TERCERA EDICIÓN

ESTRUCTURAS DE MATEMÁTICAS DISCRETAS PARA LA COMPUTACIÓN

Bernard Kolman
Drexel University

Robert C. Busby
Drexel University

Sharon Ross
DeKalb College

TRADUCCIÓN:

Oscar Alfredo Palmas Velasco
Facultad de Ciencias, UNAM

REVISIÓN TÉCNICA:

Víctor Hugo Ibarra Mercado
Lic. en Física y Matemáticas
ESFM IPN

Pearson Educación

MÉXICO • ARGENTINA • BRASIL • COLOMBIA • COSTA RICA • CHILE
ESPAÑA • GUATEMALA • PERÚ • PUERTO RICO • VENEZUELA

23973

Lista de símbolos de uso frecuente

Capítulo 1

$a, b, c, x, y, z,$	elementos de un conjunto, p. 2
$\in$	pertenece a, p. 2
$\mathbb{Z}^+$	el conjunto de todos los enteros positivos, p. 2
N	el conjunto de todos los números naturales, p. 2
Z	el conjunto de todos los enteros, p. 2
$\mathbb{R}$	el conjunto de todos los números reales, p. 2
$\varnothing$	el conjunto vacío, p. 2
$\subseteq$	es subconjunto de, p. 3
U	el conjunto universal, p. 3
$\lvert A\rvert$	la cardinalidad de A, p. 4
$P(A)$	el conjunto de todos los subconjuntos de A, p. 4
$A \cup B$	la unión de los conjuntos A y B, p. 6
$A \cap B$	la intersección de los conjuntos A y B, p. 6
$A - B$	el complemento de B con respecto a A, p. 7
$\overline{A}$	el complemento de A, p. 7
$A \oplus B$	la diferencia simétrica de los conjuntos A y B, p. 9
A^*	el conjunto de todas las sucesiones finitas de elementos de A, p. 19
Λ	la secuencia o cadena vacía, p. 19
MCD (a, b)	el máximo común divisor de a y b, p. 24
MCM (a, b)	el mínimo común múltiplo de a y b, p. 26
$\equiv r \pmod{a}$	congruente con r mód a, p. 27
$\mathbf{A}^T$	la transpuesta de la matriz $\mathbf{A}$, p. 34
$\mathbf{A} \vee \mathbf{B}$	la unión de $\mathbf{A}$ y $\mathbf{B}$, p. 35
$\mathbf{A} \wedge \mathbf{B}$	conjunción de $\mathbf{A}$ y $\mathbf{B}$, p. 35
$\mathbf{A} \odot \mathbf{B}$	el producto booleano de $\mathbf{A}$ y $\mathbf{B}$, p. 36

Capítulo 2

$\sim p$	no p, p. 47
$p \wedge q$	p y q, p. 48
$p \vee q$	p o q, p. 48
$\forall$	para todos, p. 50
$\exists$	existe, p. 50
$p \to q$	p implica a q, p. 52
$p \leftrightarrow q$	p es equivalente a q, p. 53

Capítulo 3

${}_nP_r$	el número de permutaciones de n objetos tomados r a la vez, p. 75
$n!$	n-factorial, p. 75
${}_nC_r$	el número de combinaciones de n objetos tomados r a la vez, p. 78
$p(E)$	la probabilidad del evento E, p. 87
f_E	la frecuencia de ocurrencia del evento E, p. 88

Capítulo 4

$A \times B$	el producto cartesiano de A y B, p. 102
$R(x)$	el conjunto relativo de x, p. 109
$R(A)$	el conjunto relativo de A, p. 109
$\mathbf{M}_R$	la matriz de R, p. 111
R^∞	la relación de conectividad de R, la cerradura transitiva de R, p. 117
R^*	la relación de alcanzabilidad de R, p. 121
Δ	la relación de igualdad, p. 124
$[a]$	la clase de equivalencia de a, p. 134
A/R	una partición del conjunto A determinada por la relación de equivalencia R sobre A, p. 134
$S \circ R$	la composición de R y S, p. 152

Capítulo 5

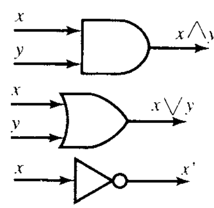
1_A	la función identidad sobre A, p. 170
f^{-1}	la inversa de la función f, p. 173
f_A	la función característica de un conjunto A, p. 177
$\lfloor x \rfloor$	el entero más grande menor que o igual a x, p. 178
$\lceil x \rceil$	el entero más pequeño mayor que o igual a x, p. 178
$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ p(a_1) & p(a_2) & \dots & p(a_n) \end{pmatrix}$	permutación del conjunto $A = \{a_1, a_2, \dots, a_n\}$, p. 181
$O(f)$	el orden de una función f, p. 190
$\Phi(f)$	la clase θ de una función f, p. 192

Capítulo 6

(V, E, γ)	la gráfica con vértices en V y en E, p. 197
D_n	la gráfica discreta sobre n vértices, p. 200
K_n	la gráfica completa sobre n vértices, p. 200
L_n	la gráfica lineal sobre n vértices, p. 200
G_e	la subgráfica obtenida omitiendo e de G, p. 202
G^R	la gráfica cociente con respecto a R, p. 202
$\chi(G)$	el número cromático de G, p. 218
P_G	el polinomio cromático de G, p. 220

Capítulo 7

$\leq$	una relación parcialmente ordenado, p. 226
$a \vee b$, LUB(a, b)	la mínima cota superior de a y b, p. 242
$a \wedge b$, GLB(a, b)	la máxima cota inferior de a y b, p. 242
a'	el complemento de a, p. 254



compuerta and, p. 269

compuerta or, p. 269

inversor (NOT), p. 269

Capítulo 8

(T, v_0)	el árbol con raíz v_0, p. 287
$T(v)$	el subárbol de T con raíz v, p. 290

Capítulo 9

S^S	el conjunto de todas las funciones de S a S, p. 335
S/R	el semigrupo cociente de un semigrupo S, p. 343
Z_n	el conjunto cociente $Z/\equiv$ (mód n), p. 344
f_R	homomorfismo natural de S sobre S/R, p. 345
aH	clase lateral izquierda de H en G, p. 363

Capítulo 10

$(V, S, v_0, \mapsto)$	gramática de estructura de oraciones, p. 370
$\Rightarrow$	derivabilidad directa, p. 370
$\langle\ \rangle ::=$	especificación BNF de una gramática, p. 378
$L(G)$	el lenguaje de G, p. 371
$\mathcal{F}$	el conjunto de funciones de transición de una máquina de estado finito, p. 391
$(S, I, \mathcal{F})$	una máquina de estado finito, p. 391
f_x	la función de transición correspondiente a la entrada x, p. 391
$(S, I, \mathcal{F}, s_0, T)$	máquina de Moore, p. 393
M/R	máquina cociente de la máquina M, p. 394
$l(w)$	la longitud de una cadena w, p. 376

Capítulo 11

e	una función codificadora (m, n), p. 422
$\delta(x, y)$	la distancia entre las palabras x y y, p. 424
$\mathbf{A} \oplus \mathbf{B}$	la suma mód 2 de $\mathbf{A}$ y $\mathbf{B}$, p. 426
$\mathbf{A} * \mathbf{B}$	el producto booleano mód 2 de $\mathbf{A}$ y $\mathbf{B}$, p. 427
d	una función decodificadora (n, m), p. 432
ϵ_j	clase lateral principal, p. 436
$x * \mathbf{H}$	el síndrome de x, p. 439

CONTENIDO

CAPÍTULO 1

CONCEPTOS FUNDAMENTALES

Requisitos previos

No hay requisitos previos formales para este capítulo; se recomienda al lector estudiarlo cuidadosamente y seguir el desarrollo de todos los ejemplos.

En este capítulo se proporciona algunas de las herramientas básicas de las matemáticas discretas. Comienza con los conjuntos, subconjuntos y sus operaciones, nociones que quizá ya sean conocidas por usted. En seguida trata de las sucesiones y utiliza esquemas tanto explícitos como recursivos. Luego se revisan algunas de las propiedades básicas de la divisibilidad de los enteros y, por último, se ve las matrices y sus operaciones. Esto proporciona el ambiente de fondo necesario para iniciar la exploración de las estructuras matemáticas.

1.1. Conjuntos y subconjuntos

Conjuntos

Un **conjunto** es un grupo o colección de objetos, a los que se conoce como **elementos** o **miembros** del mismo. Por ejemplo, la colección de todas las sillas de madera, la colección de todos los pájaros negros de una pata, o la colección de los números reales comprendidos entre cero y uno, son, cada uno, un conjunto. Bien definido, significa simplemente que es posible decidir si un objeto dado pertenece o no a la colección. Casi todos los objetos matemáticos, antes que todo, son conjuntos, independientemente de otras propiedades adicionales que puedan poseer. Así, la teoría de los conjuntos es, en cierto sentido, el cimiento sobre el que se construye prácticamente todas las matemáticas. A pesar de esto, dicha teoría (por lo menos la de la clase informal que se necesita) es fácil de aprender y de usar.

Una forma de describir un conjunto con un número finito de elementos, es hacer una lista de los elementos del conjunto y encerrarla entre llaves. Así, el conjunto de todos los enteros positivos menores que 4, puede escribirse así

$$\{1, 2, 3\}. \qquad (1)$$

No es importante el orden en que se ponga en la lista los elementos del conjunto. Así, $\{1, 3, 2\}$, $\{3, 2, 1\}$, $\{3, 1, 2\}$, $\{2, 1, 3\}$ y $\{2, 3, 1\}$ son todos representaciones del conjunto que se da en (1). Además, puede hacerse caso omiso de los elementos repetidos en la *lista* de elementos de un conjunto. Así $\{1, 3, 2, 3, 1\}$ es otra representación del conjunto dado en (1).

Se emplea letras mayúsculas, como A, B, C para designar los conjuntos, y letras minúsculas, como a, b, c, x, y, z, t para designar los miembros (o elementos) de los conjuntos.

Para indicar que x es un elemento del conjunto A, se escribe $x \in A$. También se indica el hecho de que x no es un elemento de A, escribiendo $x \notin A$.

Ejemplo 1. Sea $A = \{1, 3, 5, 7\}$. Entonces $1 \in A$, $3 \in A$, pero $2 \notin A$. ◆

En ocasiones no es conveniente o es imposible describir un conjunto por medio de una lista de todos sus elementos. Otra manera útil de definir un conjunto, es especificando una propiedad que los elementos del conjunto tengan en común. Se utiliza la notación $P(x)$ para denotar una oración o enunciado P relativo al objeto variable x. El objeto definido por $P(x)$, escrito en la forma $\{x \mid P(x)\}$, es simplemente la colección de todos los objetos x para los cuales P es sensible y cierto. Por ejemplo, $\{x \mid x \text{ es un entero positivo menor que } 4\}$ es el conjunto $\{1, 2, 3\}$ descrito en (1) mediante el listado de sus elementos.

Ejemplo 2. El conjunto formado por todas las letras de la palabra "byte" puede denotarse por $\{b, y, t, e\}$ o por $\{x \mid x \text{ es una letra de la palabra "byte"}\}$. ◆

Ejemplo 3. Aquí se presenta varios conjuntos y sus respectivas notaciones, que serán usadas en todo este libro.

(a) $Z^+ = \{x \mid x \text{ es un entero positivo}\}$.
En consecuencia, Z^+ está formado por los números usados para contar: 1, 2, 3, ...
(b) $N = \{x \mid x \text{ es un entero positivo}\}$.
En consecuencia, N está formado por los enteros positivos: 0, 1, 2, ...
(c) $Z = \{x \mid x \text{ es un entero}\}$.
En consecuencia, Z está formado por todos los enteros: . . . , −3, −2, −1, 0, 1, 2, 3, ...
(d) $R = \{x \mid x \text{ es un número real}\}$.
(e) El conjunto que no tiene elementos se denota por $\{\ \}$ o por el símbolo $\varnothing$ y se denomina conjunto vacío. ◆

Ejemplo 4. Como el cuadrado de un número real es siempre no negativo, $\{x \mid x \text{ es un número real y } x^2 = -1\} = \varnothing$. ◆

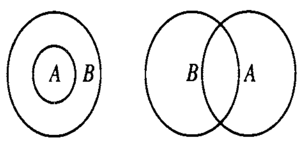
Se dice que un conjunto es completamente conocido cuando se conoce todos sus miembros. Se dice así, que dos conjuntos A y B son **iguales** si tienen los mismos elementos, y se escribe $A = B$.

Ejemplo 5. Si $A = \{1, 2, 3\}$ y $B = \{x \mid x \text{ es un entero positivo y } x^2 < 12\}$, entonces $A = B$. ◆

Ejemplo 6. Si $A = \{\text{BASIC, PASCAL, ADA}\}$ y $B = \{\text{ADA, BASIC, PASCAL}\}$, entonces $A = B$. ◆

Subconjuntos

Si cada elemento de A es también un elemento de B, es decir, si siempre que $x \in A$ ocurre que $x \in B$, se dice que A es un **subconjunto** de B o que A está **contenido en** B, y se escribe $A \subseteq B$. Si A no es un subconjunto de B, se escribe $A \nsubseteq B$. (Véase la figura 1.1.)



$A \subseteq B$ $\qquad$ $A \nsubseteq B$

Figura 1.1

A los diagramas como los que aparecen en la figura 1.1, empleados para mostrar relaciones entre conjuntos, se los llama **diagramas de Venn**, en honor del lógico británico John Venn. Los diagramas de Venn serán de mucha utilidad en la sección 1.2.

Ejemplo 7. Se tiene que $Z^+ \subseteq Z$. Por otra parte, si Q denota el conjunto de todos los números racionales, entonces $Z \subseteq Q$. ◆

Ejemplo 8. Sean $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 5\}$, y $C = \{1, 2, 3, 4, 5\}$. Entonces, $B \subseteq A$, $B \subseteq C$ y $C \subseteq A$. Sin embargo, $A \nsubseteq B$, $A \nsubseteq C$ y $C \nsubseteq B$. ◆

Ejemplo 9. Si A es un conjunto cualquiera, $A \subseteq A$. Es decir, todo conjunto es un subconjunto de sí mismo. ◆

Ejemplo 10. Sea A un conjunto y sea $B = \{A, \{A\}\}$. Entonces, como A y $\{A\}$ son elementos de B, se tiene que $A \in B$ y $\{A\} \in B$. Se desprende que $\{A\} \subseteq B$ y $\{\{A\}\} \subseteq B$. Sin embargo, no es cierto que $A \subseteq B$. ◆

Para un conjunto cualquiera A, como no hay elementos de $\varnothing$ que no estén en A, se tiene que $\varnothing \subseteq A$. (Esto se verá de nuevo en la sección 2.1.)

Es fácil ver que $A = B$ si y solamente si $A \subseteq B$ y $B \subseteq A$. (Esto se demuestra en la sección 2.3.)

Se puede expresar la conclusión de que la colección de todas las cosas, o sea de todo, no puede considerarse como un conjunto sin destruir la estructura lógica de las matemáticas. Para evitar éste y otros problemas de los que no es necesario ocuparse aquí, se supondrá que para cada caso que se presenta existe un *conjunto universal* U (que puede variar según el caso) que contiene todos los objetos para los que tiene sentido la discusión del caso. Para cualquier otro conjunto que se mencione en la presentación, se supondrá automáticamente que es un subconjunto de U. Por tanto, si se está tratando de los números reales y se menciona los conjuntos A y B, entonces se supondrá que A y B deben ser conjuntos de números reales, no matrices, ni circuitos electrónicos ni monos de laboratorio. En la mayoría de los problemas, se verá de inmediato la existencia de un conjunto universal U por el planteamiento del problema. En los diagramas de Venn, el conjunto universal U se denotará por un rectángulo, mientras que los conjuntos dentro de U serán denotados por círculos, como aparece en la figura 1.2.

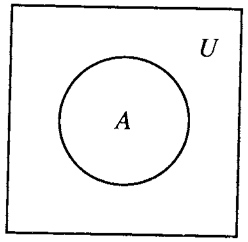


Figura 1.2

Se dice que un conjunto A es **finito** si tiene n elementos distintos, siendo $n \in N$. En este caso, a n se le llama **cardinalidad** de A y se designa por $|A|$. Por tanto, los conjuntos de los ejemplos 1, 2, 4, 5 y 6 son finitos. A un conjunto que no es finito se lo llama **infinito**. Los conjuntos presentados en los ejemplos 3 (excepto $\varnothing$) y 7 son conjuntos infinitos.

Si A es un conjunto, el conjunto de todos los subconjuntos de A se denomina **conjunto potencia** de A y se designa por $P(A)$.

Ejemplo 11. Sea $A = \{1, 2, 3\}$. Entonces $P(A)$ está formado por los siguientes subconjuntos de A: $\{\ \}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, y $\{1, 2, 3\}$ (es decir A). En una sección posterior, se contará el número de subconjuntos que puede tener un conjunto. ◆

GRUPO DE EJERCICIOS 1.1

1. Sea $A = \{1, 2, 4, a, b, c\}$. Identifique cada uno de los siguientes casos como verdadero o falso.
(a) $2 \in A$ (b) $3 \in A$ (c) $c \notin A$
(d) $\varnothing \in A$ (e) $\{\ \} \notin A$ (f) $A \in A$

2. Sea $A = \{x \mid x$ es un número real y $x < 6\}$. Identifique cada uno de los siguientes casos como verdadero o falso.
(a) $3 \in A$ (b) $6 \in A$ (c) $5 \notin A$
(d) $8 \notin A$ (e) $-8 \in A$ (f) $5.4 \notin A$

3. En cada parte, haga un conjunto con las letras de cada palabra haciendo una lista de los elementos del conjunto.
(a) AARDVARK (b) BOOK
(c) MISSISSIPPI

4. En cada parte, forme un conjunto haciendo una lista de sus elementos.
(a) El conjunto de todos los enteros positivos que son menores que diez
(b) $\{x \mid x \in Z$ y $x^2 < 12\}$

5. En cada parte, escriba el conjunto en la forma $\{x \mid P(x)\}$, en donde $P(x)$ es una propiedad que describe los elementos del conjunto.
(a) $\{2, 4, 6, 8, 10\}$ (b) $\{a, e, i, o, u\}$
(c) $\{1, 8, 27, 64, 125\}$ (d) $\{-2, -1, 0, 1, 2\}$

6. Sea $A = \{1, 2, 3, 4, 5\}$. ¿Cuáles de los siguientes conjuntos son iguales a A?
(a) $\{4, 1, 2, 3, 5\}$ (b) $\{2, 3, 4\}$ (c) $\{1, 2, 3, 4, 5, 6\}$
(d) $\{x \mid x$ es un entero y $x^2 \leq 25\}$
(e) $\{x \mid x$ es un entero positivo y $x \leq 5\}$
(f) $\{x \mid x$ es un número racional positivo y $x \leq 5\}$

7. ¿Cuáles de los siguientes conjuntos son conjuntos vacíos?
(a) $\{x \mid x$ es un número real y $x^2 - 1 = 0\}$
(b) $\{x \mid x$ es un número real y $x^2 + 1 = 0\}$
(c) $\{x \mid x$ es un número real y $x^2 = -9\}$
(d) $\{x \mid x$ es un número real y $x = 2x + 1\}$
(e) $\{x \mid x$ es un número real y $x = x + 1\}$

8. Haga una lista de todos los subconjuntos de $\{a, b\}$.

9. Haga una lista de todos los subconjuntos de {BASIC, PASCAL, ADA}.

10. Haga una lista de todos los subconjuntos de $\{\ \}$.

11. Sea $A = \{1, 2, 5, 8, 11\}$. Identifique cada uno de los siguientes casos como verdadero o falso.
(a) $\{5, 1\} \subseteq A$ (b) $\{8, 1\} \in A$
(c) $\{1, 8, 2, 11, 5\} \not\subseteq A$ (d) $\varnothing \subseteq A$
(e) $\{1, 6\} \not\subseteq A$ (f) $\{2\} \subseteq A$
(g) $\{3\} \notin A$ (h) $A \subseteq \{11, 2, 5, 1, 8, 4\}$

12. Sea $A = \{x \mid x$ es un entero y $x^2 < 16\}$. Identifique cada uno de los siguientes casos como verdadero o falso.
(a) $\{0, 1, 2, 3\} \subseteq A$ (b) $\{-3, -2, -1\} \subseteq A$
(c) $\{\ \} \subseteq A$
(d) $\{x \mid x$ es un entero y $|x| < 4\} \subseteq A$
(e) $A \subseteq \{-3, -2, -1, 0, 1, 2, 3\}$

13. Sean $A = \{1\}$, $B = \{1, a, 2, b, c\}$, $C = \{b, c\}$, $D = \{a, b\}$, y $E = \{1, a, 2, b, c, d\}$. Para cada parte, sustituya el símbolo □ por $\subseteq$ o $\not\subseteq$ para dar un enunciado verdadero.
(a) $A \ \square\ B$ (b) $\varnothing \ \square\ A$ (c) $B \ \square\ C$
(d) $C \ \square\ E$ (e) $D \ \square\ C$ (f) $B \ \square\ E$

14. En cada parte, encuentre el conjunto de cardinalidad más pequeña que contenga los conjuntos dados como subconjuntos.
(a) $\{a, b, c\}$, $\{a, d, e, f\}$, $\{b, c, e, g\}$
(b) $\{1, 2\}$, $\{1, 3\}$, $\varnothing$ (c) $\{1, a\}$, $\{b, 2\}$

15. Utilice el diagrama de Venn de la figura 1.3 para identificar cada uno de los siguientes casos como verdadero o falso.
(a) $A \subseteq B$ (b) $B \subseteq A$ (c) $C \subseteq B$
(d) $x \in B$ (e) $x \in A$ (f) $y \in B$

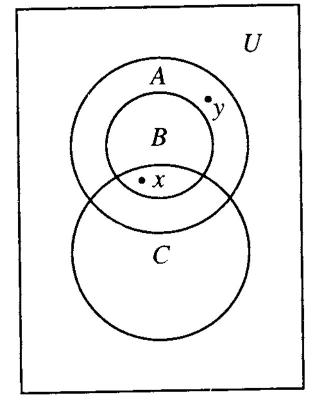


Figura 1.3

16. (a) Si $A = \{3, 7\}$, encuentre $P(A)$.
(b) ¿Qué es $|A|$? (c) ¿Qué es $P(A)$?

17. (a) Si $A = \{3, 7, 2\}$, encuentre $P(A)$.
(b) ¿Qué es $|A|$? (c) ¿Qué es $P(A)$?

18. Dibuje un diagrama de Venn que represente estas relaciones.
(a) $A \subseteq B$, $A \subseteq C$, $B \not\subseteq C$, y $C \not\subseteq B$
(b) $x \in A$, $x \in B$, $x \notin C$, $y \in B$, $y \in C$, y $y \notin A$

19. Describa todas las relaciones entre subconjuntos que existan para los conjuntos dados en el ejemplo 3.

20. Demuestre que si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

1.2. Operaciones con conjuntos

En esta sección se analizará varias operaciones que permiten combinar conjuntos dados para formar nuevos conjuntos. Estas operaciones, análogas a las operaciones conocidas que se efectúa con los números reales, jugarán un papel clave en las numerosas aplicaciones e ideas siguientes.

Si A y B son conjuntos, se define su **unión** como el conjunto formado por todos los elementos que pertenecen a A o a B y se denota por $A \cup B$. Así,

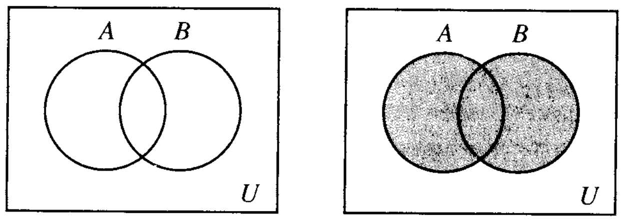
$$A \cup B = \{x \mid x \in A \text{ o bien, } x \in B\}.$$

Debe observarse que $x \in A \cup B$ si $x \in A$ o $x \in B$, o bien x pertenece a ambos, A y B.

Ejemplo 1. Sean $A = \{a, b, c, e, f\}$ y $B = \{b, d, r, s\}$. Encuentre $A \cup B$.

Solución: Como $A \cup B$ está formado por todos los elementos que pertenecen ya sea a A o a B, $A \cup B = \{a, b, c, d, e, f, r, s\}$. ◆

Puede ilustrarse la unión de dos conjuntos con un diagrama de Venn, como sigue. Si A y B son los conjuntos dados en la figura 1.4(a), entonces $A \cup B$ es el conjunto representado por la región sombreada de la figura 1.4(b).



(a) (b) $A \cup B$

Figura 1.4

Si A y B son conjuntos, se define su **intersección** como el conjunto formado por todos los elementos que pertenecen a ambos conjuntos, A y B, y se designa por $A \cap B$. En consecuencia, $A \cap B = \{x \mid x \in A \text{ y } x \in B\}$.

Ejemplo 2. Sean $A = \{a, b, c, e, f\}$, $B = \{b, e, f, r, s\}$, y $C = \{a, t, u, v\}$. Encuentre $A \cap B$, $A \cap C$, y $B \cap C$.

Solución: Los elementos b, e y f son los únicos que pertenecen a ambos conjuntos, A y B, de modo que $A \cap B = \{b, e, f\}$. De modo semejante, $A \cap C = \{a\}$. No hay elementos que pertenezcan a los dos conjuntos, B y C, de modo que $B \cap C = \{\ \}$. ◆

Cuando dos conjuntos no tienen elementos comunes, como B y C en el ejemplo 2, se denominan **conjuntos disjuntos**.

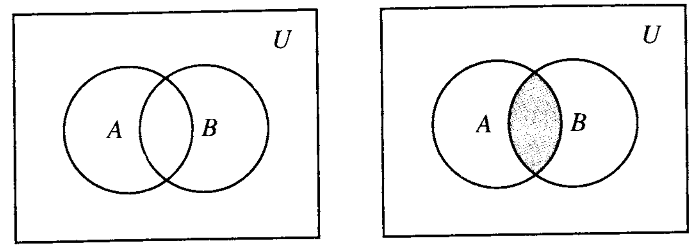
Se puede ilustrar la intersección de dos conjuntos con un diagrama de Venn, como sigue. Si A y B son los conjuntos dados en la figura 1.5(a), entonces $A \cap B$ es el conjunto representado por la región sombreada de la figura 1.5(b). La figura 1.6 muestra un diagrama de Venn para dos conjuntos disjuntos.

Las operaciones de unión e intersección pueden definirse para tres o más conjuntos de manera obvia.

$$A \cup B \cup C = \{x \mid x \in A; \text{ o, } x \in B; \text{ o, } x \in C\}$$

y

$$A \cap B \cap C = \{x \mid x \in A; \text{ y, } x \in B; \text{ y, } x \in C\}.$$



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

Figura 1.5

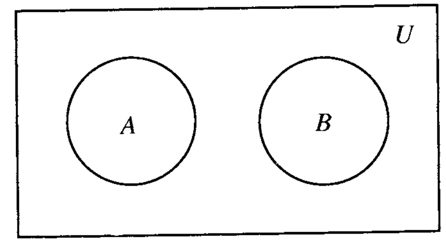


Figura 1.6

La región sombreada de la figura 1.7(b) es la unión de los conjuntos A, B y C que aparecen en la figura 1.7(a), y la región sombreada de la figura 1.7(c) es la intersección de los conjuntos A, B y C. Nótese que la figura 1.7(a) no dice nada acerca de posibles relaciones entre los conjuntos, pero que sí deja margen para todas las relaciones posibles. En general, si A_1, $A_2, \ldots, A_n$ son subconjuntos de U, entonces $A_1 \cup A_2 \cup \cdots \cup A_n$ se denotará por $\bigcup_{k=1}^{n} A_k$; y, $A_1 \cap A_2 \cap \cdots \cap A_n$ se denotará por $\bigcap_{k=1}^{n} A_k$.

Ejemplo 3. Sea $A = \{1, 2, 3, 4, 5, 7\}$, $B = \{1, 3, 8, 9\}$, y $C = \{1, 3, 6, 8\}$. Entonces $A \cap B \cap C$ es el conjunto de elementos que pertenecen a A, B y C. En consecuencia $A \cap B \cap C = \{1, 3\}$. ◆

Si A y B son dos conjuntos, se define el **complemento de B con respecto de A** como el conjunto de todos los elementos que pertenecen a A pero no a B, y se denota por $A - B$. En consecuencia,

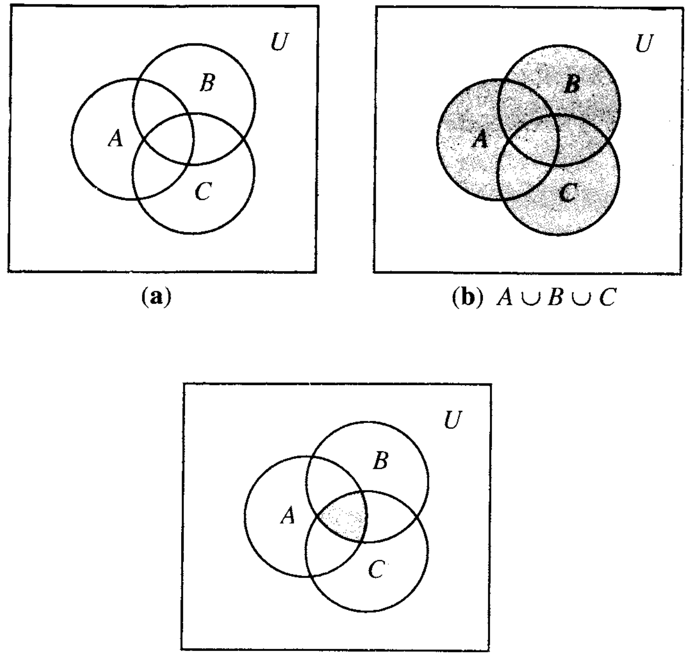
$$A - B = \{x \mid x \in A; \text{ y, } x \notin B\}.$$

Ejemplo 4. Sean $A = \{a, b, c\}$ y $B = \{b, c, d, e\}$. Entonces $A - B = \{a\}$ y $B - A = \{d, e\}$. ◆

Si A y B son los conjuntos de la figura 1.8(a), entonces $A - B$ y $B - A$ están representados por las regiones sombreadas de las figuras 1.8(b) y 1.8(c), respectivamente.

Si U es un conjunto universal que contiene a A, entonces $U - A$ se denomina **complemento** de A y se designa por $\overline{A}$. Así $\overline{A} = \{x \mid x \notin A\}$.

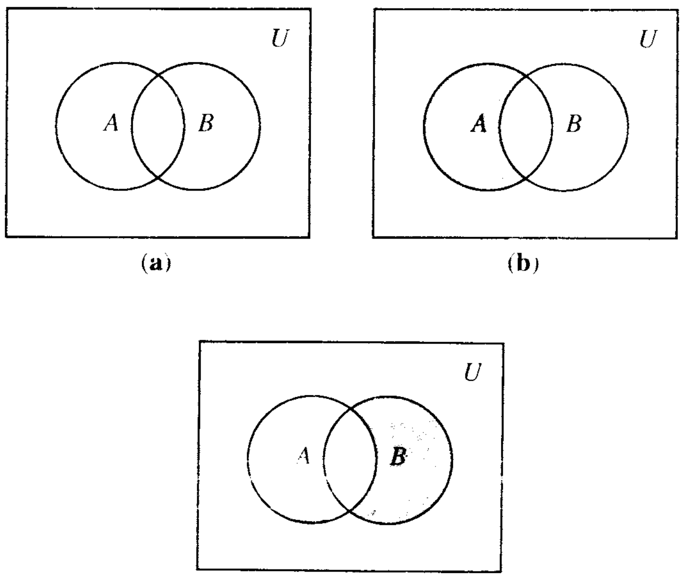
Ejemplo 5. Sean $A = \{x \mid x \text{ es un entero y } x \leq 4\}$ y $U = Z$. Entonces $\overline{A} = \{x \mid x \text{ es un entero y } x > 4\}$. ◆



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

(c) $A \cap B \cap C$

Figura 1.7



(a) (b)

(c)

Figura 1.8

Si A es el conjunto de la figura 1.9, su complemento es la región sombreada en esa figura.

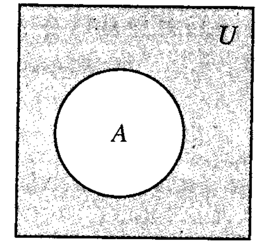


Figura 1.9

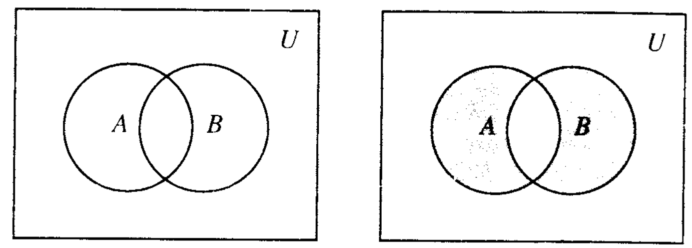
Si A y B son dos conjuntos, se define su **diferencia simétrica** como el conjunto de todos los elementos que pertenecen a A o a B, pero no a ambos, A y B, y se designa por $A \oplus B$. Así,

$$A \oplus B = \{x \mid (x \in A \text{ y } x \notin B), \text{ o } (x \in B \text{ y } x \notin A)\}.$$

Ejemplo 6. Sean $A = \{a, b, c, d\}$ y $B = \{a, c, e, f, g\}$. Entonces $A \oplus B = \{b, d, e, f, g\}$. ◆

Si A y B son como se indica en la figura 1.10(a), su diferencia simétrica es la región sombreada que aparece en la figura 1.10(b). Es fácil ver que

$$A \oplus B = (A - B) \cup (B - A).$$



(a) (b) $A \oplus B$

Figura 1.10

Propiedades algebraicas de las operaciones con conjuntos

Las operaciones con conjuntos que se acaba de definir satisfacen muchas propiedades algebraicas, algunas de las cuales son similares a las propiedades algebraicas que satisfacen los números reales y sus operaciones. Todas las propiedades principales anotadas aquí pueden ser demostradas por medio de las definiciones dadas y las reglas de la lógica. Se presentará la demostración de algunas de las propiedades y se dejará las demostraciones restantes como ejercicios para el lector. Los diagramas de Venn son útiles a menudo para sugerir o justificar el método de demostración.

Teorema 1. *Las operaciones definidas para realizarse con conjuntos satisfacen las siguientes propiedades:*

Propiedades conmutativas

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$

Propiedades asociativas

3. $A \cup (B \cup C) = (A \cup B) \cup C$
4. $A \cap (B \cap C) = (A \cap B) \cap C$

Propiedades distributivas

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Propiedades idempotentes

7. $A \cup A = A$
8. $A \cap A = A$

Propiedades del complemento

9. $\overline{(\overline{A})} = A$
10. $A \cup \overline{A} = U$
11. $A \cap \overline{A} = \varnothing$
12. $\overline{\varnothing} = U$
13. $\overline{U} = \{\,\}$
14. $\overline{A \cup B} = \overline{A} \cap \overline{B}$
15. $\overline{A \cap B} = \overline{A} \cup \overline{B}$ *Las propiedades 14 y 15 son conocidas como leyes de De Morgan.*

Propiedades de un conjunto universal

16. $A \cup U = U$
17. $A \cap U = A$

Propiedades del conjunto vacío

18. $A \cup \varnothing = A$ o $A \cup \{\,\} = A$
19. $A \cap \varnothing = \varnothing$ o $A \cap \{\,\} = \{\,\}$

Demostración: Se demostrará aquí la propiedad 14 y se dejará las demostraciones de las propiedades restantes al lector. Un estilo común de demostración para enunciados relativos a conjuntos, consiste en escoger un elemento en uno de los conjuntos y ver lo que se sabe acerca de éste. Supóngase que $x \in \overline{A \cup B}$. Entonces se sabe que $x \notin A \cup B$, de manera que $x \notin A$ y $x \notin B$. (¿Por qué?) Esto significa que $x \in \overline{A} \cap \overline{B}$ (¿por qué?), de modo que cada elemento de $\overline{A \cup B}$ pertenece a $\overline{A} \cap \overline{B}$. En consecuencia $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. Recíprocamente, supóngase que $x \in \overline{A} \cap \overline{B}$. Entonces $x \notin A$ y $x \notin B$ (¿por qué?), de modo que $x \notin A \cup B$, lo cual significa que $x \in \overline{A \cup B}$. En consecuencia, cada elemento de $\overline{A} \cap \overline{B}$ también pertenece a $\overline{A \cup B}$, y $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. Ahora se observa que $\overline{A \cup B} = \overline{A} \cap \overline{B}$. ●

El principio de adición

Supóngase ahora que A y B son conjuntos finitos de un conjunto universal U. Con frecuencia es útil tener una fórmula para $|A \cup B|$, la cardinalidad de la unión. Si A y B son conjuntos disjuntos, es decir, si $A \cap B = \varnothing$, entonces cada elemento de $A \cup B$ aparece ya sea en A o en B, pero no en ambos; por lo tanto, $|A \cup B| = |A| + |B|$. Si A y B se superponen, como se muestra en la figura 1.11, entonces los elementos de $A \cap B$ pertenecen a ambos conjuntos, y la suma $|A| + |B|$ cuenta estos elementos dos veces. Para corregir este doble conteo, se resta $|A \cap B|$. Como consecuencia, se tiene el siguiente teorema, al que se denomina a veces **principio de adición**. Debido a lo que aparece en la figura 1.11, se conoce también a éste como *principio de inclusión-exclusión.*

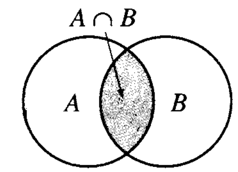


Figura 1.11

Teorema 2. *Si A y B son conjuntos finitos, entonces* $|A \cup B| = |A| + |B| - |A \cap B|$. ●

Ejemplo 7. Sean $A = \{a, b, c, d, e\}$ y $B = \{c, e, f, h, k, m\}$. Verifique el teorema 2.

Solución: Se tiene que $A \cup B = \{a, b, c, d, e, f, h, k, m\}$ y $A \cap B = \{c, e\}$. También, $|A| = 5$, $|B| = 6$, $|A \cup B| = 9$, y $|A \cap B| = 2$. Entonces $|A| + |B| - |A \cap B| = 5 + 6 - 2$, o sea 9, y el teorema 2 está verificado. ♦

Si A y B son conjuntos disjuntos, $A \cap B = \varnothing$ y $|A \cap B| = 0$, de manera que la fórmula del teorema 2 se convierte ahora en $|A \cup B| = |A| + |B|$. Este caso especial puede enunciarse en una forma que resulta útil para una variedad de situaciones de conteo.

El principio de adición para conjuntos disjuntos

Si un trabajo o tarea T_1 puede efectuarse exactamente de n maneras, y una tarea T_2 puede efectuarse exactamente de m maneras, el número de formas de realizar la tarea T_1 o la tarea T_2 es $n + m$.

La situación para tres conjuntos es un poco más complicada, como se muestra en la figura 1.12. Puede enunciarse en principio de adición para tres conjuntos sin lugar a dudas.

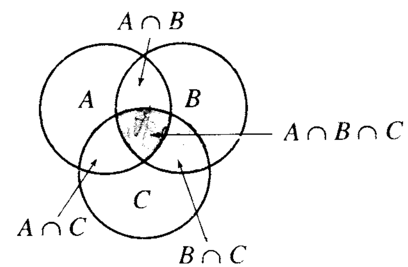


Figura 1.12

Teorema 3. *Sean A, B y C conjuntos finitos. Entonces,* $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$. ●

Ejemplo 8. Sean $A = \{a, b, c, d, e\}$, $B = \{a, b, e, g, h\}$, y $C = \{b, d, e, g, h, k, m, n\}$. Verifique el teorema 3.

Solución: Se tiene que $A \cup B \cup C = \{a, b, c, d, e, g, h, k, m, n\}$, $A \cap B = \{a, b, e\}$, $A \cap C = \{b, d, e\}$, $B \cap C = \{b, e, g, h\}$, y $A \cap B \cap C = \{b, e\}$, de manera que $|A| = 5$, $|B| = 5$, $|C| = 8$, $|A \cup B \cup C| = 10$, $|A \cap B| = 3$, $|A \cap C| = 3$, $|B \cap C| = 4$, y $|A \cap B \cap C| = 2$. En consecuencia, $|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| = 5 + 5 + 8 - 3 - 3 - 4 + 2$, o sea, 10, y el teorema 3 está verificado. ◆

Ejemplo 9. Una compañía de computadoras tiene que contratar 25 programadores para manejar trabajos de programación de sistemas y 40 programadores para programas de aplicación. De los que se contrate, se espera que diez realicen trabajos de ambos tipos. ¿Cuántos programadores deberán contratarse?

Solución: Sean A el conjunto de programadores de sistemas contratados y B, el conjunto de programadores de aplicaciones que se contrate. La compañía debe tener $|A| = 25$ y $|B| = 40$, y $|A \cap B| = 10$. El número de programadores que debe contratarse es $|A \cup B|$, pero $|A \cup B| = |A| + |B| - |A \cup B|$. Así pues, la compañía debe contratar $25 + 40 - 10$, o sea, 55 programadores. ◆

Ejemplo 10. Se ha emprendido un estudio sobre los métodos de viaje con trasbordo. A cada participante en la encuesta se le pidió que marcara AUTOBÚS, TREN o AUTOMÓVIL según fuera el medio principal de transporte empleado para ir al trabajo. Se permitió aceptar más de una respuesta. Los resultados obtenidos fueron los siguientes: AUTOBÚS, 30 personas; TREN, 35 personas; AUTOMÓVIL, 100 personas; AUTOBÚS y TREN, 15 personas; AUTOBÚS y AUTOMÓVIL, 15 personas; TREN y AUTOMÓVIL, 20 personas; y los tres medios, 5 personas. ¿Cuántas personas llenaron el cuestionario de la encuesta?

Solución: Sean B, T y A los conjuntos de personas que marcaron AUTOBÚS, TREN y AUTOMÓVIL, respectivamente. Se sabe que $|B| = 30$, $|T| = 35$, $|A| = 100$, $|B \cap T| = 15$, $|B \cap A| = 15$, $|T \cap A| = 20$, y $|B \cap T \cap A| = 5$. Por tanto, $|B| + |T| + |A| - |B \cap T| - |B \cap A| - |T \cap A| + |B \cap T \cap A| = 30 + 35 + 100 - 15 - 15 - 20 + 5$, o sea, 120, es $|A \cup B \cup C|$, el número de personas que respondieron. ◆

GRUPO DE EJERCICIOS 1.2

En los ejercicios 1 *al* 4, *sea* $U = \{a, b, c, d, e, f, g, h, k\}$, $A = \{a, b, c, g\}$, $B = \{d, e, f, g\}$, $C = \{a, c, f\}$, *y* $D = \{f, h, k\}$.

1. Calcule
(a) $A \cup B$ (b) $B \cup C$ (c) $A \cap C$
(d) $B \cap D$ (e) $A - B$ (f) $\overline{A}$
(g) $A \oplus B$ (h) $A \oplus C$

2. Calcule
(a) $A \cup D$ (b) $B \cup D$ (c) $C \cap D$
(d) $A \cap D$ (e) $B - C$ (f) $\overline{B}$
(g) $C - B$ (h) $C \oplus D$

3. Calcule
(a) $A \cup B \cup C$ (b) $A \cap B \cap C$
(c) $A \cap (B \cup C)$ (d) $(A \cup B) \cap C$
(e) $\overline{A \cup B}$ (f) $\overline{A \cap B}$

4. Calcule
(a) $A \cup \varnothing$ (b) $A \cup U$ (c) $B \cup B$
(d) $C \cap \{\,\}$ (e) $\overline{C \cup D}$ (f) $\overline{C \cap D}$

En los ejercicios 5 *y* 6, *sean* $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $A = \{1, 2, 4, 6, 8\}$, $B = \{2, 4, 5, 9\}$, $C = \{x \mid x$ *es un entero positivo y* $x^2 \leq 16\}$, *y* $D = \{7, 8\}$.

5. Calcule
(a) $A \cup B$ (b) $A \cup C$ (c) $A \cup D$
(d) $B \cup C$ (e) $A \cap C$ (f) $A \cap D$
(g) $B \cap C$ (h) $C \cap D$ (i) $A - B$
(j) $B - A$ (k) $C - D$ (l) $\overline{C}$
(m) $\overline{A}$ (n) $A \oplus B$ (o) $C \oplus D$
(p) $B \oplus C$

6. Calcule
(a) $A \cup B \cup C$ (b) $A \cap B \cap C$
(c) $A \cap (B \cup C)$ (d) $(A \cup B) \cap D$
(e) $\overline{A \cup B}$ (f) $\overline{A \cap B}$
(g) $B \cup C \cup D$ (h) $B \cap C \cap D$
(i) $A \cup \overline{A}$ (j) $A \cap \overline{A}$
(k) $A \cup \overline{A}$ (l) $A \cap (\overline{C} \cup D)$

En los ejercicios 7 *y* 8, *sean* $U = \{a, b, c, d, e, f, g, h\}$, $A = \{a, c, f, g\}$, $B = \{a, e\}$, $B = \{a, e\}$, *y* $C = \{b, h\}$.

7. Calcule
(a) $\overline{A}$ (b) $\overline{B}$ (c) $\overline{A \cup B}$
(d) $\overline{A \cap B}$ (e) $\overline{U}$ (f) $A - B$

8. Calcule
(a) $\overline{A} \cap \overline{B}$ (b) $\overline{B} \cup \overline{C}$ (c) $\overline{A \cup A}$
(d) $\overline{C} \cap \overline{C}$ (e) $A \oplus B$ (f) $B \oplus C$

9. Sea U el conjunto de los números reales, $A = \{x \mid x$ es una solución de $x^2 - 1 = 0\}$, y $B = \{-1, 4\}$. Calcule
(a) $\overline{A}$ (b) $\overline{B}$ (c) $\overline{A \cup B}$
(d) $\overline{A \cap B}$

Para los ejercicios 10 *y* 11, *consúltese la figura* 1.13.

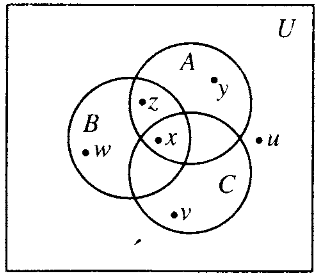


Figura 1.13

10. Identifique los siguientes casos como verdaderos o falsos.
(a) $y \in A \cap B$ (b) $x \in B \cup C$
(c) $w \in B \cap C$ (d) $u \notin C$

11. Identifique los siguientes casos como verdaderos o falsos.
(a) $x \in A \cap B \cap C$ (b) $y \in A \cup B \cup C$
(c) $z \in A \cap C$ (d) $v \in B \cap C$

12. Describa la región sombreada que aparece en la figura 1.14 por medio de uniones e intersecciones de los conjuntos A, B y C. (Hay varias descripciones posibles.)

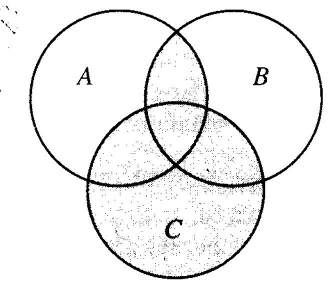


Figura 1.14

13. Sean A, B y C conjuntos finitos con $|A| = 6$, $|B| = 8$, $|C| = 6$, $|A \cup B \cup C| = 11$, $|A \cap B| = 3$, $|A \cap C| = 2$, y $|B \cap C| = 5$. Encuentre $|A \cap B \cap C|$.

14. Verifique el teorema 2 para los siguientes conjuntos.
(a) $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 5, 6, 8\}$
(b) $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7, 8, 9\}$
(c) $A = \{a, b, c, d, e, f\}$, $B = \{a, c, f, g, h, i, r\}$
(d) $A = \{a, b, c, d, e\}$, $B = \{f, g, r, s, t, u\}$
(e) $A = \{x \mid x$ es un entero positivo $< 8\}$, $B = \{x \mid x$ es un entero tal que $2 \leq x \leq 5\}$
(f) $A = \{x \mid x$ es un entero positivo y $x^2 \leq 16\}$, $B = \{x \mid x$ es un entero negativo y $x^2 \leq 25\}$

15. Si A y B son conjuntos disjuntos tales que $|A \cup B| = |A|$, ¿qué deberá ser verdadero acerca de B?

16. Verifique el teorema 3 para los siguientes conjuntos:
(a) $A = \{a, b, c, d, e\}$, $B = \{d, e, f, g, h, i, k\}$, $C = \{a, c, d, e, k, r, s, t\}$
(b) $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 7, 8, 9\}$, $C = \{1, 2, 4, 7, 10, 12\}$
(c) $A = \{x \mid x$ es un entero positivo $< 8\}$, $B = \{x \mid x$ es un entero tal que $2 \leq x \leq 4\}$, $C = \{x \mid x$ es un entero tal que $x^2 < 16\}$

17. En un estudio que se hizo con 260 estudiantes de universidad, se obtuvo los siguientes datos:
64 habían tomado un curso de matemáticas,
94 habían tomado un curso de ciencia de la computación,

58 habían tomado un curso de administración de empresas,
28 habían tomado un curso de matemáticas y uno de administración de empresas,
26 habían tomado un curso de matemáticas y un curso de ciencias de la computación,
22 habían tomado un curso de ciencias de la computación y un curso de administración de empresas, y
14 habían tomado los tres tipos de cursos.

(a) ¿Cuántos estudiantes cuyos registros fueron revisados no habían tomado ninguno de los tres tipos de cursos?
(b) De los estudiantes cuyos registros fueron estudiados, ¿cuántos habían tomado sólo un curso de ciencias de computación?

18. Una encuesta de 500 televidentes dio como resultado la siguiente información: 285 veían juegos de futbol; 195, juegos de hockey; 115, juegos de basquetbol; 45 seguían los juegos de futbol y de basquetbol; 70 preferían los juegos de futbol y hockey, 50 observaban los juegos de hockey y basquetbol, y 50 no veían ninguna de las tres clases de juegos.
(a) ¿Cuántas de las personas encuestadas observaban las tres clases de juegos?
(b) ¿Cuántas personas veían sólo uno de los deportes?

19. En un experimento de psicología, los sujetos en estudio fueron clasificados de acuerdo con el tipo de cuerpo y el género, como sigue:

	Endomorfo	Ectomorfo	Mesomorfo
Masculino	72	54	36
Femenino	62	64	38

(a) ¿Cuántos sujetos había del género masculino?
(b) ¿Cuántos sujetos eran ectomorfos?
(c) ¿Cuántos sujetos eran o del género femenino o endomorfos?
(d) ¿Cuántos sujetos no eran del género masculino y mesomorfos?
(e) ¿Cuántos sujetos eran del género masculino, o ectomorfos o mesomorfos?

20. Demuestre que $A \subseteq A \cup B$.

21. Demuestre que $A \cap B \subseteq A$.

22. (a) Dibuje un diagrama de Venn para representar la situación $C \subseteq A$ y $C \subseteq B$.
(b) Demuestre que si $C \subseteq A$ y $C \subseteq B$, entonces $C \subseteq A \cup B$.

23. (a) Dibuje un diagrama de Venn para representar la situación $A \subseteq C$ y $B \subseteq C$.
(b) Demuestre que si $A \subseteq C$ y $B \subseteq C$, entonces $A \cup B \subseteq C$.

24. Demuestre que $A - A = \varnothing$.

25. Demuestre que $A - B = A \cap \overline{B}$.

26. Demuestre que $A - (A - B) \subseteq B$.

27. Si $A \cup B = A \cup C$, ¿debe ser $B = C$? Explique.

28. Si $A \cap B = A \cap C$, ¿debe ser $B = C$? Explique.

29. Demuestre que si $A \subseteq B$ y $C \subseteq D$, entonces $A \cup C \subseteq B \cup D$ y $A \cap C \subseteq B \cap D$.

30. ¿Cuándo es $A - B = B - A$? Explique.

1.3. Sucesiones

Algunos de los conjuntos más importantes se originan en relación con las sucesiones. Una **sucesión** es simplemente una lista de objetos dispuestos en orden: un primer elemento, segundo elemento, tercer elemento, y así sucesivamente. La lista puede finalizar después de n pasos, $n \in N$, o puede continuar indefinidamente. En el primer caso, se dice que la sucesión es **finita**, y en el segundo caso, que la sucesión es **infinita**. Los elementos pueden ser todos diferentes, o puede haber algunos repetidos.

Ejemplo 1. La sucesión 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1 es una sucesión finita con elementos repetidos. El dígito cero, por ejemplo, aparece como elemento segundo, tercero, quinto, séptimo y octavo de la sucesión. ◆

Ejemplo 2. La lista 3, 8, 13, 18, 23, . . . es una sucesión infinita. Los tres puntos que tiene la expresión significan "y así sucesivamente", es decir, que continúa el patrón establecido por estos primeros elementos. ◆

Ejemplo 3. Otra sucesión infinita es 1, 4, 9, 16, 25, . . . , la lista de los cuadrados de todos los enteros positivos. ◆

Puede ocurrir que la forma en que continúe una sucesión no quede muy clara por los primeros términos, si éstos son pocos. También, puede ser útil contar con una notación compacta para describir una sucesión. Hay dos clases de fórmulas que se emplea comúnmente para describir sucesiones. En el ejemplo 2, una descripción natural de la sucesión es que los términos sucesivos se forman agregando 5 al término anterior. Si se emplea un subíndice para indicar la posición de un término en la sucesión, puede describirse la sucesión del ejemplo 2 como $a_1 = 3$, $a_n = a_{n-1} + 5$, $2 \leq n < \infty$. A una fórmula como ésta, que se refiere al término anterior para definir el siguiente término, se la llama **recursiva** o **recurrente**. Toda fórmula recursiva debe tener un punto de partida.

Por otra parte, en el ejemplo 3 es fácil describir un término usando sólo su número de posición. En la posición de orden n es el cuadrado de n; $b_n = n^2$, $1 \leq n < \infty$. A las fórmulas de este tipo se las llama **explícitas**, porque indican exactamente qué valor tiene cualquier término en particular.

Ejemplo 4. La fórmula recursiva $c_1 = 5$, $c_n = 2c_{n-1}$, $2 \leq n \leq 6$, define la sucesión finita 5, 10, 20, 40, 80, 160. ◆

Ejemplo 5. La sucesión infinita 3, 7, 11, 15, 19, 23, . . . puede definirse por la fórmula recursiva $d_1 = 3$, $d_n = d_{n-1} + 4$. ◆

Ejemplo 6. La fórmula explícita $s_n = (-4)^n$, $1 \leq n < \infty$, describe la sucesión infinita -4, 16, -64, 256, ... ◆

Ejemplo 7. La sucesión finita 87, 82, 77, 72, 67 puede definirse por la fórmula explícita, $t_n = 92 - 5n$, $1 \leq n \leq 5$.

Ejemplo 8. Una palabra inglesa ordinaria como "sturdy" puede considerarse como la sucesión finita

s, t, u, r, d, y

formada por letras del alfabeto inglés ordinario. ◆

En ejemplos como el número 8, es común omitir las comas y escribir la palabra en la forma acostumbrada, si no se presta esto a confusión. De modo similar, hasta una palabra sin significado como "abacabcd" puede considerarse como una sucesión finita de longitud 8. Las sucesiones de letras u otros símbolos, escritas sin las comas, son también llamadas **cadenas**.

Ejemplo 9. Una cadena infinita como *abababab*. . . puede considerarse como la sucesión infinita $a, b, a, b, a, b, \ldots$ ◆

Ejemplo 10. La oración "ahora es la hora de la prueba" puede considerarse como una sucesión finita de palabras españolas: ahora, es, la, hora, de, la, prueba. En este caso, los elementos de la sucesión son también palabras de longitud variable, por lo que no se podría simplemente omitir las comas. Se acostumbra usar espacios en vez de comas en este caso. ◆

El **conjunto correspondiente a una sucesión** es simplemente el conjunto de todos los elementos distintos de la sucesión. Debe observarse que una característica esencial de una sucesión es el orden que ocupan en la lista los elementos. Sin embargo, el orden en que se enliste los elementos de un conjunto carece en absoluto de significado.

Ejemplo 11
(a) El conjunto correspondiente a la sucesión del ejemplo 3 es $\{1, 4, 9, 16, 25, \ldots\}$.
(b) El conjunto correspondiente a la sucesión del ejemplo 9 es simplemente $\{a, b\}$. ◆

El concepto de sucesión es importante en la ciencia de la computación, en donde a una sucesión se la llama en ocasiones **arreglo lineal** o **lista**. Se hará una distinción simple pero útil entre una sucesión y un arreglo y se usará una notación ligeramente diferente. Si se tiene una sucesión S: $s_1, s_2, s_3, \ldots$, se piensa en todos los elementos de S como completamente determinados. El elemento s_4, por ejemplo, es algún elemento fijo de S, localizado en la posición cuatro. Por otra parte, si se cambia cualquiera de los elementos s_i, se tiene una nueva sucesión y probablemente se la llamará de alguna manera diferente de S. Así, si se comienza con la sucesión finita S: 0, 1, 2, 3, 2, 1, 1 y se cambia el 3 por un 4, para obtener 0, 1, 2, 4, 2, 1, 1, se pensaría en ésta como en una sucesión diferente, por ejemplo S'.

Un arreglo, en cambio, puede considerarse como una sucesión de posiciones, como la que se presenta en la figura 1.15 formada por casillas o cajas. Las posiciones forman una lista finita o infinita, dependiendo del tamaño deseado del arreglo. Los elementos de algún conjunto pueden ser asignados a las posiciones del arreglo S. El elemento asignado a la posición n será denotado por $S[n]$, y a la sucesión $S[1], S[2] S[3], \ldots$ se la llamará **sucesión de valores** del arreglo S. El punto por observar es que S se considera como un objeto bien definido, aun cuando a algunas de las posiciones no se les haya asignado valores o si se cambia algunos valores durante la discusión. En lo que sigue se muestra un uso de los arreglos.

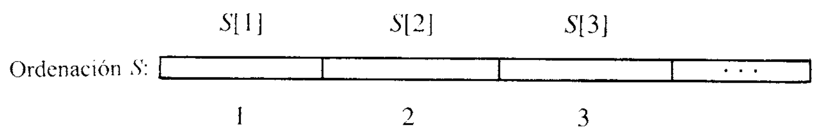


Figura 1.15

Funciones características

Un concepto muy útil para los conjuntos es la función característica. Las funciones serán estudiadas en la sección 5.1, pero por ahora se podrá avanzar por intuición y contemplar una función en un conjunto como una regla que asigna cierto "valor" a cada elemento del conjunto. Si A es un subconjunto de un conjunto universal U, la **función característica** f_A de A se define como sigue:

$$f_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A. \end{cases}$$

Se puede sumar y multiplicar las funciones características, en vista de que sus valores son números, y estas operaciones ayudan en ocasiones a demostrar teoremas relativos a propiedades de los subconjuntos.

Teorema 1. *Las funciones características de los subconjuntos satisfacen las propiedades siguientes:*
(a) $f_{A \cap B} = f_A f_B$; *es decir,* $f_{A \cap B}(x) = f_A(x) f_B(x)$ *para todos los valores de* x.
(b) $f_{A \cup B} = f_A + f_B - f_A f_B$; *es decir,* $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) f_B(x)$ *para todos los valores de* x.
(c) $f_{A \oplus B} = f_A + f_B - 2f_A f_B$; *es decir,* $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x) f_B(x)$ *para todos los valores de* x.

Demostración: (a) $f_A(x) f_B(x)$ es igual a 1 si y solamente si ambas $f_A(x)$ y $f_B(x)$ son iguales a 1, y esto ocurre si y solamente si x está en A y x está en B, es decir, si x está en $A \cap B$. Como $f_A f_B$ es 1 en $A \cap B$ y 0 en otro caso, debe ser $f_{A \cap B}$.

(b) Si $x \in A$, entonces $f_A(x) = 1$, por tanto $f_A(x) + f_B(x) - f_A(x) f_B(x) = 1 + f_B(x) - f_B(x) = 1$. De modo semejante, cuando $x \in B$, $f_A(x) + f_B(x) - f_A(x) f_B(x) = 1$. Si x no está en A ni en B, entonces $f_A(x)$ y $f_B(x)$ son 0, por lo que $f_A(x) + f_B(x) - f_A(x) f_B(x) = 0$. En consecuencia, $f_A + f_B - f_A f_B$ es 1 en $A \cup B$ y 0 de lo contrario, por lo cual debe ser $f_{A \cup B}$.

(c) Se deja la demostración de (c) como ejercicio. ●

Representación en computadora de conjuntos y subconjuntos

Las funciones características tienen otro uso más en la representación de conjuntos en una computadora. Para representar un conjunto en una computadora, debe disponerse los elementos del conjunto en una sucesión. La sucesión particular seleccionada no tiene importancia alguna. Cuando se hace la lista del conjunto $A = \{a, b, c, \ldots, r\}$, normalmente no se supone orden alguno en particular de los elementos que hay en A. Se identificará por ahora el conjunto A con la sucesión $a, b, c, \ldots, r$.

Cuando un conjunto universal U es finito, como por ejemplo, $U = \{x_1, x_2, \ldots, x_n\}$ y A es un subconjunto de U, entonces la función característica f_A asigna 1 a un elemento x_i que pertenece a A y 0 a un elemento x_i que no pertenece a A. Así f_A puede ser representada por una sucesión de ceros y unos de longitud n.

Ejemplo 12. Sea $U = \{1, 2, 3, 4, 5, 6\}$, $A = \{1, 2\}$, $B = \{2, 4, 6\}$, y $C = \{4, 5, 6\}$. Entonces $f_A(x)$ tiene valor 1 cuando x es 1 o 2 y cualquier otro valor si tiene valor 0. Por tanto, f_A corresponde a la sucesión 1, 1, 0, 0, 0, 0. De modo semejante, la sucesión finita 0, 1, 0, 1, 0, 1 representa a f_B y 0, 0, 0, 1, 1, 1 representa a f_C. ◆

Cualquier conjunto con n elementos puede ordenarse en una sucesión de longitud n, de manera que cada uno de sus subconjuntos corresponda a una sucesión de ceros y unos de longitud n, para representar la función característica de ese subconjunto. Este hecho permite representar un conjunto universal en una computadora como un arreglo A de longitud n. La asignación de un cero o un uno a cada posición $A[k]$ del arreglo especifica un subconjunto único de U.

Ejemplo 13. Sea $U = \{a, b, e, g, h, r, s, w\}$. La ordenación de longitud 8 que aparece en la figura 1.16 representa a U, ya que $A[k] = 1$ para $1 \leq k \leq 8$.

Si $S = \{a, e, r, w\}$, entonces

$$f_S(x) = \begin{cases} 1 & \text{si } x\ 1,\ 3,\ 6,\ 8 \\ 0 & \text{si } x\ 2,\ 4,\ 5,\ 7. \end{cases}$$

1	1	1	1	1	1	1	1

Figura 1.16

Por tanto, el arreglo de la figura 1.17 representa el subconjunto S. ◆

1	0	1	0	0	1	0	1

Figura 1.17

Un conjunto se denomina **numerable** si es el conjunto correspondiente a alguna sucesión. Informalmente esto significa que los miembros del conjunto pueden ser dispuestos en una lista, con un primero, segundo, tercero, . . . , elemento, y el conjunto puede, por tanto, numerarse o contarse. Se demostrará en la sección 2.4 que todos los conjuntos finitos son numerables. Sin embargo, no todos los conjuntos infinitos lo son. Al conjunto que no es numerable se lo llama **no numerable**.

El ejemplo más accesible de un conjunto no numerable es el conjunto de todos los números reales que pueden representarse por una decimal infinita de la forma $0.a_1a_2a_3. . .$, en donde a_i es un entero y $0 \leq a_i \leq 9$. Ahora se demostrará que este conjunto es no numerable. Se demostrará este resultado por contradicción; es decir, se demostrará que la numerabilidad de este conjunto implica una situación imposible. (Se verá con más detenimiento la demostración por contradicción en el capítulo 2.)

Supóngase que el conjunto de todos los decimales $0.a_1a_2a_3 \cdots$ es numerable. Entonces se podría formar la siguiente lista (sucesión) que contuviera todos estos decimales:

$$\begin{aligned} d_1 &= 0.a_1a_2a_3 \cdots \\ d_2 &= 0.b_1b_2b_3 \cdots \\ d_3 &= 0.c_1c_2c_3 \cdots \\ &\vdots \end{aligned}$$

Cada uno de nuestros decimales infinitos debe aparecer en algún lugar de esta lista. Se establecerá una contradicción construyendo un decimal infinito de este tipo que no esté en la lista. Construya ahora un número x como sigue: $x = 0.x_1x_2x_3 \cdots$, en donde x_1 es 1 si $a_1 =$ 2, de lo contrario x_1 es 2; $x_2 = 1$ si $b_2 = 2$, de lo contrario $x_2 = 2$; $x_3 = 1$ si $c_3 = 2$, de lo contrario $x_3 = 2$. Resulta claro que este proceso puede continuarse indefinidamente. El número resultante x es un decimal infinito que consta de unos y doses pero, por su construcción x difiere de cada número de la lista en alguna posición. En consecuencia, x no está en la lista, lo cual resulta ser una contradicción de acuerdo con la suposición formulada. Por tanto, independientemente de la forma en que se construya la lista, hay algún número real de la forma $0.x_1x_2x_3 \cdots$ que no está en la lista. Y de la misma forma, puede demostrarse que el conjunto de los números racionales es numerable.

Cadenas y expresiones regulares

Dado un conjunto A, se puede construir el conjunto A^* formado por todas las sucesiones finitas de los elementos de A. Con frecuencia, el conjunto A no es un conjunto de números, sino algún conjunto de símbolos. En este caso, a A se la llama **alfabeto**, y a las sucesiones finitas que forman A^* se las llama **palabras** procedentes de A, o en ocasiones **cadenas** de A. Para este caso en particular, al escribir las sucesiones que hay en A^* *no se usan* comas. Se supone que A^* contiene a la **sucesión vacía** o **cadena vacía**, que no contiene símbolos, y se designa a esta cadena por Λ. Esta cadena será útil en los capítulos 7 y 8.

Ejemplo 14. Sea $A = \{a, b, c, \ldots, z\}$, el alfabeto inglés usual. Entonces A^* está formado por todas las palabras ordinarias, tales como *ape, sequence, antidisestablishmentarianism*, y así sucesivamente, también por "palabras" tales como yxaloble, zigadongdong, cya, y pqrst. Todas las sucesiones finitas procedentes de A están en A^*, sea que tengan o no significado. ◆

Si $w_1 = s_1s_2s_3 \cdots s_n$ y $w_2 = t_1t_2t_3 \cdots t_k$ son elementos de A^* para algún conjunto A, se define la **concatenación** de w_1 y w_2 como la sucesión $s_1s_2s_3 \cdots s_nt_1t_2t_3 \cdots t_k$. La concatenación de w_1 con w_2 se escribe como $w_1 \cdot w_2$ y es otro elemento de A^*. Nótese que si w pertenece a A^*, entonces $w \cdot \Lambda = w$, y $\Lambda \cdot w = w$. Esta propiedad es conveniente y es una de las principales razones para definir la cadena vacía Λ.

Ejemplo 15. Sea $A =$ {John, Sam, Jane, swims, runs, well, quickly, slowly}. Entonces A^* contiene oraciones reales como "Jane swims quickly" y "Sam runs well", a la vez que oraciones sin sentido tales como "Well swims Jane slowly John." Aquí se separa los elementos de cada sucesión con espacios. ◆

La idea de una fórmula recursiva para una oración es útil también en escenarios más generales. En los lenguajes formales y las máquinas de estado finito que son analizadas en el capítulo 9, el concepto de expresiones regulares desempeña un papel importante, y las expresiones regulares son definidas de manera recursiva. Una **expresión regular sobre A** es una cadena construida a partir de los elementos de A y los símbolos (,),$\vee$, *, Λ, de acuerdo con la siguiente definición.

RE1. El símbolo Λ es una expresión regular.
RE2. Si $x \in A$, el símbolo x es una expresión regular.
RE3. Si α y β son expresiones regulares, entonces la expresión $\alpha\beta$ es regular.
RE4. Si α y β son expresiones regulares, entonces la expresión $(\alpha \vee \beta)$ es regular.
RE5. Si α es una expresión regular, entonces la expresión $(\alpha)^*$ es regular.

Debe notarse aquí que RE1 y RE2 proporcionan expresiones regulares iniciales. Las otras partes de la definición son usadas repetitivamente para definir en forma sucesiva conjuntos más grandes de expresiones regulares a partir de los ya definidos. En consecuencia, la definición es recursiva.

Convencionalmente, si la expresión regular α consta de un solo símbolo x, en donde $x \in A$, o si α comienza y termina con paréntesis, entonces se escribe $(\alpha)^*$ simplemente como α^*. Cuando no resulte confuso, se hará referencia a una expresión regular sobre A simplemente como una **expresión regular** (omitiendo la referencia a A).

Ejemplo 16. Sea $A = \{0, 1\}$. Demuestre que las siguientes expresiones son todas expresiones regulares sobre A.

(a) $0^*(0 \vee 1)^*$ (b) $00^*(0 \vee 1)^*1$ (c) $(01)^*(01 \vee 1^*)$

Solución: (a) Por RE2, 0 y 1 son expresiones regulares. En consecuencia $(0 \vee 1)$ es regular por RE4, y por tanto 0^* y $(0 \vee 1)^*$ son regulares por RE5 (y la convención mencionada anteriormente). Por último, se ve que $0^*(0 \vee 1)^*$ es regular por RE3.

(b) Se sabe que 0, 1, y $0^*(0 \vee 1)^*$ son todas regulares. En consecuencia, usando RE3 dos veces, $00^*(0 \vee 1)^*1$ debe ser regular.

(c) Por RE3, 01 es una expresión regular. Como 1^* es regular, $(01 \vee 1^*)$ es regular por RE4, y $(01)^*$ es regular por RE5. Entonces la regularidad de $(01)^*(01 \vee 1^*)$ se desprende de RE3. ◆

Asociado con cada expresión regular sobre A hay un subconjunto correspondiente de A^*. A tales conjuntos se los llama **subconjuntos regulares** de A^* o solamente **conjuntos regulares** si no se necesita referencia alguna a A. Para calcular el conjunto regular correspondiente a una expresión regular, se utilizan las siguientes reglas de correspondencia.

1. La expresión Λ corresponde al conjunto $\{\Lambda\}$, en donde Λ es la cadena vacía en A^*.
2. Si $x \in A$, entonces la expresión regular x corresponde al conjunto $\{x\}$.
3. Si α y β son expresiones regulares correspondientes a los subconjuntos M y N de A^*, entonces $\alpha\beta$ corresponde a $M \cdot N = \{s \cdot t \mid s \in M \text{ y } t \in N\}$. En consecuencia, $M \cdot N$ es el conjunto de todas las concatenaciones de cadenas que hay en M con cadenas de N.
4. Si las expresiones regulares α y β corresponden a los subconjuntos M y N de A^*, entonces $\alpha \vee \beta$ corresponde a $M \cup N$.
5. Si la expresión regular α corresponde al subconjunto M de A^*, entonces $(\alpha)^*$ corresponde al conjunto M^*. Nótese que M es un conjunto de cadenas procedentes de A. Los elementos de M^* son sucesiones finitas de tales cadenas y en consecuencia pueden ser interpretadas ellas mismas como cadenas de A. Nótese también que siempre se tiene $\Lambda \in M^*$.

Ejemplo 17. Sea $A = \{a, b, c\}$. Entonces la expresión regular a^* corresponde al conjunto de todas las sucesiones finitas de a's, tales como *aaa, aaaaaaa,* y así sucesivamente. La expresión regular $a(b \vee c)$ corresponde al conjunto $\{ab, ac\} \subseteq A^*$. Finalmente, la expresión regular $ab(bc)^*$ corresponde al conjunto de todas las cadenas que comienzan con ab y luego repiten los símbolos bc n veces, en donde $n \geq 0$. Este conjunto incluye las cadenas *ab, abbcbc, abbcbcbcbc,* y así sucesivamente. ◆

Ejemplo 18. Sea $A = \{0, 1\}$. Encuentre los conjuntos regulares correspondientes a las tres expresiones regulares del ejemplo 16.

Solución: (a) El conjunto correspondiente a $0^*(0 \vee 1)^*$ consta de todas las sucesiones de ceros y unos. En consecuencia, el conjunto es A^*.

(b) La expresión $00^*(0 \vee 1)^*1$ corresponde al conjunto de todas las sucesiones de ceros y unos que comienzan con por lo menos un 0 y terminan con por lo menos un 1.

(c) La expresión $(01)^*(01 \vee 1^*)$ corresponde al conjunto de todas las sucesiones de ceros y unos que, o repiten la cadena 01 un total de $n \geq 1$ veces, o comienzan con un total de $n \geq 0$ repeticiones de 01 y terminan con algún número $k \geq 0$ de unos. Este conjunto incluye, por ejemplo, las cadenas 1111, 01, 010101, 0101010111111, y 011. ◆

GRUPO DE EJERCICIOS 1.3

En los ejercicios 1 al 4, dé el conjunto correspondiente a la sucesión.

1. 2, 1, 2, 1, 2, 1, 2, 1

2. 0, 2, 4, 6, 8, 10, . . .

3. $aabbccddee \cdots zz$

4. *abbcccdddd*

5. Dé tres sucesiones diferentes que tengan $\{x, y, z\}$ como un conjunto correspondiente.

6. Dé tres sucesiones diferentes que tengan $\{1, 2, 3, \ldots\}$ como un conjunto correspondiente.

En los ejercicios 7 al 10, escriba los cuatro primeros términos (comience con $n = 1$) de la sucesión cuyo término general se da.

7. $a_n = 5^n$

8. $b_n = 3n^2 + 2n - 6$

9. $c_1 = 2.5, c_n = c_{n-1} + 1.5$

10. $d_1 = -3, d_n = -2d_{n-1} + 1$

En los ejercicios 11 al 16, escriba una fórmula para el término de orden n de la sucesión. Identifique su fórmula como recursiva o explícita.

11. 1, 3, 5, 7, . . .

12. 0, 3, 8, 15, 24, 35, . . .

13. [illegible]

14. 0, 2, 0, 2, 0, 2

15. 1, 4, 7, 10, 13, 16

16. $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \ldots$

17. Escriba una fórmula explícita para la sucesión 2, 5, 8, 11, 14, 17, ...

3n−1

18. Escriba una fórmula recursiva para la sucesión 2, 5, 7, 12, 19, 31, ...

19. Sea $A = \{x \mid x \text{ es un número real y } 0 < x < 1\}$, $B = \{x \mid x \text{ es un número real y } x^2 + 1 = 0\}$, $C = \{x \mid x = 4m, m \in Z\}$, $D = \{(x, 3) \mid x \text{ es una palabra inglesa cuya longitud es } 3\}$, y $E = \{x \mid x \in Z \text{ y } x^2 \leq 100\}$. Identifique cada conjunto como finito, numerable o no numerable.

20. Sea $A = \{ab, bc, ba\}$. En cada parte, diga si la cadena pertenece a A^*.
(a) *ababab* (b) *abc* (c) *abba*
(d) *abbcbaba* (e) *bcabbab* (f) *abbbcba*

21. Sean U = {FORTRAN, PASCAL, ADA, COBOL, LISP, BASIC, C++, FORTH}, B = {C++, BASIC, ADA}, C = {PASCAL, ADA, LISP, C++}, D = {FORTRAN, PASCAL, ADA, BASIC, FORTH}, y E = {PASCAL, ADA, COBOL, LISP, C++}. En cada uno de los siguientes casos, represente el conjunto dado por un arreglo de ceros y unos.
(a) $B \cup C$ (b) $C \cap D$ (c) $B \cap (D \cap E)$
(d) $\overline{B} \cup E$ (e) $\overline{C} \cap (B \cup E)$

22. Sea $U = \{b, d, e, g, h, k, m, n\}$, $B = \{b\}$, $C = \{d, g, m, n\}$, y $D = \{d, k, n\}$
(a) ¿Qué es $f_B(b)$?
(b) ¿Qué es $f_C(e)$?
(c) Encuentre las sucesiones de longitud 8 que corresponden a f_B, f_C y f_D.
(d) Represente $B \cup C$, $C \cup D$, y $C \cap D$ por arreglos de ceros y unos.

23. Demuestre el teorema 1(c).

24. Usando funciones características, demuestre que $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

25. Sea $A = \{+, \times, a, b\}$. Demuestre que las siguientes expresiones son regulares sobre A.
(a) $a + b(ab)^*(a \times b \vee a)$
(b) [illegible]
(c) $((a^*b \vee +)^* \vee \times ab^*)$

26. Sea $A = \{a, b, c\}$. En cada parte se enlista una cadena en A^* y una expresión regular sobre A. En

cada caso, diga si la cadena de la izquierda pertenece o no al conjunto regular correspondiente a la expresión regular de la derecha.
(a) *ac* a^*b^*c
(b) *abcc* $(abc \vee c)^*$
(c) *aaabc* $((a \vee b) \vee c)^*$
(d) *ac* $(a^*b \vee c)$
(e) *abab* $(ab)^*c$

27. Se define números T en forma recursiva como sigue:
1. 0 es un número T.
2. Si X es un número T, $X + 3$ es un número T.
Describa el conjunto de los números T.

28. Defina un número S por:
1. 8 es un número S.
2. Si X es un número S y Y es un múltiplo de X, entonces Y es un número S.
3. Si X es un número S y X es un múltiplo de Y, Y es un número S.
Describa el conjunto de los números S.

29. Sea F una función definida por todos los enteros no negativos por medio de la siguiente definición recursiva:

$$F(0) = 0, \qquad F(1) = 1,$$
$$F(N + 2) = 2F(N) + F(N + 1), \quad N \geq 0$$

Escriba los primeros seis valores de F; es decir, escriba los valores de $F(N)$ para $N = 0, 1, 2, 3, 4, 5$.

30. Sea G una función definida para todos los enteros no negativos por la siguiente definición recursiva:

$$G(0) = 1, \qquad G(1) = 2,$$
$$G(N + 2) = G(N)^2 + G(N + 1), \quad N \geq 0$$

Escriba los primeros cinco valores de G.

1.4. División en los enteros

Ahora se analizará algunos resultados que se necesitarán más adelante, acerca de la división y factorización en los enteros no negativos. Si m y n son enteros no negativos y n no es cero, puede escribirse en una gráfica los múltiplos enteros no negativos de n, en la mitad del renglón, y localizarse m como en la figura 1.18. Si m es múltiplo de n, por decir, $m = qn$, entonces se puede escribir $m = qn + r$, en donde r es 0. Por otra parte (como se ilustra en la figura 1.18), si m no es múltiplo de n, sea qn el primer múltiplo de n situado a la izquierda de m y sea r igual a $m - qn$. Entonces r es la distancia de qn a m, por lo que claramente $0 < r < n$, y una vez más se tiene $m = qn + r$. Se enuncia estas observaciones como teorema.

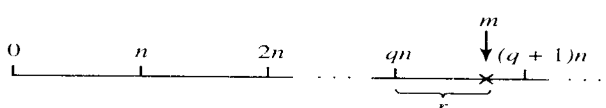


Figura 1.18

Teorema 1. *Si $n \neq 0$ y m son enteros no negativos, puede escribirse $m = qn + r$ para algunos enteros no negativos q y r con $0 \leq r < n$. Además, sólo hay una manera de hacer esto.* ●

Ejemplo 1
(a) Si n es 3 y m es 16, entonces $16 = 5(3) + 1$, por tanto q es 5 y r es 1.
(b) Si n es 10 y m es 3, entonces $3 = 0(10) + 3$, por tanto q es 0 y r es 3. ♦

Si la r del teorema 1 es cero, de manera que m sea un múltiplo de n, se escribe $n \mid m$, lo cual se lee "n divide a m". Si m no es múltiplo de n, se escribe $n \nmid m$, lo cual se lee "n no divide a m". Se demuestra ahora algunas propiedades simples de divisibilidad.

Teorema 2. *Sean a, b y c números enteros.*
(a) *Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.*
(b) *Si $a \mid b$ y $a \mid c$, en donde $b > c$, entonces $a \mid (b - c)$.*
(c) *Si $a \mid b$ o $a \mid c$, entonces $a \mid bc$.*
(d) *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*

Demostración: (a) Si $a \mid b$ y $a \mid c$, entonces $b = k_1a$ y $c = k_2a$ para algunos enteros no negativos k_1 y k_2. Por tanto $b + c = (k_1 + k_2)a$ y $a \mid (b + c)$.
(b) Ésta puede demostrarse exactamente en la misma forma que la parte (a).
(c) Como en la parte (a), se tiene $b = k_1a$ o $c = k_2a$. Entonces o $bc = k_1ac$ o $bc = k_2ab$, de manera que en cualquiera de los dos casos bc es un múltiplo de a y $a \mid bc$.
(d) Si $a \mid b$ y $b \mid c$, se tiene $b = k_1a$ y $c = k_2b$, por tanto $c = k_2b = k_2(k_1a) = (k_2k_1)a$ y por tanto $a \mid c$. ●

Un número $p > 1$ en Z^+ se llama **primo** si los únicos enteros positivos que dividen a p son p y 1.

Ejemplo 2. Los números 2, 3, 5, 7, 11 y 13 son primos, mientras que 4, 10, 16 y 21 son no primos. ♦

Es fácil escribir un grupo de pasos, o un **algoritmo**[1], para determinar si un entero positivo $n > 1$ es un número primo. Primero, se verifica si n es 2. Si $n > 2$, se podría dividir n entre todo entero comprendido entre 2 y $n - 1$, y si ninguno de éstos es un divisor de n, entonces n es primo. Para hacer más eficiente el proceso, se observa que si $mk = n$, entonces o m o k es menor que o igual a $\sqrt{n}$. Esto significa que si n no es primo, tiene un divisor k que satisface la desigualdad $1 < k \leq \sqrt{n}$, de manera que sólo se necesita probar por divisores comprendidos en este intervalo. También, si n tiene cualquier número par como divisor, debe tener a 2 como divisor. En consecuencia, después de verificar la divisibilidad entre 2, se puede saltar todos los enteros pares.

Algoritmo para probar si un entero $N > 1$ es primo:

Paso 1. Verifique si N es 2. Si lo es, N es primo. Si no lo es, prosiga con el
Paso 2. Verifique si $2 \mid N$. Si esto es afirmativo, N no es primo; de lo contrario, prosiga al
Paso 3. Calcule el entero más pequeño $K \leq \sqrt{N}$. Luego
Paso 4. Verifique si $D \mid N$, en donde D es cualquier número impar tal que $1 < D \leq K$. Si $D \mid N$, entonces N no es primo; de lo contrario, N es primo.

La prueba para saber si un entero es primo es una tarea común para computadoras. El algoritmo que se acaba de ver es demasiado ineficiente para números muy grandes, pero hay muchos otros algoritmos para probar si un entero es o no primo.

Teorema 3. *Todo entero positivo $n > 1$ puede escribirse en forma única como $p_1^{k_1}p_2^{k_2} \cdots p_s^{k_s}$, en donde $p_1 < p_2 < \cdots < p_s$ son primos distintos que dividen a n, y las k son enteros positivos que dan el número de veces que ocurre cada primo como factor de n.* ●

Se omite la demostración del teorema 3, pero se presenta varias ilustraciones.

[1] Se explicará los algoritmos en el apéndice A.

Ejemplo 3

(a) $9 = 3 \cdot 3 = 3^2$
(b) $24 = 8 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$
(c) $30 = 2 \cdot 3 \cdot 5$ ◆

Máximo común divisor

Si a, b y k están en Z^+, y $k \mid a$, $k \mid b$, se dice que k es un **divisor común** de a y b. Si d es el mayor de estos k, a d se le llama **máximo común divisor**, o MCD, de a y b, y se escribe $d = \text{MCD}(a, b)$. Este número tiene algunas propiedades interesantes. Puede escribirse como una combinación de a y b, y no sólo es más grande que todos los demás divisores comunes, sino que es también múltiplo de cada uno de éstos.

Teorema 4. *Si d es el MCD(a, b), entonces*
(a) *$d = sa + tb$ para algunos enteros s y t (éstos no son ambos positivos).*
(b) *Si c es cualquier otro divisor común de a y b, entonces $c \mid d$.*

Demostración: Sea x el entero positivo más pequeño que puede escribirse como $sa + tb$ para algunos enteros s y t, y sea c un divisor común de a y b. Como $c \mid a$ y $c \mid b$, se sabe por el teorema 2 que $c \mid x$, de manera que $c \leq x$. Si se puede demostrar que x es un divisor común de a y b, será éste entonces el máximo común divisor de a y b, y ambas partes del teorema habrán quedado demostradas. Por el teorema 1, $a = qx + r$ con $0 \leq r < x$. Resolviendo para r, se tiene $r = a - qx = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b$. Si r no es cero, entonces como $r < x$ y r es múltiplo de a y múltiplo de b, constituirá una contradicción al hecho de que x sea el número positivo más pequeño, que es la suma de los múltiplos de a y b. En consecuencia, r debe ser 0 y $x \mid a$. De la misma manera puede demostrarse que $x \mid b$, y esto completa la demostración. ●

Supóngase ahora que a, b y d están en Z^+ y que d es un divisor común de a y b, que es múltiplo de todos los demás divisores comunes de a y b. Entonces d es el máximo común divisor de a y b. Este resultado y el teorema 4(b) tienen el resultado siguiente: Supóngase que a, b y d están en Z^+. El entero d es el máximo común divisor de a y b si y solamente si

1. $d \mid a$ y $d \mid b$.
2. Siempre que ocurra que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Ejemplo 4
(a) Los divisores comunes de 12 y 30 son 2, 3 y 6, por lo que el MCD $(12, 30) = 6$ y $6 = 1 \cdot 30 + (-2) \cdot 12$.
(b) Resulta claro que el MCD$(17, 95) = 1$ ya que 17 es primo y $17 \nmid 95$, y el lector puede verificar que $1 = 28 \cdot 17 + (-5) \cdot 95$. ◆

Si el MCD$(a, b) = 1$, como en el ejemplo 4(b), se dice que a y b son **primos relativos**.

Una interrogante que queda es la de cómo calcular en general, el MCD en forma conveniente. La aplicación repetida del teorema 1 proporciona la clave para hacer esto.

Se presenta ahora un procedimiento conocido como el **algoritmo euclidiano**, para determinar el MCD(a, b). Supóngase que $a > b > 0$ (de lo contrario, intercambie a y b). Entonces, por el teorema 1, es posible escribir

$$a = k_1 b + r_1, \quad \text{en donde } k_1 \text{ y } r_1 \text{ están en } Z^+ \text{ y } 0 \leq r_1 < b. \tag{1}$$

Ahora el teorema 2 dice que si n divide a a y b, debe dividir a r_1, ya que $r_1 = a - k_1 b$. De modo similar, si n divide a b y a r_1, debe dividir a a. Se ve que los divisores comunes de a y b son los mismos que los divisores comunes de b y r_1, de manera que MCD(a, b) = MCD(b, r_1).

Se continúa ahora usando el teorema 1, como sigue:

$$\begin{array}{lll}
\text{divida } b \text{ entre } r_1: & b = k_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\
\text{divida } r_1 \text{ entre } r_2: & r_1 = k_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\
\text{divida } r_2 \text{ entre } r_3: & r_2 = k_4 r_3 + r_4 & 0 \leq r_4 < r_3 \\
\vdots & \vdots & \vdots \\
\text{divida } r_{n-2} \text{ entre } r_{n-1}: & r_{n-2} = k_n r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
\text{divida } r_{n-1} \text{ entre } r_n: & r_{n-1} = k_{n+1} r_n + r_{n+1} & 0 \leq r_{n+1} < r_n.
\end{array} \tag{2}$$

Como $a > b > r_1 > r_2 > r_3 > r_4 > \cdots$, el residuo tendrá que llegar a ser cero, por lo que en algún punto se obtendrá $r_{n+1} = 0$.

Se demuestra ahora que r_n = MCD(a, b). Se observó previamente que

$$\text{MCD}(a, b) = \text{MCD}(b, r_1).$$

Repitiendo este argumento con b y r_1, se ve que

$$\text{MCD}(b, r_1) = \text{MCD}(r_1, r_2).$$

Al continuar, se tiene

$$\text{MCD}(a, b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) = \cdots = \text{MCD}(r_{n-1}, r_n)$$

Como $r_{n-1} = k_{n+1} r_n$ se ve que MCD$(r_{n-1}, r_n) = r_n$. Por tanto, r_n = MCD(a, b).

Ejemplo 5. Sean a 190 y b 34. Entonces, usando el algoritmo euclidiano,

se divide 190 entre 34:	$190 = 5 \cdot 34 + 20$
se divide 34 entre 20:	$34 = 1 \cdot 20 + 14$
se divide 20 entre 14:	$20 = 1 \cdot 14 + 6$
se divide 14 entre 6:	$14 = 2 \cdot 6 + 2$
se divide 6 entre 2:	$6 = 3 \cdot 2 + 0.$

de manera que el MCD$(190, 34)$ es 2, el último de los divisores. ◆

En el teorema 4(a), se observó que si d = MCD(a, b), puede encontrarse enteros s y t tales que $d = sa + tb$. Los enteros s y t pueden ser encontrados como sigue. Resuelva la penúltima ecuación en (2) para r_n:

$$r_n = r_{n-2} - k_n r_{n-1}. \tag{3}$$

Resuelva ahora la antepenúltima en (2), $r_{n-3} = k_{n-1} r_{n-2} + r_{n-1}$, para r_{n-1}:

$$r_{n-1} = r_{n-3} - k_{n-1} r_{n-2}.$$

Sustituya esta expresión en (3):

$$r_n = r_{n-2} - k_n[r_{n-3} - k_{n-1} r_{n-2}].$$

Continúe trabajando, de abajo a arriba, con las ecuaciones en (2) y (1), sustituyendo a r_i por una expresión que contenga a r_{i-1} y a r_{i-2} para llegar finalmente a una expresión que sólo contenga a a y b.

Ejemplo 6. (a) Sean $a = 190$ y $b = 34$ como en el ejemplo 5. Entonces

$$\begin{aligned}
\mathrm{MCD}(190, 34) &= 2 = 14 - 2(6) \\
&= 14 - 2[20 - 1(14)] && 6 = 20 - 1 \cdot 14 \\
&= 3(14) - 2(20) \\
&= 3[34 - 1(20)] - 2(20) && 14 = 34 - 1 \cdot 20 \\
&= 3(34) - 5(190 - 5 \cdot (34)) && 20 = 190 - 5 \cdot 34 \\
&= 28(34) - 5(190).
\end{aligned}$$

Por tanto, $s = -5$ y $t = 28$. Nótese que la clave está en efectuar las operaciones aritméticas sólo parcialmente.

(b) Sean $a = 108$ y $b = 60$. Entonces

$$\begin{aligned}
\mathrm{MCD}(108, 60) &= 12 = 60 - 1(48) \\
&= 60 - 1[108 - 1(60)] && 48 = 108 - 1 \cdot 60 \\
&= 2(60) - 108.
\end{aligned}$$

Por tanto $s = -1$ y $t = 2$. ◆

Teorema 5. *Si a y b están en* Z^+, *entonces* $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, b \pm a)$.

Demostración: Si c divide a a y b, divide también a $b \pm a$, por el teorema 2. Como $a = b - (b - a) = -b + (b + a)$, se ve, también por el teorema 2, que un divisor común de b y $b \pm a$ divide también a a y b. Como a y b tienen los mismos divisores comunes que b y $b \pm a$, deben tener el mismo máximo común divisor. ●

Mínimo común múltiplo

Si a, b y k están en Z^+, y $a \mid k$, $b \mid k$, se dice que k es un **múltiplo común** de a y b. A la k más pequeña de éstas, a la que se llamará c, se la denomina **mínimo común múltiplo** o MCM, de a y b, y se escribe $c = \mathrm{MCM}(a, b)$. El siguiente resultado muestra que se puede obtener el mínimo común múltiplo a partir del máximo común divisor, por lo cual no se necesita un procedimiento aparte para determinarlo.

Teorema 6. *Si a y b son dos enteros positivos, entonces* $\mathrm{MCD}(a, b) \cdot \mathrm{MCM}(a, b) = ab$.

Demostración: Sean $p_1, p_2, \ldots, p_k$ todos los factores primos de a o de b. Entonces se puede escribir

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{y} \quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

en donde algunos de los a_i y b_i pueden ser cero. Se desprende entonces que

$$\mathrm{MCD}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$$

y

$$\mathrm{MCM}(a, b) = p_1^{\text{máx}(a_1, b_1)} p_2^{\text{máx}(a_2, b_2)} \cdots p_k^{\text{máx}(a_k, b_k)}.$$

Por tanto

$$\begin{aligned}
\mathrm{MCD}(a, b) \cdot \mathrm{MCM}(a, b) &= p_1^{a_1 + b_1} p_2^{a_2 + b_2} \cdots p_k^{a_k + b_k} \\
&= (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) \cdot (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}) \\
&= ab.
\end{aligned}$$

●

Ejemplo 7. Sean $a = 540$ y $b = 504$. Factorizando a y b en primos, se obtiene

$$a = 540 = 2^2 \cdot 3^3 \cdot 5 \text{ y } b = 504 = 2^3 \cdot 3^2 \cdot 7.$$

En consecuencia, todos los números primos que son factores de a o de b son $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ y $p_4 = 7$. Entonces $a = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^0$ y $b = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1$. Entonces se tiene

$$\begin{aligned}
\mathrm{MCD}(540, 504) &= 2^{\min(2, 3)} \cdot 3^{\min(3, 2)} \cdot 5^{\min(1, 0)} \cdot 7^{\min(0, 1)} \\
&= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \\
&= 2^2 \cdot 3^2 \quad \text{o} \quad 36.
\end{aligned}$$

También,

$$\begin{aligned}
\mathrm{MCM}(540, 504) &= 2^{\text{máx}(2, 3)} \cdot 3^{\text{máx}(3, 2)} \cdot 5^{\text{máx}(1, 0)} \cdot 7^{\text{máx}(0, 1)} \\
&= 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^1 \quad \text{o} \quad 7560.
\end{aligned}$$

Entonces $\mathrm{MCD}(540, 504) \cdot \mathrm{MCM}(540, 504) = 36 \cdot 7560 = 272, 160 = 540 \cdot 504$. Para verificar, también puede calcularse el MCD(540, 504) por el algoritmo euclidiano y obtenerse el mismo resultado. ◆

Si $a \neq 0$ y b son enteros no negativos, el teorema 1 nos dice que se puede escribir $b = qa + r$, $0 \leq r < a$. En ocasiones el residuo r es más importante que el cociente q. Nótese que $0 \leq r < a$.

Ejemplo 8. Si ahora marca el reloj las 4, ¿qué hora será 101 horas después?

Solución: Sean $a = 12$ y $b = 4 + 101$, o sea, 105. Entonces se tiene que $105 = 8 \cdot 12 + 9$. El residuo 9 contesta la pregunta. Dentro de 101 horas serán las 9. ◆

En este caso, a a se la denomina **módulo** y se escribe $b \equiv r$ (mód a), léase "b es **congruente** con r módulo a."

Ejemplo 9

(a) $29 \equiv 4$ (mód 5), ya que $29 = 5 \cdot 5 + 4$.
(b) $172 \equiv 7$ (mód 11), ya que $172 = 15 \cdot 11 + 7$.
(c) $3 \equiv 3$ (mód 6), ya que $3 = 0 \cdot 6 + 3$. ◆

Nótese que si $b \equiv r$ (mód a), entonces $0 \leq r < a$, y $b - r$ es múltiplo de a; es decir, a divide a $b - r$.

Para cada $n \in Z^+$, se define una función f_n, la función mód-n, como sigue: Si z es un entero no negativo, entonces $f_n(z) = r$, en donde $z \equiv r$ (mód n) y $0 \leq r < n$. (Nuevamente, las funciones son definidas formalmente en la sección 5.1, pero, como en la sección 1.3, es necesario pensar en una función solamente como una regla que asigna algún "valor" a cada miembro de un conjunto.)

Ejemplo 10

(a) $f_3(14) = 2$, porque $14 = 4 \cdot 3 + 2$ y $14 \equiv 2$ mód 3.
(b) $f_7(153) = 6$ ◆

Versiones en seudocódigos

Una alternativa para expresar un algoritmo en español ordinario, como previamente se hizo en esta sección, es expresarlo en algo así como un lenguaje de computadora. En todo este libro se usa un lenguaje en **seudocódigo**, que se describe completamente en el apéndice A. Aquí se proporciona versiones en seudocódigos para un algoritmo que determina si un entero es primo y para un algoritmo que calcula el máximo común divisor de dos enteros.

En el seudocódigo para el algoritmo que se emplea para determinar si un entero es primo, se supone la existencia de las funciones SQR e INT, en donde SQR(N) regresa el máximo entero que no excede a $\sqrt{N}$, e INT(X) regresa el máximo entero que no excede a X. Por ejemplo, SQR(10) = 3, SQR(25) = 5, INT(7.124) = 7, e INT(8) = 8.

```
SUBROUTINE PRIME(N)
1. IF (N = 2) THEN
   a. PRINT ('PRIME')
   b. RETURN
2. ELSE
   a. IF (N/2 = INT(N/2)) THEN
      1. PRINT ('NOT PRIME')
      2. RETURN
   b. ELSE
      1 FOR D = 3 THRU SQR(N) BY 2
      a. IF (N/D = INT (N/D)) THEN
         1. PRINT ('NOT PRIME')
         2. RETURN
   2. PRINT ('PRIME')
   3. RETURN
FIN DE LA SUBRUTINA PRIMO
```


Lo siguiente proporciona un programa de seudocódigo para determinar el máximo común divisor de dos enteros positivos. Este procedimiento es diferente del algoritmo euclidiano, pero en el capítulo 2 se verá cómo demostrar que este algoritmo sirve en efecto para determinar el máximo común divisor.

```
FUNCTION MCD(X, Y)
1. WHILE (X ≠ Y)
  a. IF (X > Y) THEN
    1. X ← X − Y
  b. ELSE
    1. Y ← Y − X
1. RETURN (X)
FIN DE LA FUNCIÓN MCD
```

Ejemplo 11. Utilice el seudocódigo para el MCD a fin de calcular el máximo común divisor de 190 y 34 (ejemplo 5).

Solución: La tabla 1.1 da los valores de X, Y, $X - Y$, o $Y - X$ al recorrer el programa.

Tabla 1.1

X	Y	$X - Y$	$Y - X$
190	34	156	
156	34	122	
122	34	88	
88	34	54	
54	34	20	
20	34		14
20	14	6	
6	14		8
6	8		2
6	2	4	
4	2	2	
2	2		

Como el último valor de X es 2, el máximo común divisor de 190 y 34 es 2. ◆

GRUPO DE EJERCICIOS 1.4

En los ejercicios 1 al 4, para los enteros dados m y n, escriba m como qn + r, con $0 \leq r < n$.

1. $m = 20$, $n = 3$ **2.** $m = 64$, $n = 37$
3. $m = 3$, $n = 22$ **4.** $m = 48$, $n = 12$

5. Escriba cada entero como un producto de potencias de primos (como en el teorema 3).
(a) 828 (b) 1666 (c) 1781
(d) 1125 (e) 107

En los ejercicios 6 *al* 9, *determine el máximo común divisor d de los enteros a y b, y escriba d como sa + tb.*

6. $a = 60$, $b = 100$ **7.** $a = 45$, $b = 33$

8. $a = 34$, $b = 58$ **9.** $a = 77$, $b = 128$

En los ejercicios 10 *al* 13, *encuentre el mínimo común múltiplo de los enteros.*

10. 72, 108 **11.** 150, 70

12. 175, 245 **13.** 32, 27

14. Si f es la función mód-7, calcule cada una de las siguientes.
(a) $f(17)$ (b) $f(48)$ (c) $f(1207)$
(d) $f(130)$ (e) $f(93)$ (f) $f(169)$

15. Si g es la función mód-6, resuelva cada una de las siguientes funciones.
(a) $g(n) = 3$ (b) $g(n) = 1$

16. Sean a y b dos enteros. Demuestre que si p es un primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$. (*Sugerencia:* Si $p \nmid a$, entonces $1 = \text{MCD}(a, p)$; use el teorema 4 para escribir $1 = sa + tp$.)

17. Demuestre que si $\text{MCD}(a, c) = 1$ y $c \mid ab$, entonces $c \mid b$.

18. Demuestre que si $\text{MCD}(a, c) = 1$, $a \mid m$, y $c \mid m$, entonces $ac \mid m$. (*Sugerencia:* Use el ejercicio 17.)

19. Demuestre que si $d = \text{MCD}(a, b)$, $a \mid b$, y $c \mid d$, entonces $ac \mid bd$.

20. Demuestre que $\text{MCD}(ca, cb) = c\,\text{MCD}(a, b)$.

21. Demuestre que $\text{MCM}(a, ab) = ab$.

22. Demuestre que si $\text{MCD}(a, b) = 1$, entonces $\text{MCM}(a, b) = ab$.

23. Sea $c = \text{MCM}(a, b)$. Demuestre que si $a \mid k$ y $b \mid k$, entonces $c \mid k$.

24. Demuestre que si a y b son enteros positivos tales que $a \mid b$ y $b \mid a$, entonces $a = b$.

25. Sean a un entero y p un entero positivo. Demuestre que si $p \mid a$, entonces $p = \text{MCD}(a, p)$.

1.5. Matrices

Una **matriz** es un arreglo rectangular de números dispuestos en m **renglones** horizontales y n **columnas** verticales:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

El **renglón *i*-ésimo de A** es $[a_{i1} \;\; a_{i2} \cdots a_{in}]$, $1 \le i \le m$, y la **columna j-ésima de A** es $\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$, $1 \le j \le n$. Se dice que **A** es ***m* por *n***, escrito como $m \times n$. Si $m = n$, se dice que **A** es una **matriz cuadrada** de orden n y que los números $a_{11}, a_{22}, \ldots, a_{nn}$ forman la **diagonal principal** de **A**. Se hace referencia al número a_{ij}, que está en el renglón i y en la columna j de **A**, como **el elemento *i, j* de A** o como la **entrada (*i, j*) de A**, y a menudo se escribe (1) como $\mathbf{A} = [a_{ij}]$.

Ejemplo 1. Sean

$$\mathbf{A} = \begin{bmatrix} 2 & 3 & 5 \\ 0 & -1 & 2 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}, \quad \mathbf{C} = [1 \;\; -1 \;\; 3 \;\; 4],$$

$$\mathbf{D} = \begin{bmatrix} -1 \\ 2 \\ 0 \end{bmatrix}, \quad \text{y} \quad \mathbf{E} = \begin{bmatrix} 1 & 0 & -1 \\ -1 & 2 & 3 \\ 2 & 4 & 5 \end{bmatrix}$$

Entonces **A** es 2×3 con $a_{12} = 3$ y $a_{23} = 2$, **B** es 2×2 con $b_{21} = 4$, **C** es 1×4, **D** es 3×1, y **E** es 3×3. ◆

Una matriz cuadrada $\mathbf{A} = [a_{ij}]$ para la cual cada entrada fuera de la diagonal principal es cero, es decir, $a_{ij} = 0$ para $i \neq j$, se llama **matriz diagonal**.

Ejemplo 2. Cada una de las siguientes es una matriz diagonal.

$$\mathbf{F} = \begin{bmatrix} 4 & 0 \\ 0 & 3 \end{bmatrix}, \quad \mathbf{G} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 5 \end{bmatrix}.$$ ◆

Las matrices tienen muchas aplicaciones en la ciencia de la computación, que se verá en el estudio de relaciones y gráficas. En este punto se presenta la siguiente aplicación simple que muestra cómo puede usarse las matrices para desplegar datos en forma tabular.

Ejemplo 3. La matriz siguiente da las distancias por aerolínea entre las ciudades indicadas.

$$\begin{array}{rc} & \begin{array}{cccc} \text{Londres} & \text{Madrid} & \text{Nueva York} & \text{Tokio} \end{array} \\ \begin{array}{r} \text{Londres} \\ \text{Madrid} \\ \text{Nueva York} \\ \text{Tokio} \end{array} & \begin{bmatrix} 0 & 785 & 3469 & 5959 \\ 785 & 0 & 3593 & 6706 \\ 3469 & 3593 & 0 & 6757 \\ 5959 & 6706 & 6757 & 0 \end{bmatrix} \end{array}$$ ◆

Se dice que dos matrices $m \times n$ $\mathbf{A} = [a_{ij}]$ y $\mathbf{B} = [b_{ij}]$ son **iguales** si $a_{ij} = b_{ij}$, $1 \le i \le m$, $1 \le j \le n$, es decir, si los elementos correspondientes son iguales.

Ejemplo 4. Si $\mathbf{A} = \begin{bmatrix} 2 & -3 & -1 \\ 0 & 5 & 2 \\ 4 & -4 & 6 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 2 & x & -1 \\ y & 5 & 2 \\ 4 & -4 & z \end{bmatrix}$, entonces $\mathbf{A} = \mathbf{B}$ si y solamente si $x = -3$, $y = 0$, y $z = 6$. ◆

Si $\mathbf{A} = [a_{ij}]$ y $\mathbf{B} = [b_{ij}]$ son matrices $m \times n$, entonces la **suma** de **A** y **B** es la matriz $\mathbf{C} = [c_{ij}]$ que se define por $c_{ij} = a_{ij} + b_{ij}$, $1 \le i \le m$, $1 \le j \le n$. Es decir, **C** se obtiene sumando los elementos correspondientes de **A** y **B**.

Ejemplo 5. Sean $\mathbf{A} = \begin{bmatrix} 3 & 4 & -1 \\ 5 & 0 & -2 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 4 & 5 & 3 \\ 0 & -3 & 2 \end{bmatrix}$. Entonces

$$\mathbf{A}+\mathbf{B}=\begin{bmatrix}3+4 & 4+5 & -1+3\\ 5+0 & 0+(-3) & -2+2\end{bmatrix}=\begin{bmatrix}7 & 9 & 2\\ 5 & -3 & 0\end{bmatrix}. \qquad \blacklozenge$$

Observe que la suma de las matrices **A** y **B** se define solamente cuando **A** y **B** tienen el mismo número de renglones y columnas. Se conviene escribir **A** + **B** solamente cuando está definida la suma.

A una matriz cuyas entradas sean todas cero se la llama **matriz cero** y se designa por **0**.

Ejemplo 6. Cada una de las siguientes es una matriz cero.

$$\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix} \quad \begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} \quad \begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}. \qquad \blacklozenge$$

Los siguientes teoremas dan algunas propiedades básicas de la adición de matrices; se omite las demostraciones.

Teorema 1

(a) $\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$.
(b) $(\mathbf{A}+\mathbf{B})+\mathbf{C}=\mathbf{A}+(\mathbf{B}+\mathbf{C})$.
(c) $\mathbf{A}+\mathbf{0}=\mathbf{0}+\mathbf{A}=\mathbf{A}$. ●

Si $\mathbf{A}=[a_{ij}]$ es una matriz $m \times p$, y $\mathbf{B}=[b_{ij}]$ es una matriz $p \times n$, entonces el producto de **A** y **B**, designado por **AB**, es la matriz $\mathbf{C}=[c_{ij}]$ $m \times n$ definida por

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{ip}b_{pj}, \qquad 1 \le i \le m, 1 \le j \le n. \qquad (2)$$

Se va a explicar (2) con más detalle. Los elementos $a_{i1}, a_{i2}, \ldots, a_{ip}$ forman el renglón i de **A**, y los elementos $b_{1j}, b_{2j}, \ldots, b_{pj}$ forman la columna j de **B**. Entonces (2) establece que para cualesquiera i y j el elemento c_{ij} de $\mathbf{C}=\mathbf{AB}$ puede calcularse de la siguiente manera (véase la figura 1.19).

1. Seleccione el renglón i de **A** y la columna j de **B**, y colóquelas una al lado de la otra.
2. Multiplique las entradas correspondientes y sume todos los productos.

Ejemplo 7. Sean $\mathbf{A}=\begin{bmatrix}2 & 3 & -4\\ 1 & 2 & 3\end{bmatrix}$ y $\mathbf{B}=\begin{bmatrix}3 & 1\\ -2 & 2\\ 5 & -3\end{bmatrix}$. Entonces

$$\mathbf{AB}=\begin{bmatrix}(2)(3)+(3)(-2)+(-4)(5) & (2)(1)+(3)(2)+(-4)(-3)\\ (1)(3)+(2)(-2)+(3)(5) & (1)(1)+(2)(2)+(3)(-3)\end{bmatrix}$$

$$=\begin{bmatrix}-20 & 20\\ 14 & -4\end{bmatrix}. \qquad \blacklozenge$$

Un **arreglo de dimensión dos** es una modificación de la idea de matriz, de la misma manera que un arreglo lineal es una modificación de la idea de sucesión. Por un **arreglo A**,

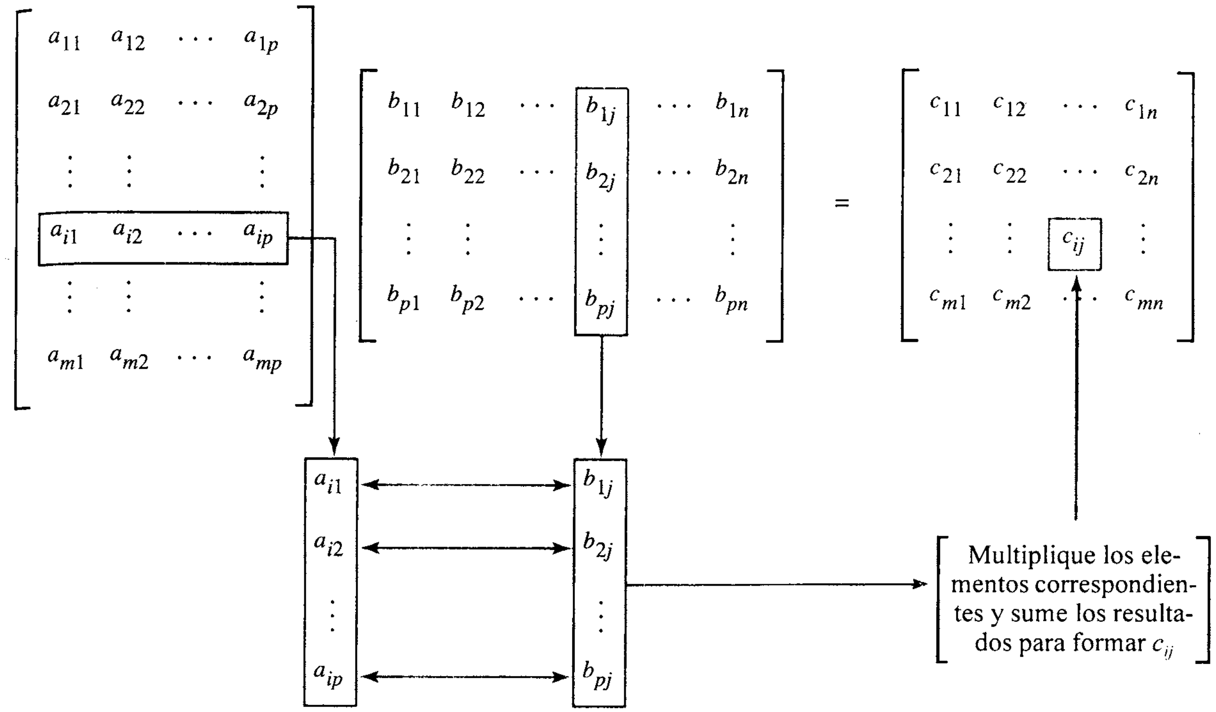


Figura 1.19

$\boldsymbol{m \times n}$ se entenderá una matriz **A** de posiciones, $m \times n$. Se puede asignar números a estas posiciones más adelante, hacer cambios posteriores en estas asignaciones, y todavía referirse a este arreglo como **A**. Éste es un modelo para almacenamiento bidimensional de información en una computadora. El número que se asigne al renglón i y a la columna j de un arreglo **A** se designará por $\mathbf{A}[i, j]$.

Como se vio con anterioridad, las propiedades de la adición de matrices se parecen a las propiedades conocidas para la adición de los números reales. Sin embargo, algunas de las propiedades de la multiplicación de matrices no se parecen a las de la multiplicación de los números reales. Primero, observe que, si **A** es una matriz $m \times p$ y **B** es una matriz $p \times n$, entonces puede calcularse **AB** y es una matriz $m \times n$. En cuanto a **BA**, existen las siguientes cuatro posibilidades:

1. **BA** puede no estar definida; es posible tener $n \neq m$.
2. **BA** puede estar definida y entonces **BA** es $p \times p$, mientras que **AB** es $m \times m$ y $p \neq m$. En consecuencia, **AB** y **BA** no son iguales.
3. **AB** y **BA** pueden ser ambas del mismo tamaño, pero no iguales como matrices.
4. **AB** = **BA**.

Se decide, como antes, escribir **AB** solamente cuando está definido el producto.

Ejemplo 8. Sean $\mathbf{A}=\begin{bmatrix}2 & 1\\ 3 & -2\end{bmatrix}$ y $\mathbf{B}=\begin{bmatrix}1 & -1\\ 2 & -3\end{bmatrix}$. Entonces $\mathbf{AB}=\begin{bmatrix}4 & -5\\ -1 & 3\end{bmatrix}$ y $\mathbf{BA}=\begin{bmatrix}-1 & 3\\ -5 & 8\end{bmatrix}$. ◆

Las propiedades básicas de la multiplicación de matrices son dadas por medio del siguiente teorema.

Teorema 2

(a) $\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}$.
(b) $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$.
(c) $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$.

●

La matriz diagonal $n \times n$

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

cuyos elementos diagonales son todos 1; se denomina **matriz identidad** de orden n. Si $\mathbf{A}$ es una matriz $m \times n$, es fácil verificar que $\mathbf{I}_m\mathbf{A} = \mathbf{A}\mathbf{I}_n = \mathbf{A}$. Si $\mathbf{A}$ es una matriz $n \times n$, y p es un entero positivo, se define

$$\mathbf{A}^p = \underbrace{\mathbf{A} \cdot \mathbf{A} \cdots \mathbf{A}}_{\text{factores } p} \quad \text{y} \quad \mathbf{A}^0 = \mathbf{I}_n.$$

Si p y q son enteros no negativos, puede demostrarse las siguientes leyes de exponentes para matrices:

$$\mathbf{A}^p\mathbf{A}^q = \mathbf{A}^{p+q} \quad \text{y} \quad (\mathbf{A}^p)^q = \mathbf{A}^{pq}.$$

Observe que la regla $(\mathbf{AB})^p = \mathbf{A}^p\mathbf{B}^p$ no es válida para matrices cuadradas. Sin embargo, si $\mathbf{AB} = \mathbf{BA}$, entonces $(\mathbf{AB})^p = \mathbf{A}^p\mathbf{B}^p$.

Si $\mathbf{A} = [a_{ij}]$ es una matriz $m \times n$, entonces la matriz $n \times m$ $\mathbf{A}^T = [a_{ij}^T]$, en donde $a_{ij}^T = a_{ji}$, $1 \leq i \leq m$, $1 \leq j \leq n$, se llama la **transpuesta de A**. En consecuencia, la transpuesta de $\mathbf{A}$ se obtiene intercambiando los renglones y las columnas de $\mathbf{A}$.

Ejemplo 9. Sean $\mathbf{A} = \begin{bmatrix} 2 & -3 & 5 \\ 6 & 1 & 3 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 3 & 4 & 5 \\ 2 & -1 & 0 \\ 1 & 6 & -2 \end{bmatrix}$. Entonces $\mathbf{A}^T = \begin{bmatrix} 2 & 6 \\ -3 & 1 \\ 5 & 3 \end{bmatrix}$ y

$$\mathbf{B}^T = \begin{bmatrix} 3 & 2 & 1 \\ 4 & -1 & 6 \\ 5 & 0 & -2 \end{bmatrix}.$$

◆

El siguiente teorema resume las propiedades básicas de la operación de transpuesta.

Teorema 3. *Si* $\mathbf{A}$ *y* $\mathbf{B}$ *son matrices, entonces*

(a) $(\mathbf{A}^T)^T = \mathbf{A}$.
(b) $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$.
(c) $(\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T$.

●

Una matriz $\mathbf{A} = [a_{ij}]$ se denomina **simétrica** si $\mathbf{A}^T = \mathbf{A}$. En consecuencia, si $\mathbf{A}$ es simétrica, debe ser una matriz cuadrada. Es fácil demostrar que $\mathbf{A}$ es simétrica si y solamente si $a_{ij} = a_{ji}$. Es decir, $\mathbf{A}$ es simétrica si y solamente si las entradas de $\mathbf{A}$ son simétricas con respecto de la diagonal principal de $\mathbf{A}$.

Ejemplo 10. Si $\mathbf{A} = \begin{bmatrix} 1 & 2 & -3 \\ 2 & 4 & 5 \\ -3 & 5 & 6 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 1 & 2 & -3 \\ 2 & 4 & 0 \\ 3 & 2 & 1 \end{bmatrix}$, entonces $\mathbf{A}$ es simétrica y $\mathbf{B}$ no es simétrica.

◆

Operaciones con matrices booleanas

Una **matriz booleana** es una matriz $m \times n$ cuyas entradas son ya sea cero o uno. Se definirá ahora tres operaciones con matrices booleanas que tienen aplicaciones útiles en el capítulo 4.

Sean $\mathbf{A} = [a_{ij}]$ y $\mathbf{B} = [b_{ij}]$ matrices booleanas $m \times n$. Se define $\mathbf{A} \vee \mathbf{B} = \mathbf{C} = [c_{ij}]$, la **unión** de $\mathbf{A}$ y $\mathbf{B}$, por

$$c_{ij} = \begin{cases} 1 & \text{si } a_{ij} = 1 \text{ o } b_{ij} = 1 \\ 0 & \text{si } a_{ij} \text{ y } b_{ij} \text{ son ambos } 0. \end{cases}$$

y $\mathbf{A} \wedge \mathbf{B} = \mathbf{D} = [d_{ij}]$, la **conjunción** de $\mathbf{A}$ y $\mathbf{B}$, por

$$d_{ij} = \begin{cases} 1 & \text{si } a_{ij} \text{ y } b_{ij} \text{ son ambos } 1 \\ 0 & \text{si } a_{ij} = 0 \text{ o } b_{ij} = 0. \end{cases}$$

Nótese que estas operaciones son sólo posibles cuando $\mathbf{A}$ y $\mathbf{B}$ tienen el mismo tamaño, precisamente como en el caso de la adición de matrices. En vez de sumar los elementos correspondientes de $\mathbf{A}$ y $\mathbf{B}$, para calcular las entradas del resultado, se examina simplemente los elementos correspondientes para los patrones particulares.

Ejemplo 11. Sean $\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$.

(a) Calcule $\mathbf{A} \vee \mathbf{B}$. (b) Calcule $\mathbf{A} \wedge \mathbf{B}$.

Solución: (a) Sea $\mathbf{A} \vee \mathbf{B} = [c_{ij}]$. Entonces, como a_{43} y b_{43} son ambos 0, se observa que $c_{43} = 0$. En todos los demás casos, ya sea a_{ij} o b_{ij} es 1, de manera que c_{ij} es también 1. En consecuencia,

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

(b) Sea $\mathbf{A} \wedge \mathbf{B} = [d_{ij}]$. Entonces, como a_{11} y b_{11} son ambos 1, $d_{11} = 1$, y como a_{23} y b_{23} son ambos 1, $d_{23} = 1$. En todos los demas casos, ya sea a_{ij} o b_{ij} es 0, de manera que $d_{ij} = 0$. En consecuencia,

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

◆

Finalmente, supóngase que $\mathbf{A} = [a_{ij}]$ es una matriz booleana $m \times p$ y $\mathbf{B} = [b_{ij}]$ es una matriz booleana $p \times n$. Nótese que la condición sobre los tamaños de **A** y **B** es exactamente la condición que se necesita para formar la matriz producto **AB**. Ahora se definirá otra clase de producto.

El **producto booleano** de **A** y **B**, que se designa por $\mathbf{A} \odot \mathbf{B}$, es la matriz booleana $m \times n$ $\mathbf{C} = [c_{ij}]$ que se define por

$$c_{ij} = \begin{cases} 1 & \text{si } a_{ik} = 1 \text{ y } b_{kj} = 1 \text{ para alguna } k,\ 1 \le k \le p \\ 0 & \text{de lo contrario.} \end{cases}$$

Esta multiplicación es similar a la multiplicación ordinaria de matrices. La fórmula anterior establece que para cualquier valor de i y j, puede calcularse el elemento c_{ij} de $\mathbf{C} = \mathbf{A} \odot \mathbf{B}$ de la siguiente manera (véase la figura 1.20 y compárese ésta con la figura 1.19).

1. Seleccione el renglón i de **A** y la columna j de **B**, y póngalas una al lado de otra.
2. Compare las entradas correspondientes. Basta con que un par de entradas correspondientes conste de dos unos, para que $c_{ij} = 1$. Si no es éste el caso, entonces $c_{ij} = 0$.

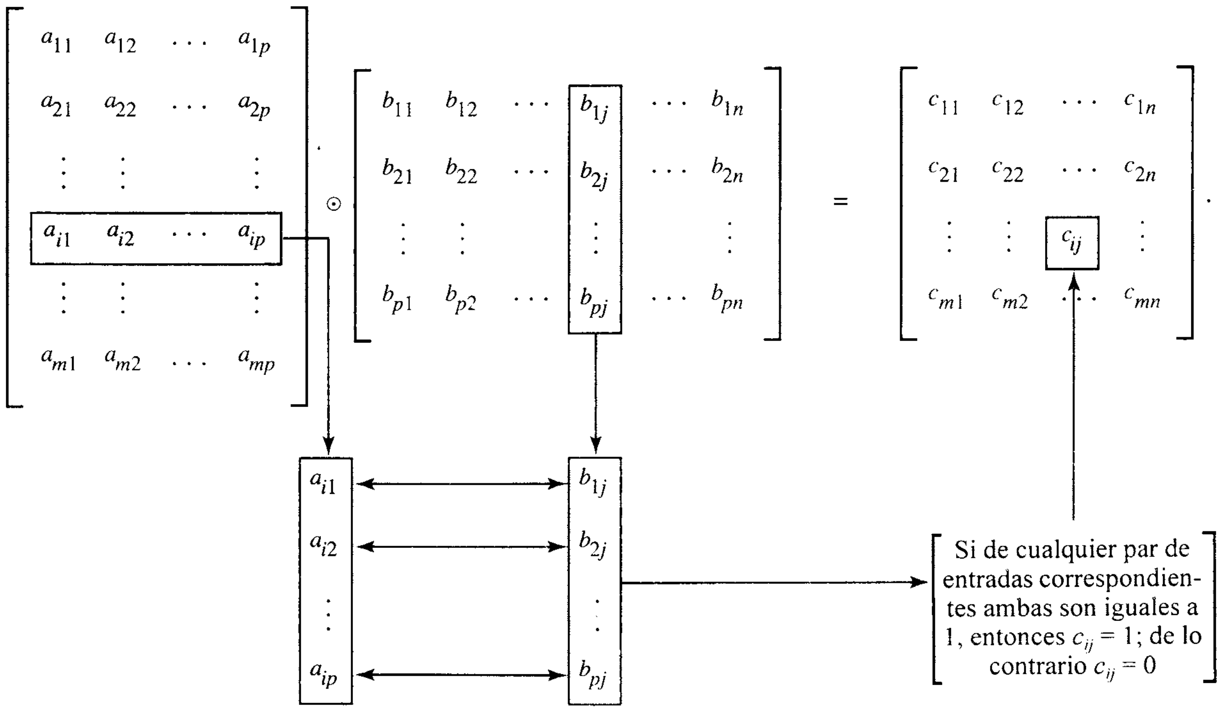


Figura 1.20

Se puede efectuar fácilmente las comparaciones indicadas y las verificaciones para cada posición del producto booleano. Así, por lo menos para los seres humanos, el cálculo de los elementos que hay en $\mathbf{A} \odot \mathbf{B}$ es considerablemente más fácil que el cálculo de los elementos que hay en **AB**.

Ejemplo 12. Sean $\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$. Calcule $\mathbf{A} \odot \mathbf{B}$.

Solución: Sea $\mathbf{A} \odot \mathbf{B} = [e_{ij}]$. Entonces $e_{11} = 1$, ya que el renglón 1 de **A** y la columna 1 de **B** tienen cada uno un 1 como primera entrada. De modo semejante, $e_{12} = 1$, ya que $a_{12} = 1$ y $b_{22} = 1$; es decir, el primer renglón de **A** y la segunda columna de **B** tienen un 1 en la segunda posición. De manera semejante se ve que $e_{13} = 1$. Por otra parte, $e_{14} = 0$, en vista de que el renglón 1 de **A** y la columna 4 de **B** no tienen "unos" comunes en ninguna posición. Procediendo de esta manera, se obtiene

$$\mathbf{A} \odot \mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

◆

El siguiente teorema, cuya demostración se deja como ejercicio, resume las propiedades básicas de las operaciones con matrices booleanas que se acaba de definir.

Teorema 4. *Si* **A**, **B** *y* **C** *son matrices booleanas de tamaños compatibles, se tiene*

1. (a) $\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A}$.
   (b) $\mathbf{A} \wedge \mathbf{B} = \mathbf{B} \wedge \mathbf{A}$.
2. (a) $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C} = \mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$.
   (b) $(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C} = \mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})$.
3. (a) $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$.
   (b) $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$.
4. $(\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C} = \mathbf{A} \odot (\mathbf{B} \odot \mathbf{C})$.

●

GRUPO DE EJERCICIOS 1.5

1. Sean $\mathbf{A} = \begin{bmatrix} 3 & -2 & 5 \\ 4 & 1 & 2 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$, y

$$\mathbf{C} = \begin{bmatrix} 2 & 3 & 4 \\ 5 & 6 & -1 \\ 2 & 0 & 8 \end{bmatrix}.$$

(a) ¿Qué es a_{12}, a_{22}, a_{23}?
(b) ¿Qué es b_{11}, b_{31}?
(c) ¿Qué es c_{13}, c_{23}, c_{33}?
(d) Haga una lista de los elementos de la diagonal principal de **C**.

2. ¿Cuáles de las siguientes son matrices diagonales?

(a) $\mathbf{A} = \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix}$ (b) $\mathbf{B} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 5 \end{bmatrix}$

(c) $\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

(d) $\mathbf{D} = \begin{bmatrix} 2 & 6 & 2 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{bmatrix}$

(e) $\mathbf{E} = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}$

3. Si $\begin{bmatrix} a+b & c+d \\ c-d & a-b \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 10 & 2 \end{bmatrix}$, encuentre a, b, c y d.

4. Si $\begin{bmatrix} a+2b & 2a-b \\ 2c+d & c-2d \end{bmatrix} = \begin{bmatrix} 4 & -2 \\ 4 & -3 \end{bmatrix}$, encuentre a, b, c y d.

En los ejercicios 5 *al* 10, *supóngase que*

$$\mathbf{A} = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 1 & -2 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \\ 2 & 3 \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 1 & -2 & 3 \\ 4 & 2 & 5 \\ 3 & 1 & 2 \end{bmatrix}, \mathbf{D} = \begin{bmatrix} -3 & 2 \\ 4 & 1 \end{bmatrix},$$

$$\mathbf{E} = \begin{bmatrix} 3 & 2 & -1 \\ 5 & 4 & -3 \\ 0 & 1 & 2 \end{bmatrix}, \text{ y } \mathbf{F} = \begin{bmatrix} -2 & 3 \\ 4 & 5 \end{bmatrix}.$$

5. En caso de ser posible, calcule cada una de las siguientes.
   (a) $\mathbf{C} + \mathbf{E}$ (b) $\mathbf{AB}$ y $\mathbf{BA}$
   (c) $\mathbf{CB} + \mathbf{F}$ (d) $\mathbf{AB} + \mathbf{DF}$

6. En caso de ser posible, calcule cada una de las siguientes.
   (a) $\mathbf{A}(\mathbf{BD})$ y $(\mathbf{AB})\mathbf{D}$
   (b) $\mathbf{A}(\mathbf{C} + \mathbf{E})$ y $\mathbf{AC} + \mathbf{AE}$
   (c) $\mathbf{FD} + \mathbf{AB}$

7. En caso de ser posible, calcule cada una de las siguientes.
   (a) $\mathbf{EB} + \mathbf{FA}$ (b) $\mathbf{A}(\mathbf{B} + \mathbf{D})$ y $\mathbf{AB} + \mathbf{AD}$
   (c) $(\mathbf{F} + \mathbf{D})\mathbf{A}$ (d) $\mathbf{AC} + \mathbf{DE}$

8. En caso de ser posible, calcule cada una de las siguientes.
   (a) $\mathbf{A}^T$ y $(\mathbf{A}^T)^T$ (b) $(\mathbf{C} + \mathbf{E})^T$ y $\mathbf{C}^T + \mathbf{E}^T$
   (c) $(\mathbf{AB})^T$ y $\mathbf{B}^T\mathbf{A}^T$ (d) $(\mathbf{B}^T\mathbf{C}) + \mathbf{A}$

9. En caso de ser posible, calcule cada una de las siguientes.
   (a) $\mathbf{A}^T(\mathbf{D} + \mathbf{F})$ (b) $(\mathbf{BC})^T$ y $\mathbf{C}^T\mathbf{B}^T$
   (c) $(\mathbf{B}^T + \mathbf{A})\mathbf{C}$ (d) $(\mathbf{D}^T + \mathbf{E})\mathbf{F}$

10. Calcule **D**.

11. Sea **A** una matriz $m \times n$. Demuestre que $\mathbf{I}_m\mathbf{A} = \mathbf{A}\mathbf{I}_n = \mathbf{A}$.

12. Sean $\mathbf{A} = \begin{bmatrix} 2 & 1 \\ 3 & -2 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} -1 & 2 \\ 3 & 4 \end{bmatrix}$. Demuestre que $\mathbf{AB} \neq \mathbf{BA}$.

13. Sea $\mathbf{A} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 4 \end{bmatrix}$
    (a) Calcule $\mathbf{A}^3$. (b) ¿Qué es $\mathbf{A}^k$?

14. Demuestre que $\mathbf{A0} = \mathbf{0}$ para cualquier matriz **A**.

15. Demuestre que $\mathbf{I}_n^T = \mathbf{I}_n$.

16. (a) Demuestre que si **A** tiene un renglón de ceros, entonces **AB** tiene un renglón correspondiente de ceros.
    (b) Demuestre que si **B** tiene una columna de ceros, entonces **AB** tiene una columna correspondiente de ceros.

17. Demuestre que la columna j del producto de matrices **AB** es igual al producto matricial $\mathbf{AB}_j$, en donde $\mathbf{B}_j$ es la columna j de **B**.

18. Si **0** es la matriz cero 2×2, determine dos matrices 2×2, **A** y **B**, con $\mathbf{A} \neq \mathbf{0}$ y $\mathbf{B} \neq \mathbf{0}$, tales que $\mathbf{AB} = \mathbf{0}$.

