- 4 Demostrar mediante razonamientos aritméticos que no puede existir un código perfecto de longitud  $n$  que corrija  $e$  errores en los casos

- (i)  $n = 5, e = 1$ ;
- (ii)  $n = 10, e = 2$ .

### 17.5 Códigos cíclicos

En este apartado denotaremos los bits de una palabra a de longitud  $n$  mediante  $a_0a_1a_2\dots a_{n-1}$ . El motivo de esta curiosa elección se explicará en breve.

Se dice que un código  $C$  es cíclico si es lineal y si

$$a_0a_1a_2 \dots a_{n-1} \in C \Rightarrow a_{n-1}a_0a_1 \dots a_{n-2} \in C.$$

La palabra  $\hat{a} = a_{n-1}a_0a_1 \dots a_{n-2}$  es el primer desplazamiento cíclico de  $a$ . Si  $C$  es cíclico, las palabras que se obtienen de  $a$  mediante un número cualquiera de desplazamientos cílicos, tales como

$$a_i a_{i+1} \dots a_{n-1} a_0 \dots a_{i-1},$$

también son de  $C$ . Por ejemplo, El código

$$C_2 = \{000, 110, 011, 101\}$$

discutido en el apartado 17.1 es cíclico.

Los códigos cílicos son útiles por dos razones. En el lado práctico, pueden realizarse mediante mecanismos sencillos conocidos como registros de desplazamiento. Ésta es una cuestión importante, pero no es adecuado entrar en los detalles en un libro como el nuestro.

En el lado teórico, que sí nos concierne, los códigos cílicos pueden construirse e investigarse por medio de la teoría algebraica de los anillos de polinomios.

La clave del tratamiento algebraico de los códigos cílicos es la correspondencia entre

la palabra  $a = a_0a_1 \dots a_{n-1}$  en  $V^n$

y

el polinomio  $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  en  $\mathbb{Z}_2[x]$

En esta correspondencia, el primer desplazamiento cíclico  $\hat{a}$  de  $a$  se representa por el polinomio  $\hat{a}(x)$ , donde

$$\begin{aligned}\hat{a}(x) &= a_{n-1} + a_0x + \dots + a_{n-2}x^{n-1} \\ &= x(a_0 + a_1x + \dots + a_{n-1}x^{n-1}) - a_{n-1}(x^n - 1) \\ &= xa(x) - a_{n-1}(x^n - 1).\end{aligned}$$

Como los coeficientes pertenecen a  $\mathbb{Z}_2$ , podríamos sustituir todas las restas por sumas, pero conservaremos los signos  $-$  para una mayor claridad. El

resultado del cálculo puede expresarse diciendo que  $\hat{a}(x)$  es igual a  $xa(x)$  módulo  $x^n - 1$ .

En el apartado 16.3 vimos cómo, dado un polinomio  $f(x)$ , la suma y producto módulo  $f(x)$  puede interpretarse formalmente como la suma y producto de clases de equivalencia de polinomios. Las clases de equivalencia forman un anillo y, si  $f(x)$  es irreducible, tenemos incluso un cuerpo. En este caso el polinomio  $f(x)$  es  $x^n - 1$ , que no es irreducible salvo en el caso trivial  $n = 1$ . De hecho, la factorización de  $x^n - 1$  jugará un papel importante en la teoría subsecuente.

Denotaremos por  $V^n[x]$  el anillo de polinomios módulo  $x^n - 1$  con coeficientes en  $\mathbb{Z}_2$ . Trabajar módulo  $x^n - 1$  es lo mismo que sustituir  $x^n$  por 1,  $x^{n+1}$  por  $x$ ,  $x^{n+2}$  por  $x^2$ , etc., de donde se sigue claramente que cada clase de polinomios módulo  $x^n - 1$  tiene un único representante de grado menor que  $n$ . Utilizaremos siempre este representante para denotar la clase de equivalencia, ya que de esta forma la correspondencia entre palabras de  $V^n$  y clases de  $V^n[x]$  es del todo evidente. Por ejemplo, en  $V^6$ ,

$$110101 \text{ se representa por } 1 + x + x^3 + x^5,$$

$$010110 \text{ se representa por } x + x^3 + x^4,$$

donde los polinomios son en realidad clases de  $V^6[x]$ . En resumen, tenemos una correspondencia biyectiva entre  $V^n$  y  $V^n[x]$  tal que, si  $a(x)$  y  $b(x)$  corresponden a  $a$  y  $b$ ,  $a(x) + b(x)$  corresponde a  $a + b$  y  $xa(x)$  corresponde al primer desplazamiento cíclico  $\hat{a}$ .

En el teorema 17.5 demostraremos que un código cíclico de  $V^n$  corresponde a un tipo particular de subconjunto de  $V^n[x]$ . Los algebraistas estudian este tipo de subconjuntos por diversos motivos y les dan un nombre especial.

**Definición.** Sea  $R$  un anillo con un producto comutativo. Se dice que un subconjunto  $S$  de  $R$  es un ideal si

- (i)  $a, b \in S \Rightarrow a + b \in S$
- (ii)  $r \in R$  y  $a \in S \Rightarrow ra \in S$ .

En otras palabras,  $S$  es cerrado respecto de la suma y respecto del producto por cualquier elemento de  $R$ .

**Teorema 17.5.** Un código de  $V^n$  es cíclico si, y sólo si, corresponde a un ideal de  $V^n[x]$ .

**DEMOSTRACIÓN:** Sea  $C$  un código cíclico representado por un subconjunto de  $V^n[x]$ . Como  $C$  es lineal, si  $a(x)$  y  $b(x)$  son de  $C$ , también lo es  $a(x) + b(x)$  y se cumple la primera condición para ser un ideal. Como  $xa(x)$  representa el primer desplazamiento cíclico de  $a(x)$ , tenemos que  $xa(x)$  es de  $C$  siempre que lo sea  $a(x)$ . Repitiendo el mismo razonamiento,  $x^i a(x)$  es de  $C$  siempre que lo sea  $a(x)$ , para todo  $i \geq 0$ . Todo polinomio  $p(x)$  es suma de potencias  $x^i$  y, como  $C$  es lineal,  $p(x)a(x)$  es de  $C$ . Por lo tanto,  $C$  es un ideal.

Recíprocamente, si  $C$  es un ideal, la condición (i) nos dice que representa un código lineal, mientras que la condición (ii) nos dice (en particular) que  $xa(x)$  es de  $C$  siempre que lo sea  $a(x)$ , de modo que  $C$  es cíclico.  $\square$

El teorema implica que la construcción de códigos cíclicos de longitud  $n$  es equivalente a la construcción de ideales en  $V^n[x]$ . Esto no es únicamente una sofistificación matemática como pudiera parecer a primera vista, ya que existe una manera simple de construir ideales. De hecho, en el siguiente apartado veremos que esta manera sencilla es esencialmente la única.

Sea  $f(x)$  un polinomio de  $Z_2[x]$  con  $\text{gr } f(x) < n$ , de forma que  $f(x)$  es la representación natural de una clase de  $V^n[x]$ . Es evidente que el conjunto de todos los múltiplos de  $f(x)$  en  $V^n[x]$  es un ideal, ya que si  $a(x)$  y  $b(x)$  son múltiplos de  $f(x)$ , también lo son  $a(x) + b(x)$  y  $p(x)a(x)$  para cualquier  $p(x)$ . Denotaremos este ideal por  $\langle f(x) \rangle$  y nos referiremos a él como el ideal generado por  $f(x)$ .

Por ejemplo, sea

$$f(x) = 1 + x^2 \quad \text{en } V^3[x].$$

Tabla 17.5.1

$p(x)$	$p(x)f(x) \bmod (x^3 - 1)$	Palabra		
0	0	0	0	0
1	$1 + x^2$	1	0	1
$x$	$1 + x$	1	1	0
$1 + x$	$x + x^2$	0	1	1
$x^2$	$x + x^2$	0	1	1
$1 + x^2$	$1 + x$	1	1	0
$x + x^2$	$1 + x^2$	1	0	1
$1 + x + x^2$	0	0	0	0

Multiplicando  $f(x)$  sucesivamente por todos los  $p(x)$  de  $V^3[x]$  (y acordándonos de reducir módulo  $x^3 - 1$ ) se obtiene la tabla 17.5.1. Así pues, el ideal  $\langle 1 + x^2 \rangle$  tiene exactamente cuatro elementos

$$0, 1 + x, x + x^2, 1 + x^2$$

y el código correspondiente en  $V^3$  es el código  $C_2$  del apartado 17.1:

$$C_2 = \{000, 110, 011, 101\}.$$

### Ejercicios 17.5

- 1 ¿Cuáles de los siguientes códigos son cíclicos?
  - $\{000, 100, 010\}$ ;
  - $\{000, 100, 010, 001\}$ ;
  - $\{000, 111\}$ ;
  - $\{0000, 1010, 0101, 1111\}$ .
- 2 Calcular las palabras del código cíclico correspondiente al ideal  $\langle 1 + x + x^2 \rangle$  de  $V^3[x]$  y hallar una matriz de paridad para este código.
- 3 Demostrar que el ideal  $\langle 1 + x \rangle$  de  $V^5[x]$  corresponde al código de  $V^5$  formado por todas las palabras de peso par. ¿Sigue siendo cierto si en lugar de 5 tomamos un entero cualquiera  $n \geq 2$ ?

### 17.6 Clasificación y propiedades de los códigos cíclicos

El siguiente teorema justifica la afirmación de que cualquier código cíclico puede obtenerse por el método esbozado al final del apartado anterior.

**Teorema 17.6.1.** *Sea  $C$  un código cíclico (un ideal) de  $V^n[x]$ . Existe un polinomio  $g(x)$  de  $C$  tal que*

$$C = \langle g(x) \rangle.$$

**DEMOSTRACIÓN:** Si  $C$  es el código trivial formado únicamente por el polinomio cero, entonces  $C = \langle 0 \rangle$ . En caso contrario,  $C$  contiene un

polinomio no nulo  $g(x)$  de grado mínimo. Sea  $f(x)$  un elemento cualquiera de  $C$ ; el algoritmo de división (teorema 15.5) nos da

$$f(x) = b(x)g(x) + r(x),$$

donde  $\text{gr } r(x) < \text{gr } g(x)$  o bien  $r(x) = 0$  (recuérdese que el polinomio cero no tiene grado). Al ser  $f(x)$  y  $g(x)$  ambos de  $C$  y ser  $C$  un ideal, tanto  $b(x)g(x)$  como

$$b(x)g(x) - f(x) = r(x)$$

son de  $C$ . A menos que  $r(x) = 0$ , esto contradice la definición de  $g(x)$  como un polinomio de grado mínimo en  $C$ . Por lo tanto,  $f(x) = b(x)g(x)$  y  $C = \langle g(x) \rangle$  tal como afirmábamos.  $\square$

El polinomio  $g(x)$  de la demostración está únicamente determinado por la propiedad de ser el de menor grado de  $C$ . Ya que si tanto  $g_1(x)$  como  $g_2(x)$  tuvieran esta propiedad, tendrían el mismo grado y sus coeficientes dominantes serían iguales a 1 (como los coeficientes son de  $\mathbb{Z}_2$ , los únicos coeficientes posibles son 0 y 1). Como  $C$  es un ideal,  $g_1(x) - g_2(x)$  sería también de  $C$  y, si no fuera cero, su grado sería estrictamente menor que el de  $g_1(x)$  y  $g_2(x)$ , contrariamente a la hipótesis. En consecuencia,  $g_1(x) = g_2(x)$ .

En el ejemplo al final del apartado anterior dimos una lista con los elementos del ideal de  $V^3[x]$  generado por  $1 + x^2$ . Si observamos la lista veremos que en este caso el único polinomio no nulo de grado mínimo es  $1 + x$  y el teorema 17.6.1 nos dice que es un generador del ideal. En general, un código cíclico puede tener más de un generador, pero sólo uno de ellos tendrá grado mínimo. A este único polinomio con esta propiedad le llamaremos el **generador canónico** de  $C$ .

**Teorema 17.6.2.** El generador canónico  $g(x)$  de un código cíclico  $C$  de  $V^n[x]$  es un divisor de  $x^n - 1$  en  $\mathbb{Z}_2[x]$ .

**DEMOSTRACIÓN:** Utilizamos de nuevo el algoritmo de división en  $\mathbb{Z}_2[x]$  y tendremos que existen polinomios  $h(x)$  y  $s(x)$  tales que

$$x^n - 1 = g(x)h(x) + s(x)$$

con  $\text{gr } s(x) < \text{gr } g(x)$  o  $s(x) = 0$ . Esta ecuación implica que  $s(x) = g(x)h(x)$  en el anillo de polinomios  $V^n[x]$  módulo  $x^n - 1$ . Como  $C$  es el

ideal de  $V^n[x]$  generado por  $g(x)$ , resulta que  $s(x)$  es de  $C$ . Esto contradice el hecho de que  $g(x)$  sea de grado mínimo en  $C$ , a menos que  $s(x) = 0$ . Por lo tanto

$$x^n - 1 = g(x)h(x) \quad \text{en } \mathbb{Z}_2[x]$$

y queda demostrado el resultado.  $\square$

Volviendo de nuevo al ejemplo en  $V^3[x]$ , comprobamos que el generador canónico divide a  $x^3 - 1$ :

$$x^3 - 1 = (1 + x)(1 + x + x^2) \quad \text{en } \mathbb{Z}_2[x].$$

Los teoremas 17.6.1 y 17.6.2 no son sólo aplicaciones elegantes de la teoría de los anillos de polinomios. Veremos a continuación que, dado un generador canónico  $g(x)$  de  $C$ , podemos determinar fácilmente la dimensión y una matriz de paridad de  $C$ .

Sea  $x^n - 1 = g(x)h(x)$  en  $\mathbb{Z}_2[x]$ , donde

$$g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}, \quad h(x) = h_0 + h_1x + \cdots + h_kx^k.$$

Vale la pena observar que los coeficientes "extremos"  $g_0, h_0, g_{n-k}$  y  $h_k$  han de ser todos 1, ya que el producto de los polinomios es  $x^n - 1$ . El polinomio  $g(x)$  corresponde a la palabra

$$\mathbf{g} = g_0g_1 \cdots g_{n-k}00 \cdots 0$$

de  $V^n$  y los polinomios  $x^i g(x)$  ( $1 \leq i \leq k-1$ ) corresponden a los desplazamientos cíclicos de  $\mathbf{g}$ , es decir, las palabras

$$\mathbf{g}_{(i)} = 00 \cdots 0g_0g_1 \cdots g_{n-k}00 \cdots 0,$$

donde hay  $i$  ceros al principio y  $k-1-i$  ceros al final. Utilizaremos la notación especial  $\vec{\mathbf{h}}$  para la palabra cuyos primeros  $k+1$  bits son los coeficientes de  $h(x)$  en orden inverso, seguidos de  $n-k-1$  ceros:

$$\vec{\mathbf{h}} = h_k h_{k-1} \cdots h_0 00 \cdots 0.$$

Denotaremos por  $H$  la matriz  $(n-k) \times n$  que tiene por filas  $\vec{\mathbf{h}}$  y los  $n-k-1$  primeros desplazamientos cíclicos de  $\vec{\mathbf{h}}$ , es decir,

$$H = \begin{pmatrix} h_k & \cdots & h_0 & 0 & \cdots \\ 0 & h_k & \cdots & h_0 & 0 & \cdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & 0 & h_k & \cdots & h_0 \end{pmatrix}$$

**Teorema 17.6.3.** La matriz  $H$  es una matriz de paridad del código cíclico  $C = \langle g(x) \rangle$  y la dimensión de  $C$  es  $k$ .

**DEMOSTRACIÓN:** Sea  $c(x) = f(x)g(x)$  un elemento cualquiera de  $C$  con

$$f(x) = f_0 + f_1x + \cdots + f_{n-1}x^{n-1}.$$

Desarrollando el producto se tiene que

$$c(x) = f_0g(x) + f_1xg(x) + \cdots + f_{n-1}x^{n-1}g(x),$$

con lo que la palabra  $c$  correspondiente a  $c(x)$  viene dada por

$$c = f_0g + f_1g(1) + \cdots + f_{n-1}g(n-1).$$

Para demostrar que  $H$  es una matriz de paridad de  $C$  (es decir,  $Hc' = 0'$ ) es suficiente ver que  $Hg'_{(i)} = 0'$  para  $0 \leq i \leq n-1$ .

Si igualamos coeficientes en el producto  $g(x)h(x) = x^n - 1$ , se obtienen las ecuaciones

$$\begin{aligned} g_0h_1 + g_1h_0 &= 0 && \text{(coeficiente de } x\text{)}, \\ g_0h_2 + g_1h_1 + g_2h_0 &= 0 && \text{(coeficiente de } x^2\text{)}, \\ &\vdots \\ g_{n-k-1}h_k + g_{n-k}h_{k-1} &= 0 && \text{(coeficiente de } x^{n-1}\text{)}. \end{aligned}$$

Por otra parte, como los coeficientes de  $1$  y  $x^n$  son ambos iguales a  $1$ , tenemos que

$$g_0h_0 + g_{n-k}h_k = 0.$$

Si recordamos que  $g_{n-k+1}, \dots, g_{n-1}$  y  $h_{k+1}, \dots, h_{n-1}$  son todos cero, las  $n$  ecuaciones pueden escribirse como

$$h_kg_{n-k+j} + h_{k-1}g_{n-k+j+1} + \cdots + h_0g_{n+j} = 0$$

para  $j = 0, 1, \dots, n-1$  y los subíndices tomados módulo  $n$ . Para valores adecuados de  $j$ , el miembro izquierdo de la ecuación es la expresión que aparece al evaluar  $Hg'_{(i)}$ . Por lo tanto,  $Hg'_{(i)} = 0'$  como se afirmaba.

Finalmente, sea  $y = y_0y_1 \cdots y_{n-1}$  de  $C$ . La primera ecuación que resulta de  $Hy' = 0'$  es

$$y_K = h_ky_0 + h_{k-1}y_1 + \cdots + h_1y_{k-1},$$

ya que  $h_0 = 1$ . Por lo tanto, los valores de  $y_0, y_1, \dots, y_{k-1}$  determinan el valor de  $y_k$ . La siguiente ecuación determina  $y_{k+1}$  en términos de  $y_0, y_1, \dots, y_k$ , y así sucesivamente. Hay  $2^k$  valores posibles de  $y_0, y_1, \dots, y_{k-1}$ , de donde  $|C| = 2^k$ .  $\square$

La teoría precedente indica que para describir los códigos cíclicos de longitud  $n$  hemos de hallar los factores de  $x^n - 1$  en  $\mathbb{Z}_2[x]$ . Por ejemplo, si  $n = 7$  la factorización de  $x^7 - 1$  en polinomios irreducibles es

$$x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3).$$

(Esta factorización está relacionada con los resultados del apartado 16.9: al ser  $8 = 2^3$ , el conjunto de factores irreducibles de  $x^8 - x$  en  $\mathbb{Z}_2[x]$  ha de consistir en todos los polinomios mónicos irreducibles cuyo grado divida a 3). La ecuación muestra que  $x^7 - 1$  tiene exactamente ocho divisores en  $\mathbb{Z}_2[x]$ ; son los divisores triviales  $1$  y  $x^7 - 1$  juntamente con

$$\begin{array}{lll} 1+x, & 1+x+x^3, & 1+x^2+x^3, \\ (1+x)(1+x+x^3), & (1+x)(1+x^2+x^3), & (1+x+x^3)(1+x^2+x^3). \end{array}$$

Cada uno de los divisores genera un código cíclico y los teoremas 17.6.1 y 17.6.2 nos aseguran que son los únicos códigos cíclicos de longitud 7. Es evidente que  $\langle 1 \rangle$  es el código que contiene todas las palabras y  $\langle x^7 - 1 \rangle = \langle 0 \rangle$  es el código que consta de la única palabra  $0'$ . Los restantes tienen más interés. En particular, sea  $C$  el código que tiene  $g(x) = 1+x+x^3$  como generador canónico, de forma que, en la notación anterior,

$$h(x) = (1+x)(1+x^2+x^3) = 1+x+x^2+x^4.$$

El teorema 17.6.3 indica que la dimensión de  $C$  es 4 y que una matriz de paridad de  $C$  es

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Puede comprobarse que las columnas de esta matriz son las mismas que las del código de Hamming de longitud 7 (ejemplo del apartado 17.4) pero en diferente orden. El código  $C$  es, esencialmente, igual al código de Hamming.

El lector atento habrá observado que no hemos dicho nada acerca de la distancia mínima  $\delta$  de un código cíclico en general. Para ciertas clases de códigos cíclicos es posible obtener resultados extremadamente útiles acerca de  $\delta$ ; estos resultados, junto con los teoremas obtenidos en este apartado, significan que tales códigos son importantes en la teoría y en la práctica. Pero estas cuestiones pertenecen a un curso de teoría de códigos que, esperemoslo, atraerá al lector una vez acabado este libro.

### Ejercicios 17.6

1 Hallar los factores irreducibles de  $x^5 - 1$  en  $\mathbb{Z}_2[x]$  y determinar todos los códigos cíclicos de longitud 5 (hay cuatro, todos ellos más bien triviales).

2 Describir todos los códigos cíclicos de longitud 7.

3 La factorización de  $x^{15} - 1$  en polinomios irreducibles en  $\mathbb{Z}_2[x]$  es

$$x^{15} - 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4) \times (1+x+x^2+x^3+x^4).$$

(i) Explicar la relación con los resultados del apartado 16.9.

(ii) ¿Cuántos códigos cíclicos hay de longitud 15?

(iii) Hallar un generador canónico de un código cíclico equivalente al código de Hamming de longitud 15.

4 Utilizar los resultados del apartado 16.9 para hallar el número de factores irreducibles de  $x^32 - x$  en  $\mathbb{Z}_2[x]$  y determinar el número de códigos cíclicos de longitud 31. Hallar un generador canónico de un código cíclico equivalente al código de Hamming de longitud 31.

### 17.7 Ejercicios diversos

1 Calcular los parámetros  $(n, k, \delta)$  del código lineal que tiene por matriz de paridad

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

2 Decidir si las siguientes palabras son o no del código definido en el ejercicio 1 y corregir aquellas que no lo sean, suponiendo que se ha cometido un solo error.

(i) 11111, (ii) 01101, (iii) 01100.

¿Cuántas palabras, en total, no pueden corregirse cambiando sólo un bit?

3 Sea  $C$  un código de peso mínimo  $\delta = 3$ . Demostrar que existe una palabra  $x$  tal que

$$\partial(x, c_1) = 1, \quad \partial(x, c_2) = 2,$$

paa ciertas palabras  $c_1$  y  $c_2$  de  $C$ . ¿Qué decisión puede tomarse si recibimos  $x$ ?

4 Calcular la matriz de paridad del código lineal formado por todas las palabras de longitud 7 de peso par.

5 Utilizando el método del apartado 17.2, demostrar que no existe ningún código  $C$  en  $V^5$  que tenga distancia mínima  $\delta = 3$  y  $|C| = 6$ .

6 Demostrar, con un análisis completo de posibilidades, que el resultado del ejercicio anterior sigue siendo cierto si sustituimos la condición  $|C| = 6$  por  $|C| = 5$ .

7 ¿Para cuáles de los siguientes valores de  $(n, k, \delta)$  es posible que exista un código lineal que los tenga como parámetros?

- (i) (12, 7, 5), (ii) (11, 4, 5)

8 Sea  $C$  un código lineal de longitud  $n$  y dimensión  $k$ , y sea  $i$  un entero  $1 \leq i \leq n$ . Demostrar que

$$C_0 = \{c \in C \mid c_i = 0\}$$

es un código lineal de dimensión  $k - 1$ .

9 Demostrar con un razonamiento aritmético que un código  $C$  de longitud  $n = 6$  y distancia mínima  $\delta = 3$  ha de cumplir  $|C| \leq 9$ . Comprobar que no existe ningún código con  $|C| = 9$  y construir uno con  $|C| = 8$ .

10 Sea  $C$  un código binario de longitud  $n$  capaz de corregir dos errores y además perfecto. Demostrar que

- (i)  $n^2 + n + 2$  es una potencia de 2;  
(ii) existe un único valor  $n \leq 10$  que cumple la condición (i);  
(iii) existe un código  $C$  con las propiedades exigidas y el valor de  $n$  obtenido en (ii), pero es trivial.

Calcular el siguiente valor de  $n$  para el que se cumple (i) (desgraciadamente, puede demostrarse que no existe ningún código en este caso, ni para cualquier otro valor de  $n$ ).

11 Obtener una condición análoga a (i) del ejercicio anterior para un código perfecto que corrija tres errores y demostrar que la condición se cumple para  $n = 7$  y  $n = 23$  (en el siguiente ejercicio demostraremos que cuando  $n = 23$  existe un código no trivial).

12 Demostrar que el polinomio  $x^{23} - 1$  puede escribirse como  $(x - 1)f(x)g(x)$  en  $\mathbf{Z}_2[x]$ , donde  $f(x)$  y  $g(x)$  son polinomios de grado 11. Demostrar que el código cíclico generado por  $f(x)$  (o por  $g(x)$ ) es un código perfecto capaz de corregir tres errores.

13 Sean  $C_1$  y  $C_2$  códigos cíclicos de longitud  $n$  con generadores  $g_1(x)$  y  $g_2(x)$ , respectivamente. Demostrar que

$$C_1 + C_2 = \{x \in V^n \mid x = c_1 + c_2 \text{ para ciertos } c_1 \in C_1, c_2 \in C_2\}$$

es un código cíclico con generador  $\text{mcd}(g_1(x), g_2(x))$ .

14 Demostrar que los códigos de Hamming son cíclicos.

15 Demostrar que si un código cíclico contiene una palabra de peso impar, entonces contiene la palabra  $111\cdots 1$ .

16 Sean  $B_1, B_2, \dots, B_7$  los bloques de un sistema de Steiner triple con siete modelos  $1, 2, \dots, 7$ . Definimos un conjunto  $C$  de siete palabras  $w^{(1)}, w^{(2)}, \dots, w^{(7)}$  en  $V^7$  mediante

$$w_j^{(i)} = \begin{cases} 1 & \text{si } j \in B_i, \\ 0 & \text{en otro caso.} \end{cases}$$

Demostrar que  $C$  es un código con distancia mínima 3.

17 Sea  $C$  el código construido mediante el método del ejercicio anterior, pero usando un plano proyectivo  $\mathbf{F}_q$  en lugar de un sistema de Steiner triple. ¿Cuál es la distancia mínima de  $C$ ?

18 Sea  $S$  el conjunto de las palabras de peso 3 de un código de Hamming de longitud  $2^r - 1$ . Para cada  $w$  de  $S$  se define un subconjunto  $B$  de  $\{1, 2, \dots, 2^r - 1\}$  mediante la regla

$$i \in B \iff w_i = 1.$$

Demostrar que los conjuntos  $B$  son los bloques de un sistema de Steiner triple.