19. Si $\mathbf{A} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, demuestre que $\mathbf{A}^2 = \mathbf{I}_2$.

20. Determine todas las matrices 2×2 $\mathbf{A} = \begin{bmatrix} 0 & a \\ b & c \end{bmatrix}$ tales que $\mathbf{A}^2 = \mathbf{I}_2$.

21. Sean **A** y **B** matrices simétricas.
    (a) Demuestre que $\mathbf{A} + \mathbf{B}$ es también simétrica.
    (b) ¿Es **AB** también simétrica?

22. Sea **A** una matriz $n \times n$.
    (a) Demuestre que $\mathbf{AA}^T$ y $\mathbf{A}^T\mathbf{A}$ son simétricas.
    (b) Demuestre que $\mathbf{A} + \mathbf{A}^T$ es simétrica.

23. Demuestre el teorema 3. [*Sugerencia:* Para la parte (c), demuestre que el elemento i, j de $(\mathbf{AB})^T$ es igual al elemento i, j de $\mathbf{B}^T\mathbf{A}^T$.]

24. En cada parte, calcule $\mathbf{A} \vee \mathbf{B}$, $\mathbf{A} \wedge \mathbf{B}$ y $\mathbf{A} \odot \mathbf{B}$ para las matrices dadas **A** y **B**.
    (a) $\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
    (b) $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$
    (c) $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$
    (d) $\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$
    (e) $\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$
    (f) $\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

25. (a) Demuestre que $\mathbf{A} \vee \mathbf{A} = \mathbf{A}$.
    (b) Demuestre que $\mathbf{A} \wedge \mathbf{A} = \mathbf{A}$.

26. (a) Demuestre que $\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A}$.
    (b) Demuestre que $\mathbf{A} \wedge \mathbf{B} = \mathbf{B} \wedge \mathbf{A}$.

27. (a) Demuestre que $\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}$.
    (b) Demuestre que $\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}$.
    (c) Demuestre que $\mathbf{A} \odot (\mathbf{B} \odot \mathbf{C}) = (\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C}$.

28. (a) Demuestre que $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$.
    (b) Demuestre que $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$.

29. Sean $\mathbf{A} = [a_{ij}]$ y $\mathbf{B} = [b_{ij}]$ dos matrices $n \times n$, y supóngase que $\mathbf{C} = [c_{ij}]$ representa a **AB**. Demuestre que si k es un entero y $k \mid a_{ij}$ para todos los valores de i, j, entonces $k \mid c_{ij}$ para todos los valores de i, j.

30. Sea p un número primo con $p > 2$, y sean **A** y **B** matrices cuyas entradas sean todas enteros. Supóngase que p divide a todas las entradas de $\mathbf{A} + \mathbf{B}$ y a todas las entradas de $\mathbf{A} - \mathbf{B}$. Demuestre que p divide a todas las entradas de **A** y a todas las entradas de **B**.

1.6. Estructuras matemáticas

Una situación que se ha visto varias veces en este capítulo, y que se verá muchas más en capítulos posteriores, es la siguiente. Se define una nueva clase de objeto matemático, por ejemplo, un conjunto o una matriz. Entonces se introduce notación para representar el nuevo tipo de objeto, y se describe una manera para determinar si dos objetos son o no lo mismo. Por lo general, el siguiente tema consiste en formas para clasificar los objetos del nuevo tipo, como por ejemplo, en finitos o infinitos para los conjuntos, y en booleanas o simétricas para las matrices. Luego se definen operaciones para examinar los objetos y las propiedades de dichas operaciones.

Una serie de objetos con la definición de las operaciones que se realizan con éstos y las propiedades que las acompañan, forma una **estructura matemática** o un **sistema matemático**. En este libro se estudia únicamente las estructuras matemáticas discretas.

Ejemplo 1. La colección de los conjuntos con las operaciones de unión, intersección y complemento, y las propiedades relacionadas, es una estructura matemática (discreta). Se denota esta estructura por [conjuntos, $\cup$, $\cap$, $^-$]. ◆

Ejemplo 2. La colección de las matrices 3×3 con las operaciones de adición, multiplicación y transpuesta es una estructura matemática que se denota por [matrices 3×3, +, *, ^{T}]. ◆

Una propiedad importante que no se ha identificado antes es la de cerradura. Una estructura es **cerrada con respecto de** una operación si esa operación produce siempre otro miembro de la colección de objetos.

Ejemplo 3. La estructura [matrices 5×5, +, *, ^{T}] es cerrada con respecto de la adición, porque la suma de dos matrices 5×5 es otra matriz 5×5. ◆

Ejemplo 4. La estructura [enteros impares, +, *] no es cerrada con respecto de la adición. La suma de dos enteros impares es un entero par. Esta estructura tiene la propiedad de cerradura para la multiplicación, ya que el producto de dos números impares es un número impar. ◆

Una operación que combina dos objetos es una **operación binaria**. Una operación que requiere sólo un objeto es una **operación unaria**. Las operaciones binarias tienen a menudo propiedades similares, como se vio con anterioridad.

Ejemplo 5

(a) La intersección de conjuntos es una operación binaria, en vista de que combina dos conjuntos para producir un nuevo conjunto.

(b) La producción de la transpuesta de una matriz es una operación unaria. ◆

A las propiedades comunes se les ha dado nombres. Por ejemplo, si el orden de los objetos no afecta el resultado de una operación binaria, se dice que la operación es **conmutativa**. Es decir, si $x \square y = y \square x$, en donde $\square$ es alguna operación binaria, $\square$ es conmutativa.

Ejemplo 6

(a) La unión y la conjunción para matrices booleanas son operaciones conmutativas.

$$\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A} \text{ y } \mathbf{A} \wedge \mathbf{B} = \mathbf{B} \wedge \mathbf{A}.$$

(b) La multiplicación ordinaria de matrices no es una operación conmutativa. $\mathbf{AB} \neq \mathbf{BA}$. ◆

Nótese que cuando se dice que una operación binaria tiene una propiedad, eso significa que el enunciado de la propiedad es verdadero cuando se usa la operación con cualesquiera de los objetos de la estructura. Si existe aunque sea un caso en que el enunciado no sea verdadero, la operación no tiene esa propiedad.

Si $\square$ es una operación binaria, entonces $\square$ es **asociativa**, es decir, **tiene la propiedad asociativa** si

$$(x \square y) \square z = x \square (y \square z).$$

Ejemplo 7. La unión de conjuntos es una operación asociativa, ya que $(A \cup B) \cup C = A \cup (B \cup C)$ siempre es verdadera. ◆

Si una estructura matemática tiene dos operaciones binarias, por ejemplo $\square$ y ∇, una **propiedad distributiva** tiene el siguiente esquema:

$$x \square (y \nabla z) = (x \square y) \nabla (x \square z).$$

Ejemplo 8

(a) Ya se conoce bien la propiedad distributiva para los números reales; si a, b y c son números reales, entonces $a \cdot (b + c) = a \cdot b + a \cdot c$. Nótese que, debido a que existe el acuerdo en la aritmética de los números reales de multiplicar antes de sumar, no se necesita paréntesis en el lado derecho.

(b) La estructura [conjuntos, $\cup$, $\cap$, $^-$] tiene dos propiedades distributivas.

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

y

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

Varias de las estructuras revisadas tienen una operación unaria y dos operaciones binarias. Surge la pregunta de si para tales estructuras las leyes de De Morgan son propiedades del sistema. Si la operación unaria es * y las operaciones binarias son $\square$ y ∇, entonces las **leyes de De Morgan** son

$$(x \square y)^* = x^* \nabla y^* \quad \text{y} \quad (x \nabla y)^* = x^* \square y^*.$$

Ejemplo 9

(a) Como se vio en la sección 1.2, los conjuntos satisfacen las leyes de De Morgan para unión, intersección y complemento: $(\overline{A \cap B}) = \overline{A} \cup \overline{B}$ y $(\overline{A \cup B}) = \overline{A} \cap \overline{B}$.

(b) La estructura [números reales, +, *, $\sqrt{\ }$] no satisface las leyes de De Morgan, ya que $\sqrt{x+y} \neq \sqrt{x} * \sqrt{y}$. ◆

Una estructura con una operación binaria $\square$ puede contener un objeto distinguido, e, con la propiedad $x \square e = e \square x = x$. A e se la llama **identidad para** $\square$. En realidad, una identidad para una operación debe ser única.

Teorema 1. *Si e es una identidad para una operación binaria $\square$, entonces e es única.*

Demostración: Supóngase que otro objeto i tiene también la propiedad de identidad, de manera que $x \square i = i \square x = x$. Entonces $e \square i = e$; pero como e es una identidad para $\square$, $i \square e = e \square i = i$. En consecuencia $i = e$. Existe cuando mucho un objeto con la propiedad de identidad para $\square$. ●

Ejemplo 10. Para la estructura [matrices $n \times n$, +, *, ^{T}], $\mathbf{I}_n$ es la identidad para multiplicación de matrices, y la matriz cero $n \times n$ es la identidad para adición de matrices. ◆

Si una operación binaria $\square$ tiene una identidad e, se dice que y es una **$\square$-inversa** de x si $x \square y = y \square x = e$.

Teorema 2. *Si $\square$ es una operación asociativa y x tiene una $\square$-inversa y, entonces y es única.*

Demostración: Supóngase que existe otra $\square$-inversa para x, por ejemplo z. Entonces $(z \square x) \square y = e \square y = y$ y $z \square (x \square y) = z \square e = z$. Como $\square$ es asociativa, $(z \square x) \square y = z \square (x \square y)$, y por tanto $y = z$. ●

Ejemplo 11

(a) En la estructura [matrices 3×3, +, *, ^{T}], cada matriz $\mathbf{A} = [a_{ij}]$ tiene una +-inversa, o inversa aditiva, $-\mathbf{A} = [-a_{ij}]$.

(b) En la estructura [enteros, +, *], sólo los enteros 1 y -1 tienen inversos multiplicativos. ♦

Ejemplo 12. Sean $\square$, $\triangledown$ y * las operaciones que se define para el conjunto $\{0, 1\}$ por medio de las tablas siguientes:

$\square$	0	1
0	0	1
1	1	0

$\triangledown$	0	1
0	0	0
1	0	1

x^*	x
0	1
1	0

Así $1 \square 0 = 1$, $0 \triangledown 1 = 0$ y $1^* = 0$.
Determine si cada uno de los siguientes casos es verdadero para $[\{0,1\}, \square, \triangledown, *]$.
(a) $\square$ es conmutativa.
(b) $\triangledown$ es asociativa.
(c) Las leyes de De Morgan son válidas.
(d) Son válidas dos propiedades distributivas para la estructura.

Solución: (a) El enunciado $x \square y = y \square x$ debe ser verdadero para todas las opciones de x y y. Aquí hay sólo un caso por verificar: ¿Es $0 \square 1 = 1 \square 0$ verdadera? Como ambas $0 \square 1$ y $1 \square 0$ son 1, $\square$ es conmutativa.

(b) Se deja como ejercicio verificar los ocho casos posibles. Véase el ejercicio 4(b).

(c) $(0 \square 0)^* = 0^* = 1$ $\quad 0^* \triangledown 0^* = 1 \triangledown 1 = 1$
$(0 \square 1)^* = 1^* = 0$ $\quad 0^* \triangledown 1^* = 1 \triangledown 0 = 0$
$(1 \square 1)^* = 0^* = 1$ $\quad 1^* \triangledown 1^* = 0 \triangledown 0 = 0.$

El último par muestra que las leyes de De Morgan no son válidas en esta estructura.

(d) Una propiedad distributiva posible es $x \square (y \triangledown z) = (x \square y) \triangledown (x \square z)$. Debe verificarse todos los casos posibles. En la tabla 1.2 se muestra una forma de organizar esto.

Tabla 1.2

x y z	$y \triangledown z$	$x \square (y \triangledown z)$	$x \square y$	$x \square z$	$(x \square y) \triangledown (x \square z)$
0 0 0	0	0	0	0	0
0 0 1	0	0	0	1	0
0 1 0	0	0	1	0	0
0 1 1	1	1	1	1	1
1 0 0	0	1	1	1	1
1 0 1	0	1	1	0	0
1 1 0	0	1	0	1	0
1 1 1	1	0	0	0	0
		(A)			(B)

Como las columnas (A) y (B) no son idénticas, esta posible propiedad distributiva no es válida en esta estructura. La verificación para la otra propiedad distributiva es el ejercicio 5. ♦

En secciones posteriores, resultará útil considerar las estructuras matemáticas como objetos y clasificarlas atendiendo a las propiedades asociadas con sus operaciones.

GRUPO DE EJERCICIOS 1.6

1. Diga si en cada parte la estructura tiene o no la propiedad de cerradura con respecto de la operación.
   (a) [conjuntos, $\cup$, $\cap$, $^-$] unión
   (b) [conjuntos, $\cup$, $\cap$, $^-$] complemento
   (c) [matrices 4×4, +, *, ^{T}] multiplicación
   (d) [matrices 3×5, +, *, ^{T}] transpuesta

2. Diga si en cada parte la estructura tiene o no la propiedad de cerradura con respecto de la operación.
   (a) [enteros, +, $-$, *, $\div$] división
   (b) [A^*, concatenación] concatenación
   (c) [matrices booleanas $n \times n$, $\vee$, $\wedge$, ^{T}] conjunción.
   (d) [números primos, +, *] adición

3. Demuestre que $\oplus$ es una operación conmutativa para conjuntos.

4. Por medio de las definiciones del ejemplo 12, (a) demuestre que $\square$ es asociativa. (b) Demuestre que $\triangledown$ es asociativa.

5. Por medio de las definiciones del ejemplo 12, determine si sigue siendo válida la otra propiedad distributiva posible.

6. Porporcione el elemento identidad, si existe alguno, para cada operación binaria en la estructura dada.
   (a) [números reales, +, *, $\sqrt{\ }$]
   (b) [conjuntos, $\cup$, $\cap$, $^-$]
   (c) $[\{0, 1\}, \square, \triangledown, *]$ como son definidos en el ejemplo 12
   (d) [subconjuntos de un conjunto finito A, $\oplus$, $-$]

7. Dé el elemento identidad, si existe alguno, para cada operación binaria en la estructura [matrices booleanas 5×5, $\vee$, $\wedge$, $\odot$].

En los ejercicios 8 *al* 14, *use la estructura* $S =$ [matrices diagonales $n \times n$, +, *, ^{T}].

8. Demuestre que S es cerrada con respecto de la adición.

9. Demuestre que S es cerrada con respecto de la multiplicación.

10. Demuestre que S es cerrada con respecto de la operación de transpuesta.

11. ¿Tiene S una identidad para la adición? Si es así ¿cuál es?

12. ¿Tiene S una identidad para la multiplicación? Si es así ¿cuál es?

13. Sea **A** una matriz diagonal $n \times n$. Describa la inversa aditiva de **A**.

14. Sea **A** una matriz diagonal $n \times n$. Describa la inversa multiplicativa de **A**.

En los ejercicios 15 *al* 20, *use la estructura* $R = [M, +, *, ^T]$, *en donde* M *es el conjunto de matrices de la forma* $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$; *a es un número real.*

15. Demuestre que R es cerrada con respecto de la adición.

16. Demuestre que R es cerrada con respecto de la multiplicación.

17. Demuestre que R es cerrada con respecto de la operación de transpuesta.

18. ¿Tiene R una identidad para la adición? Si es así ¿cuál es?

19. ¿Tiene R una identidad para la multiplicación? Si es así ¿cuál es?

20. Sea **A** un elemento de M. Describa la inversa de la adición para **A**.

IDEAS CLAVE PARA REPASO

- Conjunto: una colección de objetos bien definida.
- $\varnothing$ (conjunto vacío): el conjunto sin elementos.
- Conjuntos iguales: conjuntos con los mismos elementos.
- $A \subseteq B$ (A es un subconjunto de B): Todo elemento de A es un elemento de B.
- $|A|$ (cardinalidad de A): el número de elementos de A.

- Conjunto infinito: véase la página 4.
- $P(A)$ (conjunto potencia de A): Conjunto de todos los subconjuntos de A.
- $A \cup B$ (unión de A y B): $\{x \mid x \in A$, o bien, $x \in B\}$.
- $A \cap B$ (intersección de A y B): $\{x \mid x \in A$ y $x \in B\}$.
- Conjuntos disjuntos: dos conjuntos sin elementos en común.
- $A - B$ (complemento de B con respecto de A): $\{x \mid x \in A$ y $x \notin B\}$.
- $\overline{A}$ (complemento de A): $\{x \mid x \notin A\}$.
- Propiedades algebraicas de las operaciones con conjuntos: véase la página 9.
- Teorema (el principio de adición): Si A y B son conjuntos finitos, entonces $|A \cup B| = |A| + |B| - |A \cap B|$.
- Teorema (el principio de adición de tres conjuntos): Si A, B y C son conjuntos finitos, entonces

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

- Sucesión: lista de objetos en un orden definido.
- Fórmula recursiva: una fórmula que utiliza términos previamente definidos.
- Fórmula explícita: una fórmula que no utiliza términos previamente definidos.
- Arreglo lineal: véase la página 16.
- Función característica de un conjunto A:

$$f_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A. \end{cases}$$

- Conjunto numerable: un conjunto que corresponde a una sucesión.
- Palabra: sucesión finita de elementos de A.
- Expresión regular: véase la página 19.
- Teorema: Si $n \neq 0$ y m son enteros no negativos, puede escribirse $m = qn + r$ para algunos enteros no negativos q y r con $0 \leq r < n$. Además, sólo hay una forma de hacer esto.
- MCD(a, b): $d =$ MCD(a, b) si $d \mid a$, $d \mid b$, y d es el divisor común más grande de a y b.
- Teorema: Si d es MCD(a, b), entonces
  (a) $d = sa + tb$ para algunos enteros s y t.
  (b) Si $c \mid a$ y $c \mid b$, entonces $c \mid d$.
- Primos relativos: dos enteros a y b con MCD$(a, b) = 1$.
- Algoritmo euclidiano: método usado para determinar el MCD(a, b); véase la página 25.
- MCM(a, b): $c =$ MCM(a, b) si $a \mid c$, $b \mid c$, y c es el múltiplo común más pequeño de a y b.
- MCD$(a, b) \cdot$ MCM$(a, b) = ab$.
- Función mód-n: $f_n(z) = r$, en donde $z \equiv r$ (mód n).
- Matriz: un arreglo rectangular de números.
- Tamaño de una matriz: $\mathbf{A}$ es $m \times n$ si tiene m renglones y n columnas.
- Matriz diagonal: una matriz cuadrada con ceros en las entradas que no están en la diagonal principal.
- Matrices iguales: matrices del mismo tamaño cuyas entradas correspondientes son iguales.
- $\mathbf{A} + \mathbf{B}$: la matriz obtenida sumando las entradas correspondientes de $\mathbf{A}$ y $\mathbf{B}$.
- Matriz cero: una matriz cuyas entradas son todas igual a cero.
- $\mathbf{AB}$: véase la página 32.
- $\mathbf{I}_n$ (matriz identidad): una matriz cuadrada con unos en la diagonal y ceros en las demás partes.
- $\mathbf{A}^T$: la matriz obtenida de $\mathbf{A}$ por intercambio de renglones y columnas de $\mathbf{A}$.
- Matriz simétrica: $\mathbf{A}^T = \mathbf{A}$.
- Arreglo de dimensión dos: véase la página 32.
- Matriz booleana: una matriz cuyas entradas son ya sea uno o cero.
- $\mathbf{A} \vee \mathbf{B}$: véase la página 35.
- $\mathbf{A} \wedge \mathbf{B}$: véase la página 35.
- $\mathbf{A} \odot \mathbf{B}$: véase la página 36.
- Propiedades de las operaciones en matrices booleanas: véase la página 37.
- Estructura matemática: una serie de objetos con operaciones definidas sobre los mismos y las propiedades acompañantes.
- Operación binaria: una operación que combina dos objetos.
- Operación unaria: una operación que requiere sólo de un objeto.
- Propiedad de cerradura: cada aplicación de la operación produce otro objeto en la colección.
- Propiedad asociativa: $(x \square y) \square z = x \square (y \square z)$
- Leyes de De Morgan: $(x \square y)^* = x^* \square y^*$ y $(x \square y)^* = x^* \square y^*$.
- Identidad para $\square$: un elemento e tal que $x \square e = e \square x = x$ para todas las x que hay en la estructura.
- $\square$-inverso de x: un elemento y tal que $x \square y = y \square x = e$, en donde e es la identidad para $\square$.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes casos, escriba el programa o la subrutina que se pide, en seudocódigo (como se describe en el apéndice A) o en un lenguaje de programación que usted conozca. Pruebe su código ya sea con papel y lápiz, o ejecutándolo en una computadora.

En los ejercicios 1 *al* 3, *suponga que A y B son conjuntos finitos de enteros. Escriba una subrutina para calcular el conjunto especificado.*

1. $A \cup B$

2. $A \cap B$

3. $A - B$

4. Considere la sucesión definida en forma recursiva por

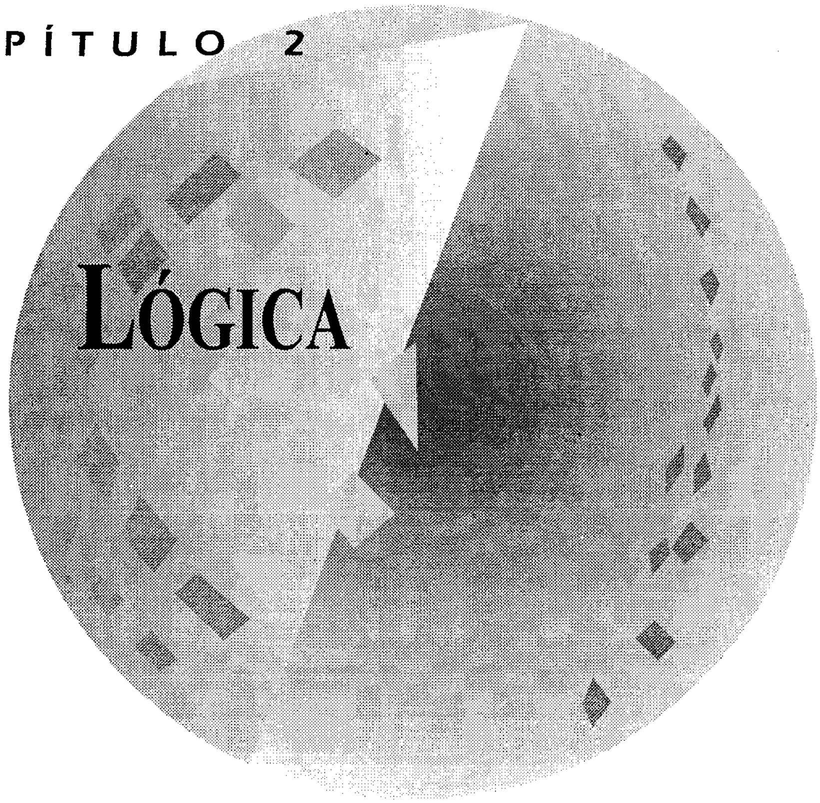
$$g(0) = 1 \qquad g(1) = -1$$
$$g(n) = 3g(n-1) - 2g(n-2)$$

(a) Escriba una subrutina que imprima los primeros 20 términos de la sucesión.
(b) Escriba una subrutina que imprima los primeros n términos de la sucesión. El usuario debe ser capaz de proporcionar el valor de n en la subrutina.

5. Escriba una subrutina para determinar el mínimo común múltiplo de dos enteros positivos.

CAPÍTULO 2

LÓGICA



Requisito previo: Capítulo 1

Lógica es la disciplina que trata de los métodos de razonamiento. En un nivel elemental, la lógica proporciona reglas y técnicas para determinar si es o no válido un argumento dado. El razonamiento lógico se emplea en matemáticas para demostrar teoremas; en ciencias de la computación, para verificar si son o no correctos los programas y para demostrar teoremas; en las ciencias físicas y naturales, para sacar conclusiones de experimentos, y en las ciencias sociales y en la vida cotidiana, para resolver una multitud de problemas. Ciertamente, se usa en forma constante el razonamiento lógico. En este capítulo se analiza algunas de las ideas básicas.

2.1. Proposiciones y operaciones lógicas

Una **proposición** o **enunciado** es una oración que declara que algo es verdadero o falso, pero no ambas cosas.

Ejemplo 1. ¿Cuáles de las siguientes son proposiciones?

(a) La Tierra es redonda.
(b) $2 + 3 = 5$
(c) ¿Habla usted inglés?
(d) $3 - x = 5$
(e) Tome dos aspirinas.
(f) La temperatura en la superficie del planeta Venus es 800°F.
(g) El Sol saldrá mañana.

Solución

(a) y (b) son proposiciones que afirman algo verdadero.
(c) es una pregunta, por lo cual no es proposición.
(d) es una afirmación declarativa, pero no una proposición, ya que es verdadera o falsa dependiendo del valor de x.
(e) no es proposición; es una orden.
(f) es una oración declarativa cuya verdad o falsedad no se conoce hasta la fecha; sin embargo, es posible determinar si es verdadera o falsa, por lo cual sí es una proposición.
(g) es una proposición, verdadera o falsa, aunque no ambas cosas; no obstante, se tendría que esperar hasta mañana para saber si fue verdadera o falsa. ◆

Conectivos lógicos y proposiciones compuestas

En matemáticas, las letras $x, y, z, \ldots$ denotan, a menudo, variables que pueden ser reemplazadas por números reales, y estas variables pueden combinarse con las operaciones comunes $+, \times, -,$ y $\div$. En lógica, las letras $p, q, r, \ldots$ denotan **variables propositivas**, es decir, variables que pueden ser reemplazadas por proposiciones. Así se puede escribir p: El Sol está brillando hoy. q: Hace frío. Las proposiciones o variables propositivas pueden combinarse por medio de conectivos lógicos para obtener **proposiciones compuestas**. Por ejemplo, se puede combinar las proposiciones anteriores con el conectivo *y* para formar la proposición compuesta p *y* q: El Sol está brillando *y* hace frío. El valor de verdad de una proposición compuesta depende solamente de los valores de verdad de las proposiciones que se estén combinando y de los tipos de conectivos que se utilice. A continuación, se verá los conectivos más importantes.

Si p es una proposición, la **negación** de p es la proposición *no* p, denotada por $\sim p$. Así $\sim p$ es la proposición "no es el caso de p." De esta definición se desprende que si p es verdadera, entonces $\sim p$ es falsa, y si p es falsa, $\sim p$ es verdadera. El valor de verdad de $\sim p$ relativo a p se da en la tabla 2.1. A una tabla como ésta, que da los valores de verdad de una proposición compuesta en función de sus partes componentes, se la llama **tabla de verdad**.

Tabla 2.1

p	$\sim p$
T	F
F	T

Estrictamente hablando, *no* no es un conectivo, en vista de que no une dos proposiciones, y $\sim p$ no es en realidad una proposición compuesta. Sin embargo, *no* es una operación unaria para la colección de proposiciones, y $\sim p$ es una proposición si p lo es.

Ejemplo 2. Dé la negación de las siguientes proposiciones.
(a) p: $2 + 3 > 1$ (b) q: Hace frío.

Solución:
(a) $\sim p$: $2 + 3$ no es mayor que 1. Es decir, $\sim p$: $2 + 3 \leq 1$. Como p es verdadera en este caso, $\sim p$ es falsa.
(b) $\sim q$: No es el caso de que haga frío. Más simplemente, $\sim q$: No hace frío. ◆

Si p y q son proposiciones, la **conjunción** de p y q es la proposición compuesta "p y q", denotada por $p \wedge q$. El conectivo *y* se denota por el símbolo $\wedge$. En el lenguaje de la sección 1.6, *y* es una operación binaria sobre el conjunto de proposiciones. La proposición compuesta $p \wedge q$ es verdadera cuando ambas, p y q, son verdaderas; de lo contrario, es falsa. Los valores de verdad de $p \wedge q$ en términos de los valores de verdad de p y q son proporcionados en la tabla de verdad que aparece en la tabla 2.2. Obsérvese que para dar la tabla de verdad de $p \wedge q$ se necesita considerar cuatro casos posibles. Esto se desprende del hecho de que cada una de las proposiciones p y q puede ser verdadera o falsa.

Tabla 2.2

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Ejemplo 3. Forme la conjunción de p y q para cada uno de los siguientes casos.
(a) p: Está nevando. q: Tengo frío.
(b) p: $2 < 3$ q: $-5 > -8$
(c) p: Está nevando. q: $3 < 5$

Solución
(a) $p \wedge q$: Está nevando y tengo frío.
(b) $p \wedge q$: $2 < 3$ y $-5 > -8$
(c) $p \wedge q$: Está nevando y $3 < 5$. ◆

El ejemplo 3(c) muestra que en lógica, a diferencia de lo que ocurre en el habla cotidiana, es posible unir dos proposiciones que no guarden relación alguna por medio del conectivo *y*.

Si p y q son proposiciones, la **disyunción** de p y q es la proposición compuesta "p o q", designada por $p \vee q$. El conectivo *o* se denota por el símbolo $\vee$. La proposición compuesta $p \vee q$ es verdadera si por lo menos una de las proposiciones p o q es verdadera; será falsa cuando ambas proposiciones p y q sean falsas. Los valores de $p \vee q$ son proporcionados en la tabla de verdad que aparece en la tabla 2.3.

Tabla 2.3

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Ejemplo 4. Forme la disyunción de p y q para cada uno de los siguientes casos.
(a) p: 2 es un entero positivo. q: $\sqrt{2}$ es un número racional.
(b) p: $2 + 3 \neq 5$ q: Londres es la capital de Francia.

Solución
(a) $p \vee q$: 2 es un entero positivo o $\sqrt{2}$ es un número racional. Como p es verdadera, la disyunción $p \vee q$ es verdadera, aun cuando q sea falsa.
(b) $p \vee q$: $2 + 3 \neq 5$ o Londres es la capital de Francia. Como ambas proposiciones p y q son falsas, $p \vee q$ es falsa. ◆

El ejemplo 4(b) demuestra que en la lógica, a diferencia de lo que sucede en el habla ordinaria, es posible unir dos proposiciones totalmente faltas de relación por el conectivo *o*.

El conectivo *o* es más complicado que el conectivo *y* porque se emplea de dos formas diferentes. Supóngase que alguien dice: "Fui en automóvil a mi trabajo o tomé el tren para ir a mi trabajo." En esta proposición compuesta se tiene la disyunción de las proposiciones p: "Fui en automóvil a mi trabajo" y q: "Tomé el tren para ir a mi trabajo." Por supuesto, ocurrió exactamente una de las dos posibilidades. No podrías haber ocurrido ambas, por lo cual el conectivo *o* se está usando en un sentido *excluyente.* Por otra parte, considérese la disyunción "Pasé matemáticas o reprobé francés." En este caso, ocurrió por lo menos una de las dos posibilidades. Empero, podrían haber ocurrido ambas, por lo que el conectivo *o* se está usando en un sentido *inclusivo.* En matemáticas y en ciencias de la computación, convencionalmente se usa el conectivo *o* siempre en sentido inclusivo.

Cuantificadores

En la sección 1.1, se definieron conjuntos especificando una propiedad $P(x)$ que tienen en común los elementos del conjunto. Así, un elemento de $\{x \mid P(x)\}$ es un objeto t para el cual la proposición $P(t)$ es verdadera. A una oración de esta naturaleza $P(x)$ se la llama **predicado**, porque en español la propiedad es gramaticalmente un predicado. $P(x)$ se denomina también **función proposicional**, porque cada selección de x da lugar a una proposición $P(x)$ que es o verdadera o falsa.

Ejemplo 5. Sea $A = \{x \mid x \text{ un entero menor que } 8\}$. Aquí $P(x)$ es la oración "x es un entero menor que 8." La propiedad común es "es un entero menor que 8". Como $P(1)$ es verdadera, $1 \in A$. ◆

La **cuantificación universal** de un predicado $P(x)$ es la proposición "Para todos los valores de x, $P(x)$ es verdadera". Se supone que solo se considera los valores de x que tengan sentido en $P(x)$. Si se desea restringir los valores de x, se puede escribir, por ejemplo, $\forall x \geq 0$ o $\forall n \in Z$. La cuantificación universal de $P(x)$ se denota por $\forall x\ P(\ )$. Al símbolo $\forall$ se lo llama cuantificador universal.

Ejemplo 6

(a) La oración $P(x)$: $-(-x) = x$ es un predicado que tiene sentido para los números reales x. La cuantificación universal de $P(x)$, $\forall x\ P(x)$, es una proposición verdadera, porque para todos los números reales $-(-x) = x$.

(b) Sea $Q(x)$: $x + 1 < 4$. Entonces $\forall x \geq 0\ Q(x)$ es una proposición falsa, porque $Q(5)$ no es verdadera. ♦

La cuantificación universal puede expresarse también en español como "para toda x", "toda x" o "para cualquier x".

Un predicado puede contener diversas variables. La cuantificación universal puede aplicarse a cada una de las variables. Por ejemplo, una propiedad conmutativa puede expresarse como $\forall x\ \forall y\ x \square y = y \square x$. El orden en que se considere los cuantificadores universales no cambia el valor de verdad. Con frecuencia, hay proposiciones matemáticas que contienen cuantificaciones universales implícitas, como por ejemplo, en el teorema 1, la sección 1.2.

En algunas situaciones sólo se requiere que haya por lo menos un valor para el cual sea verdadero el predicado. La **cuantificación existencial** de un predicado $P(x)$ es la proposición "Existe un valor de x para el cual $P(x)$ es verdadera." La cuantificación existencial de $P(x)$ se denota $\exists\ x\ P(x)$. El símbolo $\exists$ se llama cuantificador existencial. Se puede incluir restricciones en el cuantificador, como por ejemplo, $\exists\ x > 0$.

Ejemplo 7

(a) Sea $Q(x)$: $x + 1 < 4$. La cuantificación existencial de $Q(x)$, $\exists x\ Q(x)$, es una proposición verdadera, porque $Q(2)$ es una proposición verdadera.

(b) La proposición $\exists y\ y + 2 = y$ es falsa. No hay valor alguno de y para el cual la función proposicional $y + 2 = y$ produzca una proposición verdadera. ♦

El $\exists x$ puede leerse también como "hay una x", "hay alguna x", "existe una x", o "hay por lo menos una x".

La cuantificación existencial puede aplicarse a diversas variables en un predicado, y el orden en que se considera las cuantificaciones no afecta el valor de verdad. Para un predicado con diversas variables, puede aplicarse tanto la cuantificación universal como la existencial. En este caso el orden sí es importante.

Ejemplo 8. Sean **A** y **B** matrices $n \times n$.

(a) La proposición $\forall \mathbf{A}\ \exists \mathbf{B}\ (\mathbf{A} + \mathbf{B}) = \mathbf{I}_n$ se lee "por cada **A** hay una **B** tal que $\mathbf{A} + \mathbf{B} = \mathbf{I}_n$". Para una **A** dada, $\mathbf{A} = [a_{ij}]$, defina $\mathbf{B} = [b_{ij}]$ como sigue: $b_{ii} = 1 - a_{ii}$, $1 \leq i \leq n$ y $b_{ij} = -a_{ij}$, $i \neq j$, $1 \leq i \leq n$, $1 \leq j \leq n$. Entonces $\mathbf{A} + \mathbf{B} = \mathbf{I}_n$ y se ha demostrado que $\forall \mathbf{A}\ \exists \mathbf{B}\ (\mathbf{A} + \mathbf{B}) = \mathbf{I}_n$ es una proposición verdadera.

(b) $\exists \mathbf{B}\ \forall \mathbf{A}\ (\mathbf{A} + \mathbf{B}) = \mathbf{I}_n$ es la proposición "hay una **B** tal que para todas las **A**, $\mathbf{A} + \mathbf{B} = \mathbf{I}_n$". Esta proposición es falsa; ninguna **B** sola tiene esta propiedad para todas las **A**.

(c) $\exists \mathbf{B}\ \forall \mathbf{A}\ (\mathbf{A} + \mathbf{B}) = \mathbf{A}$ es verdadera. ¿Cuál es el valor para **B** que hace verdadera esta proposición? ♦

Sea p: $\forall x\ P(x)$. La negación de p es falsa cuando p es verdadera, y verdadera cuando p es falsa. Para que p sea falsa, debe haber por lo menos un valor de x para el cual $P(x)$ sea falsa. En consecuencia, p es falsa si $\exists x \sim P(x)$ es verdadera. Por otra parte, si $\exists x \sim P(x)$ es falsa, entonces para cada x, $\sim P(x)$ es falsa, por lo que $P(x)$ es verdadera; es decir, $\forall x\ P(x)$ es verdadera. Esto demuestra que la negación de p es $\exists x \sim P(x)$.

Ejemplo 9

(a) Sea p: Para todos los enteros positivos n, $n^2 + 41n + 41$ es un número primo. Entonces $\sim p$: Hay por lo menos un entero positivo n para el cual $n^2 + 41n + 41$ no es primo.

(b) Sea q: Hay algún entero k para el cual $12 = 3k$. Entonces $\sim q$: Para todos los enteros k, $12 \neq 3k$. ♦

GRUPO DE EJERCICIOS 2.1

1. ¿Cuáles de las siguientes son proposiciones?
(a) ¿Es 2 un número positivo?
(b) $x^2 + x + 1 = 0$
(c) Estudie lógica.
(d) Habrá nieve en enero.
(e) Si se caen los precios de las acciones, perderé dinero.

2. Dé la negación de cada una de las siguientes proposiciones.
(a) $2 + 7 \leq 11$
(b) 2 es un entero par y 8 es un entero impar.
(c) Lloverá mañana o nevará mañana.
(d) Si usted va en auto, entonces yo caminaré.

3. En cada uno de los siguientes casos, forme la conjunción y la disyunción de p y q.
(a) p: $3 + 1 < 5$ — q: $7 = 3 \times 6$
(b) p: Soy rico. — q: Soy feliz.
(c) p: Voy a ir en mi auto. — q: Llegaré tarde.

4. Determine la verdad o falsedad de cada una de las proposiciones siguientes.
(a) $2 < 3$ y 3 es un entero positivo.
(b) $2 \geq 3$ y 3 es un entero positivo.
(c) $2 < 3$ y 3 no es un entero positivo.
(d) $2 \geq 3$ y 3 no es un entero positivo.

5. Determine la verdad o falsedad de cada una de las proposiciones siguientes.
(a) $2 < 3$ o 3 es un entero positivo.
(b) $2 \geq 3$ o 3 es un entero positivo.
(c) $2 < 3$ o 3 no es un entero positivo.
(d) $2 \geq 3$ no es un entero positivo.

6. ¿Cuál de las siguientes proposiciones es la negación de la proposición "2 es par y -3 es negativo"?
(a) 2 es par y -3 es no negativo.
(b) 2 es impar y -3 es no negativo.
(c) 2 es par o -3 es no negativo.
(d) 2 es impar o -3 es no negativo.

7. ¿Cuál de las siguientes proposiciones es la negación de la proposición "2 es par o -3 es negativo"?
(a) 2 es par o -3 es no negativo.
(b) 2 es impar o -3 es no negativo.
(c) 2 es par y -3 es no negativo.
(d) 2 es impar y -3 es no negativo.

En los ejercicios 8 y 9 utilice p: Hoy es lunes; q: El pasto está mojado; y r: El plato se fue con la cuchara.

8. Escriba cada una de las siguientes proposiciones en términos de p, q, r y conectivos lógicos.
(a) Hoy es lunes y el plato no se fue con la cuchara.
(b) O el pasto está mojado u hoy es lunes.
(c) Hoy no es lunes y el pasto está seco.
(d) El plato se fue con la cuchara, pero el pasto está mojado.

9. Escriba una oración que corresponda a cada una de las siguientes proposiciones.
(a) $\sim r \wedge q$ (b) $\sim q \vee p$
(c) $\sim(p \vee q)$ (d) $p \vee \sim r$

En los ejercicios 10 *al* 15, *utilice* P(x): *x es par;* Q(x): *x es un número primo; y* R (x, y): *x* + *y es par. Las variables x y y representan enteros.*

10. Escriba una oración que corresponda a cada una de las siguientes proposiciones.
(a) $\forall x$ P (x) (b) $\exists x$ Q (x)

11. Escriba una oración que corresponda a cada una de las siguientes proposiciones.
(a) $\forall x \exists y$ R (x, y) (b) $\exists x \forall y$ R(x, y)

12. Escriba una oración que corresponda a cada una de las siguientes proposiciones.
(a) $\forall x$ (~Q(x)) (b) $\exists y$ (~P(y))

13. Escriba una oración que corresponda a cada una de las siguientes proposiciones.
(a) ~($\exists x$ P(x)) (b) ~($\forall x$ Q(x))

14. Escriba cada una de las siguientes proposiciones en términos de P(x), Q(x), R(x, y), conectivos lógicos, y cuantificadores.
(a) Todo entero es un número impar.
(b) La suma de dos enteros cualesquiera es un número par.

15. Determine el valor de verdad de cada proposición en los ejercicios 10 al 13.

16. Haga una tabla de verdad para cada una de las siguientes proposiciones.
(a) $(\sim p \wedge q) \vee p$ (b) $(p \vee q) \vee \sim q$

17. Haga una tabla de verdad para cada una de las siguientes proposiciones.
(a) $(p \vee q) \wedge r$ (b) $(\sim p \vee q) \wedge \sim r$

Para los ejercicios 18 *al* 20, *defina* $p \downarrow q$ *como una proposición verdadera si no son verdaderas ni p ni q.*

p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

18. Haga una tabla de verdad para $(p \downarrow q) \downarrow r$.

19. Haga una tabla de verdad para $(p \downarrow q) \wedge (p \downarrow r)$.

20. Haga una tabla de verdad para $(p \downarrow q) \downarrow (p \downarrow r)$.

2.2. Proposiciones condicionales

Si p y q son proposiciones, a la proposición compuesta si p entonces q, designada por $p \to q$, se le llama **proposición condicional**, o **implicación**. A la proposición p se le llama **antecedente** o **hipótesis**, y a la proposición q se le llama **consecuente** o **conclusión**. El conectivo *si . . . entonces* se denota por el símbolo $\to$.

Ejemplo 1. Escriba la implicación $p \to q$ para cada una de las siguientes proposiciones.
(a) p: Tengo hambre. q: Comeré.
(b) p: Está nevando. q: $3 + 5 = 8$

Solución
(a) Si tengo hambre, entonces comeré.
(b) Si está nevando, entonces $3 + 5 = 8$. ◆

El ejemplo 1(b) muestra que en lógica se usa proposiciones condicionales en un sentido más general que el acostumbrado. Así, cuando se dice "si p entonces q", se está suponiendo tácitamente que hay una relación de causa y efecto entre p y q. Es decir, nunca se usaría la proposición del ejemplo 1(b) en lenguaje ordinario, en vista de que no hay manera de lograr que la proposición p pueda tener algún efecto sobre la proposición q.

En lógica se emplea la implicación en un sentido mucho más débil. Decir que la proposición compuesta $p \to q$ es verdadera, simplemente afirma que si p es verdadera, se encontrará entonces que q también es verdadera. En otras palabras, $p \to q$ dice solamente que no se tendrá una p verdadera y una q falsa al mismo tiempo. No dice que p "ocasionó" a q en el sentido usual. La tabla 2.4 describe los valores de verdad de $p \to q$ en términos de los valores de verdad de p y de q. Debe notarse que $p \to q$ se considera falsa solamente si p es verdadera y q es falsa. En particular, si p es falsa, entonces $p \to q$ es verdadera para cualquier q. Este hecho se describe algunas veces por la proposición, "Una hipótesis falsa implica cualquier conclusión". Esta proposición es confusa, ya que parece decir que si la hipótesis es falsa, la conclusión debe ser verdadera, lo cual es obviamente tonto. De modo similar, si q es verdadera, entonces $p \to q$ será verdadera para cualquier proposición p. La implicación "Si $2 + 2 = 5$, entonces yo soy el rey de Inglaterra" es verdadera, simplemente porque p: $2 + 2 = 5$ es falsa, por lo que no es el caso de que p sea verdadera y q sea falsa simultáneamente.

Tabla 2.4

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

En el habla cotidiana, y en matemáticas, cada una de las expresiones siguientes es una forma equivalente de la proposición condicional $p \to q$: p implica a q; q, si p; p solamente si q; p es una condición suficiente para q; q es una condición necesaria para p.

Si $p \to q$ es una implicación, entonces la **recíproca** de $p \to q$ es la implicación $q \to p$, y la **contrapositiva** de $p \to q$ es la implicación $\sim q \to \sim p$.

Ejemplo 2. Dé la recíproca y la contrapositiva de la implicación "Si está lloviendo, entonces yo me mojo."

Solución: Se tiene p: Está lloviendo; y q: Yo me mojo. La recíproca es $q \to p$: Si yo me mojo, entonces está lloviendo. La contrapositiva es $\sim q \to \sim p$: Si yo no me mojo, entonces no está lloviendo. ◆

Si p y q son proposiciones, a la proposición compuesta p si y sólo si q, denotada por $p \leftrightarrow q$, se le llama **equivalencia** o **bicondicional**. El conectivo *si y sólo si* se denota por el símbolo $\leftrightarrow$. Se proporciona los valores de verdad de $p \leftrightarrow q$ en la tabla 2.5. Observe que $p \leftrightarrow q$ es verdadera sólo cuando ambas, p y q, son verdaderas o cuando ambas p y q son falsas. La equivalencia $p \leftrightarrow q$ puede también enunciarse como p es una condición necesaria y suficiente para q.

Tabla 2.5

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Ejemplo 3. ¿Es la siguiente equivalencia una proposición verdadera? $3 > 2$ si y sólo si $0 < 3 - 2$.

Solución: Sea p la proposición $3 > 2$ y sea q la proposición $0 < 3 - 2$. Como ambas, p y q, son verdaderas, se concluye que $p \leftrightarrow q$ es verdadera. ◆

En general, una proposición compuesta puede tener muchas partes componentes, siendo cada una de éstas una proposición por sí misma, representada por alguna variable proporcional. La proposición s: $p \to (q \wedge (p \to r))$ contiene tres proposiciones, p, q y r, cada una de las cuales puede, en forma independiente, ser verdadera o falsa. Hay en total 2^3, o sea 8 posibles combinaciones de valores de verdad para p, q y r, y la tabla de verdad para s debe indicar la verdad o falsedad de s en todos estos casos. Si una proposición compuesta s contiene n proposiciones componentes, habrá necesidad de tener 2^n renglones en la tabla de verdad para s. (En la sección 3.1 se ve la forma de contar las posibilidades en tales casos.) Esta tabla de verdad puede construirse sistemáticamente de la siguiente manera.

PASO 1. Las primeras n columnas de la tabla están marcadas por las variables proposicionales componentes. Se incluye columnas adicionales para todas las combinaciones intermedias de las variables, y esto culmina en una columna para la proposición completa.

PASO 2. Bajo cada uno de los primeros n encabezados, se ha anotado las 2^n posibles n-uplas de valores de verdad para las n proposiciones componentes.

PASO 3. Para cada renglón se calcula, en secuencia, todos los valores de verdad restantes.

Ejemplo 4. Calcule la tabla de verdad de la proposición $(p \to q) \leftrightarrow (\sim q \to \sim p)$. La tabla 2.6 se ha construido siguiendo los pasos 1, 2 y 3. Los números de la parte inferior de las columnas muestran el orden en que están construidos.

Tabla 2.6

p	q	$p \to q$	$\sim q$	$\sim p$	$\sim q \to \sim p$	$(p \to q) \leftrightarrow (\sim q \to \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T
		(1)	(2)	(3)	(4)	(5)

◆

Una proposición que es verdadera para todos los valores posibles de sus variables propositivas se denomina **tautología**. A una proposición que siempre es falsa se la llama **contradicción** o **falacia**, y a una proposición que puede ser o verdadera o falsa, dependiendo de los valores de verdad de sus variables propositivas, se la llama **contingencia**.

Ejemplo 5

(a) La proposición del ejemplo 4 es una tautología.

(b) La proposición $p \wedge \sim p$ es una falacia. (Verifique esto.)

(c) La proposición $(p \to q) \wedge (p \vee q)$ es una contingencia. ◆

Se ha definido ahora una nueva estructura matemática con dos operaciones binarias y una operación unaria [proposiciones, $\wedge$, $\vee$, $\sim$]. No tiene sentido decir que dos proposiciones son iguales, por lo que en lugar de esto se afirma que p y q son **lógicamente equivalentes**, o simplemente **equivalentes**, si $p \leftrightarrow q$ es una tautología. Cuando se demuestra que una equivalencia es una tautología, esto significa que sus dos partes componentes son siempre al mismo tiempo o verdaderas o falsas para cualesquiera valores de las variables propositivas. En consecuencia los dos lados son simplemente maneras diferentes de construir la misma proposición y pueden ser consideradas como "iguales." Se denota que p es equivalente a q por $p \equiv q$. Ahora se puede adaptar nuestras propiedades para operaciones para decir que esta estructura tiene una propiedad si usando equivalentes en lugar de igualdad se obtiene una proposición verdadera.

Ejemplo 6. La operación binaria $\vee$ tiene la propiedad conmutativa; es decir, $p \vee q \equiv q \vee p$. La tabla de verdad (tabla 2.7) para $(p \vee q) \leftrightarrow (q \vee p)$ muestra que la proposición es una tautología.

Tabla 2.7

p	q	$p \vee q$	$q \vee p$	$(p \vee q) \leftrightarrow (q \vee p)$
T	T	T	T	T
T	F	T	T	T
F	T	T	T	T
F	F	F	F	T

◆

Otra manera de usar una tabla de verdad para determinar si dos proposiciones son equivalentes es construir una columna para cada proposición y comparar éstas para ver si son idénticas. En el ejemplo 6 las columnas tercera y cuarta son idénticas, y esto garantizará que las proposiciones que representan son equivalentes.

La formación de $p \to q$ a partir de p y q es otra operación binaria para proposiciones, pero puede expresarse en términos de las operaciones de la sección 2.1.

Ejemplo 7. La proposición condicional $p \to q$ es equivalente a $(\sim p) \vee q$. Las columnas (1) y (3) de la tabla 2.8 muestran que, para cualesquiera valores de verdad de p y q, $p \to q$ y $(\sim p) \vee q$ tienen los mismos valores de verdad.

Tabla 2.8

p	q	$p \to q$	$\sim p$	$(\sim p) \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T
		(1)	(2)	(3)

◆

La estructura [proposiciones, $\wedge$, $\vee$, $\sim$] tiene muchas de las propiedades que [conjuntos, $\cup$, $\cap$, $^{-}$].

Teorema 1. *Las operaciones para proposiciones tienen las siguientes propiedades.*

Propiedades conmutativas

1. $p \vee q \equiv q \vee p$
2. $p \wedge q \equiv q \wedge p$

Propiedades asociativas

3. $p \vee (q \vee r) \equiv (p \vee q) \vee r$
4. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Propiedades distributivas

5. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
6. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Propiedades idempotentes

7. $p \vee p \equiv p$
8. $p \wedge p \equiv p$

Propiedades de negación

9. $\sim(\sim p) \equiv p$
10. $\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$
11. $\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$ 10 *y* 11 *son las leyes de De Morgan.*

Demostración: Se ha demostrado la propiedad 1 en el ejemplo 6. Las propiedades restantes pueden ser demostradas de la misma manera y se deja como ejercicio al lector. ●

La operación de implicación tiene también varias propiedades importantes.

Teorema 2

(a) $(p \to q) \equiv ((\sim p) \vee q)$
(b) $(p \to q) \equiv ((\sim q) \to \sim p)$
(c) $(p \leftrightarrow q) \equiv ((p \to q) \wedge (q \to p))$
(d) $\sim(p \to q) \equiv (p \wedge \sim q)$
(e) $\sim(p \leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$

Demostración: La parte (a) se demostró en el ejemplo 7 y la parte (b) en el ejemplo 4. Nótese que la parte (b) dice que una proposición condicional es equivalente a su contrapositiva.

La parte (d) da una versión alternativa para la negación de una proposición condicional. Esto podría demostrarse usando tablas de verdad, pero también es posible hacerlo aprovechando hechos demostrados previamente. Como $(p \to q) \equiv ((\sim p) \vee q)$, la negación de $p \to q$ debe ser equivalente a $\sim((\sim p) \vee q)$. Por las leyes de De Morgan, $\sim((\sim p) \vee q) \equiv (\sim(\sim p)) \wedge (\sim q)$ o $p \wedge (\sim q)$. En consecuencia $\sim(p \to q) \equiv (p \wedge (\sim q))$.

Las partes restantes del teorema 2 quedan como ejercicios. ●

El teorema 3 establece dos resultados de la sección 2.1 y otras varias propiedades para los cuantificadores universal y existencial

Teorema 3

(a) $\sim(\forall x\ P(x)) \equiv \exists x\ \sim P(x)$
(b) $\sim(\exists x\ \sim P(x)) \equiv \forall x\ P(x)$
(c) $\exists x\ (P(x) \to Q(x)) \equiv \forall x\ P(x) \to \exists x\ Q(x)$
(d) $\exists x\ P(x) \to \forall x\ Q(x) \equiv \forall x\ (P(x) \to Q(x))$
(e) $\exists x\ (P(x) \vee Q(x)) \equiv \exists x\ P(x) \vee \exists x\ Q(x)$

(g) $((\forall x\ P(x)) \vee (\forall x\ Q(x))) \to \forall x\ (P(x) \vee Q(x))$ es una tautología.
(h) $\exists x\ (P(x) \wedge Q(x)) \to \exists x\ P(x) \wedge \exists x\ Q(x)$ es una tautología. ●

El teorema siguiente da varias implicaciones importantes que son tautologías. Se hará un extenso uso de éstas en la demostración de resultados en matemáticas y ciencias de la computación, y serán ilustradas en la sección 2.3.

Teorema 4. *Cada una de las siguientes proposiciones es una tautología.*

(a) $(p \wedge q) \to p$
(b) $(p \wedge q) \to q$
(c) $p \to (p \vee q)$
(d) $q \to (p \vee q)$
(e) $\sim p \to (p \to q)$
(f) $\sim(p \to q) \to p$
(g) $(p \wedge (p \to q)) \to q$
(h) $(\sim p \wedge (p \vee q)) \to q$
(i) $(\sim q \wedge (p \to q)) \to \sim p$
(j) $((p \to q) \wedge (q \to r)) \to (p \to r)$ ●

GRUPO DE EJERCICIOS 2.2

En los ejercicios 1 *y* 2 *use los siguientes datos*: *p*: *Estoy despierto*; *q*: *Trabajo duramente*; *r*: *Sueño con mi hogar.*

1. Escriba cada una de las siguientes proposiciones en términos de *p, q, r* y de palabras de unión lógicas.
(a) Estoy despierto implica que trabajo duramente.
(b) Sueño con mi hogar solamente si estoy despierto.
(c) Trabajar duramente me basta para estar despierto.
(d) Me es necesario estar despierto para no soñar con mi hogar.

2. Escriba cada una de las siguientes proposiciones en términos de *p, q, r* y de palabras de unión lógicas.
(a) No estoy despierto si y sólo si sueño con mi hogar.
(b) Si sueño con mi hogar, entonces estoy despierto y trabajo duramente.
(c) No trabajo duramente sólo si estoy despierto y no sueño con mi hogar.
(d) No estar despierto y soñando con mi hogar me basta para trabajar duramente.

3. Enuncie la recíproca de cada una de las siguientes implicaciones.
(a) Si 2 + 2 = 4, entonces yo no soy la reina de Inglaterra.
(b) Si no soy Presidente de los Estados Unidos, entonces caminaré a mi trabajo.
(c) Si ya se me hizo tarde, entonces no tomé el tren para mi trabajo.
(d) Si tengo tiempo y no estoy demasiado cansado, entonces iré a la tienda.
(e) Si tengo suficiente dinero, entonces compraré un automóvil y compraré una casa.

4. Enuncie la contrapositiva de cada implicación del ejercicio 3.

5. Determine el valor de verdad para cada una de las siguientes proposiciones.
(a) Si 2 es par, entonces Nueva York tiene una población grande.
(b) Si 2 es par, entonces Nueva York tiene una población pequeña.
(c) Si 2 es impar, entonces Nueva York tiene una población grande.
(d) Si 2 es impar, entonces Nueva York tiene una población pequeña.

En los ejercicios 6 y 7, sean p, q y r las siguientes proposiciones: *p*: *Estudiaré estructuras discretas*; *q*: *Iré a un cine*; *r*: *Estoy de buen humor.*

6. Escriba las siguientes proposiciones en términos de *p, q, r y de conectivos lógicos.*
(a) Si no estoy de buen humor, entonces iré a un cine.
(b) No iré a un cine y estudiaré estructuras discretas.
(c) Iré a un cine sólo si no estudio estructuras discretas.

(d) Si no estudio estructuras discretas, entonces no estoy de buen humor.

7. Escriba oraciones que correspondan a las siguientes proposiciones.
(a) $((\sim p) \wedge q) \rightarrow r$ (b) $r \rightarrow (p \vee q)$
(c) $(\sim r) \rightarrow ((\sim q) \vee p)$ (d) $(q \wedge (\sim p)) \leftrightarrow r$

8. Construya tablas de verdad para determinar si cada una de las siguientes proposiciones es una tautología, una contingencia o una falacia.
(a) $p \wedge \sim p$ (b) $p \rightarrow (q \rightarrow p)$
(c) $q \rightarrow (q \rightarrow p)$ (d) $q \vee (\sim q \wedge p)$
(e) $(q \wedge p) \vee (q \wedge \sim p)$ (f) $(p \wedge q) \rightarrow p$
(g) $p \rightarrow (q \wedge p)$

9. Si $p \rightarrow q$ es falsa, ¿puede determinar el valor de verdad de $(\sim(p \wedge q)) \rightarrow q$? Explique su respuesta.

10. Si $p \rightarrow q$ es verdadera, puede determinar el valor de verdad de $(\sim p) \vee (p \rightarrow q)$? Explique su respuesta.

11. Utilice la definición de $p \downarrow q$ dada en el ejercicio 18 en la sección 2.1 y demuestre que $((p \downarrow p) \downarrow (q \downarrow q))$ es equivalente a $p \wedge q$.

12. Escriba la negación de cada una de las siguientes proposiciones.
(a) Hace mal tiempo y no iré a trabajar.
(b) Si Carolina no está enferma, entonces va a la excursión; ella la va a pasar bien.
(c) Yo no ganaré el juego o no entraré en la competencia.

13. Considere la siguiente proposición condicional: p: Si la inundación destruye mi casa o el fuego destruye mi casa, entonces mi compañía de seguros me pagará.
(a) ¿Cuál de las siguientes proposiciones es la recíproca de p?
(b) ¿Cuál de las siguientes proposiciones es la contrapositiva de p?
(i) Si mi compañía de seguros me paga, entonces la inundación destruye mi casa o el fuego destruye mi casa.
(ii) Si mi compañía de seguros me paga, entonces la inundación destruye mi casa y el fuego destruye mi casa.
(iii) Si mi compañía de seguros no me paga, entonces la inundación no destruye mi casa o el fuego no destruye mi casa.
(iv) Si mi compañía de seguros no me paga, entonces la inundación no destruye mi casa y el fuego no destruye mi casa.

14. Demuestre el teorema 1, parte 6.

15. Demuestre el teorema 1, parte 11.

16. Demuestre el teorema 2, parte (e).

17. Demuestre el teorema 4, parte (a).

18. Demuestre el teorema 4, parte (d).

19. Demuestre el teorema 4, parte (g).

20. Demuestre el teorema 4, parte (j).

2.3. Métodos de demostración

Algunos métodos de demostración que ya se ha utilizado son demostraciones directas resueltas por medio de elementos genéricos, definiciones y hechos demostrados con anterioridad, así como demostraciones por casos, como, por ejemplo, el examen de todas las situaciones posibles de valores de verdad en una tabla de verdad. A continuación se verá los métodos de demostración con mayor detalle.

Si una implicación $p \rightarrow q$ es una tautología, en donde p y q pueden ser proposiciones compuestas en las que intervenga cualquier número de variables propositivas, se dice que q **se desprende lógicamente** de p. Supóngase que una implicación de la forma

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

es una tautología. Entonces esta implicación es verdadera sin importar los valores de verdad

de cualquiera de sus componentes. En este caso, se dice que q **se desprende lógicamente** de $p_1, p_2, \ldots p_n$. Cuando q se desprende lógicamente de $p_1, p_2, \ldots p_n$, se escribe

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ \underline{p_n} \\ \therefore q \end{array}$$

en donde el símbolo $\therefore$ significa por lo tanto. Esto significa que si se sabe que p_1 es verdadera, p_2 es verdadera, ..., y p_n es verdadera, entonces se sabe que q es verdadera.

Prácticamente todos los teoremas matemáticos están compuestos por implicaciones del tipo

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q.$$

Las p_i son llamadas **hipótesis** o **premisas**, y q es llamada **conclusión**. "Demostrar el teorema" significa demostrar que la *implicación* es una tautología. Nótese que no se está tratando de demostrar que q (la conclusión) es verdadera, sino solamente que q será verdadera si todas las p_i son verdaderas. Por esta razón, las demostraciones matemáticas comienzan a menudo con la proposición "supóngase que $p_1, p_2, \ldots,$ y p_n son verdaderas" y concluyen con la proposición "por lo tanto, q es verdadera". La demostración no demuestra que q sea verdadera, sino simplemente demuestra que q tiene que ser verdadera si las p_i son todas verdaderas.

Los argumentos basados en tautologías representan métodos de razonamiento universalmente correctos. Su validez depende solamente de la forma de las proposiciones que intervienen y no de los valores de verdad de las variables que contienen. A estos argumentos se les llama **reglas de inferencia**. Los distintos pasos de la demostración matemática de un teorema deben desprenderse del uso de diversas reglas de inferencia, y la demostración matemática de un teorema debe comenzar con la hipótesis, proseguir con los distintos pasos, justificado cada uno por alguna regla de inferencia, y llegar a la conclusión.

Ejemplo 1. De acuerdo con el teorema 4(j), sección 2.2, $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ es una tautología. En consecuencia, el argumento

$$\begin{array}{l} p \rightarrow q \\ \underline{q \rightarrow r} \\ \therefore p \rightarrow r \end{array}$$

es universalmente válido, y por tanto es una regla de inferencia. ◆

Ejemplo 2. ¿Es válido el siguiente argumento?

Si invierte usted en el mercado de valores, entonces se hará rico.
Si se hace usted rico, entonces será feliz.

∴ Si usted invierte en el mercado de valores, entonces será feliz.

Solución: El argumento es de la forma dada en el ejemplo 1; por tanto, el argumento es válido aunque la conclusión pueda ser falsa. ◆

Ejemplo 3. La tautología $(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$ es el teorema 2(c), sección 2.2. En consecuencia, los siguientes argumentos son válidos.

$$\begin{array}{l} p \leftrightarrow q \\ \hline \therefore (p \to q) \wedge (q \to p) \end{array} \qquad \begin{array}{l} p \to q \\ q \to p \\ \hline \therefore p \leftrightarrow q. \end{array}$$

◆

Algunos teoremas matemáticos son equivalencias; es decir, son de la forma $p \leftrightarrow q$. Por lo general son enunciados p si y solamente si q. Por el ejemplo 3, la demostración de tal teorema es lógicamente equivalente a la demostración de ambas $p \to q$ y $q \to p$, y ésta es casi siempre la manera en que se demuestra las equivalencias. Primero se supone que p es verdadera, y se demuestra que q debe entonces ser verdadera; en seguida se supone que q es verdadera y se demuestra que p debe ser entonces verdadera.

Una regla de inferencia muy importante es

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q. \end{array}$$

Es decir, p es verdadera, y $p \to q$ es verdadera, de manera que q es verdadera. Esto se desprende del teorema 4(g), sección 2.2.

Los educadores clásicos dieron nombres latinos a algunas reglas de inferencia. El teorema 4(g) se menciona como el **modus ponens** o, en forma aproximada, el método de afirmación.

Ejemplo 4. ¿Es válido el siguiente argumento?

Fumar es saludable.
Si fumar es saludable, entonces los cigarrillos son recetados por los médicos.
∴ Los cigarrillos son recetados por los médicos.

Solución: El argumento es válido puesto que es de la forma *modus ponens*. Sin embargo, la conclusión es falsa. Observe que la primera premisa, p: fumar es saludable, es falsa. La segunda premisa, $p \to q$, entonces es verdadera y la conjunción de las dos premisas, $(p \wedge (p \to q))$, es falsa. ◆

Ejemplo 5. ¿Es válido el siguiente argumento?

Si bajan los impuestos, entonces se eleva el ingreso.
El ingreso se eleva.
∴ Los impuestos bajan.

Solución: Sean p: los impuestos bajan; y q: el ingreso se eleva. Entonces el argumento es de la forma

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore p. \end{array}$$

Supóngase que $p \to q$ y q son ambas verdaderas. Ahora $p \to q$ puede ser verdadera aun cuando p sea falsa. Entonces la conclusión p es falsa. Por tanto el argumento no es válido. Otro enfoque para responder a esta pregunta es verificar si la proposición

$((p \to q) \wedge q)$ implica lógicamente a la proposición p. Una tabla de verdad muestra que no es éste el caso. (Verifique.) ◆

Una importante técnica de demostración conocida como el **método indirecto** se desprende de la tautología $(p \to q) \leftrightarrow ((\sim q) \to (\sim p))$. Ésta establece, como se mencionó previamente, que una implicación es equivalente a su contrapositiva. Así, para demostrar $p \to q$ indirectamente, se supone que q es falsa (la proposición $\sim q$) y se demuestra que p es entonces falsa (la proposición $\sim p$).

Ejemplo 6. Sea n un entero. Demuestre que si n^2 es impar, entonces n es impar.

Solución: Sean p: n^2 es impar y q: n es impar. Se tiene que demostrar que $p \to q$ es verdadera. En vez de esto, se demuestra la contrapositiva, $\sim q \to \sim p$. Así, suponga que n no es impar, de manera que entonces es par. Entonces $n = 2k$, en donde k es un entero. Se tiene $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, de manera que n^2 es par. Se demuestra así que si n es par, entonces n^2 es par, la cual es la contrapositiva de la proposición dada. Por tanto, la proposición dada ha quedado demostrada. ◆

Otra técnica importante de demostración es la **demostración por contradicción**. Este método se basa en la tautología $((p \to q) \wedge (\sim q)) \to (\sim p)$. En consecuencia, la regla de inferencia

$$\begin{array}{l} p \to q \\ \sim q \\ \hline \therefore \;\sim p \end{array}$$

es válida. En términos simples, ésta establece que, si una proposición p implica una proposición falsa q, entonces p debe ser falsa. Ésta se aplica a menudo en caso de que q sea una falacia o contradicción, es decir, una proposición que siempre sea falsa. Se tiene un ejemplo al tomar a q como la contradicción $r \wedge (\sim r)$. En consecuencia, cualquier proposición que implique una contradicción debe ser falsa. Para poder usar la demostración por contradicción, supóngase que se desea demostrar que una proposición q se desprende lógicamente de las proposiciones $p_1, p_2, \ldots, p_n$. Suponga, como una hipótesis extra, que $\sim q$ es verdadera (es decir, que q es falsa) y que $p_1, p_2, \ldots, p_n$ son también verdaderas. Si esta hipótesis ampliada $p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge (\sim q)$ implica una contradicción, entonces por lo menos una de las proposiciones $p_1, p_2, \ldots, p_n, \sim q$ debe ser falsa. Esto significa que si todas las p_i son verdaderas, entonces $\sim q$ debe ser falsa; por tanto q debe ser verdadera. En consecuencia, q se desprende de $p_1, p_2, \ldots, p_n$. Ésta es la demostración por contradicción.

Ejemplo 7. Demuestre que no hay número racional alguno p/q cuyo cuadrado sea 2. En otras palabras, demuestre que $\sqrt{2}$ es irracional.

Solución: Esta proposición es una buena candidata para demostración por contradicción, porque no se podría verificar todos los posibles números racionales para demostrar que ninguno tiene un cuadrado de 2. Supóngase $(p/q)^2 = 2$ para algunos enteros p y q, que no tienen factores comunes. Si la elección original de p/q no está en sus términos más simples, se puede reemplazar con su forma equivalente de términos más simples. Entonces $p^2 = 2q^2$, por tanto p^2 es par. Esto implica que p es par, ya que el cuadrado de un número impar es impar. Entonces $p = 2n$ para algún entero n. Se ve que $2q^2 = p^2 = (2n)^2 = 4n^2$, de manera que $q^2 = 2n^2$. En consecuencia q^2 es par, y por tanto q es par. Se tiene ahora que ambas, p y q son pares y por tanto tienen un factor común de 2. Ésta es una contradicción a la suposición. En consecuencia, la suposición debe ser falsa. ◆

Se ha presentado varias reglas de inferencia y equivalencias lógicas que corresponden a técnicas de demostración válidas. Para demostrar un teorema de la forma (típica) $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$, se comienza con la hipótesis $p_1, p_2, \ldots, p_n$ y se demuestra que se desprende algún resultado r_1 lógicamente. Después, usando $p_1, p_2, \ldots, p_n, r_1$, se demuestra que se desprende lógicamente algúna otra proposición r_2. Se continúa este proceso, produciendo proposiciones intermedias $r_1, r_2, \ldots, r_k$, llamadas **pasos de la demostración**, hasta que se demuestre, por fin, que se desprende lógicamente la conclusión q de $p_1, p_2, \ldots, p_n, r_1, r_2, \ldots r_k$. Cada paso lógico debe ser justificado por alguna técnica de prueba válida basada sobre las reglas de inferencia que se han desarrollado, o sobre algunas otras reglas que provengan de implicaciones tautológicas que no hayan sido analizadas. En cualquier etapa, se puede reemplazar una proposición que necesite ser derivada por su proposición contrapositiva o cualquiera otra forma equivalente.

En la práctica, la construcción de demostraciones es un arte y debe aprenderse, en parte, de la observación y la experiencia. La elección de los pasos intermedios y métodos para derivarlos es una actividad creativa que no puede describirse con precisión.

Ejemplo 8. Sean m y n enteros. Demuestre que $n^2 = m^2$ si y solamente si $m = n$ o $m = -n$.

Solución: Se va a analizar la demostración como ha sido presentada. Supóngase que p es el predicado $n^2 = m^2$, q es el predicado $m = n$, y r es el predicado $m = -n$. Entonces se desea demostrar el teorema $p \leftrightarrow (q \vee r)$. Se sabe, por análisis previos, que en vez de hacer esto se puede demostrar que s: $p \rightarrow (q \vee r)$ y t:$(q \vee r) \rightarrow p$ son verdaderas. En consecuencia se supone que ya sea q: $m = n$ o r: $m = -n$ es verdadera. Si q es verdadera, entonces $m^2 = n^2$, y si r es verdadera, entonces $m^2 = (-n)^2 = n^2$, de modo que en cualquier caso p es verdadera. Se ha demostrado, por lo tanto, que la implicación t: $(q \vee r) \rightarrow p$ es verdadera.

Ahora se tiene que demostrar que s: $p \rightarrow (q \vee r)$ es verdadera; es decir, se supone p y se trata de demostrar ya sea q o r. Si p es verdadera, entonces $n^2 = m^2$, de modo que $m^2 - n^2 = 0$. Pero $m^2 - n^2 = (m - n)(m + n)$. Si r_1 es la proposición intermedia $(m - n)(m + n) = 0$, se ha demostrado que $p \rightarrow r_1$ es verdadera. Ahora se demuestra que $r_1 \rightarrow (q \vee r)$ es verdadera demostrando que la contrapositiva, $\sim(q \vee r) \rightarrow (\sim r_1)$ es verdadera. Ahora $\sim(q \vee r)$ es equivalente a $(\sim q) \wedge (\sim r)$, de modo que se demuestra que $(\sim q) \wedge (\sim r) \rightarrow (\sim r_1)$. En consecuencia, si $(\sim q)$: $m \neq n$ y $(\sim r)$: $m \neq -n$ son verdaderas; entonces $(m - n) \neq 0$ y $(m + n) \neq 0$, de manera que $(m - n)(m + n) \neq 0$ y r_1 es falsa. Se ha demostrado, por tanto, que $r_1 \rightarrow (q \vee r)$ es verdadera. Por último, de la verdad de $p \rightarrow r_1$ y $r_1 \rightarrow (q \vee r)$, puede concluirse que $p \rightarrow (q \vee r)$ es verdadera, y que el caso está terminado. ♦

Por lo general no se analiza las demostraciones en esta forma tan detallada. Se ha hecho únicamente para ilustrar que las demostraciones son pensadas uniendo, a manera de piezas, equivalencias y pasos válidos resultantes de reglas de inferencia. El detalle con que una demostración se realice depende del tipo de persona que se espera que la lea

Como observación final, se recuerda al lector que muchos teoremas matemáticos significan realmente que la proposición es verdadera para todos los objetos de un cierto tipo. Algunas veces esto no es evidente. Por tanto, el teorema del ejemplo 8 realmente establece que, para todos los enteros m y n, $m^2 = n^2$ si y sólo si $m = n$ o $m = -n$. De modo semejante, la proposición "Si x y y son números reales, y $x \neq y$, entonces $x < y$ o $y < x$" es una proposición acerca de todos los números reales x y y. Para demostrar un teorema de esta naturaleza, hay que asegurarse de que los pasos de la demostración sean válidos para todo número real. No podría suponerse, por ejemplo, que x sea 2 ni que y sea π ni $\sqrt{3}$. Esto explica por qué las demostraciones comienzan por seleccionar un elemento genérico, denotado por una variable. Por otra parte, se sabe, por la sección 2.2, que la negación de una proposición de la forma $\forall x$ P(x) es $\exists x \sim$P(x), por lo que se necesita solamente encontrar un solo ejemplo cuando la proposición es falsa.

Ejemplo 9. Demuestre o refute la proposición que expresa que si x y y son números reales, $(x^2 = y^2) \leftrightarrow (x = y)$.

Solución: La proposición puede expresarse de nuevo en la forma $\forall x\ \forall y$ R(x, y). En consecuencia, para demostrar este resultado, se necesitaría proporcionar pasos, cada uno de los cuales sería verdadera para todas las x y y. Para refutar este resultado, sólo se necesita encontrar un ejemplo para el cual la implicación sea falsa. Como $(-3)^2 = 3^2$, pero $-3 \neq 3$, el resultado es falso. A tal ejemplo se lo llama **contraejemplo**, y cualquier otro contraejemplo serviría para el caso. ♦

En resumen, si una proposición afirma que una propiedad es válida para todos los objetos de un cierto tipo, entonces, para demostrarlo, se debe seguir pasos que sean válidos para todos los objetos de ese tipo y que no hagan referencia a algún objeto en particular. Para refutar tal proposición, sólo se necesita demostrar un contraejemplo, es decir, un objeto o grupo de objetos en particular para el cual no sea válida la afirmación.

GRUPO DE EJERCICIOS 2.3

En los ejercicios 1 al 7, establezca si el argumento dado es válido o no. Si es válido, identifique la tautología o tautologías en que se basa.

1. Si voy en auto a mi trabajo, entonces llegaré cansado.
No estoy cansado cuando llego a mi trabajo.
∴ Yo no voy en auto a mi trabajo.

2. Si voy en auto a mi trabajo, entonces llegaré cansado.
Yo llego cansado a mi trabajo.
∴ Yo voy en auto a mi trabajo.

3. Si voy en auto a mi trabajo, entonces llegaré cansado.
Yo no voy en auto a mi trabajo.
∴ No llegaré cansado.

4. Si voy en auto a mi trabajo, entonces llegaré cansado.
Yo voy en auto a mi trabajo.
∴ Llegaré cansado.

5. Me volveré famoso o no me convertiré en escritor.
Me convertiré en escritor.
∴ Me volveré famoso.

6. Me volveré famoso o seré escritor.
No seré escritor.
∴ Me volveré famoso.

7. Si lo intento con ahínco y tengo talento, me convertiré en músico.
Si me convierto en músico, entonces seré feliz.
∴ Si no voy a ser feliz, entonces no intentaré con ahínco o no tengo talento.

8. (a) Demuestre que la suma de dos números pares es par.
(b) Demuestre que la suma de dos números impares es par.

9. (a) Demuestre que la estructura [enteros pares, +, *] es cerrada con respecto de *.
(b) Demuestre que la estructura [enteros impares, +, *] es cerrada con respecto de *

10. Demuestre que n^2 es par si y sólo si n es par.

11. Demuestre que $A = B$ si y sólo si $A \subseteq B$ y $B \subseteq A$.

12. Sean A y B subconjuntos de un conjunto universal U. Demuestre que $A \subseteq B$ si y solamente si $\overline{B} \subseteq \overline{A}$.

13. Demuestre que
(a) $A \subseteq B$ es una condición necesaria y suficiente para $A \cup B = B$.
(b) $A \subseteq B$ es una condición necesaria y suficiente para $A \cap B = A$.

14. Demuestre o refute: $n^2 + 41n + 41$ es un número primo para todo entero n.

15. Demuestre o refute: la suma de cinco enteros consecutivos cualesquiera es divisible entre 5.

16. Demuestre o refute: que $3 \mid (n^3 - n)$ para todo entero positivo n.

17. Demuestre o refute: $\forall x\, x^3 > x^2$.

18. Demuestre que la suma de dos números primos, cada uno mayor que 2, no es un número primo.

19. Demuestre que si dos renglones son cada un perpendicular con respecto de un tercer renglón contenido en el plano, entonces los dos renglones son paralelos.

20. Demuestre que si x es un número racional y y es un número irracional, entonces $x + y$ es un número irracional.

2.4. Inducción matemática

Se analizará aquí otra técnica de demostración. Supóngase que la proposición que se va a demostrar puede ponerse en la forma $\forall n \geq n_0\ P(n)$, en donde n_0 es algún entero fijo. Es decir, suponga que se desea demostrar que $P(n)$ es verdadera para todos los valores de $n \geq n_0$. El resultado siguiente muestra cómo puede hacerse esto. Supóngase que (a) $P(n_0)$ es verdadera y (b) si $P(k)$ es verdadera para algunos valores de $k \geq n_0$, entonces $P(k + 1)$ debe ser también verdadera. Entonces $P(n)$ es verdadera para todos los valores de $n \geq n_0$. A este resultado se le llama **principio de inducción matemática**. En consecuencia, para demostrar la verdad de una proposición $\forall n \geq n_0\ P(n)$ usando el principio de la inducción matemática, se debe comenzar por demostrar directamente que la primera proposición $P(n_0)$ es verdadera. A éste se lo conoce como **paso base** de la inducción y es, por lo general, muy fácil.

Luego se tiene que demostrar que $P(k) \rightarrow P(k + 1)$ es una tautología para cualquier selección de $k \geq n_0$. Como el único caso en que una implicación es falsa es si el antecedente es verdadero y el consecuente es falso, este paso suele hacerse demostrando que, si $P(k)$ fuera verdadera, entonces $P(k + 1)$ tendría que ser también verdadera. Nótese que esto no es lo mismo que suponer que $P(k)$ es verdadera para algún valor de k. A este paso se le llama **paso de inducción**, y por lo general se requiere algo de esfuerzo para demostrar que la implicación es siempre verdadera.

Ejemplo 1. Demuestre por inducción matemática, que para todos los valores de $n \geq 1$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Solución: Sea $P(n)$ el predicado $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$. En este ejemplo, $n_0 = 1$.

PASO BASE. Primero se debe demostrar que $P(1)$ es verdadera. $P(1)$ es la proposición $1 = \frac{1(1+1)}{2}$, la cual es claramente verdadera.

PASO DE INDUCCIÓN. Se debe demostrar ahora que para $k \geq 1$, si $P(k)$ es verdadera, entonces $P(k + 1)$ también debe ser verdadera. Se supone que para algún valor fijo $k \geq 1$,

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}. \tag{1}$$

Ahora se desea demostrar la verdad de $P(k + 1)$:

$$1 + 2 + 3 + \cdots + (k + 1) = \frac{(k+1)((k+1)+1)}{2}.$$

El primer miembro de $P(k + 1)$ puede escribirse como $1 + 2 + 3 + \cdots + k + (k + 1)$, y se tiene

$$\begin{aligned}
(1 + 2 + 3 + \cdots + k) + (k + 1) &= \frac{k(k+1)}{2} + (k + 1) && \text{Usando (1) para reemplaza a } 1 + 2 + \cdots + k\\
&= (k + 1)\left[\frac{k}{2} + 1\right] && \text{Factorizando}\\
&= \frac{(k+1)(k+2)}{2}\\
&= \frac{(k+1)((k+1)+1)}{2}. && \text{El segundo miembro de } P(k+1)
\end{aligned}$$

Se ha demostrado así que el primer miembro de $P(k + 1)$ es igual al segundo miembro de $P(k + 1)$. Por el principio de la inducción matemática, se sigue que $P(n)$ es verdadera para todos los valores de $n \geq 1$. ♦

Ejemplo 2. Sean $A_1, A_2, A_3, \ldots, A_n$ n conjuntos cualesquiera. Se demuestra por inducción matemática que

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}.$$

(Ésta es una versión extendida de una de las leyes de De Morgan.) Sea $P(n)$ el predicado que hace válido la igualdad para cualesquiera n conjuntos. Queda demostrado, por inducción matemática que, para todos los $n \geq 1$, $P(n)$ es verdadera.

PASO BASE. $P(1)$ es la proposición $\overline{A_1} = \overline{A_1}$, lo cual obviamente es verdadero.

PASO DE INDUCCIÓN. Si $P(k)$ es verdadera para cualesquiera k conjuntos, entonces el primer miembro de

$$\begin{aligned}
P(k+1) \text{ is } \overline{\left(\bigcup_{i=1}^{k+1} A_i\right)} &= \overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}}\\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}} && \text{Propiedad asociativa de } \cup\\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k)} \cap \overline{A_{k+1}} && \text{Ley de De Morgan para dos conjuntos}
\end{aligned}$$

$$= \left(\bigcap_{i=1}^{k} \overline{A_i}\right) \cap \overline{A_{k+1}} \qquad \text{Usando P}(k)$$

$$= \bigcap_{i=1}^{k+1} \overline{A_i}.$$

En consecuencia, la implicación $P(k) \to P(k+1)$ es una tautología, y por el principio de inducción matemática, $P(n)$ es verdadera para todas las $n \geq 1$. ♦

Ejemplo 3. Se demuestra por inducción matemática que cualquier conjunto finito no vacío es numerable; es decir, que puede disponerse en forma de lista.

Sea $P(n)$ el predicado que indica que si A es un conjunto cualquiera con $|A| = n \geq 1$, entonces A es numerable. (Véase el capítulo 1 para definiciones.)

PASO BASE. Aquí n_0 es 1, de manera que se considera que A sea cualquier conjunto de un elemento, por ejemplo $A = \{x\}$. En este caso x forma una secuencia por sí misma cuyo conjunto es A, por lo cual $P(1)$ es verdadera.

PASO DE INDUCCIÓN. Se quiere usar la proposición de que si A es un conjunto cualquiera con k elementos, entonces A es numerable. Escoja ahora cualquier conjunto B con $k + 1$ elementos y tome cualquier elemento x en B. Como $B - \{x\}$ es un conjunto con k elementos, la hipótesis de inducción $P(k)$ dice que hay una secuencia $x_1, x_2, \ldots, x_k$ con $B - \{x\}$ como su conjunto correspondiente. La secuencia $x_1, x_2, \ldots, x_k, x$ tiene entonces a B como conjunto correspondiente, por lo que B es numerable. Como B puede ser cualquier conjunto con $k+1$ elementos, $P(k + 1)$ es verdadera si $P(k)$ lo es. En consecuencia, por el principio de la inducción matemática, $P(n)$ es verdadera para todos los valores de $n \geq 1$. ♦

Al demostrar resultados por inducción, no debe comenzarse por suponer que $P(k+1)$ es verdadera e intentar manipular este resultado hasta que llegue a una proposición verdadera. Éste es un uso incorrecto del principio de la inducción matemática, es una equivocación común.

Existe una conexión natural entre recursión e inducción, porque los objetos que son definidos recursivamente utilizan a menudo una secuencia natural en su definición. La inducción es con frecuencia el mejor camino, tal vez el único, para demostrar resultados acerca de objetos definidos recursivamente.

Ejemplo 4. Considérese la definición siguiente de la función factorial: $1! = 1$, $n! = n(n-1)!$, $n > 1$. Supóngase que se desea demostrar para todos los valores de $n \geq 1$, $n! \geq 2^{n-1}$. Se procederá por inducción matemática. Sea $P(n)$: $n! \geq 2^{n-1}$. Aquí n_0 es 1.

PASO BASE. $P(1)$ es la proposición $1! \geq 2^0$. Como $1!$ es 1, esta proposición es verdadera.

PASO DE INDUCCIÓN. Se quiere demostrar que $P(k) \to P(k+1)$ es una tautología. Será una tautología si $P(k)$ verdadera garantiza que $P(k+1)$ es verdadera. Supóngase que $k! \geq 2^{k-1}$ para $k \geq 1$. Entonces, por la definición recursiva, el primer miembro de $P(k+1)$ es

$$\begin{aligned}(k+1)! &= (k+1)k! && \\ &\geq (k+1)2^{k-1} && \text{Usando P}(k) \\ &\geq 2 \times 2^{k-1} && k+1 \geq 2, \text{ ya que } k \geq 1 \\ &= 2^k. && \text{Segundo miembro de P}(k+1)\end{aligned}$$

En consecuencia $P(k + 1)$ es verdadera. Por el principio de la inducción matemática, se concluye que $P(n)$ es verdadera para todos los valores de $n \geq 1$. ♦

El ejemplo siguiente muestra una manera en la cual puede ser útil la inducción en la programación de computadoras. El seudocódigo que se emplea en éste y en los ejemplos siguientes se describe en el apéndice A.

Ejemplo 5. Considérese la siguiente función dada en seudocódigo.

```
FUNCTION CUAD(A)
1. C ← 0
2. D ← 0
3. WHILE(D ≠ A)
   a. C ← C + A
   b. D ← D + 1
4. RETURN(C)
FIN DE LA FUNCIÓN CUAD.
```

El nombre de la función, CUAD, sugiere que calcula el cuadrado de A. El paso 3b muestra que A debe ser un entero positivo para que el ciclo termine. Unos cuantos tanteos con valores particulares de A proporcionarán evidencia de que la función sí efectúa esta tarea. Sin embargo, supóngase que ahora se quiere demostrar que CUAD siempre calcula el cuadrado del entero positivo A, sin importar qué tan grande pueda ser A. Se dará una demostración por inducción matemática. Para cada entero $n \geq 0$, sean C_n y D_n los valores de las variables C y D, respectivamente, después de pasar por el ciclo **WHILE** n veces. En particular, C_0 y D_0 representan los valores de las variables antes de iniciarse el ciclo. Sea $P(n)$ el predicado $C_n = A \times D_n$. Se demostrará por inducción que $\forall n \geq 0$ $P(n)$ es verdadera. Aquí n_0 es 0.

PASO BASE. $P(0)$ es la proposición $C_0 = A \times D_0$, la cual es verdadera, ya que el valor de ambas, C y D es cero "después" de que el cero pasa por el ciclo **WHILE**.

PASO DE INDUCCIÓN. Se debe usar ahora

$$P(k)\colon C_k = A \times D_k \tag{2}$$

para demostrar que $P(k+1)$: $C_{k+1} = A \times D_{k+1}$. Después de pasar por el ciclo, C se incrementa por A, y D se incrementa por 1, de manera que $C_{k+1} = C_k + A$ y $D_{k+1} = D_k + 1$.

$$\begin{aligned}\text{primer miembro de P}(k+1)\colon \quad C_{k+1} &= C_k + A && \\ &= A \times D_k + A && \text{Usando (2) para reemplazar } C_k \\ &= A \times (D_k + 1) && \text{Factorizando} \\ &= A \times D_{k+1}. && \text{Segundo miembro de P}(k+1)\end{aligned}$$

Por el principio de la inducción matemática, se desprende que mientras ocurra el ciclo $C_n = A \times D_n$. El ciclo debe terminar. (¿Por qué?) Cuando termina el ciclo o lazo, $D = A$, de manera que $C = A \times A$, o sea A^2, y éste es el valor regresado por la función CUAD. ♦

El ejemplo 5 ilustra el uso de una **invariante de ciclo o de bucle**, una relación entre variables que persiste a través de todas las iteraciones del ciclo. Esta técnica para demostrar que los ciclos y programas hacen lo que se afirma que hacen es una parte importante de la teoría de la verificación de algoritmos. En el ejemplo 5, es claro que el ciclo termina si A es un entero positivo, pero para casos más complejos, esto puede demostrarse también por inducción.

Ejemplo 6. Utilice la técnica del ejemplo 5 para demostrar que el programa en seudocódigo que se da en la sección 1.4 calcula el máximo común divisor de dos enteros positivos.

Solución: Véase el seudocódigo que se dio con anterioridad.

FUNCTION GCD(X, Y)
1. **WHILE** ($X \neq Y$)
    a. **IF** ($X > Y$) **THEN**
        1. $X \leftarrow X - Y$
    b. **ELSE**
        1. $Y \leftarrow Y - X$
2. **RETURN** (X)

FIN DE LA FUNCIÓN MCD

Se afirma que si X y Y son enteros positivos, entonces MCD regresa el MCD (X, Y). Para demostrar esto, sean X_n y Y_n los valores de X y Y después de que $n \geq 0$ pasa por el lazo **WHILE**. Se afirma que P(n): MCD(X_n, Y_n) = MCD (X, Y) es verdadera para todos los valores de $n \geq 0$, y se demuestra esto por inducción matemática. Aquí n_0 es 0.

PASO BASE. $X_0 = X$, $Y_0 = Y$, ya que éstos son los valores de las variables antes de que comience el ciclo; en consecuencia P(0) es la proposición MCD(X_0, Y_0) = MCD(X, Y), la cual es verdadera.

PASO DE INDUCCIÓN. Considere ahora el primer miembro de P(k + 1), es decir, MCD(X_{k+1}, Y_{k+1}). Después de que $k + 1$ pasa por el ciclo, ya sea $X_{k+1} = X_k$ y $Y_{k+1} = Y_k - X_k$ o $X_{k+1} = X_k - Y_k$ y $Y_{k+1} = Y_k$. Entonces, si P(k): MCD(X_k, Y_k) = MCD(X, Y) es verdadera, se tiene por el teorema 5, sección 1.4, que MCD(X_{k+1}, Y_{k+1}) = MCD(X_k, Y_k) = MCD(X, Y). En consecuencia, por el principio de la inducción matemática, P(n) es verdadera para todos los valores de $n \geq 0$. La condición de salida para el ciclo es $X_n = Y_n$, y se tiene MCD(X_n, Y_n) = X_n. Por tanto, la función siempre regresa el valor del MCD(X, Y). ♦

GRUPO DE EJERCICIOS 2.4

En los ejercicios 1 *al* 12, *demuestre que la proposición es verdadera por medio de inducción matemática.*

1. $2 + 4 + 6 + \cdots + 2n = n(n + 1)$

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

3. $1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

4. $5 + 10 + 15 + \cdots + 5n = \dfrac{5n(n + 1)}{2}$

5. $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}$

6. $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n + 1)^2}{4}$

7. $1 + 5 + 9 + \cdots + (4n - 3) = n(2n - 1)$

8. $1 + a + a^2 + \cdots + a^{n-1} = \dfrac{a^n - 1}{a - 1}$

9. $a + ar + ar^2 + \cdots + ar^{n-1} = \dfrac{a(1 - r^n)}{1 - r}$, para $r \neq 1$

10. $1 + 2^n < 3^n$, para $n \geq 2$

11. $n < 2^n$, para $n > 1$

12. $1 + 2 + 3 + \cdots + n < \dfrac{(2n + 1)^2}{8}$

13. Demuestre por inducción matemática, que si un conjunto A tiene n elementos, entonces P(A) tiene 2^n elementos.

14. Demuestre por inducción matemática, que $3 \mid (n^3 - n)$ para todo entero positivo n.

15. Demuestre por inducción matemática, que si $A_1, A_2, \ldots, A_n$ son n conjuntos cualesquiera, entonces

$$\overline{\left(\bigcap_{i=1}^{n} A_i\right)} = \bigcup_{i=1}^{n} \overline{A_i}.$$

16. Demuestre por inducción matemática, que si $A_1, A_2, \ldots, A_n$ y B son $n + 1$ conjuntos cualesquiera, entonces

$$\left(\bigcup_{i=1}^{n} A_i\right) \cap B = \bigcup_{i=1}^{n} (A_i \cap B).$$

17. Demuestre por inducción matemática, que si $A_1, A_2, \ldots, A_n$ y B son n conjuntos cualesquiera, entonces

$$\left(\bigcap_{i=1}^{n} A_i\right) \cup B = \bigcap_{i=1}^{n} (A_i \cup B).$$

18. Sea P(n) la proposición $2 \mid (2n - 1)$.
(a) Demuestre que P(k) $\rightarrow$ P($k + 1$) es una tautología.
(b) Demuestre que no existe entero n para el cual P(n) sea verdadera.
(c) ¿Contradicen los resultados de las partes (a) y (b) el principio de la inducción matemática? Explique.

En los ejercicios 19 *al* 23, *demuestre la proposición dada acerca de las matrices.*

19. $(\mathbf{A}_1 + \mathbf{A}_2 + \cdots + \mathbf{A}_n)^T = \mathbf{A}_1^T + \mathbf{A}_2^T + \cdots + \mathbf{A}_n^T$

20. $(\mathbf{A}_1\mathbf{A}_2 \cdots \mathbf{A}_n)^T = \mathbf{A}_n^T \mathbf{A}_{n-1}^T \cdots \mathbf{A}_2^T\mathbf{A}_1^T$

21. $\mathbf{A}^2\mathbf{A}^n = \mathbf{A}^{2+n}$

22. $(\mathbf{A}^2)^n = \mathbf{A}^{2n}$

23. Sean **A** y **B** matrices cuadradas. Si **AB** = **BA**, entonces $(\mathbf{AB})^n = \mathbf{A}^n\mathbf{B}^n$, para $n \geq 1$.

24. Utilice inducción para demostrar que si p es un número primo y $p \mid a^n$ para $n \geq 1$, entonces $p \mid a$.

25. Demuestre que si MCD(a, b) = 1, entonces MCD (a^n, b^n) = 1 para todos los valores de $n \geq 1$. (*Sugerencia:* Utilice el ejercicio 24.)

26. (a) Encuentre el entero positivo más pequeño n_0 tal que $2^{n_0} > n_0^2$.
(b) Demuestre que $2^n > n^2$ para todos los valores de $n \geq n_0$.

En los ejercicios 27 *al* 30, *demuestre que el algoritmo dado, usado correctamente, produce el resultado establecido utilizando inducción matemática para demostrar que la relación indicada es una invariante de rizo y verificando los valores cuando deja de producirse el enlazamiento. Todas las variables representan enteros no negativos.*

27. **SUBROUTINE** COMP(X, Y; Z)
1. $Z \leftarrow X$
2. $W \leftarrow Y$
3. **WHILE** ($W > 0$)
    a. $Z \leftarrow Z + Y$
    b. $W \leftarrow W - 1$
4. **RETURN**

FIN DE LA SUBRUTINA COMP
CALCULA: $Z = X + Y^2$
INVARIANTE DE CICLO: $(Y \times W) + Z = X + Y^2$

28. SUBROUTINE DIFF $(X, Y; Z)$
1. $Z \leftarrow X$
2. $W \leftarrow Y$
3. **WHILE** $(W > 0)$
   a. $Z \leftarrow Z - 1$
   b. $W \leftarrow W - 1$
4. **RETURN**

FIN DE LA SUBRUTINA DIFF
CALCULA: $Z = X - Y$
INVARIANTE DE CICLO: $X - Z + W = Y$

29. SUBROUTINE EXP2$(N, M; R)$
1. $R \leftarrow 1$
2. $K \leftarrow 2M$
3. **WHILE** $(K > 0)$
   a. $R \leftarrow R \times N$
   b. $K \leftarrow K - 1$
4. **RETURN**

FIN DE LA SUBRUTINA EXP2
CALCULA: $R = N^{2M}$
INVARIANTE DE CICLO: $R \times N^K = N^{2M}$

30. SUBROUTINE POWER$(X, Y; Z)$
1. $Z \leftarrow 0$
2. $W \leftarrow Y$
3. **WHILE** $(W > 0)$
   a. $Z \leftarrow Z + X$
   b. $W \leftarrow W - 1$
4. $W \leftarrow Y - 1$
5. $U \leftarrow Z$
6. **WHILE** $(W > 0)$
   a. $Z \leftarrow Z + U$
   b. $W \leftarrow W - 1$
4. **RETURN**

FIN DE LA SUBRUTINA POWER
CALCULA: $Z = X \times Y^2$
INVARIANTE DE CICLO (primer ciclo):
$Z + (X \times W) = X \times Y$
INVARIANTE DE CICLO (segundo ciclo):
$Z + (X \times Y \times W) = X + Y^2$

(*Sugerencia:* Utilice el valor de Z al final del primer ciclo y utilice el que se tiene en el ciclo 2.)

IDEAS CLAVE PARA REPASO

- Proposición o enunciado: Oración declarativa que es verdadera o falsa, pero no ambas.
- Variable propositiva: Letra que denota una proposición.
- Proposición compuesta: proposición que se obtiene combinando dos o más proposiciones por medio de un conectivo lógico.
- Conectivos lógicos: "no" ($\sim$), "y" ($\wedge$), "o" ($\vee$), si entonces ($\rightarrow$), si y solamente si ($\leftrightarrow$)
- Conjunción: $p \wedge q$ (p y q).
- Disyunción: $p \vee q$ (p o q).
- Predicado (función propositiva): una oración de la forma P(x).
- Cuantificación universal: $\forall x$ P(x) [Para todos los valores de x, P(x) es verdadera.]
- Cuantificación existencial: $\exists x$ P(x) [Existe una x tal que P(x) es verdadera.]
- Proposición condicional o implicación: $p \rightarrow q$ (si p entonces q); p es el antecedente o hipótesis y q es la consecuente o conclusión.
- Recíproca de $p \rightarrow q$: $q \rightarrow p$.
- Contrapositiva de $p \rightarrow q$: $\sim q \rightarrow \sim p$.
- Equivalencia: $p \leftrightarrow q$.
- Tautología: una proposición que es verdadera para todos los valores posibles de sus variables propositivas.
- Falacia: una proposición que es falsa para todos los valores posibles de sus variables propositivas.
- Contingencia: una proposición que puede ser verdadera a falsa, dependiendo de los valores de verdad de sus variables propositivas.
- Proposiciones lógicamente equivalentes p y q: $p \equiv q$
- Métodos de demostración:
  q se desprende lógicamente de p: véase la página 58.
  Reglas de inferencia: véase la página 59.
  Modus ponens: véase la página 60.
  Método indirecto: véase la página 61.
  Demostración por contradicción: véase la página 61.
- Contraejemplo: caso que refuta un teorema o proposición.
- Principio de inducción matemática: Sea n_0 un entero fijo. Supóngase que para cada entero $n \geq n_0$ se tiene una proposición P(n). Supóngase que (a) P(n_0) es verdadera y (b) si P(k) entonces P($k + 1$) es una tautología para cada valor de $k \geq n_0$. Entonces el principio de la inducción matemática establece que P(n) es verdadera para todos los valores de $n \geq n_0$.
- Invariante de ciclo: una proposición que es verdadera antes y después de cada pasada por un ciclo o bucle de programación.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes, escriba el programa o subrutina que se solicita, en seudocódigo (como se describe en el apéndice A) o en un lenguaje de programación que usted conozca. Pruebe su código ya sea usando papel y lápiz, o ejecutándolo en una computadora.

1. Escriba un programa que imprima una tabla de verdad para $p \wedge \sim q$.

2. Escriba un programa que imprima una tabla de verdad para $(p \vee q) \rightarrow r$.

3. Escriba un programa que imprima una tabla de verdad para cualquier función propositiva de dos variables.

4. Escriba una subrutina EQUIVALENTE que determine si dos expresiones lógicas son equivalentes.

5. Escriba una subrutina que determine si una expresión lógica es una tautología, una contingencia o una falacia.

CAPÍTULO 3

CONTEO

Requisito previo: Capítulo 1

Las técnicas de conteo son importantes en matemáticas y en las ciencias de la computación, particularmente en el análisis de algoritmos. En la sección 1.2, se introdujo el principio de adición. En este capítulo se presenta otras técnicas de conteo, en forma particular las que se emplea para las permutaciones y combinaciones, y se considera dos aplicaciones de conteo, el principio de casillas y la probabilidad. Además, se analiza relaciones de recurrencia, otra herramienta para el análisis de programas de computadora.

3.1. Permutaciones

Se iniciará este tema con un resultado simple, pero general, que se utilizará con frecuencia en esta sección y en muchos otros temas.

Teorema 1. *Supóngase que va a efectuarse dos trabajos, T_1 y T_2, en secuencia. Si T_1 puede realizarse de n_1 maneras, y para cada una de estas maneras T_2 puede llevarse a cabo de n_2 maneras, entonces la secuencia T_1T_2 puede efectuarse en n_1n_2 maneras.*

Demostración: Cada elección de método para realizar T_1 dará lugar a una manera diferente de efectuar la secuencia de trabajos. Existen n_1 de estos métodos, y para cada uno de ellos puede elegirse n_2 maneras de llevar a cabo T_2. Así, en total, habrá n_1n_2 maneras de efectuar la sucesión T_1T_2. Véase la figura 3.1 en caso de que n_1 sea 3 y n_2 sea 4. ●

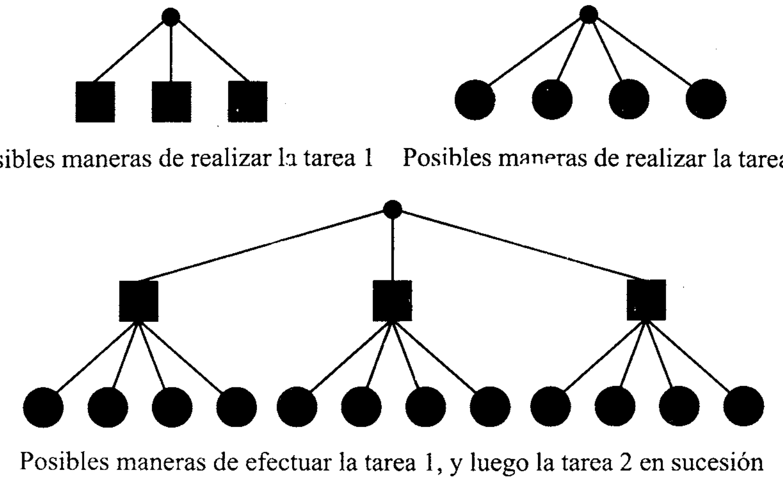


Figura 3.1

En ocasiones, el teorema 1 es llamado **principio de multiplicación del conteo**. (Se sugiere compararlo cuidadosamente con el principio de adición del conteo de la sección 1.2.) Es fácil extender el alcance del principio de multiplicación, como sigue:

Teorema 2. *Supóngase que se va a efectuar, en sucesión, los trabajos $T_1, T_2, \ldots, T_k$. Si T_1 puede realizarse de n_1 maneras, y para cada una de estas maneras T_2 puede hacerse de n_2 maneras, y para cada una de estas n_1n_2 maneras de realizar T_1T_2 en sucesión, T_3 puede llevarse a cabo de n_3 maneras, y así sucesivamente, entonces la secuencia $T_1T_2 \cdots T_k$ puede efectuarse de exactamente $n_1n_2 \cdots n_k$* maneras.

Demostración: Este resultado puede demostrarse por medio del principio de inducción matemática sobre k. ●

Ejemplo 1. Un identificador de etiqueta para un programa de computadora, consta de una letra seguida por tres dígitos. Si se permite repeticiones ¿cuántos identificadores distintos de etiqueta será posible tener?

Solución: Hay 26 posibilidades para la letra inicial y 10 posibilidades para cada uno de los tres dígitos. En consecuencia, por el principio extendido de la multiplicación, hay 26 × 10 × 10 × 10, o sea, 26 ,000 identificadores posibles de etiqueta. ◆

Ejemplo 2. Sea A un conjunto con n elementos. ¿Cuántos subconjuntos tiene A?

Solución: Se sabe, por la sección 1.3, que cada subconjunto de A está determinado por su función característica, y si A tiene n elementos, esta función puede describirse como un arreglo de ceros y unos, de longitud n. El primer elemento del arreglo puede llenarse de dos maneras (con un 0 o con un 1), y esto es igualmente cierto para todos los elementos subsecuentes. En consecuencia, por el principio extendido de la multiplicación, hay

$$\underbrace{2 \cdot 2 \cdots 2}_{n \text{ factores}} = 2^n$$

maneras de formar el arreglo, y por lo tanto 2^n subconjuntos de A. ◆

Diríjase la atención al siguiente problema de conteo. Sea A cualquier conjunto de n elementos, y supóngase que $1 \leq r \leq n$.

Problema 1. ¿Cuántas secuencias diferentes, cada una de longitud r, puede formarse utilizando elementos de A si

(a) ¿pueden repetirse elementos en la secuencia?
(b) ¿todos los elementos en la secuencia deben ser distintos?

Se observa en primera instancia, que puede formarse cualquier secuencia de longitud r llenando r casillas en orden de izquierda a derecha con elementos de A. En el caso (a) puede usarse copias de los elementos de A.

			...		
Casilla 1	Casilla 2	Casilla 3		Casilla $r - 1$	Casilla r

Sean T_1 el trabajo "llenar casilla 1", T_2 el trabajo "llenar casilla 2", y así sucesivamente. Entonces el trabajo combinado $T_1 T_2 \cdots T_r$ representa la formación de la secuencia.

Caso (a). T_1 puede efectuarse de n maneras, ya que puede copiarse cualquier elemento de A para la primera posición de la secuencia. Lo mismo ocurre para cada uno de los trabajos $T_2, T_3, \ldots, T_r$. Entonces, por el principio extendido de la multiplicación, el número de secuencias que puede formarse es

$$\underbrace{n \bullet n \bullet \cdots \bullet n}_{r \text{ factores}} = n^r.$$

Se ha comprobado, por tanto, el resultado siguiente.

Teorema 3. *Sea A un conjunto de n elementos y $1 \leq r \leq n$. Entonces, el número de secuencias de longitud r que puede formarse con elementos de A, permitiendo repeticiones, es n^r.* ●

Ejemplo 3. ¿Cuántas "palabras" de tres letras puede formarse a partir de letras del conjunto $\{a, b, y, z\}$ si se permite repetir letras?

Solución: En este caso n es 4 y r es 3, de manera que el número de tales palabras es 4^3, es decir, 64, por el teorema 3. ◆

Considérese ahora el caso (b) del problema 1. En este caso también T_1 puede efectuarse de n maneras, en vista de que puede escogerse cualquier elemento de A para la primera posición. Cualquiera que sea el elemento que se escoja, sólo quedan $(n - 1)$ elementos, de

manera que T_2 puede realizarse de $(n - 1)$ maneras, y así sucesivamente, hasta que finalmente T_r puede efectuarse de $(n - (r - 1))$, o $(n - r + 1)$ maneras. En consecuencia, por el principio extendido de la multiplicación, una secuencia de r elementos distintos tomados de A puede formarse de $n(n - 1)(n - 2) \cdots (n - r + 1)$ maneras.

A una secuencia de r elementos distintos de A suele llamársela permutación de A tomados r a la vez. Esta terminología es normal o estándar, y por ello se está adoptando, aunque sea confusa. Una mejor terminología podría ser una "permutación de r elementos escogidos de A". Muchas secuencias de interés son permutaciones de algún conjunto de n objetos, tomados r a la vez. El análisis anterior muestra que el número de tales secuencias depende sólo de n y r, y no de A. Este número se escribe a menudo ${}_nP_r$ y se denomina **número de permutaciones de *n* objetos tomados *r* a la vez**. Así se acaba de demostrar el resultado siguiente.

Teorema 4. *Si $1 \leq r \leq n$, entonces ${}_nP_r$, el número de permutaciones de n objetos tomados r a la vez, es $n \cdot (n - 1) \cdot (n - 2) \cdot \cdots \cdot (n - r + 1)$.* ●

Ejemplo 4. Sea A el conjunto $\{1, 2, 3, 4\}$. Entonces las secuencias 124, 421, 341 y 243 son algunas permutaciones de A tomando 3 elementos a la vez. Las secuencias 12, 43, 31, 24 y 21 son ejemplos de diferentes permutaciones de A, tomando dos elementos a la vez. Por el teorema 4, el número total de permutaciones de A, tomando tres elementos a la vez es ${}_4P_3$, o sea, $4 \cdot 3 \cdot 2$, o 24. El número total de permutaciones de A tomados dos a la vez, es ${}_4P_2$, o sea $4 \cdot 3$, o 12. ◆

Cuando $r = n$, se está contando los distintos arreglos de los elementos de A, con $|A| = n$, en secuencias de longitud n. Una secuencia de esta naturaleza se llama **permutación** de A. (En el capítulo 5 se emplea el término *permutación* en forma ligeramente diferente para aumentar su utilidad.) El número de permutaciones de A es así ${}_nP_n$ o sea, $n \cdot (n - 1) \cdot (n - 2) \cdot \cdots \cdot 2 \cdot 1$, si $n \geq 1$. Este número también se escribe en la forma $n!$ y se lee ***n* factorial**. Ambas, ${}_nP_r$ y $n!$ son funciones integradas en muchas calculadoras.

Ejemplo 5. Sea A el conjunto $\{a, b, c\}$. Entonces, las permutaciones posibles de A son las secuencias *abc, acb, bac, bca, cab* y *cba*. ◆

Si se conviene en definir 0! igual a 1, entonces para cada $n \geq 0$ se ve que el número de permutaciones de n objetos es $n!$. Si $n \geq 0$ y $1 \leq r \leq n$, se puede dar ahora una forma más compacta para ${}_nP_r$ como sigue.

$$\begin{aligned} {}_nP_r &= n \cdot (n - 1) \cdot (n - 2) \cdots (n - r + 1) \\ &= \frac{n \cdot (n - 1) \cdots (n - r + 1) \cdot (n - r) \cdot (n - r - 1) \cdots 2 \cdot 1}{(n - r) \cdot (n - r - 1) \cdots 2 \cdot 1} \\ &= \frac{n!}{(n - r)!}. \end{aligned}$$

Ejemplo 6. Supóngase que A es un conjunto formado por las 52 cartas de una baraja ordinaria de juego. Supóngase además que se baraja todas las cartas y que se toma una mano de cinco cartas. Una lista de las cartas de esta mano, en el orden en que fueron tomadas, es una permutación de A, tomada en cinco elementos a la vez. Algunos ejemplos serían AC, 3D, 5T, 2C, JE; 2C, 3C, 5C, QC, KD; JC, JD, JE, 4C, 4C; y 3D, 2C, AC, JE, 5C. Nótese que las manos primera y última son las mismas, pero representan diferentes permutaciones, en vista de que fueron tomadas en un orden diferente. El número de permutaciones de A, tomando cinco a la vez es ${}_{52}P_5 = \frac{52!}{47!}$ o $52 \cdot 51 \cdot 50 \cdot 49 \cdot 48$ o 311,875,200. Éste es el número de manos de cinco cartas que se puede sacar si se considera el orden en que fueron tomadas. ◆

Ejemplo 7. Si A es el conjunto en el ejemplo 5, entonces n es 3, y el número de permutaciones de A es 3! o 6. En consecuencia, todas las permutaciones de A están enlistadas en el ejemplo 5, como se afirmó. ◆

Ejemplo 8. ¿Cuántas "palabras" de tres letras distintas puede formarse con las letras de la palabra MAST?

Solución: El número es ${}_4P_3 = \frac{4!}{(4-3)!}$ o $\frac{4!}{1!}$ o 24. ◆

En el ejemplo 8, si la palabra hubiera sido MASS, ${}_4P_3$ contaría como distintas algunas permutaciones que no pueden distinguirse. Por ejemplo, si se marca las dos S como S_1 y S_2, entonces S_1AS_2 y S_2AS_1 son 2 de las 24 permutaciones contadas; pero sin marca, éstas son la misma "palabra". Hay un caso más por considerar, las permutaciones con repeticiones limitadas.

Ejemplo 9. ¿Cuántas permutaciones distintas puede hacerse con las letras de la palabra BANANA?

Solución: Se comienza por rotular las A y las N para poder distinguirlas temporalmente. Para las letras B, A_1, N_1, A_2, N_2, A_3, hay 6!, o sea 120 permutaciones. Algunas de estas permutaciones son idénticas, excepto por el orden en que aparecen las N, por ejemplo, $A_1A_2A_3BN_1N_2$ y $A_1A_2A_3BN_2N_1$. De hecho, puede enlistarse las 120 permutaciones en pares cuyos miembros difieran solamente en el orden de las dos N. Esto significa que si se suprime los rótulos de las N, sólo quedan $\frac{120}{2}$, es decir, 60 permutaciones distinguibles. Razonando de manera similar, se ve que éstas pueden ser agrupadas en conjuntos de 3!, o sea de 6, que difieran solamente por el orden de las tres A. Por ejemplo, un conjunto de 6 consta de $BNNA_1A_2A_3$, $BNNA_1A_3A_2$, $BNNA_2A_1A_3$, $BNNA_2A_3A_1$, $BNNA_3A_1A_2$ y $BNNA_3A_2A_1$. Suprimiendo las etiquetas se convertirían estas 6 en la permutación única BNNAAA. En consecuencia, hay $\frac{60}{6}$, o sea 10 permutaciones distinguibles de las letras BANANA. ◆

El siguiente teorema describe la situación general para permutaciones con repeticiones limitadas.

Teorema 5. *El número de permutaciones distinguibles que puede formarse a partir de una colección de* n *objetos, en la que el primer objeto aparece k_1 veces, el segundo objeto k_2 veces, y así sucesivamente, es*

$$\frac{n!}{k_1!k_2!\cdots k_t!}.$$ ●

Ejemplo 10. El número de "palabras" distinguibles que puede formarse con las letras de MISSISSIPPI es $\frac{11!}{1!4!4!2!}$, es decir, 34 650. ◆

GRUPO DE EJERCICIOS 3.1

1. Una clave de admisión de un banco consta de dos letras del alfabeto seguidas por dos dígitos. ¿Cuántas claves diferentes hay?

2. En un experimento psicológico, una persona debe acomodar en hilera un cuadrado, un cubo, un círculo, un triángulo y un pentágono. ¿Cuántos acomodos diferentes son posibles?

3. Se lanza al aire una moneda cuatro veces y se registra el resultado de cada lanzamiento. ¿Cuántas secuencias diferentes de cara y cruz son posibles?

4. Un menú de opciones incluye una sopa, un platillo fuerte, un postre y una bebida. Suponga que un cliente puede hacer su elección entre cuatro sopas, cinco platillos fuertes, tres postres y dos bebidas. ¿Cuántos menús diferentes puede seleccionarse?

5. Un dado legal de seis caras es lanzado cuatro veces, y se anota los números obtenidos en una secuencia. ¿Cuántas secuencias diferentes hay?

6. Calcule cada uno de los siguientes casos.
   (a) ${}_4P_4$ (b) ${}_6P_5$ (c) ${}_7P_2$
   (d) ${}_nP_{n-1}$ (e) ${}_nP_{n-2}$ (f) ${}_{n+1}P_{n-1}$

7. ¿Cuántas permutaciones hay de cada uno de los siguientes conjuntos?
   (a) $\{r, s, t, u\}$
   (b) $\{1, 2, 3, 4, 5\}$
   (c) $\{a, b, 1, 2, 3, c\}$

8. Para cada conjunto A, encuentre el número de permutaciones de A tomando los elementos r a la vez.
   (a) $A = \{1, 2, 3, 4, 5, 6, 7\}$, $r = 3$
   (b) $A = \{a, b, c, d, e, f\}$, $r = 2$
   (c) $A = \{x \mid x$ es un entero y $x^2 < 16\}$, $r = 4$

9. ¿De cuántas maneras pueden seis hombres y seis mujeres sentarse en línea si
   (a) cualquier persona puede sentarse en seguida de cualquier otra?
   (b) los hombres y las mujeres deben ocupar asientos alternados?

10. Encuentre el número de permutaciones diferentes de las letras de la palabra GROUP.

11. ¿Cuántos acomodos diferentes de las letras de la palabra BOUGHT puede formarse si las vocales deben conservarse juntas?

12. (a) Encuentre el número de permutaciones distinguibles de las letras de BOOLEAN.
    (b) Encuentre el número de permutaciones distinguibles de las letras de PASCAL.

13. (a) Encuentre el número de permutaciones distinguibles de las letras de ASSOCIATIVE.
    (b) Encuentre el número de permutaciones distinguibles de las letras de REQUIREMENTS.

14. ¿De cuántas maneras pueden sentarse siete personas en un círculo?

15. Se va a usar un librero para exhibir seis nuevos libros. Supóngase que hay ocho libros de ciencia de computación y cinco libros franceses de dónde escoger. Si se decide exhibir cuatro libros de ciencia de computación y dos libros franceses, y se pide mantener juntos los libros de cada tema ¿cuántos acomodos diferentes es posible hacer?

16. Se lanzan tres dados legales de seis caras y se anotan los números que aparecen en las caras superiores como lanzamientos triples. ¿Cuántos reportes diferentes son posibles?

17. Demuestre que $n \cdot {}_{n-1}P_{n-1} = {}_nP_n$.

18. La mayoría de las versiones de Pascal permite formar nombres de variables de ocho letras o dígitos, con la condición de que el primer carácter debe ser una letra. ¿Cuántos nombres de variables de ocho caracteres son posibles?

19. Actualmente, los códigos de área telefónicos son de tres dígitos, pero el dígito intermedio debe ser 0 o 1. Los códigos cuyos últimos dos dígitos son 1 están siendo usados para otros fines, por ejemplo, 911. Con estas condiciones ¿cuántos códigos de área hay disponibles?

20. ¿Cuántos números de Seguridad Social (EU) puede asignarse en cualquier tiempo dado? Identifique las suposiciones que haya hecho.

3.2. Combinaciones

El principio de multiplicación y los métodos de conteo para permutaciones son aplicados todos a situaciones en las que interesa el orden. En esta sección se verá algunos problemas de conteo en los que no interesa el orden.

Problema 2. Sea A cualquier conjunto de n elementos y $1 \leq r \leq n$. ¿Cuántos subconjuntos diferentes de A existen, cada uno con r elementos?

El nombre tradicional para un subconjunto de r elementos de un conjunto A de n elementos es una **combinación de A, tomando los elementos r a la vez**.

Ejemplo 1. Sea $A = \{1, 2, 3, 4\}$. Las siguientes son todas combinaciones distintas de A, con sus elementos tomados tres a la vez: $A_1 = \{1, 2, 3\}$, $A_2 = \{1, 2, 4\}$, $A_3 = \{1, 3, 4\}$, y $A_4 = \{2, 3, 4\}$. Nótese que éstos son subconjuntos, no secuencias. Por lo tanto, $A_1 = \{2, 1, 3\} = \{2, 3, 1\} = \{1, 3, 2\} = \{3, 1, 2\} = \{3, 2, 1\}$. En otras palabras, cuando se trata de combinaciones, a diferencia de las permutaciones, el orden de los elementos carece de importancia. ◆

Ejemplo 2. Sea A el conjunto de las 52 cartas de una baraja ordinaria para juego. Entonces una combinación de A, tomando cinco cartas a la vez, es sólo una mano de cinco cartas, independientemente de la forma en que hayan sido dadas. ◆

Se quiere contar ahora el número de subconjuntos de r elementos de un conjunto A de n elementos. La manera más fácil de lograrlo es usando lo que ya se sabe acerca de las permutaciones. Observe que cada permutación de los elementos de A, tomados r a la vez, puede formarse efectuando las dos tareas siguientes en secuencia.

Tarea 1. Escoja un subconjunto B de A que contenga r elementos.
Tarea 2. Escoja una permutación particular de B.

Se está tratando de calcular el número de maneras de escoger B. Se llamará a este número C. Entonces la tarea 1 puede efectuarse de C maneras, y la tarea 2 puede realizarse de $r!$ maneras. En consecuencia, el número total de maneras de efectuar ambas tareas es, por el principio de la multiplicación, $C \cdot r!$. Pero también es ${}_nP_r$. Por tanto

$$C \cdot r! = {}_nP_r = \frac{n!}{(n-r)!}.$$

Por lo tanto,

$$C = \frac{n!}{r!\,(n-r)!}.$$

Se ha demostrado así el siguiente resultado.

Teorema 1. *Sea A un conjunto con $|A| = n$, y sea $1 \leq r \leq n$. Entonces el número de combinaciones de los elementos de A, tomados r a la vez, es decir, el número de subconjuntos de r elementos de A,* es

$$\frac{n!}{r!\,(n-r)!}.$$ ●

Nótese una vez más que el número de combinaciones de A, tomando los elementos r a la vez, no depende de A, sino solamente de n y r. Este número se escribe a menudo ${}_nC_r$ y se denomina el **número de combinaciones de n objetos tomados r a la vez**. Se tiene

$$_nC_r = \frac{n!}{r!\,(n-r)!}.$$

Este cálculo puede hacerse directamente en muchas calculadoras.

Ejemplo 3. Calcule el número de manos distintas, de cinco cartas, que se puede dar tomándolas de una baraja de 52 cartas.

Solución: Este número es ${}_{52}C_5 = \frac{52!}{5!\,47!}$, o sea, 2,598,960, porque el orden en que se den las cartas es irrelevante. Compare este número con el que se calculó en la sección 3.1, ejemplo 6. ◆

En el estudio de las permutaciones, se consideraron casos en los que se permitían repeticiones. Véase ahora un caso de este tipo para combinaciones.

Considérese la situación siguiente. Una estación de radio ofrece un premio de tres discos compactos de la lista de los diez de mayor éxito. La selección de los discos se deja al ganador y se permite repeticiones. El orden en que se haga las selecciones es irrelevante. Para determinar el número de maneras en que los ganadores del premio pueden hacer sus selecciones, se utiliza una técnica de resolución de problemas que ya se ha usado antes; se modela la situación con una que ya se sabe cómo manejar.

Supóngase que las selecciones son registradas por el sistema de correo de voz de la estación. Después de identificarse apropiadamente, se pregunta a una ganadora acerca de cada una de las 10 mejores selecciones en orden. En cada paso, se le pide que oprima 1 si ella quiere ese disco compacto y 2 para continuar con la selección siguiente. El 1 puede oprimirse una segunda o una tercera vez para ordenar una segunda o tercera copia de una selección antes de oprimir el 2 para continuar. Cuando se ha registrado un total de tres unos, se detiene el proceso y el sistema le dice a la persona que llama que le serán enviados los discos seleccionados. Se tiene que hacer una grabación para cada una de estas llamadas. Un disco de la grabación será una secuencia de unos y doses. Es claro que habrá tres unos en la secuencia. Una secuencia puede contener hasta nueve doses, por ejemplo, si el ganador rehúsa los primeros nueve discos y escoge tres copias del disco número 10. Nuestro modelo para contar el número de maneras en que un ganador puede escoger sus tres discos es el siguiente. Cada selección de tres discos puede representarse por un arreglo que contenga tres unos y nueve doses o espacios en blanco, es decir, un total de 12 celdas. Algunos registros de grabación posibles son 2212212221 (seleccionando los números 4, 6, 10), 1211*bbbbbbbb* (seleccionando el número 1 y dos copias del número 2), y 222222222111 (seleccionando tres copias del número 10). El número de maneras de seleccionar tres celdas del arreglo que contengan unos es ${}_{12}C_3$, ya que el arreglo tiene 3 + 9, o sea 12 celdas, y el orden en que se haga esta selección no importa.

Teorema 2. *Supóngase que se va a hacer k selecciones de n elementos sin tomar en consideración el orden y que se permiten repeticiones, suponiendo por lo menos k copias de cada uno de los n elementos. El número de maneras en que puede hacerse estas selecciones es ${}_{(n+k-1)}C_k$.* ●

Ejemplo 4. ¿De cuántas maneras puede escoger el ganador de un premio tres discos compactos de la lista de los diez de mayor éxito, si se permite repeticiones?

Solución: Aquí n es 10 y k es 3. Por el teorema 2, hay ${}_{10+3-1}C_3$, o sea ${}_{12}C_3$ maneras de hacer las selecciones. El ganador del premio puede hacer la selección de 220 maneras. ◆

En general, cuando interesa el orden, se cuenta el número de secuencias o permutaciones, y cuando no interesa el orden, se cuenta el número de subconjuntos o combinaciones.

Algunos problemas requieren que el conteo de permutaciones y combinaciones se combine y se complemente por el uso directo del principio de la adición o de la multiplicación.

Ejemplo 5. Supóngase que una clave válida de acceso a una computadora está formada por siete caracteres, el primero de los cuales es una letra escogida del conjunto {A, B, C, D, E, F, G}, y que los seis caracteres restantes son letras escogidas del alfabeto o un dígito. ¿Cuántas claves diferentes son posibles?

Solución: Una clave puede construirse efectuando las tareas T_1 y T_2 en secuencia.

Tarea T_1: Escoja una letra de iniciación del conjunto dado.
Tarea T_2: Escoja una secuencia de letras y dígitos. Se permite repeticiones.

La tarea T_1 puede efectuarse de ${}_7C_1$ maneras. Puesto que hay 26 letras y 10 dígitos que pueden ser escogidos para cada uno de los seis caracteres restantes y, en vista de que se permite repeticiones, la tarea T_2 puede realizarse en 36^6, o sea, 2,176,782,336 maneras. Por el principio de la multiplicación, hay $7 \cdot 2176782336$, o sea 15,237,476,352 claves diferentes. ◆

Ejemplo 6. ¿Cuántos comités diferentes de siete personas puede formarse, si cada comité debe tener 3 mujeres de un conjunto disponible de 20 mujeres, y 4 hombres de un conjunto disponible de 30 hombres?

Solución: En este caso puede formarse un comité realizando las dos tareas siguientes en sucesión:

Tarea 1: Escoja 3 mujeres del conjunto de 20 mujeres.
Tarea 2: Escoja 4 hombres del conjunto de 30 hombres.

Aquí no importa el orden en que se seleccione los individuos, por lo que simplemente estaremos contando el número de subconjuntos posibles. Así, la tarea 1 puede efectuarse de ${}_{20}C_3$, o sea de 1140 maneras, y la tarea 2 puede realizarse de ${}_{30}C_4$, o sea de 27,405 maneras. Por el principio de multiplicación, hay (1140) (27405) o sea 31,241,700 comités diferentes. ◆

GRUPO DE EJERCICIOS 3.2

1. Calcule cada una de las siguientes combinaciones.
(a) ${}_7C_7$ (b) ${}_7C_4$ (c) ${}_{16}C_5$
(d) ${}_nC_{n-1}$ (e) ${}_nC_{n-2}$ (f) ${}_{n+1}C_{n-1}$

2. Demuestre que ${}_nC_r = {}_nC_{n-r}$.

3. ¿De cuántas maneras puede seleccionarse un comité de tres miembros de facultad y dos estudiantes, tomándolos de siete miembros de facultad y ocho estudiantes?

4. ¿De cuántas maneras puede darse una mano de 6 cartas si se tiene una baraja de 52 cartas?

5. En un cierto colegio, la oficina de alojamientos ha decidido nombrar, para cada piso, un consejero residente masculino y uno femenino. ¿Cuántos pares diferentes de consejeros puede seleccionarse para un edificio de siete pisos, de 12 candidatos del sexo masculino y 15 del sexo femenino?

6. Un fabricante de microcomputadoras que está preparando una campaña de publicidad, está considerando seis revistas, tres periódicos, dos estaciones de televisión y cuatro estaciones de radio. ¿De cuántas maneras puede difundirse seis anuncios si
(a) los seis deben ser hechos en revistas?
(b) dos deben aparecer en revistas, dos en periódicos, uno en televisión y uno por radio?

7. ¿Cuántas manos diferentes de 8 cartas con 5 cartas rojas y 3 negras puede repartirse de una baraja de 52 cartas?

8. (a) Encuentre el número de subconjuntos de cada tamaño posible de un conjunto que contiene cuatro elementos.
(b) Encuentre el número de subconjuntos de cada tamaño posible para un conjunto que contiene n elementos.

9. Una urna contiene 15 bolas, 8 de las cuales son rojas y 7 son negras. ¿De cuántas maneras puede escogerse 5 bolas de manera que
(a) las 5 sean rojas?
(b) las 5 sean negras?
(c) 2 sean rojas y 3 sean negras?
(d) 3 sean rojas y 2 sean negras?

10. ¿De cuántas maneras puede seleccionarse un comité de 6 personas de un conjunto de 10, si una de las personas debe ser nombrada como presidente del comité?

11. Un certificado de obsequio de una librería local permite al poseedor escoger 6 libros de la lista combinada de 10 libros de ficción de los de mayor venta y 10 libros de temas formales también de los de mayor venta. ¿De cuántas maneras diferentes puede hacerse la selección de 6 libros?

12. El plan de alimentos del colegio permite a cada estudiante escoger tres piezas de fruta cada día. Las frutas disponibles son manzanas, plátanos, duraznos, peras y ciruelas. ¿Por cuántos días puede un estudiante hacer una selección diferente?

13. Demuestre que ${}_{n+1}C_r = {}_nC_{r-1} + {}_nC_r$.

14. (a) ¿De cuántas maneras puede un estudiante escoger 8 de 10 preguntas para contestar en un examen?
(b) ¿De cuántas maneras puede un estudiante escoger 8 de 10 preguntas para contestar en un examen si las primeras 3 preguntas deben ser contestadas?

15. Se lanza al aire cinco monedas legales y se registra los resultados.
(a) ¿Cuántas secuencias diferentes de caras y cruces son posibles?
(b) ¿Cuántas de las secuencias de la parte (a) tienen exactamente una cara registrada?
(c) ¿Cuántas de las secuencias de la parte (a) tienen exactamente tres caras registradas?

16. Se lanza tres dados legales de seis caras y se registra los números que aparecen en las caras superiores.
(a) ¿Cuántas secuencias registradas diferentes son posibles?
(b) ¿Cuántos de los registros de la parte (a) contienen exactamente un seis?
(c) ¿Cuántos de los registros de la parte (a) contienen exactamente dos cuatros?

17. Si se lanza n monedas legales y se registra los resultados, ¿cuántas
(a) secuencias de registro son posibles?

(b) secuencias contienen exactamente tres cruces, suponiendo $n \geq 3$?
(c) secuencias contienen exactamente k caras, suponiendo $n \geq k$?

18. Si se lanza n dados legales de seis caras y se anota los números que aparecen en las caras superiores, ¿cuántas
(a) secuencias de registro son posibles?
(b) secuencias contienen exactamente un seis?
(c) secuencias contienen exactamente cuatro doses, suponiendo $n \geq 4$?