## 18 Funciones generadoras

### 18.1 Series de potencias y sus propiedades algebraicas

En el capítulo 15 se observó que un polinomio no es más que una sucesión de coeficientes. Las sucesiones correspondientes tienen la propiedad de tener sólo un número finito de términos; más exactamente, sólo tienen un número finito de términos no nulos. Sin embargo, pocas de las sucesiones que se encuentran en la práctica comparten esta propiedad y para poder estudiarlas algebraicamente introduciremos una generalización del concepto de polinomio.

El objeto que corresponde a una sucesión infinita  $(a_n)$ , de la misma manera que un polinomio corresponde a una sucesión finita, es una serie de potencias  $A(x)$ , y se escribe

$$A(x) = a_0 + a_1x + a_2x^2 + \dots$$

Al igual que con los polinomios, no nos preocuparemos del significado del símbolo  $x$  y de sus potencias; su función no es más que la de señalar la posición de los coeficientes.

Las series de potencias pueden sumarse y multiplicarse exactamente como los polinomios. Si tenemos

$$A(x) = a_0 + a_1x + a_2x^2 + \dots, \quad B(x) = b_0 + b_1x + b_2x^2 + \dots,$$

entonces

$$A(x) + B(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots,$$

$$A(x)B(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots.$$

En otras palabras, si  $C(x) = A(x) + B(x)$  y  $D(x) = A(x)B(x)$ , entonces los coeficientes  $c_i$  y  $d_i$  de  $C(x)$  y  $D(x)$  vienen dados, respectivamente, por las ecuaciones

$$c_i = a_i + b_i, \quad d_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 \quad (i \geq 0).$$

Con estas definiciones, las series de potencias con coeficientes en un anillo conmutativo  $R$  son elementos de otro anillo conmutativo, denotado por  $R[[x]]$ . Comprobar los axiomas de anillo es tan trivial (e igualmente tedioso) como en el anillo de polinomios  $R[x]$ . Señalemos que  $R[x]$  es un subconjunto de  $R[[x]]$  y forma un anillo con las mismas operaciones algebraicas; por este motivo se dice que  $R[x]$  es un **subanillo** de  $R[[x]]$ .

De aquí en adelante, supondremos con frecuencia que los coeficientes de nuestros polinomios y series de potencias pertenecen a un cuerpo  $F$ . Tanto  $F[x]$  como  $F[[x]]$  son anillos, y no cuerpos, pero  $F[[x]]$  se parece más a un cuerpo que  $F[x]$ , ya que tiene muchos más elementos inversibles. Recordemos (ejercicio 15.5.4) que un polinomio es inversible en  $F[x]$  sólo en el caso trivial en que es una constante no nula. La situación en  $F[[x]]$  es mucho más prometedora.

**Teorema 18.1.** Si  $F$  es un cuerpo, la serie de potencias

$$B(x) = b_0 + b_1x + b_2x^2 + \cdots,$$

es inversible en  $F[[x]]$  si, y sólo si,  $b_0 \neq 0$ .

**DEMOSTRACIÓN:** Si  $B(x)$  es inversible existe una serie de potencias  $U(x)$  tal que  $B(x)U(x) = 1$ , es decir,

$$(b_0 + b_1x + b_2x^2 + \cdots)(u_0 + u_1x + u_2x^2 + \cdots) = 1.$$

Igualando los coeficientes del término constante se obtiene  $b_0u_0 = 1$ , de forma que  $b_0 \neq 0$ .

Recíprocamente, supongamos que  $b_0 \neq 0$ . Para determinar  $U(x)$  debemos considerar las ecuaciones que se obtienen a partir de la fórmula del producto:

$$b_0u_0 = 1,$$

$$b_0u_1 + b_1u_0 = 0,$$

$$b_0u_2 + b_1u_1 + b_2u_0 = 0,$$

...

Al ser  $b_0 \neq 0$ , existe  $b_0^{-1}$  y podemos determinar la sucesión  $(u_n)$  recursivamente:

$$u_0 = b_0^{-1},$$

$$u_1 = b_0^{-1}(-b_1u_0),$$

$$u_2 = b_0^{-1}(-b_1u_1 - b_2u_0),$$

Así pues,  $B(x)$  es inversible.  $\square$

Naturalmente, escribiremos  $B(x)^{-1}$  para designar el inverso de  $B(x)$ : la demostración del teorema prueba que está únicamente determinado.

El hecho de que tantas series de potencias tengan inverso en  $F[[x]]$  es la base de los métodos que se discuten en la parte final del libro. La mayor parte de las veces  $B(x)$  será un polinomio, pero su inverso  $B(x)^{-1}$  será una serie de potencias en lugar de un polinomio.

**Ejemplo.** Demostrar que el inverso de  $1 - x$  es la serie de potencias

$$1 + x + x^2 + \cdots$$

**SOLUCIÓN:** La serie  $1 - x$  tiene término constante igual a 1 y tiene, por lo tanto, un inverso  $U(x)$ . Como en la demostración del teorema 18.1, deducimos de  $(1 - x)(u_0 + u_1x + u_2x^2 + \cdots) = 1$  las siguientes ecuaciones:

$$u_0 = 1,$$

$$u_1 - u_0 = 0,$$

$$u_2 - u_1 = 0,$$

...

Por lo tanto,  $u_0 = u_1 = u_2 = \cdots = 1$  y tenemos que

$$(1 - x)^{-1} = 1 + x + x^2 + \cdots. \quad \square$$

En la práctica acostumbraremos a usar la notación según la cual

$$B(x)^{-1} \text{ se escribe } \frac{1}{B(x)},$$

$$A(x)B(x)^{-1} \text{ se escribe } \frac{A(x)}{B(x)}.$$

Hay que recordar, sin embargo, que  $A(x)/B(x)$  no es más que el producto de las series de potencias  $A(x)$  y  $B(x)^{-1}$ . Ocurrirá a menudo que  $A(x)$  y  $B(x)$  serán polinomios, aunque por supuesto  $B(x)^{-1}$  no lo será. En este caso podemos calcular los coeficientes de  $Q(x) = A(x)/B(x)$  resolviendo las ecuaciones que se derivan de la ecuación  $B(x)Q(x) = A(x)$ , es decir,

$$(b_0 + b_1x + \dots + b_mx^m)(q_0 + q_1x + q_2x^2 + \dots) \\ = (a_0 + a_1x + \dots + a_nx^n).$$

De hecho, éste es el método tradicional para dividir  $A(x)$  entre  $B(x)$ , pero empezando por los términos constantes.

Por ejemplo, para hallar la serie de potencias de

$$\frac{1+3x}{1-2x+x^2},$$

procedemos de la siguiente forma

$$\begin{array}{r} 1+3x \\ \hline 1-2x+x^2 \end{array} \left| \begin{array}{r} 1-2x+x^2 \\ 1+5x+9x^2+13x^3+\dots \\ \hline 5x-x^2 \\ 5x-10x^2+5x^3 \\ \hline 9x^2-5x^3 \\ 9x^2-18x^3+9x^4 \\ \hline 13x^3-9x^4 \\ 13x^3-26x^4+13x^5 \\ \hline 17x^4-13x^5\dots \end{array} \right.$$

En este ejemplo es sencillo pronosticar una fórmula general para los coeficientes, pero éste no será siempre el caso.

### Ejercicios 18.1

1 Hallar los cuatro primeros términos en las series de potencias de

$$(i) \frac{1+4x}{1+5x+x^2}, \quad (ii) \frac{2+6x+x^2}{3+x+5x^2+x^3}.$$

(Puede suponerse que los coeficientes pertenecen al cuerpo  $\mathbf{R}$  de los números reales.)

2 Demostrar que el inverso de  $1+x$  en  $\mathbf{R}[[x]]$  es

$$(1+x)^{-1} = 1 - x + x^2 - x^3 + \dots,$$

es decir, el coeficiente de  $x^n$  es  $(-1)^n$ .

3 Demostrar, mediante la división de polinomios, que el inverso de  $1+x+x^2$  en  $\mathbf{Z}_2[[x]]$  es

$$(1+x+x^2)^{-1} = 1 + x + x^3 + x^4 + x^6 + x^7 + \dots$$

Conjeturar una regla para los coeficientes y demostrarla.

4 ¿Cuál es el inverso de  $1+x^2$  en  $\mathbf{Z}_2[[x]]$ ? ¿Y en  $\mathbf{Z}_3[[x]]$ ?

### 18.2 Fracciones simples

En este apartado iniciamos la tarea de hallar un método alternativo para calcular los coeficientes de la serie de potencias de  $a(x)/b(x)$ , donde  $a(x)$  y  $b(x)$  son polinomios con  $b_0 \neq 0$ . Aunque el método algorítmico de la división es adecuado para muchos propósitos, no proporciona una fórmula general para los coeficientes, fórmula que en ocasiones es deseable.

La clave del problema es la descomposición de  $a(x)/b(x)$  en *fracciones simples*, una técnica que quizás sea conocida del lector. Aproximadamente es ésta: si tenemos una factorización  $b(x) = s(x)t(x)$ , donde  $s(x)$  y  $t(x)$  no tienen factores en común no triviales, entonces podemos obtener una relación

$$\frac{a(x)}{b(x)} = \frac{f(x)}{s(x)} + \frac{g(x)}{t(x)}$$

para ciertos polinomios  $f(x)$  y  $g(x)$ . Por ejemplo, el polinomio  $2-3x+x^2$  es igual a  $(1-x)(2-x)$  y se tiene la igualdad

$$\frac{5-3x}{2-3x+x^2} = \frac{2}{1-x} + \frac{1}{2-x}.$$

Hay que insistir en que todas las "fracciones" que aparecen en tales ecuaciones son de hecho series de potencias, aunque en la práctica la

notación fraccionaria es conveniente y no da lugar a problemas. Nótese también que podemos limitarnos al caso en que el grado de  $a(x)$  sea estrictamente menor que el de  $b(x)$ , ya que se tiene

$$a(x) = b(x)q(x) + r(x),$$

donde  $r(x)$  es igual a cero o bien  $\text{gr } r(x) < \text{gr } b(x)$  y, en consecuencia,

$$\frac{a(x)}{b(x)} = q(x) + \frac{r(x)}{b(x)}.$$

El problema queda reducido entonces a hallar las fracciones simples de  $r(x)/b(x)$ . Por ejemplo,

$$\begin{aligned} \frac{7 - 2x - 5x^2 + 2x^3}{2 - 3x + x^2} &= \frac{(1 + 2x)(2 - 3x + x^2) + (5 - 3x)}{2 - 3x + x^2} \\ &= (1 + 2x) + \frac{2}{1 - x} + \frac{1}{2 - x}. \end{aligned}$$

Pasamos a enunciar con precisión el resultado que proporciona la descomposición en fracciones simples.

**Teorema 18.2.** Sea  $F$  un cuerpo y sean  $a(x)$  y  $b(x)$  polinomios de  $F[x]$  tales que

- (i)  $\text{gr } a(x) < \text{gr } b(x)$ ,
- (ii)  $b(x) = s(x)t(x)$ , donde  $s(x)$  y  $t(x)$  no tienen factores comunes no triviales,
- (iii)  $b_0 \neq 0$ .

Entonces existen polinomios  $f(x)$  y  $g(x)$  tales que

$$\text{gr } f(x) < \text{gr } s(x), \quad \text{gr } g(x) < \text{gr } t(x)$$

y

$$\frac{a(x)}{b(x)} = \frac{f(x)}{s(x)} + \frac{g(x)}{t(x)};$$

esta última ecuación se cumple en el anillo  $F[[x]]$  de series de potencias con coeficientes en  $F$ .

**DEMOSTRACIÓN:** Nótese en primer lugar que  $s(x)$  y  $t(x)$  tienen inversos en  $F[[x]]$ , ya que la igualdad  $b_0 = s_0 t_0$  y la condición  $b_0 \neq 0$  implican que  $s_0 \neq 0$  y  $t_0 \neq 0$ .

Por una cuestión de conveniencia, en lo que resta de demostración prescindiremos de la variable  $x$  para denotar los polinomios. Como 1 es un mcd de  $t$  y  $s$ , el teorema 15.6 asegura que existen polinomios  $\lambda$  y  $\mu$  tales que

$$1 = \lambda t + \mu s.$$

Multiplicando por  $a$  y poniendo  $\bar{f} = a\lambda$  y  $\bar{g} = a\mu$ , se obtiene

$$a = \bar{f}t + \bar{g}s.$$

Para sustituir  $\bar{f}$  y  $\bar{g}$  por polinomios que cumplan la condición enunciada sobre los grados, se procede de la siguiente manera. Aplicando el algoritmo de la división tenemos que

$$\bar{f} = qs + f$$

con  $\text{gr } f < \text{gr } s$  (o bien  $f = 0$ ). Sustituyendo  $\bar{f}$  en la ecuación  $a = \bar{f}t + \bar{g}s$  llegamos a

$$a = ft + gs;$$

donde  $g = \bar{g} + qt$ . Sólo resta demostrar que  $\text{gr } g < \text{gr } t$ . Tenemos que

$$\text{gr } a < \text{gr } b, \quad \text{gr } ft < \text{gr } st = \text{gr } b$$

y, al ser  $gs = a - ft$ ,

$$\text{gr } gs = \text{gr}(a - ft) < \text{gr } b = \text{gr } st.$$

Así pues,  $\text{gr } g < \text{gr } t$ , como queríamos demostrar.

Si dividimos la ecuación  $a = ft + gs$  por  $b = st$ , se obtiene el resultado buscado. (Más exactamente, hay que multiplicar por el inverso de  $b$ ). □

Es fácil demostrar que los polinomios  $f(x)$  y  $g(x)$  que satisfacen la condición del teorema 18.2 son únicos.

Sea

$$b(x) = p_1(x)^{m_1} p_2(x)^{m_2} \cdots p_k(x)^{m_k}$$

la factorización de  $b(x)$  en polinomios irreducibles. Si  $\text{gr } a(x) < \text{gr } b(x)$ , aplicando el teorema 18.2 repetidamente se tiene que

$$\frac{a(x)}{b(x)} = \frac{h_1(x)}{p_1(x)^{m_1}} + \frac{h_2(x)}{p_2(x)^{m_2}} + \cdots + \frac{h_k(x)}{p_k(x)^{m_k}},$$

donde  $\text{gr } h_i(x) < \text{gr } p_i(x)^{m_i}$  ( $1 \leq i \leq k$ ). En particular, si todos los factores irreducibles son lineales, es decir,

$$b(x) = \beta(\alpha_1 - x)^{m_1}(\alpha_2 - x)^{m_2} \cdots (\alpha_k - x)^{m_k}$$

tenemos que

$$\frac{a(x)}{b(x)} = \frac{h_1(x)}{(\alpha_1 - x)^{m_1}} + \frac{h_2(x)}{(\alpha_2 - x)^{m_2}} + \cdots + \frac{h_k(x)}{(\alpha_k - x)^{m_k}},$$

donde  $\text{gr } h_i(x) < m_i$  ( $1 \leq i \leq k$ ).

Con frecuencia, pero no siempre, es útil dar un paso más en la descomposición. Consideremos una fracción típica

$$h(x)/(\alpha - x)^m \quad \text{con } \text{gr } h(x) < m.$$

Aplicando sucesivamente el algoritmo de división (como en el ejercicio 18.2.4), podemos determinar coeficientes  $\gamma_1, \gamma_2, \dots, \gamma_m$  tales que

$$h(x) = \gamma_m + \gamma_{m-1}(\alpha - x) + \cdots + \gamma_1(\alpha - x)^{m-1},$$

de donde

$$\frac{h(x)}{(\alpha - x)^m} = \frac{\gamma_1}{\alpha - x} + \frac{\gamma_2}{(\alpha - x)^2} + \cdots + \frac{\gamma_m}{(\alpha - x)^m}.$$

De esta manera se obtiene una expresión de  $a(x)/b(x)$  en la que el numerador de cada fracción simple es constante.

En la práctica, hay varias maneras de hallar las constantes. Una de ellas es reducir a común denominador e igualar los coeficientes de la ecuación resultante, tal como se muestra en el ejemplo siguiente.

**Ejemplo.** Hallar la descomposición en fracciones simples de

$$\frac{4 + x - x^2}{3 - 5x + x^2 + x^3}.$$

**SOLUCIÓN:** Tenemos la factorización

$$\begin{aligned} 3 - 5x + x^2 + x^3 &= (1 - x)(3 - 2x - x^2) \\ &= (1 - x)(1 - x)(3 + x). \end{aligned}$$

La descomposición en fracciones simples es de la forma

$$\frac{4 + x - x^2}{3 - 5x + x^2 + x^3} = \frac{A}{1 - x} + \frac{B}{(1 - x)^2} + \frac{C}{3 + x}.$$

Para determinar  $A, B$  y  $C$  multiplicamos ambos miembros por  $(1 - x)^2(x + 3)$  y obtenemos

$$4 + x - x^2 = A(1 - x)(3 + x) + B(3 + x) + C(1 - x)^2.$$

Igualando coeficientes de  $1, x$  y  $x^2$ , llegamos a

$$\begin{aligned} 4 &= 3A + 3B + C, \\ 1 &= -2A + B - 2C, \\ -1 &= -A + C; \end{aligned}$$

por lo tanto,  $A = \frac{1}{2}$ ,  $B = 1$  y  $C = -\frac{1}{2}$ .  $\square$

Hay ocasiones en que es más sencillo hallar los coeficientes sustituyendo valores de  $x$  en las ecuaciones. Por ejemplo, la sustitución  $x = -3$  en la ecuación anterior

$$4 + x - x^2 = A(1 - x)(3 + x) + B(3 + x) + C(1 - x)^2,$$

nos da

$$4 + (-3) - (-3)^2 = C(1 - (-3))^2$$

y  $C = -\frac{1}{2}$  como antes. Igualmente, la sustitución  $x = 1$  da  $B = 1$ . Este método es la justificación de la regla de "cubrir", una regla útil que puede formularse del siguiente modo.

Sea  $(x - \alpha)^r$  la máxima potencia de  $x - \alpha$  que divide a  $b(x)$ , de manera que

$$\frac{a(x)}{b(x)} = \frac{a(x)}{(x - \alpha)^r c(x)} = \frac{K}{(x - \alpha)^r} + P(x),$$

donde  $P(x)$  es la suma de las fracciones simples restantes. Entonces  $K$  es igual al valor que se obtiene “cubriendo” el factor  $(x - \alpha)^r$  en  $a(x)/b(x)$  y haciendo  $x = \alpha$  en lo que queda; es decir,  $K = a(\alpha)/c(\alpha)$ . Por ejemplo, la constante  $C$  en la descomposición de

$$\frac{4 + x - x^2}{(3 + x)(1 - x)^2}$$

se obtiene cubriendo el factor  $3 + x$  y haciendo  $x = -\alpha$  en lo que queda:

$$C = \frac{4 - (-3) + (-3)^2}{(1 - (-3))^2} = -\frac{1}{2}.$$

La regla de cubrir es muy útil, pero hay dos cosas a tener en cuenta. La primera es que sólo proporciona el numerador de la máxima potencia de un factor lineal y los restantes coeficientes han de hallarse de algún otro modo. Y en segundo lugar, sólo debiera usarse cuando los coeficientes se suponen reales o complejos, ya que la técnica de sustituir valores depende de la hipótesis de que el polinomio y la función polinómica correspondiente son intercambiables, y eso no es cierto si los coeficientes pertenecen a un cuerpo finito (apartado 15.8). En general se supone que trabajamos en el cuerpo  $\mathbf{C}$  de los números complejos, a menos que se mencione explícitamente otro cuerpo distinto. Un buen motivo para esta suposición es que todo polinomio de  $\mathbf{C}[x]$  puede descomponerse en factores lineales, de modo que siempre puede lograrse la descomposición completa de un “cociente” en fracciones simples con numeradores constantes.

### Ejercicios 18.2

1 Usar la regla de cubrir para hallar la descomposición en fracciones simples de

$$(i) \quad \frac{3 + 4x}{(1 - x)(2 + x)}; \quad (ii) \quad \frac{2 + x + x^2}{(1 + x)(2 + x)(3 + x)}.$$

2 Hallar la descomposición en fracciones simples de

$$(i) \quad \frac{1 + 3x}{1 - 3x^2 + 2x^3}; \quad (ii) \quad \frac{-5 + 3x}{6 - 11x + 6x^2 - x^3}.$$

3 Hallar la descomposición en fracciones simples sobre  $\mathbf{Z}_3$  de  $1/(1 + x^4)$  (usar la factorización obtenida en el apartado 15.8).

4 Sea  $h(x)$  un polinomio con  $\text{gr } h(x) < m$ . Demostrar que si definimos  $q_i(x)$  y  $\gamma_i$  ( $1 \leq i \leq m$ ) mediante

$$h(x) = (\alpha - x)q_1(x) + \gamma_m,$$

$$q_{i-1}(x) = (\alpha - x)q_i(x) + \gamma_{m-i+1} \quad (2 \leq i \leq m),$$

entonces

$$h(x) = \gamma_m + \gamma_{m-1}(\alpha - x) + \cdots + \gamma_1(\alpha - x)^{m-1}.$$

5 Hallar la descomposición de  $(1 - x^4)^{-1}$  en fracciones simples sobre el cuerpo complejo  $\mathbf{C}$ .

### 18.3 El teorema del binomio para exponentes negativos

El teorema del binomio que demostramos en el apartado 4.3 puede formularse como un resultado sobre productos de polinomios con coeficientes enteros en el anillo  $\mathbf{Z}[x]$ . En concreto, afirma que el coeficiente de  $x^n$  en el polinomio  $(1 + x)^k$  es el número binomial  $\binom{k}{n}$ , es decir,

$$(1 + x)^k = \binom{k}{0} + \binom{k}{1}x + \binom{k}{2}x^2 + \cdots + \binom{k}{n}x^n + \cdots + \binom{k}{k}x^k.$$

En este capítulo hemos aprendido a ver  $(1 + x)^{-1}$  como una serie de potencias con coeficientes enteros:

$$(1 + x)^{-1} = 1 - x + x^2 - x^3 + \cdots,$$

de modo que podemos definir  $(1 + x)^{-m}$  en el anillo  $\mathbf{Z}[[x]]$  como el producto de  $m$  factores iguales a  $(1 + x)^{-1}$ . Es evidente que esta definición es válida para todo entero  $m \geq 1$  y, naturalmente, quisiéramos una fórmula que nos diera el coeficiente de  $x^n$  en la serie de potencias resultante. Esta fórmula existe y resulta ser extremadamente sencilla.

**Teorema 18.3.** El coeficiente de  $x^n$  en la serie de potencias  $(1+x)^{-m}$  es igual a

$$(-1)^n \binom{m+n-1}{n}.$$

**DEMOSTRACIÓN:** Para evitar los signos negativos consideraremos  $(1-x)^{-m}$  en lugar de  $(1+x)^{-m}$ . Como

$$(1-x)^{-1} = 1 + x + x^2 + \dots,$$

$(1-x)^{-m}$  es el producto de  $m$  factores iguales a la serie de potencias  $1 + x + x^2 + \dots$ . Demostraremos que el coeficiente de  $x^n$  en el producto de estos  $m$  factores es igual al número de selecciones no ordenadas con repetición de  $n$  de los  $m$  factores.

Súpongamos que cada factor tiene una marca, situada inicialmente en el término 1, y que hacemos una selección no ordenada con repetición de tamaño  $n$  de los  $m$  factores. Cada vez que seleccionamos un factor particular, movemos la marca hasta el siguiente término, de modo que si el factor ha sido seleccionado  $i$  veces en total, la marca acabará en  $x^i$ . De esta forma, para cada una de las  $\binom{m+n-1}{n}$  selecciones posibles obtenemos un conjunto de términos marcados, uno de cada factor, con exponente total  $n$ . Al multiplicar los factores, cada uno de estos conjuntos contribuye en 1 al coeficiente de  $x^n$ ; este coeficiente es pues igual a  $\binom{m+n-1}{n}$ . Sustituyendo  $x$  por  $-x$  se obtiene el resultado.  $\square$

Por ejemplo, el coeficiente de  $x^n$  en la serie de potencias  $(1+x)^{-2}$  es

$$(-1)^n \binom{2+n-1}{n} = (-1)^n \binom{n+1}{n} = (-1)^n (n+1),$$

de forma que la serie de potencias es igual a

$$(1+x)^{-2} = 1 - 2x + 3x^2 - 4x^3 + \dots$$

Es posible combinar el teorema 18.3 con el teorema 4.3 del binomio para exponentes positivos en una sola fórmula. Dado un entero  $\alpha$  y un entero positivo  $n$  definimos

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-n+1)}{n!}$$

y también  $\binom{\alpha}{0} = 1$ . Esta extensión del significado de los números binomiales es correcta, ya que si  $\alpha$  es un entero positivo  $k$  se obtiene la fórmula para  $\binom{k}{n}$  del teorema 4.1.2. Si  $\alpha$  es un entero negativo  $-m$  tenemos

$$\begin{aligned} \binom{-m}{n} &= \frac{(-m)(-m-1)(-m-2)\cdots(-m-n+1)}{n!} \\ &= (-1)^n \frac{m(m+1)(m+2)\cdots(m+n-1)}{n!} \\ &= (-1)^n \binom{m+n-1}{n}. \end{aligned}$$

Con esta definición extendida de  $\binom{k}{n}$  para enteros  $k$  positivos y negativos, hemos demostrado que el coeficiente de  $x^n$  en  $(1+x)^k$  es  $\binom{k}{n}$ . Si incluimos el caso trivial  $(1+x)^0 = 1$ , tenemos la siguiente forma general del teorema del binomio para todos los enteros  $k$ :

$$(1+x)^k = \binom{k}{0} + \binom{k}{1}x + \binom{k}{2}x^2 + \cdots + \binom{k}{n}x^n + \cdots$$

La forma general es una serie de potencias, pero si  $k$  es positivo tenemos que

$$\binom{k}{n} = 0 \quad \text{siempre que } n > k$$

y la serie se reduce a un polinomio.

Existen varias extensiones triviales del teorema del binomio: fórmulas para  $(a+x)^k$ ,  $(a-x)^k$ , etc. En particular, haremos un uso considerable de la fórmula para  $(1-ax)^{-m}$ , que es

$$(1-ax)^{-m} = 1 + max + \cdots + \binom{m+n-1}{n} a^n x^n + \cdots$$

Hemos presentado el teorema del binomio como una regla para hallar los coeficientes de la serie de potencias  $(1+x)^k$ . Hay muchas series de potencias que, mediante manipulaciones algebraicas convenientes, pueden expresarse en función de la serie de potencias básica; el teorema del binomio puede usarse entonces para hallar fórmulas de sus coeficientes. Por ejemplo, en el apartado 18.1 obtuvimos la serie de potencias

$$\frac{1+3x}{1-2x+x^2} = 1 + 5x + 9x^2 + 13x^3 + \cdots$$

Si tenemos en cuenta que el denominador es  $(1-x)^2$ , se puede deducir una fórmula para el término general de la siguiente manera.

$$\begin{aligned}\frac{1+3x}{1-2x+x^2} &= (1+3x)(1-x)^{-2} \\ &= (1+3x)(1+2x+\dots+(n+1)x^n+\dots).\end{aligned}$$

El coeficiente de  $x^n$  en el producto es  $(n+1)+3n = 4n+1$ , lo cual coincide con lo que los primeros valores hacían prever.

En secciones posteriores de este capítulo podremos ver cómo la técnica de las fracciones simples nos permite reducir muchas series de potencias a formas en las que puede aplicarse el teorema del binomio.

### Ejercicios 18.3

1 Obtener (y simplificar siempre que sea posible) el coeficiente de

- (i)  $x^3$  en  $(1+2x)^7$ ,
- (ii)  $x^n$  en  $(1-x)^{-4}$ ,
- (iii)  $x^{2r}$  en  $(1-x)^{-r}$ .

2 Obtener los primeros cuatro términos y el término general de la serie de potencias  $(1-x)^{-3}$ .

3 Sea  $a_n$  el coeficiente de  $x^n$  en la serie de potencias  $(1-x-x^2)^{-1}$ . Demostrar que

$$a_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots + \binom{n-r}{r},$$

donde  $r$  es el mayor entero tal que  $0 \leq r \leq n-r$ .

4 ¿Cuál es el coeficiente de  $x^n$  en la serie de potencias

$$\frac{1+2x+2x^2}{1-3x+3x^2-x^3}?$$

5 Si definimos  $a_0, a_1, \dots, a_{6r}$  y  $b_0, b_1, \dots, b_{3r}$  mediante

$$(1-x+x^2)^{3r} = a_0 + a_1x + a_2x^2 + \dots + a_{6r}x^{6r},$$

$$(1+x)^{3r} = b_0 + b_1x + b_2x^2 + \dots + b_{3r}x^{3r},$$

demostrar que

$$\sum_{i=0}^{3r} a_i b_{3r-i} = \binom{3r}{r}.$$

### 18.4 Funciones generadoras

En el capítulo 12 hicimos la observación bastante trivial de que la solución de un problema combinatorio podía expresarse a menudo como una sucesión  $(u_n)$ . Pasamos ahora a estudiar los métodos basados en la representación de  $(u_n)$  como una serie de potencias

$$U(x) = u_0 + u_1x + u_2x^2 + \dots$$

En este contexto, el término usual para referirse a  $U(x)$  es el de **función generadora** de la sucesión  $(u_n)$ . (En rigor, debiéramos decir función generadora *ordinaria*, puesto que en matemáticas se usan a menudo otros tipos de funciones generadoras. Pero en este libro sólo necesitaremos las funciones generadoras ordinarias, de manera que omitiremos la palabra "ordinaria".) Ya hemos invertido algún tiempo en señalar que  $U(x)$  *no* es una función; es simplemente un modo alternativo de escribir la sucesión  $(u_n)$  de forma que puedan llevarse a cabo ciertas manipulaciones algebraicas.

Quizá el mejor ejemplo de función generadora proviene del teorema del binomio. Podemos entender la fórmula

$$(1+x)^k = \binom{k}{0} + \binom{k}{1}x + \binom{k}{2}x^2 + \dots + \binom{k}{n}x^n + \dots$$

como una manera de decir que la función generadora de la sucesión definida por

$$u_n = \binom{k}{n},$$

para un entero  $k$  cualquiera, es

$$U(x) = (1+x)^k.$$

En lo que resta del capítulo estudiaremos funciones generadoras de sucesiones definidas mediante ecuaciones recurrentes. El método que emplearemos consta de tres etapas:

- (i) utilizar la recurrencia de  $(u_n)$  para obtener una ecuación en  $U(x)$ ;
- (ii) resolver la ecuación en  $U(x)$ ;

- (iii) utilizar el álgebra (especialmente la descomposición en fracciones simples y el teorema del binomio) para hallar una fórmula de los coeficientes de  $U(x)$ .

El ejemplo siguiente es una aplicación típica del método. La sucesión en cuestión ya fue discutida en el apartado 12.2.

**Ejemplo.** Joshua P. Stackenboom, fundador y benefactor de la Universidad de Folornia, nos ha revelado cómo se hizo millonario. Empezó sin nada y al final del primer año de trabajo honrado había obtenido un dólar. Despues del segundo año tenía cinco dólares. A partir de entonces, se propuso comprar cada año bienes por seis veces el valor de su capital al inicio del año anterior, y venderlos por cuatro veces el valor de su capital al inicio del año en curso.

Hallar una recurrencia para  $(u_n)$ , el capital del Sr. Stackenboom al final del  $n$ -ésimo año, y resolverla. ¿Cuántos años tardó en hacerse millonario?

**SOLUCIÓN:** Tenemos que  $u_0 = 0$ ,  $u_1 = 1$  y  $u_2 = 5$ . Al final del año  $n + 1$ , el capital del Sr. Stackenboom es igual al capital que tenía al acabar el año  $n$ , menos el gasto, más los ingresos. Es decir,

$$u_{n+1} = u_n - 6u_{n-1} + 4u_n.$$

Si sustituimos  $n$  por  $n + 1$  y reordenamos la ecuación, obtenemos la recurrencia

$$u_{n+2} - 5u_{n+1} + 6u_n = 0.$$

El argumento anterior demuestra que es válida para todo  $n \geq 1$ . También se cumple, por sustitución directa, para  $n = 0$ , de forma que basta con las condiciones iniciales  $u_0 = 0$  y  $u_1 = 1$ . (Hay una razón práctica que nos ha hecho especificar separadamente que  $u_2 = 5$ : ¿sabría decir cuál es?)

Sea  $U(x)$  la función generadora de la sucesión  $(u_n)$ . Utilizando los valores iniciales de  $u_0$  y  $u_1$  y la ecuación para  $u_{n+2}$  ( $n \geq 0$ ) tenemos que

$$\begin{aligned} U(x) &= u_0 + u_1x + u_2x^2 + u_3x^3 + \dots \\ &= 0 + x + (5u_1 - 6u_0)x^2 + (5u_2 - 6u_1)x^3 + \dots \\ &= x + 5(u_1x^2 + u_2x^3 + \dots) - 6(u_0x^2 + u_1x^3 + \dots). \end{aligned}$$

La expresión en el primer paréntesis es  $xU(x)$ , ya que el término  $u_0x$  que falta es igual a 0, y en el segundo es  $x^2U(x)$ . Así pues,

$$U(x) = x + 5xU(x) - 6x^2U(x),$$

de donde

$$U(x) = \frac{x}{1 - 5x + 6x^2}.$$

Como  $1 - 5x + 6x^2 = (1 - 2x)(1 - 3x)$ , podemos descomponer  $U(x)$  en fracciones simples:

$$U(x) = \frac{-1}{1 - 2x} + \frac{1}{1 - 3x}.$$

Usando los desarrollos binomiales de  $(1 - 2x)^{-1}$  y  $(1 - 3x)^{-1}$ , se obtiene

$$U(x) = -(1 + 2x + (2x)^2 + \dots) + (1 + 3x + (3x)^2 + \dots),$$

de forma que

$$u_n = 3^n - 2^n.$$

Un cálculo sencillo demuestra que el Sr. Stackenboom se hizo millonario al cabo de trece años.  $\square$

#### Ejercicios 18.4

1 Usar el método de las funciones generadoras para hallar una fórmula de  $u_n$  cuando la sucesión  $(u_n)$  está definida por

$$u_0 = 1, \quad u_1 = 1, \quad u_{n+2} - 4u_{n+1} + 4u_n = 0 \quad (n \geq 0).$$

2 Sea  $A(x)$  la función generadora de la sucesión  $(a_n)$ . ¿Cuáles son las funciones generadoras de las sucesiones  $(p_n)$ ,  $(q_n)$  y  $(r_n)$  definidas del siguiente modo?

$$(i) p_n = 5a_n; \quad (ii) q_n = a_n + 5; \quad (iii) r_n = a_{n+5}.$$

3 Demostrar que  $x(1+x)/(1-x)^3$  es la función generadora de la sucesión cuyo término  $n$ -ésimo es  $n^2$ .

4 Sea  $A(x)$  la función generadora de la sucesión  $(a_n)$  y definamos

$$s_n = a_0 + a_1 + \cdots + a_n \quad (n \geq 0).$$

Demostrar que la función generadora de  $(s_n)$  es

$$S(x) = \frac{A(x)}{1-x}.$$

Utilizar este resultado juntamente con el ejercicio 3 para hallar una fórmula para  $\sum_{i=0}^n i^2$ .

## 18.5 Recurrencias lineales homogéneas

En el apartado 12.2 hallamos una solución explícita de la recurrencia

$$u_0 = c_0, \quad u_1 = c_1, \quad u_{n+2} + a_1 u_{n+1} + a_2 u_n = 0 \quad (n \geq 0).$$

Este es el caso  $k = 2$  de la recurrencia lineal homogénea, definida por las ecuaciones

$$[RLH] \quad \begin{cases} u_0 = c_0, & u_1 = c_1, \dots, & u_{k-1} = c_{k-1}, \\ u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n = 0 & (n \geq 0). \end{cases}$$

Usaremos el método de las funciones generadoras para hallar la solución general de [RLH] para todo valor de  $k$ .

**Teorema 18.5.1.** La función generadora de la sucesión  $(u_n)$  definida por [RLH] es

$$U(x) = \frac{R(x)}{1 + a_1 x + a_2 x^2 + \cdots + a_k x^k},$$

donde  $R(x)$  es un polinomio co gr  $R(x) < k$ .

**DEMOSTRACIÓN:** Consideremos el producto

$$(1 + a_1 x + \cdots + a_k x^k) U(x) = (1 + a_1 x + \cdots + a_k x^k)(u_0 + u_1 x + \cdots + u_n x^n + \cdots).$$

La regla del producto nos dice que el coeficiente de  $x^{n+k}$  es

$$u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n \quad (n \geq 0).$$

Pero  $(u_n)$  satisface [RLH], que es cero para  $n \geq 0$ . Los únicos coeficientes que no se anulan son los de  $1, x, \dots, x^{k-1}$ , de modo que el producto es un polinomio  $R(x)$  de grado gr  $R < k$ .

Los coeficientes no nulos de  $R(x)$  pueden obtenerse efectuando el producto anterior:

$$R(x) = u_0 + (u_1 + a_1 u_0)x + \cdots + (u_{k-1} + a_1 u_{k-2} + \cdots + a_{k-1} u_0)x^{k-1}.$$

Como los valores de  $u_0, u_1, \dots, u_{k-1}$  vienen dados explícitamente por las ecuaciones [RLH],  $R(x)$  puede determinarse sustituyendo  $u_i$  por  $c_i$  ( $0 \leq i \leq k-1$ ).  $\square$

Si  $k = 2$ , en el apartado 12.2 demostramos que la forma de la solución a la recurrencia lineal homogénea dependía de si las raíces  $\alpha$  y  $\beta$  de la ecuación auxiliar

$$t^2 + a_1 t + a_2 = 0$$

eran distintas o no. Si  $\alpha \neq \beta$ , la solución es de la forma

$$u_n = A\alpha^n + B\beta^n,$$

mientras que si  $\alpha = \beta$ , la solución es

$$u_n = (Cn + D)\alpha^n.$$

En el caso general, definimos la ecuación auxiliar de [RLH] como

$$t^k + a_1 t^{k-1} + \cdots + a_k = 0;$$

la forma de las soluciones depende, como era de esperar, de las raíces de la ecuación.

Supondremos que la ecuación auxiliar tiene  $k$  raíces, lo cual será sin duda cierto si trabajamos en el cuerpo  $\mathbb{C}$  de los números complejos. Sin embargo, las  $k$  raíces no tienen por qué ser distintas; supondremos que los

distintos valores son  $\alpha_1, \alpha_2, \dots, \alpha_s$  con multiplicidades  $m_1, m_2, \dots, m_s$ . En otras palabras, la ecuación auxiliar puede escribirse como

$$(t - \alpha_1)^{m_1}(t - \alpha_2)^{m_2} \cdots (t - \alpha_s)^{m_s} = 0,$$

donde  $m_1 + m_2 + \cdots + m_s = k$ . El denominador de la fórmula que aparece en el teorema 18.5.1 se obtiene de la ecuación auxiliar dividiendo por  $t^k$  y sustituyendo  $1/t$  por  $x$ , con lo que  $U(x)$  puede escribirse como

$$U(x) = \frac{R(x)}{(1 - \alpha_1 x)^{m_1} \cdots (1 - \alpha_s x)^{m_s}}.$$

Podemos aplicar ahora el teorema del binomio y obtener una fórmula general para  $u_n$ .

**Teorema 18.5.2.** Sea  $(u_n)$  definida por [RLH] y sean  $\alpha_1, \alpha_2, \dots, \alpha_s$  las raíces de la ecuación auxiliar con multiplicidades  $m_1, m_2, \dots, m_s$ . Entonces

$$u_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_s(n)\alpha_s^n,$$

donde, para cada  $i = 1, 2, \dots, s$ ,  $P_i(n)$  es una expresión de la forma

$$A_0 + A_1 n + \cdots + A_{m_i-1} n^{m_i-1}.$$

En otras palabras,  $P_i(n)$  es un polinomio en  $n$  de grado no superior a  $m_i - 1$ .

**DEMOSTRACIÓN:** Según la teoría de las fracciones simples desarrollada en el apartado 18.2, podemos escribir  $U(x)$  como una suma de  $s$  expresiones de la forma

$$\frac{\gamma_1}{1 - \alpha x} + \frac{\gamma_2}{(1 - \alpha x)^2} + \cdots + \frac{\gamma_m}{(1 - \alpha x)^m},$$

donde, en cada expresión,  $\alpha = \alpha_i$  y  $m = m_i$  para un valor específico de  $i$  entre 1 y  $s$ . Aplicando el teorema del binomio para exponentes negativos, el coeficiente de  $x^n$  en la serie de potencias correspondiente es

$$\gamma_1 \binom{1+n-1}{n} \alpha^n + \gamma_2 \binom{2+n-1}{n} \alpha^n + \cdots + \gamma_m \binom{m+n-1}{n} \alpha^n.$$

Simplificando y usando el hecho de que  $\binom{n+l}{n} = \binom{n+l}{l}$ , podemos escribirlo como  $P(n)\alpha^n$ , donde

$$P(n) = \gamma_1 \binom{n}{0} + \gamma_2 \binom{n+1}{1} + \cdots + \gamma_m \binom{n+m-1}{m-1}.$$

Ahora bien, la fórmula

$$\binom{n+l}{l} = \frac{(n+l)(n+l-1) \cdots (n+1)}{l(l-1) \cdots 1}$$

nos dice que  $\binom{n+l}{l}$  es una función polinómica de  $n$  de grado  $l$ , lo cual demuestra que  $P(n)$  es una función polinómica de  $n$  de grado como máximo  $m - 1$ .  $\square$

En la práctica, los teoremas 18.5.1 y 18.5.2 serán la base para determinar una fórmula para  $(u_n)$ , aunque no es necesario hallar la función generadora o su descomposición en fracciones simples. Será suficiente con saber la forma final del resultado y obtener los coeficientes de los polinomios  $P_i(n)$  sustituyendo los valores iniciales de  $u_0, u_1, \dots, u_{k-1}$ .

**Ejemplo.** Hallar una fórmula para el término  $n$ -ésimo de la sucesión definida por

$$u_0 = 0, \quad u_1 = -9, \quad u_2 = -1, \quad u_3 = 21,$$

$$u_{n+4} - 5u_{n+3} + 6u_{n+2} + 4u_{n+1} - 8u_n = 0 \quad (n \geq 0).$$

**SOLUCIÓN:** La ecuación auxiliar es

$$t^4 - 5t^3 + 6t^2 + 4t - 8 = 0,$$

que es igual a

$$(t-2)^3(t+1) = 0.$$

Los  $u_n$  vienen dados por la fórmula

$$u_n = (An^2 + Bn + C)2^n + D(-1)^n,$$

donde  $A, B, C$  y  $D$  son constantes. Si sustituimos los valores iniciales de  $u_0, u_1, u_2$  y  $u_3$ , obtenemos las ecuaciones

$$\begin{aligned}C + D &= 0, \\2A + 2B + 2C + D &= -9, \\16A + 8B + 4C + D &= -1, \\72A + 24B + 8C - D &= 21.\end{aligned}$$

El método estándar para resolver ecuaciones lineales proporciona la solución  $A = 1, B = -1, C = -3, D = 3$ . Así pues,

$$u_n = (n^2 - n - 3)2^n + 3(-1)^n. \quad \square$$

### Ejercicios 18.5

1 Utilizar el método de la ecuación auxiliar para hallar una fórmula para  $u_n$  en los casos siguientes:

- (i)  $u_0 = 1, \quad u_1 = 3, \quad u_{n+2} - 3u_{n+1} - 4u_n = 0 \quad (n \geq 0);$
- (ii)  $u_0 = 2, \quad u_1 = 0, \quad u_2 = -2;$   
 $u_{n+3} - 6u_{n+2} + 11u_{n+1} - 6u_n = 0 \quad (n \geq 0);$
- (iii)  $u_0 = 1, \quad u_1 = 0, \quad u_2 = 0;$   
 $u_{n+3} - 3u_{n+2} + 2u_n = 0 \quad (n \geq 0).$

2 El profesor McBrain sube las escaleras de una forma errática. A veces sube dos peldaños de golpe, a veces sólo uno. Hallar una fórmula para  $b_n$ , el número de formas distintas en que puede subir  $n$  peldaños.

3 Sea  $(z_n)$  la sucesión definida por

$$z_0 = 1, \quad z_{n+1} = \frac{z_n - a}{z_n - b} \quad (n \geq 0),$$

donde  $a$  y  $b$  son números reales con  $b \neq 1$ . Demostrar que si la sucesión  $(u_n)$  cumple la relación

$$\frac{u_{n+1}}{u_n} = z_n - b,$$

entonces

$$u_{n+2} + (b-1)u_{n+1} + (a-b)u_n = 0 \quad (n \geq 0).$$

Hallar una fórmula para  $z_n$  si  $a = 0$  y  $b = 2$ .

4 Sean  $(u_n)$ ,  $(v_n)$  y  $(w_n)$  las sucesiones definidas mediante  $u_0 = v_0 = w_0 = 1$  y

$$\begin{pmatrix} u_{n+1} \\ v_{n+1} \\ w_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -1 & 4 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} \quad (n \geq 0).$$

Demostrar que  $(u_n)$  satisface una recurrencia lineal homogénea y hallar una fórmula para  $u_n$ .

### 18.6 Recurrencias lineales no homogéneas

En algunos casos puede usarse el método de las funciones generadoras para resolver recurrencias lineales no homogéneas

$$\begin{aligned}u_0 &= c_0, \quad u_1 = c_1, \dots, \quad u_{k-1} = c_{k-1}, \\u_{n+k} + a_1u_{n+k-1} + \dots + a_ku_n &= f(n) \quad (n \geq 0).\end{aligned}$$

La aplicabilidad del método depende de la forma particular de la función  $f(n)$ . La técnica es, aproximadamente, desarrollar  $(1 + a_1x + a_2x^2 + \dots + a_kx^k)U(x)$  y esperar que los términos en  $f(n)$  puedan tratarse de alguna forma.

**Ejemplo.** Hallar una fórmula explícita para los términos de la sucesión  $(u_n)$  definida por la recurrencia

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+2} - u_{n+1} - 6u_n = n \quad (n \geq 0).$$

**SOLUCIÓN:** Ponemos en práctica el método que acabamos de esbozar y calculamos

$$\begin{aligned}(1 - x - 6x^2)(u_0 + u_1x + u_2x^2 + \dots) \\&= u_0 + (u_1 - u_0)x + (u_2 - u_1 - 6u_0)x^2 + \dots \\&\quad + (u_{n+2} - u_{n+1} - 6u_n)x^{n+2} + \dots \\&= x + (x^3 + 2x^4 + \dots + nx^{n+2} + \dots) \\&= x + x^3(1 - x)^2.\end{aligned}$$

Al ser  $1 - x - 6x^2 = (1 + 2x)(1 - 3x)$ , la función generadora  $U(x)$  satisface la ecuación

$$(1 + 2x)(1 - 3x)U(x) = \frac{x - 2x^2 + 2x^3}{(1 - x)^2},$$

de forma que

$$U(x) = \frac{x - 2x^2 + 2x^3}{(1 + 2x)(1 - 3x)(1 - x)^2} = \frac{A}{1 + 2x} + \frac{B}{1 - 3x} + \frac{C}{1 - x} + \frac{D}{(1 - x)^2}$$

para ciertas constantes  $A, B, C$  y  $D$ .

Hay varias maneras de obtener las constantes: una de ellas es usar la regla de cubrir y hallar  $A, B$  y  $D$  sustituyendo por  $x = -\frac{1}{2}$ ,  $x = \frac{1}{3}$ ,  $x = 1$ , respectivamente. Esto nos da

$$A = -\frac{2}{9}, \quad B = \frac{1}{4}, \quad D = -\frac{1}{6}.$$

Podemos hallar  $C$  haciendo  $x = 0$  (lo que equivale a reducir a común denominador e igualar términos constantes) y obtenemos

$$A + B + C + D = 0,$$

de donde  $C = \frac{5}{36}$ . Otra manera es observar que la fórmula para  $U(x)$  implica que

$$u_n = A(-2)^n + B(3^n) + C + D(n+1)$$

y utilizar los valores  $u_0 = 0$ ,  $u_1 = 1$ ,  $u_2 = 1$ ,  $u_3 = 8$  para determinar  $A, B, C$  y  $D$ . Las ecuaciones son:

$$\begin{aligned} 0 &= A + B + C + D, \\ 1 &= -2A + 3B + C + 2D, \\ 1 &= 4A + 9B + C + 3D, \\ 8 &= -8A + 27B + C + 4D \end{aligned}$$

y la solución, nuevamente,  $A = -\frac{2}{9}$ ,  $B = \frac{1}{4}$ ,  $C = \frac{5}{36}$  y  $D = -\frac{1}{6}$ . Reagrupando términos se obtiene la fórmula

$$u_n = \frac{1}{36} [(-2)^{n+3} + 3^{n+2} - 6n - 1]. \quad \square$$

Hay muchos otros problemas que pueden atacarse con el método de las funciones generadoras. Los resultados son especialmente interesantes si se combina con métodos analíticos relativos a series de potencias, pero este tema queda fuera del marco de este libro. Afortunadamente, pueden obtenerse algunos resultados importantes únicamente con los métodos algebraicos de que disponemos. En los siguientes dos capítulos se discutirán varios resultados de este tipo.

### Ejercicios 18.6

1 Demostrar que la función generadora de la sucesión  $(u_n)$  definida por la recurrencia

$$u_0 = 1, \quad u_{n+1} - 2u_n = 4^n \quad (n \geq 0)$$

es

$$U(x) = \frac{1 - 3x}{(1 - 2x)(1 - 4x)}.$$

Deducir que  $u_n = 2^{2n-1} + 2^{n-1}$ .

2 Sea  $q_n$  el número de palabras de longitud  $n$  en el alfabeto  $\{a, b, c, d\}$  que contienen un número impar de bes. Demostrar que

$$q_{n+1} = 4^n + 2q_n \quad (n \geq 1).$$

[Indicación: dividir el conjunto de las palabras de longitud  $n+1$  que cumplen la condición entre las que empiezan por  $b$  y las que no.] Hallar la función generadora  $Q(x)$  de  $(q_n)$ , suponiendo que  $q_0 = 0$ , y demostrar que

$$q_n = \frac{1}{2}(4^n - 2^n).$$

3 Demostrar que la función generadora de la sucesión definida por

$$u_0 = 1, \quad u_{n+1} - 2u_n = n\alpha^n \quad (n \geq 0)$$

es

$$u(x) = \frac{1}{1 - 2x} + \frac{\alpha x^2}{(1 - 2x)(1 - \alpha x)^2},$$

siempre que  $\alpha \neq 2$ . Deducir una fórmula para  $u_n$ . ¿Qué ocurre si  $\alpha = 2$ ?

## 18.7 Ejercicios diversos

1 ¿Cuáles de los siguientes elementos son inversibles en  $\mathbf{R}[[x]]$  y cuáles lo son en  $\mathbf{Z}[[x]]$ ?

- (i)  $1+x$ ; (ii)  $x^2$ ; (iii)  $3+2x^3$ .

2 Hallar los cuatro primeros términos y el término general de la serie de potencias de  $(1+x)^{-5}$ .

3 Hallar el coeficiente de  $x^n$  en la serie de potencias de

$$\frac{26 - 60x + 25x^2}{(1-2x)(1-5x)^2}.$$

4 Hallar los cuatro primeros términos y el término general de la serie de potencias de

$$\frac{1-x-x^2}{(1-2x)(1-x)^2}.$$

5 Hallar una fórmula del coeficiente de  $x^n$  en la serie de potencias de  $(1+x)/(1+x+x^3)$  en  $\mathbf{Z}_3[[x]]$ .

6 Hallar la descomposición en fracciones simples sobre  $\mathbf{Z}_5$  de

$$\frac{4x+2}{x^3+2x^2+4x+3}.$$

7 Utilizar el método del ejercicio 18.4.4 para hallar una fórmula para  $\sum i^3$  y  $\sum i^4$ , donde las sumas son entre 1 y  $n$ .

8 Si  $A(x)$  es la función generadora de la sucesión  $(a_n)$ , definimos la *derivada*  $A'(x)$  como la función generadora de la sucesión  $(a'_n)$ , definida por  $a'_n = (n+1)a_{n+1}$  para  $n \geq 0$ . Demostrar que

$$(AB)'(x) = A'(x)B(x) + A(x)B'(x).$$

9 Demostrar que

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = 2^{n-1}n$$

derivando la fórmula del binomio.

10 Usar la fórmula  $(1-x^2)^{-n} = (1-x)^{-n}(1+x)^{-n}$  para demostrar la identidad

$$\sum_{i=0}^r (-1)^i \binom{n+r-i-1}{r-i} \binom{n+i-1}{i} = \begin{cases} 0 & \text{si } r \text{ es impar} \\ \binom{n+r/2-1}{r/2} & \text{si } r \text{ es par.} \end{cases}$$

11 Hallar una expresión de  $(1-x)^{-n}(1-x^k)^n$  como polinomio de grado  $n(k-1)$  y deducir la identidad

$$\binom{r}{n-1} \binom{n}{0} - \binom{r-k}{n-1} \binom{n}{1} + \binom{r-2k}{n-1} \binom{n}{2} - \cdots = 0,$$

válida siempre que  $r \geq nk$ .

12 Obtener la función generadora de la sucesión  $(u_n)$  que representa el número de maneras de distribuir  $n$  libros distintos a cuatro personas.