19. ¿De cuántas maneras puede usted escoger tres de siete libros de ficción y dos de seis libros de temas formales para llevar consigo en sus vacaciones?

20. Para manejar en carretera durante sus vacaciones, va a escoger usted 6 de las 35 casetes de rock de su colección, 3 de las 22 casetes de música clásica y 1 de las 8 casetes de música romántica. ¿De cuántas maneras puede hacer usted sus selecciones?

3.3. Principio de las casillas

En esta sección se introduce otra técnica de demostración, en la cual se utiliza los métodos de conteo que han sido estudiados.

Teorema 1 (El principio de las casillas). *Si se asigna n objetos a m casillas, y m < n, entonces por lo menos una casilla contiene dos o más objetos.*

Demostración: Considere las m casillas marcadas con los números 1 a m y los n objetos con los números 1 a n. Ahora, comenzando con el objeto 1, asigne cada objeto en orden a la casilla de igual número. Esto asigna tantos objetos como es posible a casillas individuales, pero como $m < n$, hay $n - m$ objetos a los que todavía no se ha asignado una casilla. A una casilla por lo menos tendrá que asignársele un segundo objeto. ●

Este teorema informal, que suena casi trivial, es fácil de usar y tiene un poder inesperado en la demostración de consecuencias interesantes.

Ejemplo 1. Si se escoge ocho personas aleatoriamente de algún conjunto, por lo menos dos de ellas habrán nacido el mismo día de la semana. Aquí cada persona (objeto) se asigna al día de la semana (casilla) en que nació él o ella. Como hay ocho personas y solamente siete días de la semana, el principio de las casillas dice que por lo menos dos personas deberán asignarse al mismo día de la semana. ♦

Observe usted que el principio de las casillas proporciona una prueba de existencia; debe haber un objeto u objetos con una cierta característica. En el ejemplo 1, esta característica es haber nacido en el mismo día de la semana. El principio de las casillas garantiza que hay por lo menos dos personas con esta característica, pero no da información sobre la identificación de estas personas. Sólo queda garantizada su existencia. En contraste, una prueba constructiva garantiza la existencia de un objeto u objetos que tengan una cierta característica, construyendo realmente tal objeto u objetos. Por ejemplo, se podría demostrar que, dados dos números racionales p y q, existe un número racional entre ellos, si se demuestra que $\frac{p+q}{2}$ está comprendido entre p y q.

Para usar el principio de las casillas, se debe identificar los objetos y las casillas (categorías de la característica deseada), y poder contar el número de objetos y el número de casillas.

Ejemplo 2. Demuestre que si se escoge cinco números cualesquiera del 1 al 8, entonces dos de éstos sumarán 9.

Solución: Construya cuatro conjuntos diferentes, cada uno con dos números que sumen 9 de la siguiente manera: $A_1 = \{1, 8\}, A_2 = \{2, 7\}, A_3 = \{3, 6\}, A_4 = \{4, 5\}$. Cada uno de los cinco números escogidos debe pertenecer a uno de estos conjuntos. Como sólo hay cuatro conjuntos, el principio de casillas dice que dos de los números escogidos pertenecen al mismo conjunto. Estos números suman 9. ♦

Ejemplo 3. Demuestre que si se escoge 11 números cualesquiera del conjunto $\{1, 2, \ldots, 20\}$, entonces uno de ellos será múltiplo de otro.

Solución: Todo entero positivo n puede escribirse como $n = 2^k m$, en donde m es impar y $k \geq 0$. Esto puede verse simplemente descomponiendo en factores todas las potencias de 2 (si las hay) tomadas de n. En este caso, se llamará m a la parte impar de n. Si se escoge 11 números del conjunto $\{1, 2, \ldots, 20\}$, entonces dos de ellos deben tener la misma parte impar. Esto se desprende del principio de las casillas, puesto que hay 11 números (objetos), pero solamente 10 números impares comprendidos entre 1 y 20 (casillas) que pueden ser partes impares de estos números.

Sean n_1 y n_2 dos números escogidos con la misma parte impar. Se debe tener $n_1 = 2^{k_1}m$ y $n_2 = 2^{k_2}m$, para algunos k_1 y k_2. Si $k_1 \geq k_2$, entonces n_1 es un múltiplo de n_2; de lo contrario, n_2 es un múltiplo de n_1. ♦

Ejemplo 4. Considérese la región que se ilustra en la figura 3.2. Está limitada o circundada por un hexágono regular cuyos lados tienen longitud de 1 unidad. Demuestre que si se escoge siete puntos cualesquiera en esta región, entonces dos de éstos deberán estar a una separación no mayor que 1 unidad.

Solución: Divida la región en seis triángulos equiláteros, como se muestra en la figura 3.3. Si se escoge siete puntos en la región, se puede asignar cada uno de ellos a un triángulo que lo contenga. Si el punto pertenece a varios triángulos, asígnelo arbitrariamente a uno de ellos. Entonces los siete puntos están asignados a seis regiones triangulares, de modo que por el principio de las casillas por lo menos dos puntos deben pertenecer a la misma región. Entre estos dos no puede haber una separación mayor que 1 unidad. ♦

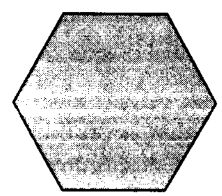


Figura 3.2

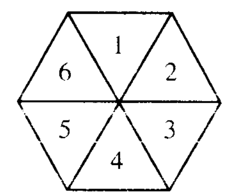


Figura 3.3

Ejemplo 5. 20 miembros de una liga de boliche usan unas camisas numeradas del 1 al 20. Cuando se escoge cualesquiera 3 de estos miembros para formar un equipo, se emplea la suma de sus números como número de código para el equipo. Demuestre que si se selecciona 8 de cualesquiera de los 20, entonces de estos 8 se puede formar por lo menos dos equipos diferentes que tengan el mismo número de código.

Solución: De los 8 jugadores de boliche seleccionados, puede formarse un total de ${}_8C_3$, o sea, 56 equipos diferentes. Éstos jugarán el papel de objetos. El número de código de equipo más grande posible es $18 + 19 + 20$, o sea, 57, y el más pequeño posible es $1 + 2 + 3$, o sea 6. En consecuencia, sólo los 52 números de código (casillas) comprendidos entre 6 y 57 inclusive, están disponibles para los 56 equipos posibles. Por el principio de las casillas, por lo menos dos equipos tendrán el mismo número de código. ♦

Principio de las casillas ampliado

Debe observarse que si hay m casillas y más de $2m$ objetos, entonces tres o más objetos tendrán que ser asignados a por lo menos una de las casillas. (Considere la distribución más uniforme de casillas que usted pueda hacer.) En general, si el número de objetos es mucho mayor que el número de casillas, puede volverse a enunciar el teorema 1 para dar una conclusión de mayor fuerza.

Véase primero algo acerca de la notación. Si n y m son enteros positivos, entonces $\lfloor n/m \rfloor$ representa el entero más grande menor que o igual al número racional n/m. En consecuencia, $\lfloor 3/2 \rfloor$ es 1, $\lfloor 9/4 \rfloor$ es 2, y $\lfloor 6/3 \rfloor$ es 2.

Teorema 2 (El principio de las casillas ampliado). *Si se asigna n objetos a m casillas, entonces una de las casillas debe contener por lo menos* $\lfloor (n-1)/m \rfloor + 1$ *objetos.*

Demostración (por contradicción): Si cada casilla contiene no más de $\lfloor (n-1)/m \rfloor$ objetos, entonces hay como máximo $m \cdot \lfloor (n-1)/m \rfloor \leq m \cdot (n-1)/m = n - 1$ objetos en total. Esto contradice las suposiciones, de modo que una de las casillas debe contener por lo menos $\lfloor (n-1)/m \rfloor + 1$ objetos. ●

Ejemplo 6. Véase una extensión del ejemplo 1. Demuestre que si se selecciona 30 personas cualesquiera, entonces se puede escoger un subconjunto de 5 tal que las 5 hayan nacido el mismo día de la semana.

Solución: Asigne cada persona al día de la semana en que ella o él haya nacido. Entonces se está asignando 30 personas a 7 casillas. Por el principio de casillas ampliado, con $n = 30$ y $m = 7$, por lo menos $\lfloor (30 - 1)/7 \rfloor + 1$, o sea 5 de las personas deben de haber nacido en el mismo día de la semana. ♦

Ejemplo 7. Demuestre que si 30 diccionarios de una biblioteca contienen un total de 61,327 páginas, entonces uno de los diccionarios debe tener por lo menos 2045 páginas.

Solución: Supóngase que las páginas son los objetos y los diccionarios, las casillas. Asigne cada página al diccionario en el cual aparezca. Entonces, por el principio de casillas ampliado, un diccionario debe contener por lo menos $\lfloor 61{,}326/30 \rfloor + 1$, o sea, 2045 páginas. ♦

GRUPO DE EJERCICIOS 3.3

1. Si se reúnen 13 personas en un salón, demuestre que por lo menos 2 de ellas deben de tener su cumpleaños en el mismo mes.

2. Demuestre que si se escoge siete números del 1 al 12, dos de ellos sumarán 13.

3. Sea T un triángulo equilátero cuyos lados son de longitud de 1 unidad. Demuestre que si se escogen cinco puntos cualesquiera que se encuentren sobre o dentro del triángulo, entre dos de ellos existirá una separación no mayor que $\frac{1}{2}$ unidad.

4. Demuestre que si se escoge ocho enteros positivos cualesquiera, dos de ellos tendrán el mismo residuo al ser divididos entre 7.

5. Demuestre que si se emplea siete colores para pintar 50 bicicletas, por lo menos 8 bicicletas serán del mismo color.

6. Hay diez personas voluntarias para formar un comité de tres personas. Cada comité de tres que puede formarse de estos 10 nombres, se escribe en una hojita de papel, haciendo una hojita para cada comité posible, y se pone las hojitas, dobladas, en 10 sombreros. Demuestre que por lo menos un sombrero contiene 12 o más hojitas de papel.

7. Seis amigos descubren que tienen un total de $21.61 entre todos para ir al cine. Demuestre que uno o más de ellos debe tener por lo menos $3.61.

8. Una tienda tiene una venta de promoción para 12 tipos de barras de dulce. Un cliente puede escoger una barra de cualquiera de cinco tipos diferentes, y no se le cobrará más que $1.75. Demuestre que, aunque las diferentes selecciones pueden tener un costo diferente, debe haber por lo menos dos maneras diferentes de escoger, de manera que el costo sea el mismo para ambas selecciones.

9. Si la tienda del ejercicio 8 permite repeticiones en las selecciones, demuestre que debe haber por lo menos 10 maneras de hacer selecciones diferentes que tengan el mismo costo.

10. Demuestre que debe haber por lo menos 90 maneras de escoger seis números del 1 al 15, de modo que todas las selecciones al sumarse den el mismo resultado.

11. ¿Cuántos amigos debe tener usted para garantizar que por lo menos cinco de ellos tengan su cumpleaños en el mismo mes?

12. Demuestre que si se selecciona cinco puntos en un cuadrado cuyos lados midan 1 pulgada de largo, por lo menos dos de los puntos deben estar separados por no más de $\sqrt{2}$ pulgadas.

13. Demuestre que si se escoge 14 números cualesquiera del 1 al 25, uno de ellos es múltiplo de otro.

14. Sobre una mesa se coloca veinte tarjetas numeradas del 1 al 20, con la cara hacia abajo. Las tarjetas son seleccionadas una a la vez y volteadas hasta haber escogido 10 de ellas. Si dos de las tarjetas suman 21, el jugador pierde. ¿Es posible ganar este juego?

15. Supóngase que se ha cambiado el juego del ejercicio 14, y que se debe escoger 12 cartas. ¿Es posible ganar este juego?

3.4. Elementos de probabilidad

Otra área en la que son importantes las técnicas de conteo es la teoría de probabilidades. En esta sección se presenta una breve introducción a la probabilidad.

Muchos experimentos no dan exactamente los mismos resultados cuando son efectuados repetidas veces. Por ejemplo, al lanzar una moneda, no hay ninguna seguridad de que se obtendrá cara o cruz, y si se lanza un dado, no hay manera de saber cuál de los seis números posibles ha de quedar hacia arriba. Los experimentos de este tipo son llamados **probabilísticos**, en contraste con los experimentos **determinísticos o deterministas**, cuyo resultado es siempre el mismo.

Espacios muestrales

Un conjunto A formado por todos los resultados de un experimento se denomina **espacio muestral** del experimento. Con un experimento dado, se puede asociar, a menudo, más de un espacio muestral, dependiendo de lo que el observador elija registrar como resultado.

Ejemplo 1. Supóngase que se lanza al aire una moneda de 5 centavos y una de un cuarto de dólar. Se describe tres posibles espacios muestrales que pueden ser asociados con este experimento.

1. Si el observador decide registrar como resultado el número de caras observadas, el espacio muestral es $A = \{0, 1, 2\}$.
2. Si el observador decide registrar la secuencia de caras (H) y de cruces (T) que observa, anotando en lista el resultado de la de 5 centavos primero, y luego el del cuarto de dólar, entonces el espacio muestral es $A = \{HH, HT, TH, TT\}$.
3. Si el observador decide registrar el hecho de que las monedas coincidan en la cara que cae (M) o que no coincidan (N), entonces el espacio muestral es $A = \{M, N\}$. ◆

Se ve en consecuencia que, además de describir el experimento, se debe indicar exactamente lo que el observador desee registrar. Entonces, el conjunto de todos los resultados de este tipo se convierte en el espacio muestral para el experimento.

Un espacio muestral puede contener un número finito o infinito de resultados.

Ejemplo 2. Determine el espacio muestral para un experimento que consiste en lanzar dos veces un dado de seis caras, y el registro de la secuencia de números que aparezcan en la cara superior del dado después de cada lanzamiento.

Solución: Un resultado del experimento puede representarse por un par ordenado de números (n, m), en donde n y m pueden ser 1, 2, 3, 4, 5 o 6. En consecuencia, el espacio A muestral contiene 6×6, o sea 36 elementos (por el principio de la multiplicación). ◆

Ejemplo 3. Un experimento consiste en sacar tres monedas en sucesión de una caja que contiene cuatro centavos y cinco monedas de diez centavos, y registrar la secuencia de resultados. Determine el espacio muestral de este experimento.

Solución: Un resultado puede registrarse como una secuencia de longitud 3 construida con las letras P (centavo) y D (décimo). En consecuencia, el espacio muestral A es

$$\{PPP, PPD, PDP, PDD, DPP, DPD, DDP, DDD\}$$ ◆

Eventos

Se dice que un enunciado acerca del resultado de un experimento, que para un resultado particular puede ser verdadero o falso, describe un **evento**. Así, para el ejemplo 2, los enunciados "Cada uno de los números registrados es menor que 3" y "La suma de los números registrados es 4" describirían eventos. El evento descrito por un enunciado se toma como el conjunto de todos los resultados para los cuales el enunciado es verdadero. Con esta interpretación, cualquier evento puede considerarse como un subconjunto del espacio muestral. Así el evento E descrito por el primer enunciado es $E = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$. De modo semejante, el evento F descrito por el segundo enunciado es $F = \{(1, 3), (2, 2), (3, 1)\}$.

Ejemplo 4. Considérese el experimento del ejemplo 2. Determine los eventos descritos por cada uno de los siguientes enunciados.
(a) La suma de los números que aparecen en las caras superiores es 8.
(b) La suma de los números que aparecen en las caras superiores es por lo menos 10.

Solución: (a) El evento consta de todos los pares ordenados cuya suma es 8. En consecuencia, el evento es $\{(2, 6), (3, 5), (4, 4), (5, 3), (6, 2)\}$.
(b) El evento consta de todos los pares ordenados cuya suma sea 10, 11 o 12. En consecuencia, el evento es $\{(4, 6), (5, 5), (5, 6), (6, 4), (6, 5), (6, 6)\}$. ◆

Si A es un espacio muestral de un experimento, entonces A mismo es un evento conocido como **evento seguro**, y al subconjunto vacío de A se le llama **evento imposible**.

Puesto que los eventos son conjuntos, pueden ser combinados aplicando las operaciones de unión, intersección y complementación para formar nuevos eventos. El espacio muestral A es el conjunto universal para estos eventos. Así, si E y F son eventos, se puede formar los nuevos eventos $E \cup F$, $E \cap F$, y $\overline{E}$. ¿Qué significan estos nuevos eventos en términos del experimento? Un resultado del experimento pertenece a $E \cup F$ cuando éste pertenece a E o a F (o a ambos). En otras palabras, el evento $E \cup F$ ocurre exactamente cuando ocurre E o F. De modo similar, el evento $E \cap F$ ocurre si y solamente si ocurren ambos, E y F. Finalmente, $\overline{E}$ ocurre si y solamente si no ocurre E.

Ejemplo 5. Considérese el experimento de lanzar un dado y registrar el número que aparece en la cara superior. Sea E el evento de que el número es par, y sea F el evento de que el número es primo. Entonces $E = \{2, 4, 6\}$ y $F = \{2, 3, 5\}$. El evento de que el número que aparezca sea o par o primo es $E \cup F = \{2, 3, 4, 5, 6\}$. El evento de que el número que aparezca sea un número par es $E \cap F = \{2\}$. Finalmente, el evento de que el número que aparezca no sea par es $\overline{E} = \{1, 3, 5\}$, y el evento de que el número que aparezca no sea primo es $\overline{F} = \{1, 4, 6\}$. ◆

Se dice que los eventos E y F son **mutuamente excluyentes** o **disjuntos** si $E \cap F = \{\ \}$. Si E y F son eventos mutuamente excluyentes, entonces E y F no pueden ocurrir ambos al mismo tiempo; si ocurre E, entonces no ocurre F, y si ocurre F, entonces no ocurre E. Si $E_1, E_2, \ldots, E_n$ todos son eventos, entonces se dice que estos conjuntos son **mutuamente excluyentes**, o **disjuntos**, si cada par de ellos es mutuamente excluyente. Una vez más, esto significa que cuando más puede ocurrir uno de los eventos en cualquier resultado dado del experimento

Asignación de probabilidades a eventos

En teoría de probabilidades, se supone que a cada evento E se le ha asignado un número $p(E)$ llamado **probabilidad del evento** E. Véase ahora las probabilidades. Se va a investigar formas en que puede asignarse dichos números, las propiedades que deben satisfacer y el significado que puede dárseles.

El número $p(E)$ refleja la evaluación de la probabilidad de que ocurra el evento E. En forma más precisa, supóngase que el experimento subyacente se efectúa repetidas veces y que, después de n de tales realizaciones, el evento E ha ocurrido n_E veces. Entonces la fracción $f_E = n_E/n$ a la que se llama **frecuencia de ocurrencia de *E* en *n* ensayos**, es una medida de la probabilidad de que ocurra E. Cuando se asigna la probabilidad $p(E)$ al evento E, significa que, según lo que se conoce, la fracción f_E tenderá cada vez con mayor cercanía a un cierto número al volverse más grande n, y que $p(E)$ es este número. Así, las probabilidades pueden ser consideradas como frecuencias idealizadas de ocurrencia de eventos, a las cuales habrán de tender las frecuencias de ocurrencia reales cuando el experimento se realice repetidamente.

Ejemplo 6. Supóngase que un experimento se realiza 2000 veces; la frecuencia de ocurrencia f_E de un evento E se registra después de 100, 500, 1000 y 2000 intentos, y la tabla 3.1 resume los resultados.

Tabla 3.1

Número de repeticiones del experimento	n_E	$f_E = n_E/n$
100	48	0.48
500	259	0.518
1000	496	0.496
2000	1002	0.501

Con base en esta tabla, se ve que la frecuencia f_E tiende a $\frac{1}{2}$ al aumentar n. Podría argumentarse, por tanto, que $p(E)$ debe hacerse igual a $\frac{1}{2}$. Por otra parte, podría requerirse una evidencia mayor antes de asignar $\frac{1}{2}$ como valor a $p(E)$. En todo caso, esta clase de evidencia nunca puede "probar" que $p(E)$ es $\frac{1}{2}$. Sólo sirve para hacer de ésta una suposición plausible. ◆

Si las probabilidades asignadas a los distintos eventos han de representar frecuencias significativas de ocurrencia de los mismos, como se ha expuesto, entonces no pueden ser asignadas de una manera totalmente arbitraria. Tienen que satisfacer ciertas condiciones. Primero, como cada frecuencia f_E debe satisfacer las desigualdades de $0 \leq f_E \leq 1$, es simplemente razonable suponer que

$$\text{P1:} \quad 0 \leq p(E) \leq 1 \quad \text{para todo evento } E \text{ de } A.$$

También, puesto que el evento A debe ocurrir cada vez (cada resultado pertenece a A), y no puede ocurrir el evento $\varnothing$, se supone que

$$\text{P2:} \quad p(A) = 1 \quad \text{y} \quad p(\varnothing) = 0.$$

Finalmente, si $E_1, E_2, \ldots, E_k$ son eventos mutuamente excluyentes, entonces

$$n_{(E_1 \cup E_2 \cup \cdots \cup E_k)} = n_{E_1} + n_{E_2} + \cdots + n_{E_k},$$

ya que sólo uno de estos eventos puede ocurrir a la vez. Si se divide ambos miembros de esta ecuación entre n, se observa que las frecuencias de ocurrencia deben satisfacer una ecuación similar. Por lo tanto se supone que

$$\text{P3:} \quad p(E_1 \cup E_2 \cup \cdots \cup E_k) = p(E_1) + p(E_2) + \cdots + p(E_k)$$

en todos los casos en que los eventos sean mutuamente excluyentes. Si el espacio muestral es finito y las probabilidades están asignadas a todos los eventos de tal manera que P1, P2 y P3 se satisfagan siempre, entonces se cuenta con un **espacio de probabilidad**. A P1, P2 y P3 se les llama **axiomas para un espacio de probabilidad**.

Es importante comprender que, matemáticamente, no se emplea el espacio de probabilidad; el único uso es el que se hace por los axiomas de probabilidad P1, P2 y P3. La teoría de la probabilidad comienza con todas las probabilidades asignadas y luego investiga las consecuencias de estas probabilidades y las relaciones entre las mismas. No se hace mención alguna de la forma en que fueron asignadas las probabilidades. Sin embargo, las conclusiones matemáticas serán útiles en una situación real solamente si las probabilidades asignadas reflejan lo que realmente ocurre en esa situación.

La experimentación no es la única forma de determinar probabilidades razonables para eventos. A veces, los axiomas de probabilidad pueden proporcionar argumentos lógicos para escoger ciertas probabilidades.

Ejemplo 7. Considérese el experimento de lanzar una moneda y anotar si resultan caras o cruces. Considérese los eventos E: salen caras y F: salen cruces. La mecánica del lanzamiento no es controlable al detalle. En consecuencia, si la moneda no tiene algún defecto que pudiera desbalancearla, puede afirmarse que tienen igual probabilidad de ocurrir E y F. Existe una simetría en la situación que hace imposible preferir un resultado respecto del otro. Este argumento permite calcular las probabilidades que deben tener E y F.

Se ha supuesto que $p(E) = p(F)$, y es claro que E y F son eventos mutuamente excluyentes y $A = E \cup F$. Así, usando las propiedades P2 y P3, se observa que

$$1 = p(A) = p(E) + p(F) = 2p(E), \text{ en vista de que } p(E) = p(F).$$

Esto demuestra que $p(E) = \frac{1}{2} = p(F)$. Con frecuencia puede asignarse probabilidades apropiadas a eventos, combinando la simetría de situaciones con los axiomas de probabilidad. ◆

Por último, se demostrará que el problema de asignar probabilidades a eventos puede reducirse a la consideración de los casos más simples. Sea A un espacio de probabilidad. Se supone que A es finito, es decir, $A = \{x_1, x_2, \ldots, x_n\}$. Entonces cada evento $\{x_k\}$, que conste de sólo un resultado, se denomina **evento elemental**. Para simplificar, se escribirá $p_k = p(\{x_k\})$. Entonces p_k se llama **probabilidad elemental correspondiente al resultado x_k**. Como los eventos elementales son mutuamente excluyentes y su unión es A, los axiomas de probabilidad dicen que

EP1: $0 \leq p_k \leq 1$, para todos los valores de k

EP2: $p_1 + p_2 + \cdots + p_n = 1$.

Si E es un evento cualquiera en A, por ejemplo $E = \{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$, entonces se puede escribir $E = \{x_{i_1}\} \cup \{x_{i_2}\} \cup \cdots \cup \{x_{i_m}\}$. Esto significa, por el axioma P2, que $p(E) = p_{i_1} + p_{i_2} + \cdots + p_{i_m}$. En consecuencia, si se conoce las probabilidades elementales, puede calcularse la probabilidad de cualquier evento E.

Ejemplo 8. Supóngase que un experimento tiene un espacio muestral $A = \{1, 2, 3, 4, 5, 6\}$ y que se ha determinado las probabilidades elementales, que son como sigue:

$$p_1 = \frac{1}{12}, \quad p_2 = \frac{1}{12}, \quad p_3 = \frac{1}{3}, \quad p_4 = \frac{1}{6}, \quad p_5 = \frac{1}{4}, \quad p_6 = \frac{1}{12}.$$

Sea E el evento "El resultado de un número par". Calcule $p(E)$.

Solución: Puesto que $E = \{2, 4, 6\}$, se observa que $p(E) = p_2 + p_4 + p_6 = \frac{1}{12} + \frac{1}{6} + \frac{1}{12}$ o $\frac{1}{3}$. De manera similar, puede determinarse la probabilidad de cualquier evento en A. ◆

Se ve así, que el problema de asignar probabilidades a todos los eventos de manera congruente puede reducirse al problema de encontrar números $p_1, p_2, \ldots, p_n$ que satisfagan a EP1 y EP2. Una vez más, matemáticamente hablando, no hay otras restricciones sobre las p_k. Sin embargo, si la estructura matemática que resulta se requiere que sea útil para una situación particular, entonces las p_k deben reflejar el comportamiento real que ocurre en esa situación.

Resultados igualmente probables

Supóngase que tienen iguales probabilidades de ocurrir todos los resultados en un espacio muestral finito A. Ésta es, desde luego, una suposición y por tanto no puede comprobarse. Se haría una suposición de esta naturaleza si la evidencia experimental o la simetría indicaran su pertinencia en una situación particular (véase el ejemplo 7). En realidad, estas situaciones son bastante comunes. Se acostumbra usar algo de terminología adicional. En ocasiones, los experimentos implican la elección de un objeto, en una forma no determinista, de alguna colección. Si se hace la selección de tal manera que todos los objetos tengan igual probabilidad de ser escogidos, se dice que se ha hecho una **selección aleatoria** o que se ha **escogido un objeto al azar** de la colección. A menudo se usará esta terminología para especificar ejemplos de experimentos con resultados igualmente probables.

Supóngase que $|A| = n$ y que estos n resultados sean igualmente probables. Entonces las probabilidades elementales son todas iguales, y como deben sumar 1, esto significa que cada probabilidad elemental es $1/n$. Ahora sea E un evento que contiene k resultados, por ejemplo $E = \{x_1, x_2, \ldots, x_k\}$. Puesto que todas las probabilidades elementales son $1/n$, se debe tener

$$p(E) = \underbrace{\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n}}_{k \text{ sumandos}} = \frac{k}{n}$$

Como $k = |E|$, se tiene el siguiente principio: Si todos los resultados son igualmente probables, entonces para cada evento E

$$p(E) = \frac{|E|}{|A|} = \frac{\text{número total de resultados en } E}{\text{número total de resultados}}.$$

En este caso, el cálculo de probabilidades se reduce a contar números de elementos en conjuntos. Por esta razón, los métodos de conteo analizados en las secciones anteriores de este capítulo son bastante útiles.

Ejemplo 9. Escoja 4 cartas al azar, de una baraja legal de 52 cartas. ¿Cuál es la probabilidad de que se escoja cuatro reyes?

Solución: Los resultados de este experimento son manos de 4 cartas; cada una tiene iguales probabilidades de ser escogida. El número de manos de 4 cartas es ${}_{52}C_4$, o sea 270,725. Sea E el evento de que todas las cartas sean reyes. El evento E contiene sólo un resultado. En consecuencia $p(E) = \frac{1}{270{,}725}$, o sea aproximadamente 0.000003694. Éste es un evento sumamente improbable. ◆

Ejemplo 10. Una caja contiene seis bolas rojas y cuatro bolas verdes. De la caja se toma cuatro bolas al azar. ¿Cuál es la probabilidad de que dos de las bolas que se haya tomado sean rojas y dos sean verdes?

Solución: El número total de resultados es el número de maneras de seleccionar cuatro objetos de entre diez, sin considerar el orden. Éste es ${}_{10}C_4$, o sea 210. Ahora el evento E, de que dos de las bolas sean rojas y dos sean verdes, puede concebirse como el resultado de efectuar dos tareas en sucesión.

Tarea 1: Escoja dos bolas rojas de las seis bolas rojas de la caja.
Tarea 2: Escoja dos bolas verdes de las cuatro bolas verdes de la caja.

La tarea 1 puede hacerse de ${}_6C_2$, o sea 15 maneras, y la tarea 2 de ${}_4C_2$, o sea 6 maneras. Por tanto, el evento E puede ocurrir en $15 \cdot 6$ sean 90 maneras, y por lo tanto, $p(E) = \frac{90}{210}$ o $\frac{3}{7}$. ◆

Ejemplo 11. Un dado legal de seis caras es lanzado tres veces y se anota la secuencia resultante de números. ¿Cuál es la probabilidad del evento E de que o los tres números sean iguales o de que ninguno de ellos sea un 4?

Solución: Puesto que se supone que el dado es legal, todos los resultados son igualmente probables. Primero, se calcula el número total de resultados del experimento. Éste es el número de secuencias de longitud 3, permitiendo repeticiones, que puede construirse partiendo del conjunto $\{1, 2, 3, 4, 5, 6\}$. Este número es 6^3, o sea 216.

El evento E no puede describirse como el resultado de efectuar dos tareas sucesivas como en el ejemplo 10. Se puede, empero, escribir E como la unión de dos eventos más simples. Sea F el evento de que los tres números registrados sean iguales, y sea G el evento de que ninguno de los números registrados sea un 4. Entonces $E = F \cup G$. Por el principio de adición (teorema 2, sección 1.2), $|F \cup G| = |F| + |G| - |F \cap G|$.

Hay sólo seis resultados en los que los números son iguales, de modo que $|F|$ es 6. El evento G consta de todas las secuencias de longitud 3 que se puede formar a partir del conjunto $\{1, 2, 3, 5, 6\}$. En consecuencia $|G|$ es 5^3, o sea 125, Finalmente, el evento $F \cap G$ consta de todas las secuencias para las cuales los tres números son iguales y ninguno es 4. Resulta claro que hay cinco maneras de que esto ocurra, de modo que $|F \cap G|$ es 5. Usando el principio de adición, $|E| = |F \cup G| = 6 + 125 - 5$, o sea 126. En consecuencia, se tiene $p(E) = \frac{126}{216}$ o $\frac{7}{12}$. ◆

Ejemplo 12. Considérese de nuevo el experimento del ejemplo 10, sacando 4 bolas al azar de una caja que contiene seis bolas rojas y cuatro bolas verdes.

(a) Si E es el evento en que no más de dos de las bolas sean rojas, calcule la probabilidad de E.

(b) Si F es el evento de que no más de tres de las bolas sean rojas, calcule la probabilidad de F.

Solución: (a) Aquí E puede descomponerse como la unión de eventos mutuamente excluyentes. Sea E_0 el evento de que ninguna de las bolas escogidas sea roja, sea E_1 el evento de que exactamente una de las bolas escogidas sea roja, y sea E_2 el evento de que exactamente dos de las bolas escogidas sean rojas. Entonces E_0, E_1 y E_2 son mutuamente excluyentes y $E = E_0 \cup E_1 \cup E_2$. Usando el principio de la adición dos veces, $|E| = |E_0| + |E_1| + |E_2|$. Si ninguna de las bolas es roja, entonces las cuatro deben ser verdes. Como sólo hay cuatro bolas verdes en la caja, sólo hay una manera de que ocurra el evento E_0. En consecuencia, $|E_0| = 1$. Si una bola es roja, entonces las otras tres deben ser verdes. Para hacer tal elección, se debe escoger una bola roja de un conjunto de seis, y luego tres bolas verdes de un conjunto de cuatro. En consecuencia, el número de resultados en E_1 es $({}_6C_1)({}_4C_3)$ o sea 24.

Exactamente de la misma manera, se puede demostrar que el número de resultados en E_2 es $({}_6C_2)({}_4C_2)$ o sea 90. Entonces $|E| = 1 + 24 + 90$, o sea 115. Por otra parte, el número total de maneras para tomar cuatro bolas de la caja es ${}_{10}C_4$, o sea 210, de modo que $p(E) = \frac{115}{210}$ o $\frac{23}{42}$.

(b) Se podría calcular $|F|$ de la misma manera que se calcula $|E|$ en la parte (a), descomponiendo F en cuatro eventos mutuamente excluyentes. Sin embargo, el análisis sería aún más largo que el de la parte (a). En lugar de desarrollarlo, se opta por ilustrar otro enfoque que con frecuencia es útil.

Sea $\overline{F}$ el evento complementario de F. Como F y $\overline{F}$ son mutuamente excluyentes y su unión es el espacio muestral, se debe tener $p(F) + p(\overline{F}) = 1$. Esta fórmula es válida para cualquier evento F y se utiliza cuando es más fácil de analizar el evento complementario. Tal es el caso aquí, en vista de que $\overline{F}$ es el evento de que todas las bolas escogidas sean rojas. Estas cuatro bolas rojas pueden ser escogidas de las seis bolas rojas en ${}_6C_4$ o sea 15 maneras, de modo que $p(\overline{F}) = \frac{15}{210}$ o $\frac{1}{14}$. Esto significa que $p(F) = 1 - \frac{1}{14}$ o $\frac{13}{14}$. ◆

GRUPO DE EJERCICIOS 3.4

En los ejercicios 1 *al* 6, *describa el espacio muestral relacionado.*

1. En una clase de 10 estudiantes, el instructor registra el número de alumnos presentes en un día dado.

2. Una moneda es lanzada tres veces al aire y se registra la secuencia de caras y cruces.

3. Una compañía de investigación de mercados realiza un estudio en el que se clasifica a las personas de acuerdo con las siguentes características.

   Género: masculino (m).o femenino (f)
   Nivel de ingresos: bajo (l), intermedio (m), alto (u)
   Fumador: sí (y), no (n)

   Se selecciona una persona al azar y se clasifica de acuerdo con lo anterior.

4. Se selecciona dos letras simultáneamente al azar de entre las letras a, b, c, d.

5. Una urna de plata y otra de cobre contienen bolas azules, rojas y verdes. Se escoge una urna al azar y luego se toma una bola al azar de esta urna.

6. Una caja contiene 12 objetos, 4 de los cuales están defectuosos. Se toma al azar un objeto y no se repone. Así se continúa, hasta haber sacado los cuatro objetos defectuosos. Se registra el número total de objetos tomados de la caja.

7. (a) Supóngase que el espacio muestral de un experimento es $\{1, 2, 3\}$. Determine todos los eventos posibles.
   (b) Sea S un espacio muestral que contiene n elementos. ¿Cuántos eventos hay para el experimento asociado?

8. Un experimento consiste en lanzar un dado y registrar el número de la cara superior. Determine cada uno de los eventos siguientes.
   (a) E: El número obtenido es por lo menos 4.
   (b) F: El número obtenido es menor que 3.
   (c) G: El número obtenido es divisible entre 3 o es primo.

9. De una baraja normal se toma una carta al azar. Sean E, F y G los siguientes eventos.

   E: La carta es negra.

   F: La carta es un diamante.

   G: La carta es un as.

   Describa los eventos siguientes mediante oraciones completas.
   (a) $E \cup G$ (b) $E \cap G$ (c) $\overline{E} \cap G$
   (d) $E \cup F \cup G$ (e) $E \cup \overline{F} \cup G$

10. Se lanza dos veces un dado y se anota en secuencia los números que aparecen en las caras superiores. Determine los elementos en cada uno de los eventos dados.
    (a) Por lo menos uno de los numeros es un 5.
    (b) Por lo menos uno de los números es un 8.
    (c) La suma de los números es menor que 7.
    (d) La suma de los números es mayor que 8.

11. Se lanza un dado y se registra el número que aparece en la cara superior. Sean E, F y G los siguientes eventos.

    E: El número es por lo menos 3.

    F: El número es cuando más 3.

    G: El número es divisible entre 2.

    (a) ¿Son E y F mutuamente excluyentes? Justifique su respuesta.
    (b) ¿Son F y G mutuamente excluyentes? Justifique su respuesta.
    (c) ¿Es $E \cup F$ el evento seguro? Justifique su respuesta.
    (d) ¿Es $E \cap F$ el evento imposible? Justifique su respuesta.

12. Sea E un evento para un experimento con espacio muestral A. Demuestre que
    (a) $E \cup \overline{E}$ es el evento seguro.
    (b) $E \cap \overline{E}$ es el evento imposible.

13. Un equipo médico clasifica a las personas de acuerdo con las siguientes características.

    Hábitos de bebida: bebe (d), se abstiene (a)

    Nivel de ingresos: bajo (l), intermedio (m), alto (u)

    Hábitos de fumar: fumador (s), no fumador (n)

    Sean E, F y G los siguientes eventos.

    E: Una persona bebe.

    F: El nivel de ingresos de una persona es bajo.

    G: Una persona fuma.

    Haga una lista de los elementos de cada uno de los siguientes eventos.
    (a) $E \cup F$ (b) $E \cap F$ (c) $(E \cup G) \cap F$

14. Sea $S - \{1, 2, 3, 4, 5, 6\}$ el espacio muestral de un experimento, y sean

    $$E = \{1, 3, 4, 5\}, \qquad F = \{2, 3\}, \qquad G = \{4\}.$$

    (a) Calcule los eventos $E \cup F$, $E \cap F$, y $\overline{F}$.
    (b) Calcule los siguientes eventos: $\overline{E} \cup F$ y $\overline{F} \cap G$.

En los ejercicios 15 *y* 16, *haga una lista de los eventos elementales para el experimento dado.*

15. Se selecciona una vocal al azar del conjunto de todas las vocales $\{a, e, i, o, u\}$.

16. Se toma una carta al azar de una baraja legal, y se registra si la carta es un trébol, espada, diamante o corazón.

17. Al lanzar un cierto dado defectuoso, los números del 1 al 6 aparecerán en la cara superior con las siguientes probabilidades:

$$p_1 = \frac{2}{18},\quad p_2 = \frac{3}{18},\quad p_3 = \frac{4}{18},\quad p_4 = \frac{3}{18},$$
$$p_5 = \frac{4}{18},\quad p_6 = \frac{2}{18}.$$

Determine la probabilidad de que
(a) aparezca en la cara superior un número impar.
(b) aparezca en la cara superior un número primo.
(c) aparezca un número menor que 5 en la cara superior.
(d) aparezca un número mayor que 3 en la cara superior.

18. Repita el ejercicio 17 suponiendo que el dado no esté defectuoso.

19. Supóngase que E y F son eventos mutuamente excluyentes, tales que $p(E) = 0.3$ y $p(F) = 0.4$. Determine la probabilidad de que
(a) no ocurra E. (b) ocurran E y F.
(c) ocurran E o F.
(d) no ocurra E o no ocurra F.

20. Considérese un experimento con espacio muestral $A = \{x_1, x_2, x_3, x_4\}$ para el cual

$$p_1 = \frac{2}{7},\quad p_2 = \frac{3}{7},\quad p_3 = \frac{1}{7},\quad p_4 = \frac{1}{7}.$$

Determine la probabilidad del evento dado.
(a) $E = \{x_1, x_2\}$ (b) $F = \{x_1, x_3, x_4\}$

21. Hay cuatro candidatos para presidente, A, B, C y D Supóngase que A tiene el doble de probabilidades de ser elegido que B; B es tres veces más probable que C, y C y D tienen igual probabilidad de ser elegidos. ¿Cuál es la probabilidad de ser electo que tiene cada uno de los candidatos?

22. El resultado de un cierto juego de azar es un entero del 1 al 5. Los enteros 1, 2 y 3 tienen igual probabilidad de ocurrir, y los enteros 4 y 5 tienen también iguales probabilidades de ocurrir. La probabilidad de que el resultado sea mayor que 2 es $\frac{1}{2}$. Determine la probabilidad de cada resultado posible.

23. Una moneda legal es lanzada cinco veces al aire. ¿Cuál es la probabilidad de obtener tres caras y dos cruces?

24. Una mujer tiene cinco pares de guantes en un cajón. Si escoge dos guantes al azar ¿Qué probabilidad existe de que los guantes sean de un mismo par?

25. Supóngase que se lanza un dado legal y que se anota el número que aparece en su cara superior. Sean E, F y G los siguientes eventos.

$$E: \{1, 2, 3, 5\},\qquad F: \{2, 4\},\qquad G: \{1, 4, 6\}.$$

Calcule la probabilidad del evento que se indica.
(a) $E \cup F$ (b) $E \cap F$ (c) $\overline{E} \cap F$
(d) $E \cup G$ (e) $\overline{E} \cup \overline{G}$ (f) $\overline{E} \cap \overline{F}$

26. Supóngase que se lanza dos dados y que se anota los números que aparecen en sus caras superiores. ¿Cuál es la probabilidad de que
(a) se obtenga un 4?
(b) se obtenga un número primo?
(c) la suma de los números sea menor que 5?
(d) la suma de los números sea por lo menos 7?

27. Supóngase que se toma dos cartas al azar de una baraja legal de 52 cartas. ¿Cuál es la probabilidad de que ambas cartas sean menores que 10 y de que ninguna de ellas sea roja?

28. Supóngase que se saca tres bolas al azar de una urna que contiene siete bolas rojas y cinco bolas negras. Calcule la probabilidad de que
(a) las tres bolas sean rojas.
(b) por lo menos dos bolas sean negras.
(c) cuando mucho dos bolas sean negras.
(d) por lo menos una bola sea roja.

29. Un canasto contiene tres manzanas, cinco plátanos, cuatro naranjas y seis peras. Se toma una fruta al azar de este canasto. Calcule la probabilidad de que
(a) se escoja una manzana o una pera.
(b) la fruta escogida no sea una naranja.

30. Un dado legal es lanzado tres veces seguidas. Encuentre la probabilidad de que los tres números resultantes
(a) incluyan exactamente dos treses.
(b) formen una secuencia creciente.
(c) incluyan por lo menos un 3.
(d) incluyan a lo más un 3.
(e) no incluyan treses.

3.5. Relaciones de recurrencia

Las definiciones recursivas de sucesiones de la sección 1.3 son ejemplos de relaciones de recurrencia. Cuando el problema es encontrar una fórmula explícita para una sucesión definida por recurrencia, la fórmula recursiva es llamada **relación recurrente**. Debe recordarse que para definir una sucesión de forma recursiva, una fórmula recursiva debe ir acompañada de información acerca del comienzo de la sucesión. A esta información se la llama **condición** o **condiciones iniciales** para la sucesión.

Ejemplo 1. a) La relación de recurrencia $a_n = a_{n-1} + 3$ con $a_1 = 4$ define de manera recursiva la sucesión 4, 7, 10, 13, ... La condición inicial es $a_1 = 4$.

(b) La relación de recurrencia $f_n = f_{n-1} + f_{n-2}$, $f_1 = f_2 = 1$, define la **sucesión de Fibonacci** 1, 1, 2, 3, 5, 8, 13, 21, ... Las condiciones iniciales son $f_1 = 1$ y $f_2 = 1$. ◆

Las relaciones de recurrencia aparecen de forma natural en muchos problemas de conteo y en el análisis de problemas de programación.

Ejemplo 2. Supóngase que se desea hacer un impreso de todas las sucesiones de n elementos que se puede hacer a partir del conjunto $\{1, 2, 3, \ldots, n\}$. Un enfoque a este problema es proceder de manera recursiva como sigue.

PASO 1. Haga una lista de todas las sucesiones que pueda formarse a partir de $\{1, 2, 3, \ldots, n-1\}$.

PASO 2. Para cada sucesión del paso 1, inserte n en su oportunidad en cada uno de los n lugares disponibles (en el frente, en el extremo y entre cada par de números de la sucesión), imprima el resultado, y elimine n.

El número de acciones de insertar-imprimir-eliminar es el número de sucesiones de n elementos. También claramente es n veces el número de sucesiones producidas en el paso 1. En consecuencia, se tiene

$$\text{número de secuencias de } n \text{ elementos} = n \times (\text{número de secuencias } (n-1)).$$

Esto da una fórmula recursiva para el número de secuencias de n elementos. ¿Cuál es la condición inicial? ◆

Una técnica para encontrar una fórmula explícita para la sucesión definida por una relación de recurrencia es el **análisis hacia atrás** (o **análisis de regreso**), como se ilustra en el ejemplo siguiente.

Ejemplo 3. La relación de recurrencia $a_n = a_{n-1} + 3$ con $a_1 = 2$ define la sucesión 2, 5, 8, ... Se efectúa un análisis hacia atrás al valor de a_n sustituyendo la definición de a_{n-1}, a_{n-2} y así sucesivamente, hasta tener un esquema claro

$$\begin{aligned} a_n &= a_{n-1} + 3 \\ &= (a_{n-2} + 3) + 3 \\ &= ((a_{n-3} + 3) + 3) + 3 \end{aligned} \qquad \text{o bien} \qquad \begin{aligned} a_n &= a_{n-1} + 3 \\ &= a_{n-2} + 2 \cdot 3 \\ &= a_{n-3} + 3 \cdot 3. \end{aligned}$$

En algún momento, este proceso producirá

$$\begin{aligned} a_n &= a_{n-(n-1)} + (n-1)\cdot 3 \\ &= a_1 + (n-1)\cdot 3 \\ &= 2 + (n-1)\cdot 3. \end{aligned}$$

Una fórmula explícita para la sucesión es $a_n = 2 + (n-1)3$. Verifique esto. ◆

Ejemplo 4. Haga un análisis hacia atrás para encontrar una fórmula explícita para la sucesión definida por la relación de recurrencia $b_n = 2b_{n-1} + 1$ con condición inicial $b_1 = 7$.

Solución: Se comienza por sustituir la definición del término anterior en la fórmula de definición.

$$\begin{aligned} b_n &= 2b_{n-1} + 1 \\ &= 2(2b_{n-2} + 1) + 1 \\ &= 2[2(2b_{n-3} + 1) + 1] + 1 \\ &= 2^3 b_{n-3} + 4 + 2 + 1 \\ &= 2^3 b_{n-3} + 2^2 + 2^1 + 1. \end{aligned}$$

Está presentándose un esquema con estas reexpresiones de b_n. (*Nota:* No hay reglas establecidas para la manera de volver a escribir estas expresiones y puede ser necesaria una cierta cantidad de experimentación.) El análisis hacia atrás terminará en

$$\begin{aligned} b_n &= 2^{n-1} b_{n-(n-1)} + 2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2^1 + 1 \\ &= 2^{n-1} b_1 + 2^{n-1} - 1 \quad \text{Utilizando el ejercicio 3, sección 2.4} \\ &= 7 \cdot 2^{n-1} + 2^{n-1} - 1. \end{aligned}$$

◆

Dos reglas útiles de suma han quedado demostradas en los ejercicios de la sección 2.4. Son transcritas de nuevo para usarlas en esta sección.

$$\text{S1:} \quad 1 + a + a^2 + a^3 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}.$$

$$\text{S2:} \quad 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

El análisis hacia atrás puede no revelar un esquema explícito para la sucesión definida por una relación de recurrencia. Se proporcionará, ahora, una técnica más general para resolver una relación de recurrencia. Primero, se da una definición. Una relación de recurrencia es una **relación lineal homogénea de grado *k*** si es de la forma

$$a_n = r_1 a_{n-1} + r_2 a_{n-2} + \cdots + r_k a_{n-k}, \quad \text{en donde las } r \text{ son constantes.}$$

Ejemplo 5

(a) La relación $c_n = (-2)c_{n-1}$ es una relación de recurrencia lineal homogénea de grado 1.
(b) La relación $a_n = a_{n-1} + 3$ no es una relación de recurrencia lineal homogénea.
(c) La relación de recurrencia $f_n = f_{n-1} + f_{n-2}$ es una relación lineal homogénea de grado 2.
(d) La relación de recurrencia $g_n = g_{n-1}^2 + g_{n-2}$ no es una relación lineal homogénea. ◆

Para una relación de recurrencia lineal homogénea de grado k, $a_n = r_1 a_{n-1} + r_2 a_{n-2} + \cdots + r_k a_{n-k}$, se llama al polinomio asociado de grado k, $x^k = r_1 x^{k-1} + r_2 x^{k-2} + \cdots + r_k$, su **ecuación característica**. Las raíces de la ecuación característica desempeñan un papel clave en la fórmula explícita para la sucesión definida por la relación de recurrencia y las condiciones iniciales. Si bien el problema puede resolverse en general, se proporciona un teorema para el grado 2 solamente. En este caso es común escribir la ecuación característica como $x^2 - r_1 x - r_2 = 0$.

Teorema 1

(a) *Si la ecuación característica $x^2 - r_1 x - r_2 = 0$ de la relación de recurrencia $a_n = r_1 a_{n-1} + r_2 a_{n-2}$ tiene dos raíces distintas, s_1 y s_2, entonces $a_n = us_1^n + vs_2^n$, en donde u y v dependen de las condiciones iniciales, es la fórmula explícita para la sucesión.*
(b) *Si la ecuación característica $x^2 - r_1 x - r_2 = 0$ tiene una sola raíz s, entonces la fórmula explícita es $a_n = us^n + vns^n$, en donde u y v dependen de las condiciones iniciales.*

Demostración: (a) Supóngase que $s_1^2 - r_1 s_1 - r_2 = 0$, $s_2^2 - r_1 s_2 - r_2 = 0$, y $a_n = us_1^n + vs_2^n$, para $n \geq 1$. Se demuestra, entonces, que esta definición de a_n define la misma sucesión que $a_n = r_1 a_{n-1} + r_2 a_{n-2}$. Primero, se observa que u y v han sido escogidas de tal manera que $a_1 = us_1 + vs_2$ y $a_2 = us_1^2 + vs_2^2$ y las condiciones iniciales quedan satisfechas. Entonces

$$\begin{aligned} a_n &= us_1^n + vs_2^n && \text{Descomponga } s_1^2 \text{ y } s_2^2. \\ &= us_1^{n-2}s_1^2 + vs_2^{n-2}s_2^2 && \text{Sustituya por } s_1^2 \text{ y } s_2^2. \\ &= us_1^{n-2}(r_1 s_1 + r_2) + vs_2^{n-2}(r_1 s_2 + r_2) \\ &= r_1 us_1^{n-1} + r_2 us_1^{n-2} + r_1 vs_2^{n-1} + r_2 vs_2^{n-2} \\ &= r_1(us_1^{n-1} + vs_2^{n-1}) + r_2(us_1^{n-2} + vs_2^{n-2}) \\ &= r_1 a_{n-1} + r_2 a_{n-2} && \text{Use las definiciones de } a_{n-1} \text{ y } a_{n-2}. \end{aligned}$$

(b) Esta parte puede demostrarse en forma similar. ●

Ejemplo 6. Encuentre una fórmula explícita para la sucesión definida por $c_n = 3c_{n-1} - 2c_{n-2}$ con las condiciones iniciales $c_1 = 5$ y $c_2 = 3$.

Solución: La relación de recurrencia $c_n = 3c_{n-1} - 2c_{n-2}$ es una relación lineal homogénea de grado 2. Su ecuación asociada es $x^2 = 3x - 2$. Volviendo a escribir ésta como $x^2 - 3x + 2 = 0$, se observa que hay dos raíces, 1 y 2. El teorema 1 dice que se puede encontrar u y v de manera que $c_1 = u(1) + v(2)$ y $c_2 = u(1)^2 + v(2)^2$. Resolviendo este sistema 2×2 se obtiene que u es 7 y v es -1.

Por el teorema 1, se obtiene $c_n = 7 \cdot 1^n + (-1) \cdot 2^n$ o sea, $c_n = 7 - 2^n$. Nótese que usando $c_n = 3c_{n-1} - 2c_{n-2}$, con las condiciones iniciales $c_1 = 5$ y $c_2 = 3$, se obtiene 5, 3, -1 y -9 como los primeros cuatro términos de la sucesión. La fórmula $c_n = 7 - 2^n$ da lugar también a 5, 3, -1 y -9 como los primeros cuatro términos. ◆

Ejemplo 7. Resuelva la relación de recurrencia $d_n = 2d_{n-1} - d_{n-2}$ con condiciones iniciales $d_1 = 1.5$ y $d_2 = 3$.

Solución: La ecuación asociada para esta relación lineal homogénea es $x^2 - 2x + 1 = 0$. Esta ecuación tiene una raíz (múltiple), 1 . En consecuencia, por el teorema 1(b), $d_n = u(1)^n + vn(1)^n$. Usando esta fórmula y las condiciones iniciales $d_1 = 1.5 = u + v(1)$ y $d_2 = 3 = u + v(2)$, se encuentra que u es 0 y v es 1.5. Entonces $d_n = 1.5n$. ◆

La sucesión de Fibonacci del ejemplo 1(b) es una sucesión muy conocida; se necesitó doscientos años para encontrar su fórmula explícita.

Ejemplo 8. La sucesión de Fibonacci se define como una relación de recurrencia lineal homogénea de grado 2, de manera que, por el teorema 1, son necesarias las raíces de la ecuación característica para describir la fórmula explícita para la sucesión. De $f_n = f_{n-1} + f_{n-2}$ y $f_1 = f_2 = 1$, se tiene $x^2 - x - 1 = 0$. Utilizando la fórmula cuadrática para obtener las raíces, se encuentra $s_1 = \frac{1+\sqrt{5}}{2}$ y $s_2 = \frac{1-\sqrt{5}}{2}$. Queda por determinar las u y v del teorema 1. Se resuelven las ecuaciones

$$1 = u\left(\frac{1+\sqrt{5}}{2}\right) + v\left(\frac{1-\sqrt{5}}{2}\right) \quad \text{y} \quad 1 = u\left(\frac{1+\sqrt{5}}{2}\right)^2 + v\left(\frac{1-\sqrt{5}}{2}\right)^2.$$

Para las condiciones iniciales dadas, u es $\frac{1}{\sqrt{5}}$ y v es $-\frac{1}{\sqrt{5}}$. La fórmula explícita para la sucesión de Fibonacci es

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$ ◆

GRUPO DE EJERCICIOS 3.5

En los ejercicios 1 *al* 6, *identifique la relación de recurrencia dada como lineal homogénea o no. Si la relación es lineal homogénea, indique su grado.*

1. $a_n = 2.5a_{n-1}$

2. $b_n = -3b_{n-1} - 2b_{n-2}$

3. $c_n = 2^n c_{n-1}$

4. $d_n = nd_{n-1}$

5. $e_n = 5e_{n-1} + 3$

6. $g_n = \sqrt{g_{n-1} + g_{n-2}}$

En los ejercicios 7 *al* 12, *utilice la técnica del análisis hacia atrás a fin de encontrar una fórmula explícita para la sucesión definida por la relación de recurrencia y la o las condiciones iniciales.*

7. $a_n = 2.5a_{n-1},\ a_1 = 4$

8. $b_n = 5b_{n-1} + 3,\ b_1 = 2$

9. $c_n = c_{n-1} + n,\ c_1 = 4$

10. $d_n = -1.1d_{n-1},\ d_1 = 5$

11. $c_n - c_{n-1} - 2,\ e_1 = 0$

12. $g_n = ng_{n-1},\ g_1 = 6$

En los ejercicios 13 *al* 18, *resuelva cada una de las relaciones de recurrencia.*

13. $a_n = 4a_{n-1} + 5a_{n-2},\ a_1 = 2,\ a_2 = 6$

14. $b_n = -3b_{n-1} - 2b_{n-2},\ b_1 = -2,\ b_2 = 4$

15. $c_n = -6c_{n-1} - 9c_{n-2},\ c_1 = 2.5,\ c_2 = 4.7$

16. $d_n = 4d_{n-1} - 4d_{n-2},\ d_1 = 1,\ d_2 = 7$

17. $e_n = 2e_{n-2},\ e_1 = \sqrt{2},\ e_2 = 6$

18. $g_n = 2g_{n-1} - 2g_{n-2},\ g_1 = 1,\ g_2 = 4$

19. Desarrolle una fórmula explícita general para una relación de recurrencia no homogénea de la forma $a_n = ra_{n-1} + s$, en donde r y s son constantes.

20. Confirme que la fórmula explícita del ejemplo 8 produce la sucesión de Fibonacci dada en el ejemplo 1(b) al calcular los primeros cinco términos de la sucesión.

IDEAS CLAVE PARA REPASO

- Teorema (principio de multiplicación del conteo): Supóngase que debe efectuarse dos tareas, T_1 y T_2 sucesivamente. Si T_1 puede efectuarse de n_1 maneras y para cada una de estas maneras, T_2 puede realizarse de n_2 maneras, entonces la sucesión T_1T_2 puede efectuarse en n_1n_2 maneras.
- Teorema (principio extendido de la multiplicación): véase la página 73.
- Teorema: Sea A un conjunto con n elementos y $1 \leq r \leq n$. Entonces el número de sucesiones de longitud r que puede formarse con n elementos de A, permitiendo repeticiones, es n^r.
- Permutación de n objetos tomados r a la vez $(1 \leq r \leq n)$: una sucesión de longitud r formada de elementos distintos.
- Teorema: Si $1 \leq r \leq n$, entonces ${}_nP_r$, el número de permutaciones de n objetos tomados r a la vez, es $n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)$ o sea $\frac{n!}{(n-r)!}$.
- Permutación: un arreglo de n elementos de un conjunto A en una sucesión de longitud n.
- Teorema: El número de permutaciones distinguibles que puede formarse a partir de una colección de n objetos en donde el primer objeto aparece k_1 veces, el segundo objeto k_2 veces, y así sucesivamente, es $\frac{n!}{k_1!k_2!\cdots k_t!}$.
- Combinación de n objetos tomados r a la vez: un subconjunto de r elementos tomados de un conjunto con n elementos.
- Teorema: Sea A un conjunto con $|A| = n$ y sea $1 < r \leq n$. Entonces ${}_nC_r$, el número de combinaciones de los elementos de A, tomados r a la vez, es $\frac{n!}{r!(n-r)!}$.
- Teorema: Supóngase que se va a hacer k selecciones de n objetos sin considerar el orden y que se permite repeticiones, suponiendo por lo menos k copias de cada uno de los n objetos. El número de maneras en que puede hacerse estas selecciones es ${}_{(n+k-1)}C_k$.
- El principio de las casillas: véase la página 82.
- El principio de las casillas extendido: véase la página 84.
- Espacio muestral: el conjunto de todos los resultados de un experimento.
- Evento: un subconjunto del espacio muestral.
- Evento seguro: un evento que ocurrirá con seguridad.
- Evento imposible: el subconjunto vacío del espacio muestral.
- Eventos mutuamente excluyentes: dos eventos cualesquiera E y F con $E \cap F = \{\ \}$.
- f_E: la frecuencia de ocurrencia del evento E en n intentos.
- $p(E)$: la probabilidad del evento E.
- Espacio de probabilidad: véase la página 89.
- Evento elemental: un evento que consta de un solo resultado.
- Selección aleatoria: véase la página 90.
- Relación de recurrencia: una fórmula recursiva para una sucesión.
- Condiciones iniciales: información acerca del comienzo de una sucesión definida de manera recursiva.
- Relación lineal homogénea de grado k: una relación de recurrencia de la forma

$$a_n = r_1a_{n-1} + r_2a_{n-2} + \cdots + r_ka_{n-k}$$

en donde las r_i son constantes.
- Ecuación característica: véase la página 97.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes casos, escriba el programa o la subrutina que se solicita en seudocódigo (como se describe en el apéndice A) o en un lenguaje de programación que usted conozca. Pruebe su código ya sea con una prueba de escritorio o con una ejecución en computadora.

1. Escriba una subrutina que acepte dos enteros positivos n y r y, si $r \leq n$, regrese el número de permutaciones de n objetos tomados r a la vez.

2. Escriba un programa que tenga como entrada los enteros positivos n y r y, si $r \leq n$, imprima las permutaciones de $1, 2, 3, \ldots, n$ tomadas r a la vez.

3. Escriba una subrutina que acepte dos enteros positivos n y r y, si $r \leq n$, regrese el número de combinaciones de n objetos tomados r a la vez.

4. Escriba un programa que tenga como entrada los enteros positivos n y r, y, si $r \leq n$, imprima las combinaciones de $1, 2, 3, \ldots, n$ tomados r a la vez.

5. (a) Escriba una subrutina recursiva que con entrada k imprima los primeros k-números de Fibonacci.
   (b) Escriba una subrutina no recursiva que con entrada k imprima el k-ésimo número de Fibonacci.

CAPÍTULO 4

RELACIONES Y DIGRAFOS

Requisitos previos: Capítulos 1 y 2

Las relaciones entre personas, números, conjuntos y muchas otras entidades pueden formalizarse en la idea de una relación binaria. En este capítulo se desarrolla el concepto de relación binaria, y se estudia varios métodos geométricos y algebraicos para representar tales objetos. También se estudia una variedad de propiedades que una relación binaria puede poseer, y se proporciona importantes ejemplos, como las relaciones de equivalencia. Por último, se presenta varios tipos de manipulaciones algebraicas útiles que puede realizarse en las relaciones binarias. Estas manipulaciones son analizadas tanto desde el punto de vista teórico como del computacional.

4.1. Conjuntos producto y particiones

Conjuntos producto

Un **par ordenado** (o **pareja ordenada**) (a, b) es un listado de los objetos a y b en un orden prescrito, donde a aparece en primer término y b, en segundo. En consecuencia, un par ordenado (o pareja ordenada) simplemente es una secuencia de longitud 2. A partir del análisis anterior de las secuencias (véase la sección 1.3), se desprende que los pares ordenados (a_1, b_1) y (a_2, b_2) son iguales si y solamente si $a_1 = a_2$ y $b_1 = b_2$.

Si A y B son dos conjuntos no vacíos, se define el **conjunto producto** o **producto cartesiano** $A \times B$ como el conjunto de todos los pares ordenados (a, b) con $a \in A$ y $b \in B$. Así,

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

Ejemplo 1. Sean

$$A = \{1, 2, 3\} \quad \text{y} \quad B = \{r, s\},$$

entonces

$$A \times B = \{(1, r), (1, s), (2, r), (2, s), (3, r), (3, s)\}.$$

Observe que los elementos de $A \times B$ pueden ser dispuestos en forma tabular conveniente como se muestra en la figura 4.1. ◆

$A \backslash B$	r	s
1	$(1, r)$	$(1, s)$
2	$(2, r)$	$(2, s)$
3	$(3, r)$	$(3, s)$

Figura 4.1

Ejemplo 2. Si A y B son como en el ejemplo 1, entonces

$$B \times A = \{(r, 1), (s, 1), (r, 2), (s, 2), (r, 3), (s, 3)\}.$$ ◆

De los ejemplos 1 y 2, se ve que $A \times B$ no necesita ser igual a $B \times A$.

Teorema 1. Para dos conjuntos finitos no vacíos cualesquiera A y B, $|A \times B| = |A||B|$.

Demostración: Supóngase que $|A| = m$ y $|B| = n$. Para formar un par ordenado (o pareja ordenada) (a, b), $a \in A$ y $b \in B$, se debe realizar dos tareas sucesivas. La tarea 1 consiste en escoger un primer elemento del conjunto A, y la tarea 2, en escoger un segundo elemento de B. Hay m maneras de efectuar la tarea 1 y n maneras de efectuar la tarea 2; por tanto, por el principio de la multiplicación (véase la sección 3.1), existen $m \times n$ maneras de formar un par ordenado (o pareja ordenada) (a, b). En otras palabras, $|A \times B| = m \cdot n = |A||B|$. ●

Ejemplo 3. Si $A = B = \mathbb{R}$, el conjunto de todos los números reales, entonces $\mathbb{R} \times \mathbb{R}$, también denotado por $\mathbb{R}^2$, es el conjunto de todos los puntos del plano. El par ordenado (o pareja ordenada) (a, b) da las coordenadas de un punto del plano. ◆

Ejemplo 4. Una compañía de investigación de mercados clasifica a una persona de acuerdo con los siguientes dos criterios:

Género: masculino (m); femenino (f)
Máximo nivel de educación terminado: escuela primaria (e); secundaria (h); universidad (c); posgrado (g)

Sean $S = \{m, f\}$ y $L = \{e, h, c, g\}$. Entonces, el conjunto producto $S \times L$ contiene todas las categorías en las que se clasifica la población. En consecuencia, la clasificación (f, g) representa una mujer que ha terminado alguna especialización, es decir, un posgrado. Hay ocho categorías en este esquema de clasificación. ◆

Ahora se define el producto cartesiano de tres o más conjuntos vacíos generalizando la definición anterior del producto cartesiano de dos conjuntos. Es decir, el **producto cartesiano** $A_1 \times A_2 \times \cdots \times A_m$ de los conjuntos no vacíos $A_1, A_2, \ldots, A_m$ es el conjunto de todas las m-uplas ordenadas $(a_1, a_2, \ldots, a_m)$, en donde $a_i \in A_i$, $i = 1, 2, \ldots, m$. En consecuencia

$$A_1 \times A_2 \times \cdots \times A_m = \{(a_1, a_2, \ldots, a_m) \mid a_i \in A_i, i = 1, 2, \ldots, m\}.$$

Ejemplo 5. Una compañía de programas de computación proporciona las tres características siguientes para cada programa que vende:

Lenguaje: FORTRAN (f); PASCAL (p); LISP (l)
Memoria: 2 megas (2); 4 megas (4); 8 megas (8)
Sistema operativo: UNIX (u); DOS (d)

Sea $L = \{f, p, l\}$, $M = \{2, 4, 8\}$ y $O = \{u, d\}$. Entonces el producto cartesiano $L \times M \times O$ contiene todas las categorías que describen un programa. Hay $3 \cdot 3 \cdot 2$ o sea 18 categorías en este esquema de clasificación. ◆

Procediendo de manera similar a la que se siguió para demostrar el teorema 1, usando el principio de multiplicación ampliado, se puede demostrar que si A_1 tiene n_1 elementos, A_2 tiene n_2 elementos, ..., y A_m tiene n_m elementos, entonces $A_1 \times A_2 \times \cdots \times A_m$ tiene $n_1 \cdot n_2 \cdots n_m$ elementos.

Particiones

Una **partición** o **conjunto cociente** de un conjunto no vacío A es una colección $\mathcal{P}$ de subconjuntos no vacíos de A tales que

1. Cada elemento de A pertenece a uno de los conjuntos en $\mathcal{P}$.
2. Si A_i y A_j son elementos distintos de $\mathcal{P}$, entonces $A_i \cap A_j = \varnothing$.

Los conjuntos que hay en $\mathcal{P}$ se llaman **bloques** o **celdas** de la partición. La figura 4.2 muestra una partición $\mathcal{P} = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7\}$ de A en siete bloques.

Ejemplo 6. Sea

$$A = \{a, b, c, d, e, f, g, h\}.$$

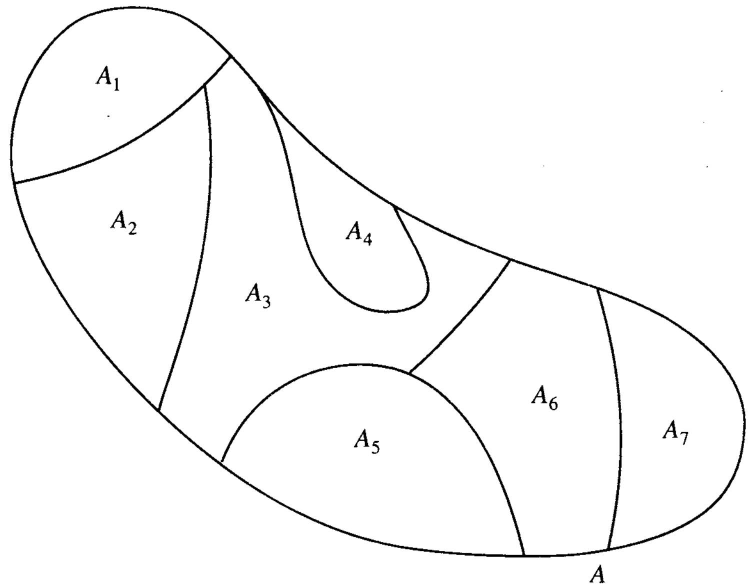


Figura 4.2

Considérense los siguientes subconjuntos de A:

$$A_1 = \{a, b, c, d\}, \quad A_2 = \{a, c, e, f, g, h\}, \quad A_3 = \{a, c, e, g\},$$

$$A_4 = \{b, d\}, \quad A_5 = \{f, h\}.$$

Entonces $\{A_1, A_2\}$ no es una partición ya que $A_1 \cap A_2 \neq \emptyset$. También, $\{A_1, A_5\}$ no es una partición, en vista de que $e \in A_1$ y $e \in A_5$. La colección $\mathscr{P} = \{A_3, A_4, A_5\}$ es una partición de A. ◆

Ejemplo 7. Considérese el conjunto A de todos los empleados de General Motors. Si se forma subconjuntos de A agrupando en cada subconjunto a todos los empleados que tienen exactamente el mismo salario, se obtiene una partición de A. Cada empleado pertenecerá a exactamente un subconjunto. ◆

Ejemplo 8. Sean

Z = conjunto de todos los enteros,
A_1 = conjunto de todos los enteros pares, y
A_2 = conjunto de todos los enteros impares.

Entonces $\{A_1, A_2\}$ es una partición de Z. ◆

Puesto que todos los miembros de una partición de un conjunto A son subconjuntos de A, se ve que la partición es un subconjunto de $P(A)$, el conjunto potencia de A. Es decir, puede considerarse las particiones como clases particulares de subconjuntos de $P(A)$.

GRUPO DE EJERCICIOS 4.1

1. En cada parte, encuentre x o y de manera que el enunciado sea verdadero.
(a) $(x, 3) = (4, 3)$
(b) $(a, 3y) = (a, 9)$
(c) $(3x + 1, 2) = (7, 2)$
(d) $(C^{++}, \text{PASCAL}) = (y, x)$

2. En cada parte, encuentre x o y de manera que el enunciado sea verdadero.
(a) $(4x, 6) = (16, y)$
(b) $(2x - 3, 3y - 1) = (5, 5)$
(c) $(x^2, 25) = (49, y)$ (d) $(x, y) = (x^2, y^2)$

3. Sean $A = \{a, b\}$ y $B = \{4, 5, 6\}$. Haga una lista de los elementos en
(a) $A \times B$ (b) $B \times A$
(c) $A \times A$ (d) $B \times B$

4. Sean A = {Fine, Yang} y B = {presidente, vicepresidente, secretario, tesorero}. Dé cada uno de los tres casos siguientes.
(a) $A \times B$ (b) $B \times A$ (c) $A \times A$

5. Un experimento de genética clasifica las moscas de las frutas de acuerdo con los dos siguientes criterios:
Género: masculino (m), femenino (f)
Alas extendidas: cortas (s), medianas (m), largas (l)
(a) ¿Cuántas categorías hay en este esquema de clasificación?
(b) Haga una lista de todas las categorías de este esquema de clasificación.

6. Un fabricante de automóviles hace tres tipos diferentes de chasís (o armazón del auto) y dos tipos de motores.
Tipo de armazón: sedán (s), coupé (c), vagoneta (v)
Tipo de motor: de gas (g), diesel (d)
Elabore una lista de todos los modelos posibles de autos.

7. Si $A = \{a, b, c\}$, $B = \{1, 2\}$, y $C = \{\#, *\}$, anote en una lista todos los elementos de $A \times B \times C$.

8. Si A tiene tres elementos y B tiene $n \geq 1$ elementos, utilice la inducción matemática para demostrar que $|A \times B| = 3n$.

9. Si $A = \{a \mid a$ es el número real$\}$ y $B = \{1, 2, 3\}$, haga un esquema de cada uno de los siguientes casos en el plano cartesiano.
(a) $A \times B$ (b) $B \times A$

10. Si $A = \{a \mid a$ es un número real y $-2 \leq a \leq 3\}$ y $B = \{b \mid b$ es un número real y $1 \leq b \leq 5\}$, haga un esquema de cada uno de los siguientes casos en el plano cartesiano.
(a) $A \times B$ (b) $B \times A$

11. Demuestre que si A_1 tiene n_1 elementos, A_2 tiene n_2 elementos, y A_3 tiene n_3 elementos, entonces $A_1 \times A_2 \times A_3$ tiene $n_1 \cdot n_2 \cdot n_3$ elementos.

12. Si $A \subseteq C$ y $B \subseteq D$, demuestre que $A \times B \subseteq C \times D$.

13. Sean $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ y
$A_1 = \{1, 2, 3, 4\}$, $A_2 = \{5, 6, 7\}$,
$A_3 = \{4, 5, 7, 9\}$, $A_4 = \{4, 8, 10\}$,
$A_5 = \{8, 9, 10\}$, $A_6 = \{1, 2, 3, 6, 8, 10\}$.
¿Cuáles de las siguientes son particiones de A?
(a) $\{A_1, A_2, A_5\}$ (b) $\{A_1, A_3, A_5\}$
(c) $\{A_3, A_6\}$ (d) $\{A_2, A_3, A_4\}$

14. Si A_1 es el conjunto de los enteros positivos y A_2 es el conjunto de todos los enteros negativos, ¿es $\{A_1, A_2\}$ una partición de Z? Explique su conclusión.

15. Si $B = \{0, 3, 6, 9, \ldots\}$, escriba una partición de B que contenga
(a) dos subconjuntos infinitos.
(b) tres subconjuntos infinitos.

16. Haga una lista con todas las particiones de $A = \{1, 2, 3\}$.

17. Haga una lista con todas las particiones de $B = \{a, b, c, d\}$.

18. El número de particiones de un conjunto con n elementos en k subconjuntos satisface la relación de recurrencia

$$S(n, k) = S(n - 1, k - 1) + k \cdot S(n - 1, k)$$

con condiciones iniciales $S(n, 1) = S(n, n) = 1$. Encuentre el número de particiones de un conjunto con cuatro elementos en dos subconjuntos, es decir, $S(4,2)$. Compare su resultado con los resultados del ejercicio 17.

19. Sean A, B, y C subconjuntos de U. Demuestre que $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

20. Utilice los conjuntos $A = \{1, 2, 4\}$, $B = \{2, 5, 7\}$ y $C = \{1, 3, 7\}$ para investigar si $A \times (B \cap C) = (A \times B) \cap (A \times C)$. Explique sus conclusiones.

4.2. Relaciones y digrafos

Relaciones

La noción de una relación entre dos conjuntos de objetos es bastante común e intuitivamente clara (más adelante se dará una definición formal). Si A es el conjunto de todos los seres humanos masculinos vivos y B es el conjunto de todos los seres humanos femeninos vivos, entonces la relación P (padre) puede definirse entre A y B. Así, si $x \in A$ y $y \in B$, entonces x está relacionada con y por la relación P si x es el padre de y, y se escribe $x\,P\,y$. Debido a que aquí interesa el orden, se hace referencia a P como a una relación de A a B. Se podría considerar también las relaciones H y M de A a B suponiendo que $x\,H\,y$ signifique que x es un hijo de y, y que $x\,M\,y$ signifique que x sea el marido de y.

Si A es el conjunto de todos los números reales, hay muchas relaciones de uso común de A a A. Un ejemplo es la relación "menor que", la cual suele denotarse por $<$, de modo que x está relacionada con y si $x < y$, y las demás relaciones de orden $>, \leq$ y $\geq$. Se ve que una relación se describe a menudo verbalmente y puede denotarse por un nombre conocido o un símbolo. El problema que se tiene con este enfoque es que se necesita analizar *cualquier relación posible* de un conjunto abstracto a otro. La mayoría de estas relaciones no tiene una descripción verbal simple ni un nombre o símbolo conocido que recuerde su naturaleza o sus propiedades. Por otra parte, suele ser difícil, y en ocasiones casi imposible, dar algunas demostraciones precisas de las propiedades que satisface una relación, si se tiene que tener una descripción verbal de la misma.

Para salvar este problema, observe que lo único que realmente interesa acerca de una relación es que se sepa con precisión cuáles elementos de A están relacionados con cuáles elementos de B. Así, supóngase que $A = \{1, 2, 3, 4\}$ y que R es la relación de A a A. Si se sabe que $1\,R\,2$, $1\,R\,3$, $1\,R\,4$, $2\,R\,3$, $2\,R\,4$, y $3\,R\,4$, entonces se sabe todo lo que se necesita saber acerca de R. En realidad, R es la relación conocida $<$, "menor que" pero no se necesita saber esto. Sería suficiente con que se diera la lista anterior de pares relacionados. En consecuencia, se puede decir que R es totalmente conocida si se conoce todos los pares relacionados con R. Se podría escribir entonces $R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$, en vista de que R es esencialmente igual a o está completamente especificada por este conjunto de pares ordenados. Cada par ordenado (o pareja ordenada) especifica que su primer elemento está relacionado con su segundo elemento, y se supone que se da, por lo menos en principio, todas las partes relacionadas posibles. Este método de especificar una relación no requiere ningún símbolo o descripción especial y por tanto es adecuado para cualquier relación que exista entre dos conjuntos cualesquiera. Nótese que desde este punto de vista, una relación de A a B simplemente es un subconjunto de $A \times B$ (que da los pares relacionados), y, recíprocamente, cualquier conjunto $A \times B$ puede considerarse una relación, aun cuando sea una relación no conocida para la cual no se tenga nombre ni descripción alternativa. Se escoge este enfoque para definir relaciones.

Sean A y B conjuntos no vacíos. Una **relación R de A a B** es un subconjunto de $A \times B$. Si $R \subseteq A \times B$ y $(a, b) \in R$, se dice que a **está relacionada con** b **por** R, y se escribe también $a\,R\,b$. Si a no está relacionada con b por R, se escribe $a \not R\, b$. Con frecuencia, A y B son iguales. En este caso, se dice a menudo que $R \subseteq A \times A$ **es una relación sobre** A, en lugar de una relación de A a A.

Las relaciones son sumamente importantes en matemáticas y sus aplicaciones. No es una exageración decir que el 90 por ciento de lo que se estudia en el resto de este libro se referirá a algún tipo de objeto que puede considerarse como una relación. Véase a continuación algunos ejemplos.

Ejemplo 1. Sea

$$A = \{1, 2, 3\} \quad \text{y} \quad B = \{r, s\}.$$

Entonces

$$R = \{(1, r), (2, s), (3, r)\}$$

es una relación de A a B. ◆

Ejemplo 2. Sean A y B conjuntos de números reales. Se define la siguiente relación R de (igualdad) de A a B:

$$a\,R\,b \quad \text{si y sólo si} \quad a = b.$$ ◆

Ejemplo 3. Sea

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

Defina la siguiente relación R (menor que) en A:

$$a\,R\,b \quad \text{si y sólo si} \quad a < b.$$

Entonces

$$R = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}.$$ ◆

Ejemplo 4. Sea $A = Z^+$, el conjunto de todos los enteros positivos. Defina la siguiente relación R en A:

$$a\,R\,b \quad \text{si y sólo si } a \text{ divide a } b.$$

Entonces $4\,R\,12$, pero $5 \not R\, 7$. ◆

Ejemplo 5. Sea A el conjunto de toda la gente del mundo. Se define la siguiente relación R sobre A: $a\,R\,b$ si y sólo si hay una secuencia $a_0, a_1, \ldots, a_n$ de personas tales que $a_0 = a$, $a_n = b$ y a_{i-1} conoce a_i, $i = 1, 2, \ldots, n$ (n dependerá de a y b). ◆

Ejemplo 6. Sea $A = \mathbb{R}$, el conjunto de todos los números reales. Se define la siguiente relación R en A:

$$x\,R\,y \quad \text{si y sólo si} \quad x \text{ y } y \text{ satisfacen la ecuación } \frac{x^2}{4} + \frac{y^2}{9} = 1.$$

El conjunto R consta de todos los puntos que están sobre la elipse de la figura 4.3. ◆

Ejemplo 7. Sea A el conjunto de todas las entradas posibles a un programa dado de computadora, y sea B el conjunto de todos los resultados posibles del mismo programa. Defina la siguiente relación R de A a B: $a\,R\,b$ si y sólo si b es el resultado producido por el programa cuando se use la entrada a. ◆

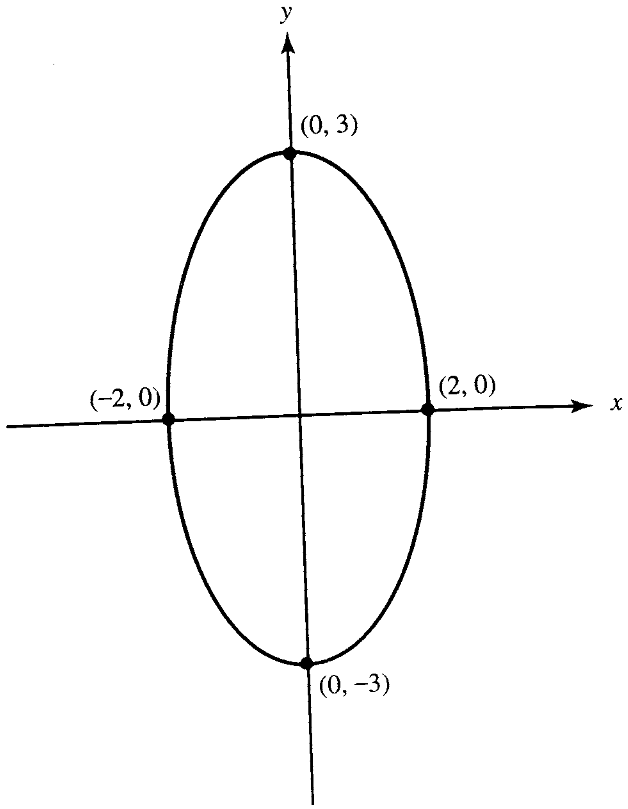


Figura 4.3

Ejemplo 8. Sea

$$A = \text{el conjunto de todas las líneas contenidas en el plano.}$$

Defina la siguiente relación R en A:

$$l_1 \; R \; l_2 \quad \text{si y sólo si} \quad l_1 \text{ es paralela a } l_2,$$

en donde l_1 y l_2 son líneas contenidas en el plano. ◆

Ejemplo 9. Una línea aérea da servicio a cinco ciudades c_1, c_2, c_3, c_4 y c_5. La tabla 4.1 muestra el costo (en dólares) del viaje de c_i a c_j. En consecuencia, el costo del viaje de c_1 a c_3 es \$100, mientras que el costo del viaje de c_4 a c_2 es \$200.

Tabla 4.1

De \ A	c_1	c_2	c_3	c_4	c_5
c_1		140	100	150	200
c_2	190		200	160	220
c_3	110	180		190	250
c_4	190	200	120		150
c_5	200	100	200	150	

Ahora se define la siguiente relación R sobre el conjunto de ciudades $A = \{c_1, c_2, c_3, c_4, c_5\}$: $c_i \; R \; c_j$ si y sólo si el costo de ir de c_i a c_j es menor o igual a 180 dólares. Determine R.

Solución: La relación R es el subconjunto de $A \times A$ formado por todas las ciudades (c_i, c_j), en donde el costo del viaje de c_i a c_j es menor o igual a 180 dólares. Por tanto

$$R = \{(c_1, c_2), (c_1, c_3), (c_1, c_4), (c_2, c_4), (c_3, c_1), (c_3, c_2), (c_4, c_3), (c_4, c_5), (c_5, c_2), (c_5, c_4)\}.$$ ◆

Conjuntos que surgen de las relaciones

Sea $R \subseteq A \times B$ una relación de A a B. Se va a definir ahora varios conjuntos importantes y útiles relacionados con R.

El **dominio** de R, denotado por Dom(R), es el conjunto de elementos de A que están relacionados con algún elemento de B. En otras palabras, Dom(R), un subconjunto de A, es el conjunto de todos los primeros elementos de los pares que forman R. De modo similar, se define el **rango** de R, designado por Ran(R), como el conjunto de elementos de B que son segundos elementos de los pares de R, es decir, todos los elementos de B que están relacionados con algún elemento de A.

Los elementos de A que no están en Dom(R) no están involucrados en la relación R de manera alguna. Esto es cierto también para los elementos de B que no estén en el rango, Ran (R).

Ejemplo 10. Si R es la relación definida en el ejemplo 1, entonces Dom(R) = A y Ran(R) = B. ◆

Ejemplo 11. Si R es la relación que se dio en el ejemplo 3, entonces Dom(R) = $\{1, 2, 3, 4\}$ y Ran(R) = $\{2, 3, 4, 5\}$. ◆

Ejemplo 12. Sea R la relación del ejemplo 6. Entonces Dom(R) = $[-2, 2]$ y Ran(R) = $[-3, 3]$. Nótese que estos conjuntos han sido dados en notación de intervalos. ◆

Si R es una relación de A a B y $x \in A$, se define $R(x)$, el **conjunto relativo en R de x**, como el conjunto de todas las y de B con la propiedad de que x está relacionada en R con y. Así, en símbolos,

$$R(x) = \{y \in B \mid x \; R \; y\}.$$

De modo semejante, si $A_1 \subseteq A$, entonces $R(A_1)$, el **conjunto relativo en R de A_1**, es el conjunto de todas las y de B con la propiedad de que x está relacionada en R con y para alguna x de A_1. Es decir,

$$R(A_1) = \{y \in B \mid x \; R \; y \text{ para alguna } x \text{ de } A_1\}.$$

Por las definiciones anteriores, se ve que $R(A_1)$ es la unión de los conjuntos $R(x)$, en donde $x \subset A_1$. Los conjuntos $R(x)$ desempeñan un papel importante en el estudio de muchos tipos de relaciones.

Ejemplo 13. Sea $A = \{a, b, c, d\}$ y sea $R = \{(a, a), (a, b), (b, c), (c, a), (d, c), (c, b)\}$. Entonces $R(a) = \{a, b\}$, $R(b) = \{c\}$, y si $A_1 = \{c, d\}$, entonces $R(A_1) = \{a, b, c\}$. ◆

Ejemplo 14. Sea R la relación del ejemplo 6, y sea $x \in$ [illegible]. Si $x \; R \; y$ para alguna y, entonces $x^2/4 + y^2/9 = 1$. Se ve que si x no está en el rango $(-2, 2)$, entonces ninguna y puede satisfacer la ecuación anterior, ya que $x^2/4 > 1$. En consecuencia, en este caso, $R(x) = \varnothing$. Si $x = -2$, entonces $x^2/4 = 1$, de manera que x sólo puede estar relacionada con 0. En consecuencia, $R(-2) = \{0\}$. De modo similar, $R(2) = \{0\}$. Finalmente, si $-2 < x < 2$ y $x\ R\ y$, entonces se debe tener $y = \sqrt{9 - (9x^2/4)}$ o $y = \sqrt{9 - (9x^2/4)}$, como se ve al resolver la ecuación $x^2/4 + y^2/9 = 1$, de modo que $R(x) = \{\sqrt{9 - (9x^2/4)}, -\sqrt{9 - (9x^2/4)}\}$. En consecuencia, por ejemplo, $R(1) = \{(3\sqrt{3})/2, -(3\sqrt{3})/2\}$. ◆

El siguiente teorema muestra el comportamiento de los conjuntos relativos en R en relación con las operaciones básicas de los conjuntos.

Teorema 1. *Sea R la relación de A a B, y sean A_1 y A_2 subconjuntos de A. Entonces*

(a) Si $A_1 \subseteq A_2$, *entonces* $R(A_1) \subseteq R(A_2)$.
(b) $R(A_1 \cup A_2) = R(A_1) \cup R(A_2)$.
(c) $R(A_1 \cap A_2) \subseteq R(A_1) \cap R(A_2)$.

Demostración: (a) Si $y \in R(A_1)$, entonces $x\ R\ y$ para alguna $x \in A_1$. Como $A_1 \subseteq A_2$, $x \in A_2$. En consecuencia, $y \in R(A_2)$, lo cual demuestra la parte (a).

(b) Si $y \in R(A_1 \cup A_2)$, entonces por definición $x\ R\ y$ para alguna x de $A_1 \cup A_2$. Si x está en A_1, entonces, como $x\ R\ y$, se debe tener $y \in R(A_1)$. Por el mismo argumento, si x está en A_2, entonces $y \in R(A_2)$. En cualquiera de los dos casos, $y \in R(A_1) \cup R(A_2)$. En consecuencia, se ha demostrado que $R(A_1 \cup A_2) \subseteq R(A_1) \cup R(A_2)$.

Recíprocamente, como $A_1 \subseteq (A_1 \cup A_2)$, la parte (a) dice que $R(A_1) \subseteq R(A_1 \cup A_2)$. De modo similar, $R(A_2) \subseteq R(A_1 \cup A_2)$. En consecuencia, $R(A_1) \cup R(A_2) \subseteq R(A_1 \cup A_2)$, y por lo tanto la parte (b) es verdadera.

(c) Si $y \in R(A_1 \cap A_2)$, entonces, para alguna x de $A_1 \cap A_2$, $x\ R\ y$. Como x está en ambos conjuntos A_1 y A_2, se desprende que y está en ambos $R(A_1)$ y $R(A_2)$; es decir, $y \in R(A_1) \cap R(A_2)$. En consecuencia, la parte (c) es verdadera. ●

Obsérvese que el teorema 1(c) no afirma que haya igualdad de conjuntos. Véase el ejercicio 16 para las condiciones en las cuales los dos conjuntos son iguales. En el ejemplo siguiente, se verá que no siempre permanece como válida la igualdad.

Ejemplo 15. Sean $A = Z$, R "$\leq$", $A_1 = \{0, 1, 2\}$ y $A_2 = \{9, 13\}$. Entonces $R(A_1)$ está formado por todos los enteros n tales que $0 \leq n$, o $1 \leq n$, o $2 \leq n$. En consecuencia $R(A_1) = \{0, 1, 2, \ldots\}$. De modo semejante, $R(A_2) = \{9, 10, 11, \ldots\}$, de modo que $R(A_1) \cap R(A_2) = \{9, 10, 11, \ldots\}$. Por otra parte, $A_1 \cap A_2 = \varnothing$; en consecuencia, $R(A_1 \cap A_2) = \varnothing$. Esto demuestra que el contenido del teorema 1(c) no es siempre una igualdad. ◆

Ejemplo 16. Sean $A = \{1, 2, 3\}$ y $B = \{x, y, z, w, p, q\}$, y considere la relación $R = \{(1, x), (1, z), (2, w), (2, p), (2, q), (3, y)\}$. Sean $A_1 = \{1, 2\}$ y $A_2 = \{2, 3\}$. Entonces, $R(A_1) = \{x, z, w, p, q\}$ y $R(A_2) = \{w, p, q, y\}$. En consecuencia $R(A_1) \cup R(A_2) = B$. Como $A_1 \cup A_2 = A$, se ve que $R(A_1 \cup A_2) = R(A) = B$, como se enuncia en el teorema 1(b). También, $R(A_1) \cap R(A_2) = \{w, p, q\} \neq R(\{2\}) = R(A_1 \cap A_2)$, de modo que en este caso la igualdad no es válida para el contenido del teorema 1(c). ◆

Resulta útil y fácilmente observable que los conjuntos $R(a)$, para a en A, determinan completamente una relación R. Este hecho es enunciado con precisión en el siguiente teorema.

Teorema 2. *Sean R y S relaciones de A a B. Si $R(a) = S(a)$ para todas las a de A, entonces $R = S$.*

Demostración: Si $a\ R\ b$, entonces $b \in R(a)$. Por lo tanto, $b \in S(a)$ y $a\ S\ b$. Un argumento completamente similar muestra que, si $a\ S\ b$, entonces $a\ R\ b$. En consecuencia, $R = S$. ●

La matriz de una relación

Es posible representar una relación entre dos conjuntos finitos con una matriz de la siguiente manera. Si $A = \{a_1, a_2, \ldots, a_m\}$ y $B = \{b_1, b_2, \ldots, b_n\}$ son conjuntos finitos que contienen m y n elementos, respectivamente, y R es una relación de A a B, se representa R por la matriz $m \times n$ $\mathbf{M}_R = [m_{ij}]$, la cual se define por

$$m_{ij} = \begin{cases} 1 & \text{si } (a_i, b_j) \in R \\ 0 & \text{si } (a_i, b_j) \notin R. \end{cases}$$

La matriz $\mathbf{M}_R$ se llama **matriz de** R. A menudo $\mathbf{M}_R$ proporciona una manera fácil de verificar si R tiene una propiedad dada.

Ejemplo 17. Sea R la relación que se definió en el ejemplo 1. Entonces la matriz de R es

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

◆

A la inversa, dados los conjuntos A y B con $|A| = m$ y $|B| = n$, una matriz $m \times n$ cuyas entradas son ceros y unos, determina una relación, como se ilustra en el ejemplo siguiente.

Ejemplo 18. Considere la matriz

$$\mathbf{M} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Como $\mathbf{M}$ es 3×4, se hace

$$A = \{a_1, a_2, a_3\} \quad \text{y} \quad B = \{b_1, b_2, b_3, b_4\}.$$

Entonces $(a_i, b_j) \in R$ si y solamente si $m_{ij} = 1$. En consecuencia,

$$R = \{(a_1, b_1), (a_1, b_4), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_3)\}.$$

◆

Digrafos

Si A es un conjunto finito y R es una relación sobre A, también se puede representar R gráficamente como sigue. Trace un pequeño círculo para cada elemento de A y marque el círculo con el elemento correspondiente de A. A estos círculos se los llama **vértices**. Trace una flecha, a la que se llama **lado (arco)**, del vértice a_i al vértice a_j si y solamente si $a_i\ R\ a_j$. La representación gráfica resultante de R se llama **gráfica dirigida** o **dígrafo** de R.

En consecuencia, si R es una relación sobre A, los lados o arcos del digrafo de R corresponden exactamente a los pares de R, y los vértices corresponden exactamente a los elementos del conjunto A. En ocasiones, cuando se desea acentuar la naturaleza geométrica de alguna propiedad de R, se puede hacer referencia a los pares mismos de R como lados o arcos y a los elementos de R como vértices.

Ejemplo 19. Sean

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

Entonces el digrafo de R es como se ilustra en la figura 4.4. ♦

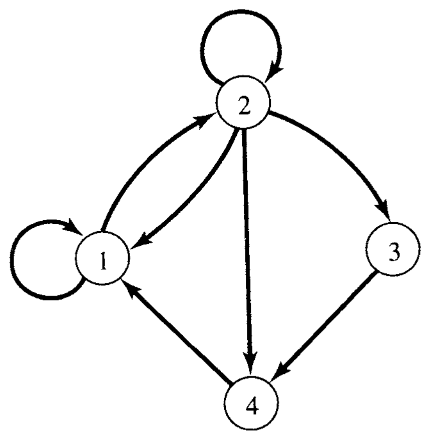


Figura 4.4

Una colección de vértices con lados entre algunos de los vértices determina una relación de manera natural.

Ejemplo 20. Encuentre la relación determinada por la figura 4.5.

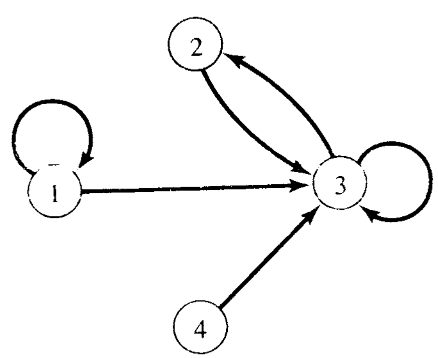


Figura 4.5

Solución: Como $a_i \, R \, a_j$ si y solamente si hay un lado de a_i a a_j, se tiene

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

En este libro, los digrafos no son sino representaciones geométricas de relaciones, y cualquier enunciado que se haga acerca de un digrafo es, en realidad, un enunciado acerca de la relación correspondiente. Esto es especialmente importante para teoremas y sus demostraciones. En algunos casos, es más fácil o más claro enunciar un resultado en términos gráficos, pero una demostración siempre se referirá a la relación subyacente. El lector debe estar consciente de que algunos autores consideran más objetos generales como digrafos, por ejemplo, permitiendo que haya varios arcos entre los mismos vértices.

Un concepto importante para las relaciones es el que inspira la forma visual de los digrafos. Si R es una relación sobre un conjunto A y $a \in A$, entonces el **grado interno** de a (relativo a la relación R) es el número de $b \in A$ tal que $(b, a) \in R$. El **grado externo** de a es el número de $b \in A$ tal que $(a, b) \in R$.

Esto significa, en términos del digrafo de R, que el grado interno de un vértice es el número de arcos que terminan en el vértice. El grado externo de un vértice es el número de arcos que salen del vértice. Nótese que el grado externo de a es $|R(a)|$.

Ejemplo 21. Considérese el digrafo de la figura 4.4. El vértice 1 tiene grado interno 3 y grado externo 2. Considérese también el digrafo que aparece en la figura 4.5. El vértice 3 tiene grado interno 4 y grado externo 2, mientras el vértice 4 tiene grado interno 0 y grado externo 1. ♦

Ejemplo 22. Sea $A = \{a, b, c, d\}$, y sea R la relación sobre A que tiene la matriz

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Construya el digrafo de R, y haga una lista de los grados internos y grados externos de todos los vértices.

Solución: El digrafo de R se ilustra en la figura 4.6. La tabla siguiente proporciona los grados internos y los externos de todos los vértices.

	a	b	c	d
Grados internos	2	3	1	1
Grados externos	1	1	3	2

♦

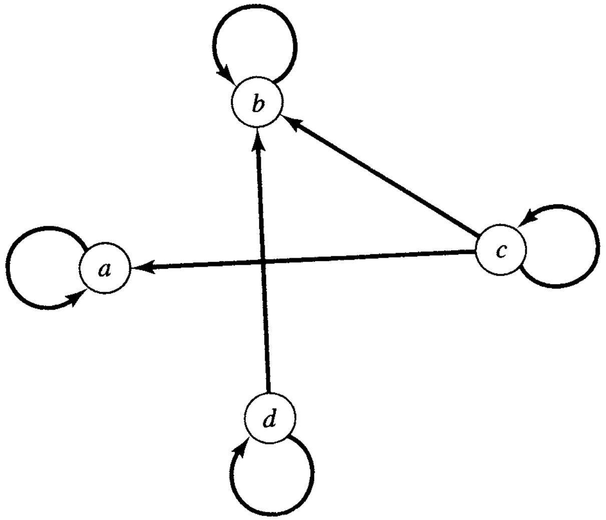


Figura 4.6

Ejemplo 23. Sea $A = \{1, 4, 5\}$, y sea R la relación que da el digrafo que aparece en la figura 4.7. Encuentre $\mathbf{M}_R$ y R.

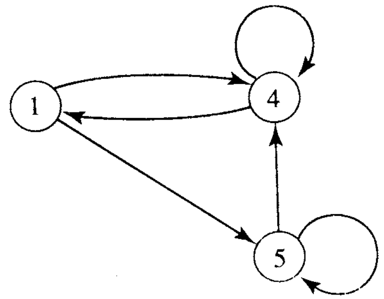


Figura 4.7

Solución:

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \qquad R = \{(1,4), (1,5), (4,1), (4,4), (5,4), (5,5)\}. \quad \blacklozenge$$

Si R es una relación sobre un conjunto A y B es un subconjunto de A, la **restricción de R a B** es $R \cap (B \times B)$.

Ejemplo 24. Sea $A = \{a, b, c, d, e, f\}$ y $R = \{(a, a), (a, c), (b, c), (a, e), (b, e), (c, e)\}$. Sea $B = \{a, b, c\}$. Entonces

$$B \times B = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$$

y la restricción de R a B es $\{(a, a), (a, c), (b, c)\}$. $\blacklozenge$

GRUPO DE EJERCICIOS 4.2

1. (a) Para la relación R definida en el ejemplo 4, ¿cuáles de los siguientes pares ordenados pertenecen a R?
   (i) $(2,3)$ (ii) $(0,8)$ (iii) $(1,3)$
   (iv) $(6,18)$ (v) $(-6,24)$ (vi) $(8,0)$

   (b) Para la relación R definida en el ejemplo 6, ¿cuáles de los siguientes pares ordenados pertenece a R?
   (i) $(2,0)$ (ii) $(0,2)$ (iii) $(0,3)$
   (iv) $(0,0)$ (v) $(1, 3/2\sqrt{3})$ (vi) $(0,0)$

En los ejercicios 2 al 10, determine el dominio, rango, matriz, y, cuando $A = B$, el digrafo de la relación R.

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

3. A = {IBM, COMPAQ, Dell, Gateway, Zenith}, B = {750C, PS60, 450SV, 4/33S, 525SX, 466V, 486SL}
   R = {(IBM, 750C), (Dell, 466V), (COMPAQ, 450SV), (Gateway, PS60)}

4. $A = \{1, 2, 3, 4\}$, $B = \{1, 4, 6, 8, 9\}$; $a\,R\,b$ si y sólo si $b = a^2$.

5. $A = \{1, 2, 3, 4, 8\} = B$; $a\,R\,b$ si y sólo si $a = b$.

6. $A = \{1, 2, 3, 4, 8\}$, $B = \{1, 4, 6, 9\}$; $a\,R\,b$ si y sólo si $a \mid b$.

7. $A = \{1, 2, 3, 4, 6\} = B$; $a\,R\,b$ si y sólo si a es múltiplo de b.

8. $A = \{1, 2, 3, 4, 5\} = B$; $a\,R\,b$ si y sólo si $a \le b$.

9. $A = \{1, 3, 5, 7, 9\}$, $B = \{2, 4, 6, 8\}$; $a\,R\,b$ si y sólo si $b < a$

10. $A = \{1, 2, 3, 4, 8\} = B$; $a\,R\,b$ si y sólo si $a + b \le 9$.

11. Sea $A = Z^+$, los enteros positivos, y R la relación definida por $a\,R\,b$ si y sólo si existe una k en Z^+ de modo que $a = b^k$ (k depende de a y b). ¿Cuáles de los siguientes pares ordenados pertenecen a R?
    (a) $(4, 16)$ (b) $(1, 7)$ (c) $(8, 2)$
    (d) $(3, 3)$ (e) $(2, 8)$ (f) $(2, 32)$

12. Sea $A = \mathbb{R}$. Considere la siguiente relación R en A; $a\,R\,b$ si y sólo si $2a + 3b = 6$. Determine Dom(R) y Ran(R).

13. Sea $A = \mathbb{R}$. Considere la siguiente relación R en A; $a\,R\,b$ si y sólo si $a^2 + b^2 = 25$. Determine Dom(R) y Ran(R).

14. Sea R la relación definida en el ejemplo 6. Determine $R(A_1)$ para cada uno de los siguientes.
    (a) $A_1 = \{1, 8\}$ (b) $A_1 = \{3, 4, 5\}$ (c) $A_1 = \{\ \}$

15. Sea R la relación definida en el ejercicio 7. Determine cada uno de los siguientes.
    (a) $R(3)$ (b) $R(6)$ (c) $R(\{2, 4, 6\})$

16. Sea R una relación de A a B. Demuestre que para todos los subconjuntos A_1 y A_2 de A.

    $R(A_1 \cap A_2) = R(A_1) \cap R(A_2)$ si y solamente si $R(a) \cap R(b) = \{\ \}$ para cualquier a, b distinta en A.

17. Sea $A = \mathbb{R}$. Dé una descripción de la relación R especificada por la región sombreada de la figura 4.8.

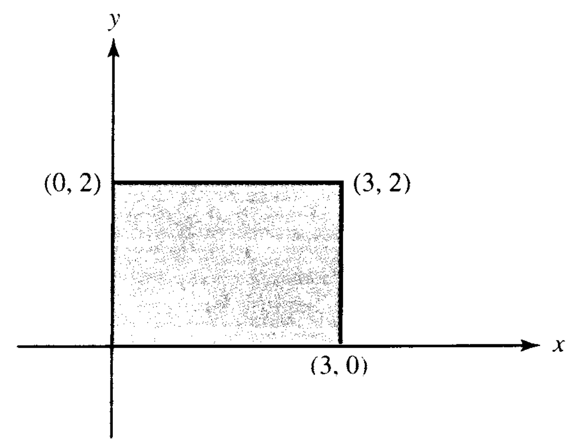


Figura 4.8

18. Si A tiene n elementos y B tiene m elementos, ¿cuántas relaciones diferentes hay de A a B?

En los ejercicios 19 y 20, dé la relación R definida en A y su digrafo.

19. Sea $A = \{1, 2, 3, 4\}$ y $\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$.

20. Sea $A = \{a, b, c, d, e\}$

y $\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$.

En los ejercicios 21 y 22, proporcione la relación determinada por el digrafo y dé su matriz.

21.

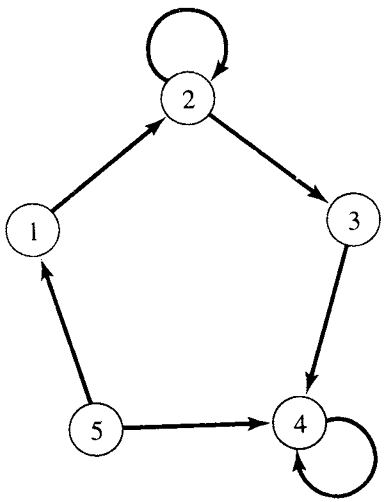


Figura 4.9

22.

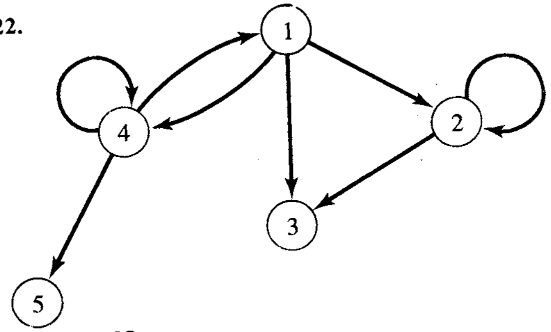


Figura 4.10

23. (a) Para el digrafo del ejercicio 21, proporcione el grado interno y el grado externo de cada vértice.
(b) Para el digrafo del ejercicio 22, proporcione el grado interno y el grado externo de cada vértice.

24. Sean $A = \{1, 2, 3, 4, 5, 6, 7\}$ y $R = \{(1, 2), (1, 4), (2, 3), (2, 5), (3, 6), (4, 7)\}$. Calcule la restricción de R a B para el subconjunto de A dado.
(a) $B = \{1, 2, 4, 5\}$
(b) $B = \{2, 3, 4, 6\}$

25. Sea S el conjunto producto $\{1, 2, 3\} \times \{a, b\}$. ¿Cuántas relaciones hay en S?

4.3. Trayectorias en relaciones y digrafos

Supóngase que R es una relación sobre un conjunto A. Una **trayectoria de longitud n** en R de a a b es una secuencia finita π: $a, x_1, x_2, \ldots, x_{n-1}, b$, que comienza con a y termina con b, tal que

$$a\ R\ x_1, x_1\ R\ x_2, \ldots, x_{n-1}\ R\ b.$$

Debe observarse que una trayectoria de longitud n involucra $n + 1$ elementos de A, aunque no sean necesariamente distintos.

Una trayectoria se concibe visualmente con más facilidad con ayuda del digrafo de la relación. Aparece como una *trayectoria* geométrica o sucesión de arcos en un digrafo de esta naturaleza, en donde se sigue las direcciones indicadas de los arcos o lados, y de hecho una trayectoria deriva su nombre de esta representación. En consecuencia, la longitud de una trayectoria es el número de arcos que hay en la misma, en donde los vértices no necesitan ser todos distintos.

Ejemplo 1. Considere el digrafo de la figura 4.11. Entonces π_1: 1, 2, 5, 4, 3 es una trayectoria de longitud 4 del vértice 1 al vértice 3, π_2: 1, 2, 5, 1 es una trayectoria de longitud 3 del vértice 1 a él mismo, y π_3: 2, 2 es una trayectoria de longitud 1 del vértice 2 a sí mismo. ♦

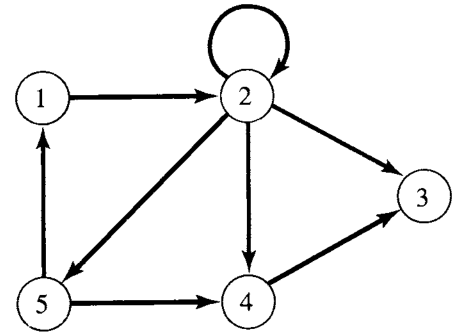


Figura 4.11

Una trayectoria que comienza y termina en el mismo vértice se llama **ciclo**. En el ejemplo 1, π_2 y π_3 son ciclos de longitud 3 y 1, respectivamente. Es claro que las trayectorias de longitud 1 pueden ser identificadas con los pares ordenados (x, y) que pertenecen a R. Las trayectorias de una relación R pueden ser usadas para definir nuevas relaciones bastante útiles. Si n es un entero positivo fijo, se define una relación R^n sobre A como sigue: $x\ R^n\ y$ significa que hay una trayectoria de longitud n de x a y en R. También puede definirse una relación R^∞ sobre A, suponiendo que $x\ R^\infty\ y$ signifique que hay alguna trayectoria en R de x a y. La longitud de una trayectoria de esta clase dependerá, en general, de x y y. A la relación R^∞ se la suele llamar **relación de conectividad** para R.

Nótese que $R^n(x)$ consta de todos los vértices que puede alcanzarse desde x por medio de una trayectoria en R de longitud n. El conjunto $R^\infty(x)$ consta de todos los vértices que puede alcanzarse desde x por alguna trayectoria de R.

Ejemplo 2. Sea A el conjunto de todos los seres humanos vivientes, y sea R la relación de conocimiento mutuo. Es decir, $a\ R\ b$ significa que a y b se conocen entre sí. Entonces $a\ R^2\ b$ significa que a y b tienen un conocido en común. En general, $a\ R^n\ b$ si a conoce a alguien x_1, quien conoce a $x_2, \ldots$, quien conoce a x_{n-1}, quien conoce a b. Finalmente, $a\ R^\infty\ b$ significa que existe alguna cadena de conocidos entre personas que comienza en a y termina en b. Por ejemplo, es interesante saber (y se desconoce) saber si cada dos estadunidenses están relacionados por R^∞. ♦

Ejemplo 3. Sea A un conjunto de ciudades de EU, y sea $x\ R\ y$ si hay un vuelo directo de x a y en por lo menos una línea aérea. Entonces x y y están relacionadas por R^n si uno puede reservar un vuelo de x a y que tenga exactamente $n - 1$ paradas intermedias, y $x\, R^{\infty}\, y$ si uno puede ir de x a y por avión. ◆

Ejemplo 4. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Sea R la relación cuyo digrafo aparece en la figura 4.12. La figura 4.13 muestra el digrafo de la relación R^2 sobre A. Una línea conecta dos vértices en la figura 4.13 si y sólo si están relacionados en R^2, es decir, si y sólo si hay una trayectoria de longitud dos conectando esos vértices en la figura 4.12. En consecuencia

$1\, R^2\, 2$	puesto que	$1\, R\, 2$	y	$2\, R\, 2$
$1\, R^2\, 4$	puesto que	$1\, R\, 2$	y	$2\, R\, 4$
$1\, R^2\, 5$	puesto que	$1\, R\, 2$	y	$2\, R\, 5$
$2\, R^2\, 2$	puesto que	$2\, R\, 2$	y	$2\, R\, 2$
$2\, R^2\, 4$	puesto que	$2\, R\, 2$	y	$2\, R\, 4$
$2\, R^2\, 5$	puesto que	$2\, R\, 2$	y	$2\, R\, 5$
$2\, R^2\, 6$	puesto que	$2\, R\, 5$	y	$5\, R\, 6$
$3\, R^2\, 5$	puesto que	$3\, R\, 4$	y	$4\, R\, 5$
$4\, R^2\, 6$	puesto que	$4\, R\, 5$	y	$5\, R\, 6$.

De modo similar, se puede construir el digrafo de R^n para cualquier valor de n. ◆

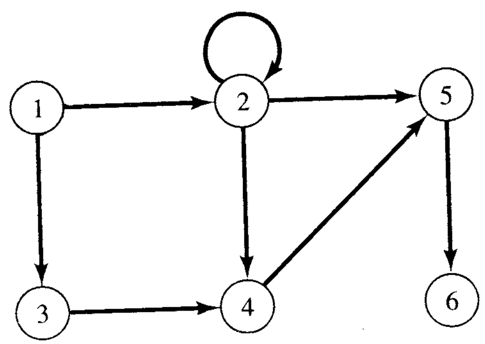


Figura 4.12

Ejemplo 5. Sea $A = \{a, b, c, d, e\}$ y
$$R = \{(a, a), (a, b), (b, c), (c, e), (c, d), (d, e)\}.$$

Calcule (a) R^2; (b) R^{∞}.

Solución: (a) El digrafo de R aparece en la figura 4.14.

$a\, R^2\, a$	puesto que	$a\, R\, a$	y	$a\, R\, a$
$a\, R^2\, b$	puesto que	$a\, R\, a$	y	$a\, R\, b$
$a\, R^2\, c$	puesto que	$a\, R\, b$	y	$b\, R\, c$
$b\, R^2\, e$	puesto que	$b\, R\, c$	y	$c\, R\, e$
$b\, R^2\, d$	puesto que	$b\, R\, c$	y	$c\, R\, d$
$c\, R^2\, e$	puesto que	$c\, R\, d$	y	$d\, R\, e$

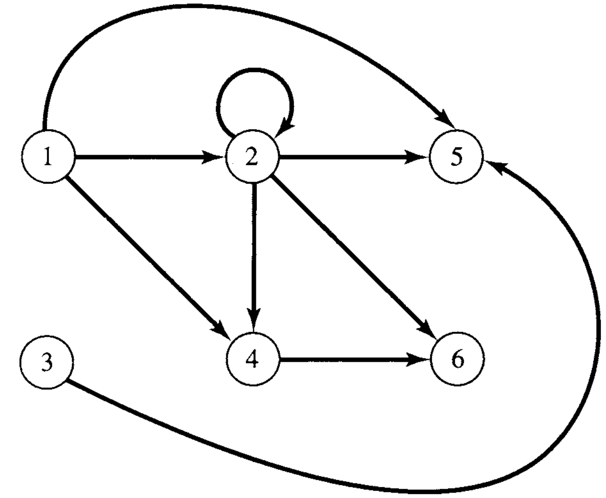


Figura 4.13

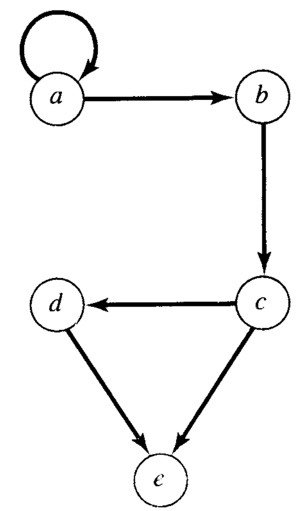


Figura 4.14

Por tanto

$$R^2 = \{(a, a), (a, b), (a, c), (b, e), (b, d), (c, e)\}.$$

(b) Para calcular R^{∞}, se necesita todos los pares ordenados de vértices para los cuales haya una trayectoria de cualquier longitud del primer vértice al segundo. De acuerdo con la figura 4.14 se ve que

$$R^{\infty} = \{(a, a), (a, b), (a, c), (a, d), (a, e), (b, c), (b, d), (b, e), (c, d), (c, e), (d, e)\}.$$

Por ejemplo, $(a, d) \in R^{\infty}$, en vista de que hay una trayectoria de longitud 3 de a a d: a, b, c, d. De modo similar, $(a, e) \in R^{\infty}$, puesto que hay una trayectoria de longitud 3 de a a e: a, b, c, e así como una trayectoria de longitud 4 de a a e: a, b, c, d, e. ◆

Sea R una relación sobre un conjunto finito $A = \{a_1, a_2, \ldots, a_n\}$, y sea $\mathbf{M}_R$ la matriz $n \times n$ que representa a R. Se va a demostrar cómo la matriz $\mathbf{M}_{R^2}$, de R^2, puede calcularse a partir de $\mathbf{M}_R$.

Teorema 1. *Si R es una relación sobre $A = \{a_1, a_2, \ldots, a_n\}$, entonces $\mathbf{M}_{R^2} = \mathbf{M}_R \odot \mathbf{M}_R$ (véase la sección 1.5).*

Demostración: Sea $\mathbf{M}_R = [m_{ij}]$ y $\mathbf{M}_{R^2} = [n_{ij}]$. Por definición, la i, el j-ésimo elemento de $\mathbf{M}_R \odot \mathbf{M}_R$ es igual a 1 si y solamente si el renglón i de $\mathbf{M}_R$ y la columna j de $\mathbf{M}_R$ tienen a 1 en la misma posición relativa, por decir, en la posición k. Esto significa que $m_{ik} = 1$ y $m_{kj} = 1$ para alguna k, $1 \leq k \leq n$. Por definición de la matriz $\mathbf{M}_R$, las condiciones anteriores significan que $a_i \, R \, a_k$ y $a_k \, R \, a_j$. En consecuencia, $a_i \, R^2 \, a_j$, y por tanto $n_{ij} = 1$. Se ha demostrado, por lo tanto, que la posición i, j de $\mathbf{M}_R \odot \mathbf{M}_R$ es igual a 1 si y solamente si $n_{ij} = 1$. Esto significa que $\mathbf{M}_R \odot \mathbf{M}_R = \mathbf{M}_{R^2}$. ●

Para abreviar, se denota generalmente $\mathbf{M}_R \odot \mathbf{M}_R$ simplemente como $(\mathbf{M}_R)^2_\odot$ (el símbolo $\odot$ recuerda que éste no es el producto matricial usual).

Ejemplo 6. Sean A y R lo mismo que en el ejemplo 5. Entonces

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Del análisis anterior, se ve que

$$\mathbf{M}_{R^2} = \mathbf{M}_R \odot \mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Al calcular $\mathbf{M}_{R^2}$ directamente de R^2, se obtiene el mismo resultado. ♦

Puede verse, por los ejemplos 5 y 6, que a menudo es más fácil calcular R^2 calculando $\mathbf{M}_R \odot \mathbf{M}_R$ en lugar de buscar el digrafo de R para todos los vértices que puedan unirse por una trayectoria de longitud 2. De igual manera, puede demostrarse que $\mathbf{M}_{R^3} = \mathbf{M}_R \odot (\mathbf{M}_R \odot \mathbf{M}_R) = (\mathbf{M}_R)^3_\odot$. En efecto, por inducción se demuestra ahora que estos dos resultados pueden generalizarse.

Teorema 2. *Para $n \geq 2$ y siendo R una relación sobre un conjunto finito A, se tiene*

$$\mathbf{M}_{R^n} = \mathbf{M}_R \odot \mathbf{M}_R \odot \cdots \odot \mathbf{M}_R \quad (n \text{ factores}).$$

Demostración: Sea $P(n)$ la afirmación de que es válido el enunciado anterior para un entero $n \geq 2$.

PASO BASE. $P(2)$ es verdadero por el teorema 1.

PASO DE INDUCCIÓN. Se demuestra ahora que si $P(k)$ es verdadero, entonces $P(k+1)$ es verdadero. Considérese la matriz $\mathbf{M}_{R^{k+1}}$. Sea $\mathbf{M}_{R^{k+1}} = [x_{ij}]$, $\mathbf{M}_{R^k} = [y_{ij}]$, y $\mathbf{M}_R = [m_{ij}]$. Si $x_{ij} = 1$, se debe tener una trayectoria de longitud $k + 1$ de a_i a a_j. Si se supone que a_s es el vértice que alcanza esta trayectoria precisamente antes del último vértice a_j, entonces hay una trayectoria de longitud k de a_i a a_s, y una trayectoria de longitud 1 de a_s a a_j. En consecuencia, $y_{is} = 1$ y $m_{sj} = 1$, de manera que $\mathbf{M}_{R^k} \odot \mathbf{M}_R$ tiene un 1 en la posición i, j. Puede verse, en forma semejante, que si $\mathbf{M}_{R^k} \odot \mathbf{M}_R$ tiene un 1 en la posición i, j, entonces $x_{ij} = 1$. Esto significa que $\mathbf{M}_{R^{k+1}} = \mathbf{M}_{R^k} \odot \mathbf{M}_R$.

Por inducción,

$$P(k)\colon \mathbf{M}_{R^k} = \mathbf{M}_R \odot \cdots \odot \mathbf{M}_R \quad (k \text{ factores}).$$

por tanto, por sustitución,

$$\mathbf{M}_{R^{k+1}} = (\mathbf{M}_R \odot \cdots \odot \mathbf{M}_R) \odot \mathbf{M}_R.$$
$$P(k+1)\colon \mathbf{M}_{R^{k+1}} = \mathbf{M}_R \odot \cdots \odot \mathbf{M}_R \odot \mathbf{M}_R \qquad (k+1 \text{ factores})$$

y $P(k + 1)$ es verdadero. En consecuencia, por el principio de la inducción matemática, $P(n)$ es verdadero para todas las $n \geq 2$. Esto demuestra el teorema. Como antes, se escribe $\mathbf{M}_R \odot \cdots \odot \mathbf{M}_R$ (n factores) como $(\mathbf{M}_R)^n_\odot$. ●

Ahora que se sabe cómo calcular la matriz de la relación R^n a partir de la matriz de R, sería conveniente ver cómo se calcula la matriz de R^∞. Se procede de la siguiente manera. Supóngase que R es una relación sobre un conjunto finito A, y que $x \in A$, $y \in A$. Se sabe que $x \, R^\infty \, y$ significa que x y y están conectadas por una trayectoria en R de longitud n para algún valor de n. En general, n dependerá de x y y, pero, es claro que, $x \, R^\infty \, y$ si y solamente si $x \, R \, y$ o $x \, R^2 \, y$ o $x \, R^3 \, y$ o .... Si R y S son relaciones sobre A, la relación $R \cup S$ se define por $x \, (R \cup S) \, y$ si y solamente si $x \, R \, y$ o $x \, S \, y$. (La relación $R \cup S$ se estudiará con más detalle en la sección 4.7.) Entonces el enunciado anterior dice que $R^\infty = R \cup R^2 \cup R^3 \cup \cdots = \bigcup_{n=1}^{\infty} R^n$. El lector puede verificar que $\mathbf{M}_{R \cup S} = \mathbf{M}_R \vee \mathbf{M}_S$, y se demostrará esto en la sección 4.7. En consecuencia,

$$\begin{aligned} \mathbf{M}_{R^\infty} &= \mathbf{M}_R \vee \mathbf{M}_{R^2} \vee \mathbf{M}_{R^3} \vee \cdots \\ &= \mathbf{M}_R \vee (\mathbf{M}_R)^2_\odot \vee (\mathbf{M}_R)^3_\odot \vee \cdots. \end{aligned}$$

La relación de **alcanzabilidad** R^* de una relación R en un conjunto A que tiene n elementos se define como sigue: $x \, R^* \, y$ significa que $x = y$ o que $x \, R^\infty \, y$. La idea es que y es alcanzable desde x si ya sea y es x o si hay alguna trayectoria de x a y. Se ve fácilmente que $\mathbf{M}_{R^*} = \mathbf{M}_{R^\infty} \vee \mathbf{I}_n$, en donde $\mathbf{I}_n$ es la matriz identidad $n \times n$. Así, el análisis demuestra que

$$\mathbf{M}_{R^*} = \mathbf{I}_n \vee \mathbf{M}_R \vee (\mathbf{M}_R)^2_\odot \vee (\mathbf{M}_R)^3_\odot \vee \cdots.$$

Sea $\pi_1 : a, x_1, x_2, \ldots, x_{n-1}, b$ una trayectoria en una relación R de longitud n de a a b, y sea $\pi_2 : b, y_1, y_2, \ldots, y_{m-1}, c$ una trayectoria en R de longitud m de b a c. Entonces la **composición de π_1 y π_2** es la trayectoria $a, x_1, x_2, \ldots, b, y_1, y_2, \ldots, y_{m-1}, c$ de longitud $n + m$, la cual se denota por $\pi_2 \circ \pi_1$. Ésta es una trayectoria de a a c.

Ejemplo 7. Considérese la relación cuyo digrafo aparece en la figura 4.15 y las trayectorias

$$\pi_1 : 1, 2, 3 \quad \text{y} \quad \pi_2 : 3, 5, 6, 2, 4.$$

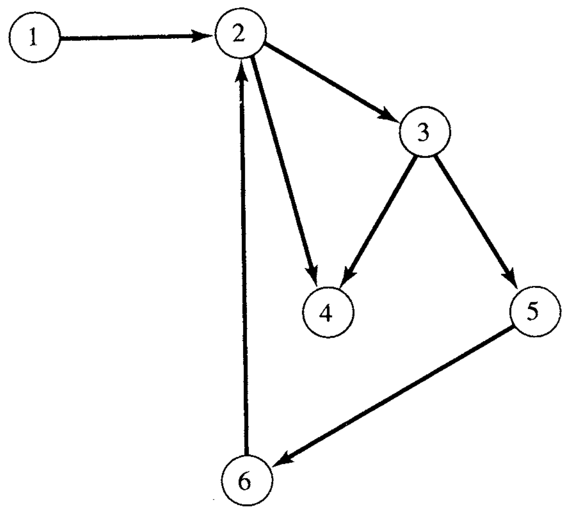


Figura 4.15

Entonces la composición de π_1 y π_2 es la trayectoria $\pi_2 \circ \pi_1 : 1, 2, 3, 5, 6, 2, 4$ de 1 a 4 de longitud 6. ◆

GRUPO DE EJERCICIOS 4.3

Para los ejercicios 1 *al* 8, *sea R la relación cuyo digrafo aparece en la figura* 4.16.

1. Haga una lista de todas las trayectorias de longitud 1.

2. (a) Haga una lista de todas las trayectorias de longitud 2, que inicien en el vértice 2.
   (b) Haga una lista de todas las trayectorias de longitud 2.

3. (a) Haga una lista de todas las trayectorias de longitud 3, que inicien en el vértice 3.
   (b) Haga una lista de todas las trayectorias de longitud 3.

4. Encuentre un ciclo que comience en el vértice 2.

5. Encuentre un ciclo que comience en el vértice 6.

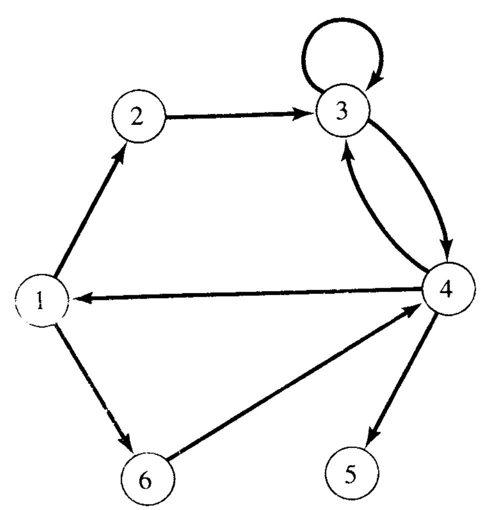


Figura 4.16

6. Trace el digrafo de R^2.

7. Determine $\mathbf{M}_{R^2}$.

8. (a) Determine R^∞.
   (b) Determine $\mathbf{M}_{R^\infty}$.

Para los ejercicios 9 *al* 15, *sea R la relación cuyo digrafo aparece en la figura* 4.17.

9. Haga una lista de todas las trayectorias de longitud 1.

10. (a) Haga una lista de todas las trayectorias de longitud 2 que inicie en el vértice c.
    (b) Encuentre todas las trayectorias de longitud 2.

11. (a) Haga una lista de todas las trayectorias de longitud 3 que inicie en el vértice a.
    (b) Determine todas las trayectorias de longitud 3.

12. (a) Encuentre un ciclo que comience en el vértice c.
    (b) Encuentre un ciclo que comience en el vértice d.

13. Dibuje el digrafo de R^2.

14. Determine $\mathbf{M}_{R^2}$.

15. (a) Determine $\mathbf{M}_{R^\infty}$.
    (b) Determine R^∞.

16. Sean R y S las relaciones sobre un conjunto A. Demuestre que

$$\mathbf{M}_{R \cup S} = \mathbf{M}_R \vee \mathbf{M}_S.$$

17. Sea R una relación sobre un conjunto A que tiene n elementos. Demuestre que $\mathbf{M}_{R^*} = \mathbf{M}_{R^\infty} \vee \mathbf{I}_n$, en donde $\mathbf{I}_n$ es la matriz identidad $n \times n$.

En los ejercicios 18 *y* 19, *sea R la relación cuyo digrafo aparece en la figura* 4.18.

18. Si $\pi_1 : 1, 2, 4, 3$ y $\pi_2 : 3, 5, 6, 4$, determine la composición $\pi_2 \circ \pi_1$.

19. Si $\pi_1 : 1, 7, 5$ y $\pi_2 : 5, 6, 7, 4, 3$, determine la composición $\pi_2 \circ \pi_1$.

20. Sea $A = \{1, 2, 3, 4, 5\}$ y R la relación definida por $a\ R\ b$ si y solamente si $a < b$.
    (a) Calcule R^2 y R^3.
    (b) Complete el siguiente enunciado: $a\ R^2\ b$ si y sólo si ________________.
    (c) Complete el siguiente enunciado: $a\ R^3\ b$ si y sólo si ________________.

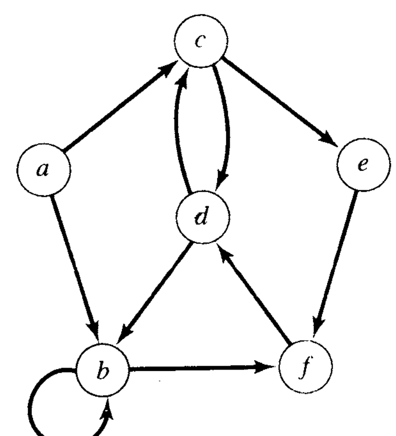


Figura 4.17

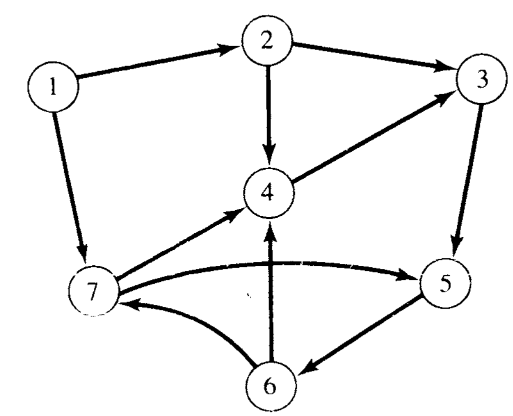


Figura 4.18

4.4. Propiedades de las relaciones

En muchas aplicaciones de las ciencias de la computación y las matemáticas aplicadas, se trata con relaciones que hay en un conjunto A más que con relaciones de A a B. Por otra parte, estas relaciones satisfacen, a menudo, ciertas propiedades que se estudiará en esta sección.