13 Sea  $c_r$  el número de maneras en que puede obtenerse un total de  $r$  al tirar cuatro dados. Demostrar que la función generadora de la sucesión  $(c_r)$  es

$$C(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)^4.$$

14 Obtener la función generadora de  $(b_r)$ , donde  $b_r$  es el número de enteros  $n$  con  $0 \leq n \leq 10^m - 1$  tales que la suma de sus cifras en base 10 es igual a  $r$ .

15 Utilizar el método de las funciones generadoras para resolver la siguiente recurrencia:

$$u_0 = 2, \quad u_1 = -6, \quad u_{n+2} + 8u_{n+1} - 9u_n = 8(3^{n+1}) \quad (n \geq 0).$$

16 Hallar la forma general de la solución a la recurrencia

$$y_{n+2} - 6y_{n+1} + 9y_n = 2^n + n \quad (n \geq 0).$$

17 Si  $k \geq 0$ , sea  $f(n, k)$  el número de  $k$ -subconjuntos de  $\{1, 2, \dots, n\}$  que no contienen dos enteros sucesivos. Demostrar que

$$f(n, k) = f(n-2, k-1) + f(n-1, k).$$

Sea  $F_k(x)$  la función generadora de los números  $f(n, k)$  para un  $k$  fijo. Hallar una recurrencia para  $F_k(x)$  y deducir que

$$f(n, k) = \binom{n-k+1}{k}.$$

18 Utilizar el método de las funciones generadoras para resolver la recurrencia

$$u_0 = 1, \quad u_{n+1} = 3u_n + 2^{n-1} \quad (n \geq 0).$$

19 La función generadora *exponencial* de la sucesión  $(u_n)$  se define como la serie de potencias

$$\tilde{u}(x) = u_0 + \frac{u_1}{1!}x + \frac{u_2}{2!}x^2 + \cdots + \frac{u_i}{i!}x^i + \cdots$$

Utilizar la recurrencia  $d_n = nd_{n-1} + (-1)^n$  del número de desarreglos para demostrar que la función generadora exponencial de  $(d_n)$  es  $e^{-x}/(1-x)$ . Deducir la conocida fórmula explícita de  $d_n$ .

20 Sea  $\tilde{Q}(x)$  la función generadora exponencial de  $(q_n)$ , donde  $q_n$  es el número de particiones de un  $n$ -conjunto. Utilizar la fórmula hallada en el ejercicio 5.7.10 para demostrar que

$$\tilde{Q}(x) = \exp(e^x - 1).$$

## 19 Particiones de un entero positivo

### 19.1 Particiones y diagramas

En el apartado 5.4 iniciamos el estudio de las particiones de un entero positivo, e hicimos notar que el problema de calcular el número  $p(n)$  de particiones de  $n$  no era sencillo. Ahora, después de haber desarrollado una variedad de técnicas (en particular, el método de las funciones generadoras) atacamos el problema con más esperanzas.

Empezaremos recordando la notación estándar

$$[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$$

de una partición de  $n$  que tiene  $\alpha_i$  partes de tamaño  $i$  ( $1 \leq i \leq n$ ). Las particiones de 5, y su representación en notación estándar, son:

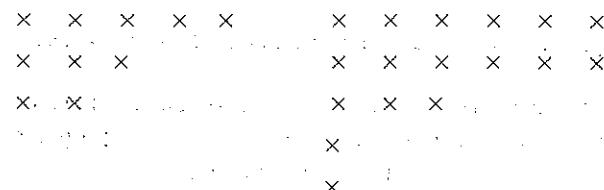
5	[5]
4 + 1	[14]
3 + 2	[23]
3 + 1 + 1	[1 <sup>2</sup> 3]
2 + 2 + 1	[12 <sup>2</sup> ]
2 + 1 + 1 + 1	[1 <sup>3</sup> 2]
1 + 1 + 1 + 1 + 1	[1 <sup>5</sup> ].

Así pues, el número de particiones de 5 es  $p(5) = 7$ . Otros valores de  $p(n)$  son

$$\begin{aligned} p(10) &= 42 \\ p(20) &= 627 \\ p(100) &= 190\,569\,292 \\ p(200) &= 3\,972\,999\,029\,388. \end{aligned}$$

Aunque no existe ninguna fórmula sencilla para  $p(n)$ , es posible obtener una fórmula exacta muy complicada mediante técnicas analíticas en las que interviene la función generadora de la sucesión  $(p(n))$ . La función generadora también puede usarse para obtener una recurrencia efectiva de  $p(n)$ : este es el punto de vista que adoptaremos. La recursión nos permitirá calcular un valor cualquiera, como  $p(200)$ , mediante operaciones aritméticas rútinarias.

Resulta conveniente usar una representación gráfica de las particiones. Las partes se disponen en orden, de mayor a menor, y cada parte está representada por una fila con el número apropiado de marcas. Por ejemplo, los diagramas



representan a las particiones

$$5 + 3 + 2$$

$$6 + 6 + 3 + 1 + 1.$$

(Un diagrama de este tipo se conoce con el nombre de *diagrama de Ferrers*, o bien *grafo de Ferrers*. Su nombre suele escribirse incorrectamente.)

Esta sencilla idea es muy útil en la demostración de teoremas sobre particiones. Un buen ejemplo es el resultado siguiente.

**Teorema 19.1.** Sean  $n$  y  $r$  enteros positivos. El número de particiones de  $n$  en  $r$  partes como máximo es igual al número de particiones de  $n+r$  en  $r$  partes exactamente.

**DEMOSTRACIÓN:** Tomemos una partición de  $n+r$  en  $r$  partes. Su diagrama contiene exactamente  $r$  marcas en la primera columna; si eliminamos dicha columna se obtiene el diagrama de una partición de  $n$  en  $r$  partes como máximo. Recíprocamente, dada una partición del segundo tipo, podemos añadir una nueva primera columna con  $r$  marcas y obtenemos una partición del primer tipo. En otras palabras, existe una biyección entre

los dos conjuntos de particiones y tienen, por lo tanto, el mismo cardinal. (La figura 19.1 ilustra la biyección.)

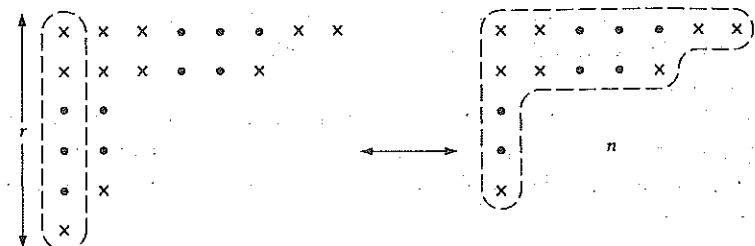


Fig. 19.1 Ilustración de la demostración del teorema 19.1.

Si  $\mathcal{P}$  es una propiedad relativa a una partición, la expresión  $p(n|\mathcal{P})$  denotará el número de particiones de  $n$  que cumplen la propiedad  $\mathcal{P}$ . Con esta notación, el teorema 19.1 puede reformularse como

$$p(n \mid \text{número de partes} \leq r) = p(n+r \mid \text{número de partes} = r).$$

### Ejercicios 19.1

1 Dibujar los diagramas de las siguientes particiones:

$$(i) [1^2 3^3 5^7], \quad (ii) [246^2 7].$$

2 Hallar los valores de  $p(n)$ ,  $1 \leq n \leq 7$ , confeccionando una lista con todas las posibles particiones.

3 Sea

$$p_k(n) = p(n \mid \text{número de partes} = k).$$

Demostrar que la siguiente fórmula (que se obtuvo en el ejercicio 5.4.2) es una consecuencia del teorema 19.1:

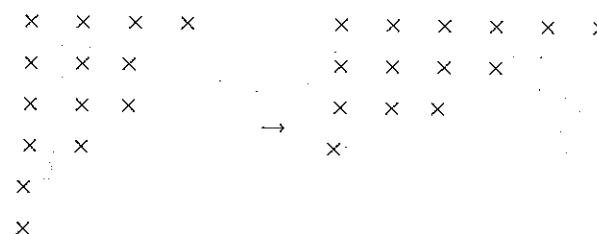
$$p_k(n) = p_k(n-k) + p_{k-1}(n-k) + \cdots + p_1(n-k).$$

Usarla para calcular  $p(8)$ .

4 Utilizar un argumento basado en diagramas para demostrar que el número de particiones de  $n$  en  $m$  partes como máximo es igual al número de particiones de  $n + \frac{1}{2}m(m+1)$  en  $m$  partes, todas ellas distintas. [Indicación: añadir un "triángulo" con  $\frac{1}{2}m(m+1)$  marcas.]

## 19.2 Particiones conjugadas

La representación diagramática de las particiones sugiere la siguiente transformación sencilla de una partición en otra: intercambiar filas y columnas en el diagrama. Por ejemplo, la partición  $\lambda = [1^2 2 3^2 4]$  se transforma en la partición  $\lambda' = [1346]$ , tal como indican los diagramas.



Diremos que dos particiones  $\lambda$  y  $\lambda'$  relacionadas de esta forma son **conjugadas**.

La transformación  $\lambda \rightarrow \lambda'$  que envía una partición a su conjugada puede aplicarse a la demostración de varios resultados útiles. Un ejemplo típico es el siguiente. Si  $m$  es la mayor de las partes de  $\lambda$ , tanto la primera fila del diagrama de  $\lambda$  como la primera columna del de  $\lambda'$  contienen  $m$  marcas. Por lo tanto,  $\lambda'$  es una partición en  $m$  partes. En otras palabras, la transformación  $\lambda \rightarrow \lambda'$  es una biyección entre el conjunto de las particiones de  $n$  con parte máxima igual a  $m$  y el conjunto de las particiones de  $n$  en  $m$  partes exactamente. Así pues, hemos demostrado que

$$p(n \mid \text{parte máxima} = m) = p(n \mid \text{número de partes} = m).$$

Una partición es **autoconjuguada** si  $\lambda = \lambda'$ .

**Teorema 19.2.** El número de particiones autoconjuguadas de  $n$  es igual al número de particiones de  $n$  en partes distintas e impares.

**DEMOSTRACIÓN:** La primera fila y columna del diagrama de una partición autoconjuguada contienen el mismo número  $k$  de marcas. Como tienen una marca en común, el número total de marcas en la primera fila y columna es el número impar  $2k - 1$ . Igualmente, si eliminamos la primera fila y columna, lo que queda de la segunda fila y columna contiene un número impar de marcas, digamos  $2l - 1$ . Continuando de esta forma se obtiene una partición de  $n$  en la que cada parte es impar y en la que todas las partes son distintas. El proceso puede visualizarse como el "enderezamiento" de las secciones en forma de  $L$  de la partición autoconjuguada en cuestión (figura 19.2).

Recíprocamente, dada una partición de  $n$  en partes impares y distintas, podemos "doblar" el diagrama para obtener una partición autoconjuguada de  $n$ .  $\square$

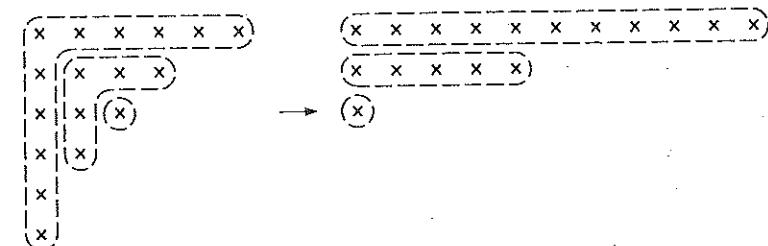


Fig. 19.2 Ilustración de la demostración del teorema 19.2.

## Ejercicios 19.2

1 Hallar los conjugados de las siguientes particiones dadas en notación estándar:

$$(i) [1^2 3 5 6], \quad (ii) [2^2 3^3 5 8].$$

2 ¿Cuáles de las siguientes particiones son autoconjuguadas?

$$(i) [1^2 2 4], \quad (ii) [1^3 4 5 6], \quad (iii) [2^2 3 5^2], \quad (iv) [1^4 2 3 4 8].$$

3 Usar el método descrito en el teorema 19.2 para hallar todas las particiones autoconjuguadas de 20.

4 Demostrar que el número de particiones autoconjungadas de  $n$  con parte máxima  $k$  es igual al número de particiones autoconjungadas de  $n - 2k + 1$  con partes no superiores a  $k - 1$ . Hallar el número de particiones autoconjungadas de 41 en las que la parte máxima es 11.

### 19.3 Particiones y funciones generadoras

En este apartado obtendremos una fórmula para la función generadora

$$P(x) = p(0) + p(1)x + p(2)x^2 + \dots,$$

donde  $p(n)$  es el número de particiones de  $n$  y, por convenio,  $p(0) = 1$ .

El punto de partida es la fórmula

$$(1 - x^i)^{-1} = 1 + x^i + x^{2i} + x^{3i} + \dots,$$

que debe considerarse como el inverso de  $1 - x^i$  en el anillo de series de potencias  $\mathbb{C}[[x]]$ . La fórmula puede obtenerse mediante un cálculo directo, o sustituyendo  $x$  por  $x^i$  ( $i \geq 1$ ) en la fórmula estándar de  $(1 - x)^{-1}$ . Para nuestros propósitos, la observación clave es que esta serie de potencias es la función generadora de los números  $f_n$  de particiones de una clase muy sencilla:

$$f_n = p(n \mid \text{cada parte es igual a } i).$$

Esto es así ya que no existen particiones de esta clase a menos que  $n$  sea un múltiplo de  $i$ , en cuyo caso hay una única partición  $n = i + i + \dots + i$ . En otras palabras,

$$f_n = \begin{cases} 1 & \text{si } n = \alpha i \quad (\alpha = 0, 1, 2, \dots), \\ 0 & \text{en otro caso.} \end{cases}$$

En consecuencia, la función generadora de  $(f_n)$  es

$$F(x) = (1 - x^i)^{-1}.$$

Sean ahora  $i$  y  $j$  dos enteros positivos y sea

$$h_n = p(n \mid \text{cada parte es igual a } i \text{ o } j).$$

¿Cuál es la función generadora  $H(x)$  de la sucesión  $(h_n)$ ?

Sean  $f_n$  y  $F(x)$  como antes y  $g_n$  el número de particiones de  $n$  en las que cada parte es igual a  $j$ . Hemos demostrado que  $F(x) = (1 - x^i)^{-1}$  y, por el mismo motivo, la función generadora  $G(x)$  de  $(g_n)$  es  $(1 - x^j)^{-1}$ . Nótese ahora que  $h_n$  es el número de maneras de escribir  $n$  como suma de  $r$  y  $n - r$ , donde  $r$  está partido en partes  $i$  y  $n - r$  en partes  $j$ . Así pues,

$$h_n = f_0 g_n + f_1 g_{n-1} + \dots + f_n g_0.$$

La regla para multiplicar series de potencias nos dice que

$$H(x) = F(x)G(x) = (1 - x^i)^{-1}(1 - x^j)^{-1}.$$

Por ejemplo, si  $i = 2$  y  $j = 3$ , el producto de las series  $(1 - x^2)^{-1}$  y  $(1 - x^3)^{-1}$  es

$$(1 + x^2 + x^4 + x^6 + x^8 + x^{10} + \dots)(1 + x^3 + x^6 + x^9 + \dots) \\ = 1 + x^2 + x^3 + x^4 + x^5 + 2x^6 + x^7 + x^8 + 2x^9 + 2x^{10} + \dots$$

El coeficiente de  $x^{10}$  es 2, y proviene de los productos  $x^4 \times x^6$  y  $x^{10} \times 1$ . Estos productos corresponden a las sumas:

$$10 = 4 + 6 = 2 + 2 + 3 + 3 + 3, \quad 10 = 10 + 0 = 2 + 2 + 2 + 2,$$

que, a su vez, corresponden a las dos maneras de escribir 10 como una partición en la que cada parte es 2 o 3.

Ahora es fácil ver cómo obtener funciones generadoras del número de particiones en las que cada parte es igual a uno de entre varios números prefijados. Por ejemplo, si

$$a_n = p(n \mid \text{cada parte es igual a } i, j \text{ o } k),$$

la función generadora correspondiente es

$$A(x) = (1 - x^i)^{-1}(1 - x^j)^{-1}(1 - x^k)^{-1}.$$

**Ejemplo.** ¿De cuántas maneras pueden cambiarse 100 pesetas en monedas de 25, 10 y 5?

**SOLUCIÓN:** Nos preguntan por el número de particiones de 100 en partes de tamaño 5, 10 o 25, y la solución es el coeficiente de  $x^{100}$  en

$$(1 - x^5)^{-1}(1 - x^{10})^{-1}(1 - x^{25})^{-1}.$$

Podemos hacer la sustitución  $y = x^5$  y hallar el coeficiente de  $y^{20}$  en  $(1 - y)^{-1}(1 - y^2)^{-1}(1 - y^5)^{-1}$ . Por otra parte, no hace falta considerar los términos más allá de  $y^{20}$ . Primero calculamos  $(1 - y^2)^{-1}(1 - y^5)^{-1}$ , es decir,

$$(1 + y^2 + y^4 + y^6 + y^8 + y^{10} + y^{12} + y^{14} + y^{16} + y^{18} + y^{20} + \dots) \\ \times (1 + y^5 + y^{10} + y^{15} + y^{20} + \dots).$$

Una buena manera de efectuar el producto es quedarse únicamente con los coeficientes y efectuar el cálculo como en la tabla 19.3.1, donde la primera fila contiene los coeficientes del primer factor y las filas restantes corresponden al producto por los términos del segundo factor.

Tabla 19.3.1

$1$	$y$	$y^2$	$y^3$	$y^4$	$y^5 \dots$	$y^{10} \dots$	$y^{15} \dots$	$y^{20}$
1	0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0	( $\times y^5$ )
					1	0	1	( $\times y^{10}$ )
						1	0	( $\times y^{15}$ )
							1	( $\times y^{20}$ )
1	0	1	0	1	1	1	1	1
					1	1	1	1
					2	1	2	1
					2	2	2	2
								3

Así pues,  $(1 - y^2)^{-1}(1 - y^5)^{-1}$  es igual a

$$1 + y^2 + y^4 + y^5 + y^6 + y^7 + y^8 + y^9 + 2y^{10} + y^{11} + 2y^{12} + y^{13} + 2y^{14} \\ + 2y^{15} + 2y^{16} + 2y^{17} + 2y^{18} + 2y^{19} + 3y^{20} + \dots.$$

El término  $(1 - y)^{-1}$  es igual a  $(1 + y + y^2 + \dots + y^{20} + \dots)$ , de manera que multiplicar por él corresponde a sumar todos los coeficientes que acabamos de obtener. Por lo tanto, el número buscado es 29.  $\square$

Es cierto que el uso del álgebra en el ejemplo anterior es más bien superfluo, ya que podríamos haber hecho los mismos cálculos utilizando la terminología original no algebraica del problema. Sin embargo, el marco algebraico tiene la ventaja de la generalidad y del potencial de desarrollos posteriores. En particular, podemos usarlo para hallar la función generadora del número  $p(n)$  de particiones sin ninguna restricción.

**Teorema 19.3.** La función generadora del número  $p(n)$  de particiones de  $n$  puede escribirse como el producto infinito

$$P(x) = \prod_{i=1}^{\infty} (1 - x^i)^{-1}.$$

**DEMOSTRACIÓN:** Sea  $m$  un entero positivo fijo y sea  $p^{(m)}(n)$  el número de particiones de  $n$  en las que cada parte es uno de los enteros  $1, 2, \dots, m$ . Entonces  $p^{(m)}(n)$  es el número de maneras de expresar  $n$  como una suma

$$n = s_1 + s_2 + \dots + s_m,$$

donde cada  $s_i$  ( $1 \leq i \leq m$ ) es a su vez suma de varios  $i$ . Esto es igual al número de maneras de elegir, para cada  $i = 1, 2, \dots, m$ , un término  $x^{s_i}$  de cada serie de potencias  $(1 - x^i)^{-1}$  de forma que el producto de los términos sea  $x^n$ . En otras palabras, la función generadora de los  $p^{(m)}(n)$  es

$$P^{(m)}(x) = (1 - x)^{-1}(1 - x^2)^{-1} \cdots (1 - x^m)^{-1}.$$

Para cada valor de  $n$  tenemos que  $p(n) = p^{(n)}(n)$ , ya que una partición de  $n$  no puede contener partes mayores que  $n$ . Esto corresponde al hecho de que los términos

$$(1 - x^i)^{-1} = 1 + x^i + x^{2i} + \dots$$

con  $i > n$  no contribuyen al coeficiente de  $x^n$  en el producto infinito  $P(x)$ . En otras palabras, el coeficiente de  $x^n$  en  $P(x)$  es el mismo que el

coeficiente de  $x^n$  en  $P^{(n)}(x)$ , y este no es más que  $p^{(n)}(n) = p(n)$ . Así pues,  $P(x)$  es la función generadora de la sucesión  $(p(n))$ .  $\square$

Tal como indicamos en el último párrafo de la demostración, la presencia de un número infinito de factores en el producto  $P(x)$  no es una dificultad seria, ya que para calcular un coeficiente cualquiera sólo hay que tener en cuenta un número finito de factores. En los apartados siguientes encontraremos otros productos infinitos de series de potencias y siempre compartirán esta propiedad, por lo que no volveremos a referirnos a la supuesta dificultad de tratar con expresiones de este tipo.

### Ejercicios 19.3

1 Hallar las funciones generadoras de las sucesiones que tienen por término  $n$ -ésimo:

- (i) el número de particiones de  $n$  en partes iguales a 3 o 5;
- (ii) el número de particiones de  $n$  en partes iguales a 2, 4 o 6.

2 Hallar el coeficiente de  $x^9$  en

$$\frac{1}{(1-x)(1-x^2)(1-x^3)}$$

multiplicando las series de potencias correspondientes. Interpretar el resultado como el número de particiones de un cierto tipo y comprobar la respuesta enumerando las particiones explícitamente.

3 ¿De cuántas maneras puede cambiarse una moneda de 100 por monedas de 50, 20, 10 y 5?

4 ¿De cuántas maneras puede obtenerse un peso de 15 kg a partir de pesos de 1, 2 y 4 kg?

### 19.4 Funciones generadoras de particiones restringidas

Una sencilla modificación de los argumentos expuestos en el apartado 19.3 nos permitirá hallar las funciones generadoras del número de particiones sujetas a varias restricciones. Por ejemplo, supongamos que cada parte

puede aparecer  $k$  veces como máximo. Entonces la contribución de las partes iguales a  $i$  provienen de los términos del polinomio

$$1 + x^i + x^{2i} + \cdots + x^{ki},$$

en lugar de la serie de potencias  $(1-x^i)^{-1} = 1 + x^i + x^{2i} + \cdots$ , con lo que la función generadora es

$$(1+x+\cdots+x^k)(1+x^2+\cdots+x^{2k})(1+x^3+\cdots+x^{3k})\cdots$$

Como

$$1 + x^i + x^{2i} + \cdots + x^{ki} = \frac{1 - x^{(k+1)i}}{1 - x^i},$$

podemos escribir la función generadora en cualquiera de las formas

$$\prod_{i=1}^{\infty} (1 + x^i + x^{2i} + \cdots + x^{ki}) = \prod_{i=1}^{\infty} \frac{1 - x^{(k+1)i}}{1 - x^i}.$$

En particular, si  $k = 1$ , tenemos la función generadora de las particiones con partes *distintas*; esta es la que aparece en primer lugar en la tabla 19.4.1, una pequeña tabla de funciones generadoras útiles.

Tabla 19.4.1

$u_n$	$U(x)$
$p(n \mid \text{las partes son distintas})$	$(1+x)(1+x^2)(1+x^3)\cdots$
$p(n \mid \text{las partes son impares})$	$\frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}$
$p(n \mid \text{las partes son pares})$	$\frac{1}{(1-x^2)(1-x^4)(1-x^6)\cdots}$
$p(n \mid \text{cada parte es } \leq m)$	$\frac{1}{(1-x)(1-x^2)\cdots(1-x^m)}$

Mediante manipulaciones algebraicas elementales podemos obtener resultados inesperados.

**Ejemplo.** Utilizar el método de las funciones generadoras para demostrar que

$$p(n \mid \text{cada parte es distinta}) = p(n \mid \text{cada parte es impar}).$$

**SOLUCIÓN:** Sean  $D(x)$  y  $O(x)$  las funciones generadoras correspondientes. Tenemos que

$$\begin{aligned} D(x) &= (1+x)(1+x^2)(1+x^3)\cdots, \\ O(x) &= (1-x)^{-1}(1-x^3)^{-1}(1-x^5)^{-1}\cdots \end{aligned}$$

Para demostrar que estas dos series de potencias son la misma, usaremos la igualdad

$$1+y = (1-y^2)/(1-y).$$

De esta forma,

$$\begin{aligned} D(x) &= \frac{(1-x^2)(1-x^4)(1-x^6)\cdots}{(1-x)(1-x^2)(1-x^3)\cdots} \\ &= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}, \end{aligned}$$

ya que todos los términos de la forma  $1-x^{2i}$  se cancelan. Así pues,  $D(x) = O(x)$  y las dos sucesiones de coeficientes son iguales.  $\square$

#### Ejercicios 19.4

- 1 Hallar la función generadora de la sucesión que tiene por término  $n$ -ésimo
  - (i)  $p(n \mid \text{cada parte aparece dos veces como máximo});$
  - (ii)  $p(n \mid \text{cada parte es una potencia de } 2);$
  - (iii)  $p(n \mid \text{la menor de las partes es } 5).$
- 2 Utilizar el método de las funciones generadoras para hallar el número de particiones de 16 en las que cada parte es un primo impar.
- 3 Hallar la función generadora de la sucesión cuyo término  $n$ -ésimo es

$$p(n \mid \text{ningún número par aparece más de una vez}).$$

Demostrar que este número es igual a

$$p(n \mid \text{cada parte aparece 3 veces como máximo}).$$

[Indicación:  $(1-y^4) = (1-y)/(1+y+y^2+y^3)$ .]

4 Demostrar que

$$(1-x)(1+x)(1+x^2)(1+x^4)\cdots(1+x^{2^m}) = 1-x^{2^{m+1}},$$

y deducir la fórmula

$$(1-x)^{-1} = (1+x)(1+x^2)(1+x^4)\cdots,$$

donde el miembro derecho es el producto de los factores  $1+x^{2^r}$  para todo  $r \geq 0$ . Deducir que todo entero positivo admite una única partición en que las partes son potencias de 2 distintas.