Relaciones reflexivas e irreflexivas

Una relación R de un conjunto A es **reflexiva** si $(a, a) \in R$ para todos los valores de $a \in A$, es decir, si $a\ R\ a$ para todas las $a \in A$. Una relación R de un conjunto A es **irreflexiva** si $a \not R\ a$ para toda $a \in A$.

Así, R es reflexiva si cada uno de sus elementos $a \in A$ está relacionado consigo mismo y es irreflexiva si ningún elemento está relacionado consigo mismo.

Ejemplo 1

(a) Sea $\Delta = \{(a, a) \mid a \in A\}$, de modo que Δ es la relación de **igualdad** en el conjunto A. Entonces Δ es reflexiva, ya que $(a, a) \in \Delta$ para todas las $a \in A$.

(b) Sea $R = \{(a, b) \in A \times A \mid a \neq b\}$, de manera que R sea la relación de **desigualdad** en el conjunto A. Entonces R es irreflexiva, ya que $(a, a) \notin R$ para todas las $a \in A$.

(c) Sea $A = \{1, 2, 3\}$, y sea $R = \{(1, 1), (1, 2)\}$. Entonces R no es reflexiva en vista de que $(2, 2) \notin R$ y $(3, 3) \notin R$. Además, R no es irreflexiva, porque $(1, 1) \in R$.

(d) Sea A un conjunto no vacío. Sea $R = \varnothing \subseteq A \times A$, la **relación vacía**. Entonces R no es reflexiva, ya que $(a, a) \notin R$ para toda $a \in A$ (el conjunto vacío no tiene elementos). Sin embargo, R es irreflexiva. ◆

Puede identificarse una relación reflexiva o irreflexiva por su matriz como sigue. La matriz de una relación reflexiva debe tener unos en todos los elementos de su diagonal principal, mientras que la matriz de una relación irreflexiva debe tener ceros en todos los elementos de su diagonal principal.

De modo semejante, se puede caracterizar el digrafo de una relación reflexiva o irreflexiva como sigue. Una relación reflexiva tiene un ciclo de longitud 1 en cada vértice, mientras que una relación irreflexiva no tiene ciclos de longitud 1. Otra manera útil de decir lo mismo utiliza la relación de igualdad Δ en un conjunto A: R es reflexiva si y sólo si $\Delta \subseteq R$, y R es irreflexiva si y sólo si $\Delta \cap R = \varnothing$.

Finalmente, puede notarse que si R es reflexiva en un conjunto A, entonces $\mathrm{Dom}(R) = \mathrm{Ran}(R) = A$.

Relaciones simétricas, asimétricas y antisimétricas

Una relación R en un conjunto A es **simétrica** si siempre que $a\ R\ b$, entonces $b\ R\ a$. Se desprende, entonces, que R no es simétrica si se tiene algunas a y $b \in A$ con $a\ R\ b$, pero $b \not R\ a$. Una relación R en un conjunto A es **asimétrica** si en todos los casos en que $a\ R\ b$, se tiene $b \not R\ a$. Se desprende, entonces, que R no es asimétrica si se tiene algunas a y $b \in A$ con ambas $a\ R\ b$ y $b\ R\ a$.

Una relación R en un conjunto A es **antisimétrica** si en todos los casos en que $a\ R\ b$ y $b\ R\ a$, se tiene $a = b$. La contrapositiva de esta definición es que R es antisimétrica si siempre que $a \neq b$, entonces $a \not R\ b$ o $b \not R\ a$. Se desprende que R no es antisimétrica si se tiene a y b en A, $a \neq b$, y ambas $a\ R\ b$ y $b\ R\ a$.

Dada una relación R, se querrá determinar cuáles propiedades siguen siendo válidas para R. Debe recordarse la siguiente observación. Una propiedad deja de ser válida en general, si puede encontrarse una situación en la que la propiedad no sea válida.

Ejemplo 2. Sea $A = Z$, el conjunto de los enteros, y sea

$$R = \{(a, b) \in A \times A \mid a < b\}$$

de manera que R sea la relación **menor que**. ¿Es R simétrica, asimétrica o antisimétrica?

Solución:

Simetría: Si $a < b$, entonces no es verdad que $b < a$, por tanto R no es simétrica.

Asimetría: Si $a < b$, entonces $b \not< a$ (b es no menor que a), por tanto R es asimétrica.

Antisimetría: Si $a \neq b$, entonces o bien, $a \not< b$ o $b \not< a$, y por tanto R es antisimétrica. ◆

Ejemplo 3. Sea A un conjunto de personas y sea

$$R = \{(x, y) \in A \times A \mid x \text{ es un primo de } y\}.$$

Entonces R es una relación simétrica (verifique). ◆

Ejemplo 4. Sea $A = \{1, 2, 3, 4\}$ y sea

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

Entonces R no es simétrica, en vista de que $(1, 2) \in R$, pero $(2, 1) \notin R$. Además, R no es asimétrica, ya que $(2, 2) \in R$. Finalmente, R es antisimétrica, porque si $a \neq b$, o bien $(a, b) \notin R$ o $(b, a) \notin R$. ◆

Ejemplo 5. Sea $A = Z^+$, el conjunto de los enteros positivos, y sea

$$R = \{(a, b) \in A \times A \mid a \text{ divide a } b\}.$$

¿R es simétrica, asimétrica o antisimétrica?

Solución:

Si $a \mid b$, no se desprende que $b \mid a$, por lo cual R no es simétrica. Por ejemplo, $2 \mid 3$, pero $3 \nmid 2$.

Si $a = b = 3$, por ejemplo, entonces $a\ R\ b$ y $b\ R\ a$, y, por tanto, R no es asimétrica.

Si $a \mid b$ y $b \mid a$, entonces $a = b$, por tanto R es antisimétrica. (Véase el ejercicio 24 de la sección 1.4.) ◆

Ahora se va a relacionar las propiedades simétricas, asimétricas o antisimétricas de una relación con las propiedades de su matriz. La matriz $\mathbf{M}_R = [m_{ij}]$ de una relación simétrica satisface la propiedad de que

$$\text{si } m_{ij} = 1 \quad \text{entonces } m_{ji} = 1$$

Por otra parte, si $m_{ji} = 0$, entonces $m_{ij} = 0$. En consecuencia, $\mathbf{M}_R$ es una matriz tal que cada par de entradas, simétricamente colocadas en torno de la diagonal principal, son ya sea ambas 0 o ambas 1. Se desprende que $\mathbf{M}_R = \mathbf{M}_R^{t}$, de manera que $\mathbf{M}_R$ es una matriz simétrica (véase la sección 1.5).

La matriz $\mathbf{M}_R = [m_{ij}]$ de una relación asimétrica R satisface la propiedad de que

$$\text{si } m_{ij} = 1, \quad \text{entonces } m_{ji} = 0.$$

Si R es asimétrica, se desprende que $m_{ii} = 0$ para todas las i; es decir, la diagonal principal de la matriz $\mathbf{M}_R$ consta en su totalidad de ceros. Esto debe ser verdadero, ya que la propiedad asimétrica implica que si $m_{ii} = 1$, entonces $m_{ii} = 0$, lo cual es una contradicción.

Finalmente, la matriz $\mathbf{M}_R = [m_{ij}]$ de una relación antisimétrica R satisface la propiedad de que si $i \neq j$, entonces $m_{ij} = 0$ o $m_{ji} = 0$.

Ejemplo 6. Considere las matrices de la figura 4.19, cada una de las cuales es la matriz de una relación, como se indica.

Las relaciones R_1 y R_2 son simétricas en vista de que las matrices $\mathbf{M}_{R_1}$ y $\mathbf{M}_{R_2}$ son matrices simétricas. La relación R_3 es antisimétrica, ya que ninguna de las posiciones de $\mathbf{M}_{R_3}$ situadas simétricamente fuera de la diagonal contiene unos a la vez. Ambas posiciones pueden tener ceros; sin embargo, los elementos de la diagonal están irrestrictos. La relación R_3 no es asimétrica porque $\mathbf{M}_{R_3}$ tiene unos en la diagonal principal.

La relación R_4 no tiene ninguna de las tres propiedades: $\mathbf{M}_{R_4}$ no es simétrica. La presencia de 1 en la posición 4, 1 de $\mathbf{M}_{R_4}$ viola tanto la asimetría como la antisimetría.

Por último, R_5 es antisimétrica pero no asimétrica, y R_6 es ambas cosas, asimétrica y antisimétrica. ◆

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \mathbf{M}_{R_1}$$

(a)

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = \mathbf{M}_{R_2}$$

(b)

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \mathbf{M}_{R_3}$$

(c)

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \mathbf{M}_{R_4}$$

(d)

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \mathbf{M}_{R_5}$$

(e)

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \mathbf{M}_{R_6}$$

(f)

Figura 4.19

Se va a considerar ahora los digrafos de estos tres tipos de relaciones. Si R es una relación asimétrica, entonces el digrafo de R no puede tener simultáneamente un lado (o arco) del vértice i al vértice j y otro lado del vértice j al vértice i. Esto es cierto para cualquier i y para cualquier j, y en particular si i es igual a j. En consecuencia, no puede haber ciclos de longitud 1, y todos los lados son "calles de un solo sentido".

Si R es una relación antisimétrica, entonces para diferentes vértices i y j no puede haber un lado del vértice i al vértice j y otro del vértice j al vértice i. Cuando $i = j$, no se impone condición alguna. En consecuencia, puede haber ciclos de longitud 1, pero una vez más, todos los lados son "de un solo sentido".

Se va a estudiar los digrafos de las relaciones simétricas con mayor detalle.

El digrafo de una relación simétrica R tiene la propiedad de que si hay un lado del vértice i al vértice j, entonces hay un lado del vértice j al vértice i. En consecuencia, si dos vértices están conectados por un lado, deben estar siempre conectados en ambas direcciones. Por esta razón, es posible y bastante útil realizar una representación diferente de una relación simétrica. Se conserva los vértices como aparecen en el digrafo, pero si dos vértices a y b están conectados por los lados en cada dirección, se reemplaza estos dos lados con un lado no dirigido, es decir, una "calle de dos sentidos". Este lado no dirigido es simplemente una línea sencilla sin flechas, que conecta a y b. El diagrama resultante será llamado **gráfica** de la relación simétrica. (A la palabra gráfica se le dará un significado más general en el capítulo 6.)

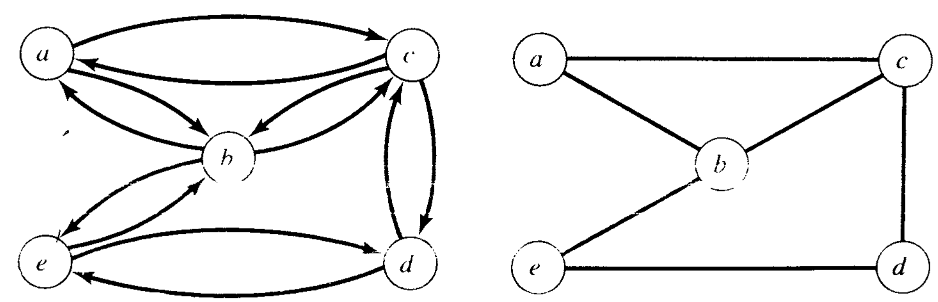
Ejemplo 7. Sea $A = \{a, b, c, d, e\}$ y sea R la relación simétrica dada por

$$R = \{(a, b), (b, a), (a, c), (c, a), (b, c), (c, b), (b, e), (e, b), (e, d), (d, e), (c, d), (d, c)\}.$$

El digrafo usual de R aparece en la figura 4.20(a), mientras que la figura 4.20(b) muestra la gráfica de R. Nótese que cada lado no dirigido corresponde a dos pares ordenados en la relación R. ◆

Un lado no dirigido entre a y b, en la gráfica de una relación simétrica R, corresponde a un conjunto $\{a, b\}$ tal que $(a, b) \in R$ y $(b, a) \in R$. En ocasiones también se hará referencia a dicho conjunto $\{a, b\}$ como a un **lado no dirigido** de la relación R y se llamará a a y b **vértices adyacentes**.

Se dirá que una relación simétrica R en un conjunto A es **conectada**, si hay una trayectoria de cualquier elemento de A a cualquier otro elemento de A. Esto significa simplemente

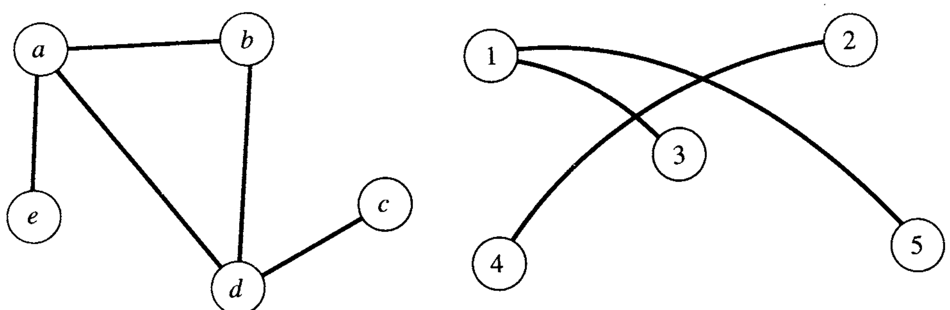


Digrafo de R
(a)

Gráfica de R
(b)

Figura 4.20

que la gráfica de R es toda de una pieza. En la figura 4.21 se muestra las gráficas de dos relaciones simétricas. La gráfica de la figura 4.21(a) es conectada, mientras que la de la figura 4.21(b) no es conectada. ♦



(a) (b)

Figura 4.21

Relaciones transitivas

Se dice que una relación R en un conjunto A es **transitiva** si siempre que se tiene $a\ R\ b$ y $b\ R\ c$, entonces $a\ R\ c$. Con frecuencia es conveniente explicar lo que significa para una relación ser no transitiva. Una relación R en A es no transitiva si existen a, b y c en A de manera que $a\ R\ b$ y $b\ R\ c$, pero $a \not R\ c$. Si no existen tales a, b y c, entonces R es transitiva.

Ejemplo 8. Sea $A = Z$, el conjunto de los enteros, y sea R la relación considerada en el ejemplo 2. para ver si R es transitiva, se supone que $a\ R\ b$ y $b\ R\ c$. En consecuencia, $a < b$ y $b < c$. Entonces se desprende que $a < c$, de modo que $a\ R\ c$. Por tanto R es transitiva. ♦

Ejemplo 9. Sea $A = Z^+$ y sea R la relación considerada en el ejemplo 5. ¿Es R transitiva?

Solución: Supóngase que $a\ R\ b$ y $b\ R\ c$, de modo que $a \mid b$ y $b \mid c$. Se desprende entonces que $a \mid c$. Véase el teorema 2(d) de la sección 1.4. En consecuencia, R es transitiva. ♦

Ejemplo 10. Sea $A = \{1, 2, 3, 4\}$ y sea

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

¿Es R transitiva?

Solución: Puesto que no existen elementos a, b y c en A tales que $a\ R\ b$ y $b\ R\ c$, pero $a \not R\ c$, se concluye que R es transitiva. ♦

Una relación R es transitiva si y sólo si su matriz $\mathbf{M}_R = [m_{ij}]$ tiene la propiedad

$$\text{si } m_{ij} = 1 \quad \text{y} \quad m_{jk} = 1, \quad \text{entonces} \quad m_{ik} = 1.$$

El primer miembro de este enunciado significa simplemente que $(\mathbf{M}_R)^2_{\odot}$ tiene un 1 en la posición i, k. Así, la transitividad de R significa que si $(\mathbf{M}_R)^2_{\odot}$ tiene un 1 en cualquier posición, entonces $\mathbf{M}_R$ debe tener un 1 en la misma posición. Por tanto, en particular, si $(\mathbf{M}_R)^2_{\odot} = \mathbf{M}_R$, entonces R es transitiva. La inversa no es verdadera.

Ejemplo 11. Sea $A = \{1, 2, 3\}$ y sea R la relación sobre A cuya matriz es

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Demuestre que R es transitiva.

Solución: Por cálculo directo, $(\mathbf{M}_R)^2_{\odot} = \mathbf{M}_R$; por lo tanto, R es transitiva. ♦

Para ver lo que la transitividad significa para el digrafo de una relación, se traduce la definición de transitividad a términos geométricos.

Si se considera los vértices particulares a y c, las condiciones $a\ R\ b$ y $b\ R\ c$ significan que hay una trayectoria de longitud 2 en R de a a c. En otras palabras, $a\ R^2\ c$. Por lo tanto, se puede reconstruir el enunciado de la definición de transitividad como sigue: Si $a\ R^2\ c$, entonces $a\ R\ c$; es decir, $R^2 \subseteq R$ (como subconjuntos de $A \times A$). En otras palabras, si a y c están conectados por una trayectoria de longitud 2 en R, entonces deben estar conectados por una trayectoria de longitud 1.

Es posible generalizar ligeramente la caracterización geométrica anterior de transitividad, de la siguiente manera.

Teorema 1. *Una relación R es transitiva si y solamente si satisface la siguiente propiedad: Si hay una trayectoria de longitud mayor que 1 del vértice a al vértice b (hay también una trayectoria de longitud 1 de a a b). Enunciado en términos algebraicos, R es transitiva si y sólo si $R^n \subseteq R$ para todas las $n \geq 1$.*

Demostración: La demostración se deja al lector. ●

Será conveniente tener una reexpresión de algunas de las propiedades anteriores en términos de conjuntos relacionados en R. Se presenta a continuación una lista de estos enunciados sin demostración.

Teorema 2. Sea R una relación sobre un conjunto A. Entonces

(a) Reflexividad de R significa que $a \in R(a)$ para todas las a en A.
(b) Simetría de R significa que $a \in R(b)$ si y sólo si $b \in R(a)$.
(c) Transitividad de R significa que si $b \in R(a)$ y $c \in R(b)$, entonces $c \in R(a)$. ●

GRUPO DE EJERCICIOS 4.4

En los ejercicios 1 al 8, sea $A = \{1, 2, 3, 4\}$. Determine si la relación es reflexiva, irreflexiva, simétrica, asimétrica, antisimétrica o transitiva.

1. $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$
2. $R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$
3. $R = \{(1, 3), (1, 1), (3, 1), (1, 2), (3, 3), (4, 4)\}$
4. $R = \{(1, 1), (2, 2), (3, 3)\}$
5. $R = \varnothing$

6. $R = A \times A$

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

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

En los ejercicios 9 y 10 (figuras 4.22 y 4.23), sea $A = \{1, 2, 3, 4, 5\}$. Determine si la relación R cuyo digrafo se da es reflexiva, irreflexiva, simétrica, asimétrica, antisimétrica o transitiva.

9.

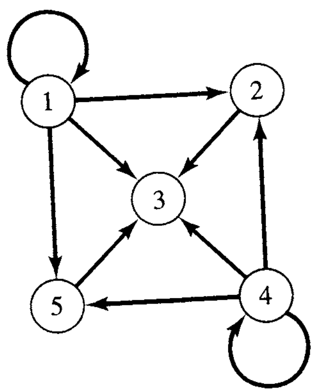


Figura 4.22

10.

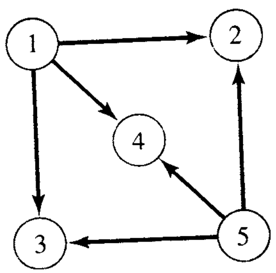


Figura 4.23

En los ejercicios 11 y 12, sea $A = \{1, 2, 3, 4\}$. Determine si la relación R cuya matriz $\mathbf{M}_R$ se da es reflexiva, irreflexiva, simétrica, asimétrica, antisimétrica o transitiva.

11. $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

12. $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

En los ejercicios 13 al 22, determine si la relación R en el conjunto A es reflexiva, irreflexiva, simétrica, asimétrica, antisimétrica o transitiva.

13. $A = Z$; $a\,R\,b$ si y sólo si $a \leq b + 1$.

14. $A = Z^+$; $a\,R\,b$ si y sólo si $|a - b| \leq 2$.

15. $A = Z^+$; $a\,R\,b$ si y sólo si $a = b^k$ para alguna $k \in Z^+$.

16. $A = Z$; $a\,R\,b$ si y sólo si $a + b$ es par.

17. $A = Z$; $a\,R\,b$ si y sólo si $|a - b| = 2$.

18. A = el conjunto de los números reales; $a\,R\,b$ si y sólo si $a^2 + b^2 = 4$.

19. $A = Z^+$; $a\,R\,b$ si y sólo si $\text{MCD}(a, b) = 1$. En este caso, se dice que a y b son **primos relativos**. (Véase la sección 1.4 para el MCD.)

20. A = el conjunto de todos los pares ordenados de números reales; $(a, b)\,R\,(c, d)$ si y sólo si $a = c$.

21. $S = \{1, 2, 3, 4\}$, $A = S \times S$; $(a, b)\,R\,(c, d)$ si y sólo si $ad = bc$.

22. A es el conjunto de todas las líneas que hay en el plano; $l_1\,R\,l_2$ si y sólo si l_1 es paralela a l_2.

23. Sea R la siguiente relación simétrica en el conjunto $A = \{1, 2, 3, 4, 5\}$.
$$R = \{(1, 2), (2, 1), (3, 4), (4, 3), (3, 5), (5, 3), (4, 5), (5, 4), (5, 5)\}.$$
Dibuje la gráfica de R.

24. Sea $A = \{a, b, c, d\}$ y sea R la relación simétrica
$$R = \{(a, b), (b, a), (a, c), (c, a), (a, d), (d, a)\}.$$
Dibuje la gráfica de R.

25. Considere la gráfica de una relación simétrica R en $A = \{1, 2, 3, 4, 5, 6, 7\}$ que aparece en la figura 4.24. Determine R (haga una lista de todos los pares).

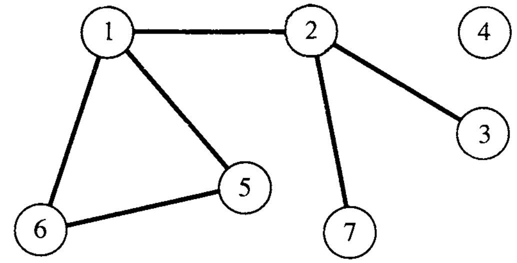


Figura 4.24

26. Considere la gráfica de una relación simétrica R en $A = \{a, b, c, d, e\}$ que aparece en la figura 4.25. Determine R (haga una lista de todos los pares).

27. Demuestre que si una relación sobre un conjunto A es transitiva e irreflexiva, entonces es asimétrica.

28. Demuestre que si una relación R en un conjunto A es simétrica, entonces la relación R^2 también es simétrica.

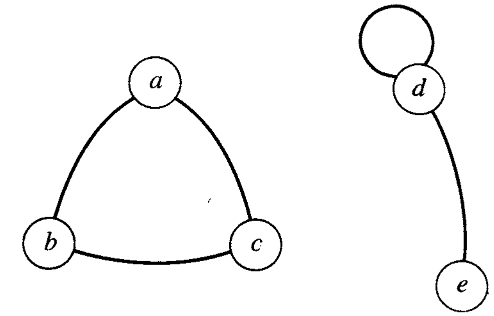


Figura 4.25

29. Demuestre, por inducción, que si una relación R en un conjunto A es simétrica, entonces R^n es simétrica para $n \geq 1$.

30. Sea R una relación no vacía en un conjunto A. Supóngase que R es simétrica y transitiva. Demuestre que R no es irreflexiva.

4.5. Relaciones de equivalencia

Una relación R en un conjunto A se llama **relación de equivalencia** si es reflexiva, simétrica y transitiva.

Ejemplo 1. Sea A el conjunto de todos los triángulos del plano y sea R la relación sobre A definida como sigue:
$$R = \{(a, b) \in A \times A \mid a \text{ es congruente con } b\}.$$
Es fácil ver que R es una relación de equivalencia. ◆

Ejemplo 2. Sea $A = \{1, 2, 3, 4\}$ y sea
$$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4)\}.$$
Es fácil verificar que R es una relación de equivalencia. ◆

Ejemplo 3. Sea $A = Z$, el conjunto de los enteros, y supóngase que se define R por $a\,R\,b$ si y sólo si $a \leq b$. ¿Es R una relación de equivalencia?

Solución: Puesto que $a \leq a$, R es reflexiva. Si $a \leq b$, no necesariamente se sigue que $b \leq a$, por lo cual R no es simétrica. Incidentalmente, R es transitiva, porque $a \leq b$ y $b \leq c$ implican que $a \leq c$. Se ve que R no es una relación de equivalencia. ◆

Ejemplo 4. Sea $A = Z$ y sea
$$R = \{(a, b) \in A \times A \mid a \equiv r \text{ (mód 2) y } b \equiv r \text{ (mód 2)}\}.$$

Es decir, $a\ R\ b$ si y sólo si a y b dan el mismo residuo, r, al ser divididos entre 2. En este caso, se escribe $a \equiv b$ (mód 2), léase "a es congruente con b módulo 2".

Demuestre que congruencia módulo 2 es una relación de equivalencia.

Solución: Primero, es claro que $a \equiv a$ (mód 2). Por lo tanto R es reflexiva. Segundo, si $a \equiv b$ (mód 2) entonces, por definición, $a \equiv r$ (mód 2) y $b \equiv r$ (mód 2), de modo que $b \equiv a$ (mód 2). R es simétrica.

Finalmente, supóngase que $a \equiv b$ (mód 2) y $b \equiv c$ (mód 2). Entonces, $a \equiv r$ (mód 2), $b \equiv r$ (mód 2), y $c \equiv r$ (mód 2). Es decir, los tres dan el mismo residuo al ser divididos entre 2. En consecuencia, $a \equiv c$ (mód 2). Por consiguiente, congruencia mód 2 es una relación de equivalencia. ◆

Ejemplo 5. Sea $A = Z$ y sea $n \in Z^+$. Se generaliza la relación definida en el ejemplo 4, como sigue. Sea

$$R = \{(a, b) \in A \times A \mid a \equiv b \text{ (mód } n)\}.$$

Es decir, $a \equiv b$ (mód n) si y sólo si a y b dan el mismo residuo al ser divididos entre n. Procediendo exactamente como en el ejemplo 4, puede demostrarse que la congruencia módulo n es una relación de equivalencia. ◆

Relaciones de equivalencia y particiones

El siguiente resultado muestra que si $\mathcal{P}$ es una partición de un conjunto A (véase la sección 4.1), entonces $\mathcal{P}$ puede usarse para construir una relación de equivalencia en A.

Teorema 1. *Sea $\mathcal{P}$ una partición de un conjunto A. Recuérdese que a los conjuntos en $\mathcal{P}$ se los llama bloques de $\mathcal{P}$. Se define la relación R en A como sigue:*

$a\ R\ b$ si y sólo si a y b son miembros del mismo bloque.

Entonces R es una relación de equivalencia en A.

Demostración

(1) Si $a \in A$, entonces es claro que a está en el mismo bloque que ella misma; por tanto, $a\ R\ a$.

(2) Si $a\ R\ b$, entonces a y b están en el mismo bloque; por tanto $b\ R\ a$.

(3) Si $a\ R\ b$ y $b\ R\ c$, entonces a, b y c deben estar todos en el mismo bloque de $\mathcal{P}$. En consecuencia $a\ R\ c$.

Puesto que R es reflexiva, simétrica y transitiva, R es una relación de equivalencia. A R se la llamará **relación de equivalencia determinada por** $\mathcal{P}$. ●

Ejemplo 6. Sea $A = \{1, 2, 3, 4\}$ y considérese la partición $\mathcal{P} = \{\{1, 2, 3\}, \{4\}\}$ de A. Determine la relación de equivalencia R en A determinada por $\mathcal{P}$.

Solución: Los bloques de $\mathcal{P}$ son $\{1, 2, 3\}$ y $\{4\}$. Cada elemento de un bloque está relacionado con cada uno de los demás elementos del mismo bloque y solamente con estos elementos. En consecuencia, en este caso,

$$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4)\}. \quad ◆$$

Si $\mathcal{P}$ es una partición de A y R es la relación de equivalencia determinada por $\mathcal{P}$, entonces los bloques de $\mathcal{P}$ pueden ser descritos fácilmente en términos de R. Si A_1 es un bloque de $\mathcal{P}$ y $a \in A_1$, se ve por definición que A_1 consta de todos los elementos x de A con $a\ R\ x$. Es decir, $A_1 = R(a)$. En consecuencia, la partición $\mathcal{P}$ es $\{R(a) \mid a \in A\}$. En palabras, $\mathcal{P}$ consta de todos los conjuntos distintos relacionados en R que tienen su origen en los elementos de A. Por ejemplo, en el ejemplo 6 los bloques $\{1, 2, 3\}$ y $\{4\}$ pueden ser descritos, respectivamente, como $R(1)$ y $R(4)$. Por supuesto, $\{1, 2, 3\}$ podría describirse también como $R(2)$ o $R(3)$, por tanto, esta manera de representar los bloques no es única.

La construcción anterior de relaciones de equivalencia partiendo de particiones es muy simple. Se estaría tentado a creer que podrían producirse de esta manera pocas relaciones de equivalencia. El hecho es, como se demostrará ahora, que todas las relaciones de equivalencia en A puede producirse a partir de particiones.

Se comienza con el resultado siguiente. Como su demostración utiliza el teorema 2 de la sección 4.4, el lector podría querer revisar ese teorema.

Lema 1†. *Sea R una relación de equivalencia en un conjunto A, y sean $a \in A$ y $b \in A$. Entonces*

$$a\ R\ b \quad \textit{si y sólo si} \quad R(a) = R(b).$$

Demostración: *Supóngase primero que* $R(a) = R(b)$. Puesto que R es reflexiva, $b \in R(b)$; por lo tanto, $b \in R(a)$, de manera que $a\ R\ b$.

A la inversa, supóngase que $a\ R\ b$. Entonces obsérvese que

1. $b \in R(a)$ por definición; por lo tanto, como R es simétrica,
2. $a \in R(b)$ por el teorema 2 (b) de la sección 4.4.

Se debe demostrar que $R(a) = R(b)$. Primero, escoja un elemento $x \in R(b)$. Puesto que R es transitiva, el hecho de que $x \in R(b)$, junto con (1) anterior, implica por el teorema 2(c) de la sección 4.4 que $x \in R(a)$. En consecuencia, $R(b) \subseteq R(a)$. Ahora escoja $y \in R(a)$. Este hecho y el inciso (2) anterior implican, como antes, que $y \in R(b)$. En consecuencia, $R(a) \subseteq R(b)$, de modo que se debe tener $R(a) = R(b)$. ●

Ahora se demuestra el resultado principal.

Teorema 2. *Sea R una relación de equivalencia sobre A, y sea $\mathcal{P}$ la colección de todos los conjuntos distintos relativos $R(a)$ para a en A. Entonces $\mathcal{P}$ es una partición de A, y R es la relación de equivalencia determinada por $\mathcal{P}$.*

Demostración: De acuerdo con la definición de partición, se debe demostrar las dos propiedades siguientes:

(a) Todo elemento de A pertenece a algún conjunto relativo.

(b) Si $R(a)$ y $R(b)$ no son idénticos, entonces $R(a) \cap R(b) = \varnothing$.

† Un lema es un teorema cuyo propósito principal es ayudar en la demostración de otro teorema.

Ahora la propiedad (a) es verdadera, ya que $a \in R(a)$ por reflexividad de R. Para demostrar la propiedad (b) se demostrará el siguiente enunciado equivalente:

$$\text{Si } R(a) \cap R(b) \neq \varnothing, \text{ entonces } R(a) = R(b).$$

Para demostrar esto, se supone que $c \in R(a) \cap R(b)$. Entonces $a\ R\ c$ y $b\ R\ c$.

Como R es simétrica, se tiene que $c\ R\ b$. Entonces $a\ R\ c$ y $c\ R\ b$, por lo que, por transitividad de R, $a\ R\ b$. El lema 1 dice que $R(a) = R(b)$. Se ha demostrado ahora que $\mathcal{P}$ es una partición. Por el lema 1 se ve que $a\ R\ b$ si y sólo si a y b pertenecen al mismo bloque de $\mathcal{P}$. En consecuencia $\mathcal{P}$ determina a R, y el teorema queda demostrado. ●

Si R es una relación de equivalencia en A, entonces a los conjuntos $R(a)$ tradicionalmente se los llama **clases de equivalencia** de R. Algunos autores denotan la clase $R(a)$ por $[a]$ (véase la sección 9.3). La partición $\mathcal{P}$ construida en el teorema 2, por lo tanto, consta de todas las clases de equivalencia de R, y esta partición será denotada por A/R. Debe recordarse que a las particiones de A se las llama también **conjuntos cociente** de A, y la notación A/R recuerda que $\mathcal{P}$ es el conjunto cociente de A que está construido a partir de R y que determina a R.

Ejemplo 7. Sea R la relación definida en el ejemplo 2. Determine A/R.

Solución: Del ejemplo 2 se tiene $R(1) = \{1, 2\} = R(2)$. También, $R(3) = \{3, 4\} = R(4)$. Por tanto, $A/R = \{\{1, 2\}, \{3, 4\}\}$. ◆

Ejemplo 8. Sea R la relación de equivalencia definida en el ejemplo 4. Determine A/R.

Solución: Primero, $R(0) = \{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$, el conjunto de los enteros pares, ya que el residuo es cero al dividir cada uno de estos números entre 2.

$$R(1) = \{\ldots, -5, -3, -1, 0, 1, 3, 5, 7, \ldots\},$$

el conjunto de los enteros impares, puesto que cada uno da un residuo de 1 al ser dividido entre 2. Por tanto, A/R consta del conjunto de los enteros pares y el conjunto de los enteros impares. ◆

De los ejemplos 7 y 8 se puede derivar un procedimiento general para determinar las particiones A/R finitas o numerables. El procedimiento es como sigue:

PASO 1. Escoja cualquier elemento de A y calcule la clase de equivalencia $R(a)$.

PASO 2. Si $R(a) \neq A$, escoja un elemento b, no incluido en $R(a)$, y calcule la clase de equivalencia $R(b)$.

PASO 3. Si A no es la unión de clases de equivalencia previamente calculadas, escoja entonces un elemento x de A que no esté en ninguna de esas clases de equivalencia y calcule $R(x)$.

PASO 4. Repita el paso 3 hasta que estén incluidos todos los elementos de A en las clases de equivalencia calculadas. Si A es numerable, este proceso podría continuar indefinidamente. En ese caso, continúe hasta que surja un patrón que le permita describir o dé una fórmula para todas las clases de equivalencia.

GRUPO DE EJERCICIOS 4.5

En los ejercicios 1 y 2, sea $A = \{a, b, c\}$. Determine si la relación R, cuya matriz $\mathbf{M}_R$ se proporciona, es una relación de equivalencia.

1. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$

2. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$

En los ejercicios 3 y 4 (figuras 4.26 y 4.27), determine si la relación R, cuyo digrafo se proporciona es una relación de equivalencia.

3.

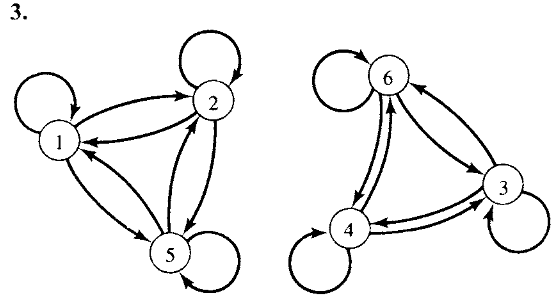


Figura 4.26

4.

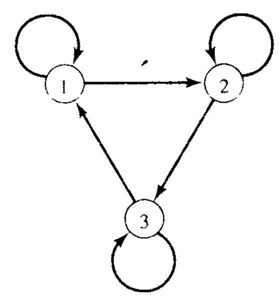


Figura 4.27

En los ejercicios 5 al 12, determine si la relación R en el conjunto A es una relación de equivalencia.

5. $A = \{a, b, c, d\}$, $R = \{(a, a), (b, a), (b, b), (c, c), (d, d), (d, c)\}$

6. $A = \{1, 2, 3, 4, 5\}$, $R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 1), (2, 3), (3, 3), (4, 4), (3, 2), (5, 5)\}$

7. $A = \{1, 2, 3, 4\}$, $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 3), (1, 3), (4, 1), (4, 4)\}$

8. A = el conjunto de todos los miembros del Software-of-the Month Club; $a\ R\ b$ si y sólo si a y b compran el mismo número de programas.

9. A = el conjunto de todos los miembros del Software-of-the Month Club; $a\ R\ b$ si y sólo si a y b compran los mismos programas.

10. A = el conjunto de toda la gente que está en la base de datos del Seguro Social; $a\ R\ b$ si y sólo si a y b tienen el mismo apellido.

11. A = el conjunto de todos los triángulos del plano; $a\ R\ b$ si y sólo si a es semejante a b.

12. $A = Z^+ \times Z^+$; $(a, b)\ R\ (c, d)$ si y sólo si $b = d$.

13. Si $\{\{a, c, e\}, \{b, d, f\}\}$ es una partición del conjunto $A = \{a, b, c, d, e, f\}$, determine la relación de equivalencia correspondiente R.

14. Si $\{\{1, 3, 5\}, \{2, 4\}\}$ es una partición del conjunto $A = \{1, 2, 3, 4, 5\}$, determine la relación de equivalencia correspondiente R.

15. Sea $S = \{1, 2, 3, 4, 5\}$ y sea $A = S \times S$. Defina la siguiente relación R en A: $(a, b)\ R\ (a', b')$ si y sólo si $ab' = a'b$.

(a) Demuestre que R es una relación de equivalencia.

(b) Calcule A/R.

16. Sea $S = \{1, 2, 3, 4\}$ y sea $A = S \times S$. Defina la relación siguiente R en A: $(a, b)\ R(a', b')$ si y sólo si $a + b = a' + b'$.
    (a) Demuestre que R es una relación de equivalencia.
    (b) Calcule A/R.

17. Una relación R en un conjunto A se llama **circular** si $a\ R\ b$ y $b\ R\ c$ implican $c\ R\ a$. Demuestre que R es reflexiva y circular si y sólo si es una relación de equivalencia.

18. Demuestre que si R_1 y R_2 son relaciones de equivalencia en A, entonces $R_1 \cap R_2$ es una relación de equivalencia en A.

19. Defina una relación de equivalencia R en Z, el conjunto de los enteros, diferente de la usada en los ejemplos 4 y 8 y cuya partición correspondiente contiene exactamente dos conjuntos infinitos.

20. Defina una relación de equivalencia R en Z, el conjunto de los enteros, cuya partición correspondiente contiene exactamente tres conjuntos infinitos.

4.6. Representación en computadora de relaciones y digrafos

El método más directo para almacenar elementos de datos es colocarlos en una lista o arreglo lineal. Esto equivale generalmente a poner elementos de datos consecutivos en lugares de almacenamiento con numeración consecutiva en la memoria de una computadora. La figura 4.28 ilustra este método para cinco elementos de datos $D_1, \ldots, D_5$. El método representa un uso eficiente de espacio y proporciona, por lo menos al nivel de la mayoría de los lenguajes de programación, acceso directo a los datos. Así, el arreglo lineal podría ser A y los datos estarían en las localidades $A[1], A[2], A[3], A[4], A[5]$, y se tendría acceso a cualquier dato D_i proporcionando simplemente su índice i.

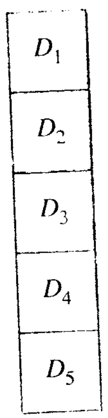


Figura 4.28

El problema principal que se tiene con este método de almacenamiento es que no se puede insertar nuevos datos entre los datos existentes sin tener que mover un número posiblemente grande de elementos. Por ejemplo, para agregar otro elemento E a la lista de la figura 4.28 y colocar E entre D_2 y D_3, se tendría que mover D_3 a $A[4]$, D_4 a $A[5]$, y D_5 a $A[6]$, si hay espacio, y luego asignar E a $A[3]$.

Un método alternativo para representar esta secuencia es por medio de una **lista enlazada**, que se muestra en forma esquemática en la figura 4.29. El almacenamiento de la unidad básica de información es la **celda de almacenamiento**. Se imagina que tales celdas

tienen espacio para dos elementos de información. El primero puede ser de datos (números o símbolos), y el segundo elemento es un **apuntador** (puntero), es decir, un número que dice (que señala) la localización de la siguiente celda por considerar. En consecuencia, las celdas pueden estar dispuestas en sucesión, pero los elementos de datos que representan no necesariamente estarán en la misma sucesión. En vez de eso, se descubre la sucesión correcta de los datos siguiendo los apuntadores de cada elemento al siguiente.

Como se ilustra en la figura 4.29, se representa la celda de almacenamiento como una caja con particiones DATOS | ●, con un punto en el lado derecho que representa un apuntador. Se dibuja una línea desde cada uno de estos puntos a la celda que el apuntador correspondiente designa como el siguiente. El símbolo ● significa que se han terminado los datos y que no se necesita seguir más apuntadores.

En la práctica, puede ponerse a funcionar el concepto de lista enlazada, utilizando dos arreglos enlazados, un arreglo de datos A y un arreglo de apuntadores P, como se muestra en la figura 4.30. Obsérvese que una vez que se ha tenido acceso a los datos de la posición $A[i]$, el número de la posición $P[i]$ da, o señala, el índice de A que contiene el siguiente elemento de datos.

Así, si se estuviera en la posición $A[3]$, logrando acceder al elemento de datos D_2, entonces la posición $P[3]$ contendría a 5, puesto que el siguiente elemento de datos, D_3, está situado en $A\ [5]$. Un cero en alguna posición de P significa que no existen más elementos de datos. En la figura 4.30, $P[4]$ es cero porque $A[4]$ contiene a D_5, el último elemento de datos. En este esquema, se necesita dos arreglos para los datos previamente representados en un solo arreglo, y sólo se tiene acceso en sucesión. En consecuencia, no se puede localizar D_2 directamente, sino que se debe ir por los enlaces hasta llegar a esta posición. La gran ventaja de este método, empero, es que el orden físico real de los datos no tiene que ser el mismo que el orden lógico o natural. En el ejemplo anterior, el orden natural es $D_1D_2D_3D_4D_5$, pero los datos no están almacenados de esta manera. Los enlaces permiten pasar de manera natural por los datos, sin importar cómo estén almacenados. Así es muy fácil agregar nuevos

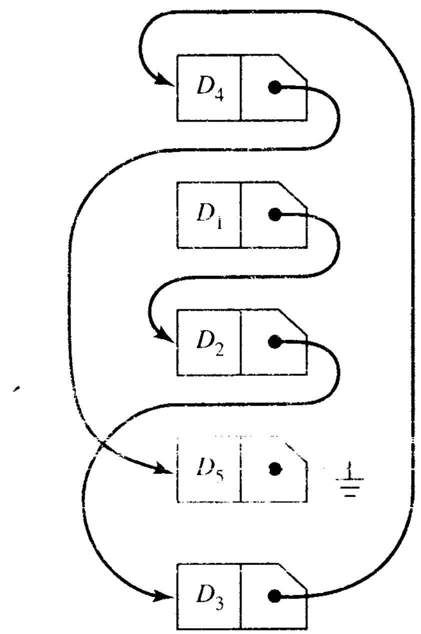


Figura 4.29

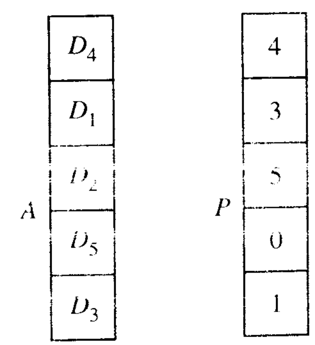


Figura 4.30

elementos en cualquier parte. Si se quiere insertar el elemento E entre D_2 y D_3, se anexa E al extremo del arreglo A, se cambia un apuntador, y se anexa otro apuntador, como se muestra en la figura 4.31. Este enfoque puede usarse sin importar qué tan larga sea la lista. Se debería tener una variable adicional START manteniendo el índice del primer elemento de datos. En las figuras 4.30 y 4.31, START contendría a 2, puesto que D_1 está en $A[2]$.

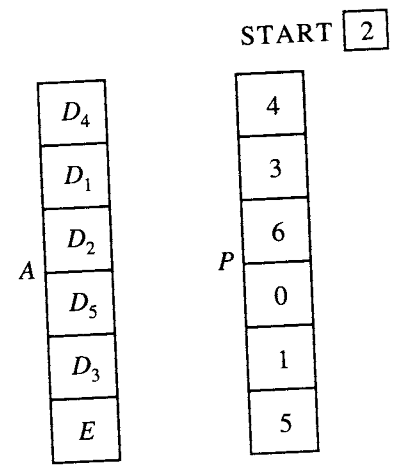


Figura 4.31

No importa qué tan grande sea el elemento de datos, dentro de las limitaciones de la computadora, de manera que A podría ser realmente un arreglo bidimensional o una matriz. El primer renglón contendría varios números con la descripción del primer elemento de datos, el segundo describiría el siguiente elemento de datos, y así sucesivamente. Los datos pueden ser un apuntador a la posición de los datos reales.

El problema de almacenar información para representar una relación o su digrafo tiene también dos soluciones similares a las presentadas antes para datos simples. En primer lugar, se sabe, por la sección 4.2, que una relación R en A puede representarse por una matriz $\mathbf{M}_R$, $n \times n$, si A tiene n elementos. La matriz $\mathbf{M}_R$ tiene entradas que son 0 o 1. Entonces, una forma directa de representar R en una computadora sería por medio de un arreglo $n \times n$ que tenga ceros y unos almacenados en cada posición. Así, si $A = \{1, 2\}$ y $R = \{(1, 1), (1, 2), (2, 2)\}$, entonces

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

y estos datos podrían ser representados por un arreglo bidimensional MAT, en el cual MAT[1, 1] = 1, MAT[1, 2] = 1, MAT[2, 1] = 0 y MAT[2, 2] = 1.

Un segundo método de almacenamiento de datos para relaciones y digrafos utiliza la idea de la lista enlazada antes descrita. Para que resulte más claro, se usa un lenguaje gráfico. Se construirá una lista enlazada que contiene todos los lados del digrafo, es decir, los pares ordenados de números que determinan esos lados. Los datos pueden ser representados por dos arreglos. TAIL y HEAD, dando el vértice inicial y el vértice final, respectivamente, para todas las flechas. Si se quiere transformar estos datos en una lista enlazada, se necesita también un arreglo NEXT (siguiente) de apuntadores que partan de cada lado al siguiente.

Considérese la relación cuyo digrafo aparece en la figura 4.32. Los vértices son los enteros 1 al 6 y de manera arbitraria se numera los lados como se muestra.

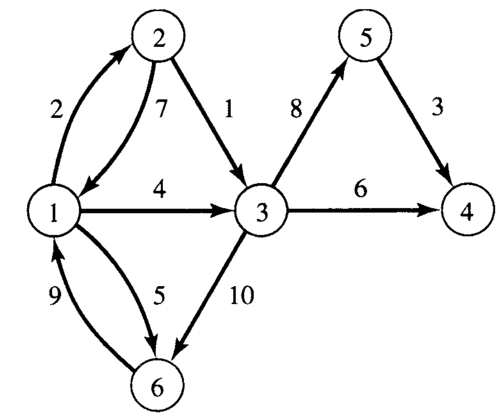


Figura 4.32

Si se desea almacenar el digrafo en forma de lista enlazada de manera que el orden lógico coincida con la numeración de los lados, se puede usar un esquema como el que se ilustra en la figura 4.33. START contiene a 2, el índice del primer elemento de datos, y al lado (2, 3) (este lado está marcado con un 1 en la figura 4.32). Este lado está almacenado en las segundas entradas de TAIL y HEAD, respectivamente. Puesto que NEXT[2] contiene 10, el siguiente lado es el que está situado en la posición 10 de TAIL y HEAD, es decir (1, 2) (lado marcado 2 en la figura 4.32).

NEXT[10] contiene a 5, de manera que se va en seguida a la posición de datos 5, la cual contiene al lado (5, 4). Este proceso continúa hasta que se llega al lado (3, 6) en la posición de datos 7. Éste es el último lado, y se indica este hecho al tener que NEXT[7] contiene 0. Se usa 0 como apuntador, para indicar la inexistencia de más datos.

Si se sigue el rastro de este proceso, se encontrará los lados exactamente en el orden que corresponde a su numeración. Se puede arreglar, de una manera similar, para pasar por los lados en cualquier orden deseado.

Este esquema y las numerosas variantes equivalentes del mismo tienen desventajas importantes. En muchos algoritmos, es eficiente localizar un vértice y luego comenzar de inmediato a investigar los lados que comienzan o terminan con este vértice. En general, esto no es posible con el mecanismo de almacenamiento que se muestra en la figura 4.33, por lo cual se proporciona ahora una modificación del mismo. Se usa un arreglo lineal adicional VERT que tiene una posición para cada vértice en el digrafo. Para cada vértice I, VERT[I] es el índice, en TAIL y HEAD, del primer lado que se desea considerar saliendo del vértice I (en el digrafo de la figura 4.32, el primer lado podría tomarse como el lado con el numero de marca más pequeño). En consecuencia, VERT, al igual que NEXT, contiene apuntadores hacia los lados. Para cada vértice I, se debe arreglar los apuntadores de NEXT de manera que enlacen todos los lados que salgan de I, que inicie en el lado al que señale VERT[I]. En cada caso, el último de estos lados se hace señalar a cero. En un sentido, los arreglos de datos TAIL y HEAD contienen realmente varias listas enlazadas de lados, una lista para cada vértice.

START	TAIL	HEAD	NEXT
2	1	3	9
	2	3	10
	2	1	4
	3	5	8
	5	4	1
	3	4	3
	3	6	0
	6	1	7
	1	6	6
	1	2	5

Figura 4.33

Este método se ilustra en la figura 4.34 para el digrafo de la figura 4.32. Aquí VERT[1] contiene a 10, de modo que el primer lado que sale del vértice 1 debe estar almacenado en la décima posición de datos. Éste es el lado (1, 3). Puesto que NEXT[10] = 9, el siguiente lado que sale del vértice 1 es (1, 6) situado en la posición de datos 9. Una vez más NEXT[9] = 1, lo cual señala hacia el lado (1, 2) en la posición de datos 1. Puesto que NEXT[1] = 0, se ha llegado al final de los lados que comienzan en el vértice 1. El orden de los lados que aquí se ha escogido difiere de la numeración de la figura 4.32.

Se pasa luego a VERT[2] y se obtiene un apuntador a la posición 2 en los datos. Éste contiene al primer lado que sale del vértice 2, es decir, (2, 3), y se puede seguir los apuntadores para visitar todos los lados que vienen desde el vértice 2. De modo semejante, se puede rastrear pasando por los lados (si los hay) que vienen de cada vértice. Nótese que VERT[4] = 0, lo cual significa que no hay lados que comiencen en el vértice 4.

La figura 4.35 muestra una alternativa a la figura 4.34 para describir el digrafo. El lector debe verificar la exactitud del método descrito en la figura 4.35. Se le recuerda una vez más al lector que la ordenación de los lados que salen de cada vértice puede ser escogida de manera arbitraria.

VERT	TAIL	HEAD	NEXT
10	1	2	0
2	2	3	3
4	2	1	0
0	3	5	6
5	5	4	0
8	3	4	7
	3	6	0
	6	1	0
	1	6	1
	1	3	9

Figura 4.34

VERT	TAIL	HEAD	NEXT
9	1	2	0
3	2	3	0
6	2	1	2
0	3	5	7
5	5	4	0
8	3	4	4
	3	6	0
	6	1	0
	1	6	10
	1	3	1

Figura 4.35

Se ve entonces que existen (por lo menos) dos métodos para almacenar los datos para una relación o digrafo, uno por medio de la matriz de la relación y otro mediante el uso de listas enlazadas. Hay varios factores que determinan la elección del método que se usará para el almacenamiento. El número total de elementos n que hay en el conjunto A, el número de pares ordenados que hay en R o la razón de este número a n^2 (el número máximo posible de pares ordenados), y la información posible que ha de obtenerse de R son todas las consideraciones. Un análisis de tales factores determinará cuál de los métodos de almacenamiento es el mejor. Se considerará dos casos.

Supóngase que $A = \{1, 2, \ldots, N\}$, y sea R una relación en A, cuya matriz $\mathbf{M}_R$ está representada por el arreglo MAT. Supóngase que R contiene P pares ordenados de manera que MAT contiene exactamente P unos. Primero, se va a considerar el problema de agregar un par (I, J) a R, y segundo, el problema de probar si R es transitiva.

Para agregar (I, J) a R se realiza el enunciado

$$\text{MAT}[I, J] \leftarrow 1.$$

Esto es sumamente sencillo con el método de almacenamiento de matriz.

Considérese ahora el siguiente algoritmo, el cual asigna RESULT al valor T (verdadero) o F (falso), dependiendo de que R sea o no transitiva. Se observa que TRANS no indica si R es o no transitiva.

ALGORITMO TRANS
1. RESULT ← T
2. **FOR** I = 1 **THRU** N
   a. **FOR** J = 1 **THRU** N
      1. **IF** (MAT[I, J] = 1) **THEN**
         a. **FOR** K = 1 **THRU** N
            1. **IF** (MAT[J, K] = 1 ∧ MAT[I, K] = 0) **THEN**
               a. RESULT ← F

FIN DEL ALGORITMO TRANS

Aquí RESULT originalmente es T, y se cambia solamente si se encuentra una situación en la que $(I, J) \in R$ y $(J, K) \in R$, pero $(I, K) \notin R$ (situación que viola la transitividad).

Ahora se proporciona un conteo del número de pasos que requiere el algoritmo TRANS. Obsérvese que I y J corren cada uno de 1 a N. Si (I, J) no está en R, sólo se efectúa la prueba uno "**IF** MAT$[I, J] = 1$", la cual será falsa, y el resto del algoritmo no se ejecutará. Puesto que $N^2 - P$ pares ordenados no pertenecen a R, se tiene $N^2 - P$ pasos que debe ejecutarse para tales elementos. Si $(I, J) \in R$, entonces la prueba "**IF** MAT $[I, J] = 1$," será verdadera y se ejecutará un ciclo adicional

a. **FOR** $K = 1$ **THRU** N
  1. **IF** (MAT$[J, K] = 1$ y MAT$[I, K] = 0$) **THEN**
    a. RESULT $\leftarrow$ F

de N pasos. Como R contiene P pares ordenados, se tiene PN pasos para tales elementos. En consecuencia, el número total de pasos que requiere el algoritmo TRANS es

$$T_A = PN + (N^2 - P).$$

Supóngase que $P = kN^2$, en donde $0 \leq k \leq 1$, puesto que P debe estar entre 0 y N^2. Entonces el algoritmo TRANS tiene su prueba por transitividad en

$$T_A = kN^3 + (1 - k)N^2$$

pasos.

Considérese ahora el mismo digrafo representado por el esquema de lista enlazada, utilizando VERT, TAIL, HEAD y NEXT. Primero se trabaja en el problema de agregar un lado (I, J). Se supone que TAIL, HEAD y NEXT tienen posiciones adicionales disponibles y que el número total de lados se cuenta por una variable P. Entonces el siguiente algoritmo agrega un lado (I, J) a la relación R.

ALGORITMO ADDEDGE
1. $P \leftarrow P + 1$
2. TAIL$[P] \leftarrow I$
3. HEAD$[P] \leftarrow J$
4. NEXT$[P] \leftarrow$ VERT$[I]$
5. VERT$[I] \leftarrow P$

FIN DEL ALGORITMO ADDEDGE

La figura 4.36 muestra la situación esquemáticamente en forma de apuntadores, tanto antes como después de agregar el lado (I, J). VERT$[I]$ apunta ahora al nuevo lado, y el apuntador de ese lado va al lado previamente señalado por VERT$[I]$, es decir (I, J'). Este método no es demasiado complicado, pero resulta claro que el método de almacenamiento de matriz tiene la ventaja para la tarea de agregar un lado.

Se considera en seguida el problema de transitividad. Para que las cosas sigan siendo sencillas, supóngase que se dispone de una función EDGE(I, J) que tiene el valor T si (I, J) está en R, o de lo contrario el valor F. Se pide al lector construir tal función en los ejercicios. El siguiente algoritmo hace la prueba de transitividad de R con este método de almacenamiento. Una vez más, RESULT tendrá el valor T si R es transitiva y, de lo contrario, tendrá el valor F.

ALGORITMO NEWTRANS
1. RESULT $\leftarrow$ T
2. **FOR** $I = 1$ **THRU** N
  a. $X \leftarrow$ VERT$[I]$
  b. **WHILE** $(X \neq 0)$
    1. $J \leftarrow$ HEAD$[X]$
    2. $Y \leftarrow$ VERT$[J]$
    3. **WHILE**$(Y \neq 0)$
      a. $K \leftarrow$ HEAD$[Y]$
      b. TEST $\leftarrow$ EDGE$[I, K]$
      c. **IF** (TEST) **THEN**
        1. $Y \leftarrow$ NEXT$[Y]$
      d. **ELSE**
        1. RESULT $\leftarrow$ F
        2. $Y \leftarrow$ NEXT$[Y]$
    4. $X \leftarrow$ NEXT$[X]$

FIN DEL ALGORITMO NEWTRANS

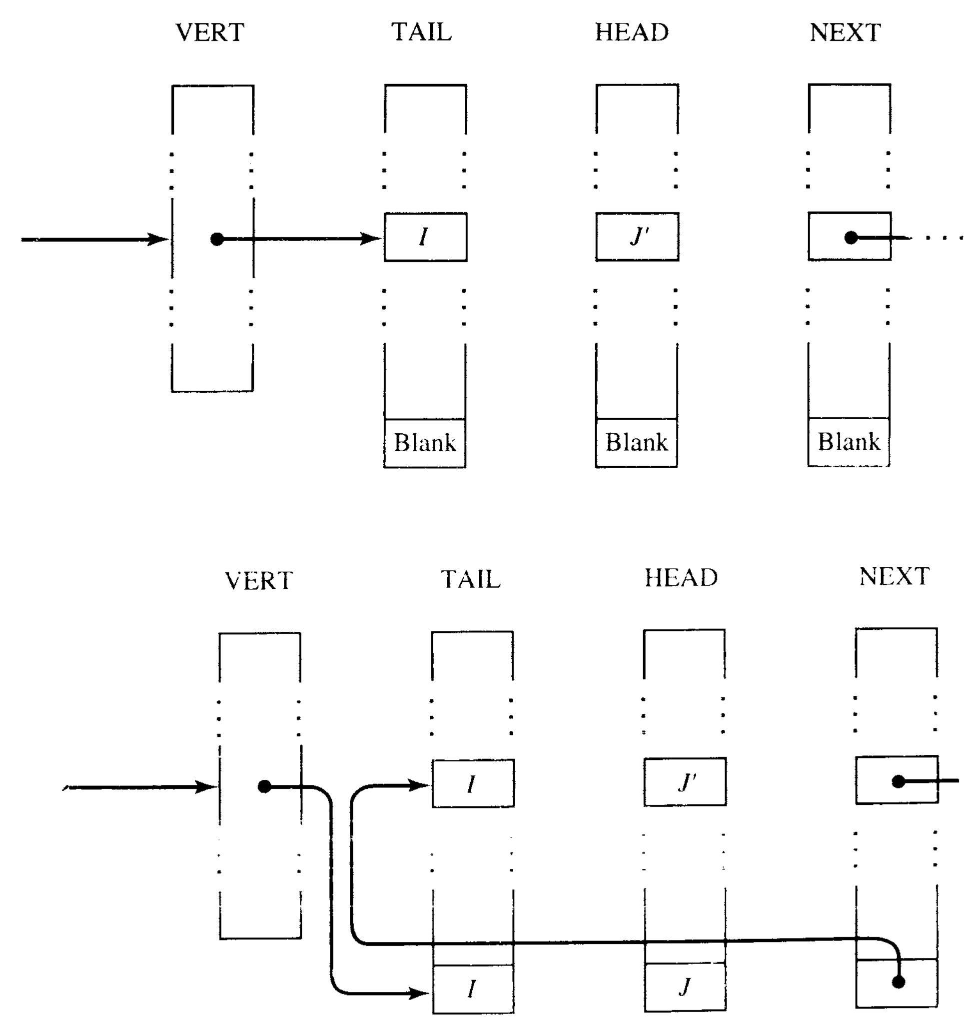


Figura 4.36

El lector debe seguir los pasos de este algoritmo con varios ejemplos sencillos. Para cada vértice I, busca en todas las trayectorias de longitud 2 que comiencen en I y verifica éstas por transitividad. Así, paulatinamente verifica cada trayectoria de longitud 2 para ver si hay una trayectoria directa equivalente. El algoritmo NEWTRANS es un poco más largo que el algoritmo TRANS que corresponde al método de almacenamiento de matriz, y el NEWTRANS utiliza también la función EDGE, pero se asemeja mucho más al método humano de determinar la transitividad de R. Además, el NEWTRANS puede ser más eficiente.

Se va a analizar el número promedio de pasos que toma el algoritmo NEWTRANS para la prueba de transitividad. Cada uno de los P lados comienza en un vértice único, así que, en promedio, $P/N = D$ lados comienzan en el vértice. No es difícil ver que una función EDGE, como la que se necesitó antes, puede seguir un promedio de D pasos, puesto que debe verificar todos los lados que comiencen en un vértice particular. El ciclo principal **FOR** del NEWTRANS será ejecutado N veces, y cada enunciado subordinado **WHILE** promediará alrededor de D ejecuciones. Como el último **WHILE** llama a EDGE cada vez, se ve que el algoritmo completo promediará alrededor de ND^3 pasos de ejecución. Como antes, se supone que $P = kN^2$ con $0 \leq k \leq 1$. Entonces NEWTRANS hace un promedio de

$$T_L = N\left(\frac{kN^2}{N}\right)^3 = k^3N^4 \quad \text{pasos.}$$

Recuerde que el algoritmo TRANS, utilizando almacenamiento de matriz, requería alrededor de $T_A = kN^3 + (1 - k)N^2$ pasos.

Considérese ahora la relación T_L / T_A del número promedio de pasos necesarios con almacenamiento enlazado comparado con el número de pasos necesarios con almacenamiento de matriz para probar R por transitividad. En consecuencia,

$$\frac{T_L}{T_A} = \frac{k^3N^4}{kN^3 + (1 - k)N^2} = \frac{k^2N}{1 + \left(\frac{1}{k} - 1\right)\frac{1}{N}}.$$

Cuando k es cercana a 1, es decir, cuando hay muchos lados, entonces T_L / T_A es casi N, por lo que $T_L = T_A N$, y el método de lista enlazada promedia N veces los pasos del método de almacenamiento de matriz. En consecuencia, el método de almacenamiento de matriz es N veces más rápido que el método de lista enlazada en la mayoría de los casos.

Por otra parte, si k es muy pequeño, entonces T_L / T_A puede ser casi cero. Esto significa que si el número de lados es pequeño en comparación con N^2, resulta en promedio, considerablemente más eficiente probar por transitividad en un método de almacenamiento de lista enlazada que con almacenamiento de matriz de adyacencia.

Por supuesto, se ha hecho una gran simplificación. No todos los pasos toman el mismo tiempo de ejecución, y cada algoritmo que haya que probar por transitividad puede acortarse deteniendo la búsqueda cuando se descubre el primer contraejemplo a la transitividad. A pesar de esto, la conclusión sigue siendo verdadera e ilustra el punto importante de que la selección de una estructura de datos para representar objetos tales como conjuntos, relaciones y digrafos tiene un efecto importante en la eficiencia con que puede obtenerse información acerca de los objetos.

Prácticamente todas las relaciones y digrafos de importancia práctica son demasiado grandes para ser explorados manualmente. En consecuencia, el almacenamiento en computadora de relaciones y la implantación algorítmica de métodos para explorarlos son de gran importancia.

GRUPO DE EJERCICIOS 4.6

1. Verifique que el arreglo de lista enlazada de la figura 4.35 describa correctamente el digrafo de la figura 4.32.

2. Construya una función EDGE(I, J) (en seudocódigo) que regrese el valor T (verdadero) si el par (i, j) está en R, y el F (falso) de lo contrario. Suponga que la relación R se da por arreglos VERT, TAIL, HEAD y NEXT, como se describe en esta sección.

3. Demuestre que la función EDGE del ejercicio 2 se ejecuta en un promedio de D pasos, siendo $D = P/N$, P es el número de lados de R, y N es el número de vértices de R. (*Sugerencia:* Suponga que P_{ij} es el número de lados que van del vértice i al vértice j. Exprese el número total de pasos ejecutados por EDGE para cada par de vértices y luego obtenga el promedio. Utilice el hecho de que $\Sigma_{\substack{i=1\\j=1}} P_{ij} = P$.)

4. Sea NUM un arreglo lineal que contiene N enteros positivos, y sea NEXT otro arreglo lineal de la misma longitud. Supóngase que START es un apuntador hacia un "primer" entero en NUM, y que para cada I, NEXT[I] apunta al "siguiente" entero de NUM que debe considerarse. Si NEXT[I] = 0, termina la lista.

   Escriba una función LOOK (NUM, NEXT, START, N, K) en seudocódigo para buscar NUM por medio de los apuntadores en NEXT para un entero K. Si se encuentra K, se regresa la posición de K en NUM. Si no, LOOK imprime "NO SE ENCONTRÓ".

5. Sea $A = \{1, 2, 3, 4\}$ y sea $R = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 1), (3, 1), (3, 4), (4, 2)\}$ una relación sobre A. Calcule la matriz $\mathbf{M}_R$ que dé la representación de R y los valores de los arreglos VERT, TAIL, HEAD y NEXT que describan R como una lista enlazada. Puede enlazar en cualquier forma razonable.

6. Sea $A = \{1, 2, 3, 4\}$ y sea R la relación cuyo digrafo aparece en la figura 4.37.

   Describa los arreglos VERT, TAIL, HEAD y NEXT, estableciendo una representación de lista enlazada de R, de manera que los lados que salen de cada vértice sean alcanzados en la lista en orden creciente (relativo a su numeración de la figura 4.37).

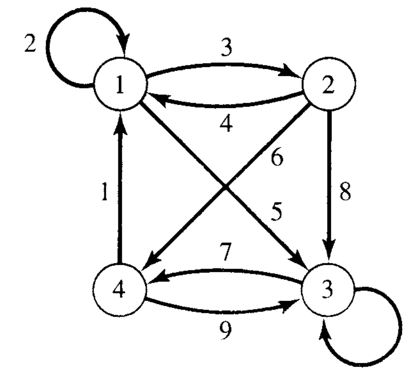


Figura 4.37

7. Considere los siguientes arreglos.

   VERT = [1, 2, 6, 4]
   TAIL = [1, 2, 2, 4, 4, 3, 4, 1]
   HEAD = [2, 2, 3, 3, 4, 4, 1, 3]
   NEXT = [8, 3, 0, 5, 7, 0, 0, 0]

   Éstos describen una relación R en el conjunto $A = \{1, 2, 3, 4\}$. Calcule el digrafo de R y la matriz $\mathbf{M}_R$.

8. Los siguientes arreglos describen una relación R en el conjunto $A = \{1, 2, 3, 4, 5\}$. Calcule el digrafo de R y la matriz $\mathbf{M}_R$.

   VERT = [6, 2, 8, 7, 10]
   TAIL = [2, 2, 2, 2, 1, 1, 4, 3, 4, 5]
   HEAD = [4, 3, 5, 1, 2, 3, 5, 4, 2, 4]
   NEXT = [3, 1, 4, 0, 0, 5, 9, 0, 0, 0]

9. Sea $A = \{1, 2, 3, 4, 5\}$ y sea R una relación sobre A tal que

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Construya una representación de lista enlazada, VERT, TAIL, HEAD, NEXT para la relación R.

10. Sea $A = \{a, b, c, d, e\}$ y sea R la relación descrita por

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Construya una representación de lista enlazada, VERT, TAIL, HEAD, NEXT para R.

4.7. Manipulación de relaciones

Igual que puede manipularse o trabajarse con los números y fórmulas aplicando las reglas del álgebra, también puede definirse operaciones que permitan manipular las relaciones. Con estas operaciones se puede cambiar, combinar y refinar relaciones existentes para producir otras nuevas.

Sean R y S las relaciones de un conjunto A a un conjunto B. Entonces, si se recuerda que R y S son simplemente subconjuntos de $A \times B$, es posible usar operaciones de conjuntos en R y S. Por ejemplo, el complemento de R, $\bar{R}$, se menciona como la **relación complementaria**. Por supuesto, es una relación de A a B que puede expresarse simplemente en términos de R:

$$a\ \bar{R}\ b \quad \text{si y sólo si} \quad a \not R\ b.$$

También puede formarse la intersección $R \cap S$ y la unión $R \cup S$ de las relaciones R y S. En términos de relaciones, se ve que $a\ (R \cap S)\ b$ significa que $a\ R\ b$ y $a\ S\ b$; $a\ (R \cup S)\ b$ significa que $a\ R\ b$ o $a\ S\ b$. Todas las operaciones teóricas de conjuntos pueden ser utilizadas de esta manera para producir nuevas relaciones. El lector debe tratar de dar una descripción relacional de la relación $R \oplus S$ (véase la sección 1.2).

Un tipo diferente de operación en una relación R de A a B es la formación de la **inversa**, que suele escribirse R^{-1}. La relación R^{-1} es una relación de B a A (orden invertido de R) que se define por

$$b\ R^{-1}\ a \quad \text{si y sólo si} \quad a\ R\ b.$$

Por lo anterior, resulta claro que $(R^{-1})^{-1} = R$. No es difícil ver que $\text{Dom}(R^{-1}) = \text{Ran}(R)$ y $\text{Ran}(R^{-1}) = \text{Dom}(R)$. Se deja estos hechos sencillos como ejercicios.

Ejemplo 1. Sea $A = \{1, 2, 3, 4\}$ y $B = \{a, b, c\}$. Sean

$$R = \{(1, a), (1, b), (2, b), (2, c), (3, b), (4, a)\}$$

y

$$S = \{(1, b), (2, c), (3, b), (4, b)\}.$$

Calcule (a) $\bar{R}$; (b) $R \cap S$; (c) $R \cup S$; y (d) R^{-1}.

Solución

(a) Se encuentra primero

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c), (4, a), (4, b), (4, c)\}.$$

Entonces el complemento de R en $A \times B$ es

$$\bar{R} = \{(1, c), (2, a), (3, a), (3, c), (4, b), (4, c)\}.$$

(b) Se tiene que $R \cap S = \{(1, b), (3, b), (2, c)\}$.

(c) Se tiene que

$$R \cup S = \{(1, a), (1, b), (2, b), (2, c), (3, b), (4, a), (4, b)\}.$$

(d) Puesto que $(x, y) \in R^{-1}$ si y sólo si $(y, x) \in R$, se tiene

$$R^{-1} = \{(a, 1), (b, 1), (b, 2), (c, 2), (b, 3), (a, 4)\}.$$ ♦

Ejemplo 2. Sea $A = \mathbb{R}$. Sea R la relación $\leq$ (menor o igual a) sobre A y sea S (mayor o igual a) $\geq$. Entonces el complemento de R es la relación $>$ (mayor que), puesto que $a \not\leq b$ significa que $a > b$. De modo similar, el complemento de S es $<$ (menor que). Por otra parte, $R^{-1} = S$, puesto que para cualquier número de a y b,

$$a\ R^{-1}\ b \quad \text{si y sólo si} \quad b\ R\ a \quad \text{si y sólo si} \quad b \leq a \quad \text{si y sólo si} \quad a \geq b.$$

De modo similar, se tiene $S^{-1} = R$. También, se observa que $R \cap S$ es la relación de igualdad, puesto que $a\ (R \cap S)\ b$ si y sólo si $a \leq b$ y $a \geq b$ si y sólo si $a = b$. Como, para cualquier a y b, es cierto que $a \leq b$ o $a \geq b$, se ve que $R \cup S = A \times B$; es decir, $R \cup S$ es la relación *universal* en la cual cualquier a está relacionada con cualquier b. ♦

Ejemplo 3. Sea $A = \{a, b, c, d, e\}$ y sean R y S dos relaciones sobre A cuyos digrafos correspondientes aparecen en la figura 4.38. Entonces el lector puede verificar los siguientes hechos:

$$\bar{R} = \{(a, a), (b, b), (a, c), (b, a), (c, b), (c, d), (c, e), (c, a), (d, b), (d, a), (d, e), (e, b), (e, a), (e, d), (e, c)\}$$

$$R^{-1} = \{(b, a), (e, b), (c, c), (c, d), (d, d), (d, b), (c, b), (d, a), (e, e)\ (e, a)\}$$

$$R \cap S = \{(a, b), (b, e), (c, c)\}.$$ ♦

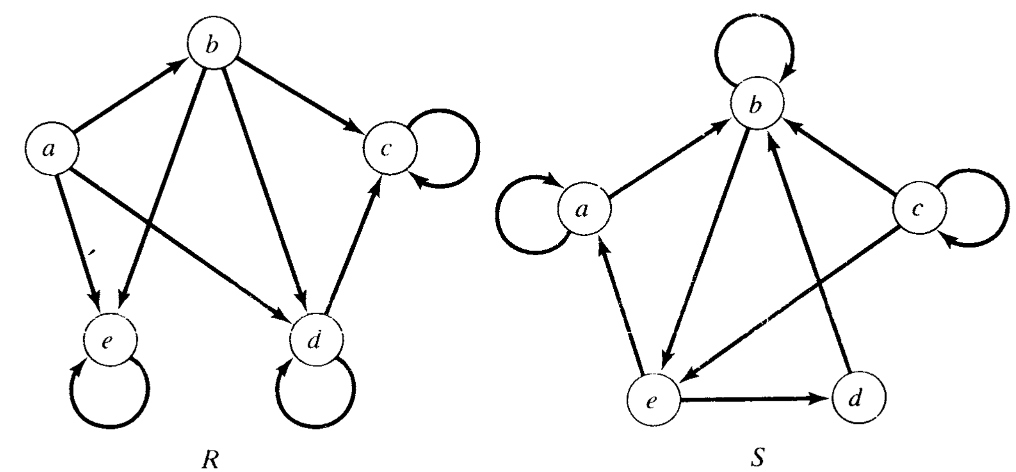


Figura 4.38

Ejemplo 4. Sea $A = \{1, 2, 3\}$ y sean R y S relaciones sobre A. Supóngase que las matrices de R y S son

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{y} \quad \mathbf{M}_S = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Entonces se puede verificar que

$$\mathbf{M}_{\overline{R}} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \qquad \mathbf{M}_{R^{-1}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix},$$

$$\mathbf{M}_{R\cap S} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad \mathbf{M}_{R\cup S} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

◆

El ejemplo 4 ilustra algunos hechos generales. Si se recuerda las operaciones en matrices booleanas de la sección 1.5, puede demostrarse (ejercicio 27) que si R y S son relaciones sobre el conjunto A, entonces

$$\mathbf{M}_{R\cap S} = \mathbf{M}_R \wedge \mathbf{M}_S$$
$$\mathbf{M}_{R\cup S} = \mathbf{M}_R \vee \mathbf{M}_S$$
$$\mathbf{M}_{R^{-1}} = (\mathbf{M}_R)^T.$$

Por otra parte, si $\mathbf{M}$ es una matriz booleana, se define el **complemento** $\overline{\mathbf{M}}$ de $\mathbf{M}$ como la matriz obtenida a partir de $\mathbf{M}$ al reemplazar cada 1 en $\mathbf{M}$ por un 0 y cada 0 por un 1. Así, si

$$\mathbf{M} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

entonces

$$\overline{\mathbf{M}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

También puede demostrarse (ejercicio 27) que si R es una relación sobre un conjunto A, entonces

$$\mathbf{M}_{\overline{R}} = \overline{\mathbf{M}}_R.$$

Se sabe que una relación simétrica es una relación R tal que $\mathbf{M}_R = (\mathbf{M}_R)^T$, y como $(\mathbf{M}_R)^T = \mathbf{M}_{R^{-1}}$, se ve que R es simétrica si y sólo si $R = R^{-1}$.

Ahora se va a demostrar algunas propiedades útiles acerca de las combinaciones de relaciones.

Teorema 1. *Supóngase que R y S son relaciones de A a B.*
(a) *Si $R \subseteq S$, entonces $R^{-1} \subseteq S^{-1}$.*
(b) *Si $R \subseteq S$, entonces $\overline{S} \subseteq \overline{R}$.*

(c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ *y* $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.
(d) $\overline{(R \cap S)} = \overline{R} \cup \overline{S}$ *y* $\overline{(R \cup S)} = \overline{R} \cap \overline{S}$.

Demostración: Las partes (b) y (d) son casos especiales de las propiedades generales de los conjuntos demostradas en la sección 1.2.

Ahora se demuestra la parte (a). Supóngase que $R \subseteq S$ y sea $(a, b) \in R^{-1}$. Entonces $(b, a) \in R$, de manera que $(b, a) \in S$. Ésta, a su vez, implica que $(a, b) \in S^{-1}$. Puesto que cada elemento de R^{-1} está en S^{-1}, la proposición queda demostrada.

A continuación, se va a demostrar la parte (c). Para la primera parte, supóngase que $(a, b) \in (R \cap S)^{-1}$. Entonces $(b, a) \in R \cap S$, de manera que $(b, a) \in R$ y $(b, a) \in S$. Esto significa que $(a, b) \in R^{-1}$ y $(a, b) \in S^{-1}$, de modo que $(a, b) \in R^{-1} \cap S^{-1}$. La contención inversa puede demostrarse invirtiendo los pasos. Hay un argumento similar que funciona para demostrar que $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$. ●

Las relaciones $\overline{R}$ y R^{-1} pueden ser empleadas para verificar si R tiene las propiedades de relaciones presentadas en la sección 4.4.

Teorema 2. *Sean R y S relaciones sobre un conjunto A.*
(a) *Si R es reflexiva, también lo es R^{-1}.*
(b) *Si R y S son reflexivas, entonces también lo son $R \cap S$ y $R \cup S$.*
(c) *R es reflexiva si y sólo si $\overline{R}$ es irreflexiva.*

Demostración: Sea Δ la relación de igualdad sobre A. Se sabe que R es reflexiva si y sólo si $\Delta \subseteq R$. Es claro que, $\Delta = \Delta^{-1}$, de modo que si $\Delta \subseteq R$, entonces $\Delta = \Delta^{-1} \subseteq R^{-1}$ por el teorema 1, de manera que R^{-1} también es reflexiva. Esto demuestra la parte (a). Para demostrar la parte (b), se observa que si $\Delta \subseteq R$ y $\Delta \subseteq S$, entonces $\Delta \subseteq R \cap S$ y $\Delta \subseteq R \cup S$. Para demostrar la parte (c), se observa que una relación S es irreflexiva si y sólo si $S \cap \Delta = \varnothing$. Entonces R es reflexiva si y sólo si $\Delta \subseteq R$ si y sólo si $\Delta \cap \overline{R} = \varnothing$ si y sólo si $\overline{R}$ es irreflexiva. ●

Ejemplo 5. Sea $A = \{1, 2, 3\}$ y considérese las dos relaciones reflexivas

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

y

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

Entonces
(a) $R^{-1} = \{(1, 1), (2, 1), (3, 1), (2, 2), (3, 3)\}$, de modo que R y R^{-1} ambas son reflexivas.
(b) $\overline{R} = \{(2, 1), (2, 3), (3, 1), (3, 2)\}$ es irreflexiva mientras que R es reflexiva.
(c) $R \cap S = \{(1, 1), (1, 2), (2, 2), (3, 3)\}$ y $R \cup S = \{(1, 1), (1, 2), (1, 3), (2, 2), (3, 2), (3, 3)\}$ ambas son reflexivas. ◆

Teorema 3. *Sea R una relacion sobre un conjunto A. Entonces*
(a) *R es simétrica si y sólo si $R = R^{-1}$.*
(b) *R es antisimétrica si y sólo si $R \cap R^{-1} \subseteq \Delta$.*
(c) *R es asimétrica si y sólo si $R \cap R^{-1} = \varnothing$.*

Demostración: La demostración es directa y se deja como ejercicio. ●

Teorema 4. *Sean R y S relaciones sobre A.*

(a) *Si R es simétrica, también lo son* R^{-1} *y* $\overline{R}$.

(b) *Si R y S son simétricas, también lo son* $R \cap S$ *y* $R \cup S$.

Demostración: Si R es simétrica, $R = R^{-1}$ y en consecuencia $(R^{-1})^{-1} = R = R^{-1}$, lo cual significa que R^{-1} también es simétrica. También, $(a, b) \in (\overline{R})^{-1}$ si y sólo si $(b, a) \in \overline{R}$ si y sólo si $(b, a) \notin R$ si y sólo si $(a, b) \notin R^{-1} = R$ si y sólo si $(a, b) \in \overline{R}$, de modo que $\overline{R}$ es simétrica y la parte (a) queda demostrada. La demostración de la parte (b) se desprende en forma inmediata del teorema 1(c). ●

Ejemplo 6. Sea $A = \{1, 2, 3\}$ y considérese las relaciones simétricas

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

y

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

Entonces

(a) $R^{-1} = \{(1,1), (2,1), (1,2), (3,1), (1,3)\}$ y $\overline{R} = \{(2,2), (2,3), (3,2), (3,3)\}$; de manera que R^{-1} y $\overline{R}$ son simétricas.

(b) $R \cap S = \{(1,1), (1,2), (2,1)\}$ y $R \cup S = \{(1,1), (1,2), (1,3), (2,1), (2,2), (3,1), (3,3)\}$, las cuales son simétricas. ♦

Teorema 5. *Sean R y S relaciones sobre A.*

(a) $(R \cap S)^2 \subseteq R^2 \cap S^2$.

(b) *Si R y S son transitivas, también lo es* $R \cap S$.

(c) *Si R y S son relaciones de equivalencia, también lo es* $R \cap S$.

Demostración: Se demuestra la parte (a) geométricamente. Se tiene que $a\ (R \cap S)^2\ b$ si y sólo si hay una trayectoria de longitud 2 que vaya de a a b en $R \cap S$. Ambos lados de esta trayectoria se encuentran en R y en S, de modo que $a\ R^2\ b$ y $a\ S^2\ b$, lo cual implica que $a(R^2 \cap S^2)b$. Para demostrar la parte (b), se recordará de la sección 4.4 que una relación T es transitiva si y sólo si $T^2 \subseteq T$. Si R y S son transitivas, entonces $R^2 \subseteq R$, $S^2 \subseteq S$, por tanto, $(R \cap S)^2 \subseteq R^2 \cap S^2$ [por la parte (a)] $\subseteq R \cap S$, de modo que $R \cap S$ es transitiva. Enseguida se demuestra la parte (c). Las relaciones R y S son cada una reflexiva, simétrica y transitiva. Las mismas propiedades son válidas para $R \cap S$ por los teoremas 2(b), 4(b) y 5(b), respectivamente. Por tanto $R \cap S$ es una relación de equivalencia. ●

Ejemplo 7. Sean R y S relaciones de equivalencia sobre un conjunto finito A, y sean A/R y A/S las particiones correspondientes (véase la sección 4.5). Puesto que $R \cap S$ es una relación de equivalencia, corresponde a una partición $A/(R \cap S)$. Ahora se describe $A/(R \cap S)$ en función de A/R y A/S. Sea W un bloque de $A/(R \cap S)$ y supóngase que a y b pertenecen a W. Entonces $a\ (R \cap S)\ b$, de manera que $a\ R\ b$ y $a\ S\ b$. En consecuencia, a y b pertenecen al mismo bloque, por decir, X, de A/R y al mismo bloque, por decir, Y, de A/S. Esto significa que $W \subseteq X \cap Y$. Los pasos que hay en este argumento son reversibles; por lo tanto, $W = X \cap Y$. En consecuencia, se puede calcular directamente la partición $A/(R \cap S)$ formando todas las intersecciones posibles de bloques en A/R con bloques en A/S. ♦

Cerraduras

Si R es una relación sobre un conjunto A, bien puede ocurrir que R carezca de algunas de las propiedades relacionales importantes que se analizó en la sección 4.4, especialmente la reflexividad, la simetría y la transitividad. Si R no posee una propiedad en particular, se puede desear agregar a R pares relacionados hasta obtener una relación que *sí* tenga la propiedad requerida. Naturalmente, se quiere agregar el menor número de pares posible, por lo cual lo que se necesita encontrar es la relación *más pequeña* R_1 en A que contenga a R y posea la propiedad que se desea. En ocasiones R_1 no existe. Si existe una relación tal como R_1, se la llama **cerradura** de R con respecto de la propiedad en cuestión.

Ejemplo 8. Supóngase que R es una relación sobre un conjunto A, y que R no es reflexiva. Esto sólo puede ocurrir porque algunos pares de la relación diagonal Δ no estén en R. Así, $R_1 = R \cup \Delta$ es la relación reflexiva más pequeña en A que contiene a R; es decir, la **cerradura reflexiva** de R es $R \cup \Delta$. ♦

Ejemplo 9. Supóngase ahora que R es una relación sobre A que no es simétrica. Entonces debe existir pares (x, y) en R tales que (y, x) no esté en R. Por supuesto, $(y, x) \in R^{-1}$, de manera que si R ha de ser simétrica se debe agregar todos los pares procedentes de R^{-1}; es decir, se debe agrandar R a $R \cup R^{-1}$. Es claro que $(R \cup R^{-1})^{-1} = R \cup R^{-1}$, como $R \cup R^{-1}$ es la relación simétrica más pequeña que contiene a R; es decir, $R \cup R^{-1}$ es la **cerradura simétrica** de R.

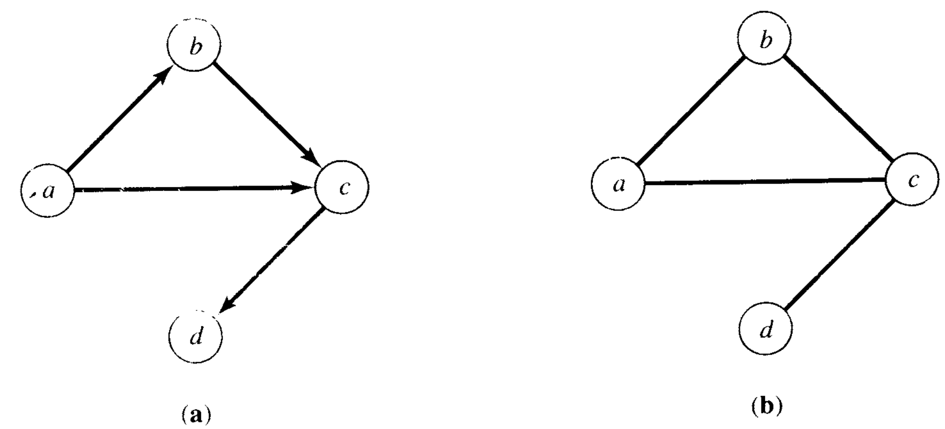
Si $A = \{a, b, c, d\}$ y $R = \{(a, b), (b, c), (a, c), (c, d)\}$, entonces $R^{-1} = \{(b, a), (c, b), (c, a), (d, c)\}$, así que la cerradura simétrica de R es

$$R \cup R^{-1} = \{(a,b), (b,a), (b,c), (c,b), (a,c), (c,a), (c,d), (d,c)\}.$$ ♦

La cerradura simétrica de una relación R resulta muy fácil de imaginar geométricamente. Todos los lados del digrafo de R se convierten en "calles de dos sentidos" en $R \cup R^{-1}$. En consecuencia, la gráfica de la cerradura simétrica de R simplemente es el digrafo de R cuyos lados son todos bidireccionales. Se ilustra en la figura 4.39(a) el digrafo de la relación R del ejemplo 9. La figura 4.39(b) muestra la gráfica de la cerradura simétrica $R \cup R^{-1}$.

La **cerradura transitiva** de una relación R es la relación transitiva más pequeña que contiene a R. Se estudiará la cerradura transitiva en la sección siguiente.

Figura 4.39



Composición

Supóngase ahora que A, B y C son conjuntos, R es una relación de A a B, y S es la relación de B a C. Entonces se puede definir una nueva relación, la **composición** de R y S, que se escribe $S \circ R$. La relación $S \circ R$ es una relación de A a C y se define de la siguiente manera. Si a está en A y c está en C, entonces $a(S \circ R)c$ si y sólo si para alguna b en B se tiene $a\,R\,b$ y $b\,S\,c$. En otras palabras, a está relacionada con c por $S \circ R$ si se puede ir de a a c en dos etapas: primero a un vértice intermedio b por la relación R y luego de b a c por la relación S. La relación $S \circ R$ podría concebirse como "S a continuación de R" puesto que representa el efecto combinado de dos relaciones, primero R y después S.

Ejemplo 10. Sea $A = \{1, 2, 3, 4\}$, $R = \{(1, 2), (1, 1), (1, 3), (2, 4), (3, 2)\}$, y $S = \{(1, 4), (1, 3), (2, 3), (3, 1), (4, 1)\}$. Puesto que $(1, 2) \in R$ y $(2, 3) \in S$, se debe tener $(1, 3) \in S \circ R$. De modo semejante, puesto que $(1, 1) \in R$ y $(1, 4) \in S$, se ve que $(1, 4) \in S \circ R$. Prosiguiendo de esta manera, se encuentra que $S \circ R = \{(1, 4), (1, 3), (1, 1), (2, 1), (3, 3)\}$. ◆

El siguiente resultado muestra cómo calcular conjuntos relativos para la composición de dos relaciones.

Teorema 6. *Sea R una relación de A a B y sea S una relación de B a C. Entonces, si A_1 es cualquier subconjunto de A, se tiene*

$$(S \circ R)(A_1) = S(R(A_1)).$$

Demostración: Si un elemento $z \in C$ está en $(S \circ R)(A_1)$, entonces $x(S \circ R)z$ para alguna x en A_1. Por la definición de composición, esto significa que $x\,R\,y$ y $y\,S\,z$ para alguna y en B. En consecuencia $y \in R(x)$, de modo que $z \in S(R(x))$. Puesto que $\{x\} \subseteq A_1$, el teorema 1(a) de la sección 4.2 dice que $S(R(x)) \subseteq S(R(A_1))$. De aquí, $z \in S(R(A_1))$, por tanto $(S \circ R)(A_1) \subseteq S(R(A_1))$.

Por el contrario, supóngase que $z \in S(R(A_1))$. Entonces $z \in S(y)$ para alguna y en $R(A_1)$ y, de modo semejante, $y \in R(x)$ para alguna x en A_1. Esto significa que $x\,R\,y$ y $y\,S\,z$, de modo que $x(S \circ R)z$. Así pues $z \in (S \circ R)(A_1)$, por tanto $S(R(A_1)) \subseteq (S \circ R)(A_1)$. Esto demuestra el teorema. ●

Ejemplo 11. Sea $A = \{a, b, c\}$ y sean R y S relaciones sobre A cuyas matrices son

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{M}_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Se ve por las matrices, que

$$\begin{array}{llll} (a, a) \in R & \text{y} \quad (a, a) \in S, & \text{por tanto} & (a, a) \in S \circ R \\ (a, c) \in R & \text{y} \quad (c, a) \in S, & \text{por tanto} & (a, a) \in S \circ R \\ (a, c) \in R & \text{y} \quad (c, c) \in S, & \text{por tanto} & (a, c) \in S \circ R. \end{array}$$

Se ve fácilmente que $(a, b) \notin S \circ R$ puesto que, si se tuviera $(a, x) \in R$ y $(x, b) \in S$, la matriz $\mathbf{M}_R$ dice que x tendría que ser a o c; pero la matriz $\mathbf{M}_S$ dice que ni (a, b) ni (c, b) es un elemento de S.

Se ve que el primer renglón de $\mathbf{M}_{S \circ R}$ es $1 \quad 0 \quad 1$. El lector puede demostrar por un análisis similar que

$$\mathbf{M}_{S \circ R} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Obsérvese que $\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S$ (verifique). ◆

El ejemplo 11 ilustra un hecho general y útil. Sean A, B y C conjuntos finitos con n, p y m elementos, respectivamente, sea R una relación de A a B, y sea S una relación de B a C. Entonces R y S tienen las matrices booleanas $\mathbf{M}_R$ y $\mathbf{M}_S$ con tamaños respectivos $n \times p$ y $p \times m$. Puede calcularse, entonces, $\mathbf{M}_R \odot \mathbf{M}_S$, y es igual a $\mathbf{M}_{S \circ R}$.

Para ver esto, sean $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_p\}$, y $C = \{c_1, \ldots, c_m\}$. Supóngase también que $\mathbf{M}_R = [r_{ij}]$, $\mathbf{M}_S = [s_{ij}]$, y $\mathbf{M}_{S \circ R} = [t_{ij}]$. Entonces $t_{ij} = 1$ si y sólo si $(a_i, c_j) \in S \circ R$, lo cual significa que para alguna k, $(a_i, b_k) \in R$ y $(b_k, c_j) \in S$. En otras palabras, $r_{ik} = 1$ y $s_{kj} = 1$ para alguna k comprendida entre 1 y p. Esta condición es idéntica a la condición necesaria para que $\mathbf{M}_R \odot \mathbf{M}_S$ tenga un 1 en posición i, j, y en consecuencia $\mathbf{M}_{S \circ R}$ y $\mathbf{M}_R \odot \mathbf{M}_S$ son iguales.

En el caso especial en el que R y S sean iguales, se tiene $S \circ R = R^2$ y $\mathbf{M}_{S \circ R} = \mathbf{M}_{R^2} = \mathbf{M}_R \odot \mathbf{M}_R$, como se demostró en la sección 4.3.

Ejemplo 12. Se va a volver a trabajar en el ejemplo 10 utilizando matrices. Se ve que

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{y} \quad \mathbf{M}_S = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Entonces

$$\mathbf{M}_R \odot \mathbf{M}_S = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

de manera que

$$S \circ R = \{(1, 1), (1, 3), (1, 4), (2, 1), (3, 3)\}$$

como se encontró antes. En casos en los que el número de pares ordenados en R y S sea grande, el método de matrices es mucho más confiable y sistemático. ◆

Teorema 7. *Sean A, B, C y D conjuntos, R una relación de A a B, S una relación de B a C, y T una relación de C a D. Entonces*

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Demostración: Las relaciones R, S y T están determinadas por sus matrices booleanas $\mathbf{M}_R$, $\mathbf{M}_S$ y $\mathbf{M}_T$, respectivamente. Como se demostró después del ejemplo 11, la matriz de la composición es la matriz producto booleana; es decir, $\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S$. En consecuencia

$$\mathbf{M}_{T \circ (S \circ R)} = \mathbf{M}_{S \circ R} \odot \mathbf{M}_T = (\mathbf{M}_R \odot \mathbf{M}_S) \odot \mathbf{M}_T.$$

De modo similar,

$$\mathbf{M}_{(T\circ S)\circ R} = \mathbf{M}_R \odot (\mathbf{M}_S \odot \mathbf{M}_T).$$

Puesto que la multiplicación de matrices booleanas es asociativa [véase el ejercicio 27(c) de la sección 1.5], se debe tener

$$(\mathbf{M}_R \odot \mathbf{M}_S) \odot \mathbf{M}_T = \mathbf{M}_R \odot (\mathbf{M}_S \odot \mathbf{M}_T),$$

y por lo tanto

$$\mathbf{M}_{T\circ(S\circ R)} = \mathbf{M}_{(T\circ S)\circ R}.$$

Entonces

$$T\circ(S\circ R) = (T\circ S)\circ R$$

ya que estas relaciones tienen las mismas matrices. ●

En general, $R\circ S \neq S\circ R$, como se muestra en el siguiente ejemplo.

Ejemplo 13. Sean $A = \{a, b\}$, $R = \{(a, a), (b, a), (b, b)\}$, y $S = \{(a, b), (b, a), (b, b)\}$. Entonces $S\circ R = \{(a, b), (b, a), (b, b)\}$, mientras que $R\circ S = \{(a, a), (a, b), (b, a), (b, b)\}$. ◆

Teorema 8. *Sean A, B y C tres conjuntos, R una relación de A a B, y S una relación de B a C. Entonces $(S\circ R)^{-1} = R^{-1}\circ S^{-1}$.*

Demostración: Sean $c \in C$ y $a \in A$. Entonces $(c, a) \in (S\circ R)^{-1}$ si y sólo si $(a, c) \in S\circ R$, es decir, si y sólo si hay una $b \in B$ con $(a, b) \in R$ y $(b, c) \in S$. Por último, ésta es equivalente al enunciado de que $(c, b) \in S^{-1}$ y $(b, a) \in R^{-1}$; es decir, $(c, a) \in R^{-1}\circ S^{-1}$. ●

GRUPO DE EJERCICIOS 4.7

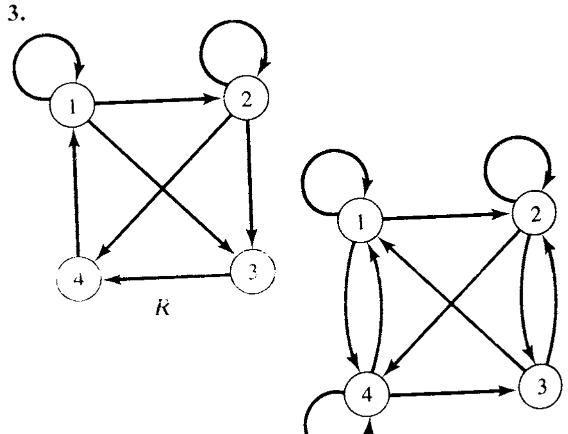
En los ejercicios 1 y 2, sean R y S las relaciones dadas de A a B. Calcule (a) $\overline{R}$ (b) $R\cap S$; (c) $R\cup S$; (d) S^{-1}.

1. $A = B = \{1, 2, 3\}$; $R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$; $S = \{(2, 1), (3, 1), (3, 2), (3, 3)\}$

2. $A = \{a, b, c\}$; $B = \{1, 2, 3\}$; $R = \{(a, 1), (b, 1), (c, 2), (c, 3)\}$; $S = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$

En los ejercicios 3 y 4, sean R y S dos relaciones cuyos digrafos correspondientes aparecen en las figuras 4.40 y 4.41. Calcule (a) $\overline{R}$; (b) $R\cap S$; (c) $R\cup S$; (d) S^{-1}.

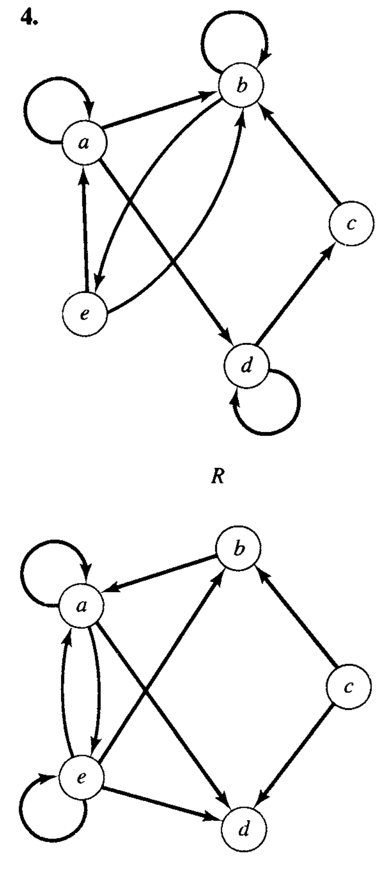
3.



R S

Figura 4.40

4.



R

S

Figura 4.41

En los ejercicios 5 y 6, sean $A = \{1, 2, 3\}$ y $B = \{1, 2, 3, 4\}$. Sean R y S las relaciones de A a B cuyas matrices son proporcionadas. Calcule (a) $\overline{S}$; (b) $R\cap S$; (c) $R\cup S$; (d) R^{-1}.

5. $\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, $\mathbf{M}_S = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$.

6. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, $\mathbf{M}_S = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$.

En los ejercicios 7 y 8, sean $A = \{1, 2, 3, 4\}$ y $B = \{1, 2, 3\}$. Dadas las matrices $\mathbf{M}_R$ y $\mathbf{M}_S$ de las relaciones R y S de A a B, calcule (a) $\mathbf{M}_{R\cap S}$; (b) $\mathbf{M}_{R\cup S}$; (c) $\mathbf{M}_{R^{-1}}$; (d) $\mathbf{M}_{\overline{S}}$.

7. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$, $\mathbf{M}_S = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

8. $\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$, $\mathbf{M}_S = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

9. Sea $A = B = \{1, 2, 3, 4\}$, $R = \{(1, 1), (1, 3), (2, 3), (3, 1), (4, 2), (4, 4)\}$, y $S = \{(1, 2), (2, 3), (3, 1), (3, 2), (4, 3)\}$. Calcule (a) $\mathbf{M}_{R\cap S}$; (b) $\mathbf{M}_{R\cup S}$; (c) $\mathbf{M}_{R^{-1}}$; (d) $\mathbf{M}_{\overline{S}}$.

10. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Supóngase que

$$R = \{(1, 2), (1, 1), (2, 1), (2, 2), (3, 3), (4, 4), (5, 5), (5, 6), (6, 5), (6, 6)\}, \text{ y}$$

$$S = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 6), (4, 4), (6, 4), (6, 6), (5, 5)\}$$

son las relaciones de equivalencia sobre A. Calcule la partición correspondiente a $R\cap S$.

11. Sea $A = \{a, b, c, d, e\}$ y supóngase que las relaciones de equivalencia R y S definidas sobre A están expresadas por

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{M}_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Calcule la partición de A correspondiente a $R\cap S$.

12. Sean $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$, y $C = \{\square, \triangle, \diamond\}$. Sean R y S las siguientes relaciones de A a B y de B a C, respectivamente.

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

$$S = \{(1, \square), (2, \triangle), (3, \triangle), (1, \diamond)\}$$

(a) Is $(b, \triangle) \in S \circ R$?
(b) Is $(c, \triangle) \in S \circ R$?
(c) Calcule $S \circ R$.

13. Sean $A = B =$ el conjunto de los números reales. Sea R la relación < (menor que) y S la relación > (mayor que). Describa (a) $R \cap S$; (b) $R \cup S$; (c) S^{-1}.

14. Sea $A =$ un conjunto de personas. Sea $a\ R\ b$ si y sólo si a y b son hermanos; sea $a\ S\ b$ si y sólo si a y b son hermanas. Describa $R \cup S$.

15. Sea $A =$ un conjunto de personas. Sea $a\ R\ b$ si y sólo si a tiene mayor edad que b; sea $a\ S\ b$ si y sólo si a es hermano de b. Describa $R \cap S$.

16. Sea $A =$ el conjunto de todas las personas que están en la base de datos del Seguro Social. Sea $a\ R\ b$ si y sólo si a y b reciben los mismos beneficios; sea $a\ S\ b$ si y sólo si a y b tienen el mismo apellido. Describa $R \cap S$.

17. Sea $A =$ un conjunto de personas. Sea $a\ R\ b$ si y sólo si a es el padre de b; sea $a\ S\ b$ si y sólo si a es la madre de b. Describa $R \cup S$.

18. Sea $A = \{2, 3, 6, 12\}$ y sean R y S las relaciones siguientes en A: $x\ R\ y$ si y sólo si $2 \mid (x - y)$; $x\ S\ y$ si y sólo si $3 \mid (x - y)$. Calcule (a) $\overline{R}$; (b) $R \cap S$; (c) $R \cup S$; (d) S^{-1}.

19. Sean $A = B = C =$ el conjunto de los números reales. Sean R y S las siguientes relaciones de A a B y de B a C, respectivamente:

$$R = \{(a, b) \mid a \leq 2b\}$$
$$S = \{(b, c) \mid b \leq 3c\}.$$

(a) ¿Es $(1, 5) \in S \circ R$?
(b) ¿Es $(2, 3) \in S \circ R$?
(c) Describa $S \circ R$.

20. Sea $A = \{1, 2, 3, 4\}$. Sean

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

(a) ¿Es $(1, 3) \in R \circ R$?
(b) ¿Es $(4, 3) \in S \circ R$?
(c) ¿Es $(1, 1) \in R \circ S$?
(d) Calcule $R \circ R$.
(e) Calcule $S \circ R$.
(f) Calcule $R \circ S$.
(g) Calcule $S \circ S$.

21. (a) ¿Cuáles propiedades de las relaciones sobre un conjunto A son conservadas por la composición? Demuestre su conclusión.
(b) Si R y S son relaciones de equivalencia en un conjunto A, ¿es $S \circ R$ una relación de equivalencia en A? Demuestre su conclusión.

En los ejercicios 22 y 23, sea $A = \{1, 2, 3, 4, 5\}$ y sean $\mathbf{M}_R$ y $\mathbf{M}_S$ las matrices de las relaciones R y S en A. Calcule (a) $\mathbf{M}_{R \circ R}$; (b) $\mathbf{M}_{S \circ R}$; (c) $\mathbf{M}_{R \circ S}$; (d) $\mathbf{M}_{S \circ S}$.

22. $$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \mathbf{M}_S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

23. $$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{M}_S = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

24. (a) Sean R y S relaciones sobre un conjunto A. Si R y S son asimétricas, demuestre o refute que $R \cap S$ y $R \cup S$ son asimétricas.
(b) Sean R y S relaciones sobre un conjunto A. Si R y S son antisimétricas, demuestre o refute que $R \cap S$ y $R \cup S$ son antisimétricas.

25. Sea R una relación de A a B y sean S y T relaciones de B a C. Demuestre o refute.
(a) $(S \cup T) \circ R = (S \circ R) \cup (T \circ R)$
(b) $(S \cap T) \circ R = (S \circ R) \cap (T \circ R)$

26. Sean R y S relaciones de A a B y sea T una relación de B a C. Demuestre que si $R \subseteq S$, entonces $T \circ R \subseteq T \circ S$.

27. Demuestre que si R y S son relaciones sobre un conjunto A, entonces
(a) $\mathbf{M}_{R \cap S} = \mathbf{M}_R \wedge \mathbf{M}_S$
(b) $\mathbf{M}_{R \cup S} = \mathbf{M}_R \vee \mathbf{M}_S$
(c) $\mathbf{M}_{R^{-1}} = (\mathbf{M}_R)^T$
(d) $\mathbf{M}_{\overline{R}} = \overline{\mathbf{M}}_R$

28. Sean R y S relaciones sobre un conjunto A. Demuestre que $(R \cap S)^n \subseteq R^n \cap S^n$, para $n \geq 1$.

29. Sea R una relación de A a B. Demuestre que
(a) $\text{Dom}(R^{-1}) = \text{Ran}(R)$
(b) $\text{Ran}(R^{-1}) = \text{Dom}(R)$

30. Demuestre el teorema 3.

4.8. Cerradura transitiva y algoritmo de Warshall

Cerradura transitiva

En esta sección se analizará una construcción que tiene varias interpretaciones y aplicaciones importantes. Supóngase que R es una relación sobre un conjunto A y que R no es transitiva. Se demostrará que la cerradura transitiva de R (véase la sección 4.7) es precisamente la relación de conectividad R^∞, definida en la sección 4.3.

Teorema 1. *Sea R una relación sobre un conjunto A. Entonces R^∞ es la cerradura transitiva de R.*

Demostración: Se recuerda que si a y b están en el conjunto A, entonces $a\ R^\infty\ b$ si y sólo si hay una trayectoria en R de a a b. Ahora R^∞ es ciertamente transitiva puesto que, si $a\ R^\infty\ b$ y $b\ R^\infty\ c$, la composición de las trayectorias de a a b y de b a c forman una trayectoria de a a c en R, y por tanto $a\ R^\infty\ c$. Para demostrar que R^∞ es la relación transitiva más pequeña que contiene a R, se debe demostrar que si S es cualquier relación transitiva en A y $R \subseteq S$, entonces $R^\infty \subseteq S$. El teorema 1 de la sección 4.4 nos dice que si S es transitiva, entonces $S^n \subseteq S$ para toda n; es decir, si a y b están conectadas por una trayectoria de longitud n, entonces $a\ S\ b$. Se sigue que $S^\infty = \bigcup_{n=1}^{\infty} S^n \subseteq S$. También es cierto que si $R \subseteq S$, entonces $R^\infty \subseteq S^\infty$, puesto que cualquier trayectoria en R también es una trayectoria en S. Juntando estos hechos, se ve que si $R \subseteq S$ y S es transitiva en A, entonces $R^\infty \subseteq S^\infty \subseteq S$. Esto significa que R^∞ es la más pequeña de todas las relaciones transitivas en A que contienen R. ●

Se ve que R^∞ tiene varias interpretaciones. Desde un punto de vista geométrico, se la llama relación de conectividad, porque especifica cuáles vértices están conectados (por trayectorias) con otros vértices. Si se incluye la relación Δ (véase la sección 4.4), entonces $R^\infty \cup \Delta$ es la relación de alcanzabilidad R^* (véase la sección 4.3), suele ser más útil. Por otra parte, desde el punto de vista algebraico, R^∞ es la cerradura transitiva de R, como se ha demostrado en el teorema 1. En esta forma, desempeña papeles importantes en la teoría de las relaciones de equivalencia y en la teoría de ciertos lenguajes (véase la sección 10.1).

Ejemplo 1. Sea $A = \{1, 2, 3, 4\}$, y sea $R = \{(1, 2), (2, 3), (3, 4), (2, 1)\}$. Encuentre la cerradura transitiva de R.

Solución

MÉTODO 1 El digrafo de R aparece en la figura 4.42. Puesto que R^∞ es la cerradura transitiva, se puede proceder geométricamente calculando todas las trayectorias. Se ve que desde el vértice 1 se tiene trayectorias a los vértices 2, 3, 4 y 1. Nótese que la trayectoria de 1 a 1 va de 1 a 2 y a 1. Se ve, de esta manera, que los pares ordenados (1, 1), (1, 2), (1, 3) y (1, 4) están en R^∞. Partiendo del vértice 2, se tiene trayectorias a los vértices 2, 1, 3 y 4, por lo cual los pares ordenados (2, 1), (2, 2), (2, 3) y (2, 4) están en R^∞. La única trayectoria que falta va del vértice 3 al vértice 4, de modo que se tiene

$$R^\infty = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4)\}.$$

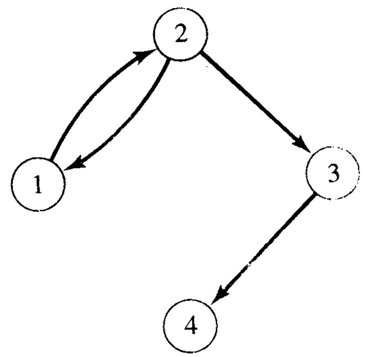


Figura 4.42

MÉTODO 2. La matriz de R es

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Se puede proceder de forma algebraica y se calcula las potencias de $\mathbf{M}_R$. Así

$$(\mathbf{M}_R)^2_\odot = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (\mathbf{M}_R)^3_\odot = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$(\mathbf{M}_R)^4_\odot = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Continuando de esta manera, se puede ver que $(\mathbf{M}_R)^n_\odot$ es igual a $(\mathbf{M}_R)^2_\odot$ si n es par, e igual a $(\mathbf{M}_R)^3_\odot$ si n es impar y mayor que 1. En consecuencia,

$$\mathbf{M}_{R^\infty} = \mathbf{M}_R \vee (\mathbf{M}_R)^2_\odot \vee (\mathbf{M}_R)^3_\odot = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

y esto da la misma relación que el método 1. ◆

En el ejemplo 1 no fue necesario considerar todas las potencias de R^n para obtener R^∞. Esta observación es cierta siempre que el conjunto A sea finito, como se demostrará ahora.

Teorema 2. *Sea A un conjunto con $|A| = n$, y sea R una relación sobre A. Entonces*

$$R^\infty = R \cup R^2 \cup \cdots \cup R^n.$$

En otras palabras, las potencias de R mayores que n no son necesarias para calcular R^∞.

Demostración: Supóngase que a y b están en A y que $a, x_1, x_2, \ldots, x_m, b$ es una trayectoria de a a b en R; es decir, $(a, x_1), (x_1, x_2), \ldots, (x_m, b)$ están todas en R. Si x_i y x_j son iguales, por decir, $i < j$, entonces la trayectoria puede dividirse en tres secciones. Primero, una trayectoria de a a x_i, luego una trayectoria de x_i a x_j, y finalmente una trayectoria de x_j a b. La trayectoria intermedia es un ciclo, puesto que $x_i = x_j$, por lo que simplemente se la deja fuera y se pone las primeras dos trayectorias juntas. Esto da una trayectoria más corta de a a b (véase la figura 4.43).

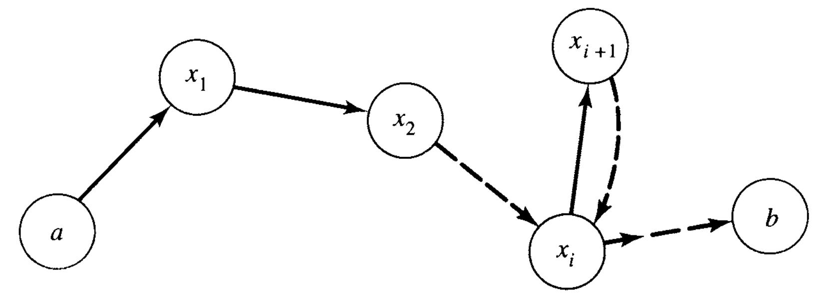


Figura 4.43

Ahora sea $a, x_1, x_2, \ldots, x_k, b$ la trayectoria más corta de a a b. Si $a \neq b$, entonces todos los vértices $a, x_1, x_2, \ldots, x_k, b$ son distintos. De lo contrario, la discusión anterior muestra que se podría encontrar una trayectoria más corta. En consecuencia, la longitud de la trayectoria es como máximo $n - 1$ (ya que $|A| = n$). Si $a = b$, entonces por razones similares, los vértices $a, x_1, x_2, \ldots, x_k$ son distintos, por lo que la longitud de la trayectoria es a lo más n. En otras palabras, si $a\ R^\infty\ b$, entonces $a\ R^k\ b$, para alguna k, $1 \leq k \leq n$. Por tanto $R^\infty = R \cup R^2 \cup \cdots \cup R^n$. ●

Los métodos empleados para resolver el ejemplo 1 presentan, cada uno, ciertas dificultades. El método gráfico no es práctico para los conjuntos y relaciones grandes, y no es sistemático. El método de matrices puede usarse en general y es suficientemente sistemático para ser programado para una computadora, pero es ineficiente y, para matrices grandes, puede ser prohibitivo por costoso. Por fortuna, se dispone de un algoritmo más eficiente para calcular la cerradura transitiva conocida como algoritmo de Warshall, en honor a su creador, el cual será descrito a continuación.

Algoritmo de Warshall

Sea R una relación sobre un conjunto $A = \{a_1, a_2, \ldots, a_n\}$. Si $x_1, x_2, \ldots, x_m$ es una trayectoria en R, entonces a todos los vértices que no sean x_1 y x_m se los llama **vértices interiores** de la trayectoria. Ahora, para $1 \leq k \leq n$, se define una matriz booleana $\mathbf{W}_k$ de la siguiente manera. $\mathbf{W}_k$ tiene un 1 en la posición i, j si y sólo si hay una trayectoria de a_i a a_j en R cuyos vértices interiores, si los hay, vienen del conjunto $\{a_1, a_2, \ldots, a_k\}$.

Como cualquier vértice debe venir del conjunto $\{a_1, a_2, \ldots, a_n\}$, se desprende que la matriz $\mathbf{W}_n$ tiene un 1 en la posición i, j si y sólo si alguna trayectoria en R conecta a a_i con a_j. En otras palabras, $\mathbf{W}_n = \mathbf{M}_{R^\infty}$. Si se define $\mathbf{W}_0$ como que es $\mathbf{M}_R$, entonces se tendrá una secuencia $\mathbf{W}_0, \mathbf{W}_1, \ldots, \mathbf{W}_n$ cuyo primer término es $\mathbf{M}_R$ y cuyo último término es $\mathbf{M}_{R^\infty}$. Ahora se mostrará cómo calcular cada matriz $\mathbf{W}_k$ a partir de la matriz anterior $\mathbf{W}_{k-1}$. Entonces se puede comenzar con la matriz de R y proseguir con un paso a la vez hasta que, después de n pasos, se llegue a la matriz de R^∞. Este procedimiento se llama **algoritmo de Warshall**. Las matrices $\mathbf{W}_k$ son diferentes de las potencias de la matriz $\mathbf{M}_R$, y esta diferencia da lugar a un ahorro considerable de pasos en el cálculo de la cerradura transitiva de R.

Supóngase que $\mathbf{W}_k = [t_{ij}]$ y $\mathbf{W}_{k-1} = [s_{ij}]$. Si $t_{ij} = 1$, entonces debe haber una trayectoria de a_i a a_j cuyos vértices interiores vengan del conjunto $\{a_1, a_2, \ldots, a_k\}$. Si el vértice a_k no es un vértice interior de esta trayectoria, entonces todos los vértices interiores deben venir realmente del conjunto $\{a_1, a_2, \ldots, a_{k-1}\}$, de manera que $s_{ij} = 1$. Si a_k es un vértice interior de la trayectoria entonces la situación es como se ilustra en la figura 4.44. Como en la demostración del teorema 2, se puede suponer que todos los vértices interiores son distintos. En consecuencia a_k aparece sólo una vez en la trayectoria, de manera que todos los vértices interiores de las subtrayectorias 1 y 2 deben venir del conjunto $\{a_1, a_2, \ldots, a_{k-1}\}$. Esto significa que $s_{ik} = 1$ y $s_{kj} = 1$.

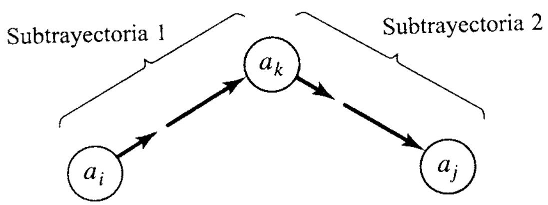


Figura 4.44

En consecuencia, $t_{ij} = 1$ si y sólo si

(1) $s_{ij} = 1$ o
(2) $s_{ik} = 1$ y $s_{kj} = 1$.

Ésta es la base para el algoritmo de Warshall. Si $\mathbf{W}_{k-1}$ tiene un 1 en la posición i, j entonces, por (1), también lo tendrá $\mathbf{W}_k$. Por (2), puede agregarse un nuevo 1 en la posición i, j de $\mathbf{W}_k$ si y sólo si la columna k de $\mathbf{W}_{k-1}$ tiene un 1 en el renglón i y el renglón k de $\mathbf{W}_{k-1}$ tiene un 1 en la columna j. Por tanto, se tiene el siguiente procedimiento para calcular $\mathbf{W}_k$ a partir de $\mathbf{W}_{k-1}$.

PASO 1. Primero transfiera a $\mathbf{W}_k$ todos los unos de $\mathbf{W}_{k-1}$.

PASO 2. Haga una lista de las posiciones $p_1, p_2, \ldots$, en la columna k de $\mathbf{W}_{k-1}$, en donde la entrada sea 1, y las posiciones $q_1, q_2, \ldots$, en el renglón k de $\mathbf{W}_{k-1}$, en donde la entrada sea 1.

PASO 3. Ponga los unos en todas las posiciones p_i, q_j de $\mathbf{W}_k$ (si no están ya allí).

Ejemplo 2. Considere la relación R que se definió en el ejemplo 1. Entonces

$$\mathbf{W}_0 = \mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

y $n = 4$.

Primero se determina $\mathbf{W}_1$ de manera que $k = 1$. $\mathbf{W}_0$ tiene unos en la posición 2 de la columna 1 y en la posición 2 del renglón 1. En consecuencia, $\mathbf{W}_1$ simplemente es $\mathbf{W}_0$ con un nuevo 1 en la posición 2, 2.

$$\mathbf{W}_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Ahora se calcula $\mathbf{W}_2$ de manera que $k = 2$. Se debe consultar la columna 2 y el renglón 2 de $\mathbf{W}_1$. La matriz $\mathbf{W}_1$ tiene unos en las posiciones 1 y 2 de la columna 2 y las posiciones 1, 2 y 3 del renglón 2.

En consecuencia, para obtener $\mathbf{W}_2$, se debe poner unos en las posiciones dadas por los pares ordenados (1, 1), (1, 2), (1, 3), (2, 1), (2, 2) y (2, 3) de la matriz $\mathbf{W}_1$ (si los unos no están ya allí). Se observa que

$$\mathbf{W}_2 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Prosiguiendo, se observa que la columna 3 de $\mathbf{W}_2$ tiene unos en las posiciones 1 y 2, y el renglón 3 de $\mathbf{W}_2$ tiene un 1 en la posición 4. Para obtener $\mathbf{W}_3$, se debe poner unos en las posiciones 1, 4 y 2, 4 de $\mathbf{W}_2$, de manera que

$$\mathbf{W}_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Finalmente, $\mathbf{W}_3$ tiene unos en las posiciones 1, 2, 3 de la columna 4 y ningún uno en el renglón 4, por tanto no se agrega unos nuevos y $\mathbf{M}_{R^\infty} = \mathbf{W}_4 = \mathbf{W}_3$. Así pues, se ha obtenido el mismo resultado que en el ejemplo 1. ◆

El procedimiento ilustrado en el ejemplo 2 da como resultado el siguiente algoritmo para calcular la matriz, CERRADURA, de la cerradura transitiva de una relación R representada por la matriz MAT, $N \times N$.

ALGORITMO WARSHALL
1. CLOSURE ← MAT
2. **FOR** K = 1 **THRU** N
   a. **FOR** I = 1 **THRU** N
      1. **FOR** J = 1 **THRU** N
         a. CLOSURE $[I, J]$ ← CLOSURE $[I, J]$
            ∨ (CLOSURE $[I, K]$ ∧ CLOSURE $[K, J]$)

FIN DEL ALGORITMO WARSHALL

Este algoritmo se estableció para proceder exactamente como se ha delineado previamente. Con un ligero rearreglo de los pasos, se puede volver un poco más eficiente. Si se considera la prueba y la línea de asignación como un paso, entonces el algoritmo WARSHALL requiere n^3 pasos en total. El producto booleano de dos matrices booleanas $n \times n$, $\mathbf{A}$ y $\mathbf{B}$ requiere también n^3 pasos, puesto que se debe calcular n^2 entradas, y cada uno de éstos requiere de n comparaciones. Para calcular todos los productos $(\mathbf{M}_R)^2_{\odot}, (\mathbf{M}_R)^3_{\odot}, \ldots, (\mathbf{M}_R)^n_{\odot}$, se requiere $n^3(n-1)$ pasos, puesto que se necesitará $n-1$ multiplicaciones de matrices. La fórmula

$$\mathbf{M}_{R^\infty} = \mathbf{M}_R \vee (\mathbf{M}_R)^2_{\odot} \vee \cdots \vee (\mathbf{M}_R)^n_{\odot}, \tag{1}$$

si se implementara directamente, requeriría alrededor de n^4 pasos sin las uniones finales. En consecuencia, el algoritmo de Warshall es una mejora significativa sobre el cálculo directo de $\mathbf{M}_{R^\infty}$ por medio de la fórmula (1).

Una aplicación interesante de la cerradura transitiva ocurre en las relaciones de equivalencia. En la sección 4.7 se demostró que si R y S son relaciones de equivalencia en un conjunto A, entonces $R \cap S$ también es una relación de equivalencia en A. La relación $R \cap S$ es la relación de equivalencia más grande contenida tanto en R como en S, puesto que es el subconjunto más grande de $A \times A$ contenido en ambos, R y S. Se desea conocer la relación de equivalencia más pequeña que contiene tanto a R como a S. El candidato natural es $R \cup S$, pero esta relación no es necesariamente transitiva. La solución se proporciona en el siguiente teorema.

Teorema 3. *Si R y S son relaciones de equivalencia en un conjunto A, entonces la relación de equivalencia más pequeña que contiene a ambas, R y S, es $(R \cup S)^\infty$.*

Demostración: Debe recordarse que Δ es la relación de igualdad en A y que una relación es reflexiva si y sólo si contiene a Δ. Entonces $\Delta \subseteq R$, $\Delta \subseteq S$ puesto que ambas son reflexivas, de modo que $\Delta \subseteq R \cup S \subseteq (R \cup S)^\infty$, y $(R \cup S)^\infty$ también es reflexiva.

Como R y S son simétricas, $R = R^{-1}$ y $S = S^{-1}$, de modo que $(R \cup S)^{-1} = R^{-1} \cup S^{-1} = R \cup S$, y $R \cup S$ también es simétrica. Por todo esto, todas las trayectorias en $R \cup S$ son "calles de dos sentidos", y se desprende de las definiciones que $(R \cup S)^\infty$ debe también ser simétrica. Como ya se sabe que $(R \cup S)^\infty$ es transitiva, es una relación de equivalencia que contiene a $R \cup S$. Es la más pequeña, porque ningún conjunto más pequeño que contenga a $R \cup S$ puede ser transitivo, por la propia definición de cerradura transitiva. ●

Ejemplo 3. Sean $A = \{1, 2, 3, 4, 5\}$, $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4), (5, 5)\}$, y $S = \{(1, 1), (2, 2), (3, 3), (4, 4), (4, 5), (5, 4), (5, 5)\}$. El lector puede verificar que ambas, R y S son relaciones de equivalencia. La partición A/R de A correspondiente a R es $\{\{1, 2\}, \{3, 4\}, \{5\}\}$, y la partición A/S de A correspondiente a S es $\{\{1\}, \{2\}, \{3\}, \{4, 5\}\}$. Encuentre la relación de equivalencia más pequeña que contenga a R y S, y calcule la partición de A que produce.

Solución: Se tiene que

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{y} \quad \mathbf{M}_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

de modo que

$$\mathbf{M}_{R \cup S} = \mathbf{M}_R \vee \mathbf{M}_S = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Ahora se calcula $\mathbf{M}_{(R \cup S)^\infty}$ por el algoritmo de Warshall. Primero, $\mathbf{W}_0 = \mathbf{M}_{R \cup S}$. En seguida, se calcula $\mathbf{W}_1$, de manera que $k = 1$. Puesto que $\mathbf{W}_0$ tiene unos en las posiciones 1 y 2 de la columna 1 y en las posiciones 1 y 2 del renglón 1, se encuentra que no tiene que añadirse a $\mathbf{W}_1$ nuevos unos. En consecuencia,

$$\mathbf{W}_1 = \mathbf{W}_0.$$

Ahora se calcula $\mathbf{W}_2$, de manera que $k = 2$. Puesto que $\mathbf{W}_1$ tiene unos en las posiciones 1 y 2 de la columna 2 y en los lugares 1 y 2 del renglón 2, se encuentra que no hay que agregar nuevos unos a $\mathbf{W}_1$. En consecuencia

$$\mathbf{W}_2 = \mathbf{W}_1.$$

En seguida, se calcula $\mathbf{W}_3$, de manera que $k = 3$. Puesto que $\mathbf{W}_2$ tiene unos en las posiciones 3 y 4 de la columna 3 y en las posiciones 3 y 4 del renglón 3, se encuentra que no hay que agregar nuevos unos a $\mathbf{W}_2$. Por tanto,

$$\mathbf{W}_3 = \mathbf{W}_2.$$

Las cosas cambian cuando se calcula $\mathbf{W}_4$. Como $\mathbf{W}_3$ tiene unos en las posiciones 3, 4 y 5 de la columna 4 y en las posiciones 3, 4 y 5 del renglón 4, se debe agregar nuevos unos a $\mathbf{W}_3$ en las posiciones 3, 5 y 5, 3. En consecuencia

$$\mathbf{W}_4 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

El lector puede verificar que $\mathbf{W}_5 = \mathbf{W}_4$ y por tanto, se tiene

$$(R \cup S)^\infty = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (3, 5), (4, 3), (4, 4), (4, 5), (5, 3), (5, 4), (5, 5)\}.$$

Entonces, la partición correspondiente de A es (verifique) $\{\{1, 2\}, \{3, 4, 5\}\}$. ◆

GRUPO DE EJERCICIOS 4.8

1. (a) Sea $A = \{1, 2, 3\}$ y sea $R = \{(1, 1), (1, 2), (2, 3), (1, 3), (3, 1), (3, 2)\}$. Calcule la matriz $\mathbf{M}_{R^\infty}$ de la cerradura transitiva R por medio de la fórmula

$$\mathbf{M}_{R^\infty} = \mathbf{M}_R \vee (\mathbf{M}_R)^2_{\odot} \vee (\mathbf{M}_R)^3_{\odot}.$$

   (b) Haga una lista de la relación R^∞ cuya matriz se calculó en la parte (a).

2. Para la relación R del ejercicio 1, calcule la cerradura transitiva R^∞ por medio del algoritmo de Warshall.

3. Sea $A = \{a_1, a_2, a_3, a_4, a_5\}$ y sea R una relación sobre A cuya matriz es

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \mathbf{W}_0.$$

   Calcule $\mathbf{W}_1$, $\mathbf{W}_2$ y $\mathbf{W}_3$ como en el algoritmo de Warshall.

4. Determine R para la relación del ejercicio 3.

5. Demuestre que si R es reflexiva y transitiva, entonces $R^n = R$ para todas las n.

6. Sea R una relación sobre un conjunto A, y sea $S = R^2$. Demuestre que si $a, b \in A$, entonces $a\ S^\infty\ b$ si y sólo si hay una trayectoria en R de a a b que tenga un número par de lados.

En los ejercicios 7 al 10, sea $A = \{1, 2, 3, 4\}$. Para la relación R cuya matriz se da, determine la matriz de la cerradura transitiva por medio del algoritmo de Warshall.

7. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

8. $\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

9. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

10. $\mathbf{M}_R = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

En los ejercicios 11 y 12, sea $A = \{1, 2, 3, 4, 5\}$ y sean R y S las relaciones de equivalencia en A cuyas matrices se dan. Calcule la matriz de la relación de equivalencia más pequeña que contenga a R y S, y haga una lista de los elementos de esta relación.

11. $\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$ $\mathbf{M}_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

12. $\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$ $\mathbf{M}_S \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

13. Calcule la partición de A que corresponda a la relación de equivalencia encontrada en el ejercicio 11.

14. Calcule la partición de A que corresponda a la relación de equivalencia encontrada en el ejercicio 12.

15. Sea $A = \{a, b, c, d, e\}$ y sean R y S las relaciones sobre A descritas por

$$M_R = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

y

$$\mathbf{M}_S = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Utilice el algoritmo de Warshall para calcular la cerradura transitiva de $R \cup S$.