#### 19.5 Una identidad misteriosa

Hemos visto que la función generadora del número de particiones con partes distintas es

$$D(x) = (1+x)(1+x^2)(1+x^3)\cdots$$

Por ejemplo, la partición  $7 = 1 + 2 + 4$  corresponde al término  $x \cdot x^2 \cdot x^4$  y contribuye en 1 al coeficiente de  $x^7$ . Consideremos ahora qué ocurre si cambiamos los signos + por -, de forma que tengamos la serie de potencias

$$\begin{aligned} Q(x) &= (1-x)(1-x^2)(1-x^3)\cdots \\ &= 1 + q_1x + q_2x^2 + \cdots. \end{aligned}$$

De nuevo, cada partición de  $n$  en partes distintas contribuye al coeficiente de  $x^n$ , pero ahora la contribución es  $(-1)^d$ , donde  $d$  es el número de partes. Por ejemplo, la partición  $7 = 1 + 2 + 4$  corresponde al término

$$(-x) \times (-x^2) \times (-x^4) = (-1)^3 x^7$$

y contribuye en  $-1$  a  $x^7$ . En general, cada partición de  $n$  con un número par de partes distintas contribuye en  $1$  a  $q_n$  y aquellas con un número impar contribuyen en  $-1$ . Así pues,

$$q_n = e_n - o_n,$$

donde

$$\begin{aligned} e_n &= p(n \mid \text{las partes son distintas y en número par}), \\ o_n &= p(n \mid \text{las partes son distintas y en número impar}). \end{aligned}$$

Es instructivo obtener los primeros términos de  $Q(x)$  multiplicando sucesivamente los factores  $1 - x^i$  para  $i = 1, 2, \dots$ . El lector que proceda concienzudamente (y correctamente) hasta  $i = 26$  hallará que

$$Q(x) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \dots$$

Hay varios aspectos misteriosos. Muchos de los coeficientes resultan ser  $0$  y los coeficientes no nulos son todos iguales a  $1$  o  $-1$ ; más aún, los signos parecen alternarse regularmente, dos signos  $+$  seguidos de dos signos  $-$ , y así sucesivamente. Utilizaremos la interpretación combinatoria de  $q_n$  para explicar este curioso comportamiento.

**Teorema 19.5.** Si  $e_n$  y  $o_n$  son como antes, entonces

$$e_n - o_n = \begin{cases} (-1)^m & \text{si } \frac{1}{2}m(3m \pm 1), \quad (m \geq 1), \\ 0 & \text{en otro caso.} \end{cases}$$

**DEMOSTRACIÓN:** Estableceremos una correspondencia  $\lambda \rightarrow \lambda^*$  que transforma las particiones contadas por  $e_n$  en aquellas contadas por  $o_n$ . Para la mayoría de los valores de  $n$  esta correspondencia será una biyección, de forma que  $e_n = o_n$ , pero si  $n = \frac{1}{2}m(3m-1)$  o  $n = \frac{1}{2}m(3m+1)$ , existirá una partición especial que impedirá la biyección.

Para una partición  $\lambda$  con partes distintas, sea  $s(\lambda)$  la menor parte de  $\lambda$ , y sea  $t(\lambda)$  la longitud de la sucesión de las partes que empiezan con la parte mayor y continúa mientras las partes decrecen en  $1$  en cada paso. En el diagrama de  $\lambda$ ,  $t(\lambda)$  está representado por la sucesión de marcas que empiezan en la esquina superior derecha y prosiguen en dirección suroeste.

Por ejemplo, si  $\lambda = [13567]$ , tenemos que  $s(\lambda) = 1$  y  $t(\lambda) = 3$  (véase la figura 19.3).

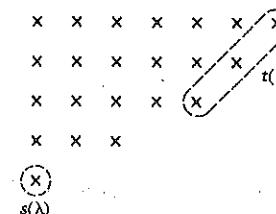


Fig. 19.3 Si  $\lambda = [13567]$ , entonces  $s(\lambda) = 1$  y  $t(\lambda) = 3$ .

Dada una partición  $\lambda$ , la definición de  $\lambda^*$  depende de  $s(\lambda)$  y de  $t(\lambda)$ .

*Caso 1:*  $s(\lambda) \leq t(\lambda)$ . En este caso,  $\lambda^*$  se obtiene eliminando la parte menor  $s(\lambda)$  y añadiendo  $1$  a cada una de las partes mayores (figura 19.4).

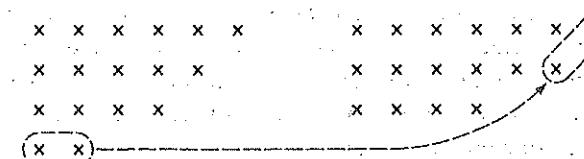


Fig. 19.4 La transformación  $\lambda \rightarrow \lambda^*$  cuando  $s(\lambda) \leq t(\lambda)$ .

*Caso 2:*  $s(\lambda) > t(\lambda)$ . En este caso,  $\lambda^*$  se obtiene eliminando  $1$  de cada una de las  $t(\lambda)$  partes mayores y creando una nueva parte menor  $t(\lambda)$ , tal como ilustra la figura 19.5.

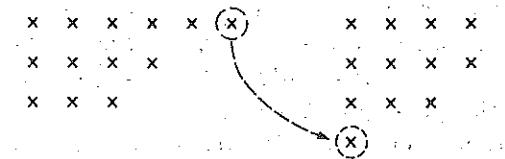


Fig. 19.5 La transformación  $\lambda \rightarrow \lambda^*$  cuando  $s(\lambda) > t(\lambda)$ .

En ambos casos, la transformación  $\lambda \rightarrow \lambda^*$  cambia en  $1$  el número

de partes, de modo que transforma una partición que tenga un número impar de partes en otra con un número par, y viceversa. Así pues, siempre que  $\lambda^*$  esté bien definida y sea una partición con partes distintas, la transformación  $\lambda \rightarrow \lambda^*$  es biyectiva. Sin embargo, hay dos situaciones excepcionales en que la definición no es correcta.

En el *Caso 1*, puede ocurrir que las zonas del diagrama que representan a  $s(\lambda)$  y  $t(\lambda)$  se solapen (figura 19.6). En este caso,  $\lambda^*$  no sería un diagrama aceptable para una partición. Esto ocurre precisamente cuando  $s(\lambda) = m$  y hay  $m$  partes:  $m, m+1, \dots, 2m-1$ . Entonces

$$n = m + (m+1) + \cdots + (2m-1) = \frac{1}{2}m(3m-1).$$

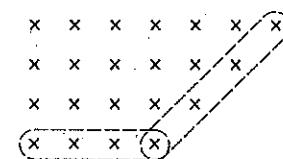


Fig. 19.6 La partición excepcional en el *Caso 1*, cuando  $s(\lambda) = t(\lambda) = 4$ .

En el *Caso 2*, también puede ocurrir que  $s(\lambda)$  y  $t(\lambda)$  se solapen (figura 19.7). En este caso,  $\lambda^*$  no es partición con partes distintas, ya que las dos partes menores son iguales.

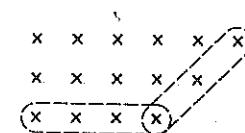


Fig. 19.7 La partición excepcional en el *Caso 2*, cuando  $s(\lambda) = 4$  y  $t(\lambda) = 3$ .

Esto ocurre precisamente cuando  $s(\lambda) = m+1$  y hay  $m$  partes:  $m, m+1, \dots, 2m$ . Por lo tanto,

$$n = (m+1) + (m+2) + \cdots + 2m = \frac{1}{2}m(3m+1).$$

En resumen, tenemos una biyección  $\lambda \rightarrow \lambda^*$  salvo si  $n = \frac{1}{2}m(3m \pm 1)$ . En los casos excepcionales hay una partición espúrea con  $m$  partes y que

contribuye en  $(-1)^m$  a la diferencia  $e_n - o_n$ . Esto demuestra el teorema.  $\square$

El teorema explica el misterioso comportamiento de los coeficientes en la expansión en serie de potencias

$$(1-x)(1-x^2)(1-x^3)\cdots = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots$$

Hemos demostrado que el coeficiente de  $x^n$  es  $e_n - o_n$  y que es cero a menos que  $n$  sea de la forma  $n = \frac{1}{2}m(3m \pm 1)$ . Los primeros enteros de esta forma son

$m$	1	2	3	4	5	5
$\frac{1}{2}(3m-1)$	1	5	12	22	35	51
$\frac{1}{2}(3m+1)$	2	7	15	26	40	57

Este resultado puede expresarse también como una identidad entre un producto infinito y una serie infinita:

$$\prod_{i=1}^{\infty} (1-x^i) = 1 + \sum_{m=1}^{\infty} (x^{\frac{1}{2}m(3m-1)} + x^{\frac{1}{2}m(3m+1)}).$$

En el siguiente apartado veremos que no se trata únicamente de una fórmula bonita.

### Ejercicios 19.5

1 Demostrar que el coeficiente de  $x^n$  en la expansión en serie de potencias de

$$(1+x)(1+x^2)(1+x^3)\cdots$$

es par salvo si  $n$  es de la forma  $\frac{1}{2}m(3m \pm 1)$ .

2 Sea  $q_{n,d}$  el número de particiones de  $n$  con  $d$  partes, todas distintas. Demostrar que

$$q_{n,d} = q_{n-d,d} + q_{n-d,d-1} \quad (1 \leq d \leq n).$$

3 Utilizar la recurrencia del ejercicio 2 para calcular  $q_{n,d}$  con  $1 \leq n \leq 22$  y  $1 \leq d \leq 6$ . Comprobar que la respuesta es compatible con el ejercicio 1.

4 Demostrar que la identidad misteriosa puede escribirse también como

$$\prod_{i=1}^{\infty} (1-x^i) = \sum_{m=-\infty}^{\infty} (-1)^m x^{\frac{1}{2}m(3m-1)}.$$

### 19.6 El cálculo de $p(n)$ .

Es posible calcular  $p(n)$  sin más que hacer una lista de las particiones de  $n$  en cierto orden (como en el ejercicio 19.7.13), pero es evidente que se trata de un método muy ineficiente. Podría mejorarse con un enfoque recursivo, como el del ejercicio 19.1.3, pero tampoco es éste un método demasiado eficiente. La identidad misteriosa del apartado anterior es la base para un buen procedimiento recursivo; éste es el método que vamos a estudiar.

El lector atento se habrá dado cuenta de que la función generadora  $P(x)$  de los números  $p(n)$  es inversa de la función generadora  $Q(x)$  de  $q_n = e_n - o_n$ ; en concreto,

$$\begin{aligned} P(x) &= (1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}\dots, \\ Q(x) &= (1-x)(1-x^2)(1-x^3)\dots \end{aligned}$$

De aquí se sigue que

$$\begin{aligned} P(x)Q(x) &= (1+p(1)x+p(2)x^2+\dots+p(n)x^n+\dots) \\ &\quad \times (1-x-x^2+x^5+x^7-x^{12}-x^{15}+\dots) \\ &= 1. \end{aligned}$$

El coeficiente de  $x^n$  ( $n \geq 1$ ) en el producto es cero. La regla de multiplicar series de potencias nos da la ecuación

$$\begin{aligned} p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) - p(n-12) - p(n-15) \\ + \dots &= 0. \end{aligned}$$

Podemos reescribirlo en la forma

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - \dots,$$

donde el miembro derecho contiene únicamente un número finito de términos, ya que sólo aparecen los  $p(n-k)$  con  $n-k \geq 0$ . Por ejemplo,

$$p(13) = p(12) + p(11) - p(8) - p(6) + p(1).$$

Estas fórmulas proporcionan un método recursivo eficiente para calcular los números  $p(n)$ . El cálculo puede disponerse como en la tabla 19.6.1, donde supondremos, por conveniencia, que los valores  $p(0) = 1$ ,  $p(1) = 1$ ,  $p(2) = 2$ ,  $p(3) = 3$ ,  $p(4) = 5$ ,  $p(5) = 7$ ,  $p(6) = 11$  son conocidos.

Tabla 19.6.1

n	7	8	9	10	11	12	13	14
$p(n-1)$	11	15	22	30	42	56	77	101
$p(n-2)$	7	11	15	22	30	42	56	77
$p(n-5)$	2	3	5	7	11	15	22	30
$p(n-7)$	1	1	2	3	5	7	11	15
$p(n-12)$	—	—	—	—	—	1	1	2
$p(n)$	15	22	30	42	56	77	101	135

Desde luego, para el cálculo de los siguientes  $p(n)$  son necesarias filas adicionales de la tabla.

Hemos cumplido nuestro propósito de hallar un método eficiente para calcular los  $p(n)$  —en los siguientes ejercicios veremos cuán eficiente es. Es notable que, aunque la forma final del método es simple, para justificarla es necesaria prácticamente toda la teoría desarrollada en el capítulo.

### Ejercicios 19.6

- Extender la tabla hasta  $p(20)$ .
- Hallar el mínimo  $n$  para el cual  $p(n) > 1000$ .
- Sea  $t(n)$  el número de términos en el miembro derecho de la ecuación de  $p(n)$ . Demostrar que

$$t(n) = \begin{cases} 2m-1 & \text{si } \frac{1}{2}m(3m-1) \leq n < \frac{1}{2}m(3m+1) \\ 2m & \text{si } \frac{1}{2}m(3m+1) \leq n < \frac{1}{2}(m+1)(3m+2). \end{cases}$$

Deducir que existe una constante  $K$  tal que  $t(n) \leq K\sqrt{n}$  para todo  $n \geq 1$ .

4 Demostrar que el número de sumas y restas necesarias para calcular  $p(n)$  por el método de este apartado es  $O(n^{3/2})$ .

## 19.7 Ejercicios diversos

1 Calcular  $p_5(9)$  y  $p_5(10)$ , donde  $p_k(n)$  es el número de particiones de  $n$  con  $k$  partes.

2 Usar los diagramas de Ferrers para demostrar que el número de particiones de  $n$  en las que cada parte es 1 o 2, es igual al número de particiones de  $n+3$  que tienen exactamente dos partes distintas.

3 Demostrar que el número de particiones de  $n$  en dos partes como máximo es  $\lfloor \frac{1}{2}n \rfloor$ .

4 Hallar las funciones generadoras de los números de:

- (i) particiones de  $n$  en las que cada parte es como máximo 5;
- (ii) particiones de  $n$  en las que sólo las partes pares pueden aparecer más de una vez;
- (iii) particiones de  $n$  en las que cada parte es un múltiplo de 3.

5 Dar una descripción alternativa de  $p(n) - p(n-1)$  como el número de particiones de  $n$  que poseen cierta propiedad.

6 Demostrar que

$$p(n+2) - 2p(n+1) + p(n) \geq 0.$$

7 Demostrar que el número de particiones de  $2n$  en tres partes, tales que la suma de dos partes cualesquiera es mayor que la tercera, es igual al número de particiones de  $n$  con tres partes exactamente.

8 Demostrar que el número de particiones de  $n$  en  $k$  partes satisface

$$p_k(n) \geq \frac{1}{k!} \binom{n-1}{k-1}.$$

9 Comprobar que si  $\lambda$  es una partición con partes  $\lambda_1, \lambda_2, \dots, \lambda_r$  tales que  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r$ , entonces las partes de la partición conjugada  $\lambda'$  vienen dadas por

$$\lambda'_i = \text{el número de partes de } \lambda \text{ no menores que } i \quad (1 \leq i \leq \lambda_1).$$

10 Sean  $\lambda$  y  $\mu$  particiones de  $n$  con partes  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r$  y  $\mu_1 \geq \mu_2 \geq \dots \geq \mu_s$ , respectivamente. Demostrar que  $\lambda$  y  $\mu$  son conjugadas si, y sólo si,

$$\lambda_1 = s, \quad \mu_1 = r, \quad \lambda_i + \mu_j \neq i + j - 1 \quad (1 \leq i \leq r, 1 \leq j \leq s).$$

11 Demostrar que el número de particiones de  $n-m$  en  $k-1$  partes exactamente, ninguna de las cuales es mayor que  $m$ , es igual al número de particiones de  $n-k$  en  $m-1$  partes, ninguna de las cuales es mayor que  $k$ .

12 Demostrar que el número de particiones de  $n$  en las que ninguna parte ocurre más de  $2^{k+1}-1$  veces, es igual al número de particiones de  $n$  en las que ningún múltiplo de  $2^k$  aparece más de una vez como una parte.

13 La siguiente regla proporciona un método para enumerar todas las particiones de  $n$  en orden lexicográfico. La primera partición es  $[n]$ . Supongamos que hemos llegado a una partición  $\lambda$  con partes  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r$ . Entonces la siguiente partición se obtiene así:

- (i) si  $\lambda_r \neq 1$ , entonces las partes de la siguiente partición son  $\lambda_1, \lambda_2, \dots, \lambda_{r-1}, \lambda_r - 1, 1$ ;
- (ii) si  $\lambda_r = \lambda_{r-1} = \dots = \lambda_{r-s+1}$  pero  $\lambda_{r-s} = x \neq 1$ , entonces las partes de la siguiente partición se obtienen sustituyendo  $\lambda_{r-s}, \lambda_{r-s+1}, \dots, \lambda_r$  por  $x-1, x-1, x-1, \dots, x-1, y$ , donde  $1 \leq y \leq x-1$  y el número de partes iguales a  $x-1$  se elige de forma que el resultado sea una partición de  $n$ .

Utilizar esta regla para enumerar las particiones de 8.

14 Escribir un programa basado en el algoritmo descrito en el ejercicio anterior.

15 Escribir un programa que calcule  $p(n)$  para  $n \leq 100$  mediante el método del apartado 19.6.

16 El mayor cuadrado contenido en la esquina superior izquierda de un diagrama de Ferrers, se conoce como el cuadrado de Durfee. Demostrar que para partición autoconjigada de  $n$  existe un entero  $k$  y una partición de  $n$  en una parte de tamaño  $k^2$  (el cuadrado de Durfee) y otras partes de tamaño par no mayores que  $2k$ . Deducir que

$$(1+x)(1+x^3)(1+x^5)\cdots = 1 + \sum_{k=1}^{\infty} \frac{x^{k^2}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}.$$

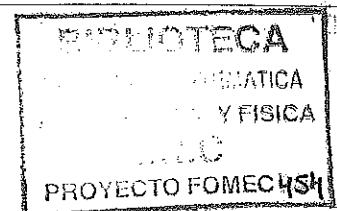
17 Utilizar la construcción del cuadrado de Durfee para demostrar que la función generadora  $P(x)$  de las particiones satisface la identidad

$$P(x) = 1 + \sum_{k=1}^{\infty} \frac{x^{k^2}}{(1-x)^2(1-x^2)^2\cdots(1-x^k)^2}.$$

18 Demostrar que

$$(1+x^2)(1+x^4)(1+x^6)\cdots = 1 + \sum_{k=1}^{\infty} \frac{x^{k(k+1)}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}.$$

## 20 Simetría y enumeración



### 20.1 El índice de ciclos de un grupo de permutaciones

En este último capítulo del libro volveremos al estudio de problemas enumerativos en los que interviene un grupo de permutaciones. Ampliaremos las técnicas básicas desarrolladas en el capítulo 14 con algo de álgebra formal basada en la teoría de las funciones generadoras, y de ahí deduciremos un elegante resultado matemático con aplicaciones prácticas importantes.

Como ejemplo de problema representativo, consideremos de cuántas maneras podemos asignar uno de los colores blanco o negro a las esquinas de un cuadrado. Como hay dos colores y cuatro esquinas, hay  $2^4 = 16$  posibilidades en total. Pero si tenemos en cuenta la simetría del cuadrado, vemos que algunas de las posibilidades son esencialmente la misma. Por ejemplo, la primera coloración de la figura 20.1 es la misma que la segunda después de una rotación de 180 grados.

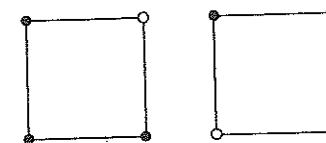


Fig. 20.1 Dos coloraciones indistinguibles.

Visto de esta manera, consideraremos dos coloraciones indistinguibles si una simetría del cuadrado transforma una en otra. En este ejemplo, es fácil hallar las coloraciones indistinguibles por tanteo: no hay más que seis, tal como muestra la figura 20.2.

Al estudiar problemas de este tipo, en general, la herramienta más importante es una notación compacta que recoja la información sobre la

estructura en ciclos de las permutaciones de un grupo. Sea  $G$  un grupo de permutaciones de un conjunto  $X$ ; con frecuencia, tomaremos  $X$  como el conjunto  $\{1, 2, \dots, n\}$ . Cada elemento  $g$  de  $G$  puede descomponerse en ciclos  $\alpha_i$  de longitud  $i$  ( $1 \leq i \leq n$ ). Recordemos que el *tipo* de  $g$  es la partición de  $n$  correspondiente

$$[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}].$$

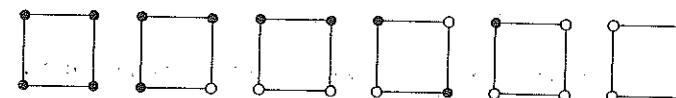


Fig. 20.2 Las seis coloraciones distinguibles.

Desde luego, se tiene que  $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$ . Asociaremos a  $g$  la expresión

$$\zeta_g(x_1, x_2, \dots, x_n) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

donde las  $x_i$  ( $1 \leq i \leq n$ ) no son más que, de momento, símbolos formales como la  $x$  de un polinomio. Por ejemplo, si  $G$  es el grupo de las simetrías de un cuadrado consideradas como permutaciones de los vértices 1, 2, 3 y 4, las expresiones  $\zeta_g$  vienen dadas por la tabla 20.1.1. Nótese que, a pesar de que los 1-ciclos se omiten de la notación en ciclos de  $g$ , es importante incluirlos en  $\zeta_g$ .

Tabla 20.1.1

$g$	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\zeta_g$
id	4	—	—	—	$x_1^4$
(1234)	—	—	—	1	$x_4$
(13)(24)	—	2	—	—	$x_2^2$
(1432)	—	—	—	1	$x_4$
(12)(34)	—	2	—	—	$x_2^2$
(14)(23)	—	2	—	—	$x_2^2$
(13)	2	1	—	—	$x_1^2 x_2$
(24)	2	1	—	—	$x_1^2 x_2$

La suma formal de los  $\zeta_g$  para todos los  $g$  de  $G$  es un “polinomio” en  $x_1, x_2, \dots, x_n$ . Si dividimos por  $|G|$  obtendremos el *índice de ciclos* del grupo de permutaciones:

$$\zeta_G(x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} \zeta_g(x_1, x_2, \dots, x_n).$$

Por ejemplo, el índice de ciclos del grupo del cuadrado, definido como antes, es

$$\frac{1}{8}(x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4),$$

donde hemos agrupado los términos que corresponden a permutaciones del mismo tipo. En general, tendremos que

$$\zeta_G(x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum c(\alpha_1, \alpha_2, \dots, \alpha_n) x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

donde  $c(\alpha_1, \dots, \alpha_n)$  es el número de permutaciones de  $G$  de tipo  $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$  y la suma es sobre todos los tipos (es decir, sobre todas las particiones de  $n$ ). Vemos así que el índice de ciclos es como el índice de un buen libro: es una lista que nos dice algo acerca de las permutaciones contenidas en  $G$ .

### Ejercicios 20.1

- Hallar por tanteo todas las coloraciones distinguibles de los vértices de un triángulo equilátero si hay tres colores disponibles. (Considerar el triángulo como un naipe coloreado por ambas caras.)
- Hay que decorar una barra uniforme de un metro de largo dividiendo su superficie en cinco bandas de 20 cm y coloreando cada banda en rojo o en azul. ¿De cuántas maneras esencialmente distintas puede hacerse?
- Hallar el índice de ciclos de
  - el grupo de simetrías de un triángulo equilátero consideradas como permutaciones de los vértices;
  - el grupo alternado  $A_4$ ;
  - el grupo simétrico  $S_5$ .

4 Se consideran los grafos de la figura 20.3 como estructuras planas en el espacio tridimensional. Hallar en cada caso el índice de ciclos del grupo de simetrías, considerado como un grupo de permutaciones de los vértices.

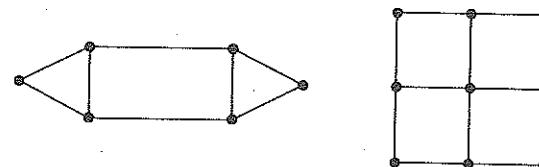


Fig. 20.3 Hallar los índices de ciclos.

## 20.2 Simetría cíclica y diedral

Para los desarrollos matemáticos posteriores necesitaremos una pequeña colección de índices de ciclos útiles, de modo que en este apartado y en el siguiente nos ocuparemos de algunos ejemplos importantes.

La simetría que ocurre con más frecuencia es la asociada a un objeto circular, como un disco coloreado o un collar. Cuando nos enfrentamos a un problema en el que interviene un objeto de este tipo, antes de empezar hay que aclarar una cuestión crucial: ¿nos permiten las condiciones del problema darle la vuelta al objeto (o reflejarlo en un espejo)? Por ejemplo, si tenemos un disco dividido en sectores iguales sólo por una cara, es evidente que no estará permitido darle la vuelta. En la figura 20.4 hay dos coloraciones en blanco y negro de una cara de un disco que, en estas condiciones, no son equivalentes.

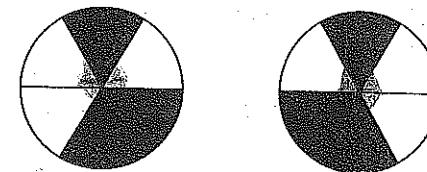


Fig. 20.4 Dos coloraciones no equivalentes de un disco.

Por otra parte, si tenemos un collar circular de cuentas coloreadas, lo normal es que sí esté permitido darle la vuelta; en consecuencia, los dos collares de la figura 20.5 deberían considerarse idénticos.

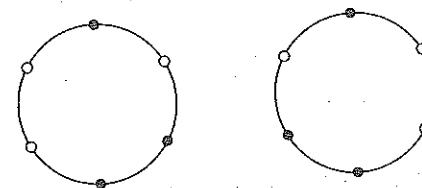


Fig. 20.5 Dos collares equivalentes.

Empezaremos por considerar la situación en que no está permitido dar la vuelta. En este caso, el grupo de simetrías es un grupo *cíclico*. Supongamos que marcamos los vértices de un  $n$ -ágono regular en el sentido de las manecillas del reloj con los símbolos  $1, 2, \dots, n$ . Una rotación de  $2\pi/n$  alrededor del centro del  $n$ -ágono corresponde en este caso a la permutación de los vértices

$$\pi = (123 \dots n).$$

El grupo de rotaciones del  $n$ -ágono es el grupo cíclico de orden  $n$  generado por  $\pi$ , es decir,

$$C_n = \{\text{id}, \pi, \pi^2, \dots, \pi^{n-1}\}.$$

Por ejemplo, si  $n = 6$ , las permutaciones y las expresiones  $\zeta_{\pi^i}$  asociadas son las siguientes:

id	(seis)	1-ciclos	$x_1^6$
$(123456)$	(un 6-ciclo)	$x_6$	
$(135)(246)$	(dos 3-ciclos)	$x_3^2$	
$(14)(25)(36)$	(tres 2-ciclos)	$x_2^3$	
$(153)(264)$	(dos 3-ciclos)	$x_3^2$	
$(165432)$	(un 6-ciclo)	$x_6$	

El índice de ciclos es, por lo tanto,  $\frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6)$ . El caso general es similar; los detalles los proporciona el siguiente teorema.