IDEAS CLAVE PARA REPASO

- $A \times B$ (conjunto producto o producto cartesiano): $\{(a, b) \mid a \in A \text{ y } b \in B\}$.
- $|A \times B| = |A|\,|B|$
- Partición o conjunto cociente; véase la página 103.
- Relación de A a B: subconjunto de $A \times B$.
- Dominio y rango de una relación: véase la página 109.
- Conjuntos relativos $R(a)$, a en A, y $R(B)$, B es un subconjunto de A: véase la página 109.
- Matriz de una relación: véase la página 111.
- Digrafo de una relación: representación gráfica de una relación: véase la página 111.
- Trayectoria de longitud n de a a b en una relación R: secuencia finita $a, x_1, x_2, \ldots, x_{n-1}, b$ tal que $a\ R\ x_1$, $x_1\ R\ x_2, \ldots, x_{n-1}\ R\ b$.
- $x\ R^n\ y$ (R una relación sobre A): Hay una trayectoria de longitud n, de x a y en R.
- $x\ R^\infty\ y$ (relación de conectividad para R). Existe alguna trayectoria en R de x a y.
- Teorema: $\mathbf{M}_{R^n} = \mathbf{M}_R \odot \mathbf{M}_R \odot \cdots \odot \mathbf{M}_R$ (n factores).
- Propiedades de las relaciones sobre un conjunto A:

Reflexiva	$(a, a) \in R$ para toda $a \in A$
Irreflexiva	$(a, a) \notin R$ para toda $a \in A$
Simétrica	$(a, b) \in R$ implica que $(b, a) \in R$
Asimétrica	$(a, b) \in R$ implica que $(b, a) \notin R$
Antisimétrica	$(a, b) \in R$ y $(b, a) \in R$ implica que $a = b$
Transitiva	$(a, b) \in R$ y $(b, c) \in R$ implica que $(a, c) \in R$

- Gráfica de una relación simétrica: véase la página 127.
- Vértices adyacentes: véase la página 127.
- Relación de equivalencia: relación reflexiva, simétrica y transitiva.
- Relación de equivalencia determinada por una partición: véase la página 132.
- Representación en computadora de la lista enlazada de una relación: véase la página 136.
- $a\ \overline{R}\ b$ (complemento de R): $a\ \overline{R}\ b$ si y sólo si $a\ \not R\ b$.
- R^{-1}: $(x, y) \in R^{-1}$ si y sólo si $(y, x) \in R$.
- $R \cup S$, $R \cap S$: véase la página 146.
- $\mathbf{M}_{R \cap S} = \mathbf{M}_R \wedge \mathbf{M}_S$
- $\mathbf{M}_{R \cup S} = \mathbf{M}_R \vee \mathbf{M}_S$
- $\mathbf{M}_{R^{-1}} = (\mathbf{M}_R)^T$
- $\mathbf{M}_{\overline{R}} = \overline{\mathbf{M}}_R$
- Si R y S son relaciones de equivalencia, también lo es $R \cap S$: véase la página 150.
- $R \circ S$: véase la página 152.
- $\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S$: véase la página 153.
- Teorema: R^∞ es la relación transitiva más pequeña en A que contiene a R: véase la página 157.
- Teorema: Si $|A| = n$, $R^\infty = R \cup R^2 \cup \cdots \cup R^n$
- Algoritmo de Warshall: calcula $\mathbf{M}_{R^\infty}$ eficientemente: véase la página 159.
- Teorema: Si R y S son relaciones de equivalencia en A, $(R \cup S)^\infty$ es la relación de equivalencia más pequeña en A que contiene tanto a A como a B.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes casos, escriba el programa o subrutina solicitado en seudocódigo (como se describe en el apéndice A) o en un lenguaje de programación que usted conozca. Pruebe su código ya sea con una prueba de escritorio o con una corrida de computadora.

1. Escriba un programa CROSS, con entrada de enteros positivos m y n y salida, el conjunto $A \times B$, en donde $A = \{1, 2, 3, \ldots, m\}$ y $B = \{1, 2, 3, \ldots, n\}$.

2. (a) Escriba una subrutina que tenga como entrada la matriz de una relación y determine si la relación es reflexiva.
   (b) Escriba una subrutina que tenga como entrada la matriz de una relación y determine si la relación es simétrica.

3. Escriba un programa que tenga como entrada la matriz de una relación y determine si la relación es de equivalencia.

4. Sean R y S relaciones representadas por las matrices $\mathbf{M}_R$ y $\mathbf{M}_S$, respectivamente. Escriba una subrutina para obtener la matriz de
   (a) $R \cup S$.
   (b) $R \cap S$.
   (c) $R \circ S$.

5. Sea R una relación representada por la matriz $\mathbf{M}_R$. Escriba una subrutina para obtener la matriz de
   (a) R^{-1}.
   (b) $\overline{R}$.

CAPÍTULO 5

FUNCIONES

Requisito previo: Capítulo 4

En este capítulo, la atención se enfoca a un tipo especial de relación, una función, que desempeña un papel importante en las matemáticas, la ciencia de la computación y en muchas aplicaciones. Se define, también, algunas funciones que se utiliza en la ciencia de la computación y se examina el crecimiento de las funciones.

5.1. Funciones

En esta sección se define el término función, un tipo especial de relación. Se estudia sus propiedades básicas y luego se analiza varios tipos especiales de funciones. En secciones posteriores del libro se mostrará algunas aplicaciones importantes de las funciones, por lo que es indispensable comprender adecuadamente el material de esta sección.

Sean A y B conjuntos no vacíos. Una **función** f de A a B, que se denota por $f: A \to B$, es una relación de A a B de tal manera que para todas las $a \in \mathrm{Dom}(f)$, $f(a)$ contiene sólo un elemento de B. Naturalmente, si a no está en Dom(f), entonces $f(a) = \varnothing$. Si $f(a) = \{b\}$, tradicionalmente identifica el conjunto $\{b\}$ con el elemento b y se escribe $f(a) = b$. Se continuará con esta costumbre, ya que no causa confusión. Entonces, la relación f puede describirse como el conjunto de pares $\{(a, f(a)) \mid a \in \text{Dom}(f)\}$. Las funciones son llamadas también **mapeos** o **transformaciones**, debido a que pueden ser consideradas geométricamente como reglas que asignan a cada elemento $a \in A$ el elemento único $f(a) \in B$ (véase la figura 5.1). El elemento a se denomina **argumento** de la función f, y a $f(a)$ se llama **valor** de la función para el argumento a y también es conocido como la **imagen** de a bajo f. La figura 5.1 es una ilustración esquemática o gráfica de la definición de función que se está empleando, y se utilizará otros diagramas similares. No deben ser confundidos con el digrafo de la relación f, el cual normalmente no se ilustra.

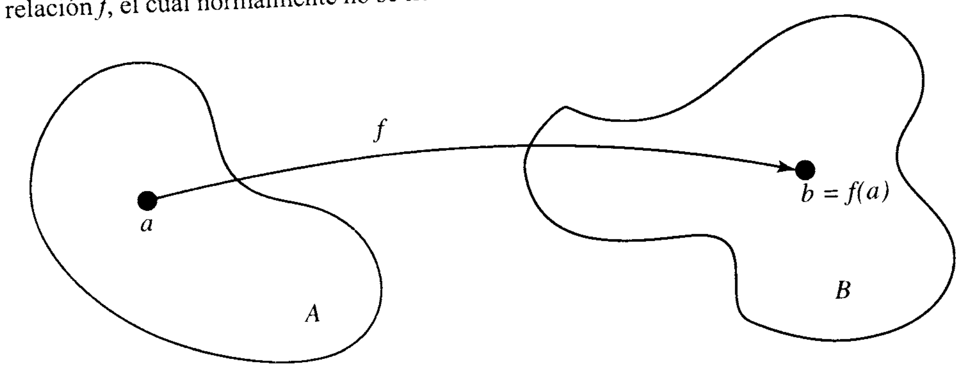


Figura 5.1

Ejemplo 1. Sean $A = \{1, 2, 3, 4\}$ y $B = \{a, b, c, d\}$, y sea

$$f = \{(1, a), (2, a), (3, d), (4, c)\}.$$

Aquí se tiene

$$\begin{aligned} f(1) &= a \\ f(2) &= a \\ f(3) &= d \\ f(4) &= c. \end{aligned}$$

Como cada conjunto $f(n)$ es un solo valor, f es una función.

Observe que el elemento $a \in B$ aparece como el segundo elemento de dos pares ordenados diferentes en f. Esto no contradice la definición de una función. En consecuencia, una función puede tomar el mismo valor en dos elementos diferentes de A. ◆

Ejemplo 2. Sean $A = \{1, 2, 3\}$ y $B = \{x, y, z\}$. Considérense las relaciones

$$R = \{(1, x), (2, x)\} \quad \text{y} \quad S = \{(1, x), (1, y), (2, z), (3, y)\}.$$

La relación S no es una función puesto que $S(1) = \{x, y\}$. La relación R es una función con $\text{Dom}(R) = \{1, 2\}$ y $\text{Ran}(R) = \{x\}$. ◆

Ejemplo 3. Sea P un programa de computadora que acepta un entero como entrada y produce un entero como salida. Sea $A = B = Z$. Entonces P determina una relación f_P que se define como sigue: $(m, n) \in f_P$ significa que n es la salida producida por el programa P cuando la entrada es m.

Es claro que f_P es una función, puesto que cualquier entrada particular corresponde a una salida única (los resultados de computadora son reproducibles; es decir, son los mismos cada vez que se corre el programa). ◆

El ejemplo 3 puede generalizarse a un programa con cualquier conjunto A de entradas posibles y el conjunto B de salidas correspondientes. Por lo tanto, en general puede pensarse en las funciones como relaciones de **entrada-salida**.

Ejemplo 4. Sea $A = \mathbb{R}$ el conjunto de todos los números reales, y sea $p(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomio real. Entonces p puede verse como una relación en A. Para cada a en $\mathbb{R}$ se determina el conjunto relativo $p(a)$ sustituyendo a en el polinomio. Entonces, como todos los conjuntos relativos $p(a)$ son conocidos, la relación p está determinada. Puesto que se produce un valor único por esta sustitución, la relación p es realmente una función. ◆

Si la fórmula que define la función no tiene sentido para todos los elementos de A, entonces se toma el dominio de la función como el conjunto de los elementos de A para los cuales sea válida la fórmula.

En matemáticas elementales, la *fórmula* (en el caso del ejemplo 4, el polinomio) suele confundirse con la *función* que produce. Esto no es un problema, a no ser que el estudiante espere que exista una fórmula para cada tipo de función.

Supóngase que, en la construcción anterior, se usara una fórmula que produjera más de un elemento en $p(x)$, por ejemplo, $p(x) = \pm\sqrt{x}$. Entonces la relación resultante no sería una función. Por esta razón, en los textos anteriores, a veces a las relaciones, se las llamaba funciones de valores múltiples.

Ejemplo 5. Un **digrafo etiquetado** es un digrafo en el que los vértices o los lados (o ambos) son etiquetados o marcados con información procedente de un conjunto. Si V es el conjunto de vértices y L es el conjunto de etiquetas de un digrafo etiquetado, entonces el etiquetado de V puede especificarse como una función $f: V \to L$, en donde, para cada $v \in V$, $f(v)$ es la etiqueta que se desea colocar a v. De modo similar, puede definirse un etiquetado de los lados E como una función $g: E \to L$, en donde, para cada $e \in E$, $g(e)$ es la etiqueta que se desea colocar a e. Un ejemplo de digrafo etiquetado es un mapa donde los vértices son etiquetados con los nombres de ciudades y los lados, con las distancias o tiempos de viaje entre las ciudades. Otro ejemplo es un diagrama de flujo de un programa en el cual los vértices son etiquetados con los pasos que hay que efectuar en determinado punto del programa; los lados indican el flujo de una parte a otra del programa. La figura 5.2 muestra un ejemplo de un digrafo etiquetado. ◆

Ejemplo 6. Sean $A = B = Z$ y supóngase que $f: A \to B$ está definida por

$$f(a) = a + 1, \quad \text{para } a \in A.$$

Aquí, como en el ejemplo 4, se define f dando una fórmula para los valores de $f(a)$. ◆

Ejemplo 7. Sea $A = Z$ y sea $B = \{0, 1\}$. Defínase $f: A \to B$ por

$$f(a) = \begin{cases} 0 & \text{si } a \text{ es par} \\ 1 & \text{si } a \text{ es impar.} \end{cases}$$

Entonces f es una función, puesto que cada conjunto $f(a)$ consta de un solo elemento. A diferencia de la situación de los ejemplos 4 y 6, los elementos $f(a)$ no están especificados por medio de una fórmula algebraica. En vez de ésta se da una descripción verbal. ♦

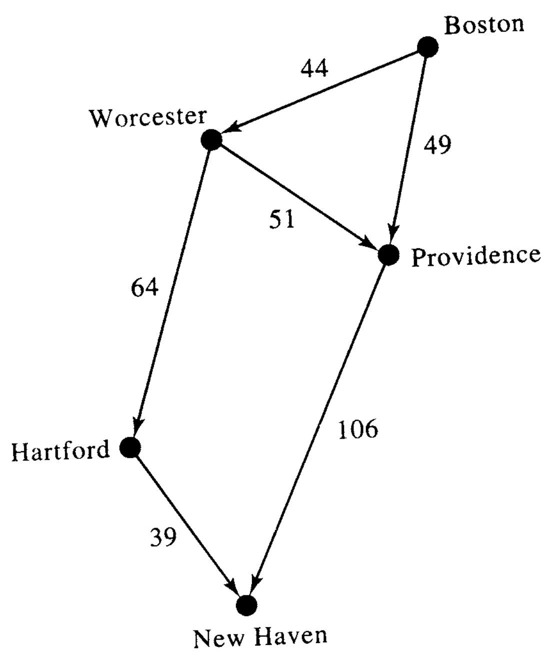


Figura 5.2

Ejemplo 8. Sea A un conjunto arbitrario no vacío. La función identidad en A, designada por 1_A, está definida por

$$1_A(a) = a.$$ ♦

El lector puede observar que 1_A es la relación a la que previamente se llamó Δ (véase la sección 4.4), la cual representa al subconjunto diagonal de $A \times A$. En el contexto de las funciones, se prefiere la notación 1_A, porque acentúa la naturaleza de entrada-salida o funcional de la relación. Es claro que, si $A_1 \subseteq A$, entonces $1_A(A_1) = A_1$.

Supóngase que $f: A \to B$ y $g: B \to C$ son funciones. Entonces la composición de f y g, $g \circ f$ (véase la sección 4.7), es una relación. Sea $a \in \text{Dom}(g \circ f)$. Entonces, por el teorema 6 de la sección 4.7, $(g \circ f)(a) = g(f(a))$. Como f y g son funciones, $f(a)$ consta de un solo elemento $b \in B$, de modo que $g(f(a)) = g(b)$. Como g también es una función, $g(b)$ contiene sólo un elemento de C. En consecuencia, cada conjunto $(g \circ f)(a)$, para a en $\text{Dom}(g \circ f)$, contiene sólo un elemento de C, de modo que $g \circ f$ es una función. Esto se ilustra esquemáticamente en la figura 5.3.

Ejemplo 9. Sean $A = B = Z$, y sea C el conjunto de los enteros pares. Supóngase que $f: A \to B$ y $g: B \to C$ están definidas por

$$f(a) = a + 1$$
$$g(b) = 2b.$$

Determine $g \circ f$.

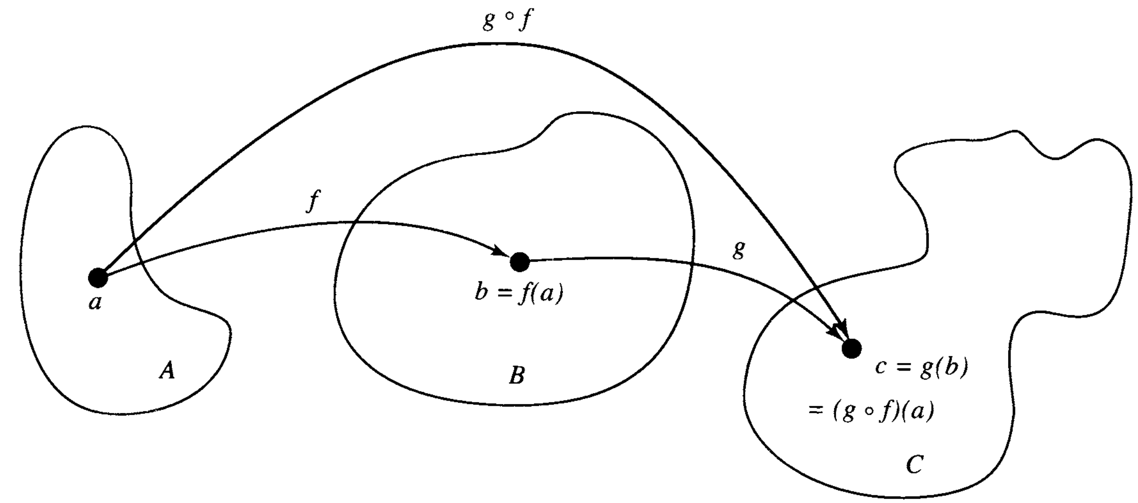


Figura 5.3

Solución: Se tiene que

$$\begin{aligned}(g \circ f)(a) &= g(f(a)) \\ &= g(a+1) \\ &= 2(a+1).\end{aligned}$$

En consecuencia, si f y g son funciones especificadas por medio de fórmulas, entonces también lo es $g \circ f$, y la fórmula para $g \circ f$ se produce sustituyendo la fórmula para f en la fórmula para g. ♦

Tipos especiales de funciones

Sea f una función de A a B. Entonces se dice que f está **definida en todas partes** si $\text{Dom}(f) = A$. Se dice que f es **sobre** si $\text{Ran}(f) = B$. Finalmente, se dice que f es **uno a uno** si no se puede tener $f(a) = f(a')$ para dos elementos distintos a y a' de A. La definición de uno a uno puede reexpresarse en la siguiente forma equivalente:

$$\text{Si } f(a) = f(a'), \quad \text{entonces } a = a'.$$

Esta última forma es a menudo más fácil de verificar en ejemplos particulares.

Ejemplo 10. Considérese la función f definida en el ejemplo 1. Puesto que $\text{Dom}(f) = A$, f está definida en todas partes. Por otra parte, $\text{Ran}(f) = \{a, c, d\} \neq B$; por lo tanto, f no es sobre. En vista de que

$$f(1) = f(2) = a,$$

se puede concluir que f no es uno a uno. ♦

Ejemplo 11. Considérese la función f definida en el ejemplo 6. ¿Cuáles de las propiedades especiales anteriores, si hay alguna, posee f?

Solución: Como la fórmula que define a f tiene sentido para todos los enteros, $\text{Dom}(f) = Z = A$, y en consecuencia f está definida en todas partes.

Supóngase que

$$f(a) = f(a')$$

para a y a' en A. Entonces

$$a + 1 = a' + 1$$

de modo que

$$a = a'.$$

Por tanto f es uno a uno.

Para ver si f es sobre, sea b un elemento arbitrario de B. ¿Puede encontrarse un elemento $a \in A$ tal que $f(a) = b$?

Puesto que

$$f(a) = a + 1,$$

se necesita un elemento a en A tal que

$$a + 1 = b.$$

Por supuesto,

$$a = b - 1$$

satisfará la ecuación deseada, puesto que $b - 1$ está en A. De allí que, $\text{Ran}(f) = B$; por lo tanto, f es sobre. ◆

Ejemplo 12. Sean $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2, b_3\}$, $C = \{c_1, c_2\}$, y $D = \{d_1, d_2, d_3, d_4\}$. Considérese las siguientes cuatro funciones, de A a B, de A a D, de B a C y D a B, respectivamente.

(a) $f_1 = \{(a_1, b_2), (a_2, b_3), (a_3, b_1)\}$.
(b) $f_2 = \{(a_1, d_2), (a_2, d_1), (a_3, d_4)\}$.
(c) $f_3 = \{(b_1, c_2), (b_2, c_2), (b_3, c_1)\}$.
(d) $f_4 = \{(d_1, b_1), (d_2, b_2), (d_3, b_1)\}$.

Determine si cada función está o no uno a uno, si cada función está o no sobre y si cada función está definida en todas partes.

Solución

(a) f_1 está definida en todas partes, es uno a uno y es sobre.
(b) f_2 está definida en todas partes y es uno a uno, pero no es sobre.
(c) f_3 está definida en todas partes y es sobre, pero no es uno a uno.
(d) f_4 no está definida en todas partes, no es uno a uno y no es sobre. ◆

Si $f: A \to B$ es una función uno a uno, entonces f asocia a cada elemento a de $\text{Dom}(f)$ un elemento $b = f(a)$ de $\text{Ran}(f)$. Cada b del $\text{Ran}(f)$ se relaciona, de esta forma, con uno y solamente un elemento de $\text{Dom}(f)$. Por esta razón, a una f de tal naturaleza se la llama, a menudo, **biyección** entre $\text{Dom}(f)$ y $\text{Ran}(f)$. Si f está también definida en todas partes y es sobre, entonces a f se la llama **correspondencia uno a uno entre A y B**.

Ejemplo 13. Sea $\mathcal{R}$ el conjunto de todas las relaciones de equivalencia en un conjunto dado A, y sea Π el conjunto de todas las particiones en A. Entonces se puede definir una función $f: \mathcal{R} \to \Pi$ como sigue. Para cada relación de equivalencia R en A, sea $f(R) = A/R$, la partición de A que corresponde a R. La discusión de la sección 4.5 muestra que f es una correspondencia uno a uno entre $\mathcal{R}$ y Π. ◆

Funciones invertibles

Se dice que una función $f: A \to B$ es **invertible** si su relación inversa, f^{-1}, también es una función. El ejemplo siguiente muestra que una función no necesariamente es invertible.

Ejemplo 14. Sea f la función del ejemplo 1. Entonces

$$f^{-1} = \{(a, 1), (a, 2), (d, 3), (c, 4)\}.$$

Se ve que f^{-1} no es una función, puesto que $f^{-1}(a) = \{1, 2\}$. ◆

Con frecuencia se emplea el siguiente teorema.

Teorema 1. *Sea $f: A \to B$ una función.*
(a) *Entonces f^{-1} es una función de B a A si y sólo si f es uno a uno.*
(b) *Si f^{-1} es una función, entonces la función f^{-1} también es uno a uno.*
(c) *f^{-1} está definida en todas partes si y sólo si f es sobre.*
(d) *f^{-1} es sobre si y sólo si f está definida en todas partes.*

Demostración: (a) Se demostrará el siguiente enunciado equivalente.

f^{-1} no es una función si y sólo si f no es uno a uno.

Supóngase, primero, que f^{-1} no es una función. Entonces, para alguna b en B, $f^{-1}(b)$ debe contener por lo menos dos elementos distintos, a_1 y a_2. Entonces $f(a_1) = b = f(a_2)$, por lo cual f no es uno a uno.

A la inversa, supóngase que f no es uno a uno. Entonces $f(a_1) = f(a_2) = b$ para dos elementos distintos a_1 y a_2 de A. En consecuencia, $f^{-1}(b)$ contiene a ambos a_1 y a_2, por lo que f^{-1} no puede ser una función.

(b) Puesto que $(f^{-1})^{-1}$ es la función f, la parte (a) demuestra que f^{-1} es uno a uno.

(c) Se recordará que $\text{Dom}(f^{-1}) = \text{Ran}(f)$. En consecuencia, $B = \text{Dom}(f^{-1})$ si y sólo si $B = \text{Ran}(f)$. En otras palabras, f^{-1} está definida en todas partes si y sólo si f es sobre.

(d) Puesto que $\text{Ran}(f^{-1}) = \text{Dom}(f)$, $A = \text{Dom}(f)$ si y sólo si $A = \text{Ran}(f^{-1})$. Es decir, f está definida en todas partes si y sólo si f^{-1} es sobre. ●

Como consecuencia inmediata del teorema 1, se observa que si f es una correspondencia de uno a uno entre A y B, entonces f^{-1} es una correspondencia de uno a uno entre B y A. Nótese también que si $f: A \to B$ es una función uno a uno, entonces la ecuación $b = f(a)$ es equivalente a $a = f^{-1}(b)$.

Ejemplo 15. Considérese la función f definida en el ejemplo 6. Como f está definida en todas partes, es uno a uno y sobre, entonces es una correspondencia uno a uno entre A y B.

En consecuencia, f es invertible, y f^{-1} es una correspondencia uno a uno entre B y A. ◆

Ejemplo 16. Sea $\mathbb{R}$ el conjunto de los números reales y supóngase que $f: \mathbb{R} \to \mathbb{R}$ está definida por $f(x) = x^2$. ¿Es f invertible?

Solución: Debe determinarse si f es uno a uno. Puesto que

$$f(2) = f(-2) = 4,$$

se llega a la conclusión de que f no es uno a uno. Por tanto f no es invertible. ◆

Hay algunos resultados útiles que se relacionan con la composición de funciones. Se resumen en el teorema siguiente.

Teorema 2. *Sea $f: A \to B$ una función cualquiera. Entonces*

(a) $1_B \circ f = f$.
(b) $f \circ 1_A = f$.

Si f es una correspondencia uno a uno entre A y B, entonces

(c) $f^{-1} \circ f = 1_A$.
(d) $f \circ f^{-1} = 1_B$.

Demostración: (a) $(1_B \circ f)(a) = 1_B(f(a)) = f(a)$, para todas las a del Dom(f). En consecuencia, por el teorema 2 de la sección 4.2, $1_B \circ f = f$.

(b) $(f \circ 1_A)(a) = f(1_A(a)) = f(a)$, para todas las a del Dom(f), de modo que $f \circ 1_A = f$.

Supóngase ahora que f es una correspondencia uno a uno entre A y B. Como señalamos antes, la ecuación $b = f(a)$ es equivalente a la ecuación $a = f^{-1}(b)$. Puesto que f y f^{-1} están definidas en todas partes y son sobre, esto significa que para todas las a en A y las b en B, $f(f^{-1}(b)) = b$ y $f^{-1}(f(a)) = a$. Entonces

(c) Para todas las a en A, $1_A(a) = a = f^{-1}(f(a)) = (f^{-1} \circ f)(a)$. En consecuencia $1_A = f^{-1} \circ f$.

(d) Para todas las b en B, $1_B(b) = b = f(f^{-1}(b)) = (f \circ f^{-1})(b)$. En consecuencia $1_B = f \circ f^{-1}$. ●

Teorema 3. (a) *Sean $f: A \to B$ y $g: B \to A$ funciones tales que $g \circ f = 1_A$ y $f \circ g = 1_B$. Entonces f es una correspondencia uno a uno entre A y B, g es una correspondencia uno a uno entre B y A, y cada una es la inversa de la otra.*

(b) *Sean $f: A \to B$ y $g: B \to C$ invertibles. Entonces $g \circ f$ es invertible, y $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Demostración: (a) Las suposiciones significan que

$$g(f(a)) = a \quad \text{y} \quad f(g(b)) = b, \quad \text{para todas las } a \text{ en } A \text{ y las } b \text{ en } B$$

Esto demuestra en particular que Ran(f) $= B$ y Ran(g) $= A$, de modo que cada función es sobre. Si $f(a_1) = f(a_2)$, entonces $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. En consecuencia, f es uno a uno. De modo semejante, se observa que g es uno a uno, por lo que ambas, f y g son invertibles. Nótese que f^{-1} está definida en todas partes puesto que Dom(f^{-1}) $=$ Ran(f) $= B$. Ahora, si b es cualquier elemento de B,

$$f^{-1}(b) = f^{-1}(f(g(b)) = (f^{-1} \circ f)(g(b)) = 1_A(g(b)) = g(b).$$

En consecuencia $g = f^{-1}$, de modo que también $f = (f^{-1})^{-1} = g^{-1}$. Entonces, como g y f son sobre, f^{-1} y g^{-1} son sobre, y por tanto f y g deben estar definidas en todas partes. Esto demuestra todas las partes de la parte a.

(b) Se sabe que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, puesto que esto es cierto para cualquier relación. Como g^{-1} y f^{-1} son funciones por suposición, también lo es su composición, y entonces $(g \circ f)^{-1}$ es una función. En consecuencia, $g \circ f$ es invertible. ●

Ejemplo 17. Sea $A = B = \mathbb{R}$, el conjunto de los números reales. Supóngase que $f: A \to B$ está expresada por la fórmula

$$f(x) = 2x^3 - 1$$

y supóngase que $g: B \to A$ está expresada por

$$g(y) = \sqrt[3]{\frac{1}{2}y + \frac{1}{2}}.$$

Demuestre que f es una biyección entre A y B, y que g es una biyección entre B y A.

Solución: Sean $x \in A$ y $y = f(x) = 2x^3 - 1$. Entonces $\frac{1}{2}(y + 1) = x^3$; por lo tanto, $x = \sqrt[3]{\frac{1}{2}y + \frac{1}{2}} = g(y) = g(f(x)) = (g \circ f)(x)$. En consecuencia $g \circ f = 1_A$. De modo semejante, $f \circ g = 1_B$, de manera que por el teorema 3(a), ambas, f y g, son biyecciones. ◆

Como lo muestra el ejemplo 17, con frecuencia es más fácil demostrar que una función, tal como f, es uno a uno y sobre construyendo una inversa en vez de proceder directamente.

Por último, se analiza brevemente algunos resultados especiales que son válidos cuando A y B son conjuntos finitos. Sean $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_n\}$, y sea f una función de A hacia B que está definida en todas partes. Si f es uno a uno, entonces $f(a_1), f(a_2), \ldots, f(a_n)$ son n elementos distintos de B. En consecuencia, debe tenerse todo B, para que f también sea sobre. Por otra parte, si f es sobre, entonces $f(a_1), \ldots, f(a_n)$ forman todo el conjunto B, y por tanto deben ser todos diferentes. De ahí que f también es uno a uno. Se ha demostrado, por tanto, lo siguiente:

Teorema 4. *Sean A y B dos conjuntos finitos con el mismo número de elementos, y sea $f: A \to B$ una función definida en todas partes.*

(a) *Si f es uno a uno, entonces f es sobre.*
(b) *Si f es sobre, entonces f es uno a uno.* ●

En consecuencia, para conjuntos finitos A y B con el mismo número de elementos, y particularmente si $A = B$, sólo se necesita demostrar que una función es uno a uno *o que es* sobre para demostrar que es una biyección.

GRUPO DE EJERCICIOS 5.1

1. Sean $A = \{a, b, c, d\}$ y $B = \{1, 2, 3\}$. Determine si la relación R de A a B es una función. Si es una función, dé su rango.
   (a) $R = \{(a, 1), (b, 2), (c, 1), (d, 2)\}$
   (b) $R = \{(a, 1), (b, 2), (a, 2), (c, 1), (d, 2)\}$
   (c) $R = \{(a, 3), (b, 2), (c, 1)\}$
   (d) $R = \{(a, 1), (b, 1), (c, 1), (d, 1)\}$

2. Determine si la relación R de A a B es una función.
   (a) A = el conjunto de todos los beneficiarios de Medicare en los Estados Unidos, $B = \{x \mid x$ es un número de nueve dígitos$\}$, $a\,R\,b$ si b es el número del Seguro Social de a.
   (b) A = un conjunto de personas de los Estados

Unidos, $B = \{x \mid x$ es un número de nueve dígitos$\}$, $a\,R\,b$ si b es el número de pasaporte de a.

En los ejercicios 3 al 6, verifique que la fórmula da una función de A a B.

3. $A = B = Z; f(a) = a^2$

4. $A = B = \mathbb{R}; f(a) = e^a$

5. $A = \mathbb{R}$, $B = \{0, 1\}$; sea Z el conjunto de los enteros y obsérvese que $Z \subseteq \mathbb{R}$. Entonces, para cualquier número real a, supóngase que

$$f(a) = \begin{cases} 0 & \text{si } a \notin Z \\ 1 & \text{si } a \in Z \end{cases}$$

6. $A = \mathbb{R}$, $B = Z$; $f(a)$ = el entero más grande menor que o igual a a.

7. Sea $A = B = C = \mathbb{R}$, y supóngase que $f : A \to B$, $g : B \to C$ están definidas por $f(a) = a - 1$ y $g(b) = b^2$. Determine
   (a) $(f \circ g)(2)$ (b) $(g \circ f)(2)$
   (c) $(g \circ f)(x)$ (d) $(f \circ g)(x)$
   (e) $(f \circ f)(y)$ (f) $(g \circ g)(y)$

8. Sea $A = B = C = \mathbb{R}$, y supóngase que $f : A \to B$, $g : B \to C$ están definidas por $f(a) = a + 1$ y $g(b) = b^2 + 2$. Determine
   (a) $(g \circ f)(-2)$ (b) $(f \circ g)(-2)$
   (c) $(g \circ f)(x)$ (d) $(f \circ g)(x)$
   (e) $(f \circ f)(y)$ (f) $(g \circ g)(y)$

9. En cada parte se da los conjuntos A y B y una función de A a B. Determine si la función es uno a uno o sobre (o ambas cosas o ninguna).
   (a) $A = \{1, 2, 3, 4\} = B$;
   $f = \{(1, 1), (2, 3), (3, 4), (4, 2)\}$
   (b) $A = \{1, 2, 3\}$; $B = \{a, b, c, d\}$;
   $f = \{(1, a), (2, a), (3, c)\}$
   (c) $A = \left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}\right\}$; $B = \{x, y, z, w\}$;
   $f = \left\{\left(\frac{1}{2}, x\right), \left(\frac{1}{4}, y\right), \left(\frac{1}{3}, w\right)\right\}$
   (d) $A = \{1.1, 7, 0.06\}$; $B = \{p, q\}$;
   $f = \{(1.1, p), (7, q), (0.06, p)\}$
   (e) $A = B = Z$; $f(a) = a - 1$

10. Sea f una función de A a B. Determine si cada función f es uno a uno y si es sobre.
   (a) $A = \mathbb{R}$, $B = \{x \mid x$ es real y $x \geq 0\}$; $f(a) = |a|$
   (b) $A = \mathbb{R} \times \mathbb{R}$, $B = \mathbb{R}$; $f((a, b)) = a$
   (c) Sea $S = \{1, 2, 3\}$, $T = \{a, b\}$. Sean $A = B = S \times T$ y supóngase que f está definida por $f(n, a) = (n, b)$, $n = 1, 2, 3$, y $f(n, b) = (1, a)$, $n = 1, 2, 3$.
   (d) $A = B = \mathbb{R} \times \mathbb{R}$; $f((a, b)) = (a + b, a - b)$
   (e) $A = \mathbb{R}$, $B = \{x \mid x$ es real y $x \geq 0\}$; $f(a) = a^2$

11. Sean $f : A \to B$ y $g : B \to A$. Verifique si $g = f^{-1}$.
   (a) $A = B = \mathbb{R}$; $f(a) = \frac{a+1}{2}$, $g(b) = 2b - 1$
   (b) $A = \{x \mid x$ es real y $x \geq 0\}$; $B = \{y \mid y$ es real y $y \geq -1\}$; $f(a) = a^2 - 1$, $g(b) = \sqrt{b+1}$
   (c) $A = B = P(S)$, en donde S es un conjunto. Si $X \in P(S)$, sea $f(X) = \overline{X} = g(X)$.
   (d) $A = B = \{1, 2, 3, 4\}$; $f = \{(1, 4), (2, 1), (3, 2), (4, 3)\}$; $g = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$

12. Sea f una función de A a B. Encuentre f^{-1}.
   (a) $A = \{x \mid x$ es real y $x \geq -1\}$; $B = \{x \mid x$ es real y $x \geq 0\}$; $f(a) = \sqrt{a+1}$
   (b) $A = B = \mathbb{R}$; $f(a) = a^3 + 1$
   (c) $A = B = \mathbb{R}$; $f(a) = \frac{2a-1}{3}$
   (d) $A = B = \{1, 2, 3, 4, 5\}$;
   $f = \{(1, 3), (2, 2), (3, 4), (4, 5), (5, 1)\}$

En los ejercicios 13 y 14, sea f una función de $A = \{1, 2, 3, 4\}$ hacia $B = \{a, b, c, d\}$. Determine si f^{-1} es una función.

13. $f = \{(1, a), (2, a), (3, c), (4, d)\}$

14. $f = \{(1, a), (2, c), (3, b), (4, d)\}$

15. Sea $A = B = C = \mathbb{R}$ y considérese las funciones $f : A \to B$ y $g : B \to C$ definidas por $f(a) = 2a + 1$, $g(b) = b/3$. Verifique el teorema 3(b): $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

16. Si un conjunto A tiene n elementos ¿cuántas funciones hay de A a A?

17. Si un conjunto A tiene n elementos ¿cuántas biyecciones hay de A a A?

18. Si A tiene m elementos y B n elementos ¿cuántas funciones hay de A a B?

19. Demuestre que si $f : A \to B$ y $g : B \to C$ son funciones uno a uno, entonces $g \circ f$ es uno a uno.

20. Demuestre que si $f : A \to B$ y $g : B \to C$ son funciones sobre, entonces $g \circ f$ es sobre.

21. Sean $f : A \to B$ y $g : B \to C$ funciones. Demuestre que si $g \circ f$ es uno a uno, entonces f es uno a uno.

22. Sean $f : A \to B$ y $g : B \to C$ funciones. Demuestre que si $g \circ f$ es sobre, entonces g es sobre.

23. Sea A un conjunto, y sea $f : A \to A$ una biyección. Para cualquier entero $k \geq 1$, sea $f^k = f \circ f \circ \cdots \circ f$ (k factores), y sea $f^{-k} = f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}$ (k factores). Defina f^0 como 1_A. Entonces f^n está definida para todas las $n \in Z$. Para cualquier $a \in A$, sea $O(a, f) = \{f^n(a) \mid n \in Z\}$. Demuestre que si $a_1, a_2 \in A$, y $O(a_1, f) \cap O(a_2, f) \neq \varnothing$, entonces $O(a_1, f) = O(a_2, f)$.

24. Sea $f : A \to B$ una función con dominio y rango finitos. Supóngase que $|\mathrm{Dom}(f)| = n$ y $|\mathrm{Ran}(f)| = m$. Demuestre que:
   (a) Si f es uno a uno, entonces $m = n$.
   (b) Si f no es uno a uno, entonces $m < n$.

25. Sean $|A| = |B| = n$ y sea $f : A \to B$ una función definida en todas partes. Demuestre que los tres enunciados siguientes son equivalentes:
   (a) f es uno a uno.
   (b) f es sobre.
   (c) f es una correspondencia biunívoca (es decir, f es uno a uno y sobre).

5.2. Funciones para la ciencia de la computación

En capítulos anteriores, se ha visto, de manera algo informal, algunas funciones empleadas comúnmente en las aplicaciones de la ciencia de la computación. En esta sección se revisa éstas y se define algunas más.

Ejemplo 1. Sea A un subconjunto del conjunto universal $U = \{u_1, u_2, u_3, \ldots, u_n\}$. La **función característica de A** se define como una función de U hacia $\{0, 1\}$ por lo siguiente:

$$f_A(u_i) = \begin{cases} 1 & \text{si } u_i \in A \\ 0 & \text{si } u_i \notin A \end{cases}$$

Si $A = \{4, 7, 9\}$ y $U = \{1, 2, 3, \ldots, 10\}$, entonces $f_A(2) = 0$, $f_A(4) = 1$, $f_A(7) = 1$, y $f_A(12)$ está indefinida. Es fácil verificar si f_A está definida en todas partes y es sobre, pero no es uno a uno. ◆

Ejemplo 2. En la sección 1.4 se definió una familia de funciones mód (módulo), una por cada entero positivo n. Cada [illegible] es una función que va de los enteros no negativos al conjunto $\{0, 1, 2, 3, \ldots, n - 1\}$. Para una n fija, cualquier entero no negativo z puede escribirse como [illegible]. Entonces [illegible]. También puede expresarse esta relación como $z \equiv r(\text{mód } n)$. Cada miembro de la familia de funciones módulo está definido en todas partes y sobre, pero no uno a uno. ◆

Ejemplo 3. Sea A el conjunto de enteros no negativos, $B = Z^+$, y supóngase que $f : A \to B$ está definida por $f(n) = n!$. ◆

Ejemplo 4. Para la versión general del principio de las casillas (sección 3.3) se requiere la **función piso**, que se define para los números racionales como $f(q)$ es el entero más grande menor que o igual a q. De nuevo se tiene aquí un ejemplo de una función que no se define por medio de una fórmula. Así

$$f(1.5) = \lfloor 1.5 \rfloor = 1, \qquad f(-3) = \lfloor -3 \rfloor = -3.$$ ◆

Ejemplo 5. Una función similar a la del ejemplo 4 es la **función techo**, que se define para los números racionales como $c(q)$, es el entero más pequeño mayor que o igual a q. También se emplea la notación $\lceil q \rceil$ para $c(q)$. Así

$$c(1.5) = \lceil 1.5 \rceil = 2, \qquad c(-3) = \lceil -3 \rceil = -3.$$ ◆

Hay muchas funciones algebraicas comunes empleadas en la ciencia de la computación, con frecuencia con dominios restringidos a subconjuntos de los enteros.

Ejemplo 6

(a) Cualquier polinomio con coeficientes enteros, p, puede usarse para definir una función en Z como sigue: Si $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ y $z \in Z$, entonces $f(z)$ es el valor de p evaluado en z.

(b) Sea $A = B = Z^+$ y supóngase que $f: A \to B$ está definida por $f(z) = 2^z$. Se llama a f **función exponencial de base 2**. Puede usarse otras bases para definir funciones similares.

(c) Sea $A = B =$ [illegible] y supóngase que $f_n: A \to B$ está definida para cada entero positivo $n > 1$ como $f_n(x) = \log_n(x)$, el logaritmo de base n de x. En las aplicaciones de la ciencia de la computación, son útiles en particular las bases 2 y 10. ◆

En general, las operaciones unarias analizadas en secciones anteriores pueden ser usadas para crear funciones similares a la función del ejemplo 3. Los conjuntos A y B de la definición de función, no necesitan ser conjuntos de números, como se verá en los ejemplos siguientes.

Ejemplo 7

(a) Sea A un conjunto finito y defina a $l: A^* \to Z$ como $l(w)$ como la longitud de la cadena w (véase la sección 1.3 para la definición de A^* y de las cadenas).

(b) Sea B un subconjunto finito del conjunto universal U y defina $pow(B)$ como el conjunto potencia de B. Entonces pow es una función que va de V, el conjunto potencia de U, hacia el conjunto potencia de V.

(c) Sea $A = B =$ el conjunto de todas las matrices 2×2 con entradas de números reales y sea $t(\mathbf{M}) = \mathbf{M}^T$, la transpuesta de $\mathbf{M}$. Entonces t está definida en todas partes, es sobre y uno a uno. ◆

Las operaciones binarias también pueden ser usadas para definir funciones. En este caso, las funciones definidas tendrán pares ordenados como entrada

Ejemplo 8

(a) Para los elementos de $Z^+ \times Z^+$, defina $g(z_1, z_2)$ como el $\text{MCD}(z_1, z_2)$. Entonces g es una función de $Z^+ \times Z^+$ a Z^+. El MCD de dos números se define en la sección 1.4.

(b) De manera similar puede definirse $m(z_1, z_2)$ como el $\text{MCM}(z_1, z_2)$. ◆

Otro tipo de función, una función booleana, juega un papel clave en casi todos los programas de computadora. Sea $B = \{\text{verdadero, falso}\}$. Entonces una función que va de un conjunto A a B se denomina **función booleana**. Los predicados de la sección 2.1 son ejemplos de funciones booleanas.

Ejemplo 9. Sea $P(x)$: x es par y $Q(y)$: y es impar. Entonces $P(4)$ es verdadero y $Q(4)$ es falso. El predicado $R(x, y)$: x es par o y es impar es una función booleana con dos variables. Aquí $R(3, 4)$ es falsa y $R(6, 4)$ es verdadera. ◆

Funciones de Hashing

En la sección 4.6 se presentó dos métodos de almacenamiento de los datos para una relación o digrafo en una computadora. En este caso se consideró un problema más general de almacenamiento de datos. Supóngase que hay que almacenar y más adelante examinar un gran número de registros de datos, por ejemplo, cuentas de clientes. En general, no se sabe cuántos registros se tiene que almacenar en un tiempo dado. Esto sugiere que es apropiado el almacenamiento de lista enlazada, porque el espacio de almacenamiento sólo se emplea cuando se le asigna un registro y no hay espacio de almacenamiento ocioso. Para examinar un registro, hay que poder encontrarlo; por esto, almacenar los datos en una sola lista enlazada no es práctico porque la búsqueda de un elemento puede tomar mucho tiempo (hablando en términos relativos). Una técnica para manejar tales problemas de almacenamiento es crear un número de listas enlazadas y definir un método para decidir a cuál lista ha de enlazarse un nuevo elemento. Este método determinará también en cuál lista ha de buscarse algún elemento deseado. Un punto clave es intentar asignar un elemento a una de las listas al azar. (Se recordará, según se vio en la sección 3.4, que esto significa que cada lista tendrá igual probabilidad de ser seleccionada.) Esto es, hacer las listas toscamente del mismo tamaño con lo que se invertirá, aproximadamente, el mismo tiempo de búsqueda para cualquier elemento.

Supóngase que se debe guardar en memoria los registros de los clientes para una compañía grande y que se va a guardar la información como registros de computadora. En primer lugar, se asigna a cada cliente un número de cuenta único de 7 dígitos. Un identificador único de un registro se llama **clave**. Por ahora no se considerará exactamente cómo y qué información va a almacenarse para cada cuenta de cliente, sólo se describirá el almacenamiento de un lugar o posición en la memoria de la computadora en donde habrá de encontrarse esta información. Para determinar a qué lista debe asignarse un registro en particular, se crea una **función de hashing** del conjunto de claves al conjunto de los números de la lista. Las funciones de hashing con frecuencia utilizan una función módulo, como se ilustra en el ejemplo siguiente.

Ejemplo 10. Supóngase que (aproximadamente) tiene que almacenarse y procesarse 10,000 registros de cuentas de clientes. La computadora de la compañía tiene capacidad para buscar en una lista de 100 elementos en un lapso aceptable. Se decide crear 101 listas enlazadas para almacenamiento, porque si la función de hashing funciona bien en la asignación "aleatoria" de registros a las listas, se esperaría ver alrededor de 100 registros por lista. Se define una función de hashing del conjunto de números de cuenta de 7 dígitos al conjunto $\{0, 1, 2, \ldots, 100\}$ como sigue

$$h(n) = n(\text{mód } 101)$$

En consecuencia

$$h(2473871) = 2473871(\text{mód } 101)$$
$$= 78.$$

Esto significa que el registro con número de cuenta 2473871 será asignado a la lista 78. Nótese que el rango de h es el conjunto $\{0, 1, 2, \ldots, 100\}$. ◆

Debido a que la función h del ejemplo 10 no es uno a uno, puede asignarse diferentes números de cuenta a la misma lista por la función de hashing. Si la primera posición de la lista 78 ya está ocupada cuando se va a almacenar el registro de clave 2473871, se dice que ha ocurrido una colisión. Hay muchos métodos para resolver las colisiones. Uno muy simple, que será suficiente para este trabajo, consiste en insertar el nuevo registro al final de la lista existente. Usando este método, cuando se desea encontrar un registro, se mezclará su clave y se hará la búsqueda en la lista h (clave) en sucesión.

Muchas otras funciones de hashing son adecuadas para esta situación. Por ejemplo, se puede descomponer el número de cuenta de 7 dígitos en un número de 3 dígitos y otro de 4, sumar ambos, y luego aplicar la función mód 101. Hay muchos factores por considerar además del número de registros por almacenar; la velocidad con que puede hacerse la búsqueda en una lista de longitud media, y el tiempo necesario para calcular el número de lista para una cuenta, son dos factores posibles para ser tomados en cuenta. Por razones que no se analizará en este momento, el módulo que se emplea en la función mód debe ser primo. La determinación de una buena función de hashing para una aplicación en particular es una tarea desafiante.

GRUPO DE EJERCICIOS 5.2

1. Sea f la función mód 10. Calcule
(a) $f(417)$ (b) $f(38)$ (c) $f(253)$

2. Sea f la función mód 7. Calcule
(a) $f(81)$ (b) $f(316)$ (c) $f(1057)$

En los ejercicios 3 y 4, use el conjunto universal $U = \{a, b, c, \ldots, y, z\}$ y la función característica para el subconjunto para calcular los valores de la función solicitada.

3. $A = \{a, e, i, o, u\}$ (a) $f_A(i)$ (b) $f_A(y)$
(c) $f_A(o)$

4. $B = \{m, n, o, p, q, r, z\}$ (a) $f_B(a)$
(b) $f_B(m)$ (c) $f_B(s)$

5. Calcule cada uno de los siguientes:
(a) $\lfloor 2.78 \rfloor$ (b) $\lfloor -2.78 \rfloor$ (c) $\lfloor 14 \rfloor$
(d) $\lfloor -17.3 \rfloor$ (e) $\lfloor 21.5 \rfloor$

6. Calcule cada uno de los siguientes:
(a) $\lceil 2.78 \rceil$ (b) $\lceil -2.78 \rceil$ (c) $\lceil 14 \rceil$
(d) $\lceil -17.3 \rceil$ (e) $\lceil 21.5 \rceil$

En los ejercicios 7 y 8, calcule los valores indicados. Observe que si el dominio de estas funciones es Z^+, entonces cada función es la fórmula explícita para una sucesión infinita. Estas sucesiones pueden ser consideradas como un tipo especial de función.

7. $f(n) = 3n^2 - 1$ (a) $f(3)$ (b) $f(17)$
(c) $f(5)$ (d) $f(12)$

8. $g(n) = 5 - 2n$ (a) $g(4)$ (b) $g(14)$
(c) $g(129)$ (d) $g(23)$

9. Sea $f_2(n) = 2^n$. Calcule cada uno de los siguientes:
(a) $f_2(1)$ (b) $f_2(3)$ (c) $f_2(5)$ (d) $f_2(10)$

10. Sea $f_3(n) = 3^n$. Calcule cada uno de los siguientes:
(a) [illegible] (b) $f_3(5)$ (c) $f_3(6)$ (d) $f_3(8)$

En los ejercicios 11 y 12, sea $lg(x) = \log_2(x)$.

11. Calcule cada uno de los siguientes:
(a) $lg(16)$ (b) $lg(128)$ (c) $lg(512)$
(d) $lg(1024)$

12. Para cada uno de los siguientes, encuentre el entero más grande menor que o igual al valor de la función, y el entero más pequeño mayor que o igual al valor de la función.
(a) $lg(10)$ (b) $lg(25)$ (c) $lg(50)$
(d) $lg(100)$ (e) $lg(256)$

13. Demuestre que la función t del ejemplo 7(c) que mapea el conjunto de matrices 5×5 a sí mismo está definida en todas partes, es sobre y uno a uno.

14. Sea $A = \{a, b, c, d\}$. Para la función l del ejemplo 7(a).
(a) Demuestre que l está definida en todas partes.
(b) Demuestre que l no es uno a uno.
(c) Demuestre o refute que l sea sobre.

15. Sea A un conjunto con n elementos, S el conjunto de las relaciones en A, y M el conjunto de las matrices booleanas $n \times n$. Defina $f: S \to M$ por $f(R) = \mathbf{M}_R$. Demuestre que f es una biyección entre S y M.

16. Sea P la función proposicional definida por $P(x, y) = (x \vee y) \wedge \sim y$. Evalúe cada uno de los siguientes casos:
(a) P (verdadera, verdadera)
(b) P (falsa, verdadera)
(c) P (verdadera, falsa)

17. Sea Q la función proposicional definida por $Q(x)$: $\exists (y \in Z^+)\ (xy = 60)$. Evalúe cada uno de los siguientes casos.
(a) $Q(3)$ (b) $Q(7)$ (c) $Q(-6)$
(d) $Q(15)$

En los ejercicios 18 a 20, utilice la función de hashing h, la cual toma los primeros tres dígitos del número de cuenta como un número y los últimos cuatro dígitos como otro número, los suma, y luego aplica la función mód 59.

18. Suponga que hay 7500 registros de clientes por almacenar utilizando esta función de hashing.
(a) ¿Cuántas listas enlazadas se requerirá para el almacenamiento de estos registros?
(b) Si se logra una distribución aproximadamente uniforme, más o menos ¿cuántos registros se almacenará por cada lista enlazada?

19. Determine a cuál lista debe agregarse la cuenta de cliente dada.
(a) 3759273 (b) 7149021 (c) 5167249

20. Determine en cuál lista habrá que buscar para encontrar la cuenta de cliente dada.
(a) 2561384 (b) 6082376 (c) 4984620

5.3. Funciones de permutación

En esta sección se estudia las biyecciones de un conjunto A a sí mismo. De importancia especial es el caso en que A es finito. Las biyecciones en un conjunto finito tienen una amplia variedad de aplicaciones en las matemáticas, ciencia de la computación y física.

Una biyección de un conjunto A a sí mismo se denomina **permutación** de A.

Ejemplo 1. Sea $A =$ y supóngase que $f: A \to A$ está definida por $f(a) = 2a + 1$. Puesto que f es uno a uno y sobre (verifique), resulta que f es una permutación de A. ◆

Si $A = \{a_1, a_2, \ldots, a_n\}$ es un conjunto finito y p es una biyección en A, se enlista los elementos de A y los valores correspondientes de la función $p(a_1), p(a_2), \ldots, p(a_n)$ en la siguiente forma

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}. \qquad (1)$$

Debe observarse que (1) describe completamente a p puesto que da el valor de p para cada elemento de A. A menudo se escribe

$$p = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}.$$

Así, si p es una permutación de un conjunto finito $A = \{a_1, a_2, \ldots, a_n\}$, entonces la secuencia $p(a_1), p(a_2), \ldots, p(a_n)$ es sólo un reacomodo de los elementos de A y por tanto corresponde exactamente a una permutación de A en el sentido de lo mostrado en la sección 3.1.

Ejemplo 2. Sea $A = \{1, 2, 3\}$. Entonces todas las permutaciones de A son

$$1_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \quad \blacklozenge$$

Ejemplo 3. Utilizando las permutaciones del ejemplo 2, calcule (a) p_4^{-1}; (b) $p_3 \circ p_2$.

Solución: (a) Considerando a p_4 como una función, se tiene

$$p_4 = \{(1, 3), (2, 1), (3, 2)\}.$$

Entonces

$$p_4^{-1} = \{(3, 1), (1, 2), (2, 3)\}$$

o bien, cuando se escribe en orden creciente del primer componente de cada par ordenado, se tiene

$$p_4^{-1} = \{(1, 2), (2, 3), (3, 1)\}.$$

En consecuencia

$$p_4^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = p_3.$$

(b) La función p_2 envía 1 a 2 y p_3 envía 2 a 3, de modo que $p_3 \circ p_2$ envía 1 a 3. También, p_2 envía 2 a 1 y p_3 envía 1 a 2, de modo que $p_3 \circ p_2$ envía 2 a 2. Finalmente p_2 envía 3 a 3 y p_3 envía 3 a 1, de modo que $p_3 \circ p_2$ envía 3 a 1. En consecuencia

$$p_3 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Puede verse el proceso de formar $p_3 \circ p_2$ como se muestra en la figura 5.4. Observe que $p_3 \circ p_2 = p_5$. $\blacklozenge$

La composición de dos permutaciones es otra permutación, a la que generalmente se hace referencia como el **producto** de estas permutaciones. En el resto de este capítulo, se seguirá conforme esta convención.

Teorema 1. *Si $A = \{a_1, a_2, \ldots, a_n\}$ es un conjunto que contiene n elementos, entonces hay $n! = n \cdot (n-1) \cdots 2 \cdot 1$ permutaciones de A.*

Demostración: Este resultado es consecuencia del teorema 4 de la sección 3.1 haciendo $r = n$.

$$p_3 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Figura 5.4

Sean $b_1, b_2, \ldots, b_r$ r elementos distintos del conjunto $A = \{a_1, a_2, \ldots, a_n\}$. La permutación $p : A \to A$ definida por

$$\begin{aligned} p(b_1) &= b_2 \\ p(b_2) &= b_3 \\ &\vdots \\ p(b_{r-1}) &= b_r \\ p(b_r) &= b_1 \\ p(x) &= x, \qquad \text{si } x \in A, \quad x \notin \{b_1, b_2, \ldots, b_r\}. \end{aligned}$$

se denomina **permutación cíclica** de longitud r, o simplemente un **ciclo** de longitud r, y se denotará por $(b_1, b_2, \ldots, b_r)$. No debe confundirse esta terminología con la que se utiliza para los ciclos en un digrafo (sección 4.3). Los dos conceptos son diferentes y en este libro se utiliza notaciones ligeramente diferentes. Si los elementos $b_1, b_2, \ldots, b_r$ están dispuestos de manera uniforme en un círculo, como se ilustra en la figura 5.5, entonces un ciclo p de longitud r mueve estos elementos en el sentido de las manecillas del reloj, de modo que b_1 es enviada a b_2, b_2 a b_3, $\ldots$, b_{r-1} a b_r, y b_r a b_1. Todos los demás elementos de A son dejados fijos por p.

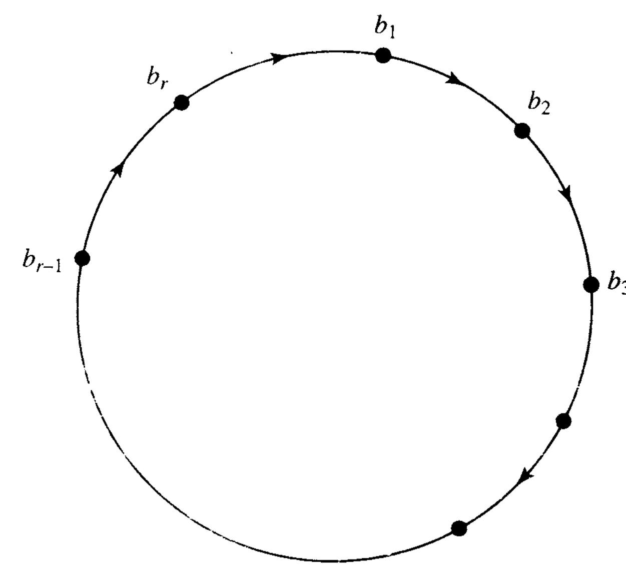


Figura 5.5

Ejemplo 4. Sea $A = \{1, 2, 3, 4, 5\}$. El ciclo $(1, 3, 5)$ denota la permutación

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

Observe que si $p = (b_1, b_2, \ldots, b_r)$ es un ciclo de longitud r, entonces se puede escribir también p comenzando con cualquier b_i, $1 \leq i \leq r$, y moviéndose en el sentido de las manecillas del reloj, como se ilustró en la figura 5.5. En consecuencia, como ciclos,

$$(3, 5, 8, 2) = (5, 8, 2, 3) = (8, 2, 3, 5) = (2, 3, 5, 8).$$

Nótese también que la notación para un ciclo no indica el número de elementos que hay en el conjunto A. En consecuencia, el ciclo $(3, 2, 1, 4)$ podría ser una permutación del conjunto $\{1, 2, 3, 4\}$ o de $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Es necesario que se diga explícitamente el conjunto en el cual se define un ciclo. Se desprende de la definición, que un ciclo en un conjunto A es de longitud 1 si y sólo si es la permutación identidad, 1_A.

Puesto que los ciclos son permutaciones, se puede formar su producto. Sin embargo, como se demuestra en el ejemplo siguiente, el producto de dos ciclos no necesita ser un ciclo.

Ejemplo 5. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Calcule $(4, 1, 3, 5) \circ (5, 6, 3)$ y $(5, 6, 3) \circ (4, 1, 3, 5)$.

Solución: Se tiene

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

y

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

Entonces

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

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

y

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

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

Observe que

$$(4, 1, 3, 5) \circ (5, 6, 3) \neq (5, 6, 3) \circ (4, 1, 3, 5)$$

y que ninguno de los productos es un ciclo. ◆

Se dice que dos ciclos de un conjunto A son **disjuntos** si ningún elemento de A aparece en ambos ciclos.

Ejemplo 6. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Entonces los ciclos $(1, 2, 5)$ y $(3, 4, 6)$ son disjuntos, mientras que los ciclos $(1, 2, 5)$ y $(2, 4, 6)$ no lo son. ◆

No es difícil demostrar que si $p_1 = (a_1, a_2, \ldots, a_r)$ y $p_2 = (b_1, b_2, \ldots, b_s)$ son ciclos disjuntos de A, entonces $p_1 \circ p_2 = p_2 \circ p_1$. Esto puede verse si se observa que p_1 afecta sólo a las a, mientras que p_2 afecta sólo a las b.

Obsérvese ahora un teorema fundamental y, en lugar de ofrecer su demostración, se proporcionará un ejemplo a manera de demostración.

Teorema 2. *Una permutación de un conjunto finito que no sea la identidad o un ciclo, puede escribirse como un producto de ciclos disjuntos de longitud* ≥ 2. ●

Ejemplo 7. Escriba la permutación

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

del conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ como producto de ciclos disjuntos.

Solución: Se comenzará con 1 y se encuentra que $p(1) = 3$, $p(3) = 6$, y $p(6) = 1$, de manera que se tiene el ciclo $(1, 3, 6)$. Enseguida se escoge el primer elemento de A que no ha aparecido en un ciclo previo. Se escoge 2, y se tiene $p(2) = 4$, $p(4) = 5$, y $p(5) = 2$, y así, se obtiene el ciclo $(2, 4, 5)$. Ahora se escoge 7, el primer elemento de A que no haya aparecido en un ciclo anterior. Puesto que $p(7) = 8$ y $p(8) = 7$, se obtiene el ciclo $(7, 8)$. Entonces, puede escribirse p como un producto de ciclos disjuntos como

$$p = (7, 8) \circ (2, 4, 5) \circ (1, 3, 6).$$ ◆

No es difícil demostrar que en el teorema 2, cuando se escribe una permutación como un producto de ciclos disjuntos, el producto es único excepto por el orden de los ciclos.

Permutaciones pares e impares

A un ciclo de longitud 2 se lo llama **transposición**. Es decir, una transpuesta es un ciclo $p = (a_i, a_j)$, en donde $p(a_i) = a_j$ y $p(a_j) = a_i$.

Observe que si $p = (a_i, a_j)$ es una transposición de A, entonces $p \circ p = 1_A$, la permutación identidad de A.

Todo ciclo puede escribirse como un producto de transposiciones. En efecto,

$$(b_1, b_2, \ldots, b_r) = (b_1, b_r) \circ (b_1, b_{r-1}) \circ \cdots \circ (b_1, b_3) \circ (b_1, b_2).$$

Esto puede verificarse por inducción en r, de la siguiente manera:

Paso base. Si $r = 2$, entonces el ciclo es sólo (b_1, b_2), el cual ya tiene la forma correcta.

PASO DE INDUCCIÓN. Si el resultado es cierto para k, sea $(b_1, b_2, \ldots, b_k, b_{k+1})$ un ciclo de longitud $k+1$. Entonces $(b_1, b_2, \ldots, b_k, b_{k+1}) = (b_1, b_{k+1}) \circ (b_1, b_2, \ldots, b_k)$, como puede verificarse al calcular la composición. Por la hipótesis de inducción, $(b_1, b_2, \ldots, b_k) = (b_1, b_k) \circ (b_1, b_{k-1}) \circ \cdots \circ (b_1, b_2)$. Al sustituir, $(b_1, b_2, \ldots, b_k, b_{k+1}) = (b_1, b_{k+1}) \circ (b_1, b_k) \circ \cdots \circ (b_1, b_3) \circ (b_1, b_2)$. Esto completa el paso de inducción. Así, por el principio de inducción matemática, el resultado es válido para todo ciclo. Por ejemplo,

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

Se obtiene el siguiente corolario del teorema 2.

Corolario 1. *Toda permutación de un conjunto finito con al menos dos elementos se puede escribir como un producto de transposiciones.* ●

Observe que las transposiciones del corolario 1 no tienen que ser disjuntas.

Ejemplo 8. Escriba la permutación p del ejemplo 7 como producto de transposiciones.

Solución: Se tiene

$$p = (7, 8) \circ (2, 4, 5) \circ (1, 3, 6).$$

Como se puede escribir

$$(1, 3, 6) = (1, 6) \circ (1, 3)$$
$$(2, 4, 5) = (2, 5) \circ (2, 4),$$

se tiene

$$p = (7, 8) \circ (2, 5) \circ (2, 4) \circ (1, 6) \circ (1, 3).$$ ◆

Se ha observado que todo ciclo se puede escribir como producto de transposiciones. Sin embargo, puede hacerse esto de diversas formas. Por ejemplo,

$$\begin{aligned}(1, 2, 3) &= (1, 3) \circ (1, 2)\\ &= (2, 1) \circ (2, 3)\\ &= (1, 3) \circ (3, 1) \circ (1, 3) \circ (1, 2) \circ (3, 2) \circ (2, 3).\end{aligned}$$

Esto implica que puede escribirse toda permutación sobre un conjunto de dos o más elementos como producto de transposiciones de diversas formas. Sin embargo, el siguiente teorema, cuya comprobación se omitirá, ordena esta situación.

Teorema 3. *Si se puede escribir una permutación de un conjunto finito como producto de un número par de transposiciones, entonces nunca puede ser escrita como producto de un número impar de transposiciones, y viceversa.* ●

Una permutación de un conjunto finito es **par** si puede ser escrita como producto de un número par de transposiciones, y es **impar** si puede ser escrita como producto de un número impar de transposiciones.

Ejemplo 9. ¿La siguiente permutación

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

es par o impar?

Solución: Primero se escribe p como un producto de ciclos disjuntos, y se obtiene

$$p = (3, 5, 6) \circ (1, 2, 4, 7).$$

A continuación, se escribe cada uno de los ciclos como producto de transposiciones:

$$(1, 2, 4, 7) = (1, 7) \circ (1, 4) \circ (1, 2)$$
$$(3, 5, 6) = (3, 6) \circ (3, 5).$$

Entonces

$$p = (3, 6) \circ (3, 5) \circ (1, 7) \circ (1, 4) \circ (1, 2).$$

Como p es producto de un número impar de transposiciones, es una permutación impar. ◆

De acuerdo con la definición de permutaciones pares e impares, se tiene que (ejercicio 14)

(a) El producto de dos permutaciones pares es par.
(b) El producto de dos permutaciones impares es par.
(c) El producto de una permutación par y una impar es impar.

Teorema 4. *Sea $A = \{a_1, a_2, \ldots, a_n\}$ un conjunto finito con n elementos, $n \geq 2$. Entonces existen $n!/2$ permutaciones pares y $n!/2$ permutaciones impares.*

Demostración: Sea A_n el conjunto de permutaciones pares de A, y sea B_n el conjunto de permutaciones impares. Se definirá una función $f\colon A_n \to B_n$, y se mostrará que es uno a uno y sobre, por lo que A_n y B_n tendrán el mismo número de elementos.

Como $n \geq 2$, se puede elegir una transpuesta particular q_0 de A. Por decir, $q_0 = (a_{n-1}, a_n)$. Se define la función $f\colon A_n \to B_n$ como

$$f(p) = q_0 \circ p, \qquad p \in A_n.$$

Observe que si $p \in A_n$, entonces p es una permutación par, de modo que $q_0 \circ p$ es una permutación impar y por lo tanto $f(p) \in B_n$. Supóngase ahora que p_1 y p_2 están en A_n y

$$f(p_1) = f(p_2).$$

Entonces

$$q_0 \circ p_1 = q_0 \circ p_2 \tag{2}$$

Ahora se compone cada lado de la ecuación (2) con q_0:

$$q_0 \circ (q_0 \circ p_1) = q_0 \circ (q_0 \circ p_2);$$

de modo que, por la propiedad asociativa,

$$(q_0 \circ q_0) \circ p_1 = (q_0 \circ q_0) \circ p_2$$

o, como $q_0 \circ q_0 = 1_A$,

$$1_A \circ p_1 = 1_A \circ p_2$$
$$p_1 = p_2.$$

Así, f es uno a uno.

Ahora, sea $q \in B_n$. Entonces $q_0 \circ q \in A_n$, y

$$\begin{aligned} f(q_0 \circ q) &= q_0 \circ (q_0 \circ q) \\ &= (q_0 \circ q_0) \circ q \\ &= 1_A \circ q \\ &= q, \end{aligned}$$

lo que significa que f es una función sobre. Como $f\colon A_n \to B_n$ es uno a uno y sobre, se concluye que A_n y B_n tienen el mismo número de elementos. Observe que $A_n \cap B_n = \varnothing$, pues ninguna permutación puede ser par e impar a la vez. Además, por el teorema 1, $|A_n \cup B_n| = n!$. Así, por el teorema 2 de la sección 1.2,

$$n! = |A_n \cup B_n| = |A_n| + |B_n| - |A_n \cap B_n| = 2|A_n|.$$

Entonces se tiene

$$|A_n| = |B_n| = \frac{n!}{2}. \quad \bullet$$

GRUPO DE EJERCICIOS 5.3

1. ¿Cuáles de las siguientes funciones $f\colon R \to R$ son permutaciones de R?
   (a) f se define como $f(a) = a - 1$.
   (b) f se define como $f(a) = a^2$.
   (c) f se define como $f(a) = a^3$.
   (d) f se define como $f(a) = e^a$.

2. ¿Cuáles de las siguientes funciones $f\colon Z \to Z$ son permutaciones de Z?
   (a) f se define como $f(a) = a + 1$.
   (b) f se define como $f(a) = (a - 1)^2$.
   (c) f se define como $f(a) = a^2 + 1$.
   (d) f se define como $f(a) = a^3 - 3$.

En los ejercicios 3 y 4, sea $A = \{1, 2, 3, 4, 5, 6\}$ y

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

3. Calcule
   (a) p_1^{-1} (b) $p_3 \circ p_1$
   (c) $(p_2 \circ p_1) \circ p_2$ (d) $p_1 \circ (p_3 \circ p_2^{-1})$

4. Calcule
   (a) p_3^{-1} (b) $p_1^{-1} \circ p_2^{-1}$
   (c) $(p_3 \circ p_2) \circ p_1$ (d) $p_3 \circ (p_2 \circ p_1)^{-1}$

En los ejercicios 5 y 6, sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Calcule los productos.

5. (a) $(3, 5, 7, 8) \circ (1, 3, 2)$
   (b) $(2, 6) \circ (3, 5, 7, 8) \circ (2, 5, 3, 1)$

6. (a) $(1, 4) \circ (2, 4, 5, 6) \circ (1, 4, 6, 7)$
   (b) $(5, 8) \circ (1, 2, 3, 4) \circ (3, 5, 6, 7)$

7. Sea $A = \{a, b, c, d, e, f, g\}$. Calcule los productos.
   (a) $(a, f, g) \circ (b, c, d, e)$
   (b) $(f, g) \circ (b, c, f) \circ (a, b, c)$

En los ejercicios 8 y 9, sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Escriba cada permutación como el producto de ciclos disjuntos.

8. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 5 & 1 & 8 & 7 & 6 \end{pmatrix}$
   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 7 & 5 & 8 & 6 \end{pmatrix}$

9. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 7 & 8 & 4 & 3 & 2 & 1 \end{pmatrix}$
   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 6 & 7 & 8 & 5 \end{pmatrix}$

10. Sea $A = \{a, b, c, d, e, f, g\}$. Escriba cada permutación como el producto de ciclos disjuntos.
    (a) $\begin{pmatrix} a & b & c & d & e & f & g \\ g & d & b & a & c & f & e \end{pmatrix}$
    (b) $\begin{pmatrix} a & b & c & d & e & f & g \\ d & e & a & b & g & f & c \end{pmatrix}$

11. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Escriba cada permutación como producto de transposiciones.
    (a) $(2, 1, 4, 5, 8, 6)$
    (b) $(3, 1, 6) \circ (4, 8, 2, 5)$

En los ejercicios 12 y 13, sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Determine si la permutación es par o impar.

12. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 1 & 6 & 5 & 8 & 7 & 3 \end{pmatrix}$
    (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 4 & 2 & 1 & 8 & 6 & 5 \end{pmatrix}$

13. (a) $(6, 4, 2, 1, 5)$
    (b) $(4, 8) \circ (3, 5, 2, 1) \circ (2, 4, 7, 1)$

14. Demuestre que
    (a) El producto de dos permutaciones pares es par.
    (b) El producto de dos permutaciones impares es par.
    (c) El producto de una permutación par y una impar es impar.

15. Sea $A = \{1, 2, 3, 4, 5\}$. Sean $f = (5, 2, 3)$ y $g = (3, 4, 1)$ permutaciones de A. Calcule lo siguiente y escriba el resultado como producto de ciclos disjuntos.
    (a) $f \circ g$ (b) $f^{-1} \circ g^{-1}$

16. Muestre que si p es una permutación de un conjunto finito A, entonces $p^2 = p \circ p$ es una permutación de A.

17. Sean $A = \{1, 2, 3, 4, 5, 6\}$ y
$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$$
    una permutación de A.
    (a) Escriba p como producto de ciclos disjuntos.
    (b) Calcule p^{-1}.
    (c) Calcule p^2.
    (d) Determine el periodo de p; es decir, el menor entero positivo k tal que $p^k = 1_A$.

18. Sean $A = \{1, 2, 3, 4, 5, 6\}$ y
$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}$$
    una permutación de A.
    (a) Escriba p como producto de ciclos disjuntos.
    (b) Calcule p^{-1}.
    (c) Calcule p^2.
    (d) Determine el periodo de p; es decir, el menor entero positivo k tal que $p^k = 1_A$.

19. (a) Utilice inducción matemática para mostrar que si p es una permutación de un conjunto finito A, entonces $p^n = p \circ p \circ \cdots \circ p$ es una permutación de A para $n \in Z^+$.
    (b) Si A es un conjunto finito y p es una permutación de A, muestre que $p^m = 1_A$ para alguna $m \in Z^+$.

20. Sea p una permutación de un conjunto A. Defina la siguiente relación R sobre A: $a\,R\,b$ si y sólo si $p^n(a) = b$ para alguna $n \in Z$. [p^0 se define como la permutación identidad y p^{-n} como $(p^{-1})^n$.] Muestre que R es una relación de equivalencia y describa las clases de equivalencia.

5.4. Crecimiento de funciones

En el análisis anterior de la representación de las relaciones en una computadora (sección 4.6), se observó que uno de los factores que determina la elección del método de almacenamiento es la eficiencia en el manejo de datos. En el ejemplo donde se verificó si una relación era transitiva, se calculó la cantidad promedio de pasos necesarios para un algoritmo con la relación guardada como una matriz y para un algoritmo con la relación guardada como una lista enlazada. Los resultados fueron que se necesitaría aproximadamente $kn^3 + (1 - k)n^2$ pasos con el almacenamiento mediante una matriz y k^3n^4 pasos si se utilizaba la lista enlazada, donde la relación contiene kn^2 parejas ordenadas. Aunque se ignora muchos detalles, estas comparaciones burdas proporcionan la información suficiente como para tomar decisiones acerca del almacenamiento adecuado de los datos. En esta sección se aplicará algunos conceptos de las secciones anteriores y se establecerá la base para un análisis más sofisticado de los algoritmos.

La idea de que una función crece más rápido que otra surge de manera natural al trabajar con funciones. En esta sección se formalizará este concepto.

Ejemplo 1. Sea R una relación sobre un conjunto A, con $|A| = n$ y $|R| = \frac{1}{2}n^2$. Si se guarda R como una matriz, entonces $t(n) = \frac{1}{2}n^3 + \frac{1}{2}n^2$ es una función que describe (de manera aproximada) el número promedio de pasos necesarios para determinar si R es transitiva, utilizando el algoritmo TRANS (sección 4.6). Al guardar R con una lista enlazada y utilizar NEWTRANS, el número promedio de pasos necesarios es (aproximadamente) $s(n) = \frac{1}{8}n^4$. La tabla 5.1 muestra que s crece más rápido que t.

Tabla 5.1

n	$t(n)$	$s(n)$
10	550	1250
50	63,750	781,250
100	505,000	12,500,000

◆

Sean f y g funciones cuyos dominios son subconjuntos de Z^+, los enteros positivos. Se dice que f es $O(g)$, lo cual se lee "f es O mayúscula de g" y a veces sólo "f es O de g", si existen constantes c y k tales que $|f(n)| \leq c \cdot |g(n)|$ para toda $n \geq k$. Si f es $O(g)$, entonces f no crece más rápido de lo que crece g.

Ejemplo 2. La función $f(n) = \frac{1}{2}n^3 + \frac{1}{2}n^2$ es $O(g)$ para $g(n) = n^3$. Para ver esto, considérese

$$\frac{1}{2}n^3 + \frac{1}{2}n^2 \leq \frac{1}{2}n^3 + \frac{1}{2}n^3 \qquad \text{si } n \geq 1$$

Así,

$$\frac{1}{2}n^3 + \frac{1}{2}n^2 \leq 1 \cdot n^3, \qquad \text{si } n \geq 1.$$

Al elegir 1 como c y 1 como k, se ha mostrado que $|f(n)| \leq c \cdot |g(n)|$ para toda $n \geq k$ y f es $O(g)$. ◆

El lector puede ver del ejemplo 2 que se puede elegir de varias formas a c, k e incluso a g. Si $|f(n)| \leq c\,|g(n)|$ para toda $n \geq k$, entonces se tiene $|f(n)| \leq C \cdot |g(n)|$ para toda $n \geq k$ para toda $C \geq c$ y $|f(n)| \leq c \cdot |g(n)|$ para toda $n \geq K$ para cualquier $K \geq k$. Para la función t del ejemplo 2, t es $O(h)$ para $h(n) = dn^3$, si $d \geq 1$, pues $|t(n)| \leq 1 \cdot |g(n)| \leq |h(n)|$. Observe también que t es $O(r(n))$ para $r(n) = n^4$, pues $\frac{1}{2}n^3 + \frac{1}{2}n^2 \leq n^3 \leq n^4$ para toda $n \geq 1$. Al analizar los algoritmos, se quiere conocer la función simple g de "crecimiento más lento" para la que f es $O(g)$.

Es común reemplazar g en $O(g)$ con la fórmula que define a g. Así, se escribe que t es $O(n^3)$. Esta notación se llama O mayúscula.

f y g tienen el **mismo orden** si f es $O(g)$ y g es $O(f)$.

Ejemplo 3. Sean $f(n) = 3n^4 - 5n^2$ y $g(n) = n^4$, definidas para los enteros positivos n. Entonces f y g tienen el mismo orden. En primer lugar,

$$\begin{aligned} 3n^4 - 5n^2 &\leq 3n^4 + 5n^2 \\ &\leq 3n^4 + 5n^4, \qquad \text{si } n \geq 1 \\ &= 8n^4. \end{aligned}$$

Sean $c = 8$ y $k = 1$; entonces $|f(n)| \leq c \cdot |g(n)|$ para toda $n \geq k$. Así, f es $O(g)$. Recíprocamente, $n^4 = 3n^4 - 2n^4 \leq 3n^4 - 5n^2$ si $n \geq 2$. Esto es porque si $n \geq 2$, entonces $n^2 > \frac{5}{2}$, $2n^2 > 5$ y $2n^4 > 5n^2$. Se utiliza 1 como c y 2 como k para concluir que g es $O(f)$. ◆

Si f es $O(g)$ pero g no es $O(f)$, f tiene **menor orden** que g o f crece más lento que g.

Ejemplo 4. La función $f(n) = n^5$ tiene menor orden que $g(n) = n^7$. Es claro que si $n \geq 1$, entonces $n^5 \leq n^7$. Supóngase que existen c y k tales que $n^7 \leq cn^5$ para toda $n \geq k$. Se elige N de modo que $N > k$ y $N^2 > c$. Entonces $N^7 \leq cN^5 < N^2 \cdot N^5$, pero esto es una contradicción. Por lo tanto, f es $O(g)$, pero g no es $O(f)$, y f tiene menor orden que g. Esto coincide con la experiencia, pues n^5 crece más lento que n^7. ◆

Se define una relación Θ, theta mayúscula, sobre las funciones cuyos dominios son subconjuntos de Z^+ como $f\,\Theta\,g$ si y sólo si f y g tienen el mismo orden.

Teorema 1. *La relación Θ definida anteriormente es una relación de equivalencia.*

Demostración: Es claro que Θ es reflexiva, pues toda función tiene el mismo orden que sí misma. Debido a que la definición de mismo orden considera a f y g de la misma forma, esta definición es simétrica y la relación Θ es simétrica.

Para ver que Θ es transitiva, supóngase que f y g tienen el mismo orden. Entonces existen c_1 y k_1 tales que $|f(n)| \leq c_1 \cdot |g(n)|$ para toda $n \geq k_1$, y que existen c_2 y k_2 tales que $|g(n)| \leq c_2 \cdot |f(n)|$ para toda $n \geq k_2$. Supóngase que g y h tienen el mismo orden; entonces existen c_3, k_3 tales que $|g(n)| \leq c_3 \cdot |h(n)|$ para toda $n \geq k_3$, y existen c_4, k_4 tales que $|h(n)| \leq c_4 \cdot |g(n)|$ para toda $n \geq k_4$.

Entonces $|f(n)| \leq c_1 \cdot |g(n)| \leq c_1(c_3 \cdot |h(n)|)$ si $n \geq k_1$ y $n \geq k_3$. Así, $|f(n)| \leq c_1c_3 \cdot |h(n)|$ para toda $n \geq$ máximo de k_1 y k_3.

De manera análoga, $|h(n)| \leq c_2c_4 \cdot |f(n)|$ para toda $n \geq$ máximo de k_2 y k_4. Así, f y h tienen el mismo orden y Θ es transitiva. ●

Las clases de equivalencia de Θ constan de las funciones que tienen el mismo orden. Se utiliza cualquier función simple en la clase de equivalencia para representar el orden de todas las funciones en esa clase. Una clase Θ es **menor** que otra clase Θ si una función representativa de la primera tiene menor orden que una función representativa de la segunda. Esto significa que las funciones de la primera clase crecen más lento que las de la segunda. La clase Θ de una función proporciona la información necesaria para el análisis de algoritmos.

Ejemplo 5. Todas las funciones que tienen el mismo orden que $g(n) = n^3$ tienen orden $\Theta(n^3)$. Los órdenes más comunes en las aplicaciones de la ciencia de la computación son $\Theta(1)$, $\Theta(n)$, $\Theta(n^2)$, $\Theta(n^3)$, $\Theta(lg(n))$, $\Theta(n\, lg(n))$ y $\Theta(2^n)$. En este caso, $\Theta(1)$ representa la clase de las funciones constantes y lg es la función logaritmo en base 2. La figura 5.6 muestra algunas de estas funciones. ♦

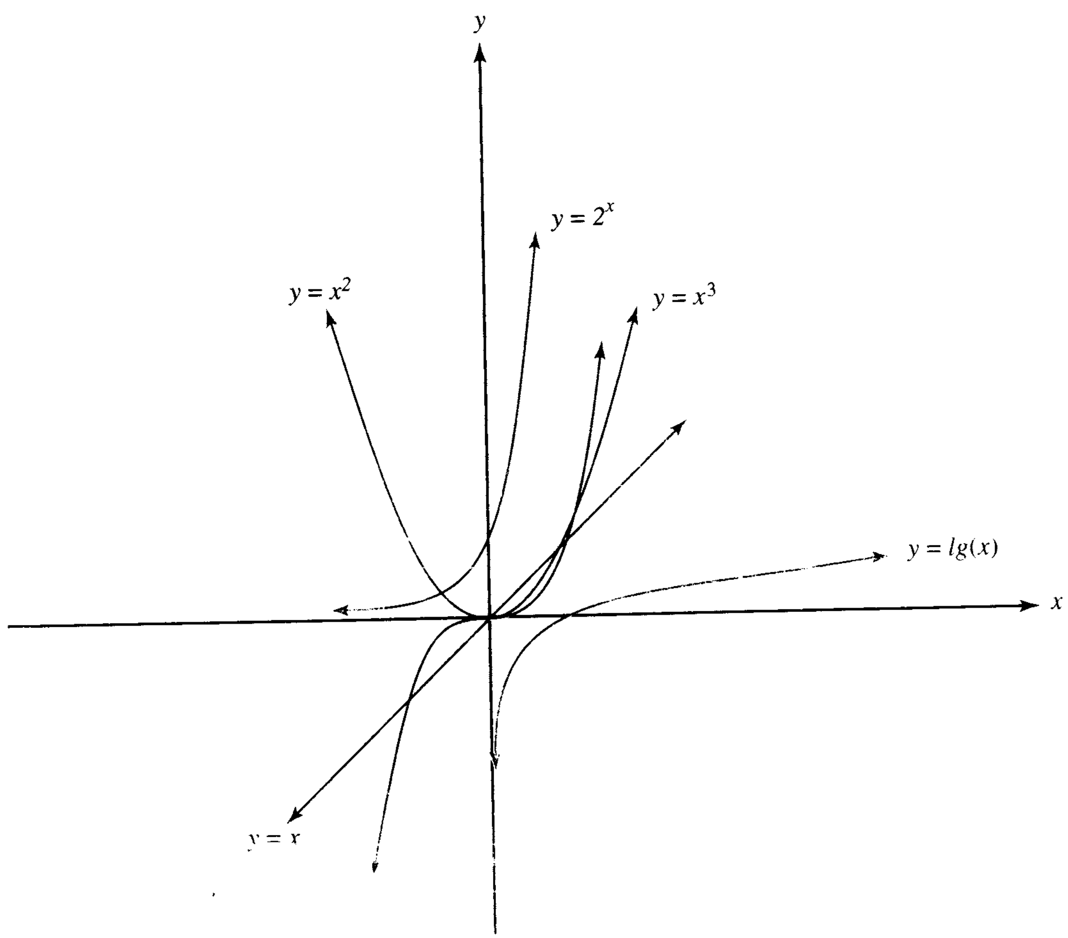


Figura 5.6

Ejemplo 6. Toda función logarítmica $f(n) = \log_b(n)$ tiene el mismo orden que $g(n) = lg(n)$. Existe una identidad de cambio de base del logaritmo, $\log_b(x) = \frac{\log_a(x)}{\log_a(b)}$ en donde $\log_a(b)$ es

una constante. Así, $|\log_b(n)| \leq \frac{1}{lg(b)}\, |lg(n)|$ y, recíprocamente, $|lg(n)| \leq lg(b) \cdot |\log_b(n)|$. Por lo tanto, g es $O(f)$ y f es $O(g)$. ♦

A veces es necesario combinar funciones que proporcionen el número de pasos necesarios para las partes de un algoritmo, como se hizo en el análisis de TRANS (sección 4.6), donde se sumó las funciones, y en el análisis de NEWTRANS, donde se multiplicó las funciones. Existen ciertas reglas generales en relación con el orden de las clases de equivalencia Θ que se puede utilizar para determinar la clase de muchas funciones y la clase de la suma y el producto de funciones ya clasificadas.

Reglas para determinar la clase Θ de una función

1. Las funciones $\Theta(1)$ son constantes y tienen crecimiento nulo, el mínimo crecimiento posible.
2. $\Theta(lg(n))$ es menor que $\Theta(n^k)$ si $k > 0$. Esto significa que la función logarítmica crece más lento que cualquier función potencia con exponente positivo.
3. $\Theta(n^a)$ es menor que $\Theta(n^b)$ si y sólo si $a < b$.
4. $\Theta(a^n)$ es menor que $\Theta(b^n)$ si y sólo si $a < b$.
5. $\Theta(n^k)$ es menor que $\Theta(a^n)$ para cualquier potencia n^k y cualquier $a > 1$. Esto significa que cualquier función exponencial con base mayor que 1 crece más rápido que cualquier función potencia.
6. Si r es distinto de cero, entonces $\Theta(rf) = \Theta(f)$ para cualquier función f.
7. Si h es una función distinta de cero y $\Theta(f)$ es menor (o igual) que $\Theta(g)$, entonces $\Theta(fh)$ es menor (o igual) que $\Theta(gh)$.
8. Si $\Theta(f)$ es menor que $\Theta(g)$, entonces $\Theta(f + g) = \Theta(g)$.

Ejemplo 7. Determine la clase Θ de las siguientes funciones.

(a) $f(n) = 4n^4 - 6n^7 + 25n^3$
(b) $g(n) = lg(n) - 3n$
(c) $h(n) = 1.1^n + n^{15}$

Solución: (a) Por las reglas 3, 6 y 8, el grado del polinomio determina la clase Θ de una función polinomial. $\Theta(f) = \Theta(n^7)$.
(b) Se utiliza las reglas 2, 6 y 8 para obtener $\Theta(g) = \Theta(n)$.
(c) Por las reglas 5 y 8, $\Theta(h) = \Theta(1.1^n)$. ♦

Ejemplo 8. Utilice las reglas para el ordenamiento de las clases Θ para ordenar las siguientes clases de menor a mayor.

$$\Theta(n\, lg(n)) \quad \Theta(1000n^2 - n) \quad \Theta(n^{0.2}) \quad \Theta(1{,}000{,}000) \quad \Theta(1.3^n) \quad \Theta(n + 10^7)$$

Solución: $\Theta(1{,}000{,}000)$ es la clase de las funciones constantes, de modo que es la primera en la lista. Por las reglas 5 y 8, $\Theta(n + 10^7)$ es menor que $\Theta(1000n^2 - n)$, pero mayor que $\Theta(n^{0.2})$. Para determinar la posición de $\Theta(n\, lg(n))$ en la lista, se aplican las reglas 2 y 7. Éstas implican que $\Theta(n\, lg(n))$ es menor que $\Theta(n^2)$ y mayor que $\Theta(n)$. La regla 5 dice que $\Theta(1.3^n)$ es la clase máxima en la lista. En orden, las clases son

$$\Theta(1{,}000{,}000) \quad \Theta(n^{0.2}) \quad \Theta(n + 10^7) \quad \Theta(n\, lg(n)) \quad \Theta(1000n^2 - n) \quad \Theta(1.3^n).$$

♦

La clase Θ de una función que describe el número de pasos realizados por un algoritmo se conoce como el **tiempo de ejecución** del algoritmo. Por ejemplo, el algoritmo TRANS tiene un tiempo promedio de ejecución de n^3. En general, los algoritmos con tiempos de ejecución exponenciales no son prácticos, excepto para valores muy pequeños de n.

GRUPO DE EJERCICIOS 5.4

En los ejercicios 1 y 2, sea f una función que describe el número de pasos necesarios para desarrollar cierto algoritmo. El número de elementos por procesar se representa como n. Para cada función, describa lo que ocurre con el número de pasos si el número de elementos se duplica.

1. (a) $f(n) = 1001$ (b) $f(n) = 3n$
(c) $f(n) = 5n^2$ (d) $f(n) = 2.5n^3$
(e) $f(n) = 1.4\ lg(n)$ (f) $f(n) = 2^n$

2. (a) $f(n) = n\ lg(n)$ (b) $f(n) = 100\ n^4$

3. Muestre que $g(n) = n!$ es $O(n^n)$.

4. Muestre que $h(n) = 1 + 2 + 3 + \cdots + n$ es $O(n^2)$.

5. Muestre que $f(n) = 8n + lg(n)$ es $O(n)$.

6. Muestre que $g(n) = n^2(7n - 2)$ es $O(n^3)$.

7. Muestre que $f(n) = n\ lg(n)$ es $O(g)$ para $g(n) = n^2$, pero que g no es $O(f)$.

8. Muestre que $f(n) = n^{100}$ es $O(g)$ para $g(n) = 2^n$, pero que g no es $O(f)$.

9. Muestre que f y g tienen el mismo orden, para $f(n) = 5n^2 + 4n + 3$ y $g(n) = n^2 + 100n$.

10. Muestre que f y g tienen el mismo orden, para $f(n) = lg(n^3)$ y $g(n) = \log_5(6n)$.

11. Determine cuáles de las siguientes funciones están en la misma clase Θ. Una función podría quedar sola en una clase.

$f_1(n) = 5n\ lg(n)$, $f_2(n) = 6n^2 - 3n + 7$,
$f_3(n) = 1.5^n$, $f_4(n) = lg(n^4)$, $f_5(n) = 13{,}463$,
$f_6(n) = -15n$, $f_7(n) = lg(lg(n))$, $f_8(n) = 9n^{0.7}$,
$f_9(n) = n!$, $f_{10}(n) = n + lg(n)$,
$f_{11}(n) = \sqrt{n} + 12n$, $f_{12}(n) = lg(n!)$

12. Ordene las clases Θ del ejercicio 11 de menor a mayor.

En los ejercicios 13 a 18, analice la operación realizada por la parte dada de seudocódigo y escriba una función que describa el número de pasos necesarios. Proporcione la clase Θ de la función.

13.
```
1   A ← 1
2.  B ← 1
3.  UNTIL (B > 100)
    a.  B ← 2A − 2
    b.  A ← A + 3
```

14.
```
1.  X ← 1
2.  Y ← 100
3.  WHILE (X < Y)
    a.  X ← X + 2
    b.  Y ← ½Y
```

15.
```
1.  I ← 1
2.  X ← 0
3.  WHILE (I ≤ N)
    a.  X ← X + 1
    b.  I ← I + 1
```

16.
```
1.  SUM ← 0
2.  FOR I = 0 THRU 2(N − 1) BY 2
    a.  SUM ← SUM + I
```

17. Sea A un arreglo de longitud N y X un elemento que se puede guardar en A. En este ejercicio, la función debe describir el número promedio de pasos necesarios para determinar si X está en A.

```
FUNCTION SEEK(A, X)
1.  FOUND ← FALSE
2.  K ← 1
3.  WHILE (NOT FOUND) AND (K < N)
    a.  IF (A[K] = X) THEN
        1.  FOUND ← TRUE
    b.  ELSE
        1.  K ← K + 1
4.  RETURN
```


18.
```
SUBROUTINE MATMUL(A, B, N, M, P, Q; C)
1.  IF (M = P) THEN
    a.  FOR I = 1 THRU N
        1.  FOR J = 1 THRU Q
            a.  C[I, J] ← 0
            b.  FOR K = 1 THRU M
                1.  C[I, J] ← C[I, J] +
                        (A[I, K] × B[K, J])
2.  ELSE
    a.  CALL PRINT ('INCOMPATIBLE')
3.  RETURN
FIN DE LA SUBRUTINA MATMUL
```

19. Demuestre la regla 3.

20. Demuestre la regla 7.

IDEAS CLAVE PARA REPASO

- Función: véase la página 167.
- Función identidad, 1_A: $1_A(a) = a$.
- Función f uno a uno de A en B: $a \neq a'$ implica que $f(a) \neq f(a')$.
- Función sobre f de A en B: $\text{Ran}(f) = B$.
- Biyección: función uno a uno y sobre.
- Correspondencia uno a uno: función sobre, uno a uno y definida en todo punto.
- Si f es una función de A en B, $1_B \circ f = f$; $f \circ 1_A = f$.
- Si f es una función invertible de A en B, $f^{-1} \circ f = 1_A$; $f \circ f^{-1} = 1_B$.
- $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- Función booleana f: $\text{Ran}(f) \subseteq \{\text{cierto, falso}\}$
- Función de hashing: véase la página 179.
- Función de permutación: una biyección de un conjunto A en sí mismo.
- Teorema: Si A es un conjunto con n elementos, entonces existen $n!$ permutaciones de A.
- Ciclo de longitud r: $(b_1, b_2, \ldots, b_r)$; véase la página 183.
- Teorema: Una permutación de un conjunto finito que no sea la identidad o un ciclo se puede escribir como un producto de ciclos disjuntos.
- Transposición: un ciclo de longitud 2.
- Corolario: Toda permutación de un conjunto finito con al menos dos elementos se puede escribir como producto de transposiciones.
- Permutación par (impar): aquella que se puede escribir como producto de un número par (impar) de transposiciones.
- Teorema: Si una permutación de un conjunto finito se puede escribir como producto de un número par de transposiciones, entonces nunca se puede escribir como producto de un número impar de transposiciones, y recíprocamente.
- El producto de:
  (a) Dos permutaciones pares es par.
  (b) Dos permutaciones impares es par.
  (c) Una permutación par y otra impar es impar.
- Teorema: Si A es un conjunto con n elementos, entonces existen $n!/2$ permutaciones pares y $n!/2$ permutaciones impares de A.
- $O(g)$ (O mayúscula de g): véase la página 191.
- f y g del mismo orden: f es $O(g)$ y g es $O(f)$.
- Teorema: La relación Θ, $f\ \Theta\ g$ si y sólo si f y g tienen el mismo orden, es una relación de equivalencia.
- Clase Θ mínima: véase la página 192.
- Reglas para determinar la clase Θ de una función: véase la página 192.
- Tiempo de ejecución de un algoritmo: clase Θ de una función que describe el número de pasos realizados por el algoritmo.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes ejercicios, escriba el programa o subrutina solicitados en seudocódigo (como se ha descrito en el apéndice A) o en un lenguaje de programación que conozca. Verifique su código con una prueba de escritorio o con una ejecución en computadora.

1. Sea $U = \{u_1, u_2, \ldots u_n\}$ el conjunto universal para ciertos conjuntos de entradas. Escriba una función CHARFCN tal que, dado un conjunto como entrada, regrese la función característica del conjunto como una sucesión.
2. Escriba una función TRANSPOSE tal que, dada una matriz $n \times n$, regrese su transpuesta.
3. Escriba un programa que escriba una permutación dada como producto de ciclos disjuntos.
4. Escriba un programa que escriba una permutación dada como producto de transposiciones.
5. Utilice el programa del ejercicio 4 como subrutina en un programa que determine si una permutación dada es impar o par.

CAPÍTULO 6

TEMAS DE LA TEORÍA DE GRÁFICAS

Requisitos previos: Capítulos 3 y 5

6.1. Gráficas

La teoría de gráficas se inicia con ideas geométricas muy simples y tiene muchas aplicaciones importantes. En los capítulos 4, 7 y 8 se analizaron algunos usos de las gráficas. En esos capítulos una gráfica se asoció con el digrafo de una relación simétrica. Al combinar esas ideas con la de función, se puede definir un tipo más general de gráfica que permite utilizar más de una arista (lado o arco) entre los mismos vértices. A veces esta gráfica se conoce como multigrafo.

Una **gráfica** G consta de un conjunto finito V de objetos llamados **vértices**, un conjunto finito F de objetos llamados **aristas** y una función γ que asigna a cada arista un subconjunto $\{v, w\}$, donde v y w son vértices (que podrían ser iguales). Se escribe $G = (V, E, \gamma)$ cuando se deba enfatizar los componentes de G. Si e es una arista, y $\gamma(e) = \{v, w\}$, se dice que e es una arista entre v y w y que e está determinada por v y w. Los vértices v y w son los

extremos de e. Si sólo existe una arista entre v y w, con frecuencia se identifica a e con el conjunto $\{v, w\}$. Esto no causará confusión alguna. Se puede eliminar la restricción de que sólo exista una cantidad finita de vértices, pero en este análisis, todas las gráficas tendrán un número finito de vértices.

Ejemplo 1. Sean $V = \{1, 2, 3, 4\}$ y $E = \{e_1, e_2, e_3, e_4, e_5\}$. Sea γ dada por

$$\gamma(e_1) = \gamma(e_5) = \{1, 2\}, \quad \gamma(e_2) = \{4, 3\}, \quad \gamma(e_3) = \{1, 3\}, \quad \gamma(e_4) = \{2, 4\}.$$

Entonces $G = (V, E, \gamma)$ es una gráfica. ◆

Por lo general, las gráficas son representadas mediante imágenes que utilizan un punto por cada vértice y una línea por cada arista. G se representa como en la figura 6.1. Es usual omitir los nombres de las aristas, pues no tienen un significado intrínseco. Además, tal vez se quiera escribir etiquetas que resulten más útiles sobre las aristas. A veces se omite las etiquetas sobre los vértices si la información gráfica es adecuada para el análisis.

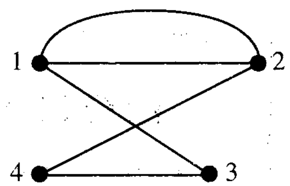


Figura 6.1

Con frecuencia, las gráficas son utilizadas para registrar información acerca de relaciones o conexiones. Una arista entre v_i y v_j indica una conexión entre los objetos v_i y v_j. En una representación geométrica de una gráfica, las conexiones son la información más importante, y por lo general varias imágenes distintas pueden representar la misma gráfica.

Ejemplo 2. Las figuras 6.2 y 6.3 también representan la gráfica G dada en el ejemplo 1. ◆

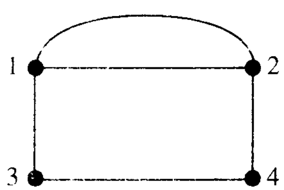


Figura 6.2

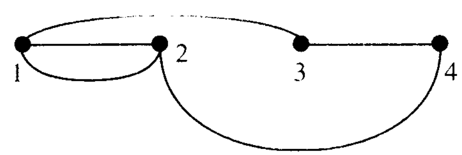


Figura 6.3

El **grado** de un vértice es el número de aristas que tienen a ese vértice como extremo. Una gráfica puede contener una arista de un vértice a sí mismo; tal arista es un bucle **cerrado** (o lazo). Un bucle cerrado contribuye en 2 unidades al grado de un vértice.

Ejemplo 3

(a) En la gráfica de la figura 6.4, el vértice A tiene grado 2, el vértice B tiene grado 4 y el vértice D tiene grado 3.

(b) En la figura 6.5, el vértice a tiene grado 4, el vértice e tiene grado 0 y el vértice b tiene grado 2.

(c) Cada vértice de la gráfica de la figura 6.6 tiene grado 2. ◆

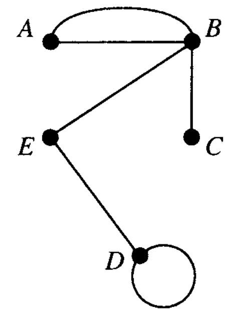


Figura 6.4

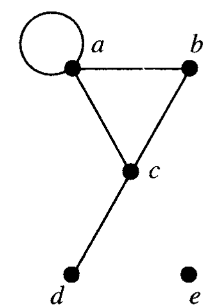


Figura 6.5

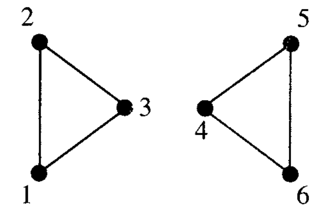


Figura 6.6

Un vértice de grado 0 es un vértice **aislado**. Dos vértices que determinan una arista son vértices **adyacentes**.

Ejemplo 4. En la figura 6.5, el vértice e es un vértice aislado. En la figura 6.5, a y b son vértices adyacentes; los vértices a y d no son adyacentes. ◆

Una **trayectoria** (o camino) en una gráfica es una sucesión π: $v_1, v_2, \ldots, v_k$ de vértices, cada uno adyacente al siguiente, y una elección de una arista entre v_i y v_{i+1}, de modo que ninguna arista es elegida más de una vez. En términos geométricos, esto significa que es posible iniciar en v_1 y viajar a través de las aristas hasta v_k y nunca utilizar la misma arista dos veces.

Un **circuito** es una trayectoria que inicia y termina con el mismo vértice. En el capítulo 4 esto fue llamado ciclo de trayectoria; la palabra circuito es más común en la teoría general de gráficas. Una trayectoria $v_1, v_2, \ldots, v_k$ es simple si ningún vértice aparece más de una vez. De manera análoga, un circuito $v_1, v_2, \ldots, v_{k-1}, v_1$ es **simple** si los vértices $v_1, v_2, \ldots, v_{k-1}$ son todos distintos.

Ejemplo 5

(a) Una trayectoria en la gráfica representada mediante la figura 6.2 es π_1: 1, 3, 4, 2.

(b) Las trayectorias en la gráfica de la figura 6.4 incluyen a π_2: D, E, B, C, π_3: A, B, E, D, D y π_4: A, B, A. Observe que en π_4 no se especifica la arista entre A y B que se utilizó primero.

(c) Algunos ejemplos de trayectorias en la gráfica de la figura 6.5 son π_5: a, b, c, a y π_6: d, c, a, a. La trayectoria π_5 es un circuito.

(d) En la figura 6.6, la sucesión 1, 2, 3, 2 no es una trayectoria, pues la única arista existente entre 2 y 3 tendría que recorrerse dos veces.

(e) La trayectoria π_7: c, a, b, c, d de la figura 6.5 no es simple. ◆

Una gráfica es **conexa** si existe una trayectoria de cualquier vértice a otro de la gráfica. En caso contrario, la gráfica es **disconexa**. Si la gráfica es disconexa, las diversas partes conexas son las **componentes** de la gráfica.

Ejemplo 6. Las gráficas de las figuras 6.1 y 6.4 son conexas. Las de las figuras 6.5 y 6.6 son disconexas. La gráfica de la figura 6.6 tiene dos componentes. ◆

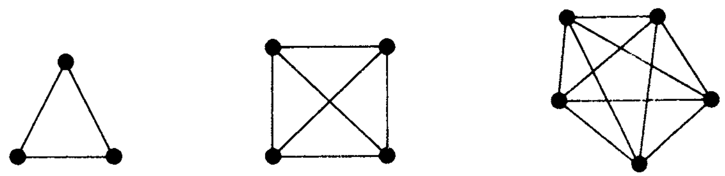
Algunas familias especiales importantes de gráficas serán útiles como ejemplos en el momento del análisis. A continuación serán presentadas.

1. Para cada entero $n \geq 1$, sea D_n la gráfica con n vértices sin aristas. La figura 6.7 muestra a D_2 y D_5. D_n es la **gráfica discreta** de n vértices.

D_2 D_5

Figura 6.7

2. Para cada entero $n \geq 1$, sea K_n la gráfica con vértices $\{v_1, v_2, \ldots, v_n\}$ y con una arista $\{v_i, v_j\}$ para cada i, j. En otras palabras, cada vértice de K_n está conectado con cualquier otro vértice. En la figura 6.8 se muestra K_3, K_4 y K_5. La gráfica K_n es la **gráfica completa** de n vértices. Mas en general, si cada vértice de una gráfica tiene el mismo grado que cualquier otro vértice, la gráfica es **regular**. Las gráficas D_n también son regulares.



K_3 K_4 K_5

Figura 6.8

3. Para cada entero $n \geq 1$, sea L_n la gráfica con n vértices $\{v_1, v_2, \ldots, v_n\}$ y con aristas $\{v_i, v_{i+1}\}$ para $1 \leq i < n$. Se muestra L_2 y L_4 en la figura 6.9. L_n es la **gráfica lineal** de n vértices.

L_2 L_4

Figura 6.9

Ejemplo 7. Todas las gráficas K_n y L_n son conexas, mientras que las gráficas D_n son disconexas. De hecho, la gráfica D_n tiene precisamente n componentes. ◆

Subgráficas y gráficas cociente

Suponga que $G = (V, E, \gamma)$ es una gráfica. Elija un subconjunto E_1 de las aristas de E y un subconjunto V_1 de los vértices en V, de modo que V_1 contenga (al menos) todos los extremos de las aristas de E_1. Entonces $H = (V_1, E_1, \gamma_1)$ también es una gráfica, donde γ_1 es γ restringida a las aristas en E_1. Tal gráfica H es una **subgráfica** de G. Las subgráficas juegan un papel importante en el análisis de las propiedades de las gráficas.

Ejemplo 8. Las gráficas de las figuras 6.11, 6.12 y 6.13 son cada una subgráfica de la gráfica de la figura 6.10. ◆

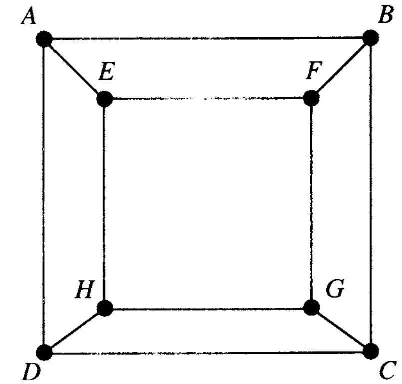


Figura 6.10

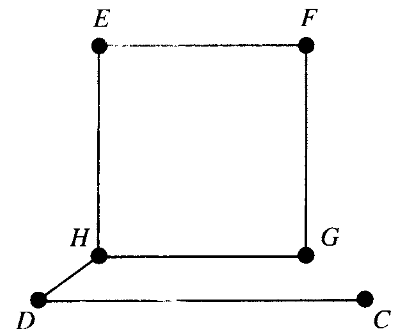


Figura 6.11

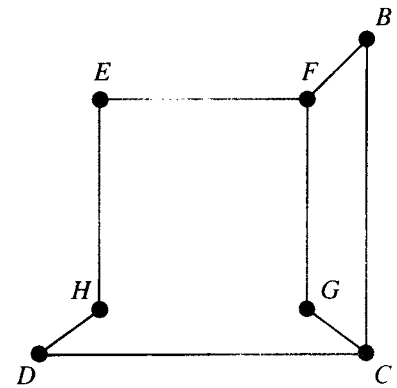


Figura 6.12

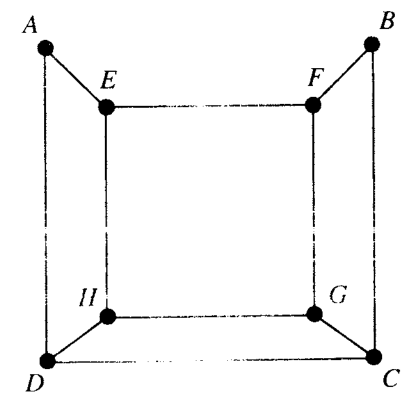


Figura 6.13

Una de las subgráficas más importantes es aquella que surge de eliminar una arista y ningún vértice. Si $G = (V, E, \gamma)$ es una gráfica y $e \in E$, entonces se denota G_e a la gráfica obtenida al omitir la arista e de E y conservar todos los vértices. Si $\underline{G}$ es la gráfica de la figura 6.10 y $e = \{A, B\}$, entonces $\underline{G}_e$ es la gráfica de la figura 6.13.

La segunda construcción importante se define para gráficas con aristas múltiples. Suponga que $G = (V, E, \gamma)$ es dicha gráfica y que R es una relación de equivalencia sobre el conjunto V. Entonces, se construye la **gráfica cociente** G^R de la siguiente manera. Los vértices de G^R son las clases de equivalencia de V producidas por R (véase la sección 4.5). Si $[v]$ y $[w]$ son las clases de equivalencia de los vértices v y w de G, entonces existe una arista en G^R de $[v]$ a $[w]$ si algún vértice en $[v]$ está conectado con algún vértice en $[w]$ en la gráfica G. De manera informal, esto sólo dice que se obtiene G^R al fusionar todos los vértices de cada clase de equivalencia en un único vértice y combinar las aristas que quedan sobrepuestas mediante tal proceso.

Ejemplo 9. Sea $\underline{G}$ la gráfica de la figura 6.14 (que no tiene aristas múltiples) y sea R la relación de equivalencia sobre V definida por la partición $\{\{A, E, I\}, \{B, F, J\}, \{C, G, K\}, \{D, H, L\}\}$. Entonces $\underline{G}^R$ aparece en la figura 6.15.

Si S también es una relación de equivalencia sobre V definida por la partición $\{\{I, J, K, L\}, \{A, E\}, \{F, B, C\}, \{D\}, \{G\}, \{H\}\}$, entonces la gráfica cociente $\underline{G}^S$ aparece en la figura 6.16. ◆

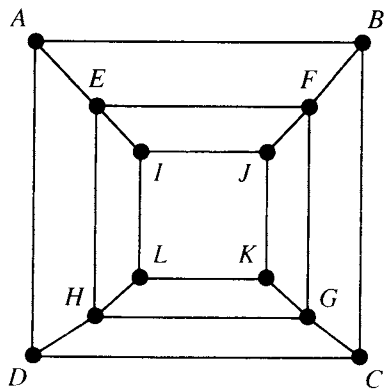


Figura 6.14

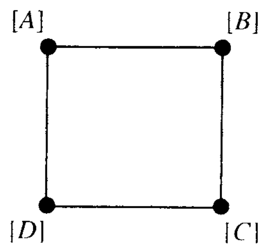


Figura 6.15

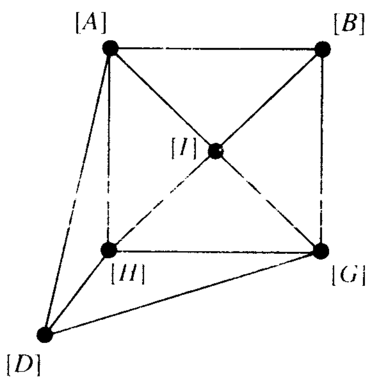


Figura 6.16

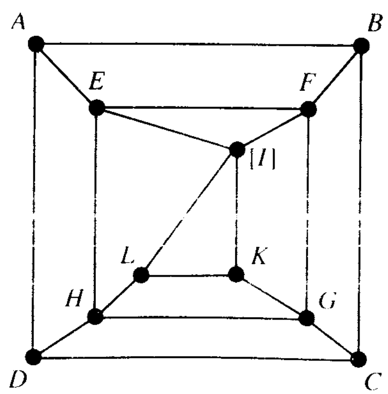


Figura 6.17

De nuevo, uno de los casos más importantes surge al utilizar sólo una arista. Si e es una arista entre el vértice v y el vértice w en una gráfica $G = \{V, E, \gamma\}$, entonces se considera la relación de equivalencia cuya partición consta de $\{v, w\}$ y $\{v_i\}$, para cada $v_i \neq v$, $v_i \neq w$. Es decir, se une v y w en un vértice y se deja lo demás igual. La gráfica cociente resultante se denota por G^e. Si $\underline{G}$ es la gráfica de la figura 6.14, y $e = \{I, J\}$, entonces $\underline{G}^e$ es la gráfica de la figura 6.17.

GRUPO DE EJERCICIOS 6.1

En los ejercicios 1 al 4, *proporcione* V, *el conjunto de vértices, y* E, *el conjunto de aristas, para las gráficas* $G = (V, E, \gamma)$ *dadas en las figuras* 6.18 *y* 6.21.

1.

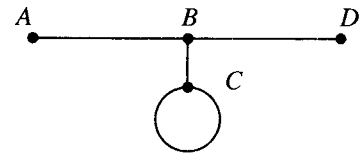


Figura 6.18

2.

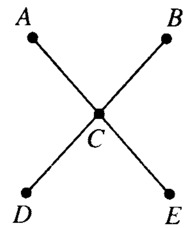


Figura 6.19

3.

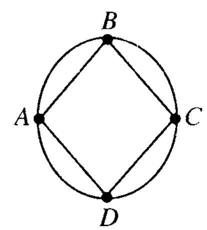


Figura 6.20

4.

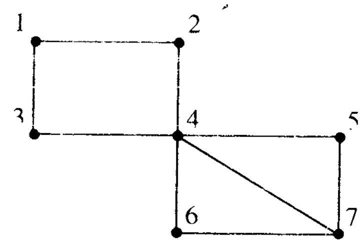


Figura 6.21

5. Trace una imagen de la gráfica $G = (V, E, \gamma)$, donde $V = \{A, B, C, D, E\}$, $E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$, y $\gamma(e_1) = \gamma(e_5) = \{A, C\}$, $\gamma(e_2) = \{A, D\}$, $\gamma(e_3) = \{E, C\}$, $\gamma(e_4) = \{B, C\}$, y $\gamma(e_6) = \{E, D\}$.

6. Trace una imagen de la gráfica $G = (V, E, \gamma)$, donde $V = \{A, B, C, D, E, F, G, H\}$, $E = \{e_1, e_2, \ldots, e_9\}$, y $\gamma(e_1) = \{A, C\}$, $\gamma(e_2) = \{A, B\}$, $\gamma(e_3) = \{D, C\}$, $\gamma(e_4) = \{B, D\}$, $\gamma(e_5) = \{E, A\}$, $\gamma(e_6) = \{E, D\}$, $\gamma(e_7) = \{F, E\}$, $\gamma(e_8) = \{E, G\}$, y $\gamma(e_9) = \{F, G\}$.

7. Proporcione el grado de cada vértice de la figura 6.18.

8. Proporcione el grado de cada vértice de la figura 6.20.

9. Enumere todas las trayectorias que comienzan en A en la figura 6.19.

10. Enumere tres circuitos que comiencen en 5 en la figura 6.21.

11. Trace la gráfica completa de siete vértices.

12. Considere K_n, la gráfica completa de n vértices. ¿Cuál es el grado de cada vértice?

13. ¿Cuáles de las gráficas de los ejercicios 1 al 4 son regulares?

14. Proporcione un ejemplo de una gráfica conexa regular de seis vértices que no sea completa.

Para los ejercicios 15 *y* 16, *utilice la gráfica de la figura* 6.22.

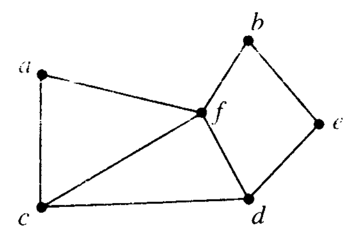


Figura 6.22

15. Si R es la relación de equivalencia definida por la partición $\{\{a, f\}, \{e, b, d\}, \{c\}\}$, determine la gráfica cociente G^R.

16. Si R es la relación de equivalencia definida por la partición $\{\{a, b\}, \{e\}, \{d\}, \{f, c\}\}$, determine la gráfica cociente G^R.

Para los ejercicios 17 *y* 18, *utilice la gráfica de la figura* 6.23.

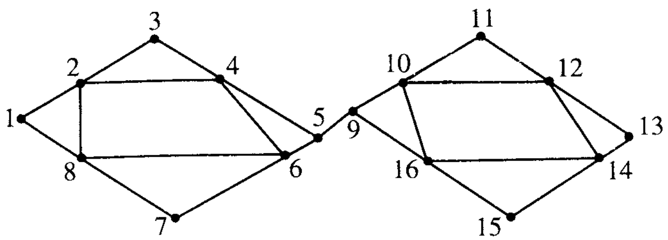


Figura 6.23

17. Sea $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), (8, 8), (9, 9), (10, 10), (11, 11), (12, 12), (13, 13), (14, 14), (15, 15), (16, 16), (1, 10), (10, 1), (3, 12), (12, 3), (5, 14), (14, 5), (2, 11), (11, 2), (4, 13), (13, 4), (6, 15), (15, 6), (7, 16), (16, 7), (8, 9), (9, 8)\}$. Trace la gráfica cociente G^R.

18. Sea $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), (8, 8), (9, 9), (10, 10), (11, 11), (12, 12), (13, 13), (14, 14), (15, 15), (16, 16), (1, 2), (2, 1), (3, 4), (4, 3), (5, 6), (6, 5), (7, 8), (8, 7), (9, 16), (16, 9), (10, 11), (11, 10), (12, 13), (13, 12), (14, 15), (15, 14)\}$. Trace la gráfica cociente G^R.

19. Complete el siguiente enunciado. Toda gráfica lineal de n vértices debe tener ________ aristas. Explique su respuesta.

20. ¿Cuál es el número total de aristas en K_n, la gráfica completa de n vértices? Justifique su respuesta.

6.2. Trayectorias (caminos) y circuitos de Euler

En esta sección y la siguiente, se analizará una clase amplia de problemas en los cuales se utiliza la teoría de gráficas. En el primer tipo de problema, la tarea es recorrer una trayectoria utilizando cada arista de la gráfica sólo una vez. Puede ser necesario o no comenzar y terminar en el mismo vértice. Un ejemplo sencillo de esto es el problema común de trazar una figura geométrica sin levantar el lápiz del papel.

Una trayectoria en una gráfica G es una **trayectoria de Euler** si incluye a cada una de las aristas sólo una vez. Un **circuito de Euler** es una trayectoria de Euler que es a la vez un circuito.

Ejemplo 1. La figura 6.24 muestra el mapa de las calles de un pequeño barrio. Se ha aprobado un reglamento de reciclado, de modo que los responsables de recoger los materiales reciclables deben iniciar y terminar cada viaje en la terminal de reciclado. Ellos desean planear la ruta del camión de modo que se cubra todo el barrio y que cada calle se recorra sólo una vez. Se puede construir una gráfica de modo que exista un vértice por cada intersección y una arista por cada calle entre dos intersecciones cualesquiera. Entonces, el problema consiste en determinar un circuito de Euler para esta gráfica. ◆

Ejemplo 2

(a) Una trayectoria de Euler en la figura 6.25 es $\pi : E, D, B, A, C, D$.

(b) Un circuito de Euler en la gráfica de la figura 6.26 es $\pi : 5, 3, 2, 1, 3, 4, 5$. ◆

Un poco de experimentación mostrará que no existe un circuito de Euler para la gráfica de la figura 6.25. También se puede ver que no es posible obtener una trayectoria de Euler para la gráfica de la figura 6.6. (¿Por qué?)

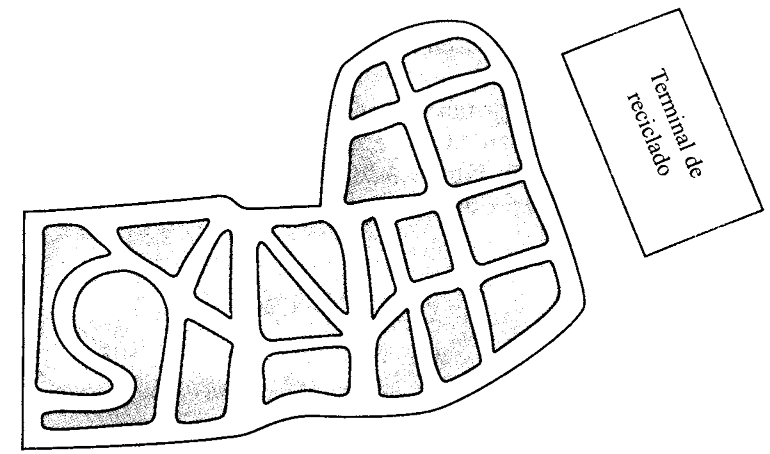


Figura 6.24

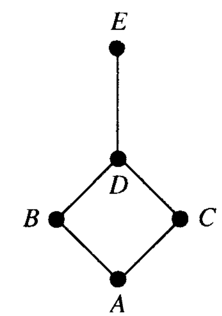


Figura 6.25

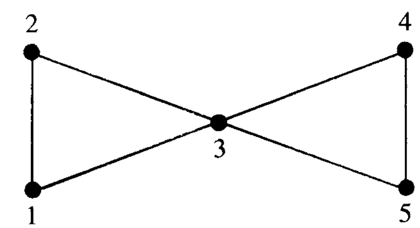
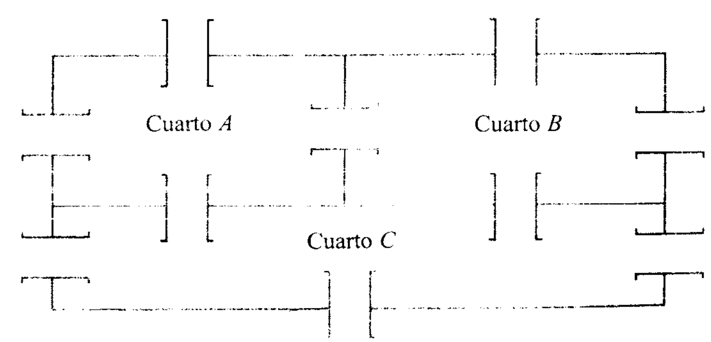


Figura 6.26

Ejemplo 3. Considere el plano de una estructura con tres cuartos, como muestra la figura 6.27.



D (Fuera)

Figura 6.27

Cada cuarto está unido con los demás cuartos: comparte una pared con ellos y con el exterior a lo largo de cada pared. El problema es el siguiente. ¿Es posible comenzar en un cuarto o en el exterior y dar la vuelta de modo que se pase por cada cuarto sólo una vez? Se puede formular este diagrama como una gráfica, donde cada cuarto y el exterior constituye un vértice y una arista corresponde a cada puerta. La figura 6.28 muestra una posible gráfica para esta estructura. La traducción del problema es si existe o no una trayectoria de Euler para esta gráfica. También se resolverá este problema más adelante. ♦

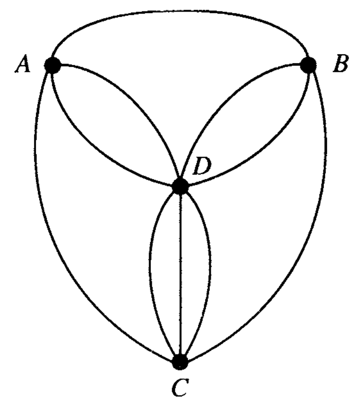


Figura 6.28

En este punto surgen de manera natural dos preguntas. ¿Es posible determinar si existe una trayectoria o circuito de Euler sin encontrarlo en forma explícita? Si debe existir una trayectoria o circuito de Euler ¿existe una forma eficiente de encontrarlo?

Considere de nuevo las gráficas del ejemplo 2. En la figura 6.25, la arista $\{D, E\}$ debe ser la primera o la última en ser visitada, ya que no existe otra forma de ir hacia o salir del vértice E. Esto significa que si G tiene un vértice de grado 1, no puede existir un circuito de Euler, y si existe una trayectoria de Euler, ésta tiene que comenzar o terminar en este vértice. Un argumento similar se aplica a cualquier vértice v de grado impar, por decir, $2n + 1$. Se puede ir hacia una de estas aristas y salir de ella hacia otra n veces, dejando una arista v sin visitar. Se puede utilizar esta última arista para salir o llegar a v, pero no hacer ambas cosas, de modo que no puede completarse el circuito. Se ha mostrado el primero de los siguientes resultados.

Teorema 1

(a) *Si una gráfica G tiene un vértice de grado impar, entonces no puede existir un circuito de Euler en G.*

(b) *Si G es una gráfica conexa y todos los vértices tienen grado par, entonces existe un circuito de Euler en G.*

Demostración: (b) Suponga que existen gráficas conexas donde todos los vértices tienen grado par, pero que no existe un circuito de Euler. Se elige la gráfica G de este tipo, con el menor número de aristas. G debe tener más de un vértice, pues si sólo tuviera un vértice de grado par, es claro que existiría un circuito de Euler. Sea v un vértice de G. Primero, observe que debe existir un circuito que comience y termine en v. Como el grado de v es al menos dos y G es conexa, deben existir distintas aristas entre v y los vértices a y b (que podrían ser el mismo vértice). Como G es conexa, debe existir una trayectoria $a, v_1, v_2, \ldots, b$. Entonces $v, a, v_1, v_2, \ldots, b, v$ es un circuito que comienza y termina en v. Suponga que $\pi: v, u, \ldots, v$ es el circuito más largo posible que comienza y termina en v. Como G no tiene un circuito de Euler, no se utiliza todas las aristas G en π. Sea G' la gráfica formada al eliminar las aristas de π en G. Como π es un circuito, al eliminar estas aristas se reduce el grado de cada vértice en 0 o 2; de modo que G' también es una gráfica donde todos sus vértices tienen grado par. La gráfica de G podría no ser conexa, pero alguna de sus partes sí lo es. Se elige la parte conexa más grande de G'. Esta parte debe tener un circuito de Euler π' ya que ciertamente tiene menos aristas que G, y se había elegido G con el menor número de aristas y sin un circuito de Euler.

Entonces, π' contiene a todos los vértices de G o existe algún vértice v que no está en π'. Pero v debe ser adyacente a algún v' en π', pues G es conexa y la arista $\{v, v'\}$ es una de las aristas eliminadas: es decir, $\{v, v'\}$ es una arista de π. En cualquier caso, algún vértice v' en π' es también vértice de π, y se puede construir un circuito mayor en G uniendo π y π' en v'. Pero esto es una contradicción, ya que π es el máximo circuito posible en G. Por tanto, no existe tal G. ●

Se ha demostrado que si G tiene vértices de grado impar, no es posible construir un circuito de Euler para G, pero puede ser posible determinar una trayectoria de Euler. En el análisis anterior se observa que un vértice de grado impar debe ser el inicio o el fin de cualquier trayectoria de Euler posible. Se tiene el siguiente teorema.

Teorema 2

(a) *Si una gráfica G tiene más de dos vértices de grado impar, entonces no puede existir una trayectoria de Euler en G.*

(b) *Si G es conexa y tiene exactamente dos vértices de grado impar, entonces existe una trayectoria de Euler en G. Cualquier trayectoria de Euler debe comenzar en un vértice de grado impar y terminar en el otro.*

Demostración: (a) Sean v_1, v_2, v_3 vértices de grado impar. Cualquier trayectoria de Euler posible debe salir (o llegar) a cada uno de los vértices v_1, v_2, v_3 sin poder regresar (o salir), ya que cada uno de estos vértices tiene grado impar. Uno de estos tres vértices podría ser el comienzo de la trayectoria de Euler y otro el final, pero esto deja al tercer vertice en un extremo de una arista sin recorrer. Por tanto, no existe una trayectoria de Euler.

(b) Sean u y v dos vértices de grado impar. Al agregar la arista $\{u, v\}$ a G se obtiene una gráfica conexa G' cuyos vértices tienen grado par. Por el teorema 1(b), existe un circuito de Euler π' en G'. Al eliminar $\{u, v\}$ de π' se obtiene una trayectoria de Euler que comienza en u (o v) y termina en v (o u). ●

Ejemplo 4. ¿Cuáles de las gráficas de las figuras 6.29, 6.30 y 6.31 tienen un circuito de Euler, una trayectoria de Euler pero no un circuito de Euler, o ninguno de éstos?

Solución: (a) En la figura 6.29, cada uno de los cuatro vértices tiene grado 3; así, por los teoremas 1 y 2, no existe un circuito ni una trayectoria de Euler.

(b) La gráfica de la figura 6.30 tiene exactamente dos vértices de grado impar. No existe un circuito de Euler, pero debe existir una trayectoria de Euler.

(c) En la figura 6.31, todos los vértices tienen grado par; así, la gráfica debe tener un circuito de Euler. ♦

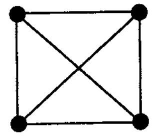


Figura 6.29

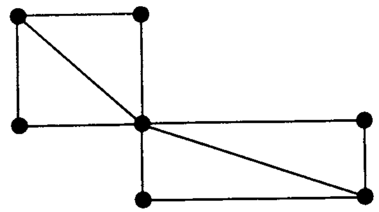


Figura 6.30

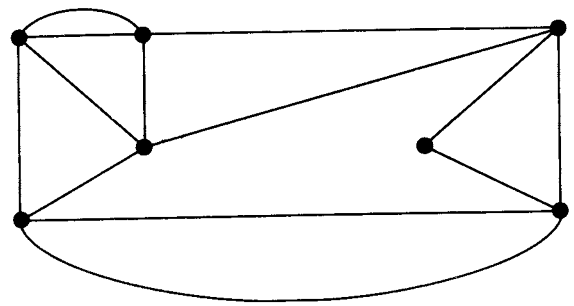


Figura 6.31

Ejemplo 5. Regrese al ejemplo 3. Observe que los cuatro vértices tienen grados 4, 4, 5 y 7, respectivamente. De modo que puede resolverse el problema mediante el teorema 2; es decir, existe una trayectoria de Euler. La figura 6.32 muestra una de éstas. ♦

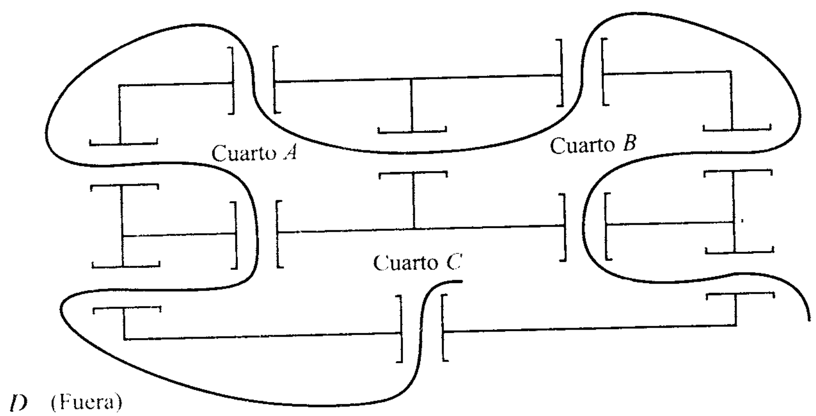


Figura 6.32

Los teoremas 1 y 2 son ejemplos de teoremas de existencia. Garantizan la existencia de un objeto de cierto tipo, pero no proporcionan información alguna para obtener el objeto. El teorema 2(b) muestra un indicio de cómo proceder. En la figura 6.33, una trayectoria de Euler debe comenzar (o terminar) en *B* y terminar (o comenzar) en *C*. Las trayectorias *B, A, D, C, A, B, C* y *B, C, A, B, A, D, C* son dos trayectorias de Euler para esta gráfica.

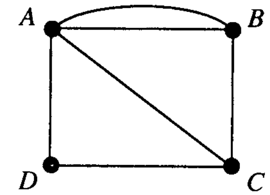


Figura 6.33

Se dará ahora un algoritmo para obtener un circuito de Euler para una gráfica conexa sin vértices de grado impar. Se necesita una definición adicional antes de comenzar el algoritmo. Una arista $\{v_i, v_j\}$ es un **puente** en una gráfica conexa de G si al eliminar $\{v_i, v_j\}$ se crea una gráfica disconexa. Por ejemplo, en la gráfica de la figura 6.4, $\{B, E\}$ es un puente.

Algoritmo de Fleury: Sea $G = (V, E, \gamma)$ una gráfica conexa con todos sus vértices de grado par.

PASO 1. Se elige un miembro v de V como vértice inicial para el circuito. Sea π: v el inicio de la trayectoria por construir.

PASO 2. Suponga que ya se ha construido π: $v, u, \ldots, w$. Si en w sólo existe una arista $\{w, z\}$, se extiende π a π: $v, u, \ldots, w, z$. Se elimina $\{w, z\}$ de E y w de V. Si en w existen varias aristas, se elige una que no sea un puente $\{w, z\}$. Extienda π a π: $v, u, \ldots, w, z$ y se elimina $\{w, z\}$ de E.

PASO 3. Repita el paso 2 hasta que no sobren aristas en E.

Fin del algoritmo

Ejemplo 6. Utilice el algoritmo de Fleury para construir un circuito de Euler para la gráfica de la figura 6.34.

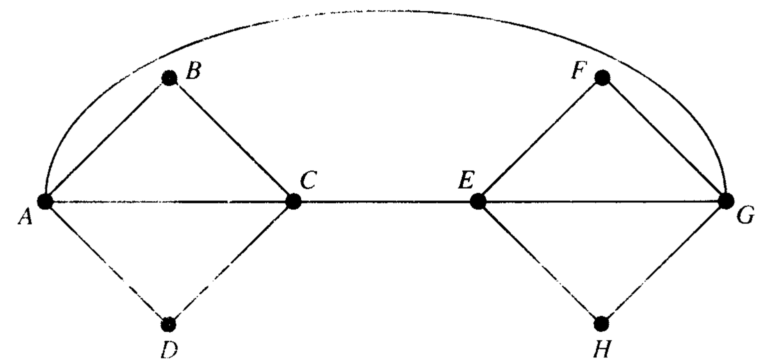


Figura 6.34

Solución: Según el paso 1, se puede comenzar en cualquier parte. Se elige el vértice *A* de manera arbitraria. La tabla 6.1 resume los resultados de la aplicación del paso 2.

Tabla 6.1

Ruta corriente	Arista siguiente	Razonamiento
π: A	$\{A, B\}$	Sin aristas desde A es un puente. Elija una sola.
π: A, B	$\{B, C\}$	Sólo una arista desde B permanece.
π: A, B, C	$\{C, A\}$	Sin aristas desde C es un puente. Elija una sola.
π: A, B, C, A	$\{A, D\}$	Sin arista desde A es un puente. Elija una sola.
π: A, B, C, A, D	$\{D, C\}$	Sin arista desde D permanece.
π: A, B, C, A, D, C	$\{C, E\}$	Sólo una arista desde C permanece.
π: A, B, C, A, D, C, E	$\{E, G\}$	Sin arista desde E es un puente. Elija una sola.
π: A, B, C, A, D, C, E, G	$\{G, F\}$	$\{A, G\}$ es un puente. Elija (G, F) o (G, H).
π: $A, B, C, A, D, C, E, G, F$	$\{F, E\}$	Sólo una arista de F permanece.
π: $A, B, C, A, D, C, E, G, F, E$	$\{E, H\}$	Sólo una arista de E permanece.
π: $A, B, C, A, D, C, E, G, F, E, H$	$\{H, G\}$	Sólo una arista de H permanece.
π: $A, B, C, A, D, C, E, G, F, E, H, G$	$\{G, A\}$	Sólo una arista de G permanece.
π: $A, B, C, A, D, C, E, G, F, E, H, G, A$		

Se ha numerado las aristas de la figura 6.35 en el orden de su elección al aplicar el paso 2. En varios lugares, se podría elegir de distintas formas. En general, si una gráfica tiene un circuito de Euler, seguramente tendrá varios circuitos de Euler diferentes. ◆

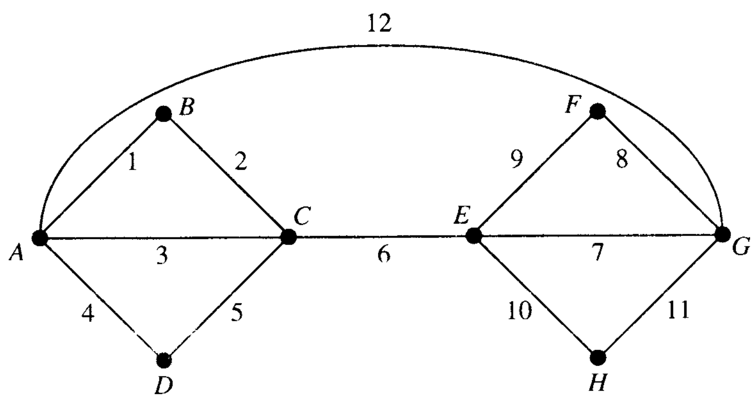


Figura 6.35

GRUPO DE EJERCICIOS 6.2

En los ejercicios 1 al 4, indique si la gráfica tiene un circuito de Euler, una trayectoria de Euler, o ninguno de éstos. Proporcione las razones de su elección.

1. (a)

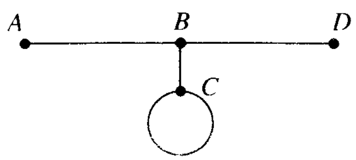


Figura 6.36

(b)

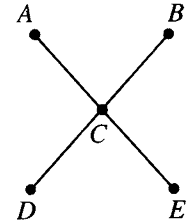


Figura 6.37

2. (a)

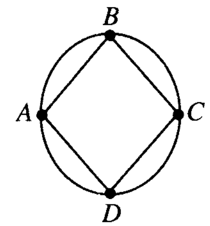


Figura 6.38

(b)

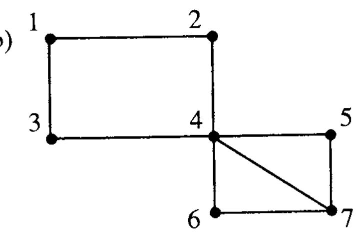


Figura 6.39

3. (a)

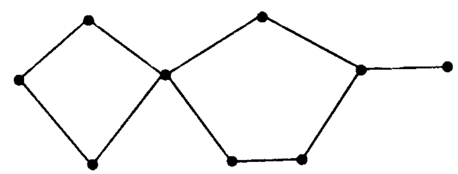


Figura 6.40

(b)

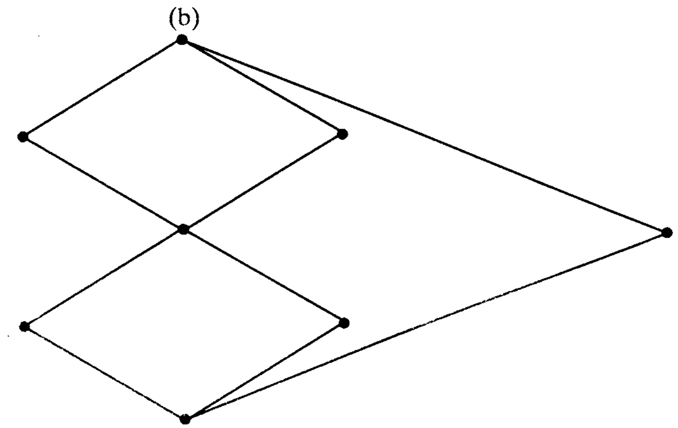


Figura 6.41

4. (a)

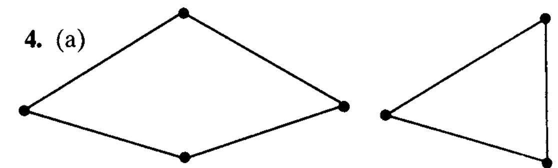


Figura 6.42

(b)

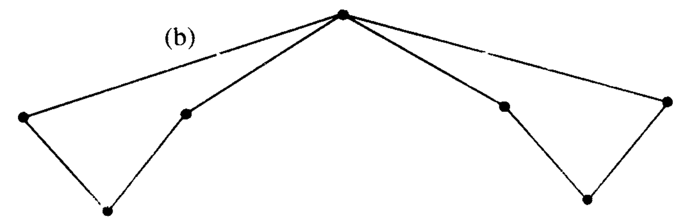


Figura 6.43

En los ejercicios 5 y 6, diga si es posible trazar la figura sin levantar el lápiz. Explique su razonamiento.

5.

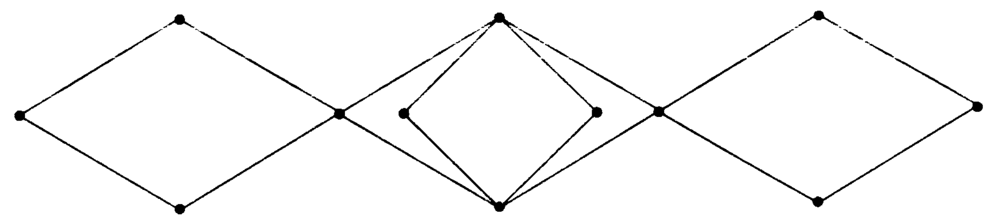


Figura 6.44

6.

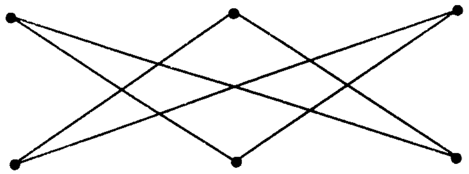


Figura 6.45

7. Utilice el algoritmo de Fleury para obtener un circuito de Euler para la gráfica de la figura 6.46.

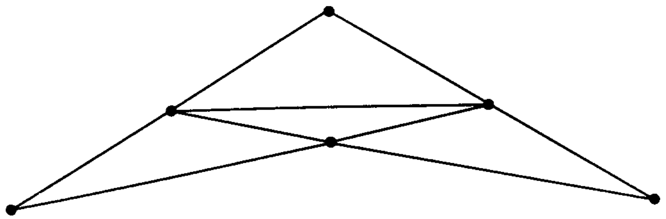


Figura 6.46

8. Utilice el algoritmo de Fleury para obtener un circuito de Euler para la gráfica de la figura 6.44.

9. Un museo de arte ha ordenado la exposición que actualmente presenta en cinco salas, como muestra la figura 6.47. ¿Existe alguna forma de recorrer la exposición de modo que usted pase por cada puerta sólo una vez? En ese caso, trace su recorrido.

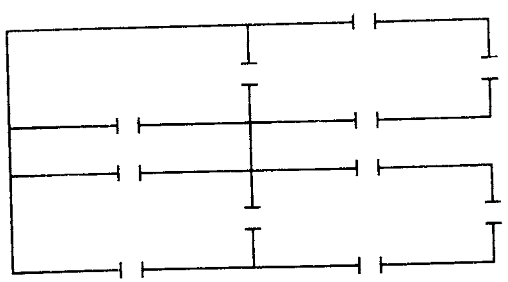


Figura 6.47

10. En la puerta de una mansión histórica, usted recibe una copia del plano de la casa (figura 6.48). ¿Es posible visitar cada cuarto de la casa pasando por cada puerta sólo una vez? Explique su razonamiento.

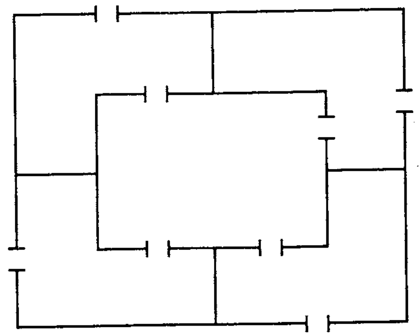


Figura 6.48

En los ejercicios 11 *al* 13 *(figuras* 6.49 *a la* 6.51*), no es posible construir un circuito de Euler para la gráfica dada. En cada una de ellas, muestre el mínimo número de aristas que debería recorrerse dos veces para visitar cada arista y regresar al vértice inicial.*

11.

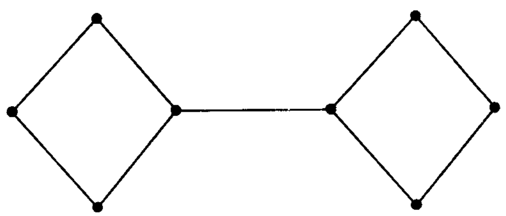


Figura 6.49

12.

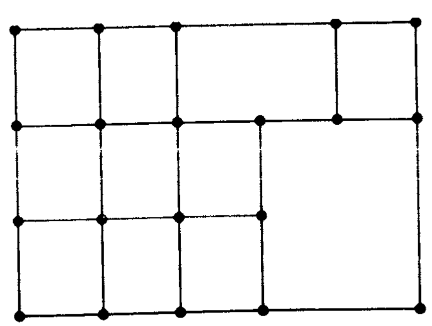


Figura 6.50

13.

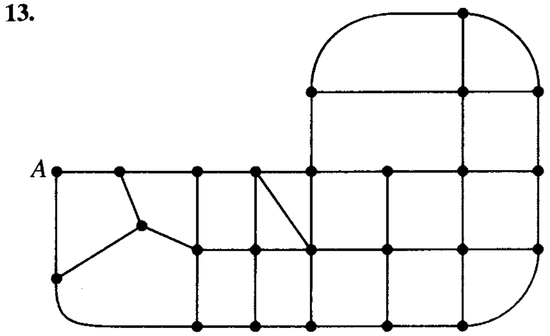


Figura 6.51

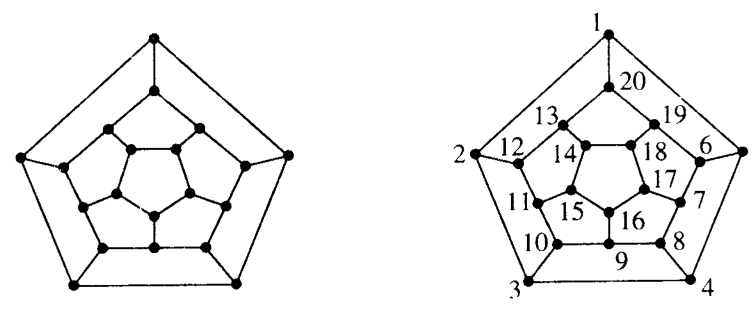
14. Utilice el algoritmo de Fleury para determinar un circuito de Euler para la versión modificada de la gráfica de la figura 6.50. Comience en la esquina superior izquierda.

15. Utilice el algoritmo de Fleury para determinar un circuito de Euler para la versión modificada de la gráfica de la figura 6.51. Comience en A.

6.3. Trayectorias y circuitos hamiltonianos

Ahora se verá a la segunda categoría de problemas de gráficas, donde la tarea consiste en visitar cada vértice sólo una vez, con la excepción del vértice inicial, si éste también debe ser el último vértice. Por ejemplo, tal trayectoria podría ser útil para alguien que deba proporcionar servicio a un conjunto de máquinas expendedoras de manera regular. Se puede representar cada máquina expendedora mediante un vértice.

Una **trayectoria hamiltoniana** es aquella que contiene cada vértice sólo una vez. Un **circuito hamiltoniano** es aquel que contiene cada vértice sólo una vez, excepto el primer vértice, que también es el último. Este tipo de trayectoria recibe el nombre del matemático Sir William Hamilton, quien desarrolló y comercializó un juego que consistía en una gráfica de madera en forma de dodecaedro regular, con las instrucciones para encontrar lo que se llama circuito hamiltoniano. La figura 6.52(a) muestra una versión plana de este sólido, con un circuito hamiltoniano (uno de muchos) mostrado en la figura 6.52(b) mediante los vértices numerados en forma consecutiva.



(a) (b)

Figura 6.52

Ejemplo 1. Considere la gráfica de la figura 6.53. La trayectoria a, b, c, d, e es una trayectoria hamiltoniana, pues contiene cada vértice sólo una vez. Sin embargo, no es difícil ver que no existe un circuito hamiltoniano para esta gráfica. Para la gráfica de la figura 6.54, la trayectoria A, D, C, B, A (puede elegirse cualquier arista de B a A) es un circuito hamiltoniano. En las figuras 6.55 y 6.56, no es posible tener una trayectoria hamiltoniana. (Verifique esta afirmación.) ◆

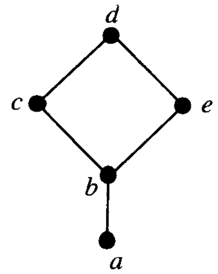


Figura 6.53

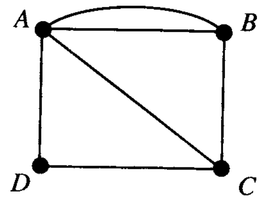


Figura 6.54

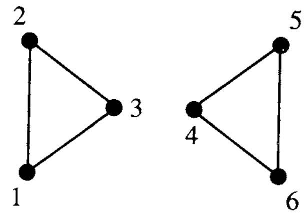


Figura 6.55

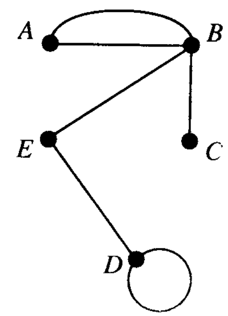


Figura 6.56

Ejemplo 2. Cualquier gráfica completa K_n tiene circuitos hamiltonianos. De hecho, si se parte de cualquier vértice, puede visitarse todos los demás en forma secuencial y en el orden deseado. ◆

Pueden surgir preguntas sobre cuestiones análogas a las correspondientes a las trayectorias y circuitos de Euler acerca de las trayectorias y circuitos hamiltonianos. ¿Es posible determinar si existe una trayectoria o circuito de Hamilton? Si debe existir una trayectoria o circuito hamiltoniano ¿existe una manera eficiente de determinarlo? Puede parecer sorprendente, considerando los teoremas 1 y 2 de la sección 6.2, que la primera cuestión acerca de las trayectorias y circuitos hamiltonianos no haya sido resuelta de manera completa hasta la fecha. Sin embargo, puede hacerse varias observaciones con base en los ejemplos.

Es claro que los bucles cerrados y las aristas múltiples no son muy útiles para determinar circuitos hamiltonianos, ya que no puede utilizarse los bucles cerrados, y sólo puede utilizarse una arista entre cualesquiera dos vértices. Así, se supondrá que cualquier gráfica mencionada no tiene bucles cerrados ni aristas múltiples.

Si una gráfica G de n vértices tiene un circuito hamiltoniano, entonces G debe tener al menos n aristas.

Ahora, se establecerá algunas respuestas parciales, las cuales establecen que si una gráfica G tiene "suficientes" aristas, entonces puede determinarse un circuito hamiltoniano.

Sea G una gráfica conexa con n vértices, $n > 2$, sin bucles cerrados ni aristas múltiples. De nuevo, éstos son enunciados de existencia; no proporcionan métodos para construir un circuito hamiltoniano.

Teorema 1. *G tiene un circuito hamiltoniano si para cualesquiera dos vértices u y v de G que no sean adyacentes, el grado de u más el grado de v es mayor o igual que n.* ●

Se omitirá la demostración de este resultado, pero mediante él puede demostrarse lo siguiente:

Corolario. *G tiene un circuito hamiltoniano si cada vértice tiene grado mayor o igual que $n/2$.*

Demostración: La suma de los grados de cualesquiera dos vértices es al menos $\frac{n}{2} + \frac{n}{2} = n$, por lo que se satisface la hipótesis del teorema 1. ●

Teorema 2. *Sea m el número de aristas de G. Entonces G tiene un circuito hamiltoniano si $m \geq \frac{1}{2}(n^2 - 3n + 6)$. (Recuerde que n es el número de vértices.)*

Demostración: Suponga que u y v son cualesquiera dos vértices no adyacentes de G. Se escribe $\deg(u)$ para el grado de u. Sea H la gráfica obtenida al eliminar u y v de G junto con las aristas que tienen a u o a v como extremos. Entonces H tiene $n - 2$ vértices y $m - \deg(u) - \deg(v)$ aristas (habría que eliminar una arista más si u y v fueran adyacentes). El número máximo de aristas que H podría tener es ${}_{n-2}C_2$ (véase la sección 3.2). Esto sucede cuando existe una arista que conecta a cada pareja distinta de vértices. Por tanto, el número de aristas de H es a lo más

$$ {}_{n-2}C_2 = \frac{(n-2)(n-3)}{2} \quad \text{o} \quad \frac{1}{2}(n^2 - 5n + 6). $$

Entonces, se tiene $m - \deg(u) - \deg(v) \leq \frac{1}{2}(n^2 - 5n + 6)$. Por lo tanto, $\deg(u) + \deg(v) \geq m - \frac{1}{2}(n^2 - 5n + 6)$. Por la hipótesis del teorema,

$$ \deg(u) + \deg(v) \geq \frac{1}{2}(n^2 - 3n + 6) - \frac{1}{2}(n^2 - 5n + 6) = n $$

Así, el resultado es consecuencia del teorema 1. ●

Ejemplo 3. Los recíprocos de los teoremas anteriores no son válidos; es decir, las condiciones dadas son suficientes, pero no necesarias, para la conclusión. Considere la gráfica representada por la figura 6.57. En este caso, n, el número de vértices, es igual a 8, cada vértice tiene grado 2 y $\deg(u) + \deg(v) = 4$ para cada pareja de vértices no adyacentes u y v. El número total de aristas también es 8. Por tanto, las premisas del teorema 1 y 2 no son satisfechas, pero ciertamente existen circuitos hamiltonianos para esta gráfica. ◆

El problema que se ha considerado tiene algunas variantes importantes. En un caso, las aristas pueden tener *pesos* que representen una distancia, un costo o algo similar. Entonces el problema es determinar un circuito hamiltoniano (o trayectoria) tal que la suma total de los pesos en la trayectoria sea mínima. Por ejemplo, los vértices podrían representar ciudades; las aristas, líneas de transporte; y el peso de una arista, el costo del viaje hacia la arista. Esta versión del problema se conoce como el problema del agente viajero. La sección 8.5 analiza otra categoría importante de problemas que implica gráficas con pesos asignados a las aristas.

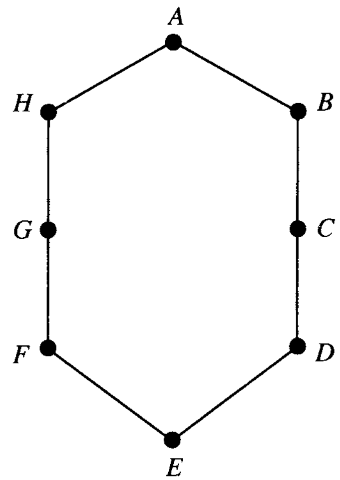


Figura 6.57

GRUPO DE EJERCICIOS 6.3

En los ejercicios 1 al 6 (figuras 6.58 a la 6.63), determine si la gráfica dada tiene un circuito hamiltoniano, una trayectoria pero no un circuito hamiltoniano, o ninguno de los dos. Si la gráfica tiene un circuito hamiltoniano, indique el circuito.

1.

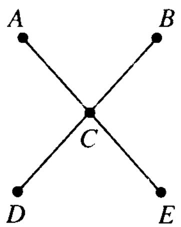


Figura 6.58

2.

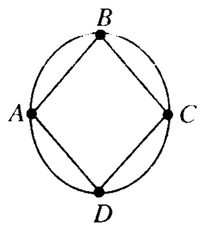


Figura 6.59

3.

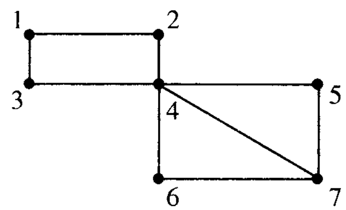


Figura 6.60

4.

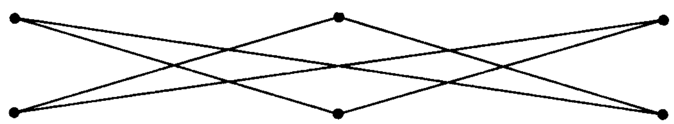


Figura 6.61

5.

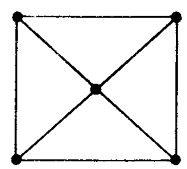


Figura 6.62

6.

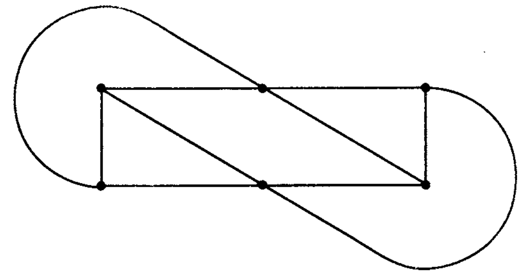


Figura 6.63

9.

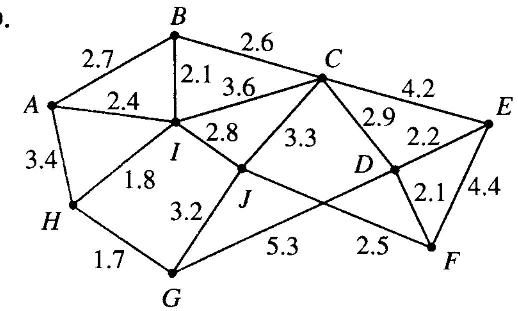


Figura 6.66

10.

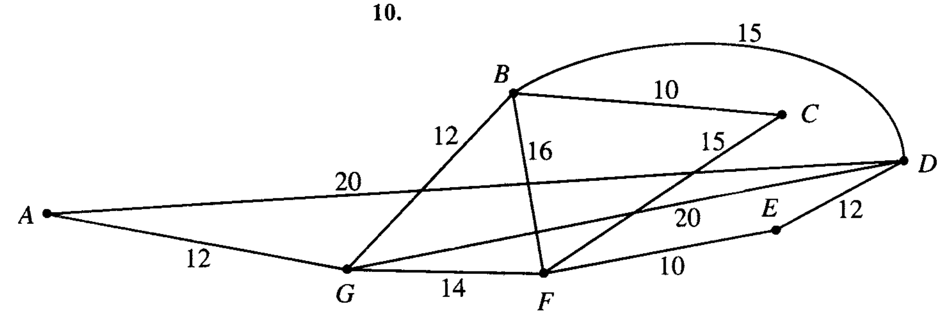


Figura 6.67

En los ejercicios 7 al 10 (figuras 6.64 a la 6.67), determine un circuito hamiltoniano para la gráfica dada.

7.

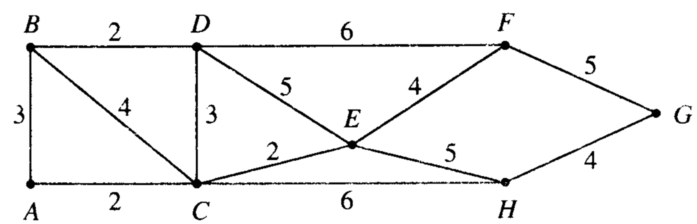


Figura 6.64

8.

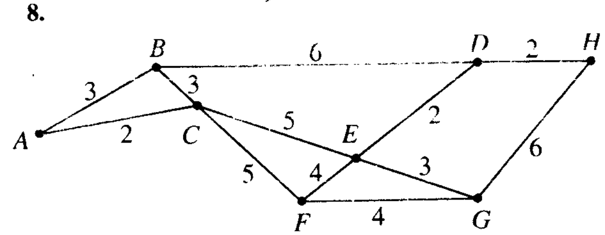


Figura 6.65

En los ejercicios 11 al 14, determine un circuito hamiltoniano de peso mínimo para la gráfica representada en la figura.

11. Figura 6.64.

12. Figura 6.65.

13. Figura 6.66.

14. Figura 6.67.

15. (a) Determine un circuito hamiltoniano de peso mínimo para la gráfica representada en la figura 6.64 si hay que comenzar y terminar en D.
(b) Determine un circuito hamiltoniano de peso mínimo para la gráfica representada en la figura 6.65 si hay que comenzar y terminar en F.

6.4. Coloración de gráficas

Suponga que $G = (V, E, \gamma)$ es una gráfica sin aristas múltiples y $C = \{c_1, c_2, \ldots, c_x\}$ es cualquier conjunto de x "colores". Cualquier función $f: V \to C$ es una **coloración de la gráfica G con x colores** (o utilizando los colores de C). Para cada vértice $v, f(v)$ es el color de v. Como por lo general se muestra una imagen de una gráfica, se piensa la coloración de manera intuitiva pintando cada vértice con un color de C. Sin embargo, los problemas de coloración de gráficas tienen varias aplicaciones prácticas, donde "color" puede tener casi cualquier significado. Por ejemplo, si la gráfica representa una red de ciudades conectadas entre sí, cada ciudad puede marcarse con el nombre de la línea aérea con más vuelos hacia y desde esa ciudad. En este caso, los vértices son las ciudades y los colores son los nombres de las líneas aéreas. Posteriormente se verá otros ejemplos.

Una coloración es **propia** si cualesquiera dos vértices adyacentes v y w tienen colores diferentes.

Ejemplo 1. Sea $C = \{r, w, b, y\}$, de modo que $x = 4$. La figura 6.68 muestra una gráfica G con una coloración propia dada por los colores de C en dos formas diferentes, una mediante tres colores de C y otra que utiliza los cuatro colores. Se muestra los colores como etiquetas, lo que ayuda a explicar por qué no se asigna nombres a los vértices. Existen muchas coloraciones propias de esta gráfica con tres o cuatro colores, pero no es difícil notar que esto no se puede hacer con dos o menos colores. (Experimente usted mismo para convencerse de que esto es cierto.) ♦

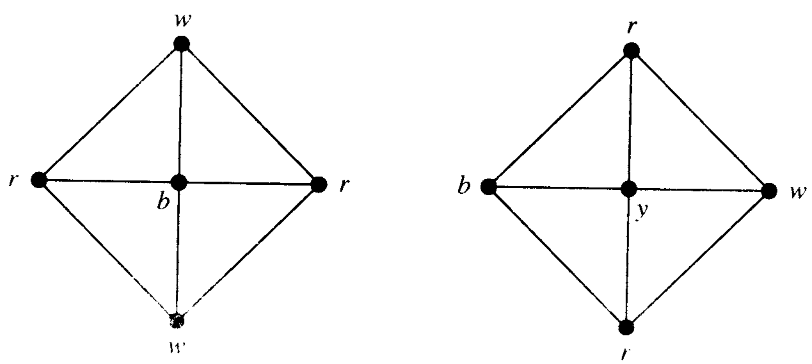


Figura 6.68

El número mínimo de colores necesarios para obtener una coloración propia de una gráfica G es el **número cromático de G**, denotado por $\chi(G)$. Para la gráfica G de la figura 6.68, el análisis lleva a creer que $\chi(G) = 3$.

De los muchos problemas que puede verse como problemas de coloración de gráficas, uno de los más antiguos es el problema de la coloración de mapas. Considere el mapa de la figura 6.69.

La coloración de un mapa es una forma de colorear cada región (país, estado, condado, provincia, etcétera) de modo que no existan dos regiones distintas que compartan una frontera común con el mismo color. El problema de coloración de un mapa consiste en determinar el menor número de colores que puede utilizarse. Se puede ver este caso como el problema de coloración propia de una gráfica, de la siguiente manera. Dado un mapa M, se

construye una gráfica G_M con un vértice para cada región y una arista que conecta cualesquiera dos vértices cuyas regiones correspondientes comparten una frontera común. Entonces, la coloración propia de G_M corresponde exactamente a la coloración de M.

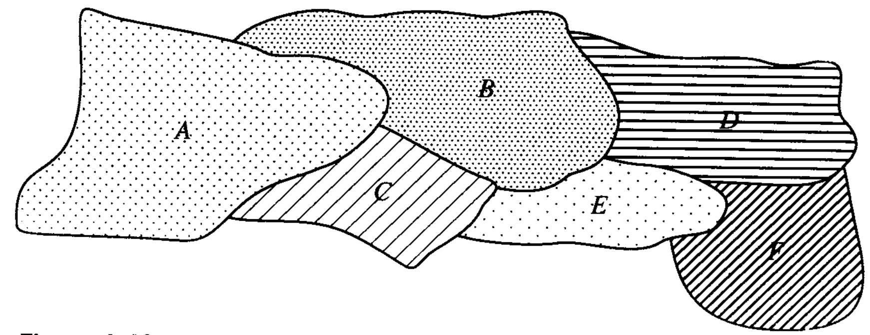


Figura 6.69

Ejemplo 2. Considere el mapa M de la figura 6.69. Entonces G_M está representada por la figura 6.70. ♦

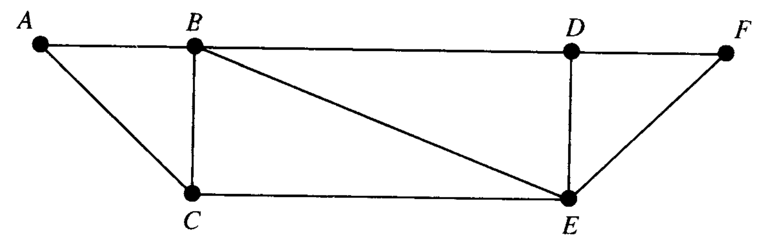


Figura 6.70

El problema de coloración de mapas data de mediados del siglo XIX y ha sido objeto activo de investigación en diversos momentos desde entonces. Se creía que bastaban cuatro colores para colorear cualquier mapa dibujado en un plano. En 1976 se demostró que esta conjetura era cierta, con la ayuda de cálculos realizados sobre casi 2000 configuraciones de gráficas. Aún no existe una demostración conocida que no dependa de una verificación por computadora.

La gráfica correspondiente a un mapa es **plana**, lo que significa que se puede trazar en un plano sin cruces de aristas, excepto por los vértices. La figura 6.70 ilustra la planaridad de la gráfica correspondiente al mapa de la figura 6.69. La gráfica K_5 no es plana, de modo que los problemas de coloración de gráficas son más generales que los problemas de coloración de mapas. En particular, se verá que se necesitan cinco colores para colorear K_5.

Los problemas referentes a la coloración de gráficas también surgen de problemas de conteo.

Ejemplo 3. Se desea guardar 15 diferentes alimentos en recipientes dentro de un único refrigerador. Algunos de ellos pueden conservarse juntos, pero otros alimentos deben guardarse por separado. Por ejemplo, las carnes frías y los quesos deben estar separados de las carnes blandas y los vegetales. Las manzanas, huevos y cebollas deben estar aislados o se contaminarían con otros alimentos. La mantequilla, margarina y queso crema pueden ser guardados juntos, pero deben estar separados de los alimentos con olores muy fuertes. Se puede construir una gráfica G de la siguiente manera. Se construye un vértice para cada alimento y se unen dos con una arista si deben ser guardados por separado en el refrigerador. Entonces $\chi(G)$ es el número mínimo de recipientes separados necesarios para guardar los 15 alimentos en forma adecuada. ◆

Se puede utilizar un método similar para calcular el número mínimo de anaqueles de laboratorio necesarios para almacenar sustancias químicas si hay que separar las sustancias que reaccionarían si fueran guardadas una junto a la otra.

Polinomios cromáticos

El problema de calcular $\chi(G)$ se encuentra íntimamente ligado con el problema de calcular el número de coloraciones propias diferentes de una gráfica G con un conjunto $C = \{c_1, c_2, \ldots, c_x\}$ de colores.

Si G es una gráfica y $x \geq 0$ es un entero, sea $P_G(x)$ el número de formas de obtener una coloración propia de G con x o menos colores. Como $P_G(x)$ es un número definido para cada x, se observa que P_G es una función. Lo que tal vez no sea tan obvio es que P_G es un polinomio en x. Se puede mostrar esto en general y se ve claramente en los ejemplos de esta sección. P_G es el **polinomio cromático** de G.

Ejemplo 4. Considere la gráfica lineal L_4 definida en la sección 6.1 y que aparece en la figura 6.9. Suponga que se tiene x colores. Puede colorearse el primer vértice con cualquier color. No importa cómo se haga, se puede colorear el segundo vértice con cualquier color distinto del elegido para el vértice 1. Por tanto, existen $x - 1$ opciones para el vértice 2. A continuación, se puede colorear el vértice 3 con cualquiera de los $x - 1$ colores no utilizados para el vértice 2. Un resultado análogo es válido para el vértice 4. Por el principio de multiplicación del conteo (sección 3.1), el número total de coloraciones propias es $x(x - 1)^3$. Así, $P_{L_4}(x) = x(x - 1)^3$. ◆

Véase del ejemplo 4 que $P_{L_4}(0) = 0$, $P_{L_4}(1) = 0$, y $P_{L_4}(2) = 2$. Por tanto, no existen coloraciones propias de L_4 que utilicen cero colores (obviamente) o un color, y existen dos que utilizan dos colores. A partir de esto se observa que $\chi(L_4) = 2$. Esta conexión es válida en general, por lo que se tiene el siguiente principio.

Si G es una gráfica sin aristas múltiples, y P_G es el polinomio cromático de G, entonces $\chi(G)$ es el menor entero positivo x tal que $P_G(x) \neq 0$.

Un argumento similar al dado en el ejemplo 4 muestra que para L_n, $n \geq 1$, $P_{L_n}(x) = x(x - 1)^{n-1}$. Así, por el principio anterior, $\chi(L_n) = 2$ para toda n.

Ejemplo 5. Para cualquier $n \geq 1$, considere la gráfica completa K_n definida en la sección 6.1. Suponga que de nuevo se puede utilizar x colores para colorear K_n. Si $x < n$, no es posible obtener una coloración propia. Así, sea $x \geq n$. Se puede colorear el vértice v_1 con cualquiera de los x colores. Para el vértice v_2, sólo restan $x - 1$, ya que v_2 está conectado con v_1. Sólo se puede colorear a v_3 con $x - 2$ colores, ya que v_3 está conectado con v_1 y con v_2 y no se puede utilizar de nuevo los colores de v_1 y v_2. De igual manera, sólo restan $x - 3$

colores para v_4, y así sucesivamente. Utilizando de nuevo el principio de multiplicación de conteo, se determina que $P_{K_n}(x) = x(x - 1)(x - 2) \cdots (x - n + 1)$. Esto muestra que $\chi(K_n) = n$. Observe que si al menos existen n colores, entonces $P_{K_n}(x)$ es el número de permutaciones de x objetos tomados de n en n (véase la sección 3.1). ◆

Suponga que una gráfica g no es conexa y que G_1 y G_2 son dos componentes de G. Esto significa que ningún vértice en G_1 está conectado con algún vértice en G_2. Así, cualquier coloración de G_1 se puede aparear con cualquier coloración de G_2. Esto puede extenderse a cualquier número de componentes, por lo que el principio de multiplicación de conteo proporciona el siguiente resultado.

Teorema 1. *Si G es una gráfica disconexa con componentes $G_1, G_2, \ldots, G_m$, entonces $P_G(x) = P_{G_1}(x)P_{G_2}(x) \cdots P_{G_m}(x)$, el producto de los polinomios cromáticos para cada componente.* ●

Ejemplo 6. Sea G la gráfica de la figura 6.6. Entonces G tiene dos componentes, cada una de las cuales es K_3. El polinomio cromático de K_3 es $x(x - 1)(x - 2)$, $x \geq 3$. Así, por el teorema 1, $P_G(x) = x^2(x - 1)^2(x - 2)^2$. Se observa que $\chi(G) = 3$ y que el número de formas distintas de colorear G mediante tres colores es $P_G(3) = 36$. Si x es 4, entonces el número total de coloraciones propias de G es $4^2 \cdot 3^2 \cdot 2^2$ o 576. ◆

Ejemplo 7. Considere la gráfica discreta D_n de la sección 6.1, con n vértices y sin aristas. Las n componentes son puntos simples. El polinomio cromático de un punto simple es x, de modo que, por el teorema 1, $P_{D_n}(x) = x^n$. Así, $\chi(D_n) = 1$ como se puede ver también directamente. ◆

Existe un teorema útil para calcular polinomios cromáticos mediante las construcciones de subgráficas y gráficas cociente de la sección 6.1. Sea $G = \{V, E, \gamma\}$ una gráfica sin aristas múltiples, y sea $e \in E$, es decir, $e = \{a, b\}$. Como en la sección 6.1, sea G_e la subgráfica de G obtenida al eliminar e, y sea G^e la gráfica cociente de G obtenida al unir los extremos de e. Entonces se obtiene el siguiente resultado.

Teorema 2. *Con la notación anterior y utilizando x colores.*

$$P_G(x) = P_{G_e}(x) - P_{G^e}(x)$$

Demostración: Considérese todas las coloraciones propias de G_e. Existen dos tipos, aquellas en que a y b tiene diferentes colores y aquellas en que a y b tienen el mismo color. Ahora bien, una coloración del primer tipo es también una coloración propia para G, ya que a y b están conectadas en G, y esta coloración les proporciona colores diferentes. Por otro lado, una coloración de G_e del segundo tipo corresponde a una coloración propia de G^e. De hecho, como a y b están combinados en G^e, deben tener el mismo color ahí. Los demás vértices de G_e tienen las mismas conexiones que en G. Así, se ha demostrado que $P_{G_e}(x) = P_G(x) + P_{G^e}(x)$ o $P_G(x) = P_{G_e}(x) - P_{G^e}(x)$. ●

Ejemplo 8. Calcule $P_G(x)$ para la gráfica G de la figura 6.71, utilizando la arista e. Entonces G^e es K_3 y G_e tiene dos componentes, una dada por un único punto y la otra es K_3. Por el teorema 1, $P_{G_e}(x) = x \cdot x(x - 1)(x - 2) = x^2(x - 1)(x - 2)$, si $x \geq 2$. Además,

$P_{G^e}(x) = x(x-1)(x-2)$. Por tanto, por el teorema 2, se observa que $P_G(x) = x^2(x-1)(x-2) - x(x-1)(x-2)$ o $x(x-1)^2(x-2)$. Es claro que $P_G(1) = P_G(2) = 0$ y $P_G(3) = 12$. Esto muestra que $\chi(G) = 3$. ◆

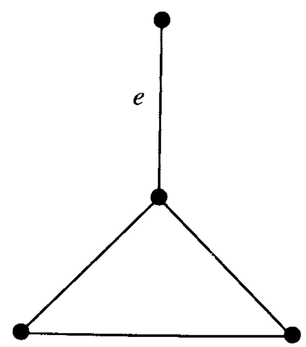


Figura 6.71

GRUPO DE EJERCICIOS 6.4

En los ejercicios 1 al 4 (figuras 6.72 a la 6.75), construya una gráfica para el mapa dado como muestra en el ejemplo 2.

1.

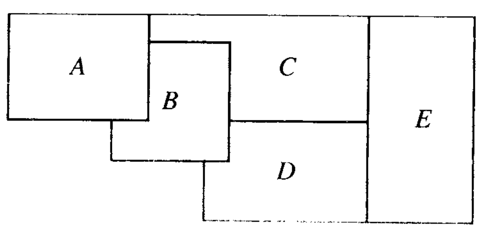


Figura 6.72

2.

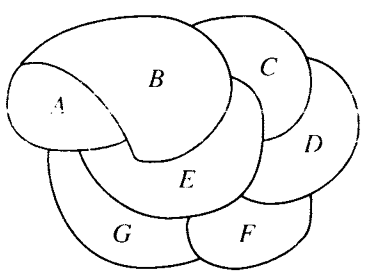


Figura 6.73

3.

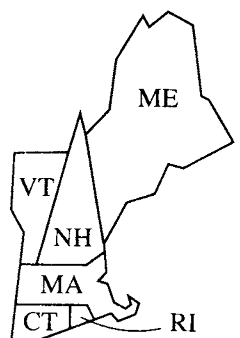


Figura 6.74

4.

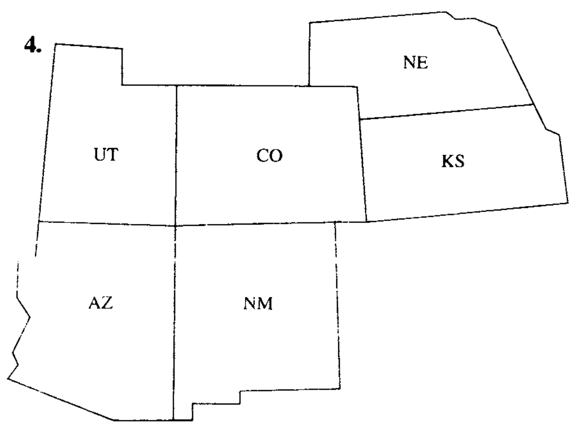


Figura 6.75

En los ejercicios 5 y 6 (figuras 6.76 a la 6.79), determine el número cromático de la gráfica por inspección.

5. (a)

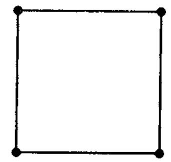


Figura 6.76

(b)

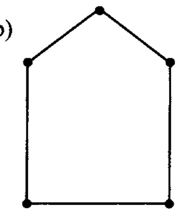


Figura 6.77

6. (a)

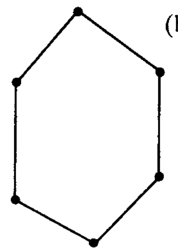


Figura 6.78

(b)

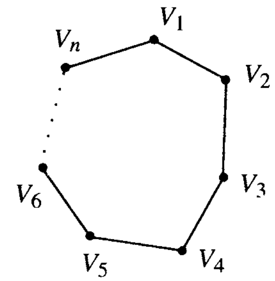


Figura 6.79

En los ejercicios 7 al 10 (figuras 6.80 a la 6.83), determine el polinomio cromático P_G para la gráfica dada y utilice P_G para determinar $\chi(G)$.

7.

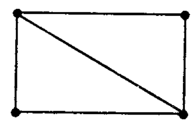


Figura 6.80

8.

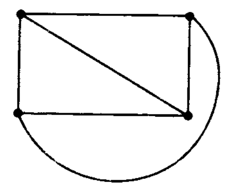


Figura 6.81

9.

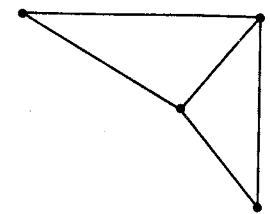


Figura 6.82

10.

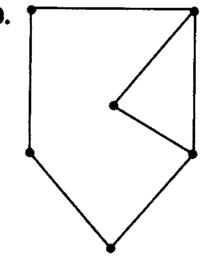


Figura 6.83

11. Determine P_G y $\chi(G)$ para la gráfica G del mapa del ejercicio 1.

12. Determine P_G y $\chi(G)$ para la gráfica G del mapa del ejercicio 3.

13. Determine P_G y $\chi(G)$ para la gráfica G del mapa dada en el ejercicio 5(a). ¿Confirma el resultado su respuesta original para el ejercicio 5(a)?

14. Determine P_G y $\chi(G)$ para la gráfica G del mapa del ejercicio 4. Considere el teorema 2 para resolverlo.

15. Demuestre, mediante inducción matemática, que $P_{L_n}(x) = x(x-1)^{n-1}$, $n > 1$.

IDEAS CLAVE PARA REPASO

- Gráfica: $G = (V, E, \gamma)$, donde V es un conjunto finito de objetos, llamados vértices, E es un conjunto de objetos, llamados aristas (lados o arcos), y γ es una función que asigna a cada arista un subconjunto de dos elementos de V.
- Grado de un vértice: número de aristas en el vértice.
- Vértices adyacentes: pareja de vértices que definen a una arista.
- Trayectoria: lista de vértices, de modo que los vértices consecutivos definen aristas y ninguna arista se utiliza más de una vez.
- Circuito: trayectoria que comienza y termina en el mismo vértice.
- Trayectoria o circuito simple: véase la página 199
- Gráfica conexa: Existe una trayectoria de cualquier vértice a otro.
- Subgráfica: véase la página 200.

- Trayectoria (o circuito) de Euler: trayectoria (circuito) que contiene todas las aristas de la gráfica sólo una vez.
- Teorema: (a) Si una gráfica G tiene un vértice de grado impar, entonces no puede existir un circuito de Euler en G. (b) Si G es una gráfica conexa y todos los vértices tienen grado par, entonces existe un circuito de Euler en G.
- Teorema: (a) Si una gráfica G tiene más de dos vértices de grado impar, entonces no puede existir una trayectoria de Euler en G. (b) Si G es conexa y tiene exactamente dos vértices de grado impar, existe una trayectoria de Euler en G.
- Puente: arista cuya eliminación haría que la gráfica fuera disconexa.
- Algoritmo de Fleury: véase la página 209.
- Trayectoria hamiltoniana: trayectoria que incluye cada vértice de la gráfica sólo una vez.
- Circuito hamiltoniano: circuito que incluye cada vértice sólo una vez, excepto el primer vértice, que también es el último.
- Teorema: Sea G una gráfica con n vértices, sin ciclos ni aristas múltiples, $n > 2$. Si para cualesquiera dos vértices u y v de G, el grado de u más el grado de v es al menos n, entonces G tiene un circuito hamiltoniano.
- Teorema: Sea G una gráfica con n vértices, sin ciclos o aristas múltiples, $n > 2$. Si el número de aristas en G es al menos $\frac{1}{2}(n^2 - 3n + 6)$, entonces G tiene un circuito hamiltoniano.
- Coloración de una gráfica utilizando x colores: véase la página 218.
- Coloración propia de una gráfica: las aristas adyacentes tienen colores diferentes.
- Número cromático de una gráfica G, $\chi(G)$: el número mínimo de colores necesarios para una coloración propia de G.
- Gráfica plana: gráfica que puede trazarse en un plano sin aristas que se crucen.
- Polinomio cromático de una gráfica G, P_G: número de coloraciones propias de G en términos del número de colores disponibles.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes ejercicios, escriba el programa o subrutina solicitado en seudocódigo (como se describe en el apéndice A) o en el lenguaje de programación que usted conozca. Verifique su código, usando lápiz y papel o en una computadora.

En cada uno de estos ejercicios, suponga que se define una gráfica por $G = (V, E, \gamma)$.

1. Escriba una función tal que, dado G y un elemento v de V, regrese el grado de v.

2. Escriba una subrutina que determine si dos vértices de G son adyacentes.

3. Escriba el código del algoritmo de Fleury.

4. Escriba una subrutina que tenga como entrada una lista de vértices de G e informe si la lista define o no una trayectoria válida que sea una trayectoria hamiltoniana.

5. Modifique el código del ejercicio 4 para que la subrutina sea válida para circuitos hamiltonianos.

CAPÍTULO 7

RELACIONES Y ESTRUCTURAS DE ORDEN

Requisito previo: Capítulo 4

En este capítulo se estudia los conjuntos parcialmente ordenados, incluyendo las retículas y las álgebras booleanas. Estas estructuras son útiles en la teoría de conjuntos, el álgebra, la ordenación y la búsqueda, y, particularmente en el caso de las álgebras booleanas, en la construcción de representaciones lógicas para los circuitos computacionales.

7.1. Conjuntos parcialmente ordenados

Una relación R en un conjunto A es un **orden parcial** si R es reflexiva, antisimétrica y transitiva. El conjunto A, junto con el orden parcial R, es un **conjunto parcialmente ordenado**, y se denotará este conjunto por (A, R). Si no existe posibilidad de confusión acerca del orden parcial, será posible referirse al conjunto parcialmente ordenado como A, en vez de (A, R).

Ejemplo 1. Sea A una colección de subconjuntos de un conjunto S. La relación $\subseteq$ de inclusión de conjuntos es un orden parcial en A, de modo que $(A, \subseteq)$ es un conjunto parcialmente ordenado. ◆

Ejemplo 2. Sea Z^+ el conjunto de enteros positivos. La relación usual $\leq$ (menor o igual que) es un orden parcial en Z^+, como $\geq$ (mayor o igual que). ◆

Ejemplo 3. La relación de divisibilidad ($a\ R\ b$ si y sólo si $a \mid b$) es un orden parcial en Z^+. ◆

Ejemplo 4. Sea $\mathcal{R}$ el conjunto de todas las relaciones de equivalencia en un conjunto A. Como $\mathcal{R}$ consta de subconjuntos de $A \times A$, $\mathcal{R}$ es un conjunto parcialmente ordenado bajo el orden parcial de contención de conjuntos. Si R y S son relaciones de equivalencia en A, puede expresarse la misma propiedad en notación relacional como sigue.

$$R \subseteq S \text{ si y sólo si } x\ R\ y \quad \text{implica} \quad x\ S\ y \text{ para toda } x, y \text{ en } A.$$

Entonces $(\mathcal{R}, \subseteq)$ es un conjunto parcialmente ordenado. ◆

Ejemplo 5. La relación $<$ en Z^+ no es un orden parcial, ya que no es reflexiva. ◆

Ejemplo 6. Sea R un orden parcial en un conjunto A, y sea R^{-1} la relación inversa de R. Entonces R^{-1} es también un orden parcial. Para ver esto, hay que recordar las caracterizaciones de las propiedades reflexiva, antisimétrica y transitiva proporcionadas en la sección 4.4. Si R tiene estas tres propiedades, entonces $\Delta \subseteq R$, $R \cap R^{-1} \subseteq \Delta$ y $R^2 \subseteq R$. Se utiliza los inversos y se obtiene $\Delta = \Delta^{-1} \subseteq R^{-1}$, $R^{-1} \cap (R^{-1})^{-1} = R^{-1} \cap R \subseteq \Delta$ y $(R^{-1})^2 \subseteq R^{-1}$, así, por la sección 4.4, R^{-1} es reflexiva, antisimétrica y transitiva. Entonces, R^{-1} es también un orden parcial. El conjunto parcialmente ordenado (A, R^{-1}) es el **dual** del conjunto parcialmente ordenado (A, R) y el orden parcial R^{-1} es el **dual** del orden parcial R. ◆

Los órdenes parciales más conocidos son las relaciones $\leq$ y $\geq$ en Z y $\mathbb{R}$. Por esta razón, cuando se habla en general de un orden parcial R sobre un conjunto A, se utilizará con frecuencia los símbolos $\leq$ y $\geq$ para R. Esto hace a las propiedades de R más simples y fáciles de recordar. Así, el lector puede ver que se utilizará el símbolo $\leq$ para diversos órdenes parciales en conjuntos diferentes. Esto no quiere decir que estas relaciones sean todas la misma o que tienen que ver con la relación familiar $\leq$ en Z o $\mathbb{R}$. Si es absolutamente necesario distinguir entre los órdenes parciales, también se utilizará símbolos como $\leq_1$, $\leq'$, $\geq_1$, $\geq'$, etcétera, para denotar órdenes parciales.

Se continuará empleando la siguiente convención. Si $(A, \leq)$ es un conjunto parcialmente ordenado, siempre se utilizará el símbolo $\geq$ para el orden parcial $\leq^{-1}$, por lo que $(A, \geq)$ será el conjunto parcialmente ordenado dual. De manera similar, el dual del conjunto parcialmente ordenado $(A, \leq_1)$ será $(A, \geq_1)$ y el dual del conjunto parcialmente ordenado $(B, \leq')$ será $(B, \geq')$. De nuevo, esta convención recuerda los conjuntos parcialmente ordenados duales familiares $(Z, \leq)$ y $(Z, \geq)$, así como los conjuntos parcialmente ordenados $(\mathbb{R}, \leq)$ y $(\mathbb{R}, \geq)$.

Si $(A, \leq)$ es un conjunto parcialmente ordenado, los elementos a y b de A son **comparables** si

$$a \leq b \quad \text{o} \quad b \leq a.$$

Observe que en un conjunto parcialmente ordenado, cada pareja de elementos no necesita ser comparable. Por ejemplo, considere el conjunto parcialmente ordenado del ejemplo 3. Los elementos 2 y 7 no son comparables, ya que $2 \nmid 7$ y $7 \nmid 2$. Así la palabra "parcial" en un conjunto parcialmente ordenado significa que algunos elementos podrían no ser comparables. Si cada pareja de elementos en un conjunto parcialmente ordenado A es comparable, se dirá que A es un conjunto **linealmente ordenado**, y el orden parcial es un **orden lineal**. También se dice que A es una **cadena**.

Ejemplo 7. El conjunto parcialmente ordenado del ejemplo 2 es linealmente ordenado. ◆

El siguiente teorema resulta útil en ciertas ocasiones, ya que muestra la forma de construir un nuevo conjunto parcialmente ordenado a partir de dos conjuntos parcialmente ordenados dados.

Teorema 1. *Si $(A, \leq)$ y $(B, \leq)$ son conjuntos parcialmente ordenados, entonces $(A \times B, \leq)$ es un conjunto parcialmente ordenado, con el orden parcial $\leq$ definido por*

$$(a, b) \leq (a', b') \qquad \text{si } a \leq a' \text{ en } A \quad \text{y} \quad b \leq b' \text{ en } B.$$

Observe que se utiliza el símbolo $\leq$ para denotar tres órdenes parciales distintos. El lector podrá determinar con facilidad el orden del que se trate en cualquier momento.

Demostración: Si $(a, b) \in A \times B$, entonces $(a, b) \leq (a, b)$, ya que $a \leq a$ en A y $b \leq b$ en B; de ese modo $\leq$ satisface la propiedad reflexiva en $A \times B$. Ahora supóngase que $(a, b) \leq (a', b')$ y $(a', b') \leq (a, b)$, donde a y $a' \in A$ y b y $b' \in B$. Entonces

$$a \leq a' \quad \text{y} \quad a' \leq a \qquad \text{en } A$$

y

$$b \leq b' \quad \text{y} \quad b' \leq b \qquad \text{en } B.$$

Como A y B son conjuntos parcialmente ordenados, la antisimetría de los órdenes parciales en A y B implica que

$$a = a' \quad \text{y} \quad b = b'.$$

Por lo tanto, $\leq$ satisface la propiedad antisimétrica en $A \times B$

Por último, supóngase que

$$(a, b) \leq (a', b') \quad \text{y} \quad (a', b') \leq (a'', b''),$$

donde $a, a', a'' \in A$ y $b, b', b'' \in B$. Entonces

$$a \leq a' \quad \text{y} \quad a' \leq a'',$$

de modo que $a \leq a''$, por la propiedad transitiva del orden parcial en A. De manera análoga,

$$b \leq b' \quad \text{y} \quad b' \leq b'',$$

de modo que $b \leq b''$, por la propiedad transitiva del orden parcial en B. Por lo tanto,

$$(a, b) \leq (a'', b'').$$

En consecuencia, la propiedad transitiva es válida para el orden parcial en $A \times B$, y se concluye que $A \times B$ es un conjunto parcialmente ordenado. ●

El orden parcial $\leq$ definido anteriormente en el producto cartesiano $A \times B$ es el **orden parcial producto**.

Si $(A, \leq)$ es un conjunto parcialmente ordenado, se dice que $a < b$ si $a \leq b$, pero $a \neq b$. Supóngase ahora que $(A, \leq)$ y $(B, \leq)$ son conjuntos parcialmente ordenados. En el teorema 1 se define el orden parcial producto en $A \times B$. Se define otro orden parcial útil en $A \times B$, denotado por $\prec$, como sigue:

$$(a, b) \prec (a', b') \quad \text{si } a < a' \quad \text{o} \quad \text{si } a = a' \text{ y } b \leq b'.$$

Este orden es llamado **lexicográfico**, u orden de "diccionario". El orden de los elementos en la primera coordenada domina, excepto en el caso de "empates", cuando la atención pasa a la segunda coordenada. Si $(A, \leq)$ y $(B, \leq)$ son conjuntos linealmente ordenados, entonces el orden lexicográfico $\prec$ en $A \times B$ también es un orden lineal.

Ejemplo 8. Sea $A = \mathbb{R}$, con el orden usual $\leq$. Entonces el plano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ puede tener un orden lexicográfico. La figura 7.1 ilustra esto. Se observa que el plano es ordenado linealmente por el orden lexicográfico. Cada recta vertical tiene el orden usual, y los puntos en una recta son menores que cualesquiera de los puntos en una recta más a la derecha. Así, en la figura 7.1, $p_1 \prec p_2, p_1 \prec p_3$ y $p_2 \prec p_3$. ◆

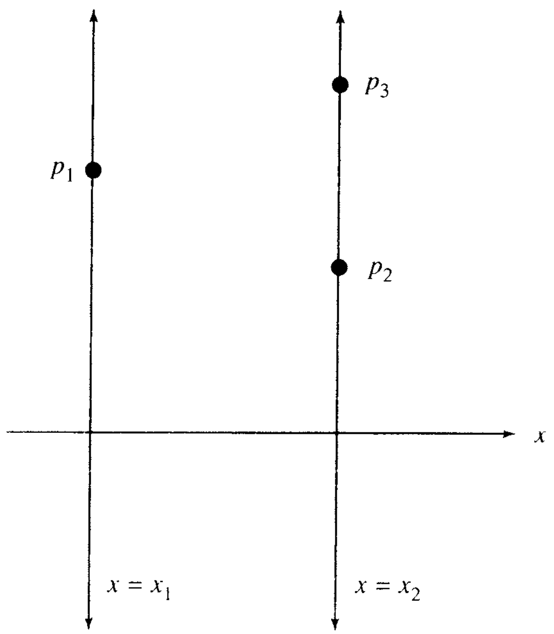


Figura 7.1

El orden lexicográfico se puede extender fácilmente a los productos cartesianos $A_1 \times A_2 \times \cdots \times A_n$ como sigue:

$$(a_1, a_2, \ldots, a_n) \prec (a_1', a_2', \ldots, a_n') \quad \text{si y sólo si}$$
$a_1 < a_1'$ o
$a_1 = a_1'$ y $a_2 < a_2'$ o

$a_1 = a_1', a_2 = a_2'$ y $a_3 < a_3'$ o . . .
$a_1 = a_1', a_2 = a_2', \ldots, a_{n-1} = a_{n-1}'$ y $a_n \leq a_n'$.

Así, la primera coordenada domina, excepto para la igualdad, en cuyo caso se considera la segunda coordenada. Si de nuevo se cumple la igualdad, se prosigue con la siguiente coordenada, y así sucesivamente.

Ejemplo 9. Sea $S = \{a, b, \ldots, z\}$ el alfabeto ordinario, ordenado linealmente en la forma usual ($a \leq b, b \leq c, \ldots, y \leq z$). Entonces, es posible identificar $S^n = S \times S \times \cdots \times S$ (n factores) con el conjunto de todas las palabras de longitud n. El orden lexicográfico en S^n tiene la propiedad de que si $w_1 \prec w_2$ ($w_1, w_2 \in S^n$), entonces w_1 debe preceder a w_2 en un diccionario. Este hecho justifica el nombre del orden.

Así, *parque* $\prec$ *parte*, *heno* $\prec$ *hipo*, *alas* $\prec$ *olas*. Esto último es válido pues $a < o$; el segundo caso se debe a que $h = h$, $e < i$; y el primero es cierto, pues $p = p$, $a = a$, $r = r$, $k < t$. ◆

Si S es un conjunto parcialmente ordenado, es posible extender el orden lexicográfico a S^* (véase la sección 1.3) de la manera siguiente.

Si $x = a_1a_2 \cdots a_n$ y $y = b_1b_2 \cdots b_k$ están en S^* con $n \leq k$, se dice que $x \prec y$ si $(a_1, \ldots, a_n) \prec (b_1, \ldots, b_n)$ en S^n bajo el orden lexicográfico de S^n. En otras palabras, se recorta a la longitud de la palabra más corta y después se compara.

En el párrafo anterior, se utilizó el hecho de que la n-ada $(a_1, a_2, \ldots, a_n) \in S^n$, y la cadena $a_1a_2 \cdots a_n \in S^*$ son realmente la misma sucesión de longitud n, escrita con dos notaciones diferentes. Las notaciones difieren por razones históricas, y serán utilizadas de manera indistinta, según el contexto.

Ejemplo 10. Sea S $\{a, b, \ldots, z\}$, ordenado de manera usual. Entonces S^* es el conjunto de todas las "palabras" posibles de cualquier longitud, aunque la palabra puede o no tener sentido.

Así, se tiene que

$$\textit{ayuda} \prec \textit{ayudando}$$

en S^*, ya que

$$\textit{ayuda} \prec \textit{ayuda}$$

en S^5. Del mismo modo,

$$\textit{ayúdame} \prec \textit{ayudamos}$$

ya que

$$\textit{ayúdame} \prec \textit{ayudamo}$$

en S^7. Como muestra el ejemplo

$$\textit{ayuda} \prec \textit{ayudando}$$

este orden incluye el *orden prefijo*; es decir, cualquier palabra es mayor que todos sus prefijos (partículas iniciales con significado, de una palabra). Ésta es también la forma de presentar las palabras en el diccionario. Así, de nuevo se obtiene el orden de diccionario, pero esta vez para palabras de cualquier longitud finita. ◆

Como un orden parcial es una relación, es posible analizar el digrafo de cualquier orden parcial sobre un conjunto finito. Se encontrará que es posible representar los digrafos de los órdenes parciales de manera más sencilla que como se hizo en el caso de las relaciones generales. El siguiente teorema proporciona el primer resultado en esta dirección.

Teorema 2. *El digrafo de un orden parcial no tiene ciclos de longitud mayor que* 1.

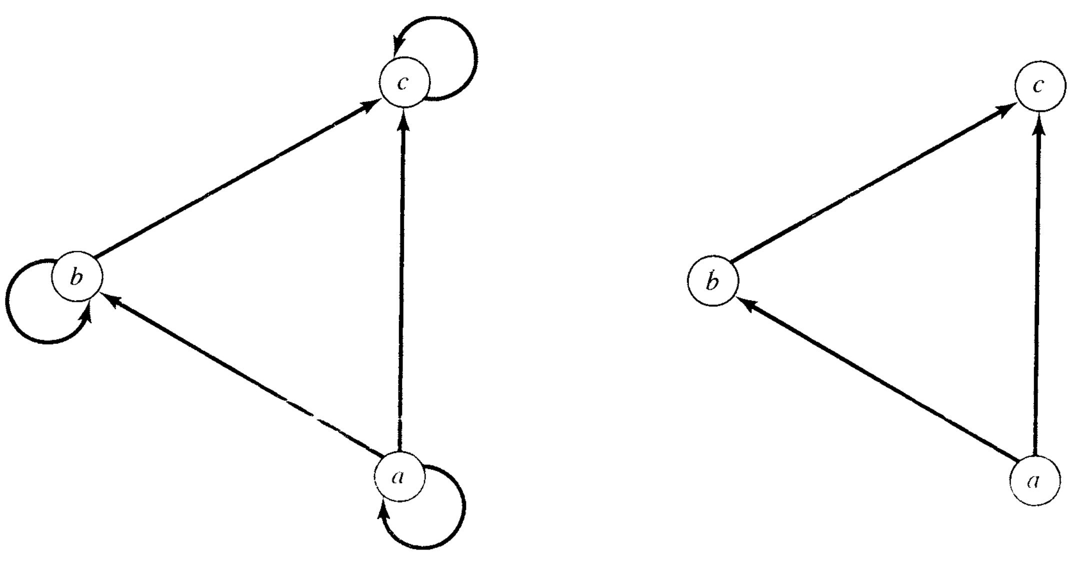
Demostración: Suponga que el digrafo del orden parcial $\leq$ en el conjunto A contiene un ciclo de longitud $n \geq 2$. Entonces existen distintos elementos $a_1, a_2, \ldots, a_n \in A$ tales que

$$a_1 \leq a_2, a_2 \leq a_3, \ldots, a_{n-1} \leq a_n, a_n \leq a_1.$$

Por la transitividad del orden parcial, utilizada $n - 1$ veces, $a_n \leq a_1$. Por antisimetría, $a_n \leq a_1$ y $a_1 \leq a_n$ implican $a_n = a_1$, lo cual contradice la hipótesis de que $a_1, a_2, \ldots, a_n$ son distintos. ●

Diagramas de Hasse

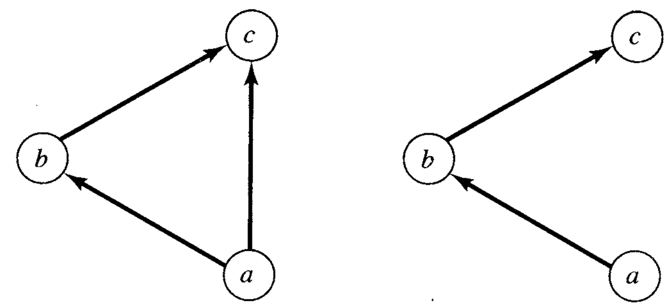
Sea A un conjunto finito. El teorema 2 ha mostrado que el digrafo de un orden parcial en A sólo tiene ciclos de longitud 1. De hecho, como un orden parcial es reflexivo, cada vértice en el digrafo del orden parcial está contenido en un ciclo de longitud 1. Para simplificar las cosas, se eliminará todos estos ciclos del digrafo. Así, el digrafo de la figura 7.2(a) se dibujaría como en la figura 7.2(b).



(a) (b)

Figura 7.2

También se eliminará las aristas implicadas por la propiedad transitiva. Así, si $a \leq b$ y $b \leq c$, esto implica que $a \leq c$. En este caso, se omite la arista de a a c; sin embargo, sí se traza las aristas de a a b y de b a c. Por ejemplo, el digrafo de la figura 7.3(a) se trazaría como en la figura 7.3(b). También se convino en trazar el digrafo de un orden parcial de modo que todas las aristas apunten hacia arriba, para omitir las flechas de las aristas. Por último, se reemplaza los círculos que representan a los vértices por puntos. Así, el diagrama de la figura 7.4 muestra la forma final del digrafo de la figura 7.2(a). El diagrama resultante de un orden parcial, mucho más sencillo que su digrafo, es el **diagrama de Hasse** del orden parcial del conjunto parcialmente ordenado. Como el diagrama de Hasse describe completamente el orden parcial asociado, se observará que es una herramienta muy útil. No confunda los diagramas de Hasse con las gráficas (capítulo 6). Ambos son formas simplificadas de representar diferentes tipos de digrafos.



(a) (b)

Figura 7.3

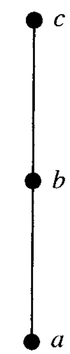


Figura 7.4

Ejemplo 11. Sea $A = \{1, 2, 3, 4, 12\}$. Considere el orden parcial de divisibilidad en A. Es decir, si a y $b \in A$, $a \leq b$ si y sólo si $a \mid b$. Trace el diagrama de Hasse del conjunto parcialmente ordenado $(A, \leq)$.

Solución: La figura 7.5 muestra el diagrama de Hasse. Para enfatizar la simplicidad del diagrama de Hasse, en la figura 7.6 se mostrará el digrafo del conjunto parcialmente ordenado de la figura 7.5. ♦

Ejemplo 12. Sea $S = \{a, b, c\}$ y $A = P(S)$. Trace el diagrama de Hasse del conjunto parcialmente ordenado A con el orden parcial $\subseteq$ (inclusión de conjuntos).

Solución: Primero se determina A, y se obtiene

$$A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Entonces, es posible trazar el diagrama de Hasse como en la figura 7.7. ♦

Observe que el diagrama de Hasse de un conjunto finito linealmente ordenado siempre tiene la forma de la figura 7.8.

Es fácil ver que si $(A, \leq)$ es un conjunto parcialmente ordenado y $(A, \geq)$ es el dual del conjunto parcialmente ordenado, el diagrama de Hasse para $(A, \geq)$ es justamente el diagrama de Hasse para $(A, \leq)$, volteado de arriba hacia abajo.

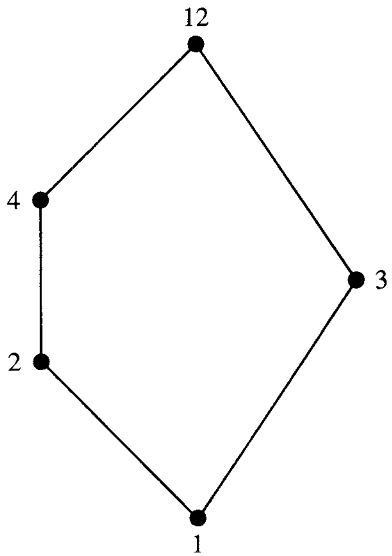


Figura 7.5

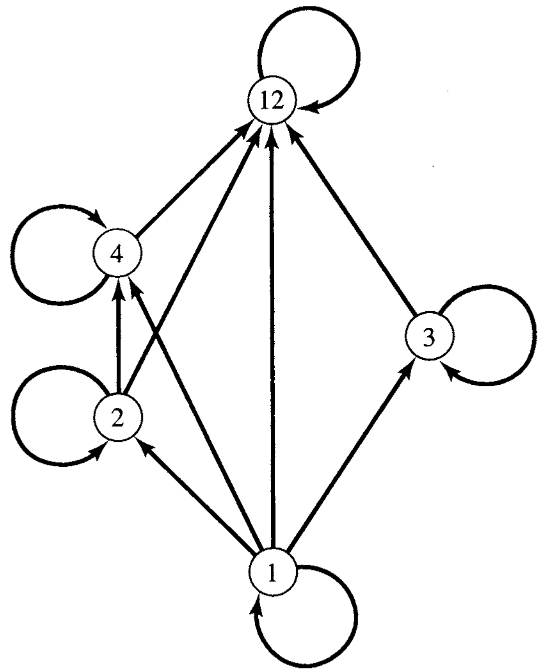


Figura 7.6

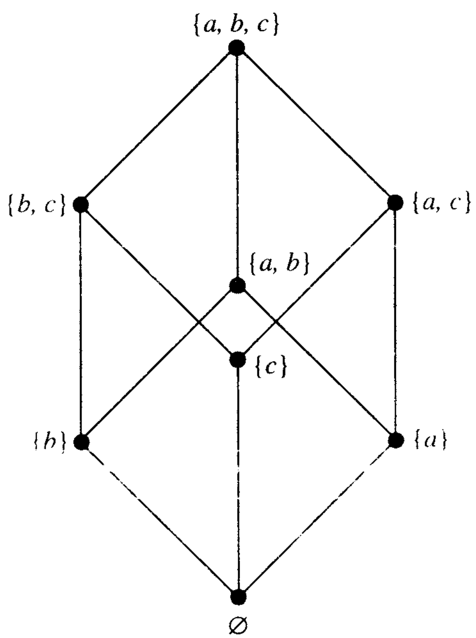


Figura 7.7

Figura 7.8

Ejemplo 13. La figura 7.9(a) muestra el diagrama de Hasse de un conjunto parcialmente ordenado $(A, \leq)$, donde $A = \{a, b, c, d, e, f\}$. La figura 7.9(b) muestra el diagrama de Hasse del conjunto parcialmente ordenado dual $(A, \geq)$. Observe que, como se mencionó anteriormente, cada uno de estos diagramas puede ser construido volteando el otro de arriba hacia abajo. ◆

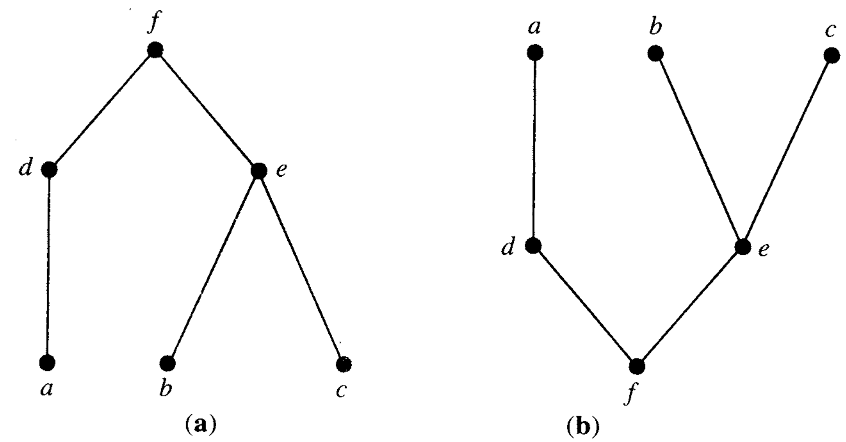


Figura 7.9

Ordenamiento topológico

Si A es un conjunto parcialmente ordenado con orden parcial $\leq$, a veces se necesita determinar un orden lineal $\prec$ para el conjunto A que sea simplemente una extensión del orden parcial dado, en el sentido de que si $a \leq b$, entonces $a \prec b$. El proceso de construcción de un orden lineal como $\prec$ es un **ordenamiento topológico**. Este problema puede surgir cuando se tenga que introducir un conjunto parcialmente ordenado finito A en una computadora. Hay que introducir los elementos de A en algún orden, y tal vez se quiera introducirlos de modo que se preserve el orden parcial. Es decir, si $a \leq b$, entonces se introduce a antes que b. Un ordenamiento topológico $\prec$ proporcionará un orden de introducción de los elementos que cumplirá esta condición.

Ejemplo 14. Proporcione un ordenamiento topológico para el conjunto parcialmente ordenado cuyo diagrama de Hasse aparece en la figura 7.10.

Solución. El orden parcial $\prec$ cuyo diagrama de Hasse aparece en la figura 7.11(a) es claramente un orden lineal. Es fácil ver que cada pareja en $\leq$ está también en el orden $\prec$, de modo que $\prec$ es un ordenamiento topológico del orden parcial $\leq$. La figura 7.11(b) y (c) muestran dos soluciones diferentes a este problema. ◆

Como muestra el ejemplo 14, existen muchas formas de ordenar topológicamente un conjunto parcialmente ordenado dado. En la sección 7.2 se proporcionará un algoritmo para generar ordenamientos topológicos.

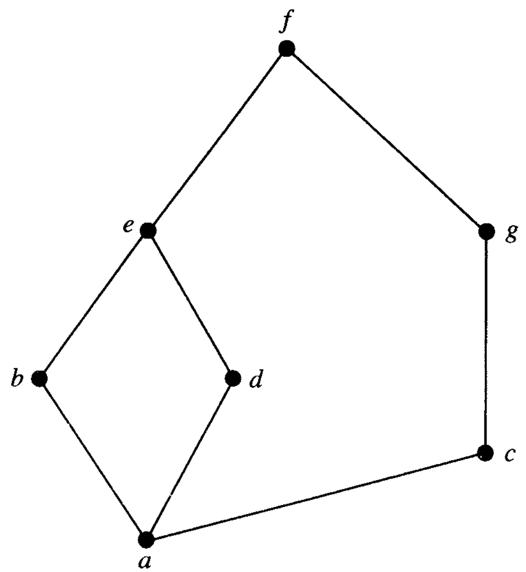
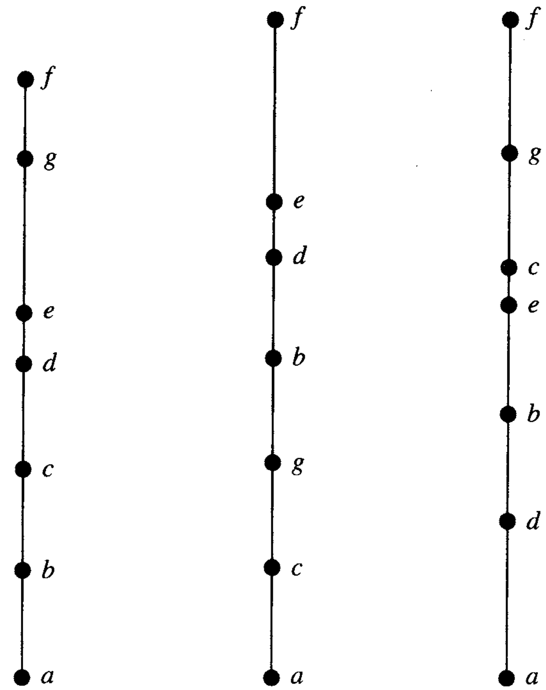


Figura 7.10



(a) (b) (c)

Figura 7.11

Isomorfismo

Sean $(A, \leq)$ y $(A', \leq')$ conjuntos parcialmente ordenados y $f: A \to A'$ una correspondencia uno a uno entre A y A'. La función f es un **isomorfismo** de $(A, \leq)$ en $(A', \leq')$ si, para cualquier a y b en A,

$$a \leq b \quad \text{si y sólo si} \quad f(a) \leq' f(b).$$

Si $f: A \to A'$ es un isomorfismo, se dice que $(A, \leq)$ y $(A', \leq')$ son conjuntos parcialmente ordenados **isomorfos**.

Ejemplo 15. Sea A el conjunto Z^+ de enteros positivos, y sea $\leq$ el orden parcial usual en A (véase el ejemplo 2). Sea A' el conjunto de enteros positivos pares y sea $\leq'$ el orden parcial usual en A'. La función $f: A \to A'$ dada por

$$f(a) = 2a$$

es un isomorfismo de $(A, \leq)$ a $(A', \leq')$.

En primer lugar, f es uno a uno, pues si $f(a) = f(b)$, entonces $2a = 2b$, de modo que $a = b$. A continuación, Dom$(f) = A$, de modo que f está definida para todo punto. Por último, si $c \in A'$, entonces $c = 2a$ para algún $a \in Z^+$; por lo que $c = f(a)$. Esto muestra que f es sobre, por lo cual f es una correspondencia uno a uno. Por último, si a y b son elementos de A, entonces es claro que $a \leq b$ si y sólo si $2a \leq 2b$. Así, f es un isomorfismo. ◆

Suponga que $f: A \to A'$ es un isomorfismo de un conjunto parcialmente ordenado $(A,$

$\leq)$ a un conjunto parcialmente ordenado $(A', \leq')$. Suponga también que B es un subconjunto de A y $B' = f(B)$ es el subconjunto correspondiente de A'. Entonces, de la definición de isomorfismo, se observa que se cumple el siguiente principio general.

Teorema 3 (Principio de Correspondencia). *Si los elementos de B tienen cualquier propiedad que los relaciona entre sí o con los demás elementos de A, y si es posible definir esta propiedad completamente en términos de la relación $\leq$, entonces los elementos de B' deben poseer exactamente la misma propiedad, definida en términos de $\leq'$.* ●

Ejemplo 16. Sea $(A, \leq)$ el conjunto parcialmente ordenado cuyo diagrama de Hasse aparece en la figura 7.12, y suponga que f es un isomorfismo de $(A, \leq)$ con algún otro conjunto parcialmente ordenado $(A', \leq')$. Observe primero que $d \leq x$ para cualquier x en A (más tarde se dirá que tal elemento d es un "elemento mínimo" de A). Entonces el elemento correspondiente $f(d)$ en A' debe satisfacer la propiedad de que $f(d) \leq' y$ para toda y en A'. Como otro ejemplo, observe que $a \not\leq b$ y $b \not\leq a$. Esta pareja **no es comparable** en A. El principio de correspondencia implica que $f(a)$ y $f(b)$ no pueden ser comparables en A'. ◆

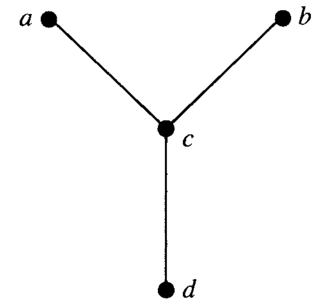


Figura 7.12

Para un conjunto finito parcialmente ordenado, uno de los objetos definidos completamente en términos del orden parcial es su diagrama de Hasse. El principio de correspondencia implica que dos conjuntos finitos parcialmente ordenados isomorfos deben tener diagramas de Hasse idénticos.

Para ser precisos, sean $(A, \leq)$ y $(A', \leq')$ conjuntos finitos parcialmente ordenados, $f: A \to A'$ una correspondencia uno a uno, y H cualquier diagrama de Hasse de $(A, \leq)$. Entonces

1. Si f es un isomorfismo y cada etiqueta a de H se reemplaza por $f(a)$, entonces H será un diagrama de Hasse para $(A', \leq')$.

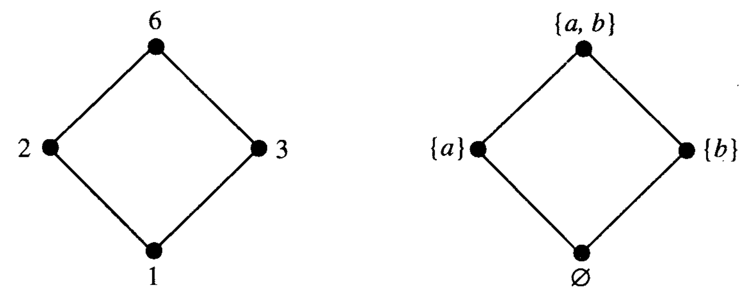
Recíprocamente,

2. Si H es un diagrama de Hasse para $(A', \leq')$, al reemplazar cada etiqueta a por $f(a)$, entonces f es un isomorfismo.

Ejemplo 17. Sean $A = \{1, 2, 3, 6\}$ y $\leq$ la relación $\mid$ (divide). La figura 7.13(a) muestra un diagrama de Hasse para $(A, \leq)$. Sean $A' = P(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$, y $\leq'$ la contención de conjuntos, $\subseteq$. Si se define $f: A \to A'$ por

$$f(1) = \varnothing, \qquad f(2) = \{a\}, \qquad f(3) = \{b\}, \qquad f(6) = \{a, b\},$$

entonces es fácil ver que f es una correspondencia uno a uno. Si cada etiqueta $a \in A$ del diagrama de Hasse se reemplaza por $f(a)$, la figura 7.13(b) muestra el resultado. Como esto es claramente un diagrama de Hasse para $(A', \leq')$, la función f es un isomorfismo. ◆



(a) (b)

Figura 7.13

GRUPO DE EJERCICIOS 7.1

1. Determine si la relación R es un orden parcial en el conjunto A.
   (a) $A = Z$, y $a\ R\ b$ si y sólo si $a = 2b$.
   (b) $A = Z$, y $a\ R\ b$ si y sólo si $b^2 \mid a$.
   (c) $A = Z$, y $a\ R\ b$ si y sólo si $a = b^k$ para algún $k \in Z^+$. Observe que k depende de a y b.
   (d) $A = \mathbb{R}$, y $a\ R\ b$ si y sólo si $a \leq b$.

2. Determine si la relación R es un orden lineal en el conjunto A.
   (a) $A = \mathbb{R}$, y $a\ R\ b$ si y sólo si $a \leq b$.
   (b) $A = \mathbb{R}$, y $a\ R\ b$ si y sólo si $a \geq b$.
   (c) $A = P(S)$, donde S es un conjunto. La relación R es la inclusión de conjuntos.
   (d) $A = \mathbb{R} \times \mathbb{R}$, y $(a, b)\ R\ (a', b')$ si y sólo si $a \leq a'$ y $b \leq b'$, donde $\leq$ es el orden parcial usual en $\mathbb{R}$.

3. En el conjunto $A = \{a, b, c\}$, determine todos los órdenes parciales $\leq$ tales que $a \leq b$.

4. ¿Qué puede decir acerca de la relación R en un conjunto A si R es un orden parcial y una relación de equivalencia?

En los ejercicios 5 y 6, determine el diagrama de Hasse de la relación R.

5. $A = \{1, 2, 3, 4\}$, $R = \{(1, 1), (1, 2), (2, 2), (2, 4), (1, 3), (3, 3), (3, 4), (1, 4), (4, 4)\}$

6. $A = \{a, b, c, d, e\}$, $R = \{(a, a), (b, b), (c, c), (a, c), (c, d), (c, e), (a, d), (d, d), (a, e), (b, c), (b, d), (b, e), (e, e)\}$

7. Describa las parejas ordenadas en la relación determinada por el diagrama de Hasse sobre el conjunto A de las figuras 7.14 y 7.15.
   (a) $A = \{1, 2, 3, 4\}$

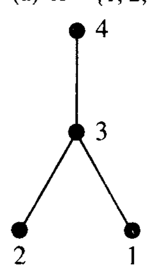


Figura 7.14

   (b) $A = \{1, 2, 3, 4\}$

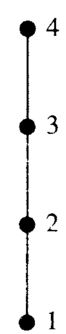


Figura 7.15

En los ejercicios 8 y 9, determine el diagrama de Hasse del orden parcial con el digrafo dado (figuras 7.16 y 7.17).

8.

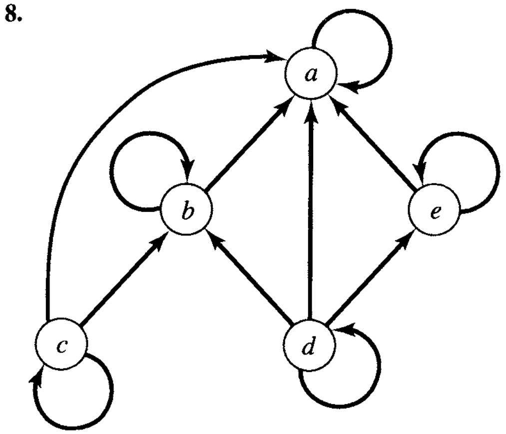


Figura 7.16

9.

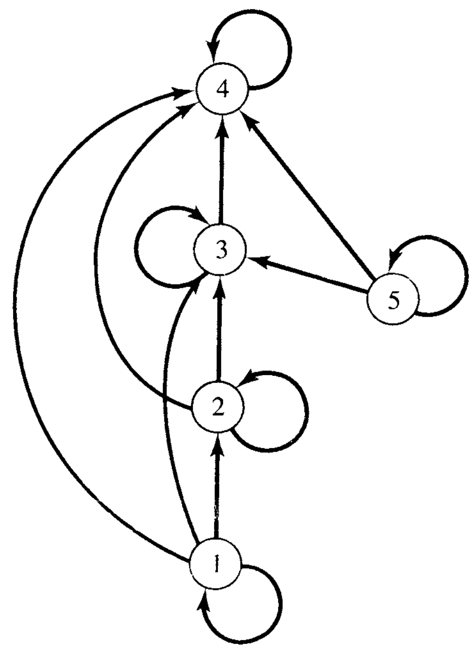


Figura 7.17

10. Determine el diagrama de Hasse de la relación en $A = \{1, 2, 3, 4, 5\}$ con la matriz que se muestra.

(a) $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

11. Determine la matriz del orden parcial con el diagrama de Hasse dado (figuras 7.18 y 7.19).
    (a)

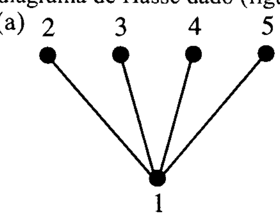


Figura 7.18

    (b)

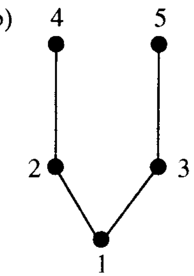


Figura 7.19

12. Sea $A = Z^+ \times Z^+$ con el orden lexicográfico. Marque cada uno de los siguientes incisos como verdadero o falso según sea el caso.
    (a) $(2, 12) \prec (5, 3)$ (b) $(3, 6) \prec (3, 24)$
    (c) $(4, 8) \prec (4, 6)$ (d) $(15, 92) \prec (12, 3)$

En los ejercicios 13 y 14, considere el orden parcial de divisibilidad en el conjunto A. Trace el diagrama de Hasse del conjunto parcialmente ordenado y determine cuáles conjuntos son linealmente ordenados.

13. (a) $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
    (b) $A = \{2, 4, 8, 16, 32\}$

14. (a) $A = \{3, 6, 12, 36, 72\}$
(b) $A = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 30, 60\}$

15. Sea $A = \{\square, A, B, C, E, O, M, P, S\}$ con el orden alfabético usual, donde $\square$ representa un carácter "blanco" y $\square \leq x$ para toda $x \in A$.
Acomode lo siguiente en orden lexicográfico (como elementos de $A \times A \times A \times A$).

(a) MOP $\square$ (b) MOPE
(c) CAP $\square$ (d) MAP $\square$
(e) BASE (f) ACE $\square$
(g) MACE (h) CAPE

En los ejercicios 16 *y* 17, *trace el diagrama de Hasse de un ordenamiento topológico para el conjunto parcialmente ordenado dado (figuras* 7.20 *y* 7.21).

16.

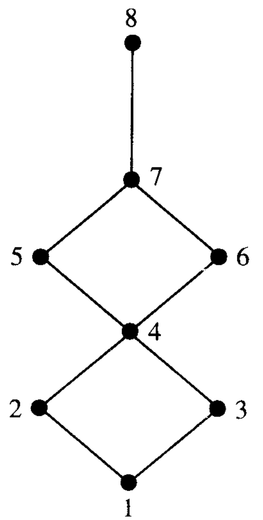


Figura 7.20

17.

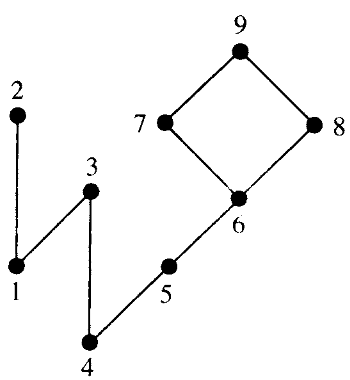


Figura 7.21

18. Si $(A, \leq)$ es un conjunto parcialmente ordenado y A' es un subconjunto de A, muestre que $(A', \leq')$ es también un conjunto parcialmente ordenado, donde $\leq'$ es la restricción de $\leq$ a A'.

19. Muestre que si R es un orden lineal en el conjunto A, entonces R^{-1} también es un orden lineal en A.

20. Una relación R en un conjunto A es un **cuasi-orden** si es transitiva e irreflexiva. Sea $A = P(S)$ el conjunto potencia de un conjunto S, y considere la siguiente relación R en A: $U \, R \, T$ si y sólo si $U \subsetneq T$ (contención propia). Muestre que R es un cuasi-orden.

21. Sea $A = \{x \mid x$ es un número real y $-5 \leq x \leq 20\}$. Muestre que la relación usual $<$ es un cuasi-orden (véase el ejercicio 20) en A.

22. Si R es un cuasi-orden en A (véase el ejercicio 20), muestre que R^{-1} también es un cuasi-orden.

23. Sea $B = \{2, 3, 6, 9, 12, 18, 24\}$ y sea $A = B \times B$. Defina la siguiente relación en A: $(a, b) \prec (a', b')$ si y sólo si $a \mid a'$ y $b \leq b'$, donde $\leq$ es el orden parcial usual. Muestre que $\prec$ es un orden parcial.

24. Sea $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ y considere el orden parcial $\leq$ de divisibilidad en A. Es decir, $a \leq b$ significa $a \mid b$. Sea $A' = P(S)$, donde $S = \{e, f, g\}$, el conjunto parcialmente ordenado con orden parcial $\subsetneq$. Muestre que $(A, \leq)$ y $(A', \subseteq)$ son conjuntos parcialmente ordenados isomorfos.

25. Sea $A = \{1, 2, 4, 8\}$ y $\leq$ el orden parcial de divisibilidad en A. Sea $A' = \{0, 1, 2, 3\}$ y $\leq'$ la relación usual "menor o igual que" en los enteros. Muestre que $(A, \leq)$ y $(A', \leq')$ son isomorfos.

7.2. Elementos extremos de conjuntos parcialmente ordenados

Ciertos elementos de un conjunto parcialmente ordenado tienen una importancia particular para muchas propiedades y aplicaciones de los conjuntos parcialmente ordenados. En esta sección se analizará estos elementos, y en secciones posteriores se verá el importante papel que juegan. En esta sección se considerará un conjunto parcialmente ordenado $(A, \leq)$ con orden parcial $\leq$.

Un elemento $a \in A$ es un **elemento máximo** de A si no existe un elemento c en A tal que $a < c$ (véase la sección 7.1). Un elemento $b \in A$ es un **elemento mínimo** de A si no existe un elemento c en A tal que $c < b$.

Esto implica que si $(A, \leq)$ es un conjunto parcialmente ordenado y $(A, \geq)$ es su conjunto parcialmente ordenado dual, un elemento $a \in A$ es un elemento máximo de $(A, \geq)$ si y sólo si a es un elemento mínimo de $(A, \leq)$. Además, a es un elemento mínimo de $(A, \geq)$ si y sólo si es un elemento máximo de $(A, \leq)$.

Ejemplo 1. Considere el conjunto parcialmente ordenado A cuyo diagrama de Hasse aparece en la figura 7.22. Los elementos a_1, a_2 y a_3 son elementos máximos de A, y los elementos b_1, b_2 y b_3 son elementos mínimos. Observe que, como no existe un segmento entre b_2 y b_3, se puede concluir que ni $b_3 \leq b_2$ ni $b_2 \leq b_3$. ◆

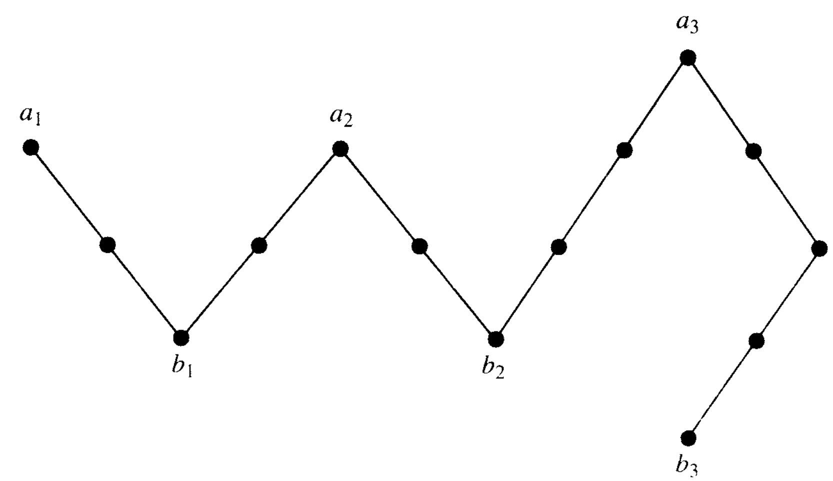


Figura 7.22

Ejemplo 2. Sea A el conjunto parcialmente ordenado de números reales no negativos con el orden parcial usual $\leq$. Entonces 0 es un elemento mínimo de A. No existen elementos máximos de A. ◆

Ejemplo 3. El conjunto parcialmente ordenado Z con el orden parcial usual $\leq$ no tiene elementos máximos ni elementos mínimos. ◆

Teorema 1. *Sea A un conjunto finito parcialmente ordenado no vacío con orden parcial $\leq$. Entonces A tiene al menos un elemento máximo y al menos un elemento mínimo.*

Demostración: Sea a cualquier elemento de A. Si a no es máximo, es posible determinar un elemento $a_1 \in A$ tal que $a < a_1$. Si a_1 no es máximo, puede determinarse un elemento $a_2 \in A$ tal que $a_1 < a_2$. Este argumento no puede continuar de manera indefinida, ya que A es un conjunto finito. Así, en cierto momento se obtendrá la cadena finita

$$a < a_1 < a_2 < \cdots < a_{k-1} < a_k,$$

que no puede extenderse. Por lo tanto, no es posible tener $a_k < b$ para cualquier $b \in A$ y a_k es un elemento máximo de $(A, \leq)$.

El mismo argumento dice que el conjunto parcialmente ordenado dual $(A, \geq)$ tiene un elemento máximo, de modo que $(A, \leq)$ tiene un elemento mínimo. ●

Puede utilizarse el concepto de elemento mínimo para proporcionar un algoritmo que determine un ordenamiento topológico de un conjunto finito parcialmente ordenado dado $(A, \leq)$. Obsérvese primero que si $a \in A$ y $B = A - \{a\}$, entonces B es también un conjunto parcialmente ordenado bajo la restricción de $\leq$ a $B \times B$ (véase la sección 4.2). Entonces, se obtiene el siguiente algoritmo, el cual produce un arreglo lineal llamado SORT. Supóngase que SORT está ordenado según el índice creciente; es decir, SORT[1] $\prec$ SORT[2] $\prec \cdots$. La relación $\prec$ en A definida de esta forma es un ordenamiento topológico de $(A, \leq)$.

Algoritmo para determinar un ordenamiento topológico de un conjunto finito parcialmente ordenado $(A, \leq)$.

PASO 1. Se elige un elemento mínimo a de A.
PASO 2. Se hace que a sea la siguiente entrada de SORT y se reemplaza A con $A - \{a\}$.
PASO 3. Se repite los pasos 1 y 2 hasta que $A = \{\ \}$.
Fin del algoritmo

Ejemplo 4. Sea $A = \{a, b, c, d, e\}$; la figura 7.23(a) muestra el diagrama de Hasse de un orden parcial $\leq$ en A. Un elemento mínimo de este conjunto parcialmente ordenado es el vértice etiquetado d (también se podría haber elegido e). Se coloca d en SORT[1] y en la figura 7.23(b) se muestra el diagrama de Hasse de $A - \{d\}$. Un elemento mínimo del nuevo A es e, de modo que e es ahora SORT[2], y la figura 7.23(c) muestra $A - \{e\}$. Este proceso continúa hasta terminar A y llenar SORT. La figura 7.23(f) muestra el arreglo completo SORT y el diagrama de Hasse del conjunto parcialmente ordenado correspondiente a SORT. Éste es un ordenamiento topológico de $(A, \leq)$. ◆

Un elemento $a \in A$ es un **elemento máximo** de A si $x \leq a$ para toda $x \in A$. Un elemento $a \in A$ es un **elemento mínimo** de A si $a \leq x$ para toda $x \in A$.

Como antes, un elemento a de $(A, \leq)$ es un elemento máximo (o mínimo) si y sólo si es el elemento mínimo (o máximo) de $(A, \geq)$.

Ejemplo 5. Considere el conjunto parcialmente ordenado definido en el ejemplo 2. Entonces 0 es un elemento mínimo; no existe un elemento máximo. ◆

Ejemplo 6. Sea $S = \{a, b, c\}$ y considere el conjunto parcialmente ordenado $A = P(S)$ definido en el ejemplo 12 de la sección 7.1. El conjunto vacío es un elemento mínimo de A, y el conjunto S es un elemento máximo de A. ◆

Ejemplo 7. El conjunto parcialmente ordenado Z con el orden parcial usual no tiene elemento mínimo ni máximo. ◆

Teorema 2. *Un conjunto parcialmente ordenado tiene a lo más un elemento máximo y a lo más un elemento mínimo.*

Demostración: Suponga que a y b son elementos máximos de un conjunto parcialmente ordenado A. Entonces, como b es un elemento máximo, se tiene que $a \leq b$. De manera análoga, como a es un elemento máximo, se tiene que $b \leq a$. La propiedad antisimétrica implica que $a = b$. Así, si el conjunto parcialmente ordenado tiene un elemento máximo, tiene sólo un elemento de este tipo. Como este hecho es válido para todos los conjuntos parcialmente ordenados, el conjunto parcialmente ordenado dual $(A, \geq)$ tiene a lo más un elemento máximo, de modo que $(A, \leq)$ también tiene a lo más un elemento mínimo. ●

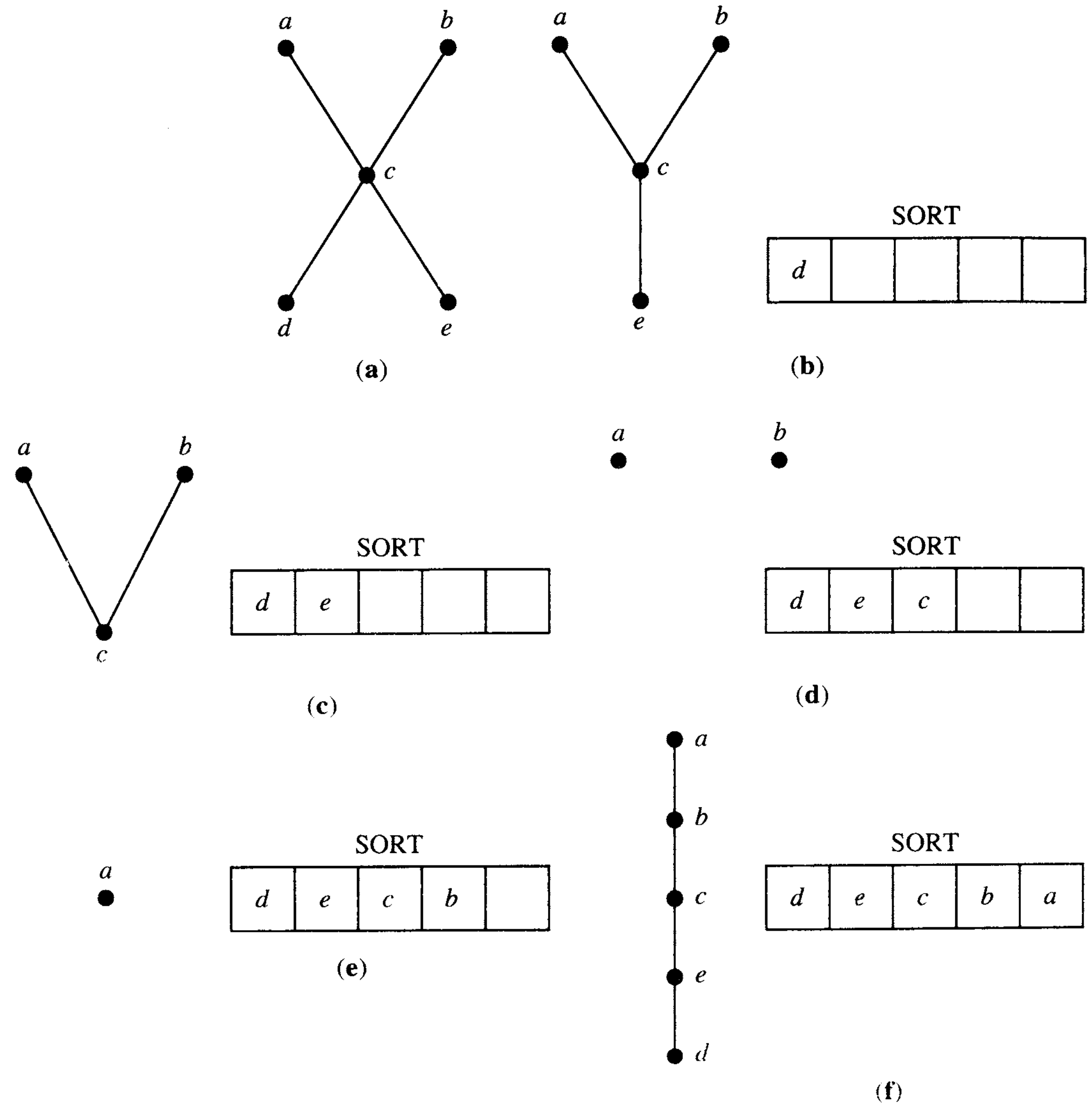


Figura 7.23

El elemento máximo de un conjunto parcialmente ordenado, si existe, se denota por I y con frecuencia es llamado **elemento unidad**. De manera análoga, el elemento mínimo de un conjunto parcialmente ordenado, si existe, se denota por 0 y con frecuencia se lo llama **elemento cero**.

Considere un conjunto parcialmente ordenado A y un subconjunto B de A. Un elemento $a \in A$ es una **cota superior** de B si $b \leq a$ para toda $b \in B$. Un elemento $a \in A$ es una **cota inferior** de B si $a \leq b$ para toda $b \in B$.

Ejemplo 8. Considere el conjunto parcialmente ordenado $A = \{a, b, c, d, e, f, g, h\}$, cuyo diagrama de Hasse aparece en la figura 7.24. Determine todas las cotas superior e inferior de los siguientes subconjuntos de A: (a) $B_1 = \{a, b\}$; (b) $B_2 = \{c, d, e\}$.

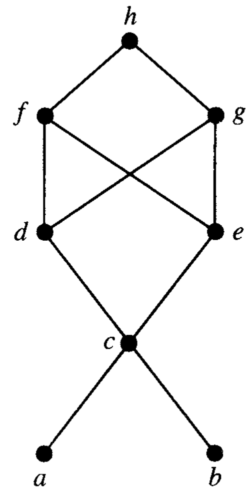


Figura 7.24

Solución

(a) B_1 no tiene cotas inferiores; sus cotas superiores son c, d, e, f, g y h.

(b) Las cotas superiores de B_2 son f, g y h; sus cotas inferiores son c, a y b. ◆

Como muestra el ejemplo 8, un subconjunto B de un conjunto parcialmente ordenado puede o no tener cotas superiores e inferiores (en A). Además, una cota superior o inferior de B puede o no pertenecer al propio B.

Sea A un conjunto parcialmente ordenado y B un subconjunto de A. Un elemento $a \in A$ es una **mínima cota superior** (LUB) de B si a es una cota superior de B y $a \leq a'$, siempre y cuando a' sea una cota superior de B. Así, $a = \text{LUB}(B)$ si $b \leq a$ para toda $b \in B$, y si $a' \in A$ es también una cota superior de B, entonces $a \leq a'$.

De manera análoga, un elemento $a \in A$ es una **máxima cota inferior** (GLB) de B si a es una cota inferior de B y $a' \leq a$, siempre y cuando a' sea una cota inferior de B. Así, $a = \text{GLB}(B)$ si $a \leq b$ para toda $b \in B$, y si $a' \in A$ es también una cota inferior de B, entonces $a' \leq a$.

Como de costumbre, las cotas superiores en $(A, \leq)$ corresponden a cotas inferiores en $(A, \geq)$ (para el mismo conjunto de elementos) y las cotas inferiores en $(A, \leq)$ corresponden a cotas superiores en $(A, \geq)$. También existen enunciados similares válidos para las máximas cotas inferiores y mínimas cotas superiores.

Ejemplo 9. Sea A el conjunto parcialmente ordenado del ejemplo 8 con los subconjuntos B_1 y B_2 definidos en ese ejemplo. Determine todas las mínimas cotas superiores y todas las máximas cotas inferiores de (a) B_1; (b) B_2.

Solución

(a) Como B_1 no tiene cotas inferiores, no tiene máximas cotas inferiores. Sin embargo,

$$\text{LUB}(B_1) = c.$$

(b) Como las cotas inferiores de B_2 son c, a y b, se determina que

$$\text{GLB}(B_2) = c.$$

Las cotas superiores de B_2 son f, g y h. Como f y g no son comparables, se concluye que B_2 no tiene una mínima cota superior. ◆

Teorema 3. *Sea $(A, \leq)$ un conjunto parcialmente ordenado. Entonces un subconjunto B de A tiene a lo más una* LUB *y a lo más una* GLB.

Demostración: La demostración es similar a la del teorema 2. ●

Se concluye esta sección con algunas observaciones acerca de las cotas LUB y GLB en un conjunto finito parcialmente ordenado A, para lo cual se utiliza el diagrama de Hasse de A. Sea $B = \{b_1, b_2, \ldots, b_r\}$. Si $a = \text{LUB}(B)$, entonces a es el primer vértice que puede ser alcanzado desde $b_1, b_2, \ldots, b_r$ mediante trayectorias verticales hacia arriba. De manera análoga, si $a = \text{GLB}(B)$, entonces a es el primer vértice que puede ser alcanzado desde $b_1, b_2, \ldots, b_r$ mediante trayectorias verticales hacia abajo.

Ejemplo 10. Sea $A = \{1, 2, 3, 4, 5, \ldots, 11\}$ el conjunto parcialmente ordenado cuyo diagrama de Hasse aparece en la figura 7.25. Determine la LUB y la GLB de $B = \{6, 7, 10\}$, si existen.

Solución: Se verificó todas las trayectorias hacia arriba desde los vértices 6, 7 y 10 y se determinó que $\text{LUB}(B) = 10$. De manera análoga, al analizar todas las trayectorias hacia abajo desde 6, 7 y 10, se determinó que $\text{GLB}(B) = 4$. ◆

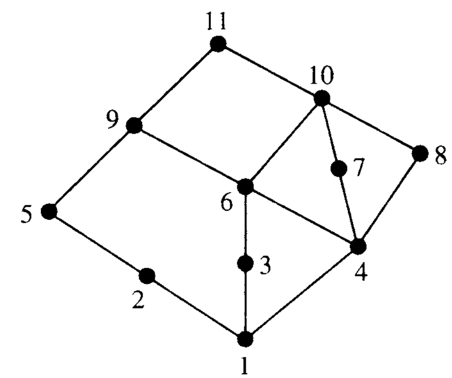


Figura 7.25

El siguiente resultado es una consecuencia inmediata del principio de correspondencia (véase la sección 7.1).

Teorema 4. *Suponga que $(A, \leq)$ y $(A', \leq')$ son conjuntos parcialmente ordenados isomorfos bajo el isomorfismo $f: A \to A'$.*

(a) *Si a es un elemento máximo (mínimo) de $(A, \leq)$, entonces $f(a)$ es un elemento máximo (mínimo) de $(A', \leq')$.*

(b) *Si a es el elemento máximo (mínimo) de $(A, \leq)$, entonces $f(a)$ es el elemento máximo (mínimo) de $(A', \leq')$.*

(c) *Si a es una cota superior (cota inferior, mínima cota superior, máxima cota inferior) de un subconjunto B de A, entonces $f(a)$ es una cota superior (cota inferior, mínima cota superior, máxima cota inferior) para el subconjunto $f(B)$ de A'.*

(d) *Si todo subconjunto de $(A, \leq)$ tiene una* LUB (GLB), *entonces todo subconjunto de $(A', \leq')$ tiene una* LUB (GLB). ●

Ejemplo 11. Muestre que los conjuntos parcialmente ordenados $(A, \leq)$ y $(A', \leq')$, cuyos diagramas de Hasse aparecen en las figuras 7.26(a) y (b), respectivamente, no son isomorfas.

(a) **(b)**

Figura 7.26

Solución: Los dos conjuntos parcialmente ordenados no son isomorfos, ya que $(A, \leq)$ tiene un elemento máximo a, mientras que $(A', \leq')$ no tiene tal elemento máximo. También se puede argumentar que no son isomorfos ya que $(A, \leq)$ no tiene un elemento mínimo, mientras que $(A', \leq')$ tiene un elemento mínimo. ◆

GRUPO DE EJERCICIOS 7.2

En los ejercicios 1 al 4, determine todos los elementos máximos y mínimos del conjunto parcialmente ordenado.

1. (a)

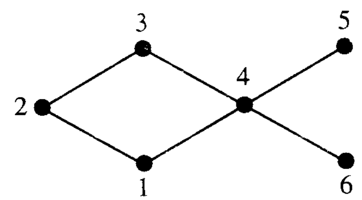


Figura 7.27

(b)

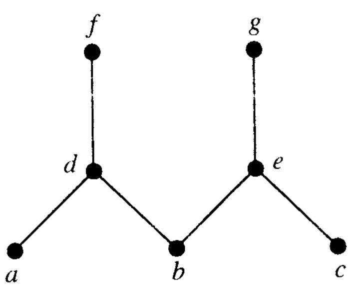


Figura 7.28

2. (a)

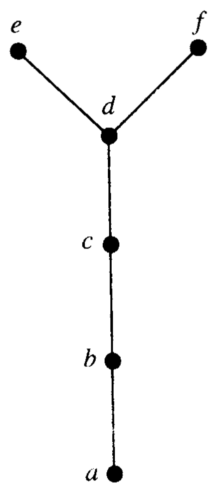


Figura 7.29

(b)

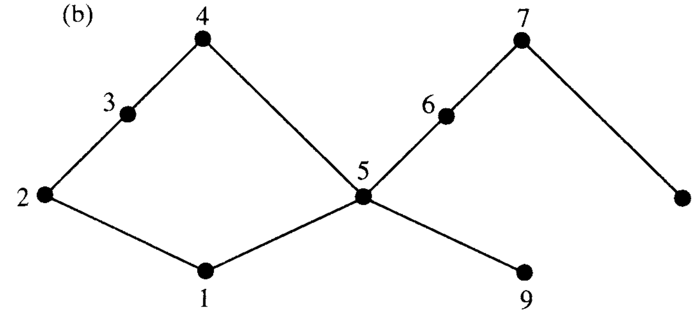


Figura 7.30

3. (a) $A = \mathbb{R}$ con el orden parcial usual $\leq$.
(b) $A = \{x \mid x$ es un número real y $0 \leq x < 1\}$ con el orden parcial usual $\leq$.

4. (a) $A = \{x \mid x$ es un número real y $0 < x \leq 1\}$ con el orden parcial usual $\leq$.
(b) $A = \{2, 3, 4, 6, 8, 24, 48\}$ con el orden parcial de divisibilidad.

En los ejercicios 5 al 8, determine los elementos máximo y mínimo, si existen, del conjunto parcialmente ordenado.

5. (a)

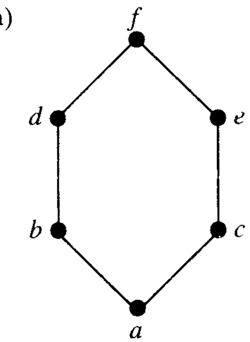


Figura 7.31

(b)

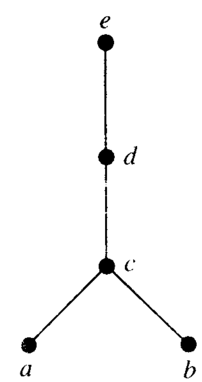


Figura 7.32

6. (a)

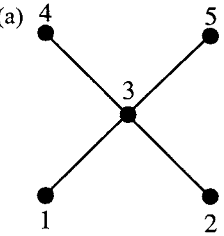


Figura 7.33

(b)

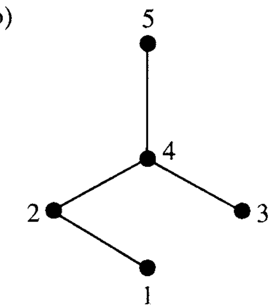


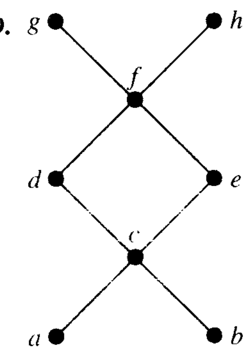
Figura 7.34

7. (a) $A = \{x \mid x$ es un número real y $0 < x < 1\}$ con el orden parcial usual $\leq$.
(b) $A = \{x \mid x$ es un número real y $0 \leq x \leq 1\}$ con el orden parcial usual $\leq$.

8. (a) $A = \{2, 4, 6, 8, 12, 18, 24, 36, 72\}$ con el orden parcial de divisibilidad.
(b) $A = \{2, 3, 4, 6, 12, 18, 24, 36\}$ con el orden parcial de divisibilidad.

En los ejercicios 9 al 18, determine, si existen, (a) *todas las cotas superiores de B;* (b) *todas las cotas inferiores de B;* (c) *la mínima cota superior de B;* (d) *la máxima cota inferior de B.*

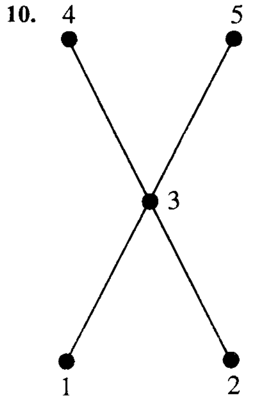
9.



$B = \{c, d, e\}$

Figura 7.35

10.

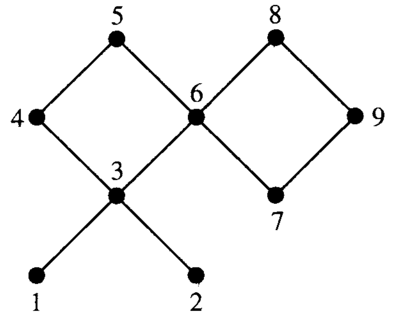


$B = \{1, 2, 3, 4, 5\}$
Figura 7.36

11.

$B = \{b, c, d\}$
Figura 7.37

12.



$B = \{3, 4, 6\}$
Figura 7.38

13. $(A, \leq)$ es el conjunto parcialmente ordenado del ejercicio 9; $B = \{b, h, g\}$.

14. (a) $(A, \leq)$ es el conjunto parcialmente ordenado del ejercicio 12; $B = \{4, 6, 9\}$.
(b) $(A, \leq)$ es el conjunto parcialmente ordenado del ejercicio 12; $B = \{3, 4, 8\}$.

15. $A = \mathbb{R}$ y $\leq$ denota el orden parcial usual; $B = \{x \mid x$ es un número real y $1 < x < 2\}$.

16. $A = \mathbb{R}$ y $\leq$ denota el orden parcial usual; $B = \{x \mid x$ es un número real y $1 \leq x < 2\}$.

17. $A = P(\{a, b, c\})$ y $\leq$ denota el orden parcial usual de contención; $B = P(\{a, b\})$.

18. $A = \{2, 3, 4, 6, 8, 12, 24, 48\}$ y $\leq$ denota el orden parcial de divisibilidad; $B = \{4, 6, 12\}$.

19. Construya el diagrama de Hasse de un ordenamiento topológico del conjunto parcialmente ordenado cuyo diagrama de Hasse aparece en la figura 7.35. Utilice el algoritmo SORT.

20. Construya el diagrama de Hasse de un ordenamiento topológico del conjunto parcialmente ordenado cuyo diagrama de Hasse aparece en la figura 7.36. Utilice el algoritmo SORT.

7.3. Retículas

Una **retícula** es un conjunto parcialmente ordenado $(L, \leq)$ tal que cada subconjunto $\{a, b\}$ de dos elementos tiene un mínima cota superior y una máxima cota inferior. Se denota LUB $(\{a, b\})$ como $a \vee b$ y es llamada **unión** de a y b. De igual manera, se denota GLB $(\{a, b\})$

mediante $a \wedge b$ y se la llama **conjunción** de a y b. Con frecuencia, las estructuras de tipo retícula aparecen en la computación y las aplicaciones matemáticas. Observe que una retícula es una estructura matemática como la descrita en la sección 1.6, con dos operaciones binarias, unión y conjunción.

Ejemplo 1. Sea S un conjunto y sea $L = P(S)$. Como se ha visto, la contención $\subseteq$ es un orden parcial en L. Sean A y B pertenecientes al conjunto parcialmente ordenado $(L, \subseteq)$. Entonces $A \vee B$ es el conjunto $A \cup B$. Para ver esto, observe que $A \subseteq A \cup B$, $B \subseteq A \cup B$, y, si $A \subseteq C$ y $B \subseteq C$, entonces $A \cup B \subseteq C$. De manera análoga, se puede mostrar que el elemento $A \wedge B$ en $(L, \subseteq)$ es el conjunto $A \cap B$. L es una retícula. ◆

Ejemplo 2. Considere el conjunto parcialmente ordenado $(Z^+, \leq)$, donde para a y b en Z^+, $a \leq b$ si y sólo si $a \mid b$. Entonces L es una retícula donde la unión y la conjunción de a y b son su mínimo común múltiplo y su máximo común divisor, respectivamente (véase la sección 1.4). Es decir,

$$a \vee b = \text{MCM}(a, b) \quad \text{y} \quad a \wedge b = \text{MCD}(a, b).$$ ◆

Ejemplo 3. Sea n un entero positivo y sea D_n el conjunto de todos los divisores positivos de n. Entonces D_n es una retícula bajo la relación de divisibilidad, como en el ejemplo 2. Así, si $n = 20$, se tiene $D_{20} = \{1, 2, 4, 5, 10, 20\}$. La figura 7.39(a) muestra el diagrama de Hasse de D_{20}. Si $n = 30$, se tiene $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. La figura 7.39(b) muestra el diagrama de Hasse de D_{30}. ◆

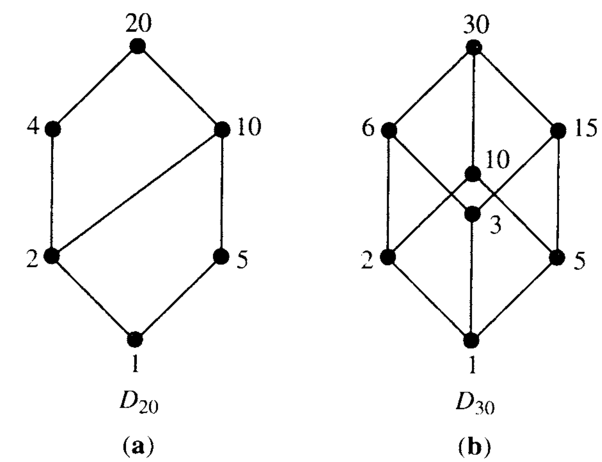


Figura 7.39

Ejemplo 4. ¿Cuáles de los diagramas de Hasse de la figura 7.40 representan retículas?

Solución. Los diagramas de Hasse (a), (b), (d) y (e) representan retículas. El diagrama (c) no representa una retícula, ya que $f \vee g$ no existe. El diagrama (f) no representa una retícula ya que no existen $d \wedge e$ ni $b \vee c$. El diagrama (g) no representa una retícula ya que $c \wedge d$ no existe. ◆

Ejemplo 5. Se ha observado ya en el ejemplo 4 de la sección 7.1 que el conjunto $\mathcal{R}$ de todas las relaciones de equivalencia en un conjunto A es un conjunto parcialmente ordenado bajo el orden parcial de contención de conjuntos. Se puede ahora concluir que $\mathcal{R}$ es una retícula, donde la conjunción de las relaciones de equivalencia R y S es su intersección $R \cap S$ y su unión es $(R \cup S)^\infty$, la cerradura transitiva de su unión (véase la sección 4.8). ♦

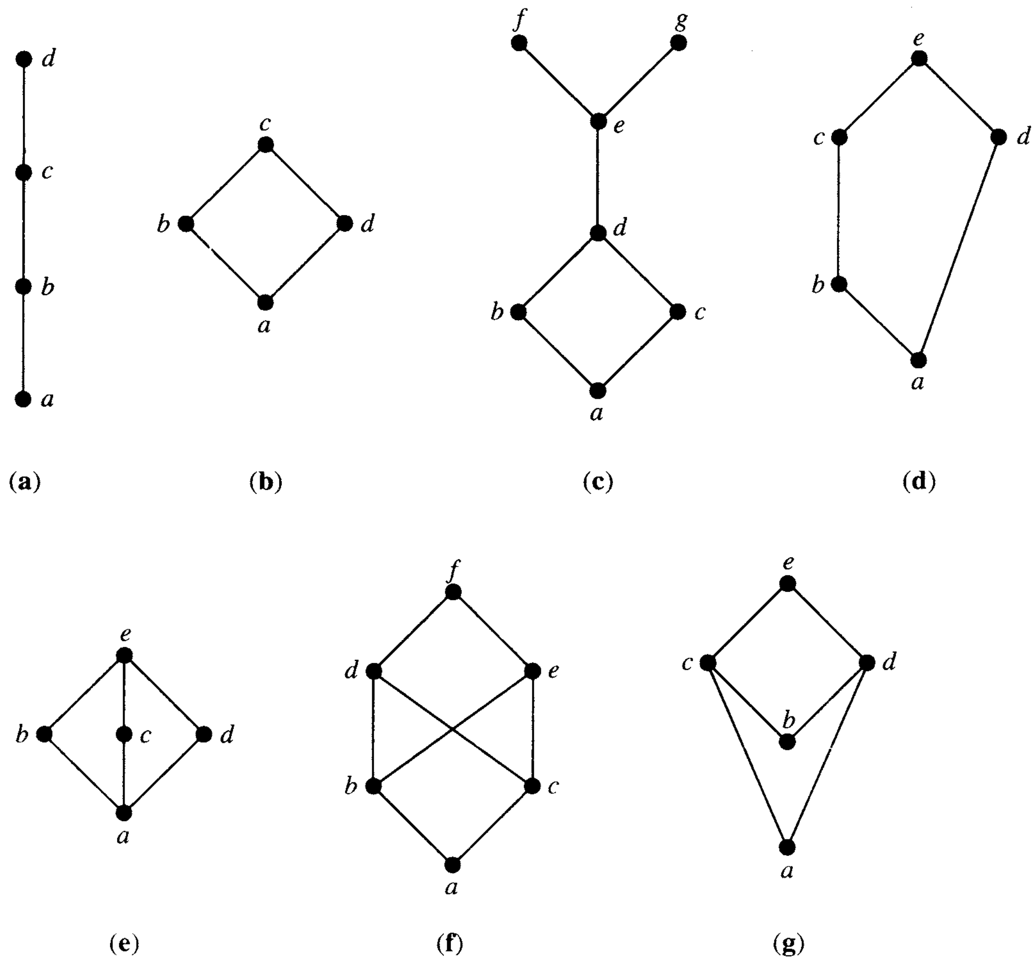


Figura 7.40

Sea $(L, \leq)$ un conjunto parcialmente ordenado y sea $(L, \geq)$ el conjunto parcialmente ordenado dual. Si $(L, \leq)$ es una retícula, se puede mostrar que $(L, \geq)$ también es una retícula. De hecho, para cualesquiera a y b en L, la mínima cota superior de a y b en $(L, \leq)$ es igual a la máxima cota inferior de a y b en $(L, \geq)$. De manera análoga, la máxima cota inferior de a y b en $(L, \leq)$ es igual a la mínima cota superior de a y b en $(L, \geq)$. Si L es un conjunto finito, puede observarse con facilidad que esta propiedad es válida, al examinar los diagramas de Hasse del conjunto parcialmente ordenado y su dual.