**Teorema 20.2.1.** Sea  $C_n$  el grupo cíclico de permutaciones generado por  $\pi = (123\dots n)$ . Entonces para cada divisor  $d$  de  $n$  hay  $\phi(d)$  permutaciones de  $C_n$  que tienen  $n/d$  ciclos de longitud  $d$ . El índice de ciclos es, por lo tanto,

$$\zeta_{C_n}(x_1, x_2, \dots, x_n) = \frac{1}{n} \sum_{d|n} \phi(d) x_d^{n/d}$$

**DEMOSTRACIÓN:** De acuerdo con el teorema 13.9, un grupo cíclico de orden  $n$  contiene  $\phi(d)$  elementos de orden  $d$  para cada divisor  $d$  de  $n$ . En este caso, las  $\phi(d)$  permutaciones son las de la forma  $\pi^{kn/d}$ , donde  $1 \leq k \leq d$  y  $\text{mcd}(k, d) = 1$ . Sólo nos queda demostrar que cada una de estas permutaciones posee  $n/d$  ciclos de longitud  $d$ .

Sea  $m$  la longitud del ciclo más corto de la permutación  $\pi^i$  ( $1 \leq i \leq n-1$ ) y supongamos que  $x$  está en un ciclo de longitud  $m$ . Entonces

$$\pi^{im}(x) = (\pi^i)^m(x) = x.$$

Para cada  $y$  de  $\{1, 2, \dots, n\}$ , tanto  $x$  como  $y$  están en el ciclo  $\pi$ , de manera que  $y = \pi^r(x)$  para algún  $r$ . Ahora bien,

$$(\pi^i)^m(y) = \pi^{im}\pi^r(x) = \pi^r\pi^{im}(x) = \pi^r(x) = y,$$

de forma que  $y$  está en un ciclo de  $\pi^i$  cuya longitud divide a  $m$ . Pero  $m$  es la longitud mínima de un ciclo, con lo que este ciclo tiene longitud  $m$ . Así pues, todos los ciclos de  $\pi^i$  tienen la misma longitud  $m$ . Si el orden de  $\pi^i$  es  $d$ , habrá de ser  $d = m$ , con lo que hay  $n/d$  ciclos de longitud  $d$ , tal como afirmábamos.  $\square$

Vale la pena señalar que si hacemos la sustitución  $x_i = 1$  ( $1 \leq i \leq n$ ) en el resultado anterior, recuperaremos la fórmula clásica

$$\frac{1}{n} \sum_{d|n} \phi(d) = 1$$

que obtuvimos por primera vez en el apartado 3.3.

Pasamos ahora al caso en que se permite la simetría especular. En primer lugar, supongamos que  $n$  es par y  $n \geq 4$ , y sea  $n' = \frac{1}{2}n$ , de forma que los vértices de nuestro  $n$ -ágono son  $1, 2, \dots, n', n' + 1, \dots, n$ . Girar

el polígono respecto de la bisectriz perpendicular al lado  $1n$  es lo mismo que efectuar una “reflexión” sobre este eje (figura 20.6) y la permutación correspondiente es

$$\sigma = (1\ n)(2\ n-1)\cdots(n'\ n'+1).$$

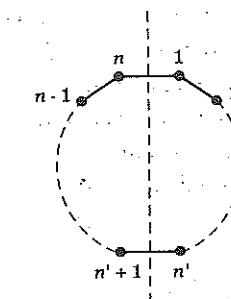


Fig. 20.6 Simetría de un polígono par.

Si tomamos  $\pi = (123\dots n)$  como antes, tenemos que

$$\sigma\pi = (1\ n-1)(2\ n-2)\cdots(n'-1\ n'+1)(n')(n),$$

que representa una reflexión respecto del eje  $nn'$ .

Hay  $n' = \frac{1}{2}n$  reflexiones sobre las bisectrices perpendiculares a los lados y corresponden a las permutaciones

$$\sigma, \sigma\pi^2, \sigma\pi^4, \dots, \sigma\pi^{n-2}.$$

También hay  $n' = \frac{1}{2}n$  reflexiones sobre los ejes que unen vértices opuestos y estas corresponden a las permutaciones

$$\sigma\pi, \sigma\pi^3, \sigma\pi^5, \dots, \sigma\pi^{n-1}.$$

Tenemos pues un grupo de  $2n$  permutaciones, las  $n$  rotaciones  $\pi^i$  y las  $n$  reflexiones  $\sigma\pi^i$ . Se conoce con el nombre de grupo diedral de orden  $2n$  y lo denotaremos por  $D_{2n}$ . (Advertencia: algunos autores escriben  $D_n$  en lugar de  $D_{2n}$ .)

Si  $n$  es impar, pongamos  $n = 2n' + 1$ , se tienen también  $n$  reflexiones; aunque ahora son todas del mismo tipo: reflexiones sobre un eje que une un vértice con el punto medio del lado opuesto. Por ejemplo, si elegimos  $n'$  como vértice (figura 20.7), se tiene que

$$\sigma = (1\ n)(2\ n - 1) \cdots (n' - 1\ n' + 1)(n').$$

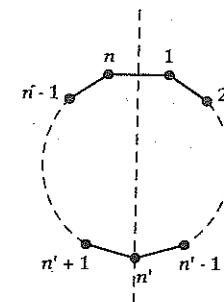


Fig. 20.7 Simetría de un polígono impar.

De nuevo tenemos un grupo diedral de orden  $2n$  que consta de las  $n$  rotaciones  $\pi^i$  y de las  $n$  reflexiones  $\sigma\pi^i$  ( $0 \leq i \leq n - 1$ ).

**Teorema 20.2.** El índice de ciclos de  $D_{2n}$  es

$$\frac{1}{2} \zeta_{C_n}(x_1, x_2, \dots, x_n) + \begin{cases} \frac{1}{4} (x_2^{n/2} + x_1^2 x_2^{n/2-1}) & \text{si } n \text{ es par,} \\ \frac{1}{2} x_1 x_2^{(n-1)/2} & \text{si } n \text{ es impar.} \end{cases}$$

**DEMOSTRACIÓN:** En el caso par,  $D_{2n}$  contiene  $n$  elementos de  $C_n$  junto con  $\frac{1}{2}n$  permutaciones (como  $\sigma$ ) de tipo  $[2^{n/2}]$  y  $\frac{1}{2}n$  permutaciones (como  $\sigma\pi$ ) de tipo  $[1^2 2^{n/2-1}]$ . Así pues,  $\zeta_{D_{2n}}(x_1, x_2, \dots, x_n)$  es igual a

$$\frac{1}{2n} \left( \sum_{d|n} \phi(d) x_d^{n/d} + \frac{n}{2} x_2^{n/2} + \frac{n}{2} x_1^2 x_2^{n/2-1} \right)$$

y se reduce a la expresión del enunciado. En el caso impar tenemos las  $n$  permutaciones de  $C_n$  junto con  $n$  permutaciones de tipo  $[12^{n/2-1}]$  y el resultado se obtiene como antes.  $\square$

### Ejercicios 20.2

- Escribir los índices de ciclos de  $C_{12}$ ,  $D_{12}$  y  $D_{14}$  con todos sus términos.
  - Calcular el índice de ciclos de  $D_{2p}$  si  $p$  es un primo impar y demostrar que
- $$\zeta_{D_{2p}}(r, r, \dots, r)$$
- es un entero para todo entero positivo  $r$ .
- Hallar todos los subgrupos de  $D_{12}$  y hacer un esquema del retículo de sus subgrupos.
  - Los grupos  $C_{12}$ ,  $D_{12}$  y  $A_4$  tienen todos orden 12. Hallar el número de elementos de cada orden en cada grupo y concluir que no hay dos de ellos isomorfos.
  - Uno de los grupos  $C_4 \times C_3$ ,  $C_6 \times C_2$  o  $C_6 \times D_2$  no es isomorfo a ninguno de los grupos estudiados en el ejercicio 4. ¿Cuál es?

### 20.3 Simetría en tres dimensiones

La mayoría de la gente se familiariza con las propiedades de simetría de un cubo ordinario (figura 20.8) en su tierna infancia, pero la descripción matemática de tales propiedades no suele formar parte de su educación. En este apartado intentaremos poner remedio a esta deficiencia.

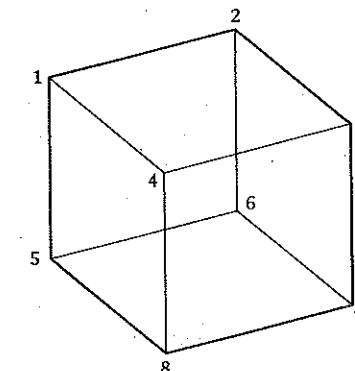


Fig. 20.8 Un cubo.

Empezaremos con una cuestión general importante: al discutir la simetría de objetos tridimensionales sólo consideraremos simetrías *rotacionales*. El lector quizás se pregunte por qué excluimos las simetrías por reflexión. Después de todo, al tratar con collares hemos de tener en cuenta las reflexiones si queremos obtener un modelo correcto de la situación. Esto es así porque podemos obtener una reflexión de un collar bidimensional utilizando una rotación (dándole la vuelta) en tres dimensiones. Pero no hay manera de conseguir una reflexión de un objeto sólido tridimensional mediante un movimiento efectivo del objeto.

Por ejemplo, en la figura 20.8, la reflexión del cubo en el plano horizontal a través del centro, corresponde a la permutación  $(15)(26)(37)(48)$  de los vértices, pero no existe ningún movimiento físico del cubo que efectúe esta permutación.

Teniendo esto en cuenta, daremos una tabla de las simetrías rotacionales del cubo (tabla 20.3.1); hay 24 en total, de acuerdo con el ejercicio 14.3.2. Clasificaremos las rotaciones según el eje y el orden de cada clase, y en cada caso daremos una permutación representativa de los vértices (numerados como en la figura 20.8). Nótese que una rotación de orden  $m$  es lo mismo que una rotación de ángulo  $2\pi/m$ . Así pues, el índice de ciclos del grupo, considerado como grupo de permutaciones de los vértices, es

$$\frac{1}{24}(x_1^8 + 8x_1^2x_3^2 + 9x_2^4 + 6x_4^2).$$

Tabla 20.3.1

Eje	Orden	Permutación	Número
Recta que une puntos medios de caras opuestas	4	$(1234)(5678)$	6
El mismo	2	$(13)(24)(57)(68)$	3
Recta que une puntos medios de lados opuestos	2	$(15)(24)(37)(46)$	6
Recta que une esquinas opuestas	3	$(245)(386)$	8
	1	id	1

En la práctica, es frecuente que un problema haga referencia a las caras y no a los vértices del cubo (los cubos con que juegan los niños

tienen coloreadas las caras y no los vértices!). Una forma de tratar este tipo de problemas es trabajar con permutaciones de las caras: por ejemplo, la primera simetría de la tabla anterior induce una permutación  $(A)(B)(CDEF)$  de las seis caras, donde  $A$  y  $B$  son las caras superior e inferior de la figura 20.8,  $C$  es la cara frontal, etc. También podemos considerar el problema bajo un punto de vista distinto utilizando la construcción que se muestra en la figura 20.9.

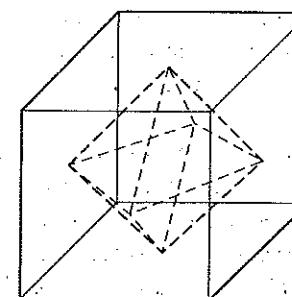


Fig. 20.9 Un cubo y su octaedro dual.

Añadimos un nuevo vértice en el centro de cada cara del cubo y unimos dos de los nuevos vértices mediante una arista si las caras correspondientes son adyacentes. De esta forma obtenemos un octaedro regular inscrito en el cubo, conocido como el *dual* del cubo. Cada simetría del cubo es una simetría del octaedro, y viceversa. Como las caras del cubo corresponden a los vértices del octaedro, cualquier problema acerca del primero puede traducirse en un problema sobre este último. En particular, el índice de ciclos del grupo de simetría que actúa sobre las caras del cubo es el mismo que el índice de ciclos del grupo de simetría que actúa sobre los vértices del octaedro. Este índice puede encontrarse en la tabla que cierra este apartado.

Hasta ahora hemos discutido únicamente grupos de simetrías rotacionales en tres dimensiones. Es evidente que los grupos cíclicos  $C_n$  y diedrales  $D_{2n}$  también aparecen en este contexto, por ejemplo, como grupos de rotaciones de un prisma con  $n$  caras (figura 20.10). Podría esperarse que hubiera muchas otras clases de grupos de simetrías rotacionales, pero de hecho no es así. Aparte de los cíclicos, diedrales y del cúbico-octaédrico,

sólo existen otros dos grupos de simetrías rotacionales en tres dimensiones. Este resultado puede obtenerse a partir de la teoría desarrollada en el capítulo 14 y su demostración se esboza en los ejercicios 14.7.19–21. Para nuestros propósitos, será suficiente señalar que los dos grupos restantes también están asociados a poliedros regulares.

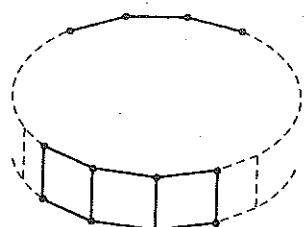


Fig. 20.10 Un prisma con  $n$  lados.

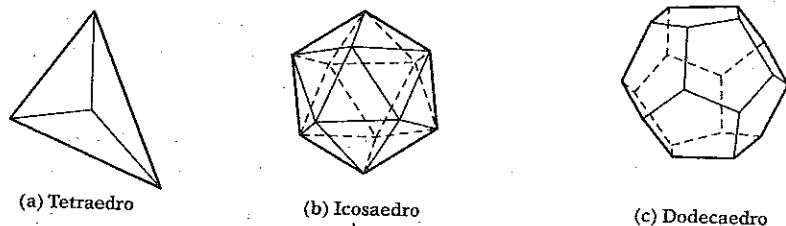


Fig. 20.11 Poliedros regulares.

En primer lugar, tenemos el grupo de rotaciones del tetraedro regular (figura 20.11a) que discutimos en el apartado 14.3. Como grupo de permutaciones de los vértices, contiene la identidad, tres permutaciones de tipo  $[2^2]$  y ocho permutaciones de tipo  $[13]$ . Como grupo de permutaciones de las caras tiene la misma forma, lo cual corresponde al hecho de que el dual del tetraedro es otro tetraedro.

En segundo lugar tenemos el grupo de rotaciones del icosaedro regular (figura 20.11b) y su dual, el dodecaedro regular (figura 20.11c). Este grupo fascinante posee varias propiedades notables, pero nos contentaremos con indicar los índices de ciclos. La tabla 20.3.2 nos da el índice de ciclos de cada grupo  $G$  de simetrías rotacionales que actúa como un grupo de

permutaciones del conjunto  $X$  de los vértices de un poliedro regular en el espacio tridimensional.

Tabla 20.3.2

Poliedro	$ X $	$ G $	Índice de ciclos
Tetraedro	4	12	$\frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2)$
Octaedro	6	24	$\frac{1}{24}(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2)$
Cubo	8	24	$\frac{1}{24}(x_1^8 + 8x_1^2x_3^2 + 9x_2^4 + 6x_4^2)$
Icosaedro	12	60	$\frac{1}{60}(x_1^{12} + 24x_1^2x_5^2 + 15x_2^6 + 20x_3^4)$
Dodecaedro	20	60	$\frac{1}{60}(x_1^{20} + 20x_1^2x_3^6 + 15x_2^{10} + 24x_5^4)$

### Ejercicios 20.3

1 En el ejercicio 14.3.1 demostramos que el grupo de simetrías rotacionales de un tetraedro regular es isomorfo al grupo alternado  $A_4$ , es decir, al grupo de las permutaciones pares de los vértices. Demostrar que una permutación impar de los vértices corresponde a una reflexión del tetraedro, o bien a una reflexión seguida de una rotación.

2 Hallar el índice de ciclos del grupo de simetrías rotacionales del tetraedro, considerado como grupo de permutaciones de las aristas.

3 El índice de ciclos dado anteriormente especifica los tipos de las permutaciones que corresponden a las simetrías rotacionales del grupo del dodecaedro. Numerar los vértices del dodecaedro (utilizando la figura 20.11c) y escribir una permutación de cada tipo.

4 Obtener una permutación que corresponda a una reflexión del dodecaedro.

### 20.4 El número de coloraciones no equivalentes

En este apartado volvemos al problema general de hallar el número de coloraciones distinguibles cuando interviene un grupo de permutaciones. Un ejemplo sencillo, que discutimos en el apartado 20.1, es el de colorear en

blanco y negro los vértices de un cuadrado: en este caso hay 16 coloraciones en total, pero sólo 6 son esencialmente distintas si tenemos en cuenta la simetría (figura 20.2).

En general, supongamos que tenemos un grupo  $G$  de permutaciones de un  $n$ -conjunto  $X$  y que podemos asignar a cada elemento de  $X$  uno entre  $r$  colores. Si indicamos el conjunto de colores por  $K$ , entonces una *coloración* no es más que una función  $\omega$  de  $X$  en  $K$ . Hay  $r^n$  coloraciones en total; denotaremos este conjunto por  $\Omega$ .

Ahora bien, cada permutación de  $g$  de  $G$  induce una permutación  $\hat{g}$  de  $\Omega$  de la siguiente forma. Dada una coloración  $\omega$ , definimos  $\hat{g}(\omega)$  como la coloración que asigna a  $x$  el color que  $\omega$  asigna a  $g(x)$ , es decir,

$$(\hat{g}(\omega))(x) = \omega(g(x)).$$

La definición se ilustra en la figura 20.12, donde  $g$  es la rotación de  $90^\circ$  en sentido horario y  $\omega$  es la coloración que se muestra a la derecha.

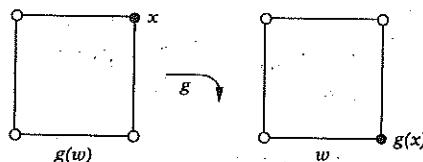


Fig. 20.12 Ilustración de la definición de  $\hat{g}(\omega)$ .

La función que transforma  $g$  en  $\hat{g}$  es la representación de  $G$  como un grupo  $\hat{G}$  de permutaciones de  $\Omega$ . Dos coloraciones son indistinguibles si una puede transformarse en la otra mediante alguna permutación  $\hat{g}$ , es decir, si pertenecen a la misma órbita de  $\hat{G}$  en  $\Omega$ . Así pues, el número de coloraciones distinguibles (también diremos *no equivalentes*) no es más que el número de órbitas de la acción de  $\hat{G}$  sobre  $\Omega$ .

Recordemos que el teorema 14.4 nos daba una fórmula general del número de órbitas. Pero antes de aplicarlo comprobaremos que la representación  $g \rightarrow \hat{g}$  es fiel, de forma que el grupo imagen  $\hat{G}$  será isomorfo a  $G$ . Supongamos que  $\hat{g}_1 = \hat{g}_2$ , con lo que

$$(\hat{g}_1(\omega))(x) = (\hat{g}_2(\omega))(x)$$

y, en consecuencia,

$$\omega(g_1(x)) = \omega(g_2(x)) \quad (\omega \in \Omega, x \in X).$$

Como la ecuación es cierta para todo  $\omega$ , también lo es particular para la coloración que asigna un color especificado a  $g_1(x)$  y otro color a los restantes elementos de  $X$ . En este caso la ecuación implica que  $g_1(x) = g_2(x)$  para todo  $x$  de  $X$  y concluimos que  $g_1 = g_2$ . Por lo tanto, la representación  $g \rightarrow \hat{g}$  es fiel y estamos listos para aplicar el teorema 14.4. La elegancia del resultado justifica las preparaciones.

**Teorema 20.4.** Si  $G$  es un grupo de permutaciones de  $X$  y  $\zeta_G(x_1, \dots, x_n)$  es su índice de ciclos, entonces el número de coloraciones no equivalentes de  $X$  con  $r$  colores es

$$\zeta_G(r, r, \dots, r).$$

**DEMOSTRACIÓN:** Hemos demostrado que  $|G| = |\hat{G}|$ . La fórmula que da el número de órbitas de  $\hat{G}$  en  $\Omega$  es

$$\frac{1}{|\hat{G}|} \sum_{\hat{g} \in \hat{G}} |F(\hat{g})| = \frac{1}{|G|} \sum_{g \in G} |F(g)|,$$

donde  $F(\hat{g})$  es el conjunto de coloraciones fijas por  $\hat{g}$ .

Sea  $\omega$  una coloración fija por  $\hat{g}$ , de modo que  $\hat{g}(\omega) = \omega$ , y sea  $(xyz\dots)$  un ciclo de  $g$ . Tenemos que

$$\omega(y) = \omega(g(x)) = (\hat{g}(\omega))(x) = \omega(x),$$

con lo que  $\omega$  asigna el mismo color a  $x$  que a  $y$ . Por el mismo argumento, podemos demostrar que  $y$  y  $z$  tienen el mismo color, y así sucesivamente hasta demostrar que  $\omega$  es constante en cada ciclo de  $g$ . Si  $g$  tiene  $k$  ciclos, el número de coloraciones con esta propiedad es exactamente  $r^k$ , ya que podemos colorear un elemento de cada ciclo arbitrariamente y los colores restantes están ya determinados. Si  $g$  tiene  $\alpha_i$  ciclos de longitud  $i$  ( $1 \leq i \leq n$ ), tendremos  $\alpha_1 + \dots + \alpha_n = k$  y

$$|F(\hat{g})| = r^k = r^{(\alpha_1 + \dots + \alpha_n)} = \zeta_g(r, r, \dots, r).$$

Si sustituimos en la fórmula de órbitas anterior, el resultado que se obtiene es precisamente  $\zeta_G(r, r, \dots, r)$ .  $\square$

El teorema implica que el problema de hallar el número de coloraciones no equivalentes si hay  $r$  colores disponibles puede reducirse al problema de calcular el índice de ciclos. Si el índice de ciclos es conocido, para obtener el resultado no tenemos más que sustituir cada  $x_1, \dots, x_n$  por  $r$ . Por ejemplo, el número de coloraciones no equivalentes de los vértices de un cuadrado es

$$\frac{1}{8}(r^4 + 2r^3 + 3r^2 + 2r),$$

fórmula que se obtiene haciendo  $x_1 = x_2 = x_3 = x_4 = r$  en el índice de ciclos calculado en el apartado 20.1. Si  $r = 2$ , obtenemos

$$\frac{1}{8}(16 + 16 + 24 + 4) = 6,$$

que coincide con la figura 20.2. A partir de los índices de ciclos calculados en los apartados 20.2 y 20.3, pueden obtenerse fórmulas parecidas para otros polígonos y poliedros regulares.

Para variar, daremos un ejemplo relativo a la simetría de un polígono irregular: un rectángulo.

**Ejemplo.** Los participantes en el Clásico Maratón de la Universidad de Folornia (instaurado el año pasado) no se distinguen, como es costumbre, por el número de la camiseta, sino por insignias rectangulares hechas con telas de colores, tal como muestra la figura 20.13. Desgraciadamente, la mayor parte de los corredores son eminentes profesores, propensos a enganchar las insignias boca abajo o con el anverso en el lugar del reverso (o de ambos modos si son de la Facultad de Medicina). Si este año pretenden competir 160 corredores, ¿cuál es el mínimo número de colores necesario para hacer las insignias?

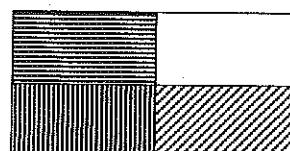


Fig. 20.13 El último avance tecnológico de la Universidad de Folornia.

**SOLUCIÓN:** Los segmentos de la insignia pueden identificarse con los vértices del rectángulo, que numeraremos 1, 2, 3 y 4 en sentido horario con el 1 en el vértice superior izquierdo. El grupo a tener en cuenta consiste en las permutaciones

id	(posición correcta)
(13)(24)	(boca abajo)
(12)(34)	(anverso en el reverso)
(14)(23)	(los de Medicina).

Así pues, el índice de ciclos del grupo del rectángulo es

$$\frac{1}{4}(x_1^4 + 3x_2^2)$$

y el número de insignias con  $r$  colores es  $\frac{1}{4}(r^4 + 3r^2)$ . El mínimo  $r$  para el cual

$$\frac{1}{4}(r^4 + 3r^2) \geq 160$$

es 5; éste es el número de colores necesario.  $\square$

#### Ejercicios 20.4

1 Utilizar la tabla de índices de ciclos del apartado 20.3 para obtener el número de maneras de colorear con  $r$  colores:

- (i) los vértices de un tetraedro;
- (ii) las caras de un tetraedro;
- (iii) las caras de un cubo.

2 Hallar el índice de ciclos del grupo de simetrías de una barra uniforme dividida longitudinalmente en  $m$  partes iguales (los casos  $m$  par y  $m$  impar han de tratarse por separado). Hallar el número de maneras de colorear las partes si hay  $r$  colores disponibles.

3 ¿De cuántas maneras no equivalentes pueden colorearse con rojo, blanco y azul las caras de un dodecaedro regular?

4 Se divide un círculo por una cara en ocho sectores iguales y cada sector se pinta de rojo, verde o amarillo. ¿Cuántos discos diferentes pueden obtenerse de este modo?

## 20.5 Conjuntos de coloraciones y funciones generadoras

El teorema 20.4 es sólo un caso especial de un resultado todavía más completo y elegante. Este resultado nos permitirá calcular no sólo el número de coloraciones no equivalentes, sino también cuántas de ellas usan cada color un número determinado de veces. Por ejemplo, las seis coloraciones en blanco y negro no equivalentes de los vértices del cuadrado pueden clasificarse (véase la tabla 20.5.1) según el número de vértices blancos y negros.

Tabla 20.5.1

Negro	Blanco	Número de coloraciones
4	0	1
3	1	1
2	2	2
1	3	1
0	4	1

Podemos representar estos números sencillamente como coeficientes de la *función generadora*

$$U(b, w) = b^4 + b^3w + 2b^2w^2 + bw^3 + w^4.$$

Nuestro objetivo es demostrar cómo puede obtenerse  $U(b, w)$  a partir del índice de ciclos apropiado.

Sea  $X$  el conjunto a colorear y sea  $K = \{a, b, \dots, h\}$  el conjunto de colores disponibles. A cada coloración  $\omega : X \rightarrow K$  le asociamos una expresión formal, el **índicador** de  $\omega$ , definido por

$$\text{ind}(\omega) = a^{n_a}b^{n_b} \cdots h^{n_h},$$

donde  $n_a, n_b, \dots, n_h$  son el número de elementos de  $X$  que reciben los colores  $a, b, \dots, h$  respectivamente. Es evidente que  $n_a + n_b + \cdots + n_h = n$ , donde  $n = |X|$ .

Dado un subconjunto  $A$  del conjunto  $\Omega$  de todas las coloraciones, definimos la función generadora  $U_A$  como la suma formal

$$U_A(a, b, \dots, h) = \sum_{\omega \in A} \text{ind}(\omega).$$

Es evidente que al agrupar los términos de  $U_A$ , el coeficiente del término  $a^s b^t \cdots$  es precisamente el número de coloraciones de  $A$  en las que el color  $a$  se usa  $s$  veces, el color  $b$  se usa  $t$  veces, etc.

Necesitaremos una fórmula explícita para una función generadora particular de esta forma. Supongamos que tenemos una partición

$$X = X_1 \cup X_2 \cup \cdots \cup X_k$$

con  $|X_i| = m_i$  ( $1 \leq i \leq k$ ) y  $m_1 + m_2 + \cdots + m_k = n$ .

**Teorema 20.5.** Sea una partición de  $X$  como la anterior y sea  $B$  el conjunto de coloraciones  $\omega : X \rightarrow \{a, b, \dots, h\}$  que asignan el mismo color a cada elemento de  $X_i$  ( $1 \leq i \leq k$ ). Entonces

$$U_B(a, b, \dots, h) = (a^{m_1} + b^{m_1} + \cdots + h^{m_1})(a^{m_2} + b^{m_2} + \cdots + h^{m_2}) \times \cdots \times (a^{m_k} + b^{m_k} + \cdots + h^{m_k}).$$

**DEMOSTRACIÓN:** Construiremos una correspondencia biyectiva entre las coloraciones de  $B$  y los términos que se obtienen desarrollando el producto de la derecha. Dada una coloración  $\omega$ , supongamos que  $\omega$  asigna el color  $c_1$  a todo  $X_1$ , el color  $c_2$  a todo  $X_2$ , y así sucesivamente; entonces elegimos los términos

$c_1^{m_1}$  del primer paréntesis,

$c_2^{m_2}$  del segundo paréntesis,

$c_k^{m_k}$  del último paréntesis.

Recíprocamente, cada elección de este tipo determina una única coloración que satisface las condiciones para pertenecer a  $B$ .

El producto de los términos elegidos que corresponden a  $\omega$  es exactamente el indicador  $\text{ind}(\omega)$ , de forma que al desarrollar el miembro derecho de la ecuación se obtiene

$$\sum_{\omega \in B} \text{ind}(\omega).$$

Pero ésta es la definición de  $U_B$  y tenemos el resultado.  $\square$

Si hacemos  $a = b = \dots = h = 1$  en la fórmula de  $U_{\Omega}(a, b, \dots, h)$ , cada factor se reduce a  $r$ , el número de colores. Así pues, el número total de coloraciones de  $B$  es  $r^k$ , en concordancia con el hecho de que hemos de asignar a cada uno de los  $k$  conjuntos  $X_1, \dots, X_k$  uno de los  $r$  colores.

El motivo principal de haber demostrado el teorema 20.5 es que es un paso importante en la demostración del teorema principal que se dará en el apartado siguiente. De todas formas, el resultado tiene interés por sí mismo en ciertas situaciones.

**Ejemplo.** Cinco familias preparan una fiesta para sus niños. Cada niño recibirá un regalo, una pelota o una golosina, y los niños de una misma familia recibirán todos el mismo regalo. Dos de las familias tienen cuatro niños y las restantes tienen dos cada una. Calcular la función generadora para el número de maneras de distribuir los regalos y hallar el número de maneras en que pueden repartirse seis pelotas y ocho golosinas.

**SOLUCIÓN:** El conjunto  $X$  es el conjunto de los niños, dividido en dos subconjuntos de tamaño 4 y tres de tamaño 2. Los "colores" son  $p$  (la pelota) y  $g$  (la golosina). Según el teorema 20.5 la función generadora es

$$(p^4 + g^4)^2(p^2 + g^2)^3 = (p^8 + 2p^4g^4 + g^8)(p^6 + 3p^4g^2 + 3p^2g^4 + g^6).$$

Podríamos desarrollar el producto y hallar todos los coeficientes, pero sólo necesitamos el coeficiente de  $b^6g^8$  y fácilmente puede verse que es  $(2 \times 3) + (1 \times 1) = 7$ .  $\square$

### Ejercicios 20.5

- 1 Calcular la función generadora del conjunto de coloraciones que asignan el mismo color a cada elemento de una parte de  $X$ , donde  $|X| = 10$  y
  - hay tres colores disponibles y  $X$  se divide en dos conjuntos iguales;
  - hay dos colores disponibles y  $X$  se divide en conjuntos de tamaños 4, 2, 2 y 2.
- 2 En el ejemplo anterior, supongamos que hay seis familias, tres de ellas con cuatro niños, una con tres y dos con dos. ¿De cuántas maneras pueden distribuirse 11 pelotas y 8 golosinas?

### 20.6 El teorema de Pólya

Estamos a punto para la culminación de nuestros esfuerzos: un teorema descubierto por George Pólya en 1935. Es una elegante combinación de la teoría de grupos de permutaciones y del potente método de las funciones generadoras.

Sea  $G$  un grupo de permutaciones de un conjunto  $X$  y sea  $\hat{G}$  el grupo inducido de permutaciones del conjunto  $\Omega$  de coloraciones de  $X$ , definido mediante la regla  $(\hat{g}(\omega))(x) = \omega(g(x))$ . Queremos obtener la función generadora  $U_D(a, b, \dots, h)$ , donde  $D$  es un conjunto de coloraciones que contiene un representante de cada órbita de  $\hat{G}$  en  $\Omega$ . El coeficiente de  $a^s b^t \dots$  en  $U_D$  será el número de coloraciones distinguibles en las que el color  $a$  se usa  $s$  veces, el color  $b$  se usa  $t$  veces, etc.

El teorema de Pólya asegura que  $U_D$  se obtiene a partir del índice de ciclos sustituyendo  $x_i$  por

$$a^i + b^i + \dots + h^i$$

para  $1 \leq i \leq n$ ). Antes de embarcarnos en la demostración, veamos cómo funciona todo esto en el caso sencillo de las coloraciones en blanco y negro de los vértices de un cuadrado. El índice de ciclos es

$$\frac{1}{8}(x_1^4 + 2x_1^2x_2 + 3x_2^2 + 2x_4),$$

y tenemos que hacer las sustituciones

$$x_1 = b + w, \quad x_2 = b^2 + w^2, \quad x_3 = b^3 + w^3, \quad x_4 = b^4 + w^4.$$

Se obtiene

$$\begin{aligned} U_D(b, w) &= \frac{1}{8}[(b+w)^4 + 2(b+w)^2(b^2+w^2) + 3(b^2+w^2)^2 + 2(b^4+w^4)] \\ &= b^4 + b^3w + 2b^2w^2 + bw^3 + w^4 \end{aligned}$$

de conformidad con la tabla 20.5.1. Un poco animados ya, pasamos a atacar el teorema general.

**Teorema 20.6.** Sea  $\zeta_G(x_1, x_2, \dots, x_n)$  el índice de ciclos de un grupo  $G$  de permutaciones de un conjunto  $X$ . La función generadora  $U_D(a, b, \dots, h)$  del número de coloraciones de  $X$  no equivalentes, si los colores disponibles son  $a, b, \dots, h$ , viene dada por

$$U_D(a, b, \dots, h) = \zeta_G(\sigma_1, \sigma_2, \dots, \sigma_n),$$

donde

$$\sigma_i = a^i + b^i + \dots + h^i \quad (1 \leq i \leq n).$$

**DEMOSTRACIÓN:** Empezaremos por hallar una fórmula alternativa a

$$U_D(a, b, \dots, h) = \sum_{\omega \in D} \text{ind}(\omega),$$

donde  $D$  es un conjunto de coloraciones que contiene un representante de cada órbita de  $\hat{G}$  en  $\Omega$ . Para ello invocamos la forma “ponderada” del teorema 14.4, tal como se indica en el ejercicio 14.4.5. Si aplicamos este resultado a la acción de  $\hat{G}$  en  $\Omega$  se obtiene

$$\sum_{\omega \in D} \text{ind}(\omega) = \frac{1}{|\hat{G}|} \sum_{\hat{g} \in \hat{G}} \left[ \sum_{\omega \in F(\hat{g})} \text{ind}(\omega) \right]$$

Ahora bien, la suma entre corchetes es, por definición,  $U_{F(\hat{g})}$ . Además, una coloración  $\omega$  es de  $F(\hat{g})$  si, y sólo si, es constante en cada ciclo de  $\hat{g}$ , tal como se vio en la demostración del teorema 20.4. Por lo tanto, la forma explícita de  $U_{F(\hat{g})}$  nos la da el teorema 20.5:

$$\begin{aligned} U_{F(\hat{g})}(a, b, \dots, h) &= (a^{m_1} + \dots + h^{m_1}) \times \dots \times (a^{m_k} + \dots + h^{m_k}) \\ &= \sigma_{m_1} \dots \sigma_{m_k}, \end{aligned}$$

donde  $m_1, m_2, \dots, m_k$  son las longitudes de los ciclos de  $\hat{g}$ . En otras palabras, si  $\hat{g}$  tiene  $\alpha_i$  ciclos de longitud  $i$  ( $1 \leq i \leq n$ ), entonces

$$\begin{aligned} U_{F(\hat{g})}(a, b, \dots, h) &= \sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \dots \sigma_n^{\alpha_n} \\ &= \zeta_g(\sigma_1, \sigma_2, \dots, \sigma_n). \end{aligned}$$

Como la representación  $g \rightarrow \hat{g}$  es una biyección, tenemos que  $|G| = |\hat{G}|$  y sustituyendo la expresión anterior de  $U_{F(\hat{g})}$  obtenemos

$$U_D(a, b, \dots, h) = \zeta_G(\sigma_1, \sigma_2, \dots, \sigma_n),$$

tal como queríamos demostrar.  $\square$

El teorema de Pólya nos proporciona un procedimiento mecánico para calcular el número de coloraciones no equivalentes de varios tipos. En general, la tarea principal es calcular el índice de ciclos del grupo que interviene y por este motivo nos hemos armado con una pequeña lista de índices de ciclos útiles. La tarea secundaria es expandir la expresión que resulta al sustituir  $x_i$  en el índice de ciclos y hallar los coeficientes buscados. Esto último puede ser laborioso, aunque a menudo no es necesario completar todos los detalles.

**Ejemplo.** (Apartado 14.4 revisitado). Cuántos collares pueden hacerse con 3 cuentas negras y 13 blancas?

**SOLUCIÓN:** El grupo en cuestión es el grupo diedral  $D_{32}$  que actúa en los vértices de 16-gono y, según el teorema 20.2.2, el índice de ciclos es

$$\frac{1}{32} (x_1^{16} + 9x_2^8 + 2x_4^4 + 4x_8^2 + 8x_{16} + 8x_1^2x_2^7).$$

Para hallar el número buscado, hacemos la sustitución  $x_i = b^i + w^i$  ( $1 \leq i \leq 16$ ) y calculamos el coeficiente de  $b^3w^{13}$ . Se ve que las potencias impares de  $b$  y  $w$  sólo pueden provenir de los términos  $x_1^{16}$  y  $8x_1^2x_2^7$ , así que necesitamos el coeficiente de  $b^3w^{13}$  en

$$\begin{aligned} \frac{1}{32} [(b+w)^{16} + \dots + 8(b+w)^2(b^2+w^2)^7] &= \frac{1}{32} [(b^{16} + \dots + \binom{16}{3}b^3w^{13} + \dots + w^{16}) + \dots \\ &\quad \dots + 8(b^2+2bw+w^2) \times (b^{14} + \dots + 7b^2w^{12}+w^{14})]. \end{aligned}$$

Por lo tanto, la respuesta es

$$\frac{1}{32} \left( \frac{16 \times 15 \times 14}{3 \times 2 \times 1} + 8 \times 2 \times 7 \right) = 21.$$

En el ejemplo anterior, los términos que contribuyen a la respuesta son precisamente aquéllos que contribuyen a la “suma de puntos fijos” que aparecía en el apartado 14.4 cuando utilizábamos un método más elemental. Lo cual no es de extrañar, ya que el nuevo método está basado en el antiguo.

**Ejercicios 20.6**

- 1 ¿De cuántas maneras pueden colorearse las caras de un cubo de forma que haya dos caras rojas, una blanca y tres azules?
- 2 Construir explícitamente la función generadora  $U_D(a, v)$  del número de maneras de colorear las caras de un octaedro regular si se dispone de los colores azul y verde.
- 3 (i) ¿Cuántos discos pueden obtenerse al dividir una cara de un disco en cinco sectores iguales y colorear dos de rojo, dos de blanco y uno de azul?  
(ii) ¿Cuántos collares pueden construirse con dos cuentas rojas, dos blancas y una azul?
- 4 Si sólo intervienen dos colores, es conveniente usar los símbolos 1 y  $x$  en lugar de  $b$  y  $w$  (o de los nombres de otros colores cualesquiera). De esta forma obtenemos una función generadora de la forma

$$f_0 + f_1x + f_2x^2 + \cdots + f_nx^n,$$

donde  $f_i$  es el número de configuraciones con  $i$  objetos negros y  $n - i$  blancos. Obtener la función generadora explícitamente para el problema, discutido en el ejemplo, de los collares con 16 cuentas blancas o negras.

5 Los químicos estudian qué moléculas pueden formarse con un átomo C (carbono) unido a cuatro radicales que pueden ser HOCH<sub>2</sub> (hidroximetilo), C<sub>2</sub>H<sub>5</sub> (etilo), Cl (clorino) o H (hidrógeno). Hay buenas razones para imaginar esta situación como un átomo C colocado en el centro de un tetraedro regular y los cuatro radicales en los vértices.

- (i) Demostrar que hay 36 moléculas posibles.
- (ii) Demostrar que hay 15 moléculas que contienen un radical H.
- (iii) Calcular la función generadora

$$H(x) = h_0 + h_1x + h_2x^2 + h_3x^3 + h_4x^4,$$

donde  $h_i$  ( $0 \leq i \leq 4$ ) es el número de moléculas que contienen exactamente  $i$  radicales H.

**20.7 Ejercicios diversos**

- 1 Demostrar que el índice de ciclos del grupo de simetrías rotacionales del cubo, considerado como grupo de permutaciones de las aristas, es

$$\frac{1}{24}(x_1^{12} + 3x_2^6 + 6x_4^3 + 6x_1^2x_5^2 + 8x_3^4).$$

- 2 Sea  $\Delta$  un grupo abstracto que contiene elementos  $\pi$  e  $\sigma$  tales que

- (i)  $\pi$  tiene orden  $n$ ,
- (ii)  $\sigma$  tiene orden 2,
- (iii)  $\sigma\pi = \pi^{-1}\sigma$ .

Supongamos también que todo elemento de  $\Delta$  puede expresarse como un producto de términos iguales a  $\pi$ ,  $\pi^{-1}$  o  $\sigma$  (nótese que  $\sigma = \sigma^{-1}$ ). Demostrar que todo elemento de  $\Delta$  puede expresarse de forma única como  $\sigma^e\pi^i$  ( $e = 0$  o  $1$ ,  $1 \leq i \leq n-1$ ) y deducir que  $\Delta \approx D_{2n}$ .

- 3 Demostrar que  $D_{2n} \times C_2 \approx D_{4n}$  para todo entero positivo impar  $n$ .
- 4 Describir el centro  $Z(D_{2n})$ , distinguiendo según que  $n$  sea par o impar.
- 5 Calcular el número de maneras de colorear un disco dividido en  $p$  sectores por una cara si se dispone de tres colores para cada sector y  $p$  es un primo impar.
- 6 Calcular el número de collares que pueden construirse con  $p$  cuentas si se dispone de tres colores y  $p$  es un primo impar.
- 7 Se tiran seis dados indistinguibles. Utilizar el teorema 20.5 para construir una función generadora  $U^*(a_1, a_2, \dots, a_6)$  del número de maneras de obtener un resultado dado si los primeros cuatro dados muestran el mismo número y los dos últimos también. Sustituyendo  $x^i$  por  $a_i$  ( $1 \leq i \leq 6$ ), hallar el número de maneras en que puede obtenerse de este modo un total de 18.
- 8 Calcular el número de maneras distintas de colorear las caras de un dodecaedro con tres colores, con la condición de que cada color se use al menos una vez.
- 9 Se colocan tres bolas rojas, dos azules y una amarilla en los vértices de un octaedro. ¿De cuántas maneras puede hacerse?
- 10 Demostrar que si  $n_1 + n_2$  es un primo impar, el número de collares que pueden hacerse con  $n_1$  cuentas negras y  $n_2$  blancas es igual a

$$\frac{1}{2(n_1 + n_2)} \binom{n_1 + n_2}{n_1} + \frac{1}{2} \binom{\frac{1}{2}(n_1 + n_2 - 1)}{\lfloor \frac{1}{2}n_1 \rfloor}.$$

- 11 Se pinta un lápiz sin afilar (totalmente cilíndrico) en siete bandas de igual tamaño. Se dispone de los colores rojo, verde y amarillo. ¿De cuántas maneras puede hacerse si hay

- (i) dos bandas rojas, dos verdes y tres amarillas;  
(ii) cuatro bandas rojas, una verde y dos amarillas.

12 Calcular el número de maneras de colorear las caras de un dodecaedro regular de manera que haya seis caras rojas, cuatro amarillas y dos azules.

13 En el ejercicio 14.7.21 obtuvimos tres grupos finitos de rotaciones "especiales" de órdenes 12, 24 y 60. Se trata de los grupos de simetría rotacional del tetraedro regular, del cubo y del dodecaedro regular. Describir en cada caso las rotaciones geométricamente, especificando un eje representativo de cada rotación de cada orden.

14 Calcular el centro de cada uno de los tres grupos discutidos en el ejercicio anterior.

15 Demostrar que el grupo del dodecaedro regular es isomorfo al grupo alternado  $A_5$ .

## Soluciones a ejercicios escogidos

### Ejercicios 1.1

- 3 Tomar  $c = a - b = a + (-b)$ .

### Ejercicios 1.2

- 4 (i) Sí, -4. (ii) No. (iii) Sí, 0.

6

1	2	3	4	25
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	5

$$s = 10, t = 5.$$

### Ejercicios 1.3

- 2  $t_1 = 2, t_n = 2t_{n-1}$  ( $n \geq 2$ ).  
4 (i)  $u_n = 3n - 2$ . (ii)  $u_n = (n!)^2$ .

### Ejercicios 1.4

- 2  $S_n = (\frac{1}{2}n(n+1))^2$ .  
5 (i)  $n_0 = -2$ . (ii)  $n_0 = 6$ .

### Ejercicios 1.5

- 2 11 111 000 001, 30 420, 1545.  
3 (i) 221. (ii) 1468.

### Ejercicios 1.6

- 2 Si  $a = pc, b = qc$ , entonces  $xa + yb = (xp + yq)c$ .

### Ejercicios 1.7

- 1  $\text{mcd}(721, 448) = 7$ .  
5  $\text{mcd}(966, 686) = 14$ , una solución es  $x = -110, y = 155$ .

**Ejercicios 1.8**

- 2  $201 = 3 \times 67$ ,  $1001 = 7 \times 11 \times 13$ ,  $201\ 000 = 2^3 \times 3 \times 5^3 \times 67$ .  
 9 11.

**Ejercicios 2.1**

- 2 Tomar  $g(i) = i$  para  $1 \leq i \leq 5$ .  
 3 (i) Sí, si  $U$  incluye a los ciudadanos fallecidos. (ii) No,  $x$  puede no tener ninguna hija o tener varias hijas. (iii) No, las mujeres no tienen esposas.

**Ejercicios 2.2**

- 1 (i) Inyectiva. (ii) Biyectiva. (iii) Inyectiva. (iv) Ni inyectiva ni exhaustiva.  
 2 Nótese que  $u(n) = u(n-7)$   $n \geq 8$ .

**Ejercicios 2.3**

- 1 (i)  $n = 5$ ,  $f(i) = 2i$ . (ii)  $n = 6$ ,  $f(i) = 2 - 5i$ . (iii)  $n = 8$ ,  $f(i) = (i+2)^2 + 1$ .

**Ejercicios 2.4**

- 1 3, 12.  
 5 El conjunto  $\{n+1, n+2, \dots, 2n\}$  lo demuestra.

**Ejercicios 2.5**

- 1 (i) Una inyección adecuada es la inclusión  $i : \mathbb{N} \rightarrow \mathbb{Z}$ . (ii)  $i(n) = -n$ .  
 (iii)  $i(n) = n + 10^6 - 1$ .  
 3 Considerar  $N = 6p_1p_2 \cdots p_k - 1$ , donde se supone que  $p_1, p_2, \dots, p_k$  son todos los primos de la forma  $6m + 5$ .

**Ejercicios 3.1**

- 1 49.  
 2 Los múltiplos de 2 y los múltiplos de 3 no son disjuntos.

**Ejercicios 3.2**

- 1 20.  
 3 No, ya que 3 no es divisor de 40.  
 5  $26^4, 25^4$ .

**Ejercicios 3.3**

- 1 18, 8, 12.  
 4  $\phi(a)\phi(b) = \phi(ab)$  si  $\text{mcd}(a, b) = 1$ .

**Ejercicios 3.4**

- 1  $4^3$ .  
 3 7.

**Ejercicios 3.5**

- 1 14 529 715 200.  
 2 5040.

**Ejercicios 3.6**

- 1  $(137)(2548)(6)(9)$ .  
 3 9.  
 4  $\alpha_1 = (12)(34)$ ,  $\alpha_2 = (13)(24)$ ,  $\alpha_3 = (14)(23)$ .

**Ejercicios 4.1**

- 3 El complementario de un  $r$ -subconjunto es un  $(n-r)$ -subconjunto.  
 5 1820, 6188.  
 6 Los  $r$  ceros pueden estar en cualquiera de las  $n$  posiciones.

**Ejercicios 4.2**

- 2  $\binom{n+5}{2}$ .  
 3  $\frac{1}{2}(n+1)(n+2)$ .

**Ejercicios 4.3**

- 2 (i) 462. (ii) 45. (iii) 10. (iv) 34 560.  
 4 Hacer  $x = 1$  y  $x = -1$ .

**Ejercicios 4.4**

- 1 8, 6.  
 2 582.  
 3 9.

**Ejercicios 4.5**

1

$n$	95	96	97	98	99	100
$\phi(n)$	72	32	96	42	60	40
$\mu(n)$	1	0	-1	0	0	0

4  $d|x$  y  $d|n$  si, y sólo si,  $d|n-x$  y  $d|n$ .**Ejercicios 4.6**1 (i)  $4v = 7k$ . (ii) Al menos cuatro.

2 (i) 123, 456. (ii) Imposible. (iii) 123, 234, 345, 456, 567, 167, 127.

4  $v' = k, k' = v - k, r' = vr/k - r$ .**Ejercicios 4.7**

1 4, 12, 30, 66, 132.

2 (i) Imposible. (ii) Posible.

**Ejercicios 5.1**

1 1 127 966 1701 1050 266 28 1.

**Ejercicios 5.2**2  $\{1, 11, 6\}, \{2, 7\}, \{5\}, \{9\}$ .

3 (i) 24. (iii) 6.

4  $n!, (n-1)!$ .6 Dado  $a$ , puede no existir un  $b$  tal que  $a \sim b$ .**Ejercicios 5.3**

1 34 650.

2 126 000, 756.

5 (i) 2520. (ii) 2520.

**Ejercicios 5.4**

1 Hay 15 particiones.

2 Restar 1 a cada parte.

**Ejercicios 5.5**2 Una permutación conveniente es  $\sigma = (1)(268974)(35)$ .3  $\pi\tau = \tau^{-1}(\tau\pi)\tau$ .

5 265.

6 15.

**Ejercicios 5.6**1  $\operatorname{sgn} \alpha = 1, \operatorname{sgn} \beta = -1, \operatorname{sgn} \gamma = 1$ .

4 (i) Posible. (ii) Imposible.

**Ejercicios 6.1**

2 (i) Falso. (ii) Falso. (iii) Podría ser cierto, pero de hecho es falso.

3 6, 5.

**Ejercicios 6.2**3  $x = 2, y = 1$ . No hay solución en  $\mathbb{Z}_5$ .

4 3, 5.

**Ejercicios 6.3**

4 6, 13, 7, 8.

5 4.

**Ejercicios 6.4**

1 (i) Sí. (ii) No. (iii) Sí.

2  $v = 4n + 3, k = 2n + 1, r_2 = n$ .**Ejercicios 6.5**

AS	KH	QC	JD
KC	AD	JS	QH
QD	JC	AH	KS
JH	QS	KD	AC

3 Ya que 4 no es primo.

**Ejercicios 7.1**1  $c_1 = t(x_0y), p_0 = u(x_0y); c_{i+1} = t(x_iy + c_i), p_i = u(x_iy + c_i)$  ( $1 \leq i \leq n-1$ );  $p_n = c_n$ .

**Ejercicios 7.2**

- 1 101, 23, 78; 58, 23, 78; 46, 23, 61.  
 2 27, 13, 78; 11, 31, 25; 60, 138, 78.

**Ejercicios 7.3**

- 2 153.

**Ejercicios 7.4**

- 3 El valor de  $q$  es el producto de  $n$  y  $m$ .

**Ejercicios 7.5**

- 1 (i)  $n$ . (ii)  $n - 1$ . (iii)  $x_1 > x_2 > \dots > x_n$ .  
 3 (iii)  $(a_k, b_k) = (f_{k+1}, f_k)$ , donde  $f_k$  se define mediante  $f_1 = 1, f_2 = 2, f_r = f_{r+1} + f_{r+2}$  ( $r \leq 2$ ).

**Ejercicios 7.6**

- 1 (i)  $n^3$ . (ii)  $n^2$ . (iii)  $3^n$ . (iv)  $n^n$ .  
 4 Porque  $\log_a n = \log_b n / \log_b a = C \log_b n$ .

**Ejercicios 7.7**

- 2 54, 9.  
 4  $ax + bz = m_1 + m_4 - m_5 + m_7; ay + bt = m_3 + m_5; cx + dz = m_2 + m_4; cy + dt = m_1 - m_2 + m_3 + m_6$ .

**Ejercicios 7.8**

1	3	4	5	1	2	7	8	6	9
3	4	1	2	5	7	6	8	9	
3	1	2	4	5	6	7	8	9	
1	2	3	4	5	6	7	8	9	

Las siguientes pasadas no tienen ningún efecto.

**Ejercicios 8.1**

- 1 No.  
 3  $\frac{1}{2}n(n - 1)$  aristas;  $n \geq 5$  es imposible.

**Ejercicios 8.2**

- 1 El segundo grafo no tiene 3-ciclos.

**Ejercicios 8.3**

- 1 (i) No. (ii) Sí. (iii) No. (iv) No.  
 2  $n - 1 - d_1, n - 1 - d_2, \dots, n - 1 - d_n$ .  
 3 Sólo hay dos posibilidades.  
 5 No puede haber vértices de grados 0 y  $n - 1$  en el mismo grafo.