Ejemplo 6. Sea S un conjunto y $L = P(S)$. Entonces $(L, \subseteq)$ es una retícula, y su retícula dual es $(L, \supseteq)$, donde $\subseteq$ está "contenido en" y $\supseteq$ "contiene a". El análisis anterior a este ejemplo muestra, entonces, que en el conjunto parcialmente ordenado $(L, \supseteq)$, la unión $A \vee B$ es el conjunto $A \cap B$, y la conjunción $A \wedge B$ es el conjunto $A \cup B$. ♦

Teorema 1. *Si $(L_1, \leq)$ y $(L_2, \leq)$ son retículas, entonces $(L, \leq)$ es una retícula, donde $L = L_1 \times L_2$, y el orden parcial $\leq$ de L es el orden parcial producto.*

Demostración: Se denota la unión y la conjunción en L_1 mediante $\vee_1$ y $\wedge_1$, respectivamente, y la unión y la conjunción en L_2 mediante $\vee_2$ y $\wedge_2$, respectivamente. Por el teorema 1 de la sección 7.1, L es un conjunto parcialmente ordenado. Ahora se debe mostrar que si (a_1, b_1) y $(a_2, b_2) \in L$, entonces $(a_1, b_1) \vee (a_2, b_2)$ y $(a_1, b_1) \wedge (a_2, b_2)$ existen en L. Se deja como un ejercicio verificar que

$$(a_1, b_1) \vee (a_2, b_2) = (a_1 \vee_1 a_2, b_1 \vee_2 b_2)$$

$$(a_1, b_1) \wedge (a_2, b_2) = (a_1 \wedge_1 a_2, b_1 \wedge_2 b_2).$$

Así, L es una retícula. ●

Ejemplo 7. Sean L_1 y L_2 las retículas de la figura 7.41(a) y (b), respectivamente. Entonces $L = L_1 \times L_2$ es la retícula de la figura 7.41(c). ♦

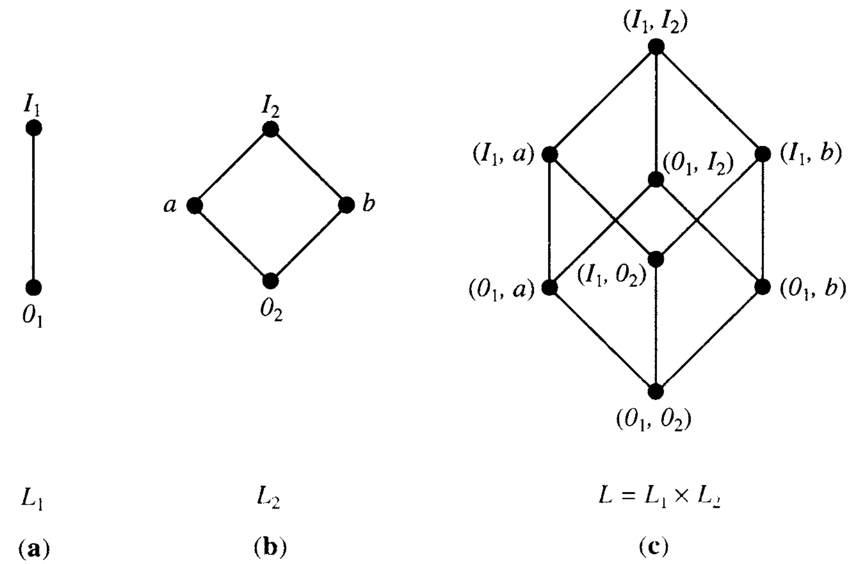
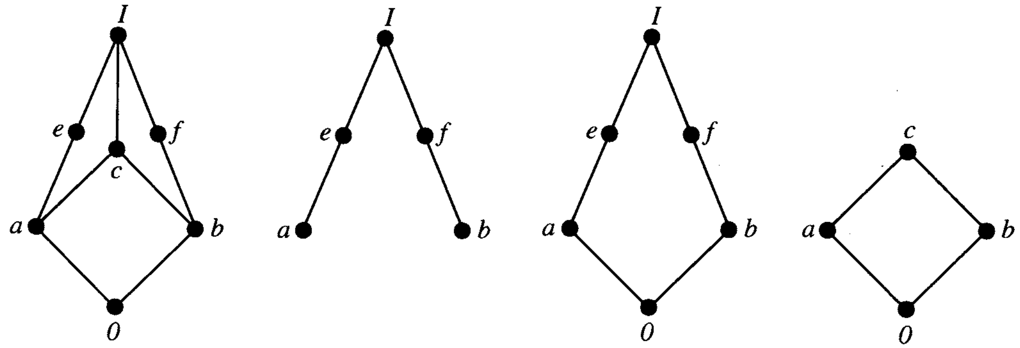


Figura 7.41

Sea $(L, \leq)$ una retícula. Un subconjunto no vacío S de L es una **subretícula** de L si $a \vee b \in S$ y $a \wedge b \in S$ siempre que $a \in S$ y $b \in S$.

Ejemplo 8. La retícula D_n de todos los divisores positivos de n (véase el ejemplo 3) es una subretícula de la retícula Z^+ bajo la relación de divisibilidad (véase el ejemplo 2). ♦

Ejemplo 9. Considere la retícula L de la figura 7.42(a). El subconjunto parcialmente ordenado S_b que aparece en la figura 7.42(b) no es una subretícula de L, ya que $a \wedge b \notin S_b$ y $a \vee b \notin S_b$. El subconjunto parcialmente ordenado S_c de la figura 7.42(c) no es una subretícula de L ya que $a \vee b \notin S_c$. Observe, sin embargo, que S_c es una retícula cuando se considera como conjunto parcialmente ordenado en sí mismo. El subconjunto parcialmente ordenado S_d de la figura 7.42(d) es una subretícula de L. ♦



(a) (b) (c) (d)

Figura 7.42

Retículas isomorfas

Si $f: L_1 \to L_2$ es un isomorfismo del conjunto parcialmente ordenado $(L_1, \leq_1)$ al conjunto parcialmente ordenado $(L_2, \leq_2)$, entonces el teorema 4 de la sección 7.2 dice que L_1 es una retícula si y sólo si L_2 es una retícula. De hecho, si a y b son elementos de L_1, entonces $f(a \wedge b) = f(a) \wedge f(b)$ y $f(a \vee b) = f(a) \vee f(b)$. Si dos retículas son isomorfas como conjuntos parcialmente ordenados, se dice que son **retículas isomorfas**.

Ejemplo 10. Sea L la retícula D_6, y sea L' la retícula $P(S)$ bajo la relación de contención, donde $S = \{a, b\}$. Estos conjuntos parcialmente ordenados fueron analizados en el ejemplo 16 de la sección 7.1, donde se muestra que son isomorfos. Así, como ambos son retículas, son retículas isomorfas. ◆

Si $f: A \to B$ es una correspondencia uno a uno de una retícula $(A, \leq)$ a un conjunto B, entonces se puede utilizar la función f para definir un orden parcial $\leq'$ en B. Si b_1 y b_2 están en B, entonces $b_1 = f(a_1)$ y $b_2 = f(a_2)$ para ciertos elementos únicos a_1 y a_2 de A.

Se define $b_1 \leq' b_2$ (en B) si $a_1 \leq a_2$ (en A). Si A y B son finitos, entonces puede describirse este proceso de manera geométrica, como sigue. Se construye el diagrama de Hasse para $(A, \leq)$. Después, se reemplaza cada etiqueta a por el elemento correspondiente $f(a)$ de B. El resultado es el diagrama de Hasse del orden parcial $\leq'$ en B.

Cuando B recibe este orden parcial $\leq'$, f es un isomorfismo del conjunto parcialmente ordenado $(A, \leq)$ en el conjunto parcialmente ordenado $(B, \leq')$. Para ver esto, observe que ya se ha supuesto que f es una correspondencia uno a uno. La definición de $\leq'$ establece que, para cualquier a_1 y a_2 en A, $a_1 \leq a_2$ si y sólo si $f(a_1) \leq' f(a_2)$. Así, f es un isomorfismo. Como $(A, \leq)$ es una retícula, también lo es $(B, \leq')$, y ambas son retículas isomorfas.

Ejemplo 11. Si A es un conjunto, sea $\mathcal{R}$ el conjunto de todas las relaciones de equivalencia en A y sea Π el conjunto de todas las particiones en A. En el ejemplo 13 de la sección 5.1 se construyó una correspondencia uno a uno f de $\mathcal{R}$ en Π. En el ejemplo 4 de la sección 7.1 se consideró el orden parcial $\subseteq$ en $\mathcal{R}$. Con este orden parcial se puede construir, utilizando f como se explicó anteriormente, un orden parcial $\leq'$ en Π. Por construcción, si $\mathcal{P}_1$ y $\mathcal{P}_2$ son particiones de A y R_1 y R_2, respectivamente, son las relaciones de equivalencia correspondientes a estas particiones, entonces $\mathcal{P}_1 \leq \mathcal{P}_2$ significará que $R_1 \subseteq R_2$. Como en el ejemplo 5 se mostró que $(\mathcal{R}, \subseteq)$ es una retícula, y se sabe que f es un isomorfismo, esto implica que $(\Pi, \leq')$ también es una retícula. En el ejercicio 29 se describió el orden parcial $\leq'$ directamente en términos de las propias particiones. ◆

Propiedades de las retículas

Antes de demostrar diversas propiedades de las retículas, hay que recordar el significado de $a \vee b$ y $a \wedge b$.

1. $a \leq a \vee b$ y $b \leq a \vee b$; $a \vee b$ es una cota superior de a y b.
2. Si $a \leq c$ y $b \leq c$, entonces $a \vee b \leq c$; $a \vee b$ es la mínima cota superior de a y b.

1′. $a \wedge b \leq a$, y $a \wedge b \leq b$; $a \wedge b$ es una cota inferior de a y b.

2′. Si $c \leq a$ y $c \leq b$, entonces $c \leq a$; $a \wedge b$; $a \wedge b$ es una máxima cota inferior de a y b.

Teorema 2. *Sea L una retícula. Entonces para toda a y b en L,*
(a) $a \vee b = b$ si y sólo si $a \leq b$.
(b) $a \wedge b = a$ si y sólo si $a \leq b$.
(c) $a \wedge b = a$ si y sólo si $a \vee b = b$.

Demostración: (a) Suponga que $a \vee b = b$. Como $a \leq a \vee b = b$, se tiene que $a \leq b$. Recíprocamente, si $a \leq b$, entonces, como $b \leq b$, b es una cota superior de a y b; de modo que por la definición de mínima cota superior, se tiene que $a \vee b \leq b$. Como $a \vee b$ es una cota superior, $b \leq a \vee b$, así $a \vee b = b$.

(b) La demostración es idéntica a la demostración de la parte (a), y se dejará como ejercicio al lector.

(c) La demostración es consecuencia de las partes (a) y (b). ●

Ejemplo 12. Sea L un conjunto linealmente ordenado. Si a y $b \in L$, entonces $a \leq b$ o $b \leq a$. El teorema 2 implica que L es una retícula, ya que cada pareja de elementos tiene una mínima cota superior y una máxima cota inferior. ◆

Teorema 3. *Sea L una retícula. Entonces*

1. (a) $a \vee a = a$
   (b) $a \wedge a = a$ — ***Propiedades de idempotencia***
2. (a) $a \vee b = b \vee a$
   (b) $a \wedge b = b \wedge a$ — ***Propiedades conmutativas***
3. (a) $a \vee (b \vee c) = (a \vee b) \vee c$
   (b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ — ***Propiedades asociativas***

4. (a) $a \vee (a \wedge b) = a$ **_Propiedades de absorción_**
   (b) $a \wedge (a \vee b) = a$

Demostración

1. Las proposiciones son consecuencia de la definición de LUB y GLB.
2. Tanto la definición de LUB como la de GLB consideran a y b en forma simétrica, de lo que se siguen los resultados.
3. (a) Por la definición de LUB, se tiene que $a \le a \vee (b \vee c)$ y $b \vee c \le a \vee (b \vee c)$. Además, $b \le b \vee c$ y $c \le b \vee c$, de modo que, por transitividad, $b \le a \vee (b \vee c)$ y $c \le a \vee (b \vee c)$. Así, $a \vee (b \vee c)$ es una cota superior de a y b, de modo que por la definición de mínima cota superior se tiene

$$a \vee b \le a \vee (b \vee c).$$

   Como $a \vee (b \vee c)$ es una cota superior de $a \vee b$ y c, se obtiene

$$(a \vee b) \vee c \le a \vee (b \vee c).$$

   De manera análoga, $a \vee (b \vee c) \le (a \vee b) \vee c$. Por la antisimetría de $\le$, se sigue la propiedad 3(a).
   (b) La demostración es análoga a la demostración de la parte (a) y se omite.
4. (a) Como $a \wedge b \le a$ y $a \le a$, se observa que a es una cota superior de $a \wedge b$ y a; así, $a \vee (a \wedge b) \le a$. Por otro lado, por la definición de LUB, se tiene que $a \le a \vee (a \wedge b)$, de modo que $a \vee (a \wedge b) = a$.
   (b) La demostración es análoga a la demostración de la parte (a) y se omite. ●

La propiedad 3 implica que se puede escribir $a \vee (b \vee c)$ y $(a \vee b) \vee c$ sólo como $a \vee b \vee c$, y de manera análoga para $a \wedge b \wedge c$. Además, se puede escribir

$$\text{LUB}(\{a_1, a_2, \ldots, a_n\}) \quad \text{como} \quad a_1 \vee a_2 \vee \cdots \vee a_n$$
$$\text{GLB}(\{a_1, a_2, \ldots, a_n\}) \quad \text{como} \quad a_1 \wedge a_2 \wedge \cdots \wedge a_n,$$

ya que es posible mostrar por inducción que estas uniones y conjunciones son independientes de la agrupación de términos.

Teorema 4. *Sea L una retícula. Entonces, para toda a, b y c en L,*

1. Si $a \le b$, entonces
   (a) $a \vee c \le b \vee c$.
   (b) $a \wedge c \le b \wedge c$.
2. $a \le c$ y $b \le c$ si y sólo si $a \vee b \le c$.
3. $c \le a$ y $c \le b$ si y sólo si $c \le a \wedge b$
4. Si $a \le b$ y $c \le d$, entonces
   (a) $a \vee c \le b \vee d$.
   (b) $a \wedge c \le b \wedge d$.

Demostración: La demostración se deja como ejercicio. ●

Tipos especiales de retículas

Una retícula L está **acotada** si tiene un elemento máximo I y un elemento mínimo 0 (véase la sección 7.2).

Ejemplo 13. La retícula Z^+ bajo el orden parcial de divisibilidad, definida en el ejemplo 2, no es una retícula acotada, pues tiene un elemento mínimo, el número 1, pero no tiene un elemento máximo. ◆

Ejemplo 14. La retícula Z bajo el orden parcial $\le$ no es acotada, pues no tiene elemento máximo ni mínimo. ◆

Ejemplo 15. La retícula $P(S)$ de todos los subconjuntos de un conjunto S, definida en el ejemplo 1, está acotada. Su elemento máximo es S y su elemento mínimo es $\varnothing$. ◆

Si L es una retícula acotada, entonces para toda $a \in A$

$$0 \le a \le I$$
$$a \vee 0 = a, \qquad a \wedge 0 = 0$$
$$a \vee I = I, \qquad a \wedge I = a.$$

Teorema 5. *Sea $L = \{a_1, a_2, \ldots, a_n\}$ una retícula finita. Entonces L es acotada.*

Demostración: El elemento máximo de L es $a_1 \vee a_2 \vee \cdots \vee a_n$, y su elemento mínimo es $a_1 \wedge a_2 \wedge \cdots \wedge a_n$. ●

Una retícula L es **distributiva** si para cualesquiera elementos a, b y c en L, se tiene las siguientes **propiedades distributivas**:

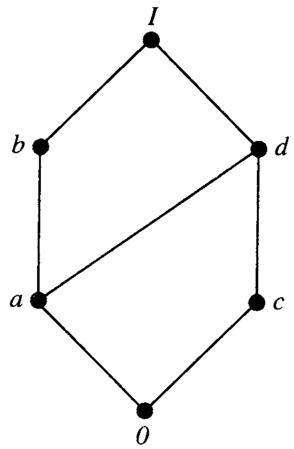
1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

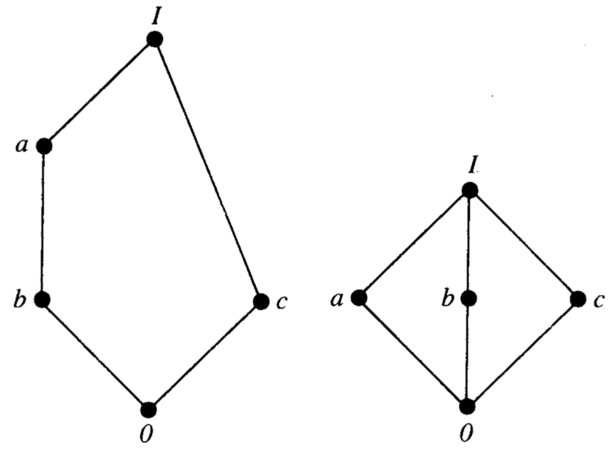
Si L no es distributiva, se dice que L es **no distributiva**.

Se deja como ejercicio mostrar que la propiedad distributiva es válida cuando cualesquiera dos de los elementos a, b y c son iguales o cuando cualquiera de los elementos es 0 o I. Esta observación reduce el número de casos que se debe revisar para verificar que es válida alguna propiedad distributiva. Sin embargo, la verificación de una propiedad distributiva es, por lo general, una tarea tediosa.

Ejemplo 16. Para un conjunto S, la retícula $P(S)$ es distributiva, ya que la unión y la intersección (la unión y la conjunción, respectivamente) satisfacen cada una la propiedad distributiva, como muestra la sección 1.2. ◆

Ejemplo 17. La retícula de la figura 7.43 es distributiva, como puede verse al verificar las propiedades distributivas para todas las ternas ordenadas elegidas de los elementos a, b, c y d. ◆





(a) (b)

Figura 7.43

Figura 7.44

Ejemplo 18. Muestre que las retículas de la figura 7.44 son no distributivas.

Solución

(a) Se tiene que

$$a \wedge (b \vee c) = a \wedge I = a$$

mientras que

$$(a \wedge b) \vee (a \wedge c) = b \vee 0 = b.$$

(b) Observe que

$$a \wedge (b \vee c) = a \wedge I = a$$

mientras que

$$(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0.$$

◆

Las retículas no distributivas analizadas en el ejemplo 18 son útiles para mostrar que una retícula dada es no distributiva, como garantiza el siguiente teorema, cuya demostración se omitirá.

Teorema 6. *Una retícula L es no distributiva si y sólo si contiene una subretícula isomorfa a alguna de las dos retículas del ejemplo* 18. ●

Puede utilizarse el teorema 6 de manera eficiente mediante la inspección del diagrama de Hasse de L.

Sea L una retícula acotada con elemento máximo I y elemento mínimo 0, y sea $a \in L$. Un elemento $a' \in L$ es un **complemento** de a si

$$a \vee a' = I \quad \text{y} \quad a \wedge a' = 0.$$

Observe que

$$0' = I \quad \text{y} \quad I' = 0.$$

Ejemplo 19. La retícula $L = P(S)$ es tal que todo elemento tiene un complemento, ya que si $A \in L$, entonces su conjunto complemento $\overline{A}$ tiene las propiedades $A \vee \overline{A} = S$ y $A \wedge \overline{A} = \varnothing$. ◆

Ejemplo 20. Cada una de las retículas de la figura 7.44 tienen la propiedad de que todo elemento tiene un complemento. El elemento c tiene en ambos casos dos complementos, a y b. ◆

Ejemplo 21. Considere las retículas D_{20} y D_{30} analizadas en el ejemplo 3 y que aparecen en la figura 7.39. Observe que todo elemento en D_{30} tiene un complemento. Por ejemplo, si $a = 5$, entonces $a' = 6$. Sin embargo, los elementos 2 y 10 en D_{20} no tienen complementos. ◆

Los ejemplos 20 y 21 muestran que un elemento a de una retícula no necesariamente tiene un complemento, y podría tener más de un complemento. Sin embargo, para una retícula distributiva acotada, la situación es más restrictiva, como muestra el siguiente teorema.

Teorema 7. *Sea L una retícula distributiva acotada. Si existe un complemento, es único.*

Demostración: Sean a' y a'' complementos del elemento $a \in L$. Entonces

$$a \vee a' = I, \qquad a \vee a'' = I$$
$$a \wedge a' = 0, \qquad a \wedge a'' = 0.$$

Se utiliza las leyes distributivas para obtener

$$\begin{aligned} a' = a' \vee 0 &= a' \vee (a \wedge a'') = (a' \vee a) \wedge (a' \vee a'') \\ &= (a \vee a') \wedge (a' \vee a'') \\ &= I \wedge (a' \vee a'') = a' \vee a''. \end{aligned}$$

Además,

$$\begin{aligned} a'' = a'' \vee 0 &= a'' \vee (a \wedge a') = (a'' \vee a) \wedge (a'' \vee a') \\ &= (a \vee a'') \wedge (a' \vee a'') \\ &= I \wedge (a' \vee a'') = a' \vee a''. \end{aligned}$$

Por lo tanto,

$$a' = a''.$$

●

Una retícula L es **complementada** si está acotada y si todo elemento en L tiene un complemento.

Ejemplo 22. La retícula $L = P(S)$ es complementada. Observe que, en este caso, cada elemento de L tiene un único complemento, lo que se puede ver en forma directa o mediante el teorema 7. ◆

Ejemplo 23. Las retículas analizadas en el ejemplo 20 y que aparecen en la figura 7.44 son complementadas. En este caso, los complementos no son únicos. ◆

GRUPO DE EJERCICIOS 7.3

En los ejercicios 1 al 3 (figuras 7.45 a la 7.50), determine si el diagrama de Hasse representa una retícula.

1. (a)

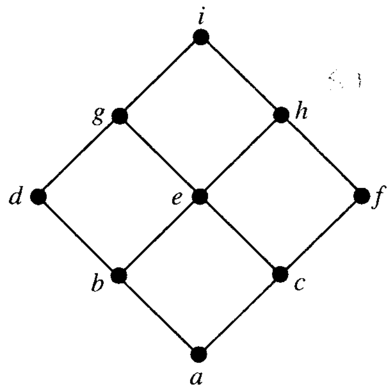


Figura 7.45

(b)

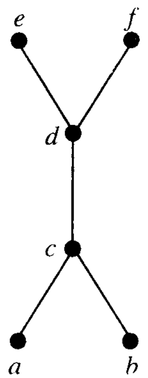


Figura 7.46

2. (a)

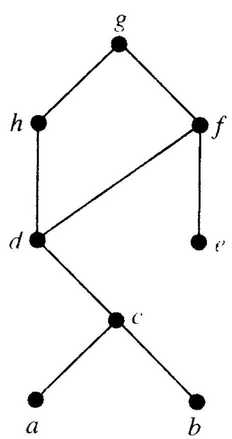


Figura 7.47

(b)

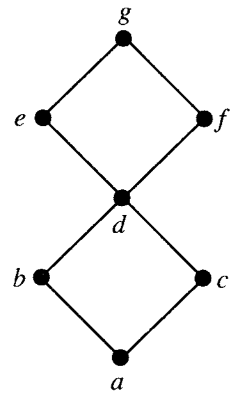


Figura 7.48

3. (a)

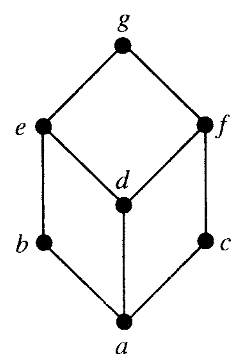


Figura 7.49

(b)

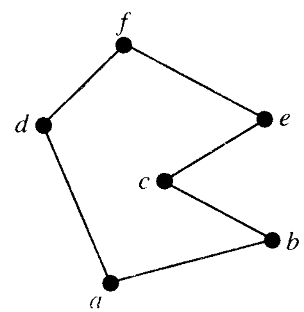


Figura 7.50

4. ¿Es una retícula el conjunto $A = \{2, 3, 6, 12, 24, 36, 72\}$, parcialmente ordenado bajo la relación de divisibilidad?

5. Si L_1 y L_2 son las retículas de la figura 7.51, trace el diagrama de Hasse de $L_1 \times L_2$ con el orden parcial producto.

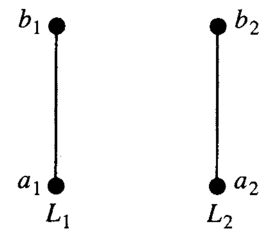


Figura 7.51

6. Sea $L = P(S)$ la retícula de todos los subconjuntos de un conjunto S bajo la relación de contención. Sea T un subconjunto de S. Muestre que $P(T)$ es una subretícula de L.

7. Sea L una retícula y sean a y b elementos de L tales que $a \leq b$. Se define el **intervalo** $[a, b]$ como el conjunto de $x \in L$ tales que $a \leq x \leq b$. Demuestre que $[a, b]$ es una subretícula de L.

8. Muestre que un subconjunto de un conjunto parcial y linealmente ordenado es una subretícula.

9. Determine todas las subretículas de D_{24} que contienen al menos cinco elementos.

10. Proporcione los diagramas de Hasse de todas las retículas no isomorfas con uno, dos, tres, cuatro o cinco elementos.

11. Muestre que si una retícula acotada tiene dos o más elementos, entonces $0 \neq I$.

12. Demuestre el teorema 2(b).

13. Muestre que la retícula Z^+ bajo el orden parcial usual $\leq$ es distributiva.

14. Muestre que la retícula D_n es distributiva para cualquier n.

15. Muestre que un conjunto parcial y linealmente ordenado es una retícula distributiva.

16. Muestre que una subretícula de una retícula distributiva es distributiva

17. Muestre que si L_1 y L_2 son retículas distributivas, entonces $L = L_1 \times L_2$ también es distributiva, donde el orden de L es el producto de las órdenes en L_1 y L_2.

18. ¿Es distributiva la retícula dual de una retícula distributiva? Justifique su conclusión.

19. Muestre que si $a \leq (b \wedge c)$ para a, b y c en un conjunto parcialmente ordenado L, entonces a, b y c satisfacen las propiedades distributivas de una retícula.

20. Demuestre que si a y b son elementos en una retícula distributiva acotada, y si a tiene un complemento a', entonces

$$a \vee (a' \wedge b) = a \vee b$$
$$a \wedge (a' \vee b) = a \wedge b.$$

21. Sea L una retícula distributiva. Muestre que si existe a tal que $a \wedge x = a \wedge y$ y $a \vee x = a \vee y$, entonces $x = y$.

22. Una retícula es **modular** si, para toda a, b y c, $a \leq c$ implica $a \vee (b \wedge c) = (a \vee b) \wedge c$.
   (a) Muestre que una retícula distributiva es modular.
   (b) Muestre que la retícula de la figura 7.52 es una retícula no distributiva que es modular.

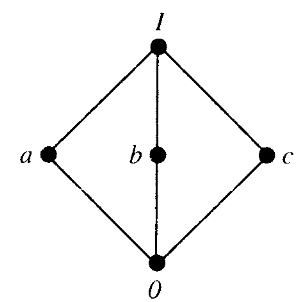


Figura 7.52

23. Determine el complemento de cada elemento en D_{42}.

24. Determine el complemento de cada elemento en D_{105}.

En los ejercicios 25 y 26 (figuras 7.53 a 7.56), determine si cada una de las retículas es distributiva, complementada, o ambas.

25. (a)

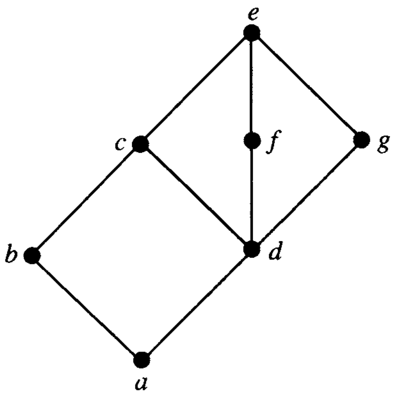


Figura 7.53

(b)

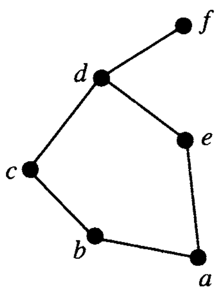


Figura 7.54

26. (a)

(b)

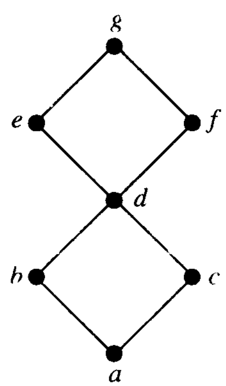


Figura 7.55 **Figura 7.56**

27. Sea L una retícula acotada, con al menos dos elementos. Muestre que ningún elemento de L es su propio complemento.

28. Considere la retícula complementada de la figura 7.57. Proporcione los complementos de cada uno de los elementos.

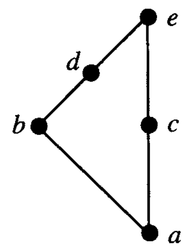


Figura 7.57

29. Sean $\mathcal{P}_1 = \{A_1, A_2, \ldots\}$, $\mathcal{P}_2 = \{B_1, B_2, \ldots\}$ dos particiones de un conjunto S. Muestre que $\mathcal{P}_1 \leq \mathcal{P}_2$ (véase la definición en el ejemplo 11) si y sólo si cada A_i está contenido en algún B_j.

30. Sea $S = \{a, b, c\}$ y $L = P(S)$. Demuestre que $(L, \subseteq)$ es isomorfo a D_{42}.

7.4. Álgebras booleanas finitas

En esta sección se analizará cierto tipo de retículas que tiene muchas aplicaciones en la ciencia de la computación. En el ejemplo 6 de la sección 7.3 se vio que si S es un conjunto, $L = P(S)$ y $\subseteq$ es la relación usual de contención, entonces el conjunto parcialmente ordenado $(L, \subseteq)$ es una retícula. Estas retículas tienen muchas propiedades que no son compartidas por todas las retículas en general. Por esta razón, es más sencillo trabajar con ellas, y juegan un papel más importante en diversas aplicaciones.

Se restringirá nuestra atención en las retículas $(P(S), \subseteq)$, donde S es un conjunto finito; se comenzará por determinar todos los ejemplos esencialmente diferentes.

Teorema 1. *Si $S_1 = \{x_1, x_2, \ldots, x_n\}$ y $S_2 = \{y_1, y_2, \ldots, y_n\}$ son dos conjuntos finitos cualesquiera con n elementos, entonces las retículas $(P(S_1), \subseteq)$ y $(P(S_2), \subseteq)$ son isomorfas. En particular, puede trazarse los diagramas de Hasse de estas retículas de manera idéntica.*

Demostración: Se ordena los conjuntos como en la figura 7.58, de modo que cada elemento de S_1 se encuentre directamente sobre el elemento en S_2 con el número correspondiente. Para cada subconjunto A de S_1, sea $f(A)$ el subconjunto de S_2 formado por todos los elementos correspondientes con los elementos de A. La figura 7.59 muestra un subconjunto típico A de S_1 y el subconjunto correspondiente $f(A)$ de S_2. Es fácil ver que la función f, descrita antes, es una correspondencia uno a uno de los subconjuntos de S_1 a los subconjuntos de S_2. También es claro que si A y B son subconjuntos arbitrarios de S_1, entonces $A \subseteq B$ si y sólo si $f(A) \subseteq f(B)$. Se omitirá los detalles. Así, las retículas $(P(S_1), \subseteq)$ y $(P(S_2), \subseteq)$ son isomorfas. ●

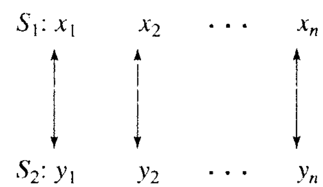


Figura 7.58

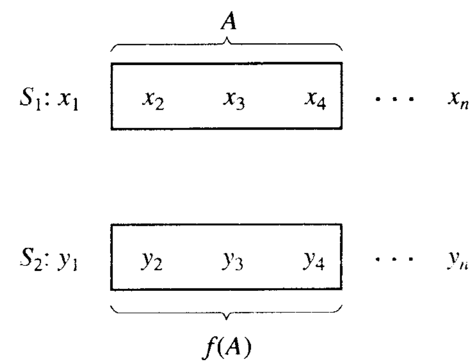
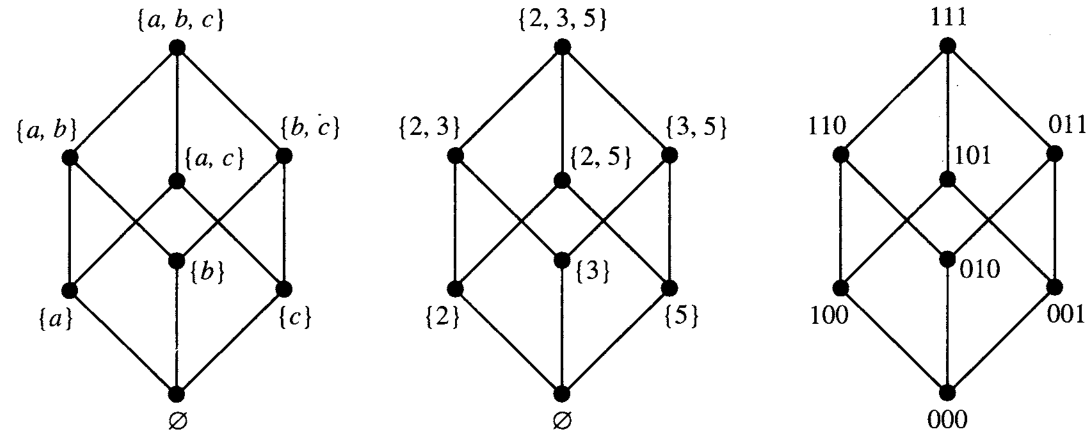


Figura 7.59

El punto esencial de este teorema es que la retícula $(P(S), \subseteq)$ queda determinada completamente como conjunto parcialmente ordenado por el número $|S|$ y no depende de la naturaleza de los elementos en S.

Ejemplo 1. La figura 7.60(a) y (b) muestra los diagramas de Hasse para las retículas $(P(S), \subseteq)$ y $(P(T), \subseteq)$, respectivamente, donde $S = \{a, b, c\}$ y $T = \{2, 3, 5\}$. Es claro de la figura que las dos retículas son isomorfas. De hecho, se observa que un posible isomorfismo $f: S \to T$ está dado por



(a) (b) (c)

Figura 7.60

$$f(\{a\}) = \{2\}, \quad f(\{b\}) = \{3\}, \quad f(\{c\}) = \{5\},$$
$$f(\{a, b\}) = \{2, 3\}, \quad f(\{b, c\}) = \{3, 5\}, \quad f(\{a, c\}) = \{2, 5\},$$
$$f(\{a, b, c\}) = \{2, 3, 5\} \quad f(\varnothing) = \varnothing. \quad \blacklozenge$$

Así, para cada $n = 0, 1, 2, \ldots,$ sólo existe un tipo de retícula de la forma $(P(S), \subseteq)$. Esta retícula sólo depende de n, no de S, y tiene 2^n elementos, como se mostró en el ejemplo 2 de la sección 3.1. Recuérdese de la sección 1.3 que si un conjunto S tiene n elementos, entonces es posible representar todos los subconjuntos de S mediante sucesiones de longitud n de ceros y unos. Por lo tanto, se puede etiquetar el diagrama de Hasse de una retícula $(P(S), \subseteq)$ mediante tales sucesiones. Al hacer esto, se libera al diagrama de la dependencia de un conjunto particular S y se enfatiza el hecho de que sólo depende de n.

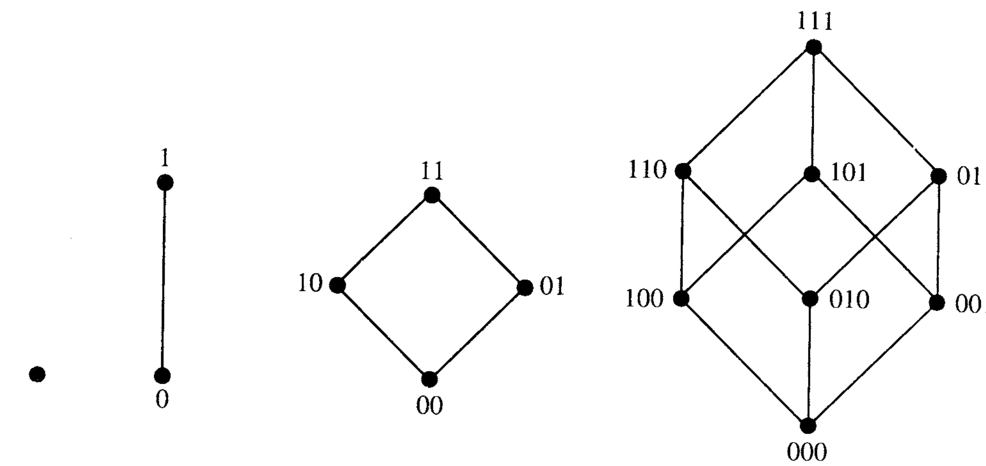
Ejemplo 2. La figura 7.60(c) muestra la forma en que los diagramas de la 7.60(a) y (b) pueden ser etiquetados mediante sucesiones de ceros y unos. Este etiquetado sirve también para describir la retícula de la figura 7.60(a) y (b), o igualmente, la retícula $(P(S), \subseteq)$ que surge de cualquier conjunto S con tres elementos. ◆

Si el diagrama de Hasse de la retícula correspondiente a un conjunto con n elementos es etiquetado mediante sucesiones de ceros y unos de longitud n, como se describió antes, entonces la retícula resultante se denota B_n. Puede describirse de manera directa las propiedades del orden parcial en B_n como sigue. Si $x = a_1a_2 \cdots a_n$ y $y = b_1b_2 \cdots b_n$ son dos elementos de B_n, entonces

1. $x \leq y$ si y sólo si $a_k \leq b_k$ (como números cero o uno) para $k = 1, 2, \ldots, n$.
2. $x \wedge y = c_1c_2 \cdots c_n$, donde $c_k = \min\{a_k, b_k\}$.
3. $x \vee y = d_1d_2 \cdots d_n$, donde $d_k = \max\{a_k, b_k\}$.
4. x tiene un complemento $x' = z_1z_2 \cdots z_n$, donde $z_k = 1$ si $x_k = 0$ y $z_k = 0$ si $x_k = 1$.

Como puede verse, estos enunciados son ciertos observando que $(B_n, \leq)$ es isomorfo a $(P(S), \subseteq)$, de modo que cada x y y en B_n corresponde a los subconjuntos A y B de S. Entonces

$x \leq y, x \wedge y, x \vee y, y\, x'$, definidos anteriormente, corresponden a $A \subseteq B, A \cap B, A \cup B$ y $\bar{A}$ (complemento del conjunto), respectivamente. (Verifique.) La figura 7.61 muestra los diagramas de Hasse de las retículas B_n para $n = 0, 1, 2, 3$.



$n = 0$ $n = 1$ $n = 2$ $n = 3$

Figura 7.61

Se ha visto que cada retícula $(P(S), \subseteq)$ es isomorfa a B_n, donde $n = |S|$. Otras retículas también pueden ser isomorfas con algún B_n y por lo tanto tienen todas las propiedades especiales que posee B_n.

Ejemplo 3. En el ejemplo 17 de la sección 7.1 se consideró la retícula D_6 formada por todos los divisores enteros positivos de 6 bajo el orden parcial de divisibilidad. En ese ejemplo se muestra el diagrama de Hasse de D_6 y ahora se observa que D_6 es isomorfa a B_2. De hecho, $f: D_6 \to B_2$ es un isomorfismo, donde

$$f(1) = 00, \quad f(2) = 10, \quad f(3) = 01, \quad f(6) = 11. \quad \blacklozenge$$

Por lo tanto, se ha llegado a la siguiente definición. Una retícula finita es un **álgebra booleana** si es isomorfa a B_n para algún entero no negativo n. Así, cada B_n es un álgebra booleana, al igual que cada retícula $(P(S), \subseteq)$, donde S es un conjunto finito. El ejemplo 3 muestra que D_6 también es un álgebra booleana.

En esta sección sólo se trabajará con conjuntos parcialmente ordenados finitos. Sin embargo, para quien tenga curiosidad, se remarca el hecho de que existen conjuntos parcialmente ordenados que comparten todas las propiedades importantes de las retículas $(P(S), \subseteq)$ (para conjuntos infinitos S, por supuesto), pero que no son isomorfos a alguna de estas retículas. Esto refuerza la restricción de la definición de álgebra booleana al caso finito, lo que basta para las aplicaciones que serán presentadas.

Ejemplo 4. Considérese las retículas D_{20} y D_{30} de todos los divisores enteros positivos de 20 y 30, respectivamente, bajo el orden parcial de divisibilidad. Estos conjuntos parcialmente ordenados fueron presentados en el ejemplo 3 de la sección 7.3, y se mostró sus diagramas de Hasse en la figura 7.39. Como D_{20} tiene cinco elementos y $5 \neq 2^n$ para cualquier entero $n \geq 0$, se concluye que D_{20} no es un álgebra booleana. El conjunto parcialmente ordenado D_{30} tiene ocho elementos; como $8 = 2^3$, podría ser un álgebra booleana. Al comparar la figura 7.39(b) y la figura 7.61, se observa que D_{30} es isomorfo a B_3. De hecho, se ve que la correspondencia uno a uno $f = D_{30} \to B_3$ dada por

$$f(1) = 000, \quad f(2) = 100, \quad f(3) = 010,$$
$$f(5) = 001, \quad f(6) = 110, \quad f(10) = 101,$$
$$f(15) = 011, \quad f(30) = 111,$$

es un isomorfismo. Así, D_{30} es un álgebra booleana. ◆

Si una retícula finita L no contiene 2^n elementos para algún entero no negativo n, se sabe que L no puede ser un álgebra booleana. Si $|L| = 2^n$, entonces L podría ser un álgebra booleana. Si L es relativamente pequeño, se podría comparar su diagrama de Hasse con el de B_n. De esta forma se vio en el ejemplo 4 que D_{30} es un álgebra booleana. Sin embargo, esta técnica podría dejar de ser práctica si L es grande. En ese caso, se podría mostrar que L es un álgebra booleana construyendo de manera directa un isomorfismo con cierto B_n, o de manera equivalente, con $(P(S), \subseteq)$ para algún conjunto finito S. Por ejemplo, supóngase que se desea saber si una retícula D_n es un álgebra booleana, y se necesita un método que funcione sin importar el tamaño de n. El siguiente teorema proporciona una respuesta parcial.

Teorema 2. *Sea*

$$n = p_1 p_2 \cdots p_k,$$

donde los p_i son primos distintos. Entonces D_n es un álgebra booleana.

Demostración: Sea $S = \{p_1, p_2, \ldots, p_k\}$. Si $T \subseteq S$ y a_T es el producto de los primos en T, entonces $a_T \mid n$. Cualquier divisor de n debe ser de la forma a_T para algún subconjunto T de S (donde $a_\varnothing = 1$). El lector puede verificar que si V y T son subconjuntos de S, $V \subseteq T$ si y sólo si $a_V \mid a_T$. Además, la demostración del teorema 6 de la sección 1.4 muestra que $a_{V \cap T} = a_V \wedge a_T = \text{MCD}(a_V, a_T)$ y $a_{V \cup T} = a_V \vee a_T = \text{MCM}(a_V, a_T)$. Así, la función $f: P(S) \to D_n$ dada por $f(T) = a_T$ es un isomorfismo de $P(S)$ a D_n. Como $P(S)$ es un álgebra booleana, también D_n lo es. ●

Ejemplo 5. Como $210 = 2 \cdot 3 \cdot 5 \cdot 7$, $66 = 2 \cdot 3 \cdot 11$ y $646 = 2 \cdot 17 \cdot 19$, el teorema 2 implica que D_{210}, D_{66} y D_{646} son álgebras booleanas. ◆

En otros casos de retículas L de gran tamaño, se podría demostrar que L no es un álgebra booleana mostrando que el orden parcial de L no tiene las propiedades necesarias. Un álgebra booleana es isomorfa a algún B_n y por lo tanto con alguna retícula $(P(S), \subseteq)$. Así, un álgebra booleana debe ser una retícula acotada y complementada (véase la sección 7.3). En otras palabras, tendrá un elemento máximo I correspondiente al conjunto S y un elemento mínimo 0 correspondiente al subconjunto $\varnothing$. Además, cada elemento x de L tendrá un complemento x'. De acuerdo con el ejemplo 16, L debe ser también distributiva. El principio de correspondencia (véase la sección 7.1) nos dice entonces que se cumple la siguiente regla.

Teorema 3 (Regla de sustitución para álgebras booleanas). *Cualquier fórmula que implique $\cup$ o $\cap$ o que se cumpla para subconjuntos arbitrarios de un conjunto S sigue siendo válida para elementos arbitrarios de un álgebra booleana L si $\wedge$ se sustituye por $\cap$ y $\vee$ por $\cup$.* ●

Ejemplo 6. Si L es cualquier álgebra booleana y x, y, z están en L, entonces se cumplen las siguientes tres propiedades.

1. $(x')' = x$ ***Propiedad de involución***
2. $(x \wedge y)' = x' \vee y'$
3. $(x \vee y)' = x' \wedge y'$ ***Leyes de De Morgan***

Esto es cierto por la regla de sustitución para álgebras booleanas, pues se sabe que las fórmulas correspondientes

1′. $\overline{(\overline{A})} = A$.
2′. $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.
3′. $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$.

son válidas para subconjuntos arbitrarios A y B de un conjunto S. ◆

De manera similar, puede enumerarse otras propiedades que deben ser válidas en cualquier álgebra booleana por la regla de sustitución. A continuación, se hace un resumen de todas las propiedades básicas de un álgebra booleana $(L, \leq)$ y, junto a éstas, se enumera la propiedad correspondiente para subconjuntos de un conjunto S. Se supone que x, y, z son elementos arbitrarios en L y A, B, C son subconjuntos arbitrarios de S. Además, se denota los elementos máximo y mínimo de L como I y 0, respectivamente.

1. $x \leq y$ si y sólo si $x \vee y = y$.	1′. $A \subseteq B$ si y sólo si $A \cup B = B$.
2. $x \leq y$ si y sólo si $x \wedge y = x$.	2′. $A \subseteq B$ si y sólo si $A \cap B = A$.
3. (a) $x \vee x = x$. (b) $x \wedge x = x$.	3′. (a) $A \cup A = A$. (b) $A \cap A = A$.
4. (a) $x \vee y = y \vee x$. (b) $x \wedge y = y \wedge x$.	4′. (a) $A \cup B = B \cup A$. (b) $A \cap B = B \cap A$.
5. (a) $x \vee (y \vee z) = (x \vee y) \vee z$. (b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.	5′. (a) $A \cup (B \cup C) = (A \cup B) \cup C$. (b) $A \cap (B \cap C) = (A \cap B) \cap C$.
6. (a) $x \vee (x \wedge y) = x$. (b) $x \wedge (x \vee y) = x$.	6′. (a) $A \cup (A \cap B) = A$. (b) $A \cap (A \cup B) = A$.
7. $0 \leq x \leq I$ para toda x en L.	7′. $\varnothing \subseteq A \subseteq S$ para todo A en $P(S)$.
8. (a) $x \vee 0 = x$. (b) $x \wedge 0 = 0$.	8′. (a) $A \cup \varnothing = A$. (b) $A \cap \varnothing = \varnothing$.
9. (a) $x \vee I = I$. (b) $x \wedge I = x$.	9′. (a) $A \cup S = S$. (b) $A \cap S = A$.
10. (a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. (b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.	10′. (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
11. Todo elemento x tiene un *único* complemento x' que satisface (a) $x \vee x' = I$. (b) $x \wedge x' = 0$.	11′. Todo elemento A tiene un *único* complemento $\overline{A}$ que satisface (a) $A \cup \overline{A} = S$. (b) $A \cap \overline{A} = \varnothing$.

12. (a) $0' = I$.	12′. (a) $\overline{\varnothing} = S$.
(b) $I' = 0$.	(b) $\overline{S} = \varnothing$.
13. $(x')' = x$.	13′. $\overline{(\overline{A})} = A$.
14. (a) $(x \wedge y)' = x' \vee y'$.	14′. (a) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.
(b) $(x \vee y)' = x' \wedge y'$.	(b) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$.

Así, se podría mostrar que una retícula L no es un álgebra booleana mostrando que no posee una o más de estas propiedades.

Ejemplo 7. Muestre que la retícula cuyo diagrama de Hasse aparece en la figura 7.62 no es un álgebra booleana.

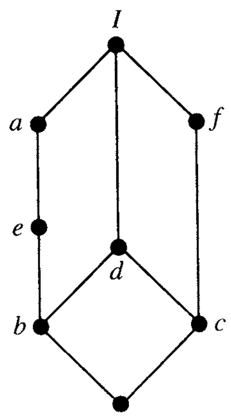


Figura 7.62

Solución: Los elementos a y e son ambos complementos de c; es decir, ambos satisfacen las propiedades 11(a) y 11(b) con respecto del elemento c. Pero la propiedad 11 dice que tal elemento es único en cualquier álgebra booleana. Así, la retícula dada no puede ser un álgebra booleana. ◆

Ejemplo 8. Muestre que si n es un entero positivo y $p^2 \mid n$, donde p es un número primo, entonces D_n no es un álgebra booleana.

Solución: Supóngase que $p^2 \mid n$ de modo que $n = p^2q$ para algún entero positivo q. Como p también es divisor de n, p es un elemento de D_n. Así, por las observaciones anteriores, si D_n es un álgebra booleana, entonces p debe tener un complemento p'. Entonces MCD $(p, p') = 1$ y MCM $(p, p') = n$. Por el teorema 6 de la sección 1.4, $pp' = n$, de modo que $p' = n/p = pq$. Esto muestra que MCD $(p, pq) = 1$, lo que es imposible, pues p y pq tienen a p como divisor común. Por lo tanto, D_n no puede ser un álgebra booleana. ◆

Si se combina el ejemplo 8 y el teorema 2, se ve que D_n es un álgebra booleana si y sólo si n es el producto de primos distintos, es decir, si y sólo si ningún primo divide a n más de una vez.

Ejemplo 9. Si $n = 40$, entonces $n = 2^3 \cdot 5$, de modo que 2 divide a n tres veces. Si $n = 75$, entonces $n = 3 \cdot 5^2$, de modo que 5 divide a n dos veces. Así, D_{40} y D_{75} no son álgebras booleanas. ◆

Ahora se resumirá lo que ha sido mostrado en relación con las álgebras booleanas. Puede intentarse demostrar que una retícula L es un álgebra booleana examinando su diagrama de Hasse o construyendo de manera directa un isomorfismo entre L y B_n o $(P(S), \subseteq)$. Puede intentarse mostrar que L no es un álgebra booleana verificando el número de elementos en L o las propiedades de su orden parcial. Si L es un álgebra booleana, entonces es posible utilizar cualesquiera de las propiedades 1 a 14 para manipular o simplificar expresiones que impliquen elementos de L. Sólo hay que proceder como si los elementos fuesen subconjuntos y las manipulaciones fuesen como las que surgen en la teoría de conjuntos.

A partir de este momento se denotará el álgebra booleana B_1 como B. Así, B sólo tiene los dos elementos 0 y 1. A veces es útil saber que cualquier álgebra booleana B_n puede ser descrita en términos de B. El siguiente teorema proporciona esta descripción.

Teorema 4. *Para cualesquiera $n \geq 1$, B_n es el producto $B \times B \times \cdots \times B$ de B, con n factores, donde $B \times B \times \cdots \times B$ tiene el orden parcial producto.*

Demostración: Por definición, B_n está formado por todas las n-adas de ceros y unos; es decir, todas las n-adas de elementos de B. Así, como conjunto, B_n es igual a $B \times B \times \cdots \times B$ (n factores). Además, si $x = x_1x_2\cdots x_n$ y $y = y_1y_2\cdots y_n$ son dos elementos de B_n, entonces se sabe que

$$x \leq y \quad \text{si y sólo si} \quad x_k \leq y_k \qquad \text{para toda } k.$$

Por lo tanto, B_n, identificado con $B \times B \times \cdots \times B$ (n factores), tiene el orden parcial producto. ●

GRUPO DE EJERCICIOS 7.4

En los ejercicios 1 al 10, determine si el conjunto parcialmente ordenado es un álgebra booleana. Explique.

1.

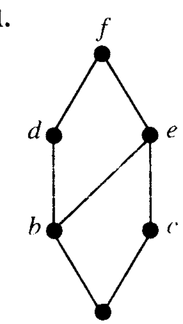


Figura 7.63

2.

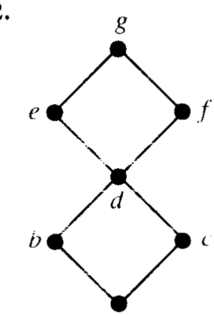


Figura 7.64

3.

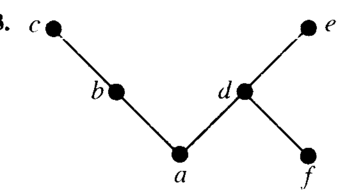


Figura 7.65

4.

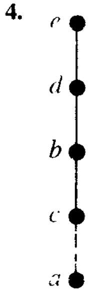


Figura 7.66

5.

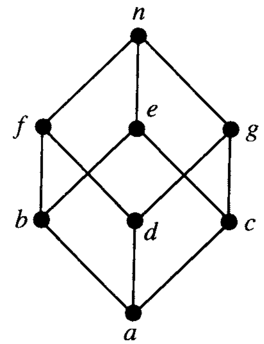


Figura 7.67

6.

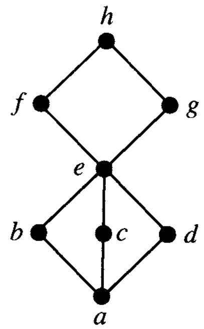


Figura 7.68

7.

Figura 7.69

8.

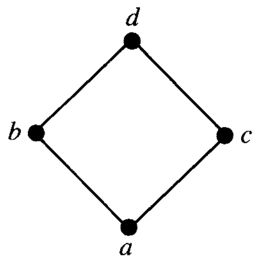


Figura 7.70

9. D_{385}

10. D_{60}

11. ¿Existen álgebras booleanas con tres elementos? ¿Por que sí o por qué no?

12. Muestre que en un álgebra booleana, para cualesquiera a y b, $a \le b$ si y sólo si $b' \le a'$.

13. Muestre que en un álgebra booleana, para cualesquiera a y b, $a = b$ si y sólo si $(a \wedge b') \vee (a' \wedge b) = 0$.

14. Muestre que en un álgebra booleana, para cualesquiera a, b y c,
(a) Si $a \le b$, entonces $a \vee c \le b \vee c$
(b) Si $a \le b$, entonces $a \wedge c \le b \wedge c$.

15. Muestre que en un álgebra booleana, los siguientes enunciados son equivalentes para cualesquiera a y b.
(a) $a \vee b = b$
(b) $a \wedge b = a$
(c) $a' \vee b = I$
(d) $a \wedge b' = 0$
(e) $a \le b$

16. Muestre que en un álgebra booleana, para cualesquiera a y b,

$$(a \wedge b) \vee (a \wedge b') = a.$$

17. Muestre que en un álgebra booleana, para cualesquiera a y b,

$$b \wedge (a \vee (a' \wedge (b \vee b'))) = b.$$

18. Muestre que en un álgebra booleana, para cualesquiera a, b y c,

$$(a \wedge b \wedge c) \vee (b \wedge c) = b \wedge c.$$

19. Muestre que en un álgebra booleana, para cualesquiera a, b y c,

$$((a \vee c) \wedge (b' \vee c))' = (a' \vee b) \wedge c'.$$

20. Muestre que en un álgebra booleana, para cualesquiera a, b y c, si $a \le b$, entonces

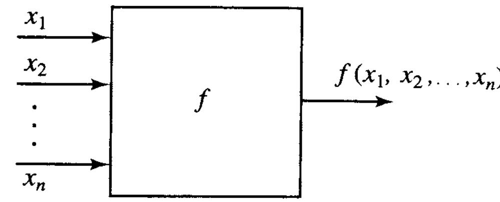
$$a \vee (b \wedge c) = b \wedge (a \vee c).$$

7.5. Funciones de álgebras booleanas

Las tablas que enumeran los valores de una función f para todos los elementos de B_n, como la que se muestra en la figura 7.71(a), con frecuencia son llamadas tablas de verdad para f. Esto se debe a que son similares a las tablas empleadas en la lógica (véase la sección 2.1). Suponga que los x_k representan proposiciones, y $f(x_1, x_2, \ldots, x_n)$ representa un enunciado compuesto construido a partir de los x_k. Si piensa que el valor 0 para un enunciado significa que el enunciado es falso, y que 1 significa que el enunciado es verdadero, entonces las tablas, como la de la figura 7.71(a), muestran la forma en que la verdad o falsedad de $f(x_1, x_2, \ldots, x_n)$ depende de la verdad o falsedad de los enunciados x_k que lo componen. Así, tales

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

(a)



(b)

Figura 7.71

tablas son llamadas, con frecuencia, **tablas de verdad**, incluso cuando surgen en áreas distintas de la lógica, como en las álgebras booleanas.

La razón de la importancia de tales funciones es que, como se muestra de manera esquemática en la figura 7.71(b), pueden ser utilizadas para representar los requisitos de salida de un circuito para los posibles valores de entrada. Así, cada x_i representa un circuito de entrada capaz de transportar dos voltajes indicadores (un voltaje para 0 y un voltaje distinto para 1). La función f representa la respuesta de salida deseada en todos los casos. Tales requisitos ocurren en la etapa de diseño de los circuitos computacionales combinatorios y secuenciales.

Observe con cuidado que la especificación de una función $f: B_n \to B$ sólo enumera los requisitos del circuito. No indica cómo cumplir estos requisitos. Una forma importante de producir funciones de B_n a B es mediante el uso de polinomios booleanos, los cuales son considerados a continuación.

Polinomios booleanos

Sea $x_1, x_2, \ldots, x_n$ un conjunto de n símbolos o variables. Un **polinomio booleano** $p(x_1, x_2, \ldots, x_n)$ en las variables x_k se define de manera recursiva como sigue:

1. $x_1, x_2, \ldots, x_n$ son todos polinomios booleanos.
2. Los símbolos 0 y 1 son polinomios booleanos.
3. Si $p(x_1, x_2, \ldots, x_n)$ y $q(x_1, x_2, \ldots, x_n)$ son dos polinomios booleanos, entonces también lo son

$$p(x_1, x_2, \ldots, x_n) \vee q(x_1, x_2, \ldots, x_n)$$

y

$$p(x_1, x_2, \ldots, x_n) \wedge q(x_1, x_2, \ldots, x_n).$$

4. Si $p(x_1, x_2, \ldots, x_n)$ es un polinomio booleano, entonces también lo es

$$(p(x_1, x_2, \ldots, x_n))'.$$

Por tradición, $(0)'$ se denota $0'$, $(1)'$ se denota $1'$ y $(x_k)'$ se denota x'_k.

5. No existen polinomios booleanos en las variables x_k distintos de los que pueden ser obtenidos aplicando las reglas 1, 2, 3 y 4.

Los polinomios booleanos también reciben el nombre de **expresiones booleanas**.

Ejemplo 1. Los siguientes son polinomios booleanos en las variables x, y, z.

$$p_1(x, y, z) = (x \vee y) \wedge z$$
$$p_2(x, y, z) = (x \vee y') \vee (y \wedge 1)$$
$$p_3(x, y, z) = (x \vee (y' \wedge z)) \vee (x \wedge (y \wedge 1))$$
$$p_4(x, y, z) = (x \vee (y \vee z')) \wedge ((x' \wedge z)' \wedge (y' \vee 0)).$$ ◆

Por lo general, los polinomios comunes en varias variables, como $x^2y + z^4$, $xy + yz + x^2y^2$, $x^3y^3 + xz^4$, etcétera, son interpretados como expresiones que representan cálculos algebraicos con incógnitas. Como tales, están sujetos a las reglas usuales de la aritmética. Así, los polinomios $x^2 + 2x + 1$ y $(x + 1)(x + 1)$ son considerados equivalentes, al igual que los polinomios $x(xy + yz)(x + z)$ y $x^3y + 2x^2yz + xyz^2$, ya que en cada caso se puede convertir uno en el otro mediante una manipulación algebraica.

De igual manera, es posible interpretar los polinomios booleanos de manera que representen cálculos booleanos con elementos no específicos de B, es decir, con ceros y unos. Como tales, estos polinomios están sujetos a las reglas de la aritmética booleana; es decir, a las reglas que obedecen $\wedge$, $\vee$ y $'$ en las álgebras booleanas. Como en el caso de los polinomios comunes, dos polinomios booleanos son equivalentes si es posible transformar uno en el otro con manipulaciones booleanas.

En la sección 5.1 se muestra la forma en que los polinomios ordinarios podrían producir funciones mediante la sustitución. Este proceso funciona sin importar que los polinomios tengan una o más variables. Así, el polinomio $xy + yz^3$ produce una función $f: \mathbb{R}^3 \to \mathbb{R}$ haciendo $f(x, y, z) = xy + yz^3$. Por ejemplo, $f(3, 4, 2) = (3)(4) + (4)(2^3) = 44$. De manera similar, los polinomios booleanos que implican n variables producen funciones de B_n en B. Estas funciones booleanas son una generalización natural de las presentadas en la sección 5.2.

Ejemplo 2. Considérese el polinomio booleano

$$p(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \vee (x_2' \wedge x_3)).$$

Construya la tabla de verdad para la función booleana $f: B_3 \to B$ determinada por este polinomio booleano.

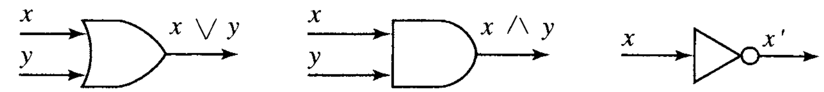
Solución: La función booleana $f: B_3 \to B$ se describe sustituyendo las 2^3 ternas ordenadas de valores de B en vez de x_1, x_2 y x_3. La figura 7.72 muestra la tabla de verdad para la función resultante. ◆

Los polinomios booleanos también pueden ser escritos de manera gráfica o esquemática. Si x y y son variables, entonces los polinomios básicos $x \vee y$, $x \wedge y$ y x' aparecen de manera esquemática en la figura 7.73. Cada símbolo tiene líneas para las variables a la izquierda y una línea a la derecha que representa al polinomio como un todo. El símbolo para $x \vee y$ es una **compuerta or**, el de $x \wedge y$ es una **compuerta and** y el símbolo para x' es

x_1	x_2	x_3	$f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \vee (x_2' \wedge x_3))$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Figuras 7.72

un **inversor**. Los nombres lógicos surgen debido a que las tablas de verdad que muestran las funciones representadas por $x \vee y$ y $x \wedge y$ son análogos exactos de la tabla de verdad para los conectivos "o" (disyunción) e "y" (conjunción), respectivamente.



(a) (b) (c)

Figura 7.73

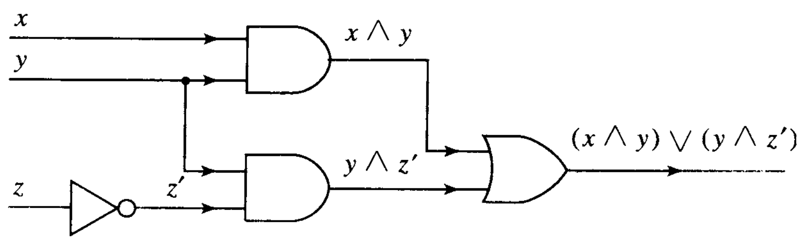
Recuerde que se puede utilizar las funciones de B_n a B para describir el comportamiento deseado de circuitos con n entradas 0 o 1, y una salida 0 o 1. En el caso de las funciones correspondientes a los polinomios booleanos $x \vee y$, $x \wedge y$ y x', puede implantarse los circuitos deseados; también se utiliza las formas esquemáticas de la figura 7.73 para representar estos circuitos. Al sustituir varias veces $\vee$, $\wedge$ y $'$ en estas formas esquemáticas, es posible crear una forma esquemática para representar cualquier polinomio booleano. Por las razones dadas, tales diagramas son los **diagramas lógicos** del polinomio.

Ejemplo 3. Sea $p(x, y, z) = (x \wedge y) \vee (y \wedge z')$. La figura 7.74(a) muestra la tabla de verdad para la función correspondiente $f: B_3 \to B$. La figura 7.74(b) muestra el diagrama lógico para p. ◆

Supóngase que p es un polinomio booleano de n variables, y f es la función correspondiente de B_n a B. Se conoce que f puede ser pensada como una descripción del comportamiento de un circuito con n entradas y una salida. De la misma forma, el diagrama lógico de p se puede ver como una descripción de la construcción de dicho circuito, al menos en términos de compuertas or, compuertas and e inversores. Así, si la función f, que describe el comportamiento deseado de un circuito, puede obtenerse de un polinomio booleano p, entonces el diagrama lógico para p proporcionará una forma de construir un circuito con tal comportamiento. En general, muchos polinomios distintos producirán la misma función. Los diagramas lógicos de estos polinomios representarán métodos alternativos para construir el circuito deseado. Es casi imposible sobrestimar la importancia de estos hechos para el estudio de los circuitos computacionales.

x	y	z	$f(x, y, z) = (x \wedge y) \vee (y \wedge z')$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

(a)



(b)

Figura 7.74

GRUPO DE EJERCICIOS 7.5

1. Considere el polinomio booleano
$$p(x, y, z) = x \wedge (y \vee z').$$
Si $B = \{0, 1\}$, calcule la tabla de verdad de la función $f: B_3 \to B$ definida por p.

2. Considere el polinomio booleano
$$p(x, y, z) = (x \vee y) \wedge (z \vee x').$$
Si $B = \{0, 1\}$, calcule la tabla de verdad de la función $f: B_3 \to B$ definida por p.

3. Considere el polinomio booleano
$$p(x, y, z) = (x \wedge y') \vee (y \wedge (x' \vee y)).$$
Si $B = \{0, 1\}$, calcule la tabla de verdad de la función $f: B_3 \to B$ definida por p.

4. Considere el polinomio booleano
$$p(x, y, z) = (x \wedge y) \vee (x' \wedge (y \wedge z')).$$
Si $B = \{0, 1\}$, calcule la tabla de verdad de la función $f: B_3 \to B$ definida por p.

En los ejercicios 5 al 8, aplique las reglas de la aritmética booleana para mostrar que los polinomios booleanos dados son equivalentes.

5. $(x \vee y) \wedge (x' \vee y)$; y

6. $x \wedge (y \vee (y' \wedge (y \vee y')))$; x

7. $(z' \vee x) \wedge ((x \wedge y) \vee z) \wedge (z' \vee y)$; $x \wedge y$

8. $[(x \wedge z) \vee (y' \vee z)'] \vee [(y \wedge z) \vee (x \wedge z')]$; $x \vee y$

9. Construya un diagrama lógico que implemente la función f de
(a) El ejercicio 1. (b) El ejercicio 2.

10. Construya un diagrama lógico que implemente la función f de
(a) El ejercicio 3. (b) El ejercicio 4.

7.6. Funciones booleanas como polinomios booleanos (diseño de circuitos)

En la sección 7.5 se consideraron funciones de B_n a B, donde B es el álgebra booleana $\{0, 1\}$. Se observó que tales funciones pueden representar requisitos de entrada/salida para modelos de muchos circuitos computacionales prácticos. También se señaló que si la función está dada por cierta expresión booleana, entonces puede construirse un diagrama lógico para él y por lo tanto modelar la implantación de la función. En esta sección se muestra que todas las funciones de B_n en B están dadas por expresiones booleanas, por lo que es posible construir los diagramas lógicos para cualquier función de este tipo. El análisis ilustra un método para determinar una expresión booleana que produzca una función dada.

Si $f: B_n \to B$, sea $S(f) = \{b \in B_n \mid f(b) = 1\}$. Se tiene entonces el siguiente resultado.

Teorema 1. *Sean f, f_1 y f_2 tres funciones de B_n en B.*
(a) *Si $S(f) = S(f_1) \cup S(f_2)$, entonces $f(b) = f_1(b) \vee f_2(b)$ para toda b en B.*
(b) *Si $S(f) = S(f_1) \cap S(f_2)$, entonces $f(b) = f_1(b) \wedge f_2(b)$ para toda b en B.*
($\vee$ *y* $\wedge$ *son* GLB *y* LUB, *respectivamente, en B.*)

Demostración: (a) Sea $b \in B_n$. Si $b \in S(f)$, entonces, por la definición de $S(f)$, $f(b) = 1$. Como $S(f) = S(f_1) \cup S(f_2)$, entonces $b \in S(f_1)$ o $b \in S(f_2)$, o está en ambos. En cualquier caso, $f_1(b) \vee f_2(b) = 1$. Ahora, si $b \notin S(f)$, entonces $f(b) = 0$. También se debe tener $b \notin S(f_1)$y $b \notin S(f_2)$, de modo que $f_1(b) = 0$ y $f_2(b) = 0$. Esto significa que $f_1(b) \vee f_2(b) = 0$. Así, para toda $b \in B_n$, $f(b) = f_1(b) \vee f_2(b)$.
(b) Esta parte se demuestra de una manera completamente análoga a la utilizada en la parte (a). ●

Recuérdese que una función $f: B_n \to B$ se puede ver como una función $f(x_1, x_2, \ldots, x_n)$ de n variables, cada una de las cuales puede asumir los valores 0 o 1. Si $E(x_1, x_2, \ldots, x_n)$ es una expresión booleana, entonces la función que produce se genera al sustituir todas las combinaciones de ceros y unos en los términos x_i de la expresión.

Ejemplo 1. Sea $f_1 : B_2 \to B$ producida por la expresión $E(x, y) = x'$, y sea $f_2 : B_2 \to B$ producida por la expresión $E(x, y) = y'$. Entonces, las tablas de verdad de f_1 y f_2 aparecen en la figura 7.75(a) y (b), respectivamente. Sea $f: B_2 \to B$ la función cuya tabla de verdad aparece en la figura 7.75(c). Es claro que $S(f) = S(f_1) \cup S(f_2)$, pues f_1 es igual a 1 en los elementos (0, 0) y (0, 1) de B_2, f_2 es 1 en los elementos (0, 0) y (1, 0) de B_2 y f es 1 en los elementos (0, 0), (0, 1) y (1, 0) de B_2. Por el teorema 1, $f = f_1 \vee f_2$, de modo que una expresión booleana que produce f es $x' \vee y'$. Esto se verifica fácilmente. ◆

x	y	$f_1(x, y)$
0	0	1
0	1	1
1	0	0
1	1	0

(a)

x	y	$f_2(x, y)$
0	0	1
0	1	0
1	0	1
1	1	0

(b)

x	y	$f(x, y)$
0	0	1
0	1	1
1	0	1
1	1	0

(c)

Figura 7.75

No es difícil mostrar que cualquier función $f: B_n \to B$ para la cual $S(f)$ tiene precisamente un elemento es producida por una expresión booleana. La tabla 7.1 muestra la correspondencia entre las funciones de dos variables que son iguales a 1 justo en un elemento y las expresiones booleanas que producen estas funciones.

Tabla 7.1

$S(f)$	Expresión que produce f
$\{(0, 0)\}$	$x' \wedge y'$
$\{(0, 1)\}$	$x' \wedge y$
$\{(1, 0)\}$	$x \wedge y'$
$\{(1, 1)\}$	$x \wedge y$

Ejemplo 2. Sea $f: B_2 \to B$ la función cuya tabla de verdad aparece en la figura 7.76(a). Esta función sólo es igual a 1 en el elemento (0, 1) de B_2; es decir, $S(f) = \{(0, 1)\}$. Así, $f(x, y) = 1$ sólo cuando $x = 0$ y $y = 1$. Esto también es cierto para la expresión $E(x, y) = x' \wedge y$, de modo que f es producida por esta expresión.

x	y	$f(x, y)$
0	0	0
0	1	1
1	0	0
1	1	0

(a)

x	y	z	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

(b)

Figura 7.76

La función $f: B_3 \to B$ cuya tabla de verdad aparece en la figura 7.76(b) tiene $S(f) = \{(0, 1, 1)\}$; es decir, f es igual a 1 sólo cuando $x = 0$, $y = 1$ y $z = 1$. Esto también es cierto para la expresión booleana $x' \wedge y \wedge z$, que por lo tanto debe producir a f. ◆

Si $b \in B_n$, entonces b es una secuencia $(c_1, c_2, \ldots, c_n)$ de longitud n, donde cada c_k es 0 o 1. Sea E_b la expresión booleana $\bar{x}_1 \wedge \bar{x}_2 \wedge \cdots \wedge \bar{x}_n$, donde $\bar{x}_k = x_k$ cuando $c_k = 1$ y $\bar{x}_k = x_k'$ cuando $c_k = 0$. Tal expresión es un **minitérmino**. El ejemplo 2 ilustra el hecho de que cualquier función $f: B_n \to B$ para la que $S(f)$ es un único elemento de B_n es producida por un minitérmino. De hecho, si $S(f) = \{b\}$, es fácil ver que la expresión minitérmino E_b produce a f. Se tiene entonces el siguiente resultado.

Teorema 2. *Cualquier función $f: B_n \to B$ es producida por una expresión booleana.*

Demostración: Sea $S(f) = \{b_1, b_2, \ldots, b_k\}$ y para cada i, sea $f_i: B_n \to B$ la función definida por

$$f_i(b_i) = 1$$
$$f_i(b) = 0, \quad \text{si } b \neq b_i.$$

Entonces $S(f_i) = \{b_i\}$, de modo que $S(f) = S(f_1) \cup \cdots \cup S(f_n)$ y por el teorema 1,

$$f = f_1 \vee f_2 \vee \cdots \vee f_n.$$

Según el análisis anterior, cada f_i es producida por el minitérmino E_{b_i}. Así, f es producida por la expresión booleana

$$E_{b_1} \vee E_{b_2} \vee \cdots \vee E_{b_n}$$

y esto concluye la demostración. ●

Ejemplo 3. Considérese la función $f: B_3 \to B$ cuya tabla de verdad aparece en la figura 7.77. Como $S(f) = \{(0, 1, 1), (1, 1, 1)\}$, el teorema 2 muestra que f es producida por la expresión booleana $E(x, y, z) = E_{(0,1,1)} \vee E_{(1,1,1)} = (x' \wedge y \wedge z) \vee (x \wedge y \wedge z)$. Sin embargo, ésta no es la expresión booleana más sencilla que produce a f. Se utilizan las propiedades del álgebra booleana para escribir

$$\begin{aligned}(x' \wedge y \wedge z) \vee (x \wedge y \wedge z) &= (x' \vee x) \wedge (y \wedge z)\\ &= 1 \wedge (y \wedge z) = y \wedge z.\end{aligned}$$

Así, f también es producida por la expresión simple $y \wedge z$. ◆

x	y	z	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Figura 7.77

El proceso de escritura de una función como una combinación "or" de minitérminos y la simplificación de la expresión resultante se puede sistematizar de varias formas. Ahora se mostrará un procedimiento gráfico que utiliza lo que se conoce como mapa de Karnaugh. Los seres humanos pueden utilizar este procedimiento con las funciones $f: B_n \to B$, si n no es demasiado grande. Se ilustrará el método para $n = 2$, 3 y 4. Si n es grande o si se desea utilizar un algoritmo programable, son preferibles otras técnicas.

Considérese primero el caso en que $n = 2$, de modo que f es una función de dos variables, por decir, x y y. En la figura 7.78(a) se muestra una matriz 2×2 de cuadrados, donde cada cuadrado contiene una entrada posible b de B_2. En la figura 7.78(b) se ha reem-

0 0	0 1
1 0	1 1

(a)

	y'	y
x'	$x' \wedge y'$	$x' \wedge y$
x	$x \wedge y'$	$x \wedge y$

(b)

Figura 7.78

plazado cada entrada b con el minitérmino correspondiente E_b. Las etiquetas de los cuadrados en la figura 7.78 sólo sirven como referencia. En el futuro no se mostrará estas etiquetas, sino que se dará por hecho que el lector recuerda sus posiciones. En la figura 7.78(b) se observa que la variable x siempre aparece en la primera fila como x' y siempre aparece en la segunda fila como x. Se etiqueta estas filas de acuerdo con esto, y se realiza un etiquetado similar con las columnas.

Ejemplo 4. Sea $f: B_2 \to B$ la función cuya tabla de verdad aparece en la figura 7.79(a). En la figura 7.79(b) se ha ordenado los valores de f en los cuadrados adecuados, y se conservan las etiquetas de las filas y las columnas. El arreglo resultante de 2×2 de ceros y unos es el **mapa de Karnaugh** de f. Como $S(f) = \{(0, 0), (0, 1)\}$, la expresión correspondiente para f es $(x' \wedge y') \vee (x' \wedge y) = x' \wedge (y' \vee y) = x'$. ◆

x	y	$f(x, y)$
0	0	1
0	1	1
1	0	0
1	1	0

Tabla de verdad de f

(a)

	y'	y
x'	1	1
x	0	0

Mapa de Karnaugh de f

(b)

Figura 7.79

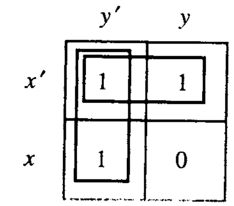
El resultado del ejemplo 4 es típico. Cuando los valores 1 de una función $f: B_2 \to B$ llenan exactamente una fila o columna, la etiqueta de esa fila o columna proporciona la expresión booleana para f. Por supuesto, ya se sabía que si los valores 1 de f llenan justo un cuadrado, entonces f es producida por el minitérmino correspondiente. Se puede mostrar que mientras más grande sea el rectángulo de valores 1 de f, menor será la expresión para f. Por último, si los valores 1 de f no están en un rectángulo, puede descomponerse estos valores en la unión de rectángulos (que pueden traslaparse). Entonces, por el teorema 1, es posible determinar la expresión booleana para f calculando las expresiones correspondientes a cada rectángulo y combinándolas con $\vee$.

Ejemplo 5. Considérese la función $f: B_2 \to B$ cuya tabla de verdad aparece en la figura 7.80(a). En la figura 7.80(b) se muestra el mapa de Karnaugh de f y se descompone los valores 1 en los dos rectángulos indicados. La expresión para la función que tiene valores 1

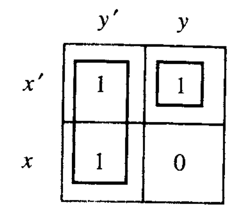
en el rectángulo horizontal es x' (verifique esto). La función que tiene todos sus valores 1 en el rectángulo vertical corresponde a la expresión y' (verifique). Así, f corresponde a la expresión $x' \vee y'$. En la figura 7.80(c) se muestra una descomposición diferente de los valores 1 de f en rectángulos. Esta descomposición también es correcta, pero conduce a la expresión más compleja $y' \vee (x' \wedge y)$. Se observa que la descomposición en rectángulos no es única y que se debería intentar utilizar los rectángulos más grandes posibles. ◆

x	y	$f(x, y)$
0	0	1
0	1	1
1	0	1
1	1	0

(a)



(b)



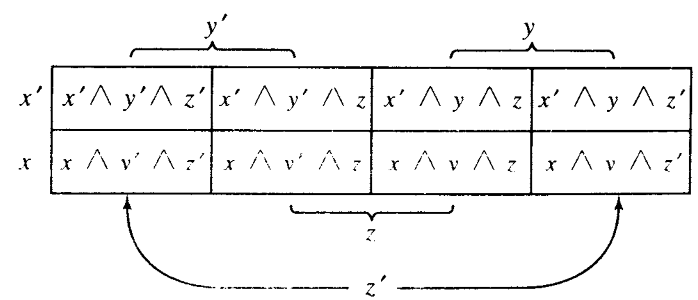
(c)

Figura 7.80

Ahora, se revisará el caso de una función $f: B_3 \to B$, que se considera como una función de x, y, z. Se podría proceder como en el caso de dos variables y construir un cubo de lado 2 que contenga los valores de f. Esto podría funcionar, pero es difícil dibujar y utilizar figuras tridimensionales, y la idea no se podría generalizar. En vez de esto, se utiliza un rectángulo de lado 2×4. En la figura 7.81(a) y (b) se muestran las entradas (de B_3) y minitérminos correspondientes a cada cuadrado de dicho rectángulo.

	0 0	0 1	1 1	1 0
0	0 0 0	0 0 1	0 1 1	0 1 0
1	1 0 0	1 0 1	1 1 1	1 1 0

(a)



(b)

Figura 7.81

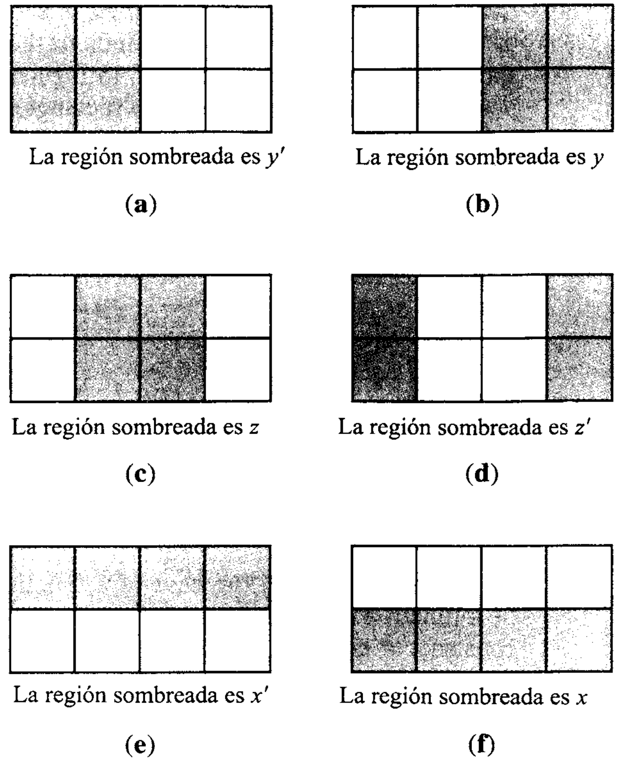


Figura 7.82

Considérense las áreas rectangulares de la figura 7.82. Si los valores 1 para una función $f: B_3 \to B$ llenan exactamente uno de los rectángulos mostrados, entonces la expresión booleana para esta función es una de las seis expresiones x, y, z, x', y', o z', como indica la figura 7.82.

Considérese la situación de la figura 7.82(a). El teorema 1(a) muestra que es posible calcular f uniendo todos los minitérminos con los cuadrados de la región, mediante el símbolo $\vee$. Así, f es producida por

$$\begin{aligned}(x' \wedge y' \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y' \wedge z') \vee (x \wedge y' \wedge z) \\ &= ((x' \vee x) \wedge (y' \wedge z')) \vee ((x' \vee x) \wedge (y' \wedge z)) \\ &= (1 \wedge (y' \wedge z')) \vee (1 \wedge (y' \wedge z)) \\ &= (y' \wedge z') \vee (y' \wedge z) \\ &= y' \wedge (z' \vee z) = y' \wedge 1 = y'.\end{aligned}$$

Un cálculo similar muestra que las otras cinco regiones tienen la etiqueta correcta.

Si se piensa que los extremos izquierdo y derecho de nuestro rectángulo básico se unen para formar un cilindro, como se muestra en la figura 7.83, puede decirse que las seis grandes regiones de la figura 7.82 constan de dos columnas adyacentes cualesquiera del cilindro, o del semicilindro superior o inferior.

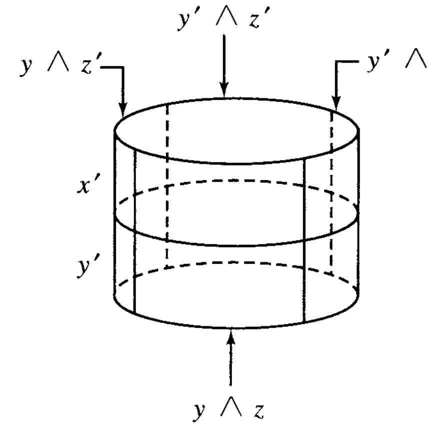


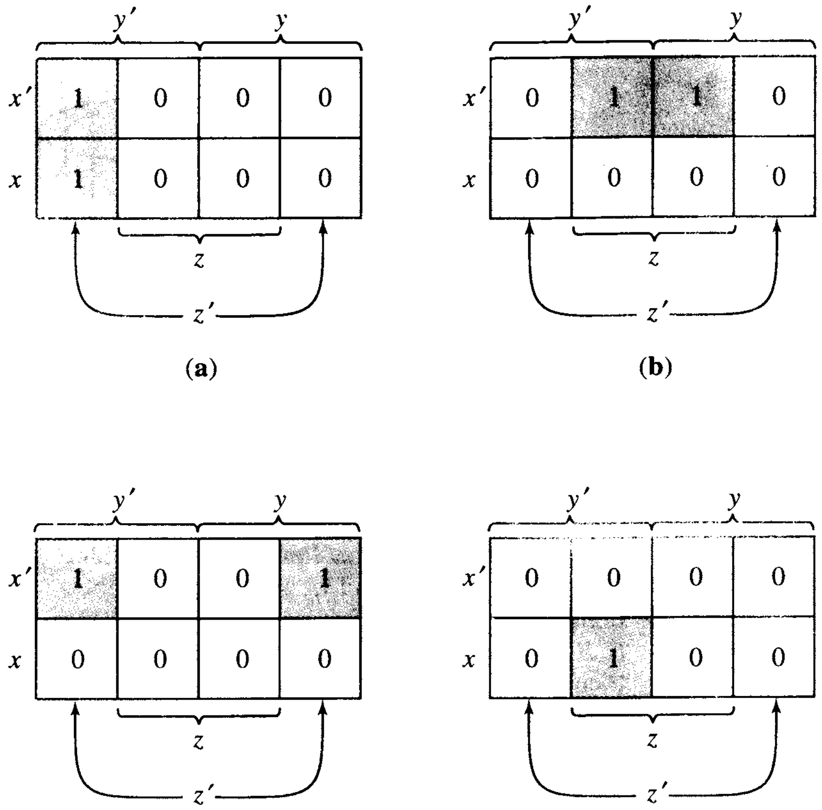
Figura 7.83

Las seis regiones básicas que aparecen en la figura 7.82 son las únicas donde hay que considerar las expresiones booleanas correspondientes. Ésta es la razón de su uso para etiquetar la figura 7.81(b) y serán conservadas como etiquetas de todos los mapas de Karnaugh de funciones de B_3 a B. El teorema 1(b) dice que, si los valores 1 de una función $f: B_2 \to B$ forman precisamente la intersección de dos o tres de las seis regiones básicas, entonces es posible calcular una expresión booleana para f combinando las expresiones para estas regiones básicas con símbolos $\wedge$.

Así, si los valores 1 de la función f son como se muestra en la figura 7.84(a), entonces son obtenidos intersecando las regiones que aparecen en la figura 7.82(a) y (d). Por lo tanto, la expresión booleana para f es $y' \wedge z'$. Es posible realizar deducciones similares para las otras tres columnas. Si los valores 1 de f son como muestra la figura 7.84(b), es posible obtenerlos intersecando las regiones de la figura 7.82(c) y (e), de modo que una expresión booleana para f es $z \wedge x'$. De manera análoga, es posible calcular la expresión para cualquier función cuyos valores 1 llenen dos cuadrados adyacentes en forma horizontal. Existen ocho de tales funciones si de nuevo se considera que el rectángulo forma un cilindro. Así, se incluye el caso en que los valores 1 de f son como en la figura 7.84(c). La expresión booleana resultante es $z' \wedge x'$.

Si se intersecan tres de las regiones básicas y la intersección no está vacía, esta intersección debe ser un único cuadrado, y la expresión booleana resultante es un minitérmino. En la figura 7.84(d), los valores 1 de f forman la intersección de las tres regiones de la figura 7.82(a), (c) y (f). El minitérmino correspondiente es $y' \wedge z \wedge x$. Así, no se tiene que recordar la posición de los minitérminos en la figura 7.81(b), sino que se puede reconstruirla.

Se ha visto la forma de calcular una expresión booleana para cualquier función $f: B_3 \to B$ cuyos valores 1 forman un rectángulo de cuadrados adyacentes (en el cilindro) de tamaño $2^n \times 2^m$, $n = 0, 1$; $m = 0, 1, 2$. En general, si el conjunto de valores 1 de f no forman tal rectángulo, se puede escribir este conjunto como la unión de tales rectángulos. Entonces, se calcula una expresión booleana para f combinando la expresión asociada a cada rectángulo con símbolos $\vee$. Esto es cierto por el teorema 1(a). El análisis anterior muestra que mientras más grandes sean los rectángulos elegidos, más sencilla será la expresión booleana resultante.



(a) (b)

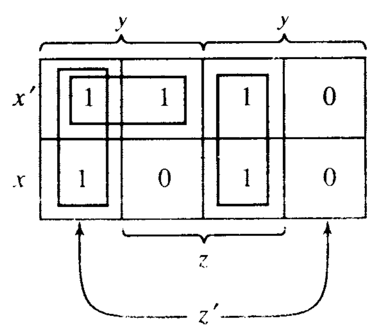
(c) (d)

Figura 7.84

Ejemplo 6. Considérese la función f cuya tabla de verdad y mapa de Karnaugh correspondientes aparecen en la figura 7.85. Puede deducirse la colocación de los unos localizando las entradas correspondientes en la figura 7.81(a). La figura 7.85(b) muestra una descomposición de los valores 1 de f. Esto permite ver que una expresión booleana para f es $(y' \wedge z') \vee (x' \wedge y') \vee (y \wedge z)$. ◆

x	y	z	$f(x, y, z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

(a)



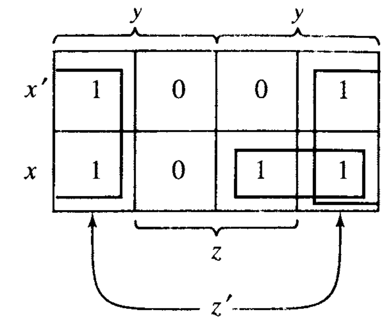
(b)

Figura 7.85

Ejemplo 7. La figura 7.86 muestra la tabla de verdad y el mapa de Karnaugh correspondientes a una función f. La descomposición en rectángulos que aparece en la figura 7.86(b) utiliza la idea de que la primera y última columnas son considerados adyacentes (enrollando el cilindro). Así, los símbolos son dejados con los extremos abiertos para indicar que se unen en un rectángulo 2×2 correspondiente a z'. La expresión booleana resultante es $z' \vee (x \wedge y)$ (verifique). ◆

x	y	z	$f(x, y, z)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

(a)



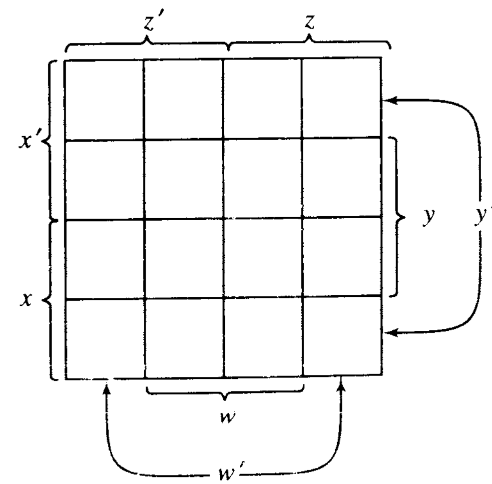
(b)

Figura 7.86

Por último, sin más comentarios, en la figura 7.87 se presenta la distribución de entradas y las etiquetas correspondientes de los rectángulos para el caso de una función $f: B_4 \to B$, considerada como función de x, y, z, y w. De nuevo, se considera la primera y última columnas como adyacentes, y la primera y última filas como adyacentes, enrollando en ambos casos; se analiza los rectángulos cuyos lados tienen una longitud dada por cierta potencia de 2, de modo que la longitud es 1, 2 o 4. Se obtiene la expresión correspondiente a tales rectángulos intersecando los grandes rectángulos etiquetados de la figura 7.88.

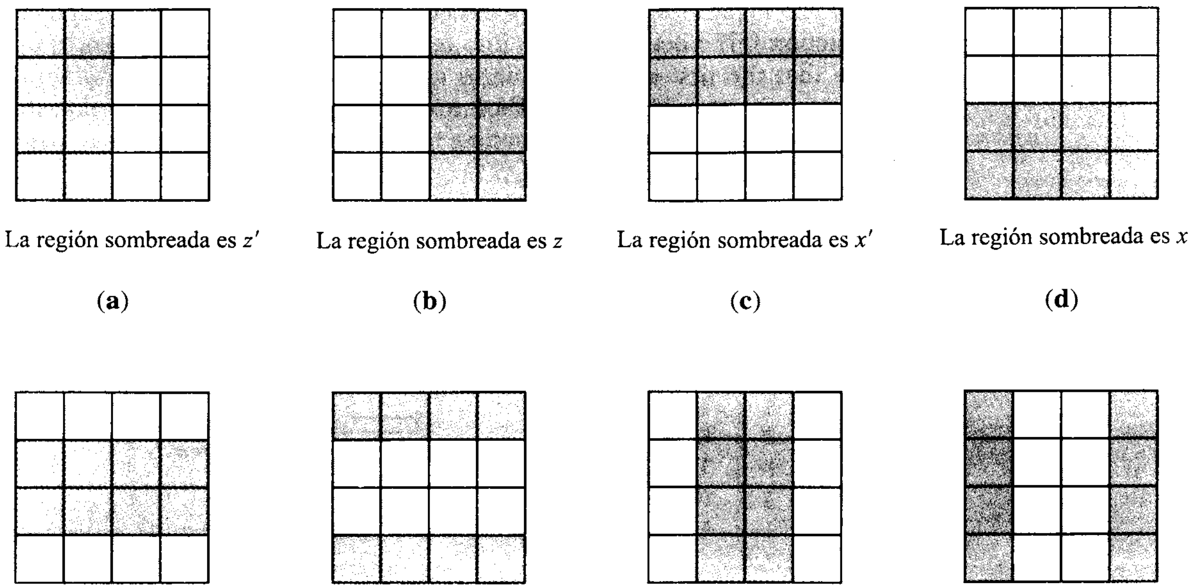
	00	01	11	10
00	0000	0001	0011	0010
01	0100	0101	0111	0110
11	1100	1101	1111	1110
10	1000	1001	1011	1010

(a)



(b)

Figura 7.87



La región sombreada es z' (a) | La región sombreada es z (b) | La región sombreada es x' (c) | La región sombreada es x (d)

La región sombreada es y (e) | La región sombreada es y' (f) | La región sombreada es w (g) | La región sombreada es w' (h)

Figura 7.88

Ejemplo 8. La figura 7.89 muestra el mapa de Karnaugh de una función $f: B_4 \to B$. Se coloca los valores 1 considerando la posición de las entradas en la figura 7.87(a). Así, $f(0101) = 1, f(0001) = 0$, etcétera.

El cuadrado central 2×2 representa la expresión booleana $w \wedge y$ (verifique).

Las cuatro esquinas forman también un cuadrado de lado 2, pues las orillas derecha e izquierda, por un lado, y superior e inferior por el otro, son consideradas adyacentes. Desde un punto de vista geométrico, se puede ver que si se enrolla el rectángulo en forma horizontal (obteniendo un cilindro) y luego, en forma vertical, se obtiene un toro o tubo interior. En este tubo interior, las cuatro esquinas forman un cuadrado de lado 2 el cual representa la expresión booleana $w' \wedge y'$ (verifique).

Esto implica que la descomposición anterior conduce a la expresión booleana

$$(w \wedge y) \vee (w' \wedge y')$$

para f. ◆

Ejemplo 9. En la figura 7.90 aparece el mapa de Karnaugh de una función $f: B_4 \to B$. La descomposición de valores 1 en rectángulos de lados 2^n, que se muestra en la figura, utiliza de nuevo la propiedad de enrollamiento de las filas superior e inferior. La expresión resultante para f es (verifique)

$$(z' \wedge y') \vee (x' \wedge y' \wedge z) \vee (x \wedge y \wedge z \wedge w).$$

El primer término proviene del cuadrado 2×2 formado al unir el rectángulo 1×2 de la esquina superior izquierda y el rectángulo 1×2 de la esquina inferior izquierda. El segundo

proviene del rectángulo de lado 1×2 en la esquina superior derecha, y el último es un minitérmino correspondiente al cuadrado aislado. ◆

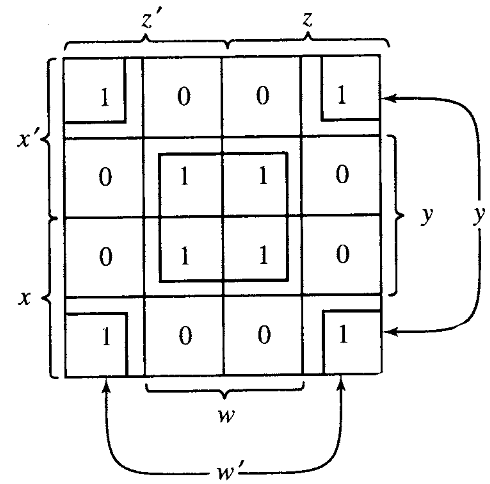


Figura 7.89

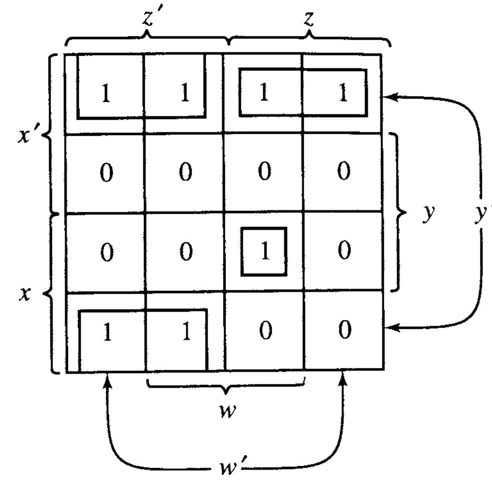


Figura 7.90

GRUPO DE EJERCICIOS 7.6

En los ejercicios 1 al 6, construya mapas de Karnaugh para las funciones con las tablas de verdad dadas.

1.

x	y	$f(x, y)$
0	0	1
0	1	0
1	0	0
1	1	1

2.

x	y	$f(x, y)$
0	0	1
0	1	0
1	0	1
1	1	0

3.

x	y	z	$f(x, y, z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

4.

x	y	z	$f(x, y, z)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

5.

x	y	z	w	$f(x, y, z, w)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	0
1	1	1	0	1
1	1	1	1	1

6.

x	y	z	w	$f(x, y, z, w)$
0	0	0	0	1
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	1
1	1	0	1	0
1	1	1	0	1
1	1	1	1	0

En los ejercicios 7 *al* 14 *(figuras* 7.91 *al* 7.98*), se proporcionan mapas de Karnaugh de funciones, así como una descomposición de valores* 1 *en rectángulos. Escriba la expresión booleana para estas funciones, que surgen de los mapas y las descomposiciones rectangulares.*

7.

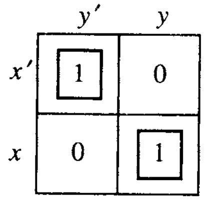


Figura 7.91

8.

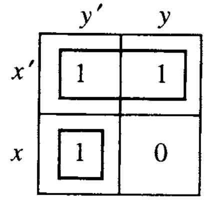


Figura 7.92

9.

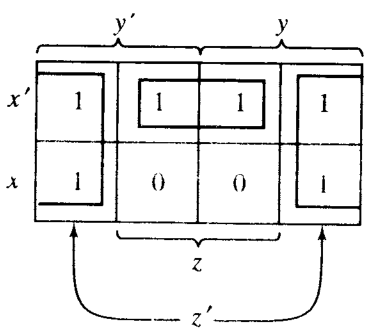


Figura 7.93

10.

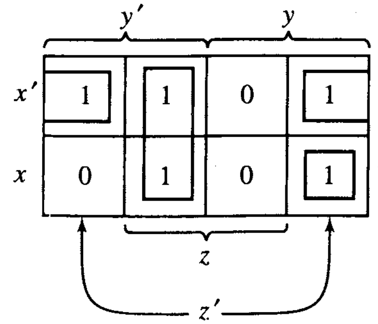


Figura 7.94

11.

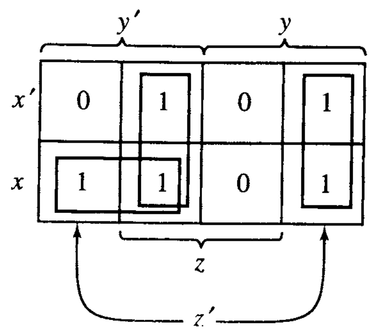


Figura 7.95

12.

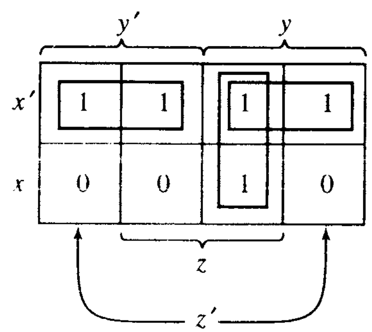


Figura 7.96

13.

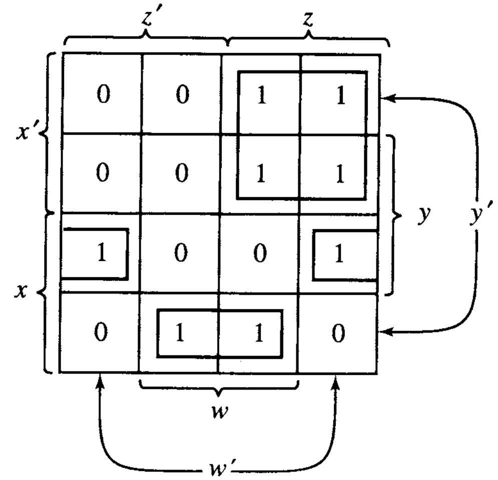


Figura 7.97

14.

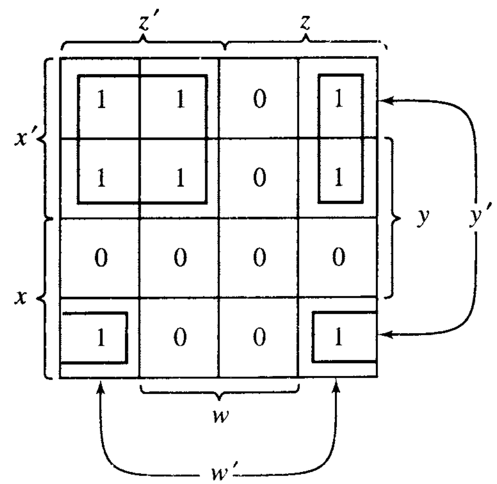


Figura 7.98

En los ejercicios 15 *al* 20*, utilice el método del mapa de Karnaugh para determinar una expresión booleana para la función f.*

15. Sea f la función del ejercicio 1.

16. Sea f la función del ejercicio 2.

17. Sea f la función del ejercicio 3.

18. Sea f la función del ejercicio 4.

19. Sea f la función del ejercicio 5.

20. Sea f la función del ejercicio 6.

IDEAS CLAVE PARA REPASO

- Orden parcial en un conjunto: relación que es reflexiva, antisimétrica y transitiva.
- Conjunto parcialmente ordenado: conjunto junto con un orden parcial.
- Conjunto linealmente ordenado: conjunto parcialmente ordenado en donde toda pareja de elementos es comparable.
- Teorema: Si A y B son conjuntos parcialmente ordenados, entonces $A \times B$ es un conjunto parcialmente ordenado con el orden parcial producto.
- Dual de un conjunto $(A, \leq)$: el conjunto parcialmente ordenado $(A, \geq)$, donde $\geq$ denota la inversa de $\leq$.
- Diagrama de Hasse: véase la página 231.

- Ordenamiento topológico: véase la página 233.
- Isomorfismo de conjuntos parcialmente ordenados: véase la página 234.
- Elemento maximal (minimal) de un conjunto parcialmente ordenado: véase la página 239.
- Teorema: Un conjunto parcialmente ordenado no vacío, finito, tiene al menos un elemento máximo y al menos un elemento mínimo.
- Elemento máximo (mínimo) de un conjunto parcialmente ordenado A: véase la página 240.
- Teorema: Un conjunto parcialmente ordenado tiene cuando mucho un elemento máximo y cuando mucho un elemento mínimo.
- Cota superior (inferior) del subconjunto B del conjunto parcialmente ordenado A: elemento $a \in A$ tal que $b \leq a$ $(a \leq b)$ para toda $b \in B$.
- Mínima cota superior (máxima cota inferior) del subconjunto B del conjunto parcialmente ordenado A: elemento $a \in A$ tal que a es una cota superior (inferior) de B y $a \leq a'$ $(a' \leq a)$, donde a' es cualquier cota superior (inferior) de B.
- Retícula: un conjunto parcialmente ordenado donde cada subconjunto con dos elementos tiene una LUB y una GLB.
- Teorema: Si L_1 y L_2 son retículas, entonces $L = L_1 \times L_2$ es una retícula.
- Teorema: Sea L una retícula y $a, b \in L$. Entonces
  (a) $a \vee b = b$ si y sólo si $a \leq b$.
  (b) $a \wedge b = a$ si y sólo si $a \leq b$.
  (c) $a \wedge b = a$ si y sólo si $a \vee b = b$.
- Teorema: Sea L una retícula. Entonces
  1. (a) $a \vee a = a$
     (b) $a \wedge a = a$
  2. (a) $a \vee b = b \vee a$
     (b) $a \wedge b = b \wedge a$
  3. (a) $a \vee (b \vee c) = (a \vee b) \vee c$
     (b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
  4. (a) $a \vee (a \wedge b) = a$
     (b) $a \wedge (a \vee b) = a$
- Teorema: Sea L una retícula y $a, b, c \in L$.
  1. Si $a \leq b$, entonces
     (a) $a \vee c \leq b \vee c$.
     (b) $a \wedge c \leq b \wedge c$.
  2. $a \leq c$ y $b \leq c$ si y sólo si $a \vee b \leq c$.
  3. $c \leq a$ y $c \leq b$ si y sólo si $c \leq a \wedge b$.
  4. Si $a \leq b$ y $c \leq d$, entonces
     (a) $a \vee c \leq b \vee d$.
     (b) $a \wedge c \leq b \wedge d$.
- Retículas isomorfas: véase la página 250.
- Retícula acotada: retícula que tiene un elemento máximo I y un elemento mínimo 0.
- Teorema: Una retícula finita es acotada.
- Retícula distributiva: retícula que satisface las leyes distributivas:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

- Complemento de a: elemento $a' \in L$ (retícula acotada) tal que

$$a \vee a' = I \quad \text{y} \quad a \wedge a' = 0$$

- Teorema: Sea L una retícula distributiva acotada. Si existe un complemento, entonces es único.
- Retícula complementada: retícula acotada en la que cada elemento tiene un complemento.
- Álgebra booleana: una retícula isomorfa con $(P(S), \subseteq)$ para algún conjunto finito S.
- Propiedades de un álgebra booleana: véase la página 263.
- Tablas de verdad: véase la página 267.
- Expresión booleana: véase la página 268.
- Minitérmino: una expresión booleana de la forma $\overline{x}_1 \wedge \overline{x}_2 \wedge \cdots \wedge \overline{x}_n$, donde cada $\overline{x}_k$ es x_k o x'_k.
- Teorema: Cualquier función $f: B_n \rightarrow B$ es producida por una expresión booleana.
- Mapa de Karnaugh: véase la página 274.

EJERCICIOS DE CODIFICACIÓN

Para lo siguiente, escriba el programa o subrutina solicitado en seudocódigo (según lo descrito en el apéndice A) o en un lenguaje de programación que usted conozca. Verifique su código con papel y lápiz o con una ejecución de computadora.

1. Escriba una subrutina que determine si una relación R representada por su matriz es un orden parcial.

Para los ejercicios 2 al 4, sea

$$B_n = \{(x_1, x_2, x_3, \ldots, x_n) \mid x_i \in \{0, 1\}\}$$

y $x, y \in B_n$.

2. Escriba una subrutina que determine si $x \leq y$.

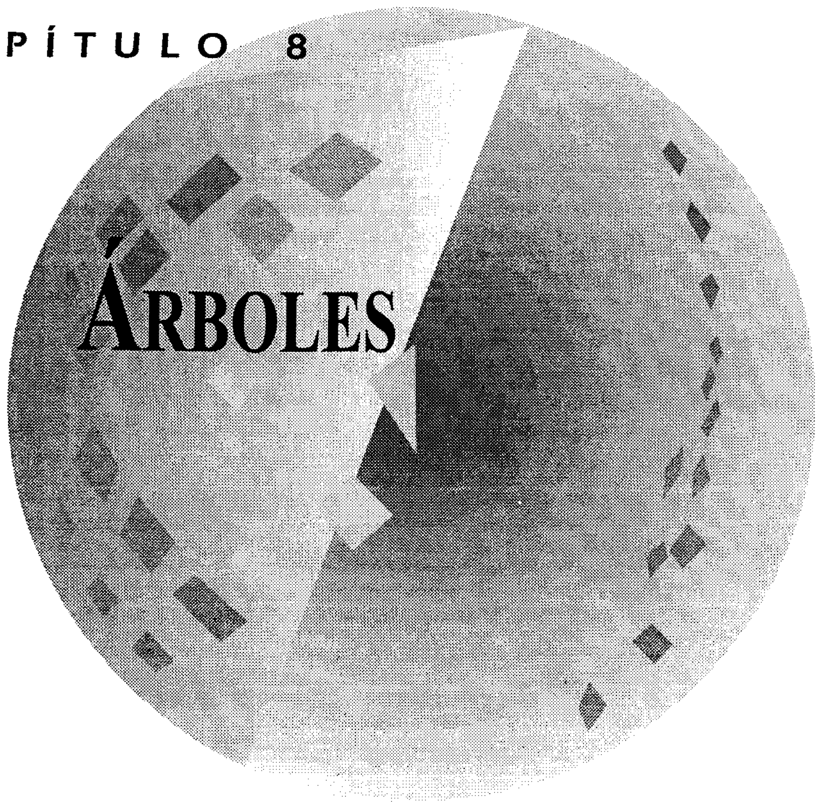
3. (a) Escriba una función que calcule $x \wedge y$.
(b) Escriba una función que calcule $x \vee y$.
(c) Escriba una función que calcule x'.

4. Escriba una subrutina tal que, dada x, produzca el minitérmino correspondiente.

5. Sea $B = \{0, 1\}$. Escriba un programa que imprima una tabla de verdad para la función $f: B_3 \rightarrow B$ definida por

$$p(x, y, z) = (x \wedge y') \vee (y \wedge (x' \vee y)).$$

CAPÍTULO 8



ÁRBOLES

Requisito previo: Capítulo 4

En este capítulo se estudiará las relaciones llamadas árboles, así como sus propiedades y aplicaciones en los algoritmos computacionales.

8.1. Árboles

En esta sección se estudiará un tipo especial de relación de excepcional utilidad, con gran variedad de aplicaciones en la ciencia de la computación y que por lo general se representa mediante su digrafo. Estas relaciones son esenciales para construir bases de datos y compiladores de lenguajes, por nombrar sólo dos áreas importantes. Son los árboles, a veces llamados árboles con raíz (o enraizados), por la apariencia de sus digrafos.

Sea A un conjunto y T una relación en A. T es un **árbol** si existe un vértice v_0 en A con la propiedad de que existe una única trayectoria en T de v_0 hacia cualquier otro vértice en A, pero no existe una trayectoria de v_0 a v_0.

Más adelante se mostrará que el vértice v_0 descrito en la definición anterior, es único.

Con frecuencia es llamado **raíz** del árbol T, y T es entonces un **árbol con raíz**. Escríbase (T, v_0) para denotar un árbol T con raíz v_0.

Si (T, v_0) es un árbol con raíz sobre el conjunto A, un elemento v de A es un **vértice en** ***T***. Esta terminología simplifica el análisis, ya que con frecuencia sucede que el conjunto subyacente A de T carece de importancia.

Con el fin de que sea más fácil entender la naturaleza de los árboles, se procederá a demostrar algunas propiedades sencillas de éstos.

Teorema 1. *Sea (T, v_0) un árbol con raíz. Entonces*

(a) *No existen ciclos en T.*

(b) *v_0 es la única raíz en T.*

(c) *Cada vértice en T distinto de v_0 tiene grado interno uno, y v_0 tiene grado interno cero.*

Demostración: (a) Supóngase que existe un ciclo q en T, que comienza y termina en el vértice v. Por la definición de árbol, se sabe que $v \neq v_0$, y debe existir una trayectoria p de v_0 a v. Entonces $q \circ p$ (véase la sección 4.3) es una trayectoria de v_0 a v diferente de p, lo cual contradice la definición de árbol.

(b) Si v_0' es otra raíz de T, existe una trayectoria p de v_0 a v_0' y una trayectoria q de v_0' a v_0 (ya que v_0' es una raíz). Entonces $q \circ p$ es un ciclo de v_0 a v_0, lo que por definición es imposible. Por lo tanto, el vértice v_0 es la única raíz.

(c) Sea w_1 un vértice en T distinto de v_0. Entonces existe una única trayectoria $v_0, \ldots, v_k, w_1$ de v_0 a w_1 en T. Esto significa que $(v_k, w_1) \in T$, de modo que w_1 tiene al menos grado interno uno. Si el grado interno de w_1 es mayor que uno, deben existir vértices w_2 y w_3 distintos tales que (w_2, w_1) y (w_3, w_1) se encuentran ambos en T. Si $w_2 \neq v_0$ y $w_3 \neq v_0$, existen trayectorias p_2 de v_0 a w_2 y p_3 de v_0 a w_3, por definición. Entonces $(w_2, w_1) \circ p_2$ y $(w_3, w_1) \circ p_3$ son dos trayectorias diferentes de v_0 a w_1, y esto contradice la definición de un árbol con raíz v_0. Por lo tanto, el grado interno de w_1 es uno. Se deja como ejercicio la conclusión de la demostración si $w_2 = v_0$ o $w_3 = v_0$ y mostrar que v_0 tiene grado interno cero. ●

El teorema 1 resume las propiedades geométricas de un árbol. Con estas propiedades en mente, es posible analizar la apariencia del digrafo de un árbol típico.

Primero se traza la raíz v_0. Ninguna arista entra a v_0, pero pueden salir varias, las cuales son trazadas hacia abajo. Los vértices terminales de las aristas que comienzan en v_0 son los vértices de **nivel 1**, mientras que v_0 está en el **nivel 0**. También se acostumbra decir que v_0 es el **padre** de estos vértices de nivel 1, y los vértices del nivel 1 son los **hijos** de v_0. La figura 8.1(a) muestra esto. Cada vértice en el nivel 1 no tiene otras aristas que entren en él, por la parte (c) del teorema 1, pero cada uno de estos vértices puede tener aristas que salgan de él. Se trazan las aristas que salen de un vértice de nivel 1 hacia abajo y terminan en diversos vértices, que están en el **nivel 2**. La figura 8.1(b) muestra la situación en este punto. En estos niveles también existe una relación padre-hijo (y en toda pareja consecutiva de niveles). Por ejemplo, v_3 es el padre de los tres hijos v_7, v_8 y v_9. Por lo general, los hijos de cada uno de los vértices son llamados **hermanos**.

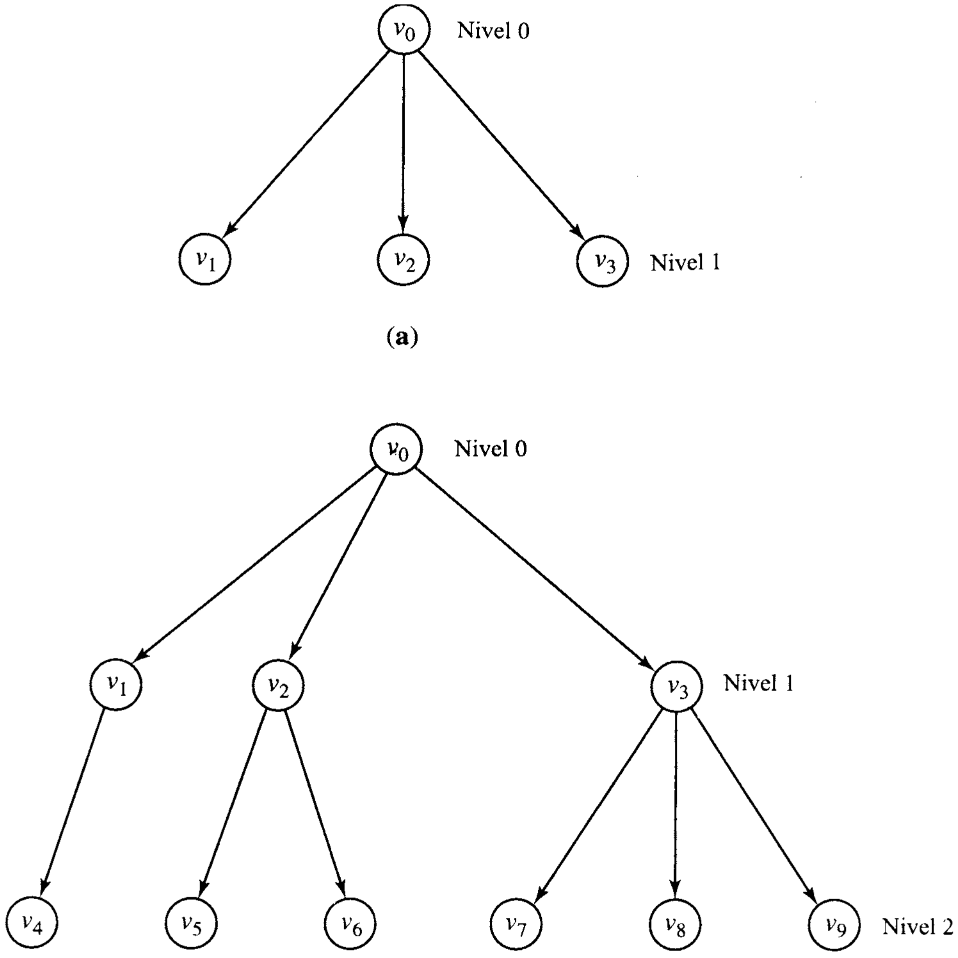


Figura 8.1

El proceso anterior continúa con tantos niveles como sean necesarios para completar el digrafo. Si se observa el digrafo de arriba hacia abajo, se entiende por qué a estas relaciones se las llama árboles. El nivel más grande de un árbol es la **altura** de éste.

Debe observarse que un árbol puede tener una infinidad de niveles y que cualquier nivel distinto del nivel 0 puede contener un número infinito de vértices. De hecho, cualquier vértice puede tener una infinidad de hijos. Sin embargo, en este análisis se supondrá que los árboles tienen un número finito de vértices. Así, los árboles siempre tendrán un nivel inferior (con el número mayor). Los vértices del árbol que no tienen hijos son las **hojas** del árbol.

Los vértices de un árbol que se encuentran en cualquier nivel forman simplemente un conjunto de vértices en A. Sin embargo, por lo general, es útil suponer que los hijos de cada vértice del árbol están linealmente ordenados. Así, si un vértice v tiene cuatro hijos, se supondrá que están ordenados, por lo que se hará referencia a ellos como el primero, segundo, tercero y cuarto hijo de v. Siempre que se trace el digrafo de un árbol, se supondrá un

orden en cada nivel, al disponer los hijos de izquierda a derecha. Un árbol de este tipo es un **árbol ordenado**. Por lo general, el orden de los hijos en un árbol no se menciona de manera explícita. Si se necesita el orden, por lo general se realiza cuando surge la necesidad, y suele especificarse mediante la forma en que se traza el digrafo del árbol. Es fácil verificar las siguientes propiedades relacionales de los árboles.

Teorema 2. *Sea (T, v_0) un árbol con raíz sobre un conjunto A. Entonces*
(a) *T es irreflexivo.*
(b) *T es asimétrico.*
(c) *Si $(a, b) \in T$ y $(b, c) \in T$, entonces $(a, c) \notin T$, para toda a, b y c en A.*

Demostración: La demostración queda como ejercicio. ●

Ejemplo 1. Sea A el conjunto de todas las mujeres hijos de una mujer v_0. Se define la siguiente relación T en A: Si v_1 y v_2 son elementos de A, entonces $v_1\ T\ v_2$ si y sólo si v_1 es la madre de v_2. La relación T en A es un árbol con raíz v_0. ◆

Ejemplo 2. Sean $A = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}\}$ y $T = \{(v_2, v_3), (v_2, v_1), (v_4, v_5), (v_4, v_6), (v_5, v_8), (v_6, v_7), (v_4, v_2), (v_7, v_9), (v_7, v_{10})\}$. Muestre que T es un árbol con raíz e identifique ésta.

Solución: Como ninguna trayectoria comienza en los vértices v_1, v_3, v_8, v_9 y v_{10}, estos vértices no pueden ser raíces de un árbol. No existen trayectorias de los vértices v_6, v_7, v_2 y v_5 al vértice v_4, por lo que se debe eliminar estos vértices como posibles raíces. Así, si T es un árbol con raíz, ésta debe ser el vértice v_4. Es fácil mostrar que existe una trayectoria de v_4 hacia cualquier otro vértice. Por ejemplo, la trayectoria v_4, v_6, v_7, v_9 va de v_4 a v_9, ya que (v_4, v_6), (v_6, v_7) y (v_7, v_9) se encuentran en T. Se traza el digrafo de T, comenzando con el vértice v_4, con las aristas hacia abajo. La figura 8.2 muestra el resultado. Una rápida inspección de este digrafo muestra que las trayecto-

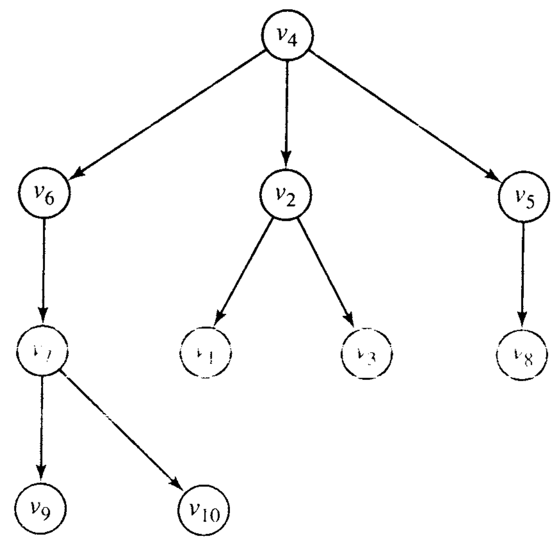


Figura 8.2

rias del vértice v_4 hacia cualquier otro vértice son únicas, y no existen trayectorias de v_4 a v_4. Así, T es un árbol con raíz v_4. ◆

Si n es un entero positivo, un árbol T es un ***n*-árbol** (árbol n-ario) si cada vértice tiene a lo más n hijos. Si todos los vértices de T distintos de las hojas tienen exactamente n hijos, T es un ***n*-árbol completo**. En particular, con frecuencia se dice que un 2-árbol es un **árbol binario**, y un 2-árbol completo es un **árbol binario completo**.

Los árboles binarios son muy importantes, ya que existen métodos eficientes para implementarlos y hacer búsquedas en ellos en las computadoras. Se verá algunos de estos métodos en la sección 8.3, y también que es posible reorganizar cualquier árbol como un árbol binario.

Sea (T, v_0) un árbol con raíz sobre el conjunto A, y sea v un vértice de T. Sea B el conjunto que consta de v y todos sus **hijos**, es decir, todos los vértices de T que pueden ser alcanzados mediante una trayectoria que comience en v. Observe que $B \subseteq A$. Sea $T(v)$ la restricción de la relación T a B; es decir, $T \cap (B \times B)$ (véase la sección 4.2). En otras palabras, $T(v)$ es el árbol obtenido de T de la siguiente manera. Se eliminan todos los vértices que no sean hijos de v y todas las aristas que no comienzan o terminan en un vértice de este tipo. Se obtiene el siguiente resultado.

Teorema 3. *Si (T, v_0) es un árbol con raíz y $v \in T$, entonces $T(v)$ también es un árbol con raíz v. $T(v)$ es el* **subárbol** *de T que comienza en v.*

Demostración: Por definición de $T(v)$, se observa que existe una trayectoria de v a cualquier otro vértice en $T(v)$. Si existe un vértice w en $T(v)$ tal que existen dos trayectorias distintas q y q' de v a w y si p es la trayectoria en T de v_0 a v, entonces $q \circ p$ y $q' \circ p$ serían dos trayectorias distintas en T de v_0 a w. Esto es imposible, ya que T es un árbol con raíz v_0. Por lo que cada trayectoria de v hacia otro vértice w en $T(v)$ debe ser único. Así, si q es un ciclo en v en $T(v)$, entonces q es también un ciclo en T. Esto contradice el teorema 1(a); por lo tanto, q no puede existir. Esto implica que $T(v)$ es un árbol con raíz v. ●

Ejemplo 3. Considere el árbol T del ejemplo 2. Este árbol tiene raíz v_4 y aparece en la figura 8.2. En la figura 8.3 se ha trazado los subárboles $T(v_5)$, $T(v_2)$ y $T(v_6)$ de T. ◆

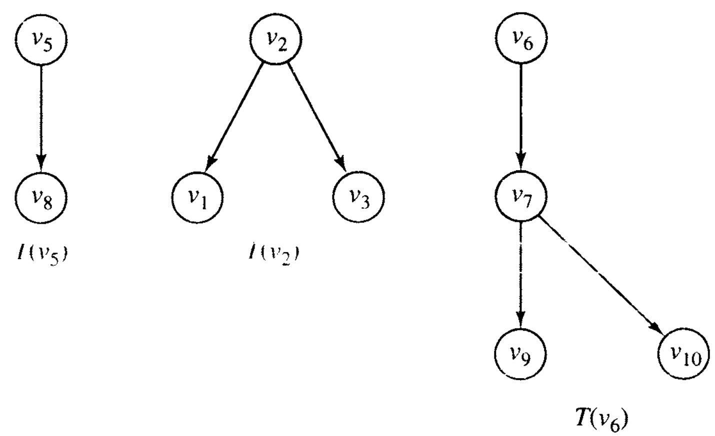


Figura 8.3

GRUPO DE EJERCICIOS 8.1

En los ejercicios 1 *al* 8, *cada relación R se define en el conjunto A. En cada caso, determine si R es un árbol y, de ser así, encuentre su raíz.*

1. $A = \{a, b, c, d, e\}$
$R = \{(a, d), (b, c), (c, a), (d, e)\}$

2. $A = \{a, b, c, d, e\}$
$R = \{(a, b), (b, e), (c, d), (d, b), (c, a)\}$

3. $A = \{a, b, c, d, e, f\}$
$R = \{(a, b), (c, e), (f, a), (f, c), (f, d)\}$

4. $A = \{1, 2, 3, 4, 5, 6\}$
$R = \{(2, 1), (3, 4), (5, 2), (6, 5), (6, 3)\}$

5. $A = \{1, 2, 3, 4, 5, 6\}$
$R = \{(1, 1), (2, 1), (2, 3), (3, 4), (4, 5), (4, 6)\}$

6. $A = \{1, 2, 3, 4, 5, 6\}$
$R = \{(1, 2), (1, 3), (4, 5), (4, 6)\}$

7. $A = \{t, u, v, w, x, y, z\}$
$R = \{(t, u), (u, w), (u, x), (u, v), (v, z), (v, y)\}$

8. $A = \{u, v, w, x, y, z\}$
$R = \{(u, x), (u, v), (w, v), (x, z), (x, y)\}$

En los ejercicios 9 *al* 13, *considere el árbol con raíz (T, v_0) de la figura* 8.4.

9. (a) Enumere todos los vértices de nivel 3.
(b) Enumere todas las hojas.

10. (a) ¿Cuáles son los hermanos de v_8?
(b) ¿Cuáles son los hijos de v_8?

11. (a) Calcule el árbol $T(v_2)$.
(b) Calcule el árbol $T(v_3)$.

12. (a) ¿Cuál es la altura de (T, v_0)?
(b) ¿Cuál es la altura de $T(v_3)$?

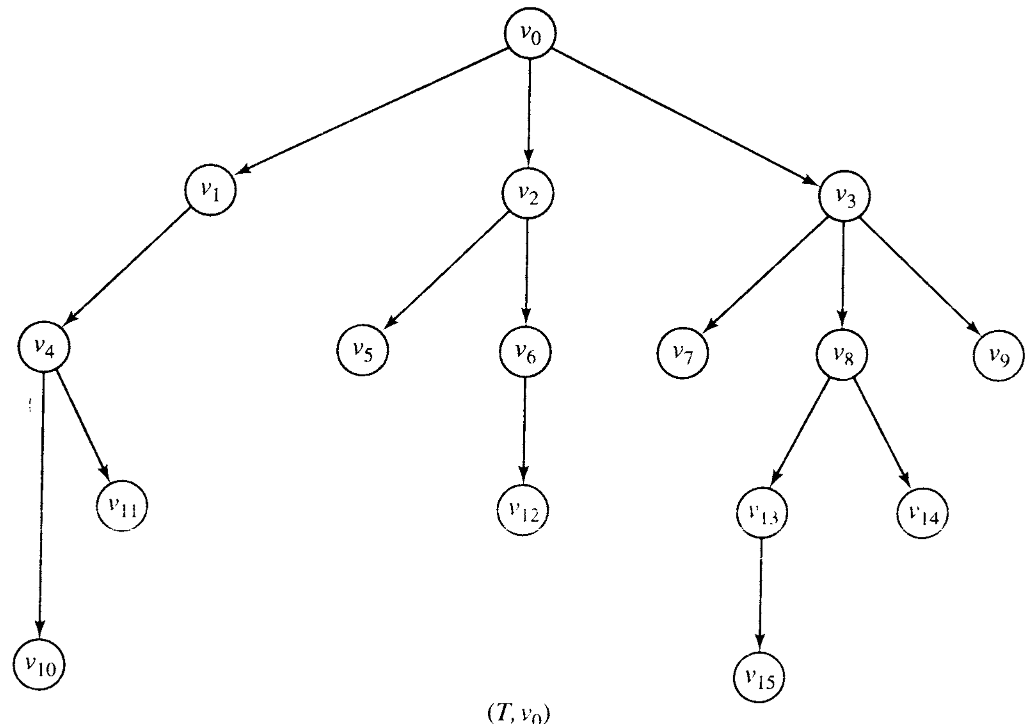


Figura 8.4

13. ¿Es (T, v_0) un n-árbol? En caso de ser así ¿para cuál entero n? ¿Es (T, v_0) un n-árbol completo? Si lo es ¿para cuál entero n?

14. Demuestre el teorema 2.

15. Sea T un árbol. Suponga que T tiene r vértices y s aristas. Determine una fórmula que relacione r con s.

16. Trace todos los árboles no ordenados posibles sobre el conjunto $S = \{a, b, c\}$.

17. (a) ¿Cuál es la altura máxima de un árbol sobre $S = \{a, b, c, d, e\}$? Explique.

(b) ¿Cuál es la altura máxima para un árbol binario completo sobre $S = \{a, b, c, d, e\}$?

18. Muestre que si (T, v_0) es un árbol con raíz, entonces v_0 tiene grado interno cero.

19. Muestre que el número máximo de vértices en un árbol binario de altura n es $2^{n+1} - 1$.

20. Si T es un n-árbol completo con exactamente tres niveles, demuestre que el número de vértices de T debe ser $1 + kn$, donde $2 \le k \le n + 1$.

8.2. Árboles etiquetados

A veces es útil etiquetar los vértices o aristas de un digrafo para indicar su uso para un propósito específico. Esto es particularmente cierto para muchos usos de los árboles en la ciencia de la computación. Ahora se proporcionará varios ejemplos donde los conjuntos de vértices de los árboles no son importantes, sino que la utilidad del árbol se enfatiza mediante las etiquetas sobre estos vértices. Así, se representará los vértices como puntos y se mostrará la etiqueta de cada vértice junto al punto que representa dicho vértice.