**Ejercicios 8.4**

- 1 3.  
 4 Hay un camino euleriano pero ningún ciclo hamiltoniano.  
 5 No.

**Ejercicios 8.5**

- 4 Calcular componente a componente.

**Ejercicios 8.6**

- 1 (i)  $n$ . (ii) 2. (iii) 3.  
 2 3, 4, 4.

**Ejercicios 9.1**

- 2 3.  
 4  $[\log_2 20] = 5$ .  
 5 12, 13.  
 7 2.

**Ejercicios 9.2**

- 1 5.  
 2 (i) 6. (ii) 6. (iii) 5.  
 3 (i) 16, 55, 33, 63, 81, 76. (ii) 12, 21, 17, 28, 32, 51, 19, 84, 38, 49, 77, 73, 56.

**Ejercicios 9.3**

- 3 El AGM es único.  
 4 Cuatro AGM, peso 20.

**Ejercicios 9.4**

- 1  $G$  es conexo.  
 2 3.

**Ejercicios 9.5**

- 2 No conexo.
- 3  $n - 1, 1; n - 1, [n/2]$ .
- 5 El número de vértices en el nivel  $i$  es  $\leq k(k - 1)^{i-1}$ .

**Ejercicios 9.6**

- 1  $v \ a \ d \ e \ b \ g \ h \ w$ .
- 2 A D C F.

**Ejercicios 10.1**

- 2 (i) s. (ii) r. (iii) rs. (iv) Cada  $x$  está relacionado con cada  $y$ .
- 3 No.

**Ejercicios 10.2**

- 1 (i) 3. (ii) 5. (iii) 3.
- 3 Dar a  $x_iy_j$  el color  $i + j \pmod n$ .

**Ejercicios 10.3**

- 2  $Q = E$ .

**Ejercicios 10.4**

- 1  $\Gamma\{x_2, x_3, x_4\} = \{y_2, y_4\}$ .
- 2 (i) Por ejemplo,  $x_2y_5x_5y_1$ . (ii)  $M' = \{x_2y_5, x_3y_2, x_4y_4, x_5y_1\}$ . (iv) Sí.

**Ejercicios 10.5**

- 2 Todos los 3-subconjuntos, salvo  $\{x_1, x_2, x_3\}$ .

**Ejercicios 10.6**

- 1 Se toman  $a, l, b, e, t, s$  como representantes de los conjuntos en el orden dado.
- 3 Hay cinco conjuntos que contienen únicamente los cuatro elementos  $\{a, e, m, r\}$ .

**Ejercicios 11.1**

- 1  $c, b, a, d, e, f; d, e, f, a, d$ .
- 2  $1, 2, 4, 5, 6, 7, 8, 3, 9$ .

**Ejercicios 11.2**

- 1 Camino crítico  $s, p, q, z, t$ .
- 2 Actividades críticas  $\alpha_1, \alpha_3, \alpha_8, \alpha_{11}$ .

**Ejercicios 11.3**

- 1 El corte  $\{s, b\}, \{a, c, d, t\}$  tiene capacidad 10.
- 2 Flujo: 4, 5, 1, 3, 4, 2, 5, 2. Corte:  $\{s, a, b, d\}, \{c, t\}$ .

**Ejercicios 11.4**

- 1 (i) 11. (ii)  $s, c, b, d, t; 12$ . (iii)  $\{s, b, c, e\}, \{a, d, t\}$ . (iv)  $f^*$  es un flujo máximo.
- 2 Flujo máximo = 38.

**Ejercicios 11.5**

- 1 Flujo máximo = 55.
- 2 Flujo máximo = 39.

**Ejercicios 12.1**

- 1 En el método recursivo, el número de multiplicaciones es  $O(n)$ .
- 3 El mismo número de multiplicaciones, menos necesidad de memoria.

**Ejercicios 12.2**

- 1 (i)  $(2(4^n) + 3(-1)^n)/5$ . (ii)  $3n - 2$ .
- 4 (i)  $F_n = q_{n-1}$ .

**Ejercicios 12.3**

- 3  $a_n = 2n - \sqrt{n}$ .

**Ejercicios 12.4**

- 1 9; hay cuatro estrategias óptimas.
- 2 21; adjudicar 2, 2, 1 ó 0, 2, 3.

**Ejercicios 12.5**

- 2  $x_1 = 1, x_2 = 0, x_3 = 5$ ; beneficio 184.  $x_1 = 4, x_2 = 0, x_3 = 0$ ; beneficio 166.

**Ejercicios 12.6**

- 1 Longitud 14, tres caminos posibles.  
 2  $x_1 = 2, x_2 = 1, x_3 = 1$ ; óptimo 34.

**Ejercicios 13.1**

- 1  $+$  tiene las cuatro propiedades,  $-$  todas salvo la asociativa,  $\times$  todas salvo el inverso.

**Ejercicios 13.2**

- 3 (i) Todos los  $n \geq 2$ . (ii) Ningún  $n$ . (iii)  $n$  primo.

**Ejercicios 13.3**

- 2 (i)  $xy = 1 \Rightarrow x = y^{-1}$ .  
 3 Utilizar la parte (ii) de la pregunta anterior.  
 5  $(ab)c = c$ , pero  $a(bc) = b$ .

**Ejercicios 13.4**

- 1 10, 4; 6, 6.  
 3 Órdenes de  $A, B = 7, 6$ .  
 4 La matriz  $\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$  tiene orden 2 para todo  $b$ .

**Ejercicios 13.5**

- 2 (iii) O bien cada elemento tiene orden 1 o 2, o bien hay un elemento  $x$  con  $x^2 \neq 1$ .

**Ejercicios 13.6**

- 1  $U \approx \langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6 = 1\}$ .  
 2 La función que envía  $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$  a  $m$  es un isomorfismo de  $M$  en  $\mathbf{Z}$ .

**Ejercicios 13.7**

- 1  $K_1$  sí,  $K_2$  no,  $K_3$  no.  
 2  $H = \{i, x\}$  y  $K = \{i, y\}$  es un ejemplo.  
 4  $Z(G)$  es la intersección de todos los  $C(g)$  con  $g \in G$ .

**Ejercicios 13.8**

- 2 Clases laterales:  $\{i, x\}, \{r, z\}, \{s, y\}$ .  
 3 Orden 1:  $\{\text{identidad}\}$ ; Orden 2:  $\{\text{identidad y una reflexión}\}$ ; Orden 5:  $\{\text{identidad y 4 rotaciones}\}$ ; Orden 10: todo el grupo.

**Ejercicios 13.9**

- 1  $\langle z^7 \rangle = C_{24}, \langle z^8 \rangle = C_3, \langle z^9 \rangle = C_8$ .  
 2  $\phi(60) = 16$ .

**Ejercicios 14.1**

- 1 (i) No. (ii) Sí. (iii) Sí. (iv) No.  
 2 (i) 4. (ii) 2. (iii) 115.  
 3 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 15.  
 5 El grupo tiene orden 12.

**Ejercicios 14.2**

- 1 id, (15)(24).  
 2  $\neg\{1, 6, 7\}, \{2, 4, 5\}, \{3\}$ .  
 3  $\{1, 3\}, \{2\}, \{4\}, \{5, 7\}, \{6, 8\}$ .

**Ejercicios 14.3**

- 3  $\{a, f\}, \{b, c, d, e\}; |G_a| = 4, |G_b| = 2, |G| = 8$ .

**Ejercicios 14.4**

- 2 21.  
 4 42.

**Ejercicios 14.5**

- 2 (i) Sí. (ii) Sí. (iii) No. (iv) No.

**Ejercicios 14.6**

- 1 24.  
 3 (13)(24);  $g_3$ .  
 5  $\sigma = (78)$ .

**Ejercicios 15.1**

- 1 (iv)  $m^4$ . (vi) Hay seis.

**Ejercicios 15.2**

- 1  $\{1, 3, 7, 9\}$ , cíclico, generado por 3;  $\{1, 2, \dots, 10\}$ , cíclico, generado por 2;  
 $\{1, 5, 7, 11\}$ , no cíclico,  $C_2 \times C_2$ .
- 3  $U(\Gamma) = \{1, i, -1, -i\}$ , cíclico, generado por  $i$ .

**Ejercicios 15.3**

- 2 5 es un generador.

**Ejercicios 15.4**

- 1 (i)  $x^3 + 4x^2 + x + 3, x^5 + 2x^4 + x^3 + 3x + 2$ .  
(ii)  $x^4 + x^3 + x^2 + 4x + 3, x^7 + x^4 + x^3 + x^2 + 3x + 2$ .
- 4 Cierto si  $m$  es primo.

**Ejercicios 15.5**

- 1  $q = x, r = x + 1$ .  
2  $q = x^3 + 4x^2 + x + 2, r = 2x + 1$ .

**Ejercicios 15.6**

- 1  $x + 1; \lambda(x) = 1, \mu(x) = 2x + 2$ .  
2  $x + 4$ .  
3 (i)  $x^2 + 1$ . (ii)  $x + 1$ . (iii)  $x^3 + 1$ .

**Ejercicios 15.7**

- 6  $\mathbb{Z}_{15}$  no es un cuerpo, la factorización en  $\mathbb{Z}_{15}[x]$  no es única.

**Ejercicios 15.8**

- 1 (i)  $(x+2)(x+3)$ . (ii)  $(x+8)(x+9)(x+10)$ . (iii)  $(x^2+2)(x^2+3x+3)$ .  
2  $x^2+1, x^2+x+2, x^2+2x+2$ .

**Ejercicios 16.1**

- 1 Si  $c = 2x + 1$ , los generadores son  $c, c^3 = x + 1, c^5 = x + 2, c^7 = 2x + 2$ .  
2  $x, 2, 2x, 1$ .

**Ejercicios 16.2**

- 1 (i)  $0 = w, 1 = y$ . (iii) 2.

**Ejercicios 16.3**

- 2 Tomar  $0 \rightarrow w, 1 \rightarrow y, x \rightarrow z, x + 1 \rightarrow t$ .  
3  $3, 7, 11, 19, 23$ ; los grupos son cílicos.  
4 El número de polinomios mónicos irreducibles es  $> 0$ .

**Ejercicios 16.4**

- 1 (i) 3. (ii) 2. (iii) 5.  
3 (i) Reducible. (ii) Irreducible, primitivo. (iii) Reducible.  
4  $\phi(31) = 30$ , es decir, todos salvo 0 y 1.  
5 4, 5, 6, 7.

**Ejercicios 16.5**

1	66	23	50	41
	03	79	88	97
	10	87	99	78
	31	98	77	89

**Ejercicios 16.6**

- 2 (i)  $(0, 2), (1, 4), (2, 4)$ . (ii)  $x = 1, x + 3y = 1, x + y = 1$ . (iii)  $(1, 0)$ .  
3 (i) 3. (ii) 2. (iii) 4. (iv) 2.

**Ejercicios 16.7**

- 1 13 semanas, el esquema es un plano proyectivo sobre  $\mathbb{F}_3$ .  
2 El complementario de cada cuadrágulo es una recta.

**Ejercicios 16.8**

- 1  $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$ .

**Ejercicios 16.9**

- 1  $(p^4 - p^2)/4, (p^5 - p)/5, (p^6 - p^3 - p^2 + p)/6$ .  
2  $x^4 + x^3 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1$ .  
3  $x, x + 1, x^2 + x + 1$  y los polinomios obtenidos en la pregunta 2.

5 (iii) 2, 4, 8, 64.

**Ejercicios 17.1**

- 1 (i)  $\delta = 2$ , detecta 1, corrige 0. (ii)  $\delta = 2$ , detecta 1, corrige 0. (iii)  $\delta = 3$ , detecta 2, corrige 1.  
 2 (ii) y (iii) pueden extenderse.

**Ejercicios 17.2**

- 1  $k = 1, \delta = n$ .  
 3 2;  $\{00\ 000\ 000, 11\ 111\ 000, 00\ 011\ 111, 11\ 100\ 111\}$ .

**Ejercicios 17.3**

- 1 8 palabras.  
 2  $n = 7, k = 3, \delta = 3$ .  
 4 (i) 6. (ii) 10.

**Ejercicios 17.4**

- 1 100 110.  
 2 2048; sólo la segunda palabra es del código.  
 3 (i) 12. (iii) 15.

**Ejercicios 17.5**

- 1 (i) No. (ii) No (no es lineal). (iii) Sí. (iv) Sí.  
 2 000, 111;  $H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$  por ejemplo.

**Ejercicios 17.6**

- 1  $(x+1)(x^4+x^3+x^2+x+1)$ .  
 3 (ii) 32. (iii)  $x^4+x+1$ .

**Ejercicios 18.1**

- 1 (i)  $1 - x + 4x^2 - 19x^3$ . (ii)  $\frac{2}{3} + \frac{16}{9}x - \frac{37}{27}x^2 - \frac{221}{81}x^3$ .  
 4  $1 + x^2 + x^4 + x^6 + \dots; 1 + 2x^2 + x^4 + 2x^6 + \dots$

**Ejercicios 18.2**

- 1 (i)  $\frac{7}{3}/(1-x) + (-\frac{5}{3})/(2+x)$ . (ii)  $1/(1+x) + (-4)/(2+x) + 4/(3+x)$ .

- 3  $(2+2x)/(1+2x+2x^2) + (2+x)/(1+x+2x^2)$ .  
 5  $\frac{1}{4}\{(1+x)^{-1} + (1-x)^{-1} + i(i-x)^{-1} + i(i+x)^{-1}\}$ .

**Ejercicios 18.3**

- 1 (i) 280. (ii)  $(n+1)(n+2)(n+3)/6$ . (iii)  $\binom{3r-1}{r-1}$ .  
 4  $\frac{1}{2}(5n^2 + 3n + 2)$ .

**Ejercicios 18.4**

- 1  $(1 - \frac{1}{2}n)2^n$ .  
 2 (i)  $5A(x)$ . (ii)  $A(x) + 5(1-x)^{-1}$ .  
 (iii)  $x^{-5}(A(x) - a_0 - a_1x - a_2x^2 - a_3x^3 - a_4x^4)$ .

**Ejercicios 18.5**

- 1 (i)  $(4^{n+1} + (-1)^n)/5$ . (ii)  $5 - 2^{n+2} + 3^n$ . (iii)  $(8 - 6n + (-2)^n)/9$ .  
 2  $b_n = F_n$  (como en el ejercicio 12.2.2).  
 3 Si  $a = 0$  y  $b = 2$ ,  $z_n = (-1)^n 3(2^{n+1} + (-1)^n)^{-1}$ .

**Ejercicios 18.6**

- 2  $Q(x) = x/(1-2x)(1-4x)$ .

**Ejercicios 19.1**

- 2 1, 2, 3, 5, 711, 15.

**Ejercicios 19.2**

- 1 (i)  $[12^2 3^2 5]$ . (ii)  $[1^3 2^2 57^2]$ .  
 2 (i) No. (ii) No. (iii) Sí. (iv) Sí.  
 3 Hay siete de ellos.  
 4 7.

**Ejercicios 19.3**

- 1 (i)  $(1-x^3)^{-1}(1-x^5)^{-1}$ . (ii)  $(1-x^2)^{-1}(1-x^4)^{-1}(1-x^6)^{-1}$ .  
 3 49.  
 4 25.

**Ejercicios 19.4**

- 1 (i)  $(1+x+x^2)(1+x^2+x^4)(1+x^3+x^6)\dots$

- (ii)  $(1-x)^{-1}(1-x^2)^{-1}(1-x^4)^{-1}\dots$   
 (iii)  $x^5(1-x^5)^{-1}(1-x^6)^{-1}(1-x^7)^{-1}\dots$

### Ejercicios 19.5

- 2 Restar 1 a cada parte.

### Ejercicios 19.6

- 1  $p(15) = 176, p(16) = 231, p(17) = 297, p(18) = 385, p(19) = 490, p(20) = 627.$   
 2 22.

### Ejercicios 20.1

- 1 10 coloraciones distinguibles.  
 2 20.  
 3 (i)  $(x_1^3 + 3x_1x_2 + 2x_3)/6.$   
     (ii)  $(x_1^4 + 8x_1x_3 + 3x_2^2)/12.$   
     (iii)  $(x_5^1 + 10x_1^3x_2 + 20x_1^2x_3 + 15x_1x_2^2 + 30x_1x_4 + 20x_2x_3 + 24x_5)/120.$   
 4  $(x_1^6 + x_1^2x_2^2 + 2x_2^3)/4; (x_1^9 + 2x_1x_4^2 + x_1x_2^4 + 4x_1^3x_2^3)/8.$

### Ejercicios 20.2

- 2  $(x_1^p + (p-1)x_p + px_1x_2^{p-1})/2p$ ; utilizar el teorema de Fermat.  
 5  $C_6 \times C_2.$

### Ejercicios 20.3

- 2  $(x_1^6 + 8x_3^2 + 3x_1^2x_2^2)/12.$

### Ejercicios 20.4

- 1 (i)  $(r^4 + 11r^2)/12.$  (ii)  $(r^4 + 11r^2)/12.$  (iii)  $(r^6 + 3r^4 + 12r^3 + 8r^2)/24.$   
 3 9099.  
 4 834.

### Ejercicios 20.5

- 1 (i)  $(a^5 + b^5 + c^5)^2.$  (ii)  $(a^4 + b^4)(a^2 + b^2)^3.$   
 2 6.

### Ejercicios 20.6

- 1 3.  
 3 (i) 6. (ii) 4.

## Glosario

- acción, 352  
 alfabeto, 59  
 algoritmo, 151  
     de etiquetaje, 269  
     de Euclides  
     para enteros, 20  
     para polinomios, 374  
     voraz, 195  
 altura de un árbol con raíz, 204  
 anillo, 360  
 árbol, 190  
     binario, 208  
     con raíz m-ario, 205  
     con raíz, 203  
     generador, 213  
 arco, 254  
 arista-coloración, 233  
 automorfismo de un grafo, 338  
 axioma del buen orden, 6  
 axiomas, 1  
 base, 15  
     de la inducción, 12  
 beneficio de etapa, 290  
 binomial  
     coeficiente, 79  
     número, 71  
 teorema para exponentes negativos, 457  
     teorema, 77  
 bipartido, 197  
 bit, 421  
 biyección, 34  
 bloque, 90  
 búsqueda  
     en anchura, 222  
     en profundidad, 218  
 camino, 187  
     alternado, 244  
 completo  
     emparejamiento, 242  
     grafo bipartido, 232  
     grafo, 181  
 componente, 187  
 composición de funciones, 32  
 condición de Hall, 242  
 conexo, 187  
 congruente, 128  
 conjugado  
     elemento, 332, 355  
     partición, 478  
     permutación, 116

conjunto, 1  
 de aristas, 178  
 de índices, 101  
 de vértices, 169  
 diferencia, 140  
 producto, 53, 56  
 vacío, 1  
 conjuntos disjuntos, 50  
 conmutador, 332  
 corte, 263  
 cota inferior, 5  
 cota superior, 7  
 crítico  
   actividad, 260  
   análisis de caminos, 260  
   camino, 260  
 cuadrado de Durfee, 495  
 cuadrado latino, 143  
 cuadrados latinos  
   mutuamente ortogonales, 146  
   latinos ortogonales, 144  
 cuadrángulo, 408  
 cuaterniones, 384  
 cuerpo, 364  
   de Galois, 396  
   no conmutativo, 384  
 decisión  
   árbol, 206  
   variable, 289  
 deficiencia, 245  
 definición recursiva, 7  
 derivada  
   de un polinomio, 384  
   de una serie de potencias, 472  
 desarreglo, 83  
 descodificación del vecino más próximo, 423  
 diagrama de Ferrers, 482  
 diagrama de flujo, 267  
 digrafo, 254  
 dimensión, 425  
 dirigido  
   camino, 255  
   ciclo, 255

grafo, 254  
 recorrido, 255  
 discreto, 6  
 diseño, 90  
 distancia entre palabras, 423  
 distancia mínima, 423  
 distribución, 42, 108  
 divisor  
   de un entero, 17  
   de un polinomio, 375  
 ecuación auxiliar  
   para recurrencias lineales, 279  
   para [RLH], 464  
 ecuación de clases, 357  
 eficiencia, 167  
 elemento inversible  
   de un anillo, 352  
   de  $Z_m$ , 135  
 elemento inverso  
   en un anillo, 362  
   en un grupo, 364  
   en  $Z_m$ , 135  
 elemento primitivo, 393  
 emparejamiento, 241  
 emparejamiento máximo, 241  
 entero gaussiano, 364  
 enteros módulo  $m$ , 132  
 enteros, 1  
 equivalencia  
   clase, 105  
   relación, 105  
 estabilizador, 342  
 factor  
   un entero, 17  
   un polinomio, 374  
 factorial, 9  
 familia de conjuntos, 101  
 finito, 44  
 flujo, 261  
   de entrada, 261  
   de salida, 261  
   forma estándar de una matriz de paridad, 430

fórmula de inversión de Möbius, 88  
 fracciones simples, 452  
 fuente, 261  
 función, 31  
   de Euler, 56  
   de inclusión, 35  
   de Möbius, 88  
   de peso, 214  
   exhaustiva, 34  
   generadora, 461  
 función inversa, 36  
   por la derecha, 38  
   por la izquierda, 38  
 función inyectiva, 34  
 función multiplicativa, 100  
 función polinómica, 379  
 generador  
   canónico, 440  
   de un grupo cíclico, 316  
 grado, 371  
   de entrada, 257  
   de salida, 257  
 grafo, 178  
   de Heawood, 251  
   de incidencia, 418  
   de Petersen, 183  
   ponderado, 214  
   r-regular, 185  
   regular, 185  
   rueda, 181  
 grupo, 303  
   abeliano, 309  
   aditivo de un cuerpo, 364  
   alternado, 337  
   cíclico infinito, 316  
   comutativo, 309  
   de automorfismos, 338  
   de orden infinito, 304  
   de permutaciones, 336  
   diedral, 503  
   multiplicativo de un cuerpo, 364  
   simétrico, 305  
   montículo, 211

hipótesis de inducción, 12  
 hoja, 204  
 ideal, 437  
   generado por  $f(x)$ , 438  
 identidad  
   función, 36  
 identificador, 153  
 impar  
   grafo, 201  
   permutación, 122  
   vértice, 185  
 indicador, 514  
 índice de un subgrupo, 325  
 inducción fuerte, 13  
 inducción, 10  
 infinito, 44  
 instrucción iterativa, 157  
 intersección, 1  
 invariante, 162  
 inversión, 359  
 k-cubo, 200  
 lineal  
   código, 425  
   polinomio, 378  
   recurrencia, 279  
 lista de adyacencias, 180  
 lista de adyacente, 180  
 logaritmo de Jacobi, 418  
 longitud  
   ciclo, 188  
   un código, 421  
   una palabra, 59  
 matriz de paridad, 428  
 máximo, 748  
 máximo común divisor  
   de enteros, 19  
   de polinomios, 374  
 merge sort, 284  
 método de Horner, 382  
 mientras-hacer, 157  
 mínimo, 6, 47

común múltiplo, 26  
residuo no negativo, 131  
módulo, 129  
multinomial  
    coeficiente, 112  
    número, 110  
    teorema, 112  
  
n-conjunto, 70  
neutro de un grupo, 304  
nilpotente, 384  
no numerable, 46  
numerable, 46  
número cromático, 194  
número de Stirling (de segunda clase), 103  
números de Fibonacci, 282  
  
 $O(g(n))$ , 166  
operación, 82  
    operación binaria, 303  
optimización recursiva, 285  
órbita, 340  
orden  
    de un elemento, 311  
    de un grupo, 304  
    lexicográfico de las particiones, 495  
ordenación, 172  
    de la burbuja, 173  
    de Williams, 209  
    por inserción, 174  
óvalo, 340  
  
palabra, 59  
    de un código, 421  
par  
    permutación, 122  
    subgrupo, 321  
    vértice, 185  
para-hasta-hacer, 157  
partes de una partición, 475  
partición, 101  
    autoconjungada, 479  
    de un entero, 113

permutación, 63  
peso de una palabra, 427  
pila, 220  
plano afín, 401  
polinomio, 367  
    constante, 368  
    irreducible, 377  
    mónico, 369  
    primitivo irreducible, 394  
primo, 22  
    cuerpo, 390  
    factorización, 22  
primos entre sí, 21  
principio  
    de adición, 50  
    de la criba, 80  
    de la multiplicación, 54  
    de las cajas, 42  
problema  
    problema de inversión, 291  
    problema de la mochila, 295  
    problema del árbol generador minimal, 215  
    problema del camino más corto, 225  
producto de polinomios, 368  
producto directo, 317  
programa, 153  
programación dinámica, 289  
programación estructurada, 158  
proyectivo  
    geometría, 404  
    plano, 405  
punto de una geometría finita, 400  
puntos diagonales en un cuadrágulo, 408  
puntos en el infinito, 404  
puntuación, 274  
  
r-ciclo, 188  
r-subconjunto, 70  
raíz  
    de un árbol, 203  
    de una ecuación polinómica, 380

recorrido, 186  
    euleriano, 189  
recta del infinito, 404  
recta en una geometría finita, 400  
rectángulo latino, 237  
recubrimiento de vértices, 253  
recurrencia lineal homogénea [RLH], 464  
recurrencia lineal no homogénea, 469  
red, 257  
    de actividad, 258  
relación, 230  
    de orden, 4  
    reflexiva, 104  
    simétrica, 105  
replicación, 91  
representación de un grupo por permutaciones, 351  
representación fiel, 353  
representación no fiel, 351  
resto, 14  
  
secuencia gráfica, 201  
selección ordenada  
    con repetición, 75  
    sin repetición, 60, 70  
sentencia condicional, 155  
sentencia de asignación, 154  
serie de potencias, 447  
si-entonces-si no, 155  
signo de una permutación, 122  
símbolo de Prüfer, 230  
sistema triple de Steiner, 98  
subanillo, 448  
subconjunto, 1  
    generador, 388  
    propio, 47  
subcuerpo, 417  
subgrupo, 319  
sucesión de puntuaciones, 274  
sucesión, 32  
suma de polinomios, 368  
sumidero, 261

t-diseño, 94  
tabla de grupo, 306  
tamaño, 41  
teorema  
    chino del resto, 147  
    de Enter, 137  
    de Fermat, 137  
    de Lagrange, 325  
    de Pólya, 517  
    del elemento primitivo, 392  
    del factor, 379  
    del flujo máximo y corte mínimo, 264  
    fundamental de la aritmética, 24  
tipo de una permutación, 115  
tiempo flotante, 260  
transformación de etapa, 290  
transitivo  
    campeonato, 274  
    relación, 104  
transversal, 249  
    simultáneo, 253  
trasposición, 119  
triángulo de Pascal, 72  
  
unión, 1  
  
valor  
    absoluto, 32  
    booleano, 155  
    de un flujo, 261  
    de un identificador, 153  
    de una función, 31  
    de verdad, 155  
variable de estado, 290  
vecino, 180  
vértice  
    de articulación, 230  
    coloración, 194  
    interno, 204