Ejemplo 1. Considere la expresión algebraica con cada operación entre paréntesis

$$(3 - (2 \times x)) + ((x - 2) - (3 + x)).$$

En esta expresión se supone que no es posible realizar operaciones como $-$, $+$, $\times$ o $\div$ hasta evaluar ambos argumentos; es decir, hasta realizar todos los cálculos dentro de los argumentos de la izquierda y de la derecha. Por lo tanto, no es posible realizar la suma central hasta haber evaluado $(3 - (2 \times x))$ y $((x - 2) - (3 + x))$. No es posible realizar la resta central en $((x - 2) - (3 + x))$ hasta haber evaluado $(x - 2)$ y $(3 + x)$, y así sucesivamente. Es fácil ver que cada una de estas expresiones tiene un **operador central**, que corresponde al último cálculo que puede realizarse. Así, $+$ es central para la expresión principal anterior, $-$ es central para $(3 - (2 \times x))$, y así sucesivamente. Una importante representación gráfica de una expresión de este tipo es un árbol binario etiquetado. En este árbol, se etiqueta la raíz con el operador central de la expresión principal. Se etiqueta los dos hijos de la raíz mediante el operador central de las expresiones para los argumentos de la izquierda y derecha, respectivamente. Si un argumento es constante o variable, en vez de ser una expresión, se utiliza esta constante o variable para etiquetar el vértice descendiente que corresponde. Se continúa este proceso hasta concluir con la expresión. La figura 8.5 muestra el árbol para la expresión original de este ejemplo. Para ilustrar aun más la técnica, la figura 8.6 muestra el árbol correspondiente a la expresión con cada operación entre paréntesis

$$(3 \times (1 - x)) \div ((4 + (7 - (y + 2))) \times (7 + (x \div y))). \quad \blacklozenge$$

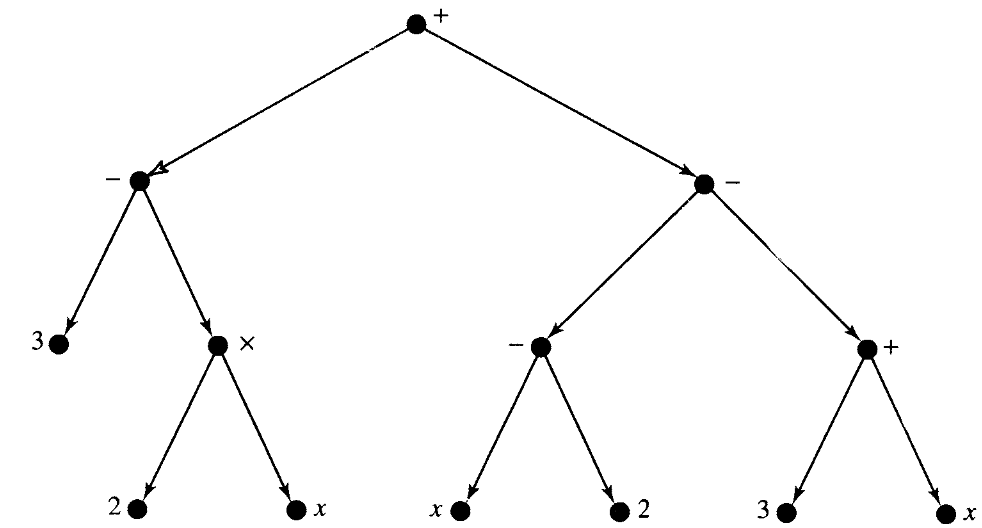


Figura 8.5

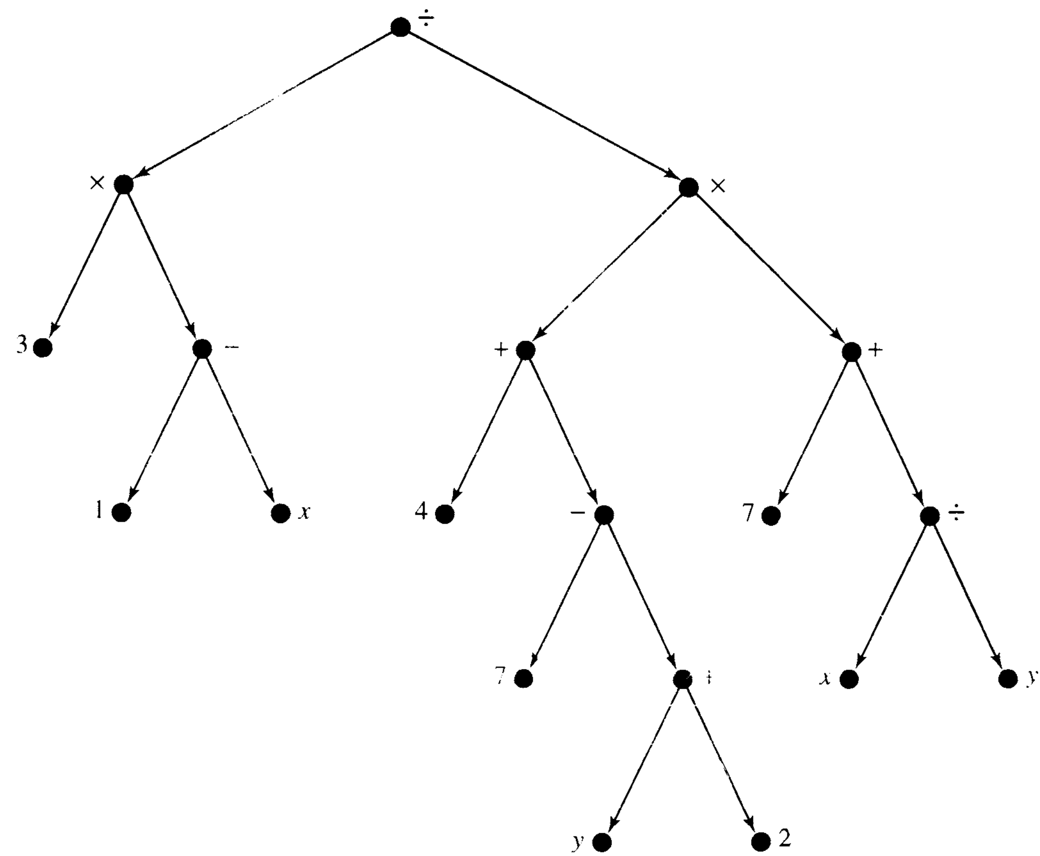


Figura 8.6

El último ejemplo de árbol etiquetado es importante para la implementación en computadora de una estructura de datos de tipo árbol. Se comienza con un n-árbol (T, v_0). Cada vértice en T tiene a lo más n hijos. Imagínese que, *potencialmente,* cada vértice tiene exactamente n hijos, ordenados de 1 a n, pero que puede faltar alguno de los hijos en la sucesión. Se etiqueta los hijos restantes de acuerdo con la posición que ocupan en la sucesión hipotética. Así, se etiqueta los hijos de cualquier vértice con distintos números del conjunto $\{1, 2, \ldots, n\}$.

Con frecuencia, se dice que un digrafo etiquetado como éste es **posicional**, y también se utilizará este término. Observe que los árboles posicionales también son árboles ordenados. Al trazar los digrafos de un árbol posicional, se supondrá que las posiciones de los n hijos para cada vértice son ordenados de forma simétrica bajo el vértice, y se coloca en la posición adecuada cada hijo realmente existente.

La figura 8.7 muestra el digrafo de un 3-árbol (árbol ternario), donde todas las posiciones reales etiquetadas. Si realmente existe la descendencia 1 de cualquier vértice v, se traza la arista de v hacia ese hijo inclinada a la izquierda. Se traza el hijo 2 de cualquier vértice v de manera vertical, hacia abajo de v, cuando exista. De manera similar, se traza los hijos etiquetados con 3 hacia la derecha. Es claro que no se etiqueta la raíz, ya que no es un hijo.

El **árbol binario posicional** es de particular importancia. En este caso, por razones obvias, se etiqueta las posiciones de los hijos potenciales como *izquierda* y *derecha*, en vez de 1 y 2. La figura 8.8 muestra el digrafo de un árbol binario posicional, donde se etiqueta los hijos como L para izquierda y R para derecha. Los árboles etiquetados pueden tener varios conjuntos de etiquetas. Por lo general, se omite las etiquetas izquierda-derecha en un árbol binario posicional para enfatizar otras etiquetas útiles.

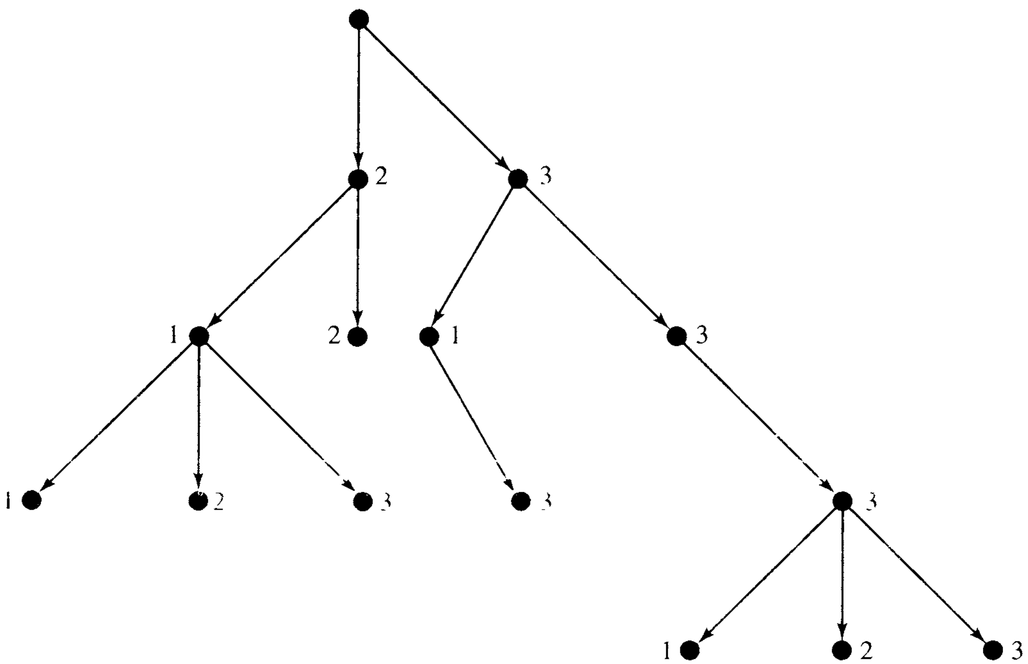


Figura 8.7

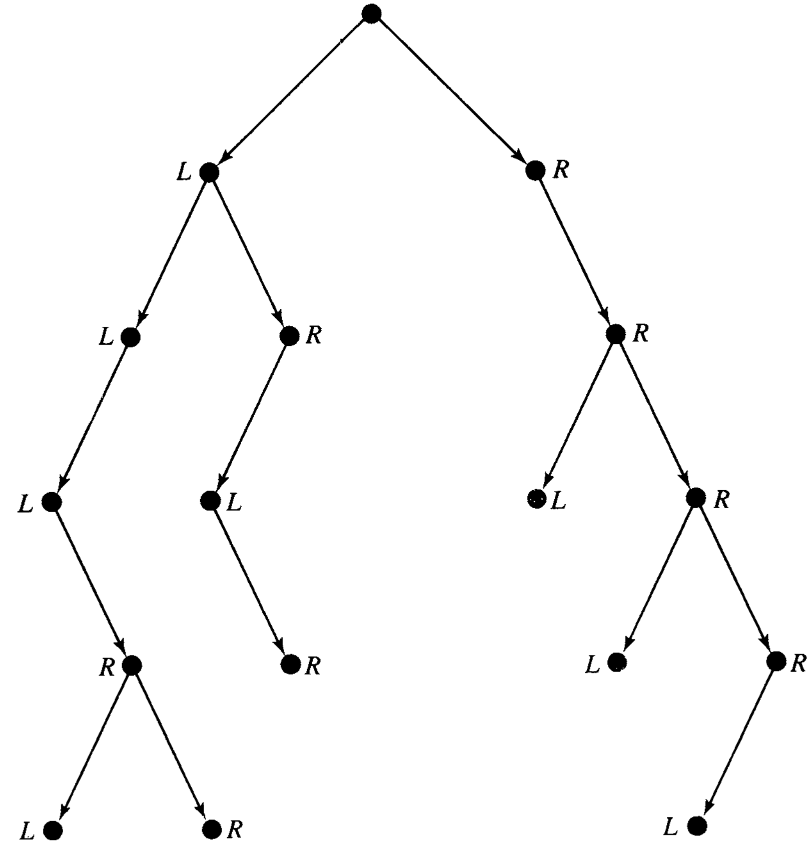


Figura 8.8

Entonces, se indica las posiciones de los hijos mediante la dirección de las aristas, como en la figura 8.8.

Representación de los árboles binarios posicionales en computadora

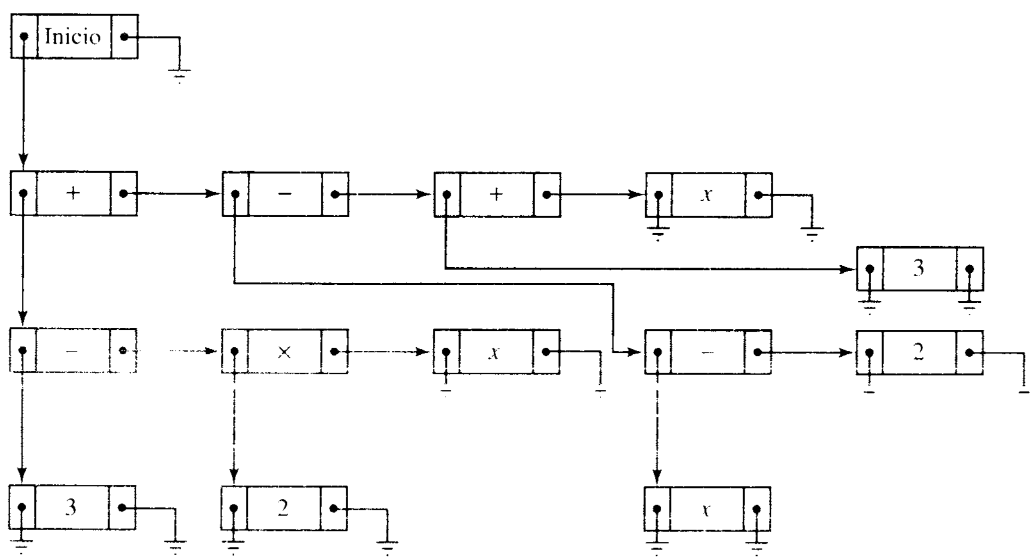
En la sección 4.6 se analizó una unidad de almacenamiento de información idealizada llamada celda. Una celda tiene dos elementos: los datos (en algún orden) y un apuntador a la siguiente celda; es decir, se indica la dirección donde se localiza la siguiente celda. Una colección de tales celdas, enlazadas mediante sus apuntadores, es una lista enlazada. El análisis en la sección 4.6 incluye ambas representaciones gráficas de listas enlazadas, y la implementación de éstas mediante arreglos.

Se necesita una versión extendida de este concepto, una **lista doblemente enlazada**, donde cada celda contenga dos apuntadores y un elemento de datos. Se utilizará el símbolo gráfico ◄● ●► para representar estas nuevas celdas. El espacio central representa el almacenamiento de datos y los dos apuntadores, llamados **apuntador izquierdo** y **apuntador derecho**, representados como antes mediante puntos y flechas. Una vez más, se utiliza el símbolo ● para un apuntador, para indicar que no existen datos adicionales. A veces, una lista doblemente enlazada se ordena de modo que cada celda apunte tanto a la celda siguiente como a la anterior. Esto es muy útil si se quiere buscar a través de un conjunto de elementos de datos en cualquier dirección. Aquí se utiliza las listas doblemente enlazadas para algo muy diferente: para representar los árboles binarios etiquetados posicionales. Cada celda corresponde a un vértice, y la parte de datos puede contener una etiqueta para el vértice o un apuntador hacia esa etiqueta. Los apuntadores izquierdo y derecho estarán dirigidos hacia los vértices hijos izquierdo y derecho, si existen. Si no existe alguno de los hijos, el apuntador correspondiente es ● .

Se implementa esta representación con tres arreglos: LEFT, que contiene los apuntadores dirigidos a los hijos de la izquierda; RIGHT, los apuntadores a los hijos de la derecha, y DATA, con la información o las etiquetas relacionadas con cada vértice, o apuntadores hacia tal información. El valor 0, utilizado como apuntador, indica que el hijo correspondiente no existe. A las listas enlazadas y a los arreglos se les agrega una entrada inicial que apunta a la raíz del árbol.

Ejemplo 2. Considérese de nuevo el árbol binario posicional de la figura 8.5. En la figura 8.9(a) se representa este árbol como una lista doblemente enlazada, en forma simbólica. En la figura 8.9(b) se muestra la implementación de esta lista mediante tres arreglos (véase también la sección 4.6). La primera fila de estos arreglos es un punto de partida, cuyo apuntador izquierdo apunta a la raíz del árbol. A manera de ejemplo de cómo interpretar los tres arreglos, considérese la quinta entrada del arreglo DATA, que es $\times$. La quinta entrada en LEFT es 6, lo que indica que el hijo izquierdo de $\times$ está en la sexta entrada en DATA, es decir, 2. De manera similar, la quinta entrada en RIGHT es 7, de modo que el hijo izquierdo de $\times$ es la séptima entrada en DATA, o x. ◆

Ejemplo 3. Ahora considérese el árbol de la figura 8.6. La figura 8.10(a) muestra este árbol como una lista doblemente enlazada. Como antes, la figura 8.10(b) muestra la implementación de esta lista enlazada en tres arreglos. De nuevo, la primera entrada es un punto de partida cuyo apuntador izquierdo apunta a la raíz del árbol. Se ha enumerado los vértices de un modo un tanto inusual para mostrar que, si los apuntadores están correctamente determinados, es posible utilizar cualquier orden en los vértices. ◆



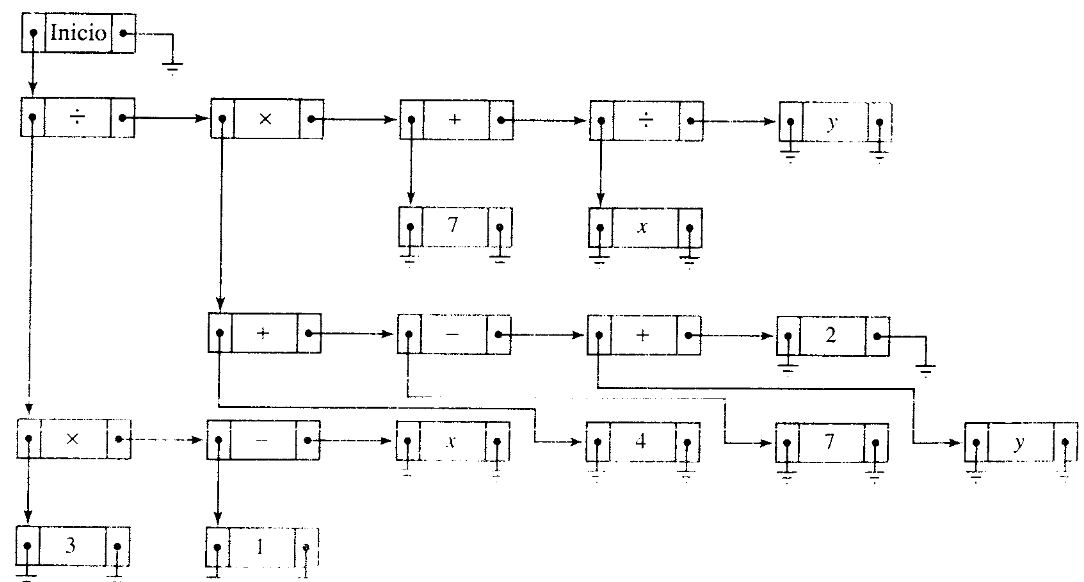
(a)

Figura 8.9

ÍNDICE	LEFT	DATA	RIGHT
1	2		0
2	3	+	8
3	4	−	5
4	0	3	0
5	6	×	7
6	0	2	0
7	0	x	0
8	9	−	12
9	10	−	11
10	0	x	0
11	0	2	0
12	13	+	14
13	0	3	0
14	0	x	0

(b)

Figura 8.9 ***(cont.)***



(a)

Figura 8.10

ÍNDICE	LEFT	DATA	RIGHT
1	7	☒	0
2	0	3	0
3	2	×	5
4	0	1	0
5	4	−	6
6	0	x	0
7	3	÷	15
8	0	4	0
9	8	+	11
10	0	7	0
11	10	−	13
12	0	y	0
13	12	+	14
14	0	2	0
15	9	×	17
16	0	7	0
17	16	+	19
18	0	x	0
19	18	÷	20
20	0	y	0

(b)

Figura 8.10 *(cont.)*

GRUPO DE EJERCICIOS 8.2

En los ejercicios 1 *al* 10, *construya el árbol de la expresión algebraica.*

1. $(7 + (6 - 2)) - (x - (y - 4))$

2. $(x + (y - (x + y))) \times ((3 \div (2 \times 7)) \times 4)$

3. $3 - (x + (6 \times (4 \div (2 - 3))))$

4. $(((2 \times 7) + x) \div y) \div (3 - 11)$

5. $((2 + x) - (2 \times x)) - (x - 2)$

6. $(11 - (11 \times (11 + 11))) + (11 + (11 \times 11))$

7. $(3 - (2 - (11 - (9 - 4)))) \div (2 + (3 + (4 + 7)))$

8. $(x \div y) \div ((x \times 3) - (z \div 4))$

9. $((2 \times x) + (3 - (4 \times x))) + (x - (3 \times 11))$

10. $((1 + 1) + (1 - 2)) \div ((2 - x) + 1)$

11. Construya los digrafos de todos los árboles binarios posicionales distintos con tres o menos lados, y altura 2.

12. ¿Cuántos árboles binarios posicionales distintos existen con altura 2?

13. ¿Cuántos 3-árboles posicionales distintos existen con altura 2?

14. Construya los digrafos de todos los 3-árboles posicionales distintos con dos o menos lados.

15. A continuación aparece la representación de un árbol binario etiquetado posicional mediante una lista doblemente enlazada. Construya el digrafo de este árbol con cada vértice etiquetado como se indica.

ÍNDICE	LEFT	DATA	RIGHT
1	8	☒	0
2	5	D	7
3	9	E	0
4	2	C	3
5	0	F	0
6	0	B	4
7	0	G	0
8	6	A	0
9	0	H	0

16. Proporcione los arreglos LEFT, DATA y RIGHT que describan al árbol de la figura 8.11 como una lista doblemente enlazada.

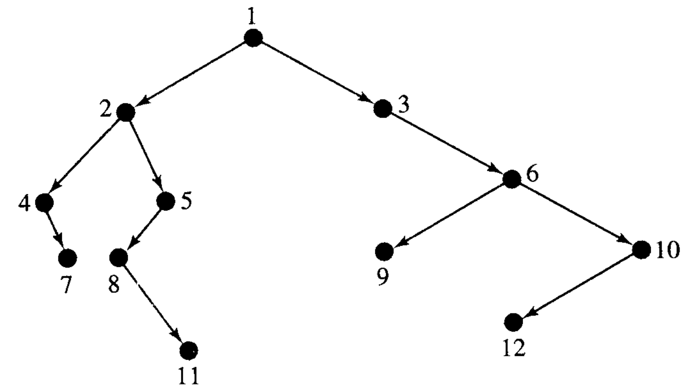


Figura 8.11

En los ejercicios 17 *al* 20, *proporcione los arreglos LEFT, DATA y RIGHT que describan al árbol creado en el ejercicio indicado.*

17. Ejercicio 1.

18. Ejercicio 4.

19. Ejercicio 5.

20. Ejercicio 8.

8.3. Búsqueda en árboles

En muchas ocasiones es útil considerar cada vértice de un árbol T exactamente una vez en cierto orden específico. Cada vez que se encuentra cada vértice, tal vez se desee realizar alguna acción o cálculo adecuado para la aplicación representada por el árbol. Por ejemplo, si el árbol T está etiquetado, se podría mostrar la etiqueta de cada vértice. Si T es el árbol de una expresión algebraica, para cada vértice se podría realizar el cálculo indicado por el operador que etiqueta a cada vértice. La realización de las tareas adecuadas en cada vértice es una **visita** del vértice. Éste es un término conveniente, no específico, que permite escribir algoritmos sin detallar lo que constituye una "visita" en cada caso particular.

El proceso de visita de cada vértice de un árbol en cierto orden específico es una **búsqueda en el árbol**. En algunos textos, se llama a este proceso **caminar** o **recorrer** el árbol.

Considérense las búsquedas en árboles binarios posicionales. Recuerde que en un árbol binario posicional, cada vértice tiene dos hijos potenciales. Se denota estos hijos potenciales como v_L (el hijo izquierdo) y v_R (el hijo derecho), donde uno o ambos pueden estar ausentes. Si un árbol binario T no es posicional, siempre puede ser etiquetado de modo que se convierta en posicional.

Sea T un árbol binario posicional con raíz v. Entonces, si existe v_L, el subárbol $T(v_L)$ (véase la sección 8.1) es el **subárbol izquierdo** de T y si existe v_R, el subárbol $T(v_R)$ es el **subárbol derecho** de T.

Observe que si $T(v_L)$ existe, entonces es un árbol binario posicional con raíz v_L, y de manera análoga, $T(v_R)$ es un árbol binario posicional con raíz v_R. Esta notación permite especificar algoritmos de búsqueda de una manera recursiva, natural y poderosa. Recuerde que los algoritmos recursivos se refieren a sí mismos. Primero, se describirá un método de búsqueda llamado **búsqueda en preorden**. Por el momento, no se especificará los detalles de la visita a un vértice de un árbol. Considere el siguiente algoritmo de búsqueda en un árbol binario posicional T con raíz v.

ALGORITMO PREORDEN
PASO 1. Visite v.
PASO 2. Si existe v_L, entonces aplique este algoritmo a $(T(v_L), v_L)$.
PASO 3. Si existe v_R, entonces aplique este algoritmo a $(T(v_R), v_R)$.
Fin del algoritmo

De manera informal, se observa que una búsqueda en preorden de un árbol consta de tres pasos:

1. Visite la raíz.
2. Busque en el subárbol izquierdo, si éste existe.
3. Busque en el subárbol derecho, si éste existe.

Ejemplo 1. Sea T el árbol binario posicional etiquetado cuyo digrafo aparece en la figura 8.12(a). La raíz de este árbol es el vértice etiquetado con A. Suponga que, para cualquier vértice v de T, la visita de v imprime la etiqueta de v. Ahora aplique el algoritmo de búsqueda en preorden a este árbol. Observe primero que si un árbol sólo tiene un vértice, su raíz, entonces una búsqueda en este árbol sólo imprime la etiqueta de la raíz. En la figura 8.12(b) se ha colocado cuadros alrededor de los subárboles de T y numerado estos subárboles (en la esquina de los cuadros) para una referencia conveniente.

Según el algoritmo PREORDEN, aplicado a T, se visita la raíz y se imprime A, después, se busca en el subárbol 1 y luego en el subárbol 7. Al aplicar PREORDEN al subárbol 1, se visita la raíz del subárbol 1 y se imprime B; después, se busca en el subárbol 2, y por último en el subárbol 4. La búsqueda en el subárbol 2 imprime primero el símbolo C y después busca en el subárbol 3. El subárbol 3 sólo tiene un vértice, por lo que, como se mencionó antes, una búsqueda en este árbol proporciona el símbolo D. Hasta este punto, la búsqueda ha producido la cadena $ABCD$. Observe que se ha interrumpido la búsqueda en cada árbol (excepto el subárbol 3, que es una hoja de T) para aplicar el procedimiento de búsqueda a un subárbol. Así, no es posible terminar la búsqueda de T con la búsqueda en el subárbol 7, sino que se debe aplicar el procedimiento de búsqueda a los subárboles 2 y 4. No es posible completar la búsqueda en el subárbol 2 hasta que se busque en el subárbol 3, y así sucesivamente. La contabilidad originada por estas interrupciones produce las etiquetas en el orden deseado, y la recursión es una forma sencilla de especificar esta contabilidad.

Regresando a la búsqueda, se ha completado la búsqueda en el subárbol 2; ahora se debe buscar en el subárbol 4, ya que éste es el subárbol derecho del árbol 1. Así, se imprime E y se busca en los subárboles 5 y 6, en ese orden. Con estas búsquedas se obtiene F y G.

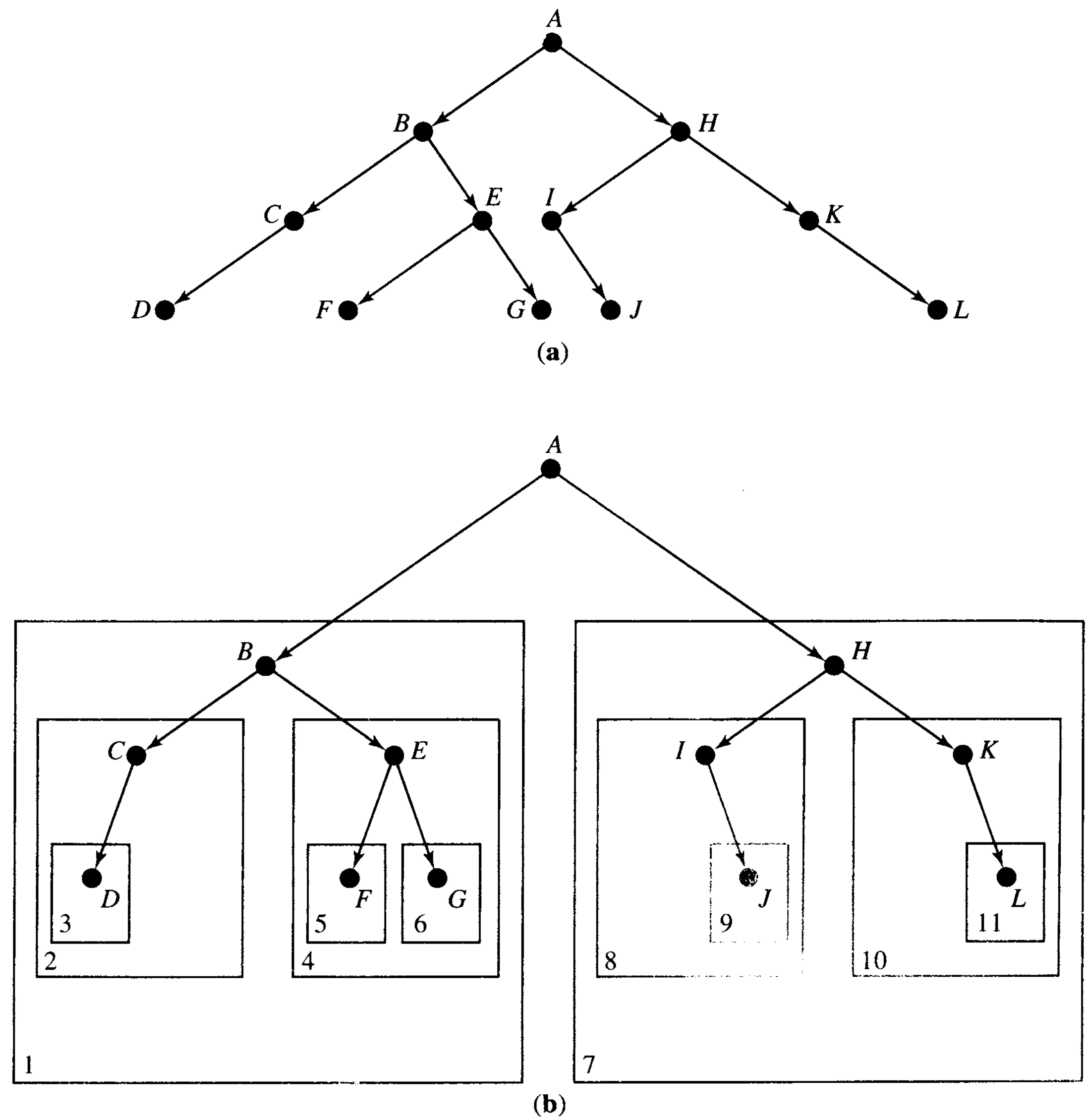


Figura 8.12

Ahora ha terminado la búsqueda en el subárbol 1, y se continúa con el subárbol 7. Al aplicar el mismo procedimiento, puede verse que la búsqueda en el subárbol 7 produce finalmente la cadena $HIJKL$. Entonces, el resultado de la búsqueda completa en T imprime la cadena $ABCDEFGHIJKL$. ◆

Ejemplo 2. Considere la expresión con cada operación entre paréntesis $(a - b) \times (c + (d \div e))$. La figura 8.13(a) muestra el digrafo del árbol binario posicional etiquetado que representa a esta expresión. Se aplica el procedimiento de búsqueda PREORDEN a este árbol, como en el ejemplo 1. La figura 8.13(b) muestra los diversos subárboles encontrados en la búsqueda. Si se procede como en el ejemplo 1 y se supone de nuevo que la visita a v sólo

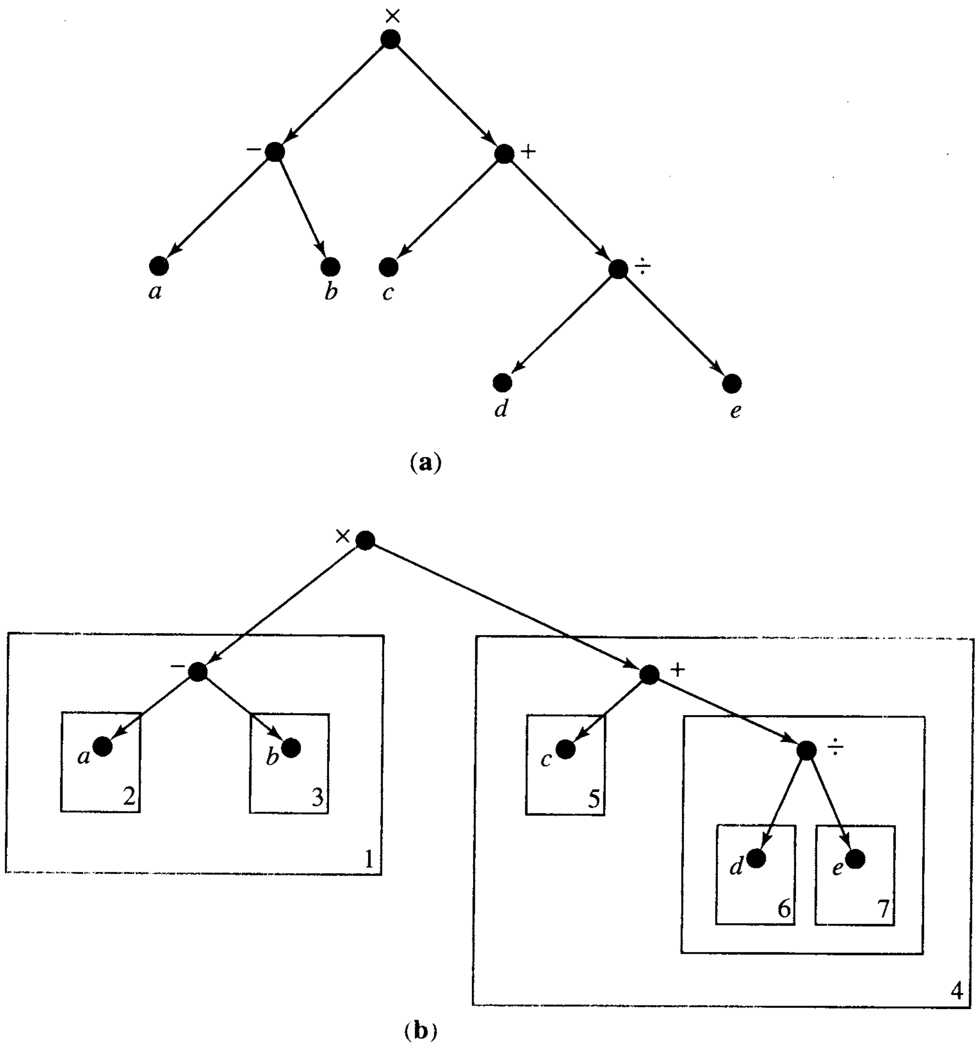


Figura 8.13

imprime la etiqueta de v, se observa que la cadena $\times - a\ b + c \div d\ e$ es el resultado de la búsqueda. Ésta es la **forma prefija** o **polaca** de la expresión algebraica dada. Una vez más, la numeración de las cajas en la figura 8.13(b) muestra el orden en que se aplica el algoritmo PREORDEN a los subárboles. ◆

La forma polaca de una expresión algebraica es interesante, ya que representa la expresión sin ambigüedades ni necesidad de paréntesis. Para evaluar una expresión en forma polaca, se procede como sigue. Muévase de izquierda a derecha hasta encontrar una cadena de la forma Fxy, donde F es el símbolo de una operación binaria (por decir, $+$, $-$, $\times$, y así sucesivamente) y x y y son números. Se evalúa xFy y se sustituye la respuesta en vez de la cadena Fxy. Se continuará con este procedimiento hasta que sólo quede un número.

Por ejemplo, en la expresión anterior, sean $a = 6$, $b = 4$, $c = 5$, $d = 2$ y $e = 2$.

Entonces se debe evaluar $\times - 64 + 5 \div 22$. Esto se lleva a cabo con la siguiente sucesión de pasos.

1. $\times - 6\,4 + 5 \div 2\,2$.	
2. $\times\ 2 + 5 \div 2\,2$,	ya que la primera cadena del tipo correcto es $-6\,4$ y $6 - 4 = 2$.
3. $\times\ 2 + 5\ 1$	reemplazando $\div\ 2\,2$ por $2 \div 2$ o 1.
4. $\times\ 2\ 6$	reemplazando $+\ 5\ 1$ por $5 + 1$ o 6.
5. 12	reemplazando $\times\ 2\ 6$ por 2×6.

Este ejemplo es una de las razones principales para que se dé el nombre de búsqueda en preorden, ya que el símbolo de operación precede al argumento.

Considérese ahora las siguientes descripciones informales de otros dos procedimientos para realizar una búsqueda en un árbol binario posicional T con raíz v.

ALGORITMO ENTREORDEN
PASO 1. Busque en el subárbol izquierdo ($T(v_L)$, v_L), si éste existe.
PASO 2. Visite la raíz v.
PASO 3. Busque en el subárbol derecho ($T(v_R)$, v_R), si éste existe.
Fin del algoritmo

ALGORITMO POSTORDEN
PASO 1. Busque en el subárbol izquierdo ($T(v_L)$, v_L), si éste existe.
PASO 2. Busque en el subárbol derecho ($T(v_R)$, v_R), si éste existe.
PASO 3. Visite la raíz v.
Fin del algoritmo

Como indica el nombre de los algoritmos, éstas son las búsquedas **entreorden** y **postorden**, respectivamente. Los nombres indican el momento en que se visita la raíz del (sub)árbol con respecto del momento en que se visita los subárboles izquierdo y derecho. De manera informal, en una búsqueda en preorden, el orden es raíz, izquierdo, derecho; para una búsqueda en entreorden, es izquierdo, raíz, derecho; y para una búsqueda en postorden, es izquierdo, derecho y raíz.

Ejemplo 3. Considere el árbol de la figura 8.12(b) y aplique el algoritmo ENTREORDEN para realizar la búsqueda. Primero, debe buscarse en el subárbol 1. Para esto, hay que buscar primero en el subárbol 2, y esto a su vez requiere que se busque en el subárbol 3. Como antes, una búsqueda en un árbol con un único vértice imprime la etiqueta de éste. Así, D es el primer símbolo impreso. La búsqueda en el subárbol 2 imprime C y después se detiene, pues no existe el subárbol derecho de C. A continuación se visita la raíz del subárbol 1 y se imprime B, por lo que se procede a buscar en el subárbol 4, con lo que se obtiene F, E y G, en ese orden. Después, se visita la raíz de T, se imprime A y se procede a la búsqueda en el subárbol 7. El lector debe completar el análisis de la búsqueda en el subárbol 7 para mostrar que el subárbol produce la cadena $IJHKL$. Así, la búsqueda completa produce la cadena $DCBFEGAIJHKL$.

Suponga ahora que se aplica el algoritmo POSTORDEN, para buscar en el mismo árbol. De nuevo, la búsqueda en un árbol con un vértice produce la etiqueta de ese vértice. En general, se debe buscar en el subárbol izquierdo y el derecho de un árbol con raíz v antes de imprimir la etiqueta de v.

Si se observa de nuevo la figura 8.12(b), se ve que hay que buscar en los subárboles 1 y 7 antes de imprimir A. Se debe buscar en los subárboles 2 y 4 antes de imprimir B, y así sucesivamente.

La búsqueda en el subárbol 2 requiere que se busque en el subárbol 3, y D es el primer símbolo impreso. La búsqueda en el subárbol 2 continúa, imprimiendo C. Ahora se busca en el subárbol 4 y se obtiene F, G y E. Después, se visita la raíz del subárbol 1 y se imprime B. Luego se busca en el subárbol 7 y se imprime los símbolos J, I, L, K y H. Por último, se visita la raíz de T e se imprime A. Así, se imprime la cadena $DCFGEBJILKHA$. ♦

Ejemplo 4. Ahora se aplicarán las búsquedas en entreorden y en postorden al árbol de la expresión algebraica del ejemplo 2 [véase la figura 8.13(a)]. El uso del algoritmo ENTREORDEN produce la cadena $a - b \times c + d \div e$. Observe que ésta es precisamente la expresión con la que se inicia el ejemplo 2, sin los paréntesis. Como los símbolos algebraicos se encuentran entre sus argumentos, ésta es llamada con frecuencia **notación entrefija**, lo cual explica el nombre de ENTREORDEN. La expresión anterior es ambigua sin paréntesis. Podría provenir de la expresión $a - (b \times ((c + d) \div e))$, con lo que se obtendría un árbol diferente. Así, no es posible recuperar el árbol a partir de la salida del procedimiento de búsqueda ENTREORDEN, pero se puede mostrar que el árbol es recuperable a partir de la forma polaca obtenida mediante PREORDEN. Por esto, se prefiere usar la notación polaca en general para las aplicaciones de las computadoras, aunque la forma entrefija resulta ser más familiar.

El uso del procedimiento de búsqueda POSTORDEN en este árbol produce la cadena $ab - cde \div + \times$. Ésta es la forma **posfija**, **polaca inversa** o **sufija** de la expresión. Se evalúa de manera similar a la forma polaca, pero el símbolo del operador está *después* de sus argumentos y no *antes*. Si $a = 2, b = 1, c = 3, d = 4$ y $e = 2$, se evalúa la expresión anterior con los siguientes pasos.

1. $2\ 1 - 3\ 4\ 2 \div + \times$.
2. $1\ 3\ 4\ 2 \div + \times$ reemplazando $2\ 1 -$ por $2 - 1$ o 1.
3. $1\ 3\ 2 + \times$ reemplazando $4\ 2 \div$ por $4 \div 2$ o 2.
4. $1\ 5 \times$ reemplazando $3\ 2 +$ por $3 + 2$ o 5.
5. 5 reemplazando $1\ 5 \times$ por 1×5 o 5. ♦

La forma polaca inversa también carece de paréntesis, y por medio de ella puede recuperarse el árbol de la expresión. Se utiliza con más frecuencia que la forma polaca.

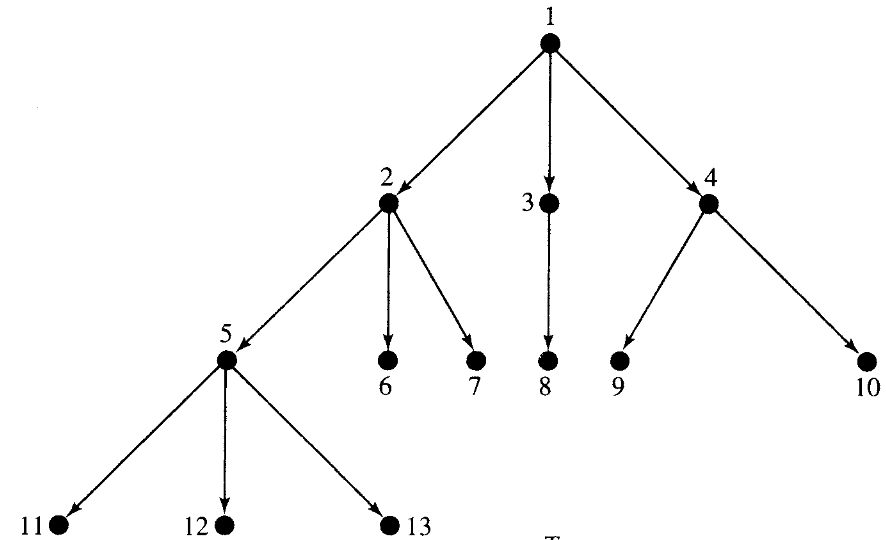
Búsqueda en árboles generales

Hasta ahora, sólo se ha mostrado la forma de realizar búsquedas en árboles posicionales binarios. Ahora se mostrará que cualquier árbol ordenado T (véase la sección 8.1) se puede representar como un árbol posicional binario, el cual, aunque diferente de T, captura toda la estructura de éste y se puede utilizar para recuperar T. Con la descripción posicional binaria del árbol, puede aplicarse la representación computacional y los métodos de búsqueda desarrollados con anterioridad. Debido a que es posible ordenar cualquier árbol, puede utilizarse esta técnica en cualquier árbol (finito).

Sean T un árbol ordenado y A el conjunto de todos los vértices de T. Se define un árbol posicional binario $B(T)$ sobre el conjunto de vértices A, como sigue. Si $v \in A$, entonces, el hijo izquierdo v_L de v en $B(T)$ es el primer hijo de v en T, si éste existe. El hijo derecho v_R de v en $B(T)$ es el siguiente hermano de v en T (en el orden dado de los hermanos de T), si es que éste existe.

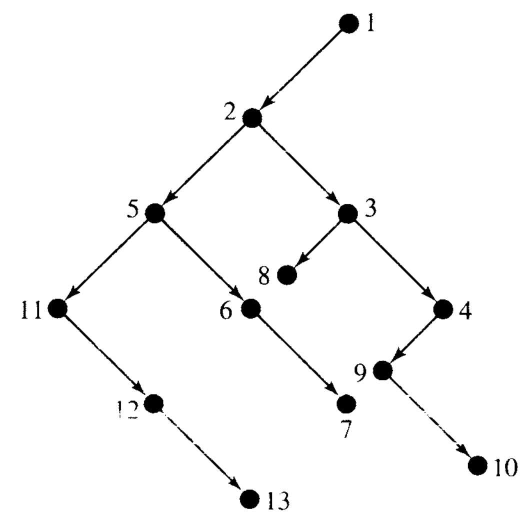
Ejemplo 5. La figura 8.14(a) muestra el digrafo de un árbol etiquetado T. Se supone que cada conjunto de hermanos está ordenado de izquierda a derecha, como en el dibujo. Así, los hijos del vértice 1, es decir, los vértices 2, 3 y 4, quedan ordenados con el vértice 2 en primer lugar, el 3, en segundo y el 4, en tercero. De manera similar, el primer hijo del vértice 5 es el vértice 11, el segundo es el vértice 12 y el tercero es el vértice 13.

En la figura 8.14(b) aparece el digrafo del árbol posicional binario correspondiente, $B(T)$. Para obtener la figura 8.14(b), basta trazar una arista izquierda desde cada uno de los



T

(a)



$B(T)$

(b)

Figura 8.14

vértices v hacia su primer hijo (si v tiene hijos). Después se traza una arista derecha de cada uno de los vértices v hacia su siguiente hermano (en el orden dado), si v tiene un siguiente hermano. Así, la arista izquierda del vértice 2, en la figura 8.14(b), va al vértice 5, ya que el vértice 5 es el primer hijo del vértice 2 en el árbol T. Además, la arista derecha del vértice 2, en la figura 8.14(b), va hacia el vértice 3, ya que el vértice 3 es el siguiente hermano en el renglón (entre todos los hijos del vértice 1). Con frecuencia, la representación de $B(T)$ a manera de lista doblemente enlazada se llama **representación en lista enlazada de T.** ◆

Ejemplo 6. La figura 8.15(a) muestra el digrafo de otro árbol etiquetado, con los hermanos ordenados de izquierda a derecha, como se indica. La figura 8.15(b) muestra el digrafo del árbol correspondiente $B(T)$, y la figura 8.15(c) proporciona una representación en forma de arreglo de $B(T)$. Como se ha mencionado, los datos en la figura 8.15(c) son una representación en lista enlazada de T. ◆

Versiones en seudocódigo

Los tres algoritmos de búsqueda de esta sección tienen versiones directas en seudocódigo, las cuales son presentadas aquí. En cada caso, se supone que se ha definido con anterioridad la subrutina VISIT.

SUBROUTINE PREORDER(T, v)
1. **CALL** VISIT(v)
2. **IF** (v_L exists) **THEN**
   a. **CALL** PREORDER($T(v_L)$, v_L)
3. **IF** (v_R exists) **THEN**
   a. **CALL** PREORDER($T(v_R)$, v_R)
4. **RETURN**

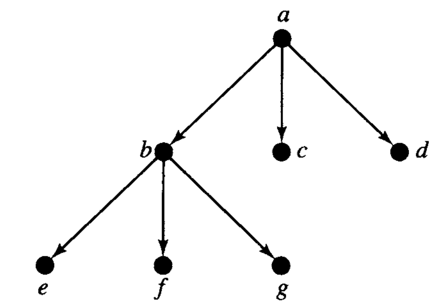
FIN DE LA SUBRUTINA PREORDEN

SUBROUTINE INORDER(T, v)
1. **IF** (v_L exists) **THEN**
   a. **CALL** INORDER($T(v_L)$, v_L)
2. **CALL** VISIT(v)
3. **IF** (v_R exists) **THEN**
   a. **CALL** INORDER($T(v_R)$, v_R)
4. **RETURN**

FIN DE LA SUBRUTINA ENTREORDEN

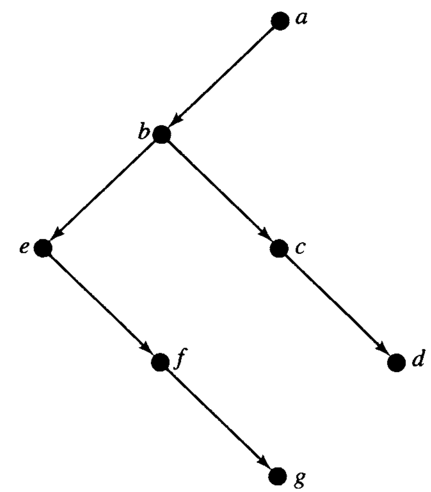
SUBROUTINE POSTORDER(T, v)
1. **IF** (v_L exists) **THEN**
   a. **CALL** POSTORDER($T(v_L)$, v_L)
2. **IF** (v_R exists) **THEN**
   a. **CALL** POSTORDER($T(v_R)$, v_R)
3. **CALL** VISIT(v)
4. **RETURN**

FIN DE LA SUBRUTINA POSTORDEN



T

(a)



$B(T)$

(b)

ÍNDICE	LEFT	DATA	RIGHT
1	2	☒	0
2	3	*a*	0
3	6	*b*	4
4	0	*c*	5
5	0	*d*	0
6	0	*e*	7
7	0	*f*	8
8	0	*g*	0

(c)

Figura 8.15

GRUPO DE EJERCICIOS 8.3

En los ejercicios 1 *al* 4 *(figuras* 8.16 *a la* 8.19*) aparecen los digrafos de árboles posicionales binarios etiquetados. En cada caso, la visita a un nodo imprime la etiqueta de ese nodo. Para cada ejercicio, muestre cuál es el resultado de realizar una búsqueda en preorden del árbol cuyo digrafo se muestra.*

1.

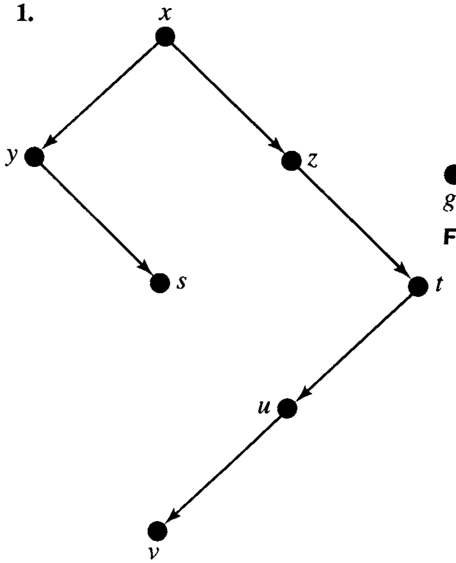


Figura 8.16

2.

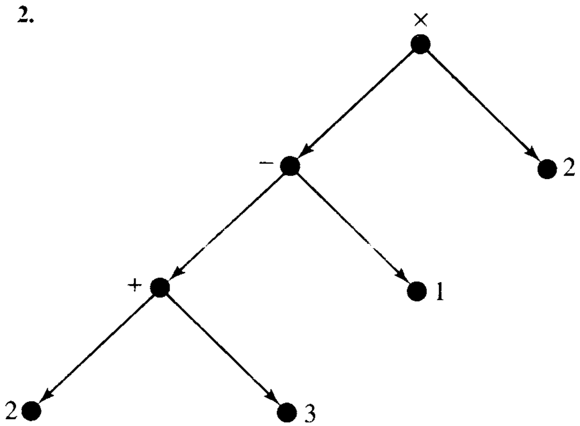


Figura 8.17

3.

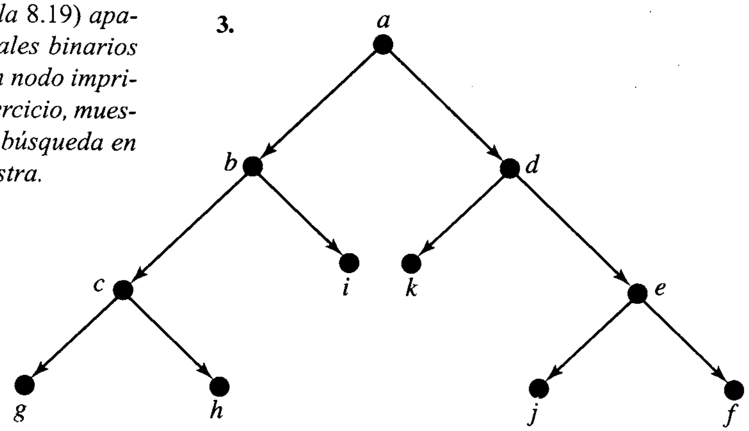


Figura 8.18

4.

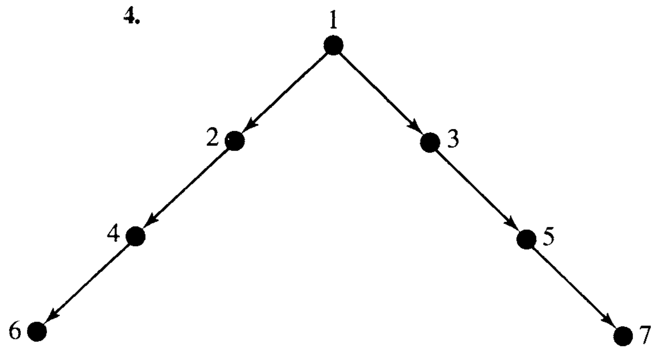


Figura 8.19

En los ejercicios 5 *al* 12*, la visita a un nodo significa imprimir la etiqueta del nodo.*

5. Muestre cuál es el resultado de realizar una búsqueda en entreorden del árbol de la figura 8.16.

6. Muestre cuál es el resultado de realizar una búsqueda en entreorden del árbol de la figura 8.17.

7. Muestre cuál es el resultado de realizar una búsqueda en entreorden del árbol de la figura 8.18.

8. Muestre cuál es el resultado de realizar una búsqueda en entreorden del árbol de la figura 8.19.

9. Muestre cuál es el resultado de realizar una búsqueda en postorden del árbol de la figura 8.16.

10. Muestre cuál es el resultado de realizar una búsqueda en postorden del árbol de la figura 8.17.

11. Muestre cuál es el resultado de realizar una búsqueda en postorden del árbol de la figura 8.18.

12. Muestre cuál es el resultado de realizar una búsqueda en postorden del árbol de la figura 8.19.

13. Considere el digrafo del árbol de la figura 8.20 y la siguiente lista de palabras. Suponga que la visita a un nodo de este árbol significa imprimir la palabra correspondiente al número que etiqueta ese nodo. Imprima la frase que se obtiene al realizar una búsqueda en postorden del árbol.

1. UNA	7. YO
2. PÚRPURA	8. UNA
3. VEA	9. ESPERO
4. NUNCA	10. YO
5. VACA	11. VI
6. NUNCA	12. QUE

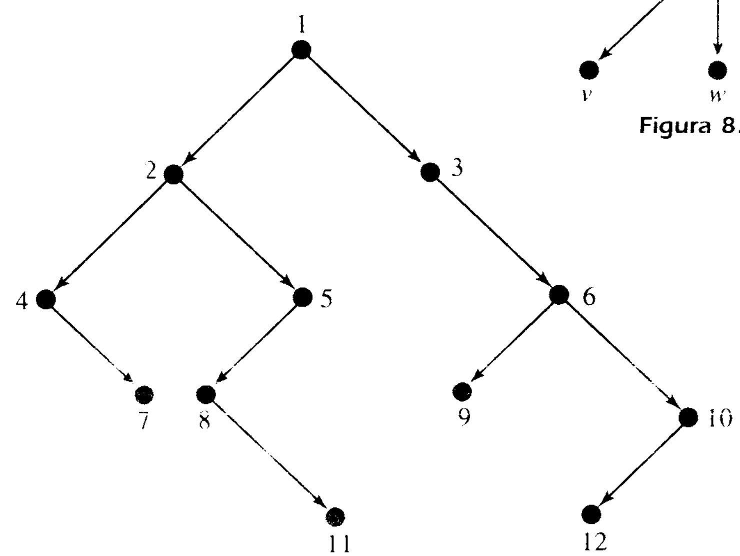


Figura 8.20

En los ejercicios 14 *y* 15*, evalúe la expresión, dada en notación polaca o prefija.*

14. $\times - + 3\ 4 - 7\ 2 \div 12 \times 3 - 6\ 4$

15. $\div - \times 3\ x \times 4\ y + 15 \times 2 - 6\ y$, donde x es 2 y y es 3.

En los ejercicios 16 *y* 17*, evalúe la expresión, dada en notación polaca inversa o posfija.*

16. $4\ 3\ 2 \div - 5 \times 4\ 2 \times 5 \times 3 \div \div$

17. $x\ 2 - 3 + 2\ 3\ y + - w\ 3 - \times \div$, donde x es 7, y es 2 y w es 1.

18. Considere el árbol etiquetado cuyo digrafo aparece en la figura 8.21. Trace el digrafo del árbol posicional binario correspondiente $B(T)$. Etiquete los vértices de $B(T)$ para mostrar su correspondencia con los vértices de T.

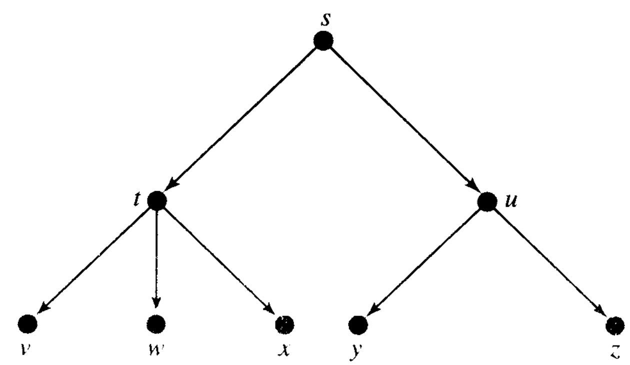


Figura 8.21

19. A continuación aparece, en forma de arreglo, la representación en lista doblemente enlazada de un árbol etiquetado T (no binario). Trace el digrafo del árbol binario etiquetado $B(T)$ guardado en los arreglos, y del árbol etiquetado T dado por la representación binaria $B(T)$.

ÍNDICE	LEFT	DATA	RIGHT
1	2		0
2	3	a	0
3	4	b	5
4	6	c	7
5	8	d	0
6	0	e	10
7	0	f	0
8	0	g	11
9	0	h	0
10	0	i	9
11	0	j	12
12	0	k	0

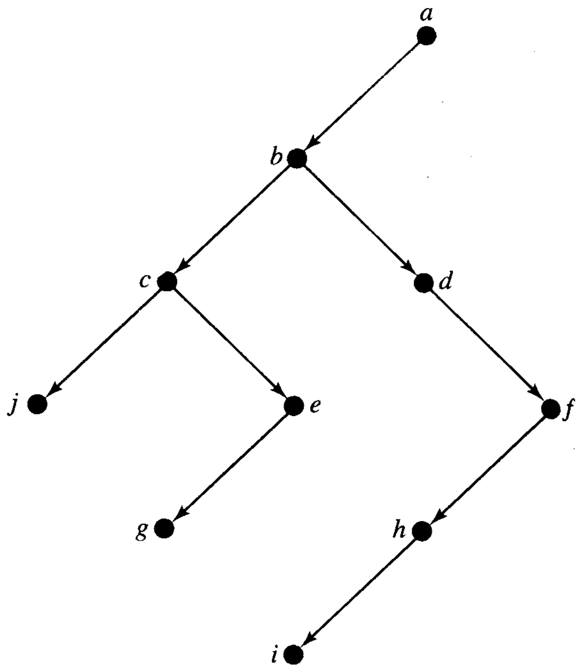


Figura 8.22

20. Considere el digrafo del árbol binario posicional etiquetado de la figura 8.22. Si este árbol es la forma binaria $B(T)$ de algún árbol T, trace el digrafo del árbol etiquetado T.

8.4. Árboles no dirigidos

Un **árbol no dirigido** es la cerradura simétrica de un árbol (véase la sección 4.7); es decir, es un árbol con todas sus aristas bidireccionales. Como se acostumbra con las relaciones simétricas, se representa un árbol no dirigido mediante su gráfica, en vez de su digrafo. La gráfica de un árbol no dirigido T tendrá una única línea sin flechas que une los vértices a y b siempre que (a, b) y (b, a) pertenezcan a T. El conjunto $\{a, b\}$, donde (a, b) y (b, a) están en T, es una **arista no dirigida** de T (véase la sección 4.4). En este caso, los vértices a y b son **vértices adyacentes**. Así, cada arista no dirigida $\{a, b\}$ corresponde a dos aristas ordinarias (a, b) y (b, a). Las líneas en la gráfica de un árbol no dirigido T corresponden a las aristas no dirigidas en T.

Ejemplo 1. La figura 8.23(a) muestra la gráfica de un árbol no dirigido T. En la figura 8.23(b) y (c), se muestra los digrafos de los árboles ordinarios T_1 y T_2, respectivamente, que tienen a T como cerradura simétrica. Esto muestra que un árbol no dirigido corresponde, en general, a muchos árboles dirigidos. Se incluye las etiquetas para mostrar la correspondencia de los vértices subyacentes en las tres relaciones. Observe que la gráfica de T en la figura 8.23(a) tiene seis líneas (aristas no dirigidas), aunque la relación T contiene 12 parejas. ◆

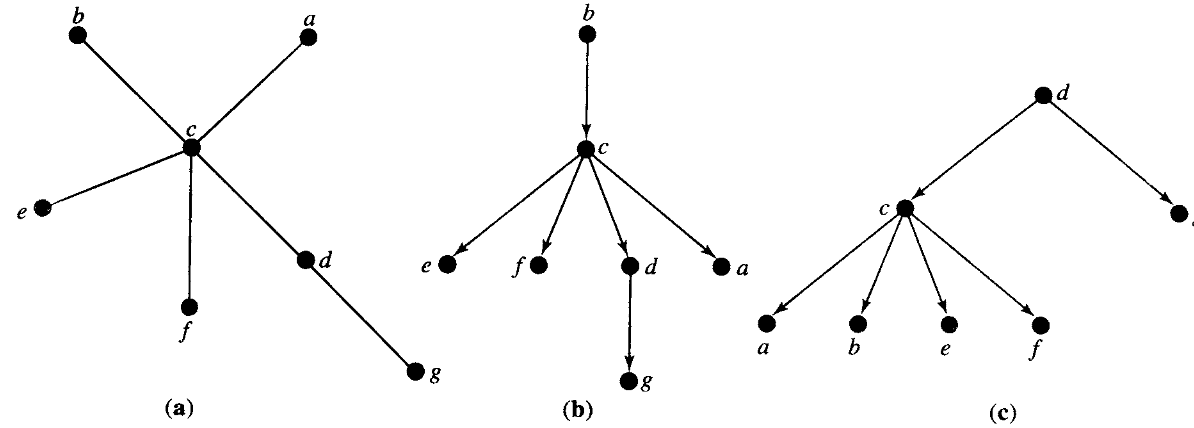
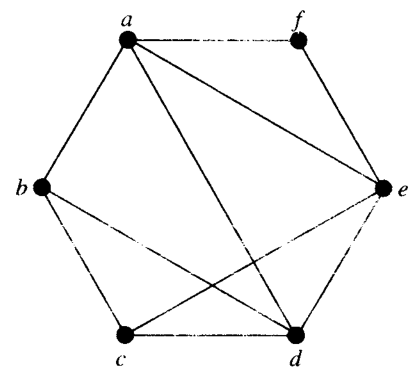


Figura 8.23

Se quiere presentar algunas definiciones alternativas útiles de un árbol no dirigido, y para esto se necesita algunos comentarios acerca de las relaciones simétricas.

Sea R una relación simétrica y sea p: $v_1, v_2, \ldots, v_n$ una trayectoria en R. Se dice que p es **simple** si no existen dos aristas de p correspondientes a la misma arista no dirigida. Si, además, v_1 es igual a v_n (de modo que p sea un ciclo), p es un **ciclo simple**.

Ejemplo 2. La figura 8.24 muestra la gráfica de una relación simétrica R. La trayectoria a, b, c, e, d es simple, pero la trayectoria f, e, d, c, d, a no lo es, ya que d, c y c, d corresponden a la misma arista no dirigida. También, f, e, a, d, b, a, f y d, a, b, d son ciclos simples, pero f, e, d, c, e, f no es un ciclo simple, ya que f, e y e, f corresponden a la misma arista no dirigida. ◆



R

Figura 8.24

Una relación simétrica R es **acíclica** si no contiene ciclos simples. Se puede mostrar que si R contiene ciclos, entonces contiene un ciclo simple. Recuerde (véase la sección 4.4) que una relación simétrica R es conexa si existe una trayectoria en R desde un vértice hacia cualquier otro vértice.

El siguiente teorema proporciona una útil proposición equivalente a la definición anterior de un árbol no dirigido.

Teorema 1. *Sea R una relación simétrica en un conjunto A. Entonces las siguientes proposiciones son equivalentes.*

(a) *R es un árbol no dirigido.*

(b) *R es conexo y acíclico.*

Demostración: Se demostrará que la parte (a) implica la parte (b), y se omitirá la demostración de que la parte (b) implica la parte (a). Suponga que R es un árbol no dirigido, lo que significa que R es la cerradura simétrica de algún árbol T en A. Observe primero que si $(a, b) \in R$, se debe tener $(a, b) \in T$ o $(b, a) \in T$. En términos geométricos, esto significa que cada arista no dirigida en la gráfica de R aparece en el digrafo de T, dirigida en un sentido o en el otro.

Por contradicción, se mostrará que R no tiene ciclos simples. Suponga que R tiene un ciclo simple p: $v_1, v_2, \ldots, v_n, v_1$. Para cada arista (v_i, v_j) en p, se elige la pareja (v_i, v_j) o (v_j, v_i) que esté en T. El resultado es una figura cerrada con aristas en T, donde cada arista debe apuntar en una dirección. Ahora existen tres posibilidades: todas las flechas apuntan en el sentido de las manecillas del reloj, como en la figura 8.25(a), todas apuntan en sentido contrario al de las manecillas del reloj o alguna pareja aparece como en la figura 8.25(b). La figura 8.25(b) es imposible, ya que en un árbol T, cada vértice tiene grado interno 1 (véase el teorema 1 de la sección 8.1). Pero cualquiera de los otros dos casos implicaría que T tiene un ciclo, lo cual también es imposible. Así, la existencia del ciclo p en R lleva a una contradicción y por lo tanto es imposible.

También se debe mostrar que R es conexa. Sea v_0 la raíz del árbol T. Entonces, si a y b son dos vértices en A, deben existir trayectorias p de v_0 a a y q de v_0 a b, como en la figura 8.25(c). Ahora, todas las trayectorias en T son reversibles en R, de modo que $q \circ p^{-1}$, que aparece en la figura 8.25(d), conecta a con b en R, donde p^{-1} es la trayectoria inversa de p. Como a y b son arbitrarios, R es conexa, y queda demostrada la parte (b). ●

Existen otras caracterizaciones útiles de los árboles no dirigidos. Se establecerá dos de ellas sin demostración en el siguiente teorema.

Teorema 2. *Sea R una relación simétrica en un conjunto A. Entonces R es un árbol no dirigido si y sólo si cualquiera de las siguientes proposiciones es verdadera.*

(a) *R es acíclica, y si se agrega cualquier arista no dirigida a R, la nueva relación no será acíclica.*

(b) *R es conexa, y si se elimina cualquier arista no dirigida de R, la nueva relación no será conexa.* ●

El siguiente teorema ayudará a determinar cierto tipo de árboles.

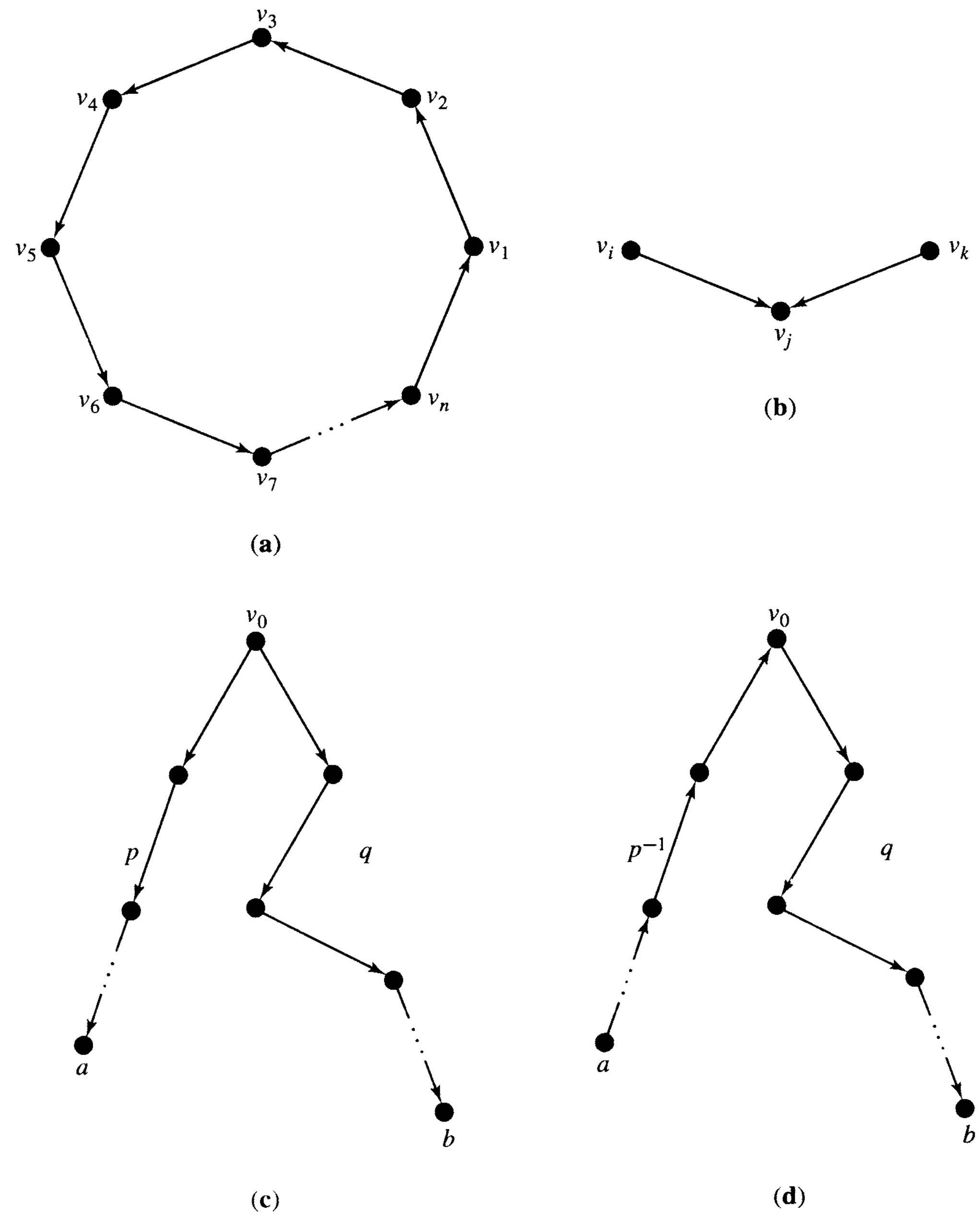


Figura 8.25

Teorema 3. *Un árbol con n vértices tiene $n - 1$ aristas.*

Demostración: Como un árbol es conexo, deben existir al menos $n - 1$ aristas para conectar los n vértices. Supóngase que existen más de $n - 1$ aristas. Entonces la raíz tiene grado interno 1 o algún otro vértice tiene grado interno al menos 2. Pero por el teorema 1 de la sección 8.1, esto es imposible. Así, existen exactamente $n - 1$ aristas. ●

Árboles de expansión de relaciones conexas

Si R es una relación simétrica conexa sobre un conjunto A, un árbol T en A es un **árbol de expansión** para R si T es un árbol con exactamente los mismos vértices que R y que se puede obtener de R eliminando algunas aristas de R.

Ejemplo 3. La relación simétrica R cuya gráfica aparece en la figura 8.26(a) tiene el árbol T' como árbol de expansión, cuyo digrafo aparece en la figura 8.26(b). También, el árbol T'' es un árbol de expansión para R, cuyo digrafo es mostrado en la figura 8.26(c). Como R, T' y T'' son relaciones en el mismo conjunto A, se ha etiquetado los vértices para mostrar la correspondencia de los elementos. Como muestra este ejemplo, los árboles de expansión no son únicos. ◆

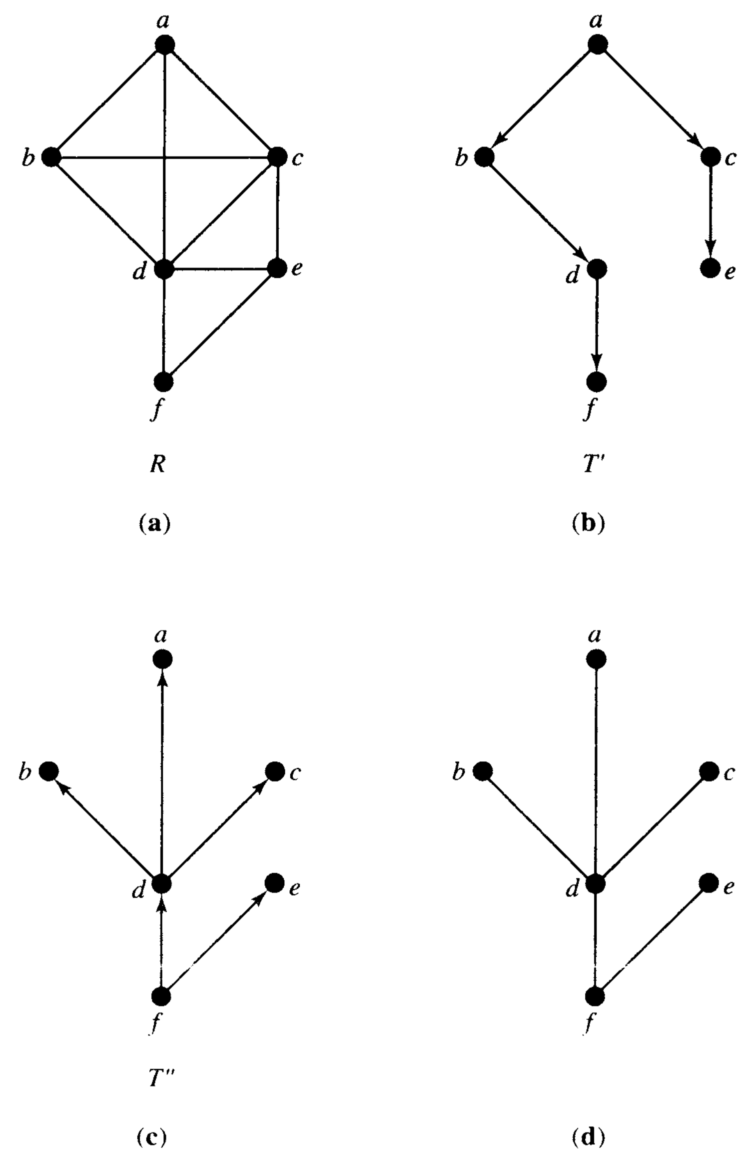


Figura 8.26

A veces existe interés en un **árbol de expansión no dirigido** para una relación simétrica conexa R. Este árbol es la cerradura simétrica de un árbol de expansión. La figura 8.26(d) muestra un árbol de expansión no dirigido para R, deducido del árbol de expansión de la figura 8.26(c). Si R es una relación complicada que es simétrica y conexa, podría ser difícil diseñar un esquema para la búsqueda en R; es decir, para visitar cada uno de sus vértices una vez en cierta forma sistemática. Si R se reduce a un árbol de expansión, puede utilizarse los algoritmos de búsqueda analizados en la sección 8.3.

El teorema 2(b) sugiere un algoritmo para determinar un árbol de expansión no dirigido para una relación R. Sólo hay que eliminar varias aristas no dirigidas de R hasta llegar a un punto donde la eliminación de una más de las aristas no dirigidas produciría una relación no conexa. El resultado será un árbol de expansión no dirigido.

Ejemplo 4. En la figura 8.27(a), se repite la gráfica de la figura 8.26(a). A continuación se muestra el resultado de eliminar varias aristas no dirigidas, lo que culmina en la figura 8.27(f), el árbol de expansión no dirigido, acorde con la figura 8.26(d). ◆

Este algoritmo es bueno para relaciones pequeñas, cuyas gráficas son fáciles de trazar. Para relaciones de mayor tamaño, tal vez guardado en una computadora, el algoritmo es ineficiente, ya que en cada etapa se debe verificar la conexidad, y esto exige un algoritmo complicado. Ahora se presentará un método más eficiente, que además produce un árbol de expansión, en vez de un árbol de expansión no dirigido.

Sea R una relación en un conjunto A, y sean $a, b \in A$. *Sea* $A_0 = A - \{a, b\}$, y $A' = A_0 \cup \{a'\}$, donde a' es un nuevo elemento que no está en A. Defina una relación R' en A' como sigue. Suponga que $u, v \in A'$, $u \neq a'$, $v \neq a'$. Sea $(a', u) \in R'$ si y sólo si $(a, u) \in R$ o $(b, u) \in R$. Sea $(u, a') \in R'$ si y sólo si $(u, a) \in R$ o $(u, b) \in R$. Por último, sea $(u, v) \in R'$ si y sólo si $(u, v) \in R$. Se dice que R' es el resultado de unir los vértices a y b. Esto es similar a la unión de vértices analizada en la sección 6.1.

Imagine, en el digrafo de R, que los vértices son alfileres, y que las aristas son ligas elásticas que pueden encogerse hasta la longitud cero. Ahora, acerque físicamente los alfileres a y b, encogiendo la arista entre ellos (si existe), hasta una longitud cero. El digrafo resultante es el digrafo de R'. Si R es simétrica, se puede realizar la misma operación en la gráfica de R.

Ejemplo 5. La figura 8.28(a) muestra la gráfica de una relación simétrica R. En la figura 8.28(b) se muestra el resultado de unir los vértices v_0 y v_1 en un nuevo vértice v_0'. En la figura 8.28(c) se muestra el resultado de unir los vértices v_0' y v_2 de la relación cuya gráfica aparece en la figura 8.28(b) en un nuevo vértice v_0''. Observe en la figura 8.28(c) que se ha combinado las aristas no dirigidas que estaban presentes entre v_0' y v_3 y entre v_2 y v_3 en una arista no dirigida. ◆

La forma algebraica de este proceso de unión también es muy importante. Se centrará la atención en las relaciones simétricas y sus gráficas. Gracias a la sección 4.2, se sabe cómo construir la matriz de una relación R.

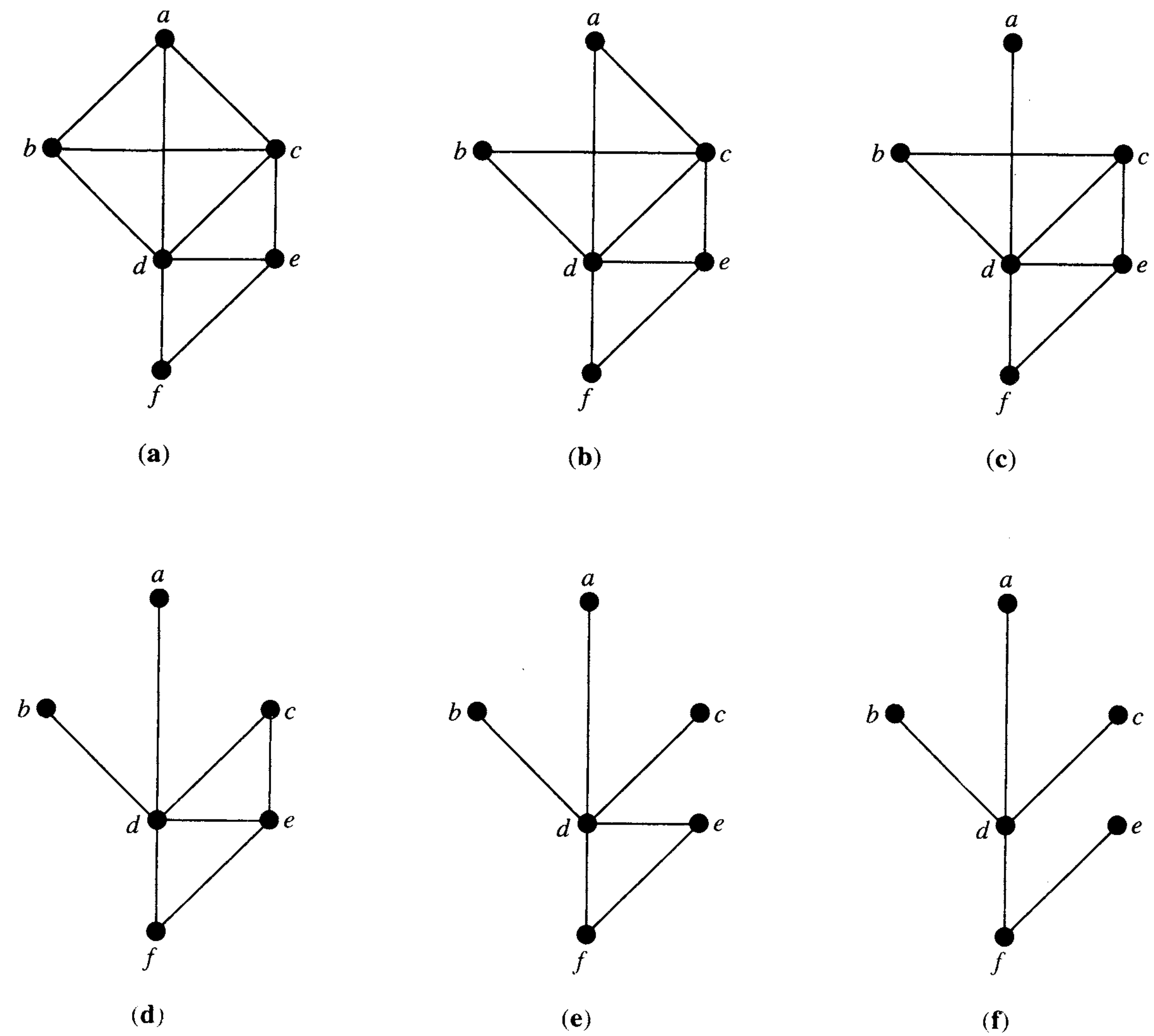


Figura 8.27

Si R es una relación en A, se hará referencia, temporalmente, a los elementos de A como vértices de R. Esto facilitará el análisis.

Supóngase ahora que se une los vértices a y b de una relación R en un nuevo vértice a' que reemplaza a ambos vértices para obtener la relación R'. Para determinar la matriz de R', se procede de la siguiente manera.

Paso 1. El renglón i representa el vértice a y el renglón j representa el vértice b. Se reemplaza el renglón i con la unión de los renglones i y j. La unión de las dos n-adas de ceros y unos tiene un 1 en una posición precisamente cuando alguna de las dos n-adas tiene un 1 en esa posición.

Paso 2. Se reemplaza la columna i por la unión de las columnas i y j

Paso 3. Se restaura la diagonal principal con sus valores originales en R.

Paso 4. Se elimina el renglón j y la columna j.

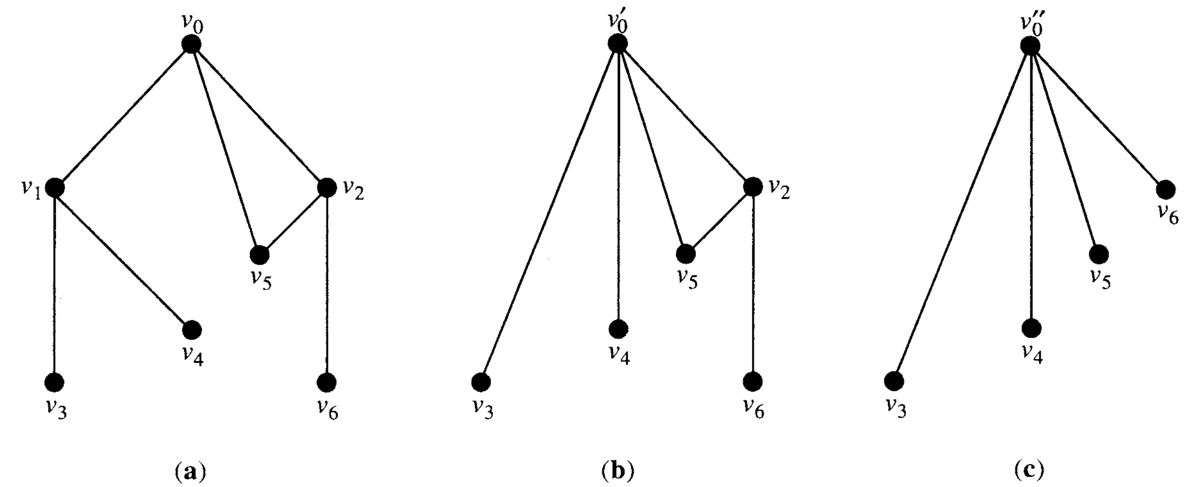


Figura 8.28

Se hace la siguiente observación con respecto del paso 3. Si $e = (a, b) \in R$ y se une a y b, entonces e será un ciclo de longitud 1 en a'. Esta situación no es la deseable, ya que no corresponde a "encoger (a, b) hasta cero". El paso 3 corrige esto.

Ejemplo 6. La figura 8.29 proporciona las matrices para las relaciones simétricas correspondientes cuyas gráficas fueron dadas en la figura 8.28. En la figura 8.29(b), se ha unido los vértices v_0 y v_1 en v_0'. Observe que esto se hace considerando la unión de los dos primeros renglones e introduciendo el resultado en el renglón 1. Se hace lo mismo para las columnas, después se restaura la diagonal y se elimina el renglón 2 y la columna 2. Si se une los vértices v_0' y v_2 en la gráfica cuya matriz está dada en la figura 8.29(b), la gráfica resultante tiene la matriz de la figura 8.29(c). ◆

$$
\begin{array}{c}
 \\ v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6
\end{array}
\begin{array}{c}
\begin{array}{ccccccc} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \end{array} \\
\begin{bmatrix}
0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0
\end{bmatrix}
\end{array}
\qquad
\begin{array}{c}
 \\ v_0' \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6
\end{array}
\begin{array}{c}
\begin{array}{cccccc} v_0' & v_2 & v_3 & v_4 & v_5 & v_6 \end{array} \\
\begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0
\end{bmatrix}
\end{array}
\qquad
\begin{array}{c}
 \\ v_0'' \\ v_3 \\ v_4 \\ v_5 \\ v_6
\end{array}
\begin{array}{c}
\begin{array}{ccccc} v_0'' & v_3 & v_4 & v_5 & v_6 \end{array} \\
\begin{bmatrix}
0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0
\end{bmatrix}
\end{array}
$$

(a) (b) (c)

Figura 8.29

Ahora puede proporcionarse un algoritmo para determinar un árbol de expansión para una relación simétrica conexa R en el conjunto $A = \{v_1, v_2, \ldots, v_n\}$. El método es un caso especial de un algoritmo llamado **algoritmo de Prim**. Los pasos son los siguientes:

Paso 1. Se elige un vértice v_1 de R, y se ordena la matriz de R de modo que el primer renglón corresponda a v_1.

PASO 2. Se elige un vértice v_2 de R, tal que $(v_1, v_2) \in R$, se une v_1 y v_2 en un nuevo vértice v_1' que representa a $\{v_1, v_2\}$ y se reemplaza v_1 por v_1'. Se calcula la matriz de la relación resultante R'. El vértice v_1' es un vértice unido.

PASO 3. Se repite los pasos 1 y 2 en R' y en todas las relaciones subsecuentes hasta obtener una relación con un único vértice. En cada paso, se mantiene un registro del conjunto de vértices originales representada por cada vértice unido.

PASO 4. Se construye el árbol de expansión de la siguiente manera. En cada etapa, al unir los vértices a y b, se elige una arista en R de uno de los vértices originales representados por a hacia uno de los vértices originales representados por b.

Ejemplo 7. Se aplica el algoritmo de Prim a la relación simétrica cuya gráfica está en la figura 8.30.

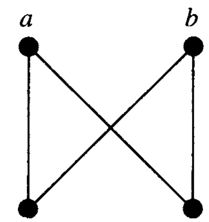


Figura 8.30

En la tabla 8.1, se muestra las matrices obtenidas al reducir mediante uniones el conjunto original de vértices, hasta obtener un único vértice, y en cada etapa se mantiene un registro del conjunto de vértices originales representados por cada vértice unido, así como del nuevo vértice que va a unirse.

Tabla 8.1

Matriz	Vértices originales representados por los vértices unidos	Nuevo vértice por unir (con el primer renglón)
$\begin{array}{c c} & \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \end{array} & \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$	—	c
$\begin{array}{c c} & \begin{array}{ccc} a' & b & d \end{array} \\ \begin{array}{c} a' \\ b \\ d \end{array} & \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \end{array}$	$a' \leftrightarrow \{a, c\}$	b
$\begin{array}{c c} & \begin{array}{cc} a'' & d \end{array} \\ \begin{array}{c} a'' \\ d \end{array} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array}$	$a'' \leftrightarrow \{a, c, b\}$	d
$\begin{array}{c c} & a''' \\ a''' & [0] \end{array}$	$a''' \leftrightarrow \{a, c, d, b\}$	—

El primer vértice elegido es a, y se elige c como el vértice por unir con a, ya que existe un 1 en el vértice c en el renglón 1. También se elige la arista (a, c) de la gráfica original. En la segunda etapa, existe un 1 en el vértice b en el renglón 1, por lo que se une b con el vértice a'. Se elige una arista en la relación original R a partir de un vértice de $\{a, c\}$ a b, por decir (c, b). En la tercera etapa, se debe unir d con el vértice a''. De nuevo, se necesita una arista en R de un vértice de $\{a, b, c\}$ a d, por decir (a, d). Las aristas seleccionadas (a, c), (c, b) y (a, d) forman el árbol de expansión para R, el cual aparece en la figura 8.31. Observe que el primer vértice elegido es la raíz del árbol de expansión construido. ◆

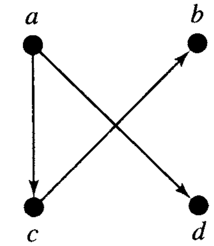


Figura 8.31

GRUPO DE EJERCICIOS 8.4

En los ejercicios 1 *al* 6 *(figuras* 8.32 *a la* 8.37*), utilice el algoritmo de Prim para construir un árbol de expansión para la gráfica conexa mostrada. Utilice el vértice indicado como la raíz del árbol y trace el digrafo del árbol de expansión obtenido.*

1. Utilice e como la raíz.

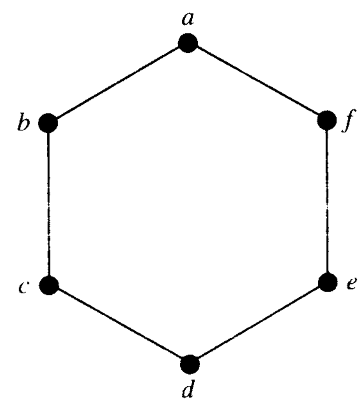


Figura 8.32

2. Utilice 5 como la raíz.

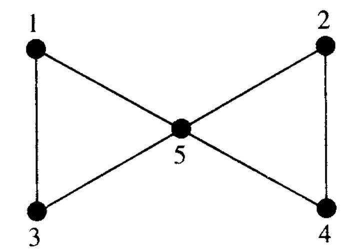


Figura 8.33

3. Utilice c como la raíz.

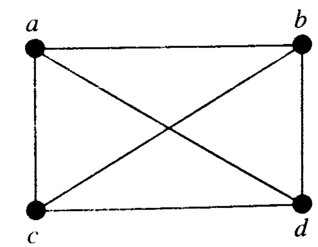


Figura 8.34

4. Utilice 4 como la raíz.

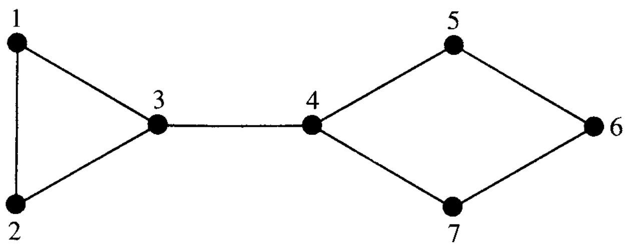


Figura 8.35

5. Utilice e como la raíz.

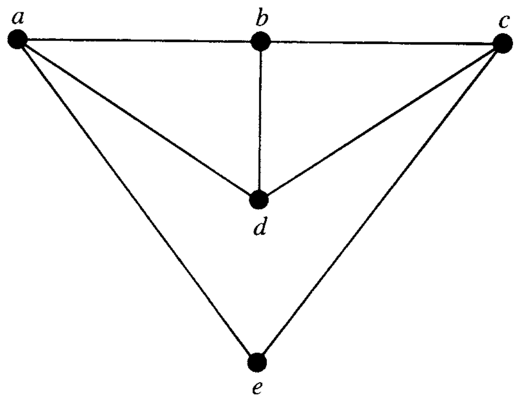


Figura 8.36

6. Utilice d como la raíz.

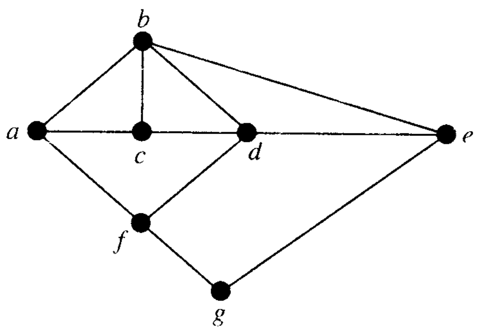


Figura 8.37

En los ejercicios 7 al 12, construya un árbol de expansión no dirigido para la gráfica conexa G, eliminando aristas. Muestre la gráfica del árbol de expansión no dirigido resultante.

7. Sea G la gráfica de la figura 8.32.

8. Sea G la gráfica de la figura 8.33.

9. Sea G la gráfica de la figura 8.34.

10. Sea G la gráfica de la figura 8.35.

11. Sea G la gráfica de la figura 8.36.

12. Sea G la gráfica de la figura 8.37.

13. Considere la gráfica conexa de la figura 8.38. Muestre las gráficas de tres árboles de expansión no dirigidos diferentes.

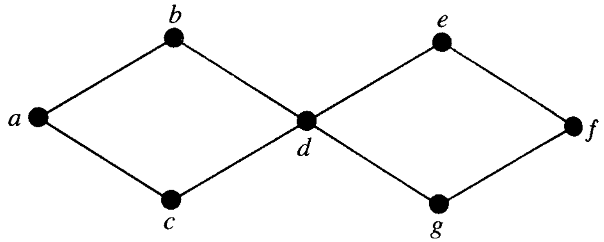


Figura 8.38

14. Para la gráfica conexa de la figura 8.39, muestre las gráficas de todos los árboles de expansión no dirigidos.

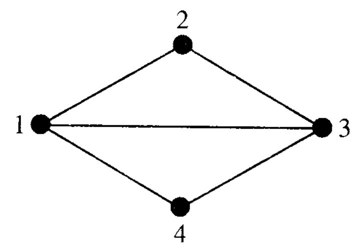


Figura 8.39

15. Para el árbol no dirigido de la figura 8.40 muestre los digrafos de todos los árboles de expansión. ¿Cuántos existen?

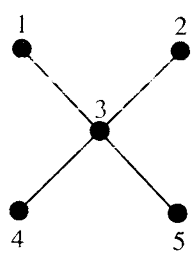


Figura 8.40

16. Para cada una de las gráficas de la figura 8.41 proporcione todos los árboles de expansión.

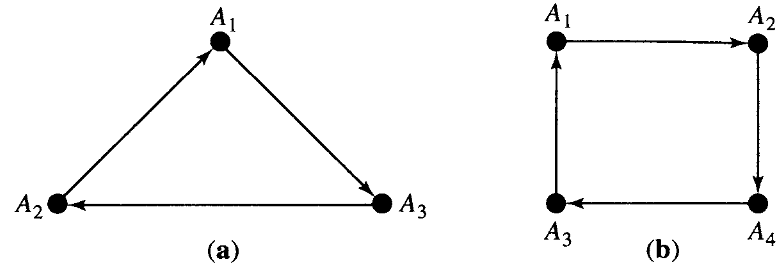


Figura 8.41

17. Para cada una de las gráficas de la figura 8.42 ¿cuántos árboles de expansión diferentes existen?

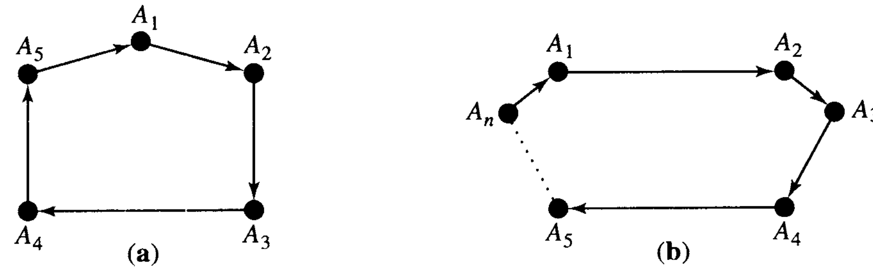


Figura 8.42

18. Establezca su conclusión para la figura 8.42(b) como un teorema y demuéstrelo.

8.5. Árboles de expansión mínima

En muchas aplicaciones de las relaciones simétricas conexas, la gráfica (no dirigida) de la relación modela una situación donde las aristas y los vértices contienen información. Una **gráfica con pesos** es una gráfica donde cada arista está etiquetada con un valor numérico que denota su **peso**.

Ejemplo 1. Un pequeño pueblo mantiene un sistema de veredas para transitar entre las áreas de recreación en el pueblo. El sistema se modela mediante una gráfica con pesos en la figura 8.43, donde los pesos representan las distancias en kilómetros que hay entre los sitios. ◆

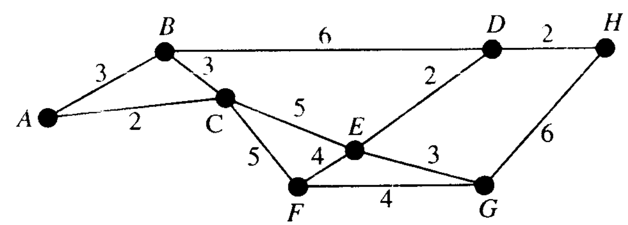


Figura 8.43

Ejemplo 2. Una compañía de comunicación investiga el costo de la actualización de las conexiones entre sus estaciones de transmisión. La gráfica con pesos de la figura 8.44 muestra las estaciones y el costo en millones de dólares para la actualización de cada conexión. ♦

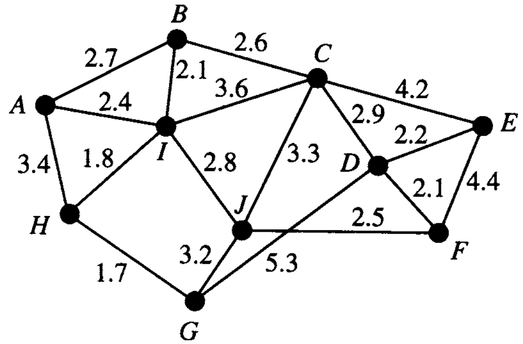


Figura 8.44

El peso de una arista (v_i, v_j) es la **distancia entre los vértices** v_i y v_j. Un vértice u es un **vecino más cercano del vértice v** si u y v son adyacentes y ningún otro vértice queda unido con v mediante una arista de menor peso que (u, v). Observe que, a diferencia de lo que sucede en la gramática, v puede tener más de un vecino cercano.

Ejemplo 3. En la gráfica de la figura 8.43, el vértice C es uno de los vecinos más cercanos del vértice A. Ambos vértices E y G son vecinos más cercanos de F. ♦

Un vértice v es un **vecino más cercano de un conjunto de vértices** $V = \{v_1, v_2, \ldots, v_k\}$ en una gráfica si v es adyacente a algún miembro v_i de V y ningún otro vértice adyacente a un miembro de V está unido mediante una arista de menor peso que (v, v_i).

Ejemplo 4. En relación con la gráfica de la figura 8.44, sea $V = \{C, E, J\}$. Entonces el vértice D es un vecino más cercano de V, ya que (D, E) tiene peso 2.2 y ningún otro vértice adyacente a C, E o J se une a uno de estos vértices mediante una arista de menor peso. ♦

En las aplicaciones de las gráficas con pesos, con frecuencia se necesita determinar un árbol de expansión no dirigido para el cual el peso total de las aristas en el árbol sea el menor posible. Este árbol se conoce como **árbol de expansión mínima**. El algoritmo de Prim (sección 8.4) se puede adaptar fácilmente para producir un árbol de expansión mínima para una gráfica con pesos. A continuación se enunciará el algoritmo de Prim como si fuera aplicado a una relación simétrica conexa, dada por su gráfica de pesos no dirigida.

Algoritmo de Prim: Sea R una relación simétrica, conexa con n vértices.

Paso 1. Se elige un vértice v_1 de R. Sea $V = \{v_1\}$ y $E = \{\ \}$.

Paso 2. Se elige uno de los vecinos más cercanos a v_i de V, que sea adyacente a v_j, $v_j \in V$, y tal que la arista (v_i, v_j) no forme un ciclo con miembros de E. Se agrega v_i a V y (v_i, v_j) a E.

Paso 3. Se repite el paso 2 hasta que $|E| = n - 1$. Entonces V contiene los n vértices de R y E contiene las aristas de un árbol de expansión mínima para R.

Fin del algoritmo

En esta versión del algoritmo de Prim, se comienza en cualquier vértice de R y se construye un árbol de expansión mínima agregando una arista a un vecino más cercano del conjunto de vértices ya unidos, siempre que al agregar esta arista no se forme un ciclo. Esto es un ejemplo de **algoritmo ambicioso**. En cada etapa se elige lo "mejor", con base en las condiciones locales, en vez de observar la situación global. Los algoritmos ambiciosos no siempre producen soluciones óptimas, pero es posible mostrar que en este caso la solución es óptima.

Teorema 1. *El algoritmo de Prim dado arriba produce un árbol de expansión mínima para la relación.*

Demostración: Sea T el árbol obtenido mediante el algoritmo de Prim para R y $t_1, t_2, \ldots, t_{n-1}$ sus aristas. Suponga que T no es un árbol de expansión mínima para R. Entre los árboles de expansión mínima de R, sea S uno con la siguiente propiedad: $t_1, t_2, \ldots, t_i$ son aristas en S con $I < n - 1$ tan grande como sea posible. Es decir, ningún árbol de expansión mínima de R contiene a $t_1, t_2, \ldots, t_i, t_{i+1}$. Ahora considere $S \cup \{t_{i+1}\}$. Esta gráfica debe contener un ciclo simple ya que tiene n aristas. La figura 8.45 ilustra esta situación. Cuando t_{i+1} fue seleccionada mediante el algoritmo de Prim, ya sea s_j o s_k también estaba disponible para la selección, por decir, s_j, de modo que el peso de t_{i+1} es menor o igual que el de s_j. Así $S - \{s_j\} \cup \{t_{i+1}\}$ es un árbol de expansión mínima de R que contiene a $t_1, t_2, \ldots, t_i, t_{i+1}$. Pero esto contradice la elección de i. Por lo tanto, T es un árbol de expansión mínima para R. ●

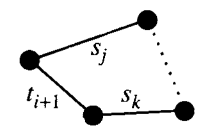


Figura 8.45

Ejemplo 5. El pueblo del ejemplo 1 planea pavimentar algunas de las veredas de manera que sirvan para transitar y también para andar en bicicleta. Como una primera etapa, el pueblo quiere unir todas las áreas recreativas con rutas de bicicleta, de la manera más barata posible. Si los costos de construcción son iguales en todas las partes del sistema, utilice el algoritmo de Prim para determinar un plan de pavimentación.

Solución: En relación con la figura 8.43, si se elige A como el primer vértice, el vecino más cercano es C, a 2 kilómetros de distancia. Así (A, C) es la primera arista elegida. Con respecto del conjunto de vértices $\{A, C\}$, B es el vecino más cercano, y se puede elegir (A, B) o (B, C) como la siguiente arista. De manera arbitraria, se elige (B, C). B es un vecino más cercano para $\{A, B, C\}$, pero la única arista disponible (A, B) formaría un ciclo, por lo que se debe pasar al siguiente vecino más cercano y elegir (C, F) [o (C, E)]. La figura 8.46(a) a (c) muestra los pasos iniciales y la figura 8.46(d) muestra un posible resultado final. La figura 8.46(e) muestra un árbol de expansión mínima, obtenido mediante el algoritmo de Prim comenzando con el vértice E. En cada caso, las rutas para bicicleta cubrirían 21 kilómetros. ♦

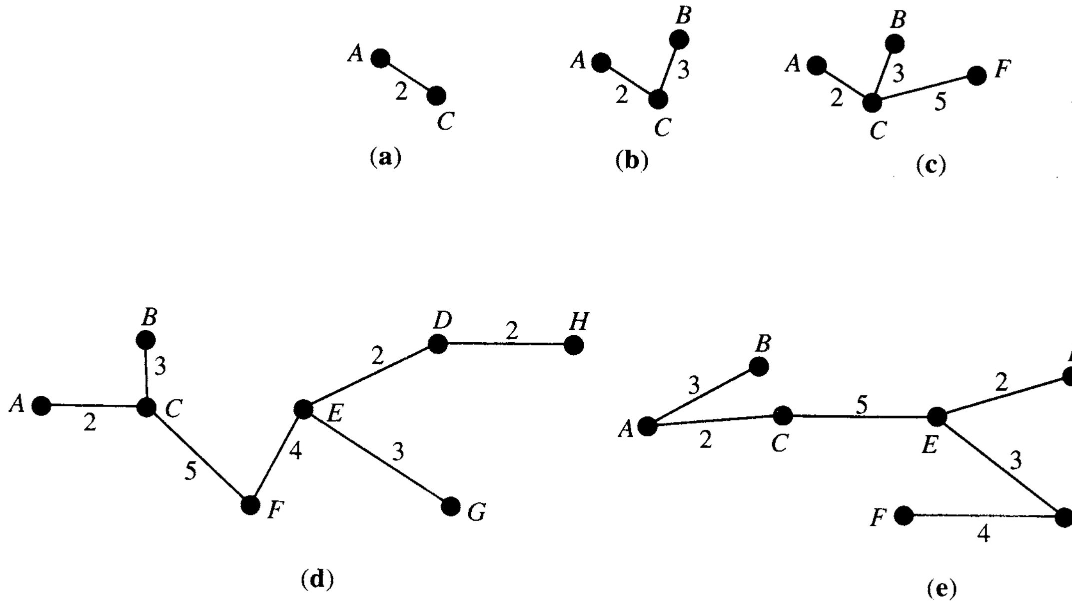


Figura 8.46

Ejemplo 6. Puede determinarse un árbol de expansión mínima para la red de comunicación del ejemplo 2 utilizando el algoritmo de Prim, comenzando en cualquier vértice. La figura 8.47 muestra un árbol de expansión mínima obtenido partiendo de I. El costo total de actualización de estas conexiones sería de \$20,800,000. ◆

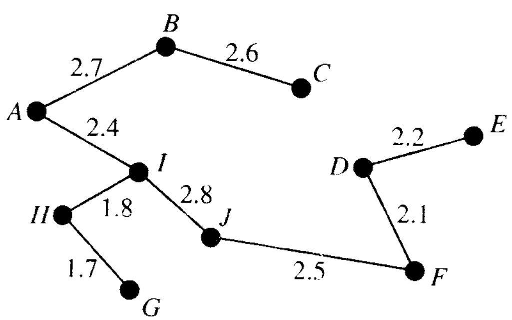


Figura 8.47

Si una relación simétrica conexa R tiene n vértices, entonces el algoritmo de Prim tiene un tiempo de ejecución $O(n^2)$. (Esto se puede mejorar un poco.) Si R tiene relativamente pocas aristas, podría ser más eficiente utilizar otro algoritmo. Esto es similar al caso de determinación si una relación es transitiva, como en la sección 4.6. El algoritmo de Kruskal es otro ejemplo de algoritmo ambicioso con el que se obtiene una solución óptima.

ALGORITMO DE KRUSKAL: Sea R una relación simétrica, conexa con n vértices y sea $S = \{e_1, e_2, \ldots, e_k\}$ el conjunto de todas las aristas con pesos de R.

PASO 1. Se elige una arista e_1 en S de peso mínimo. Sea $E = \{e_1\}$. Se reemplaza S por $S - \{e_1\}$.

PASO 2. Se selecciona una arista e_i de menor peso que no forme un ciclo con los miembros de E. Se reemplaza E con $E \cup \{e_i\}$ y S con $S - \{e_i\}$.

PASO 3. Se repite el paso 2 hasta que $|E| = n - 1$.

Fin del algoritmo

Como R tiene n vértices, las $n - 1$ aristas en E formarán un árbol de expansión. El proceso de selección en el paso 2 garantiza que éste es un árbol de expansión mínima. (Se omite la demostración.) En pocas palabras, el tiempo de ejecución del algoritmo de Kruskal es $O(k\, lg(k))$, donde k es el número de aristas en R.

Ejemplo 7. La figura 8.48 proporciona un árbol de expansión mínima generado mediante el algoritmo de Kruskal para las veredas del ejemplo 1. Una secuencia de selecciones de aristas es (D, E), (D, H), (A, C), (A, B), (E, G), (E, F) y (C, E) para un peso total de 21 kilómetros. Naturalmente, cualquiera de los algoritmos para obtener árboles de expansión mínimos produce árboles del mismo peso. ◆

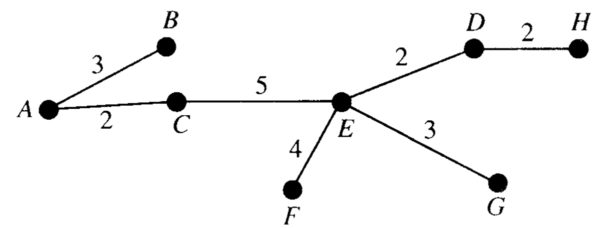


Figura 8.48

Ejemplo 8. Utilice el algoritmo de Kruskal y determine un árbol de expansión mínima para la relación dada en la gráfica de la figura 8.49.

Solución: Inicialmente, existen dos aristas de menor peso (B, C) y (E, F). Se eligen ambas. Después hay tres aristas (A, G), (B, G) y (D, E), de peso 12. Todas éstas pueden ser agregadas sin crear ciclos. La arista (F, G) de peso 14 es la arista restante de menor peso. Al agregar (F, G) se obtiene seis aristas de una gráfica de 7 vértices, de modo que se ha determinado un árbol de expansión mínima. ◆

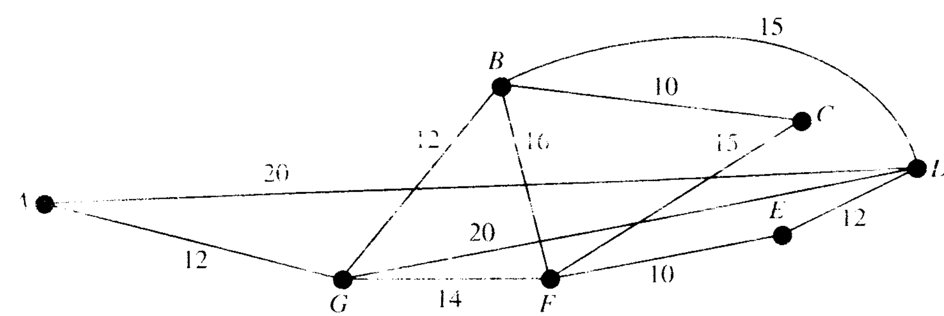


Figura 8.49

GRUPO DE EJERCICIOS 8.5

En los ejercicios 1 al 6, utilice el algoritmo de Prim de esta sección y determine un árbol de expansión mínima para la gráfica conexa indicada. Utilice el vértice especificado como vértice inicial.

1. Sea G la gráfica de la figura 8.43. Comience en F.

2. Sea G la gráfica de la figura 8.44. Comience en A.

3. Sea G la gráfica de la figura 8.49. Comience en G.

4. Sea G la gráfica de la figura 8.50. Comience en E.

5. Sea G la gráfica de la figura 8.51. Comience en K.

6. Sea G la gráfica de la figura 8.51. Comience en M.

En los ejercicios 7 al 9, utilice el algoritmo de Kruskal y determine un árbol de expansión mínima para la gráfica indicada.

7. Sea G la gráfica de la figura 8.44.

8. Sea G la gráfica de la figura 8.50.

9. Sea G la gráfica de la figura 8.51.

10. Las distancias entre ocho ciudades están dadas en la tabla de la página 327. Utilice el algoritmo de Kruskal y determine un árbol de expansión mínima cuyos vértices son las ciudades. ¿Cuál es la distancia total para el árbol?

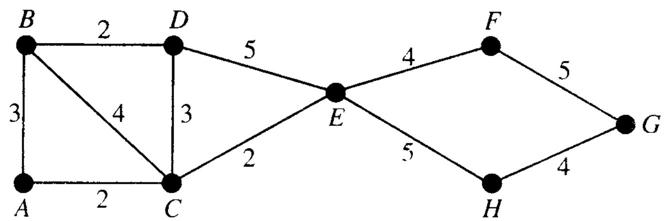


Figura 8.50

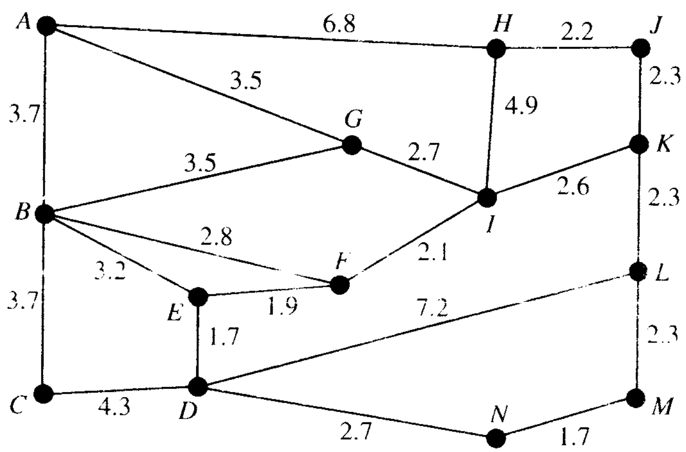


Figura 8.51

	Abbeville	Aiken	Allendale	Anderson	Asheville	Athens	Atlanta	Augusta
Abbeville		69	121	30	113	70	135	63
Aiken	69		52	97	170	117	163	16
Allendale	121	52		149	222	160	206	59
Anderson	30	97	149		92	63	122	93
Asheville	113	170	222	92		155	204	174
Athens	70	117	160	63	155		66	101
Atlanta	135	163	206	122	204	66		147
Augusta	63	16	59	93	174	101	147	

11. Suponga que al construir un árbol de expansión mínima se debe incluir una cierta arista. Proporcione una versión modificada del algoritmo de Kruskal para este caso.

12. Repita el ejercicio 10 con el requisito de que debe incluirse la ruta de Atlanta a Augusta. ¿Cuánto hace crecer esto al árbol?

13. Modifique el algoritmo de Kruskal para obtener un árbol de expansión máxima; es decir, uno con la suma máxima de pesos.

14. Suponga que la gráfica de la figura 8.51 representa los flujos posibles a través de un sistema de tuberías. Determine un árbol de expansión que proporcione el flujo máximo posible en este sistema.

15. Modifique el algoritmo de Prim de esta sección para determinar un árbol de expansión máxima.

16. Utilice el algoritmo de Prim modificado del ejercicio 15 para determinar un árbol de expansión máxima para la gráfica de la figura 8.51.

17. En el ejemplo 5 se muestran dos árboles de expansión mínima para la misma gráfica. ¿En qué casos tiene una gráfica con pesos un único árbol de expansión mínima? Justifique su respuesta.

18. Modifique el algoritmo de Prim para determinar un árbol de expansión máxima, si se debe incluir cierta arista en el árbol.

IDEAS CLAVE PARA REPASO

- Árbol: relación sobre un conjunto finito A tal que existe un vértice $v_0 \in A$ con la propiedad de que existe una única trayectoria de v_0 hacia cualquier otro vértice en A y ninguna trayectoria de v_0 hacia v_0.
- Raíz del árbol: vértice v_0 en la definición anterior.
- Árbol con raíz (T, v_0): árbol T con raíz v_0.
- Teorema. Sea (T, v_0) un árbol con raíz. Entonces
  - (a) No existen ciclos en T.
  - (b) v_0 es la única raíz de T.
  - (c) Cada vértice en T, distinto de v_0, tiene grado interno uno y v_0 tiene grado interno cero.
- Nivel: véase la página 287.
- Hojas: vértices sin hijos.
- Teorema. Sea T un árbol con raíz sobre un conjunto A. Entonces
  - (a) T es irreflexivo.
  - (b) T es asimétrico.
  - (c) Si $(a, b) \in T$ y $(b, c) \in T$, entonces $(a, c) \notin T$, para toda a, b y c en A.
- n-árbol: árbol donde cada vértice tiene a lo más n hijos.
- Árbol binario: 2-árbol.
- Teorema. Si (T, v_0) es un árbol con raíz y $v \in T$, entonces $T(v)$ es también un árbol con raíz v.
- $T(v)$: subárbol de T que comienza en v.
- Árbol posicional binario: véase la página 294.
- Representación de los árboles en computadora: véase la página 295.
- Búsqueda en preorden: véase la página 300.
- Búsqueda en entreorden: véase la página 303.

- Búsqueda en postorden: véase la página 303.
- Notación polaca inversa: véase la página 304.
- Búsqueda en árboles generales: véase la página 304.
- Representación en lista enlazada de un árbol: véase la página 306.
- Árbol no dirigido: cerradura simétrica de un árbol.
- Trayectoria simple: ninguna pareja de aristas corresponden a la misma arista no dirigida.
- Relación simétrica conexa R: existe una trayectoria en R de cualquier vértice a otro vértice.
- Teorema: un árbol con n vértices tiene $n - 1$ aristas.
- Árbol de expansión para una relación simétrica conexa R: árbol que llega a todos los vértices de R y cuyas aristas son todas aristas de R.
- Árbol de expansión no dirigido: cerradura simétrica de un árbol de expansión.
- Algoritmo de Prim: véase la página 317.
- Gráfica con pesos: una gráfica cuyas aristas están etiquetadas con un valor numérico.
- Distancia entre vértices v_i y v_j: peso de (v_i, v_j).
- Vecino más cercano de v: véase la página 322.
- Árbol de expansión mínima: árbol de expansión no dirigido donde el peso total de las aristas es el menor posible.
- Algoritmo de Prim (segunda versión): véase la página 322.
- Algoritmo ambicioso: véase la página 323.
- Algoritmo de Kruskal: véase la página 324.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes ejercicios, escriba el programa o subrutina solicitado en seudocódigo (según lo descrito en el apéndice A) o en un lenguaje de programación que usted conozca. Verifique su código con papel y lápiz o con una ejecución en computadora.

1. Utilice los arreglos LEFT, DATA y RIGHT (sección 8.2) en un programa para guardar letras, de modo que un recorrido en postorden del árbol creado imprima las letras en orden alfabético.

2. Escriba un programa tal que su entrada sea un árbol ordenado y tenga como salida el árbol posicional binario correspondiente (según lo descrito en la sección 8.3).

3. Escriba una subrutina para realizar la unión de los vértices descritos en el algoritmo de Prim de la página 317.

4. Escriba un código para la segunda versión del algoritmo de Prim (sección 8.5).

5. Escriba el código para el algoritmo de Kruskal.

CAPÍTULO 9

SEMIGRUPOS Y GRUPOS

Requisito previo: Capítulo 7

En la sección 1.6 se presentó el concepto de estructura matemática. En los capítulos posteriores se desarrolló otros tipos de sistemas matemáticos, como [proposiciones, $\wedge$, $\vee$, ~], que no tenían un nombre específico, o como B_n, el álgebra booleana sobre n elementos, que sí tiene un nombre. En este capítulo se identificarán otros dos tipos de estructuras matemáticas, los semigrupos y los grupos. Se utilizará los semigrupos en el estudio de las máquinas de estado finito en el capítulo 10. También se desarrollará las ideas básicas de la teoría de grupos, mismas que serán aplicadas a la teoría de códigos en el capítulo 11.

9.1. Repaso de las operaciones binarias

Ya se ha definido las operaciones binarias (véase la sección 1.6) y en la sección 5.2 se observa que es posible utilizar una operación binaria para definir una función. Ahora se realizará el proceso en sentido contrario y se definirá una operación binaria como una función con ciertas propiedades.

Una **operación binaria sobre un conjunto** A es una función definida para todo punto $f: A \times A \to A$. Observe las propiedades que debe satisfacer una operación binaria:

1. Como $\mathrm{Dom}(f) = A \times A$, f asigna un elemento $f(a, b)$ de A a cada pareja ordenada (a, b) en $A \times A$. Es decir, la operación binaria debe estar definida para cada pareja ordenada de elementos de A.
2. Como una operación binaria es una función, sólo se asigna un elemento de A a cada pareja ordenada.

De esta forma se puede decir que una operación binaria es una regla que asigna a cada pareja ordenada de elementos de A un único elemento de A. El lector debe observar que esta definición es más restrictiva que la del capítulo 1, pero se ha realizado el cambio para simplificar el análisis en este capítulo. A continuación se verá algunos ejemplos.

Se acostumbra denotar las operaciones binarias mediante un símbolo, como $*$, en vez de f, y denotar el elemento asignado a (a, b) como $a * b$ [en vez de $*(a, b)$]. Se debe enfatizar que si a y b son elementos en A, entonces $a * b \in A$; por lo general se describe esta propiedad diciendo que A es **cerrado** bajo la operación $*$.

Ejemplo 1. Sea $A = Z$. Se define $a * b$ como $a + b$. Entonces $*$ es una operación binaria sobre Z. ◆

Ejemplo 2. Sea $A = \mathbb{R}$. Se define $a * b$ como a/b. Entonces $*$ no es una operación binaria, pues no está definida para cada pareja de elementos de A. Por ejemplo, $3 * 0$ no está definida, pues no se puede dividir entre cero. ◆

Ejemplo 3. Sea $A = Z^+$. Se define $a * b$ como $a - b$. Entonces $*$ no es una operación binaria, pues no asigna un elemento de A a cada pareja de elementos de A; por ejemplo, $2 * 5 \notin A$. ◆

Ejemplo 4. Sea $A = Z$. Se define $a * b$ como un número menor que a y b. Entonces $*$ no es una operación binaria, pues no asigna un *único* elemento de A a cada pareja ordenada de elementos de A; por ejemplo, $8 * 6$ podría ser 5, 4, 3, 1, etcétera. Así, en este caso, $*$ sería una relación de $A \times A$ en A, pero no una función. ◆

Ejemplo 5. Sea $A = Z$. Se define $a * b$ como $\text{máx}\{a, b\}$. Entonces $*$ es una operación binaria; por ejemplo, $2 * 4 = 4$, $-3 * (-5) = -3$. ◆

Ejemplo 6. Sea $A = P(S)$, para algún conjunto S. Si V y W son subconjuntos de S, se define $V * W$ como $V \cup W$. Entonces $*$ es una operación binaria sobre A. Además, si se define $V * W$ como $V \cap W$, entonces $*$ es otra operación binaria sobre A. ◆

Como muestra el ejemplo 6, es posible definir muchas operaciones binarias sobre el mismo conjunto.

Ejemplo 7. Sea M el conjunto de todas las matrices booleanas $n \times n$. Se define $\mathbf{A} * \mathbf{B}$ como $\mathbf{A} \vee \mathbf{B}$ (véase la sección 1.5). Entonces $*$ es una operación binaria. Lo mismo ocurre para $\mathbf{A} \wedge \mathbf{B}$. ◆

Ejemplo 8. Sea L una retícula. Se define $a * b$ como $a \wedge b$ (la máxima cota inferior de a y b). Entonces $*$ es una operación binaria sobre L. Esto también es cierto para $a \vee b$ (la mínima cota superior de a y b). ◆

Tablas

Si $A = \{a_1, a_2, \ldots, a_n\}$ es un conjunto finito, es posible definir una operación binaria sobre A mediante una tabla como la que aparece en la figura 9.1. La entrada en la posición i, j denota el elemento $a_i * a_j$.

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

Figura 9.1

Ejemplo 9. Sea $A = \{0, 1\}$. Se define las operaciones binarias $\vee$ y $\wedge$ con las tablas siguientes:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

◆

Si $A = \{a, b\}$, se determinará el número de operaciones binarias que es posible definir sobre A. Se puede describir cualquier operación binaria $*$ en A mediante la tabla

$*$	a	b
a		
b		

Como es posible llenar cada espacio en blanco con el elemento a o b, se concluye que existen $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ o 16 formas de completar la tabla. Así, existen 16 operaciones binarias sobre A.

Propiedades de las operaciones binarias

Varias de las propiedades definidas para las operaciones binarias en la sección 1.6 tienen una importancia particular en este capítulo. Serán vistas de nuevo a continuación.

Una operación binaria sobre un conjunto A es **conmutativa** si

$$a * b = b * a$$

para todos los elementos a y b en A.

Ejemplo 10. La operación binaria de suma en Z (analizada en el ejemplo 1) es conmutativa. ◆

Ejemplo 11. La operación binaria de resta en Z no es conmutativa, pues

$$2 - 3 \neq 3 - 2. \qquad ◆$$

Una operación binaria descrita por una tabla es conmutativa si y sólo si las entradas de la tabla son simétricas con respecto de la diagonal principal.

Ejemplo 12. ¿Cuáles de las siguientes operaciones binarias sobre $A = \{a, b, c, d\}$ son conmutativas?

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

(a)

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

(b)

Solución: La operación en (a) no es conmutativa, pues $a * b$ es c y $b * a$ es b. La operación en (b) es conmutativa, pues las entradas de la tabla son simétricas con respecto de la diagonal principal. ◆

Una operación binaria * sobre un conjunto A es **asociativa** si

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

para todos los elementos a, b y c en A.

Ejemplo 13. La operación binaria de suma en Z es asociativa. ◆

Ejemplo 14. La operación binaria de resta en Z no es asociativa, pues

$$2 - (3 - 5) \neq (2 - 3) - 5. \qquad ◆$$

Ejemplo 15. Sea L una retícula. La operación binaria definida como $a * b = a \wedge b$ (véase el ejemplo 8) es conmutativa y asociativa. También satisface la propiedad **idempotente** $a \wedge a = a$. También es cierto un recíproco parcial, como muestra el ejemplo 16. ◆

Ejemplo 16. Sea * una operación binaria sobre un conjunto A y supóngase que * satisface las siguientes propiedades para cualesquiera a, b, c en A.

1. $a = a * a$ Propiedad idempotente
2. $a * b = b * a$ Propiedad conmutativa

3. $a * (b * c) = (a * b) * c$ Propiedad asociativa

Se define una relación $\leq$ sobre A como

$$a \leq b \quad \text{si y sólo si } a = a * b.$$

Muestre que $(A, \leq)$ es un conjunto parcialmente ordenado, y que para toda a, b en A, GLB$(a, b) = a * b$.

Solución: Se debe mostrar que $\leq$ es reflexiva, antisimétrica y transitiva. Como $a = a * a$, entonces $a \leq a$ para toda a en A, y $\leq$ es reflexiva.

Ahora, supóngase que $a \leq b$ y $b \leq a$. Entonces, por definición y por la propiedad 2, $a = a * b = b * a = b$, de modo que $a = b$. Por lo tanto, $\leq$ es antisimétrica.

Si $a \leq b$ y $b \leq c$, entonces $a = a * b = a * (b * c) = (a * b) * c = a * c$, de modo que $a \leq c$ y $\leq$ es transitiva.

Por último, se debe mostrar que para toda a y b en A, $a * b = a \wedge b$ (la máxima cota inferior de a y b con respecto de $\leq$). Se tiene que $a * b = a * (b * b) = (a * b) * b$, de modo que $a * b \leq b$. De manera análoga, se puede mostrar que $a * b \leq b$, por lo cual $a * b$ es una cota inferior para a y b. Ahora, si $c \leq a$ y $c \leq b$, entonces $c = c * a$ y $c = c * b$ por definición. Así, $c = (c * a) * b = c * (a * b)$, de modo que $c \leq a * b$. Esto muestra que $a * b$ es la máxima cota inferior de a y b. ◆

GRUPO DE EJERCICIOS 9.1

En los ejercicios 1 *al* 8, *determine si la descripción de * es una descripción válida de una operación binaria sobre el conjunto.*

1. En $\mathbb{R}$, donde $a * b$ es ab (la multiplicación ordinaria).
2. En Z^+, donde $a * b$ es a/b.
3. En Z, donde $a * b$ es a^b.
4. En Z^+, donde $a * b$ es a^b.
5. En Z^+, donde $a * b$ es $a - b$.
6. En $\mathbb{R}$, donde $a * b$ es $a\sqrt{b}$.
7. En $\mathbb{R}$, donde $a * b$ es el máximo número racional menor que ab.
8. En Z, donde $a * b$ es $2a + b$.

En los ejercicios 9 *al* 17, *determine si la operación binaria * es conmutativa y si es asociativa sobre el conjunto.*

9. En Z^+, donde $a * b$ es $a + b + 2$.
10. En Z, donde $a * b$ es ab.
11. En $\mathbb{R}$, donde $a * b$ es $a \times |b|$.
12. En el conjunto de números reales distintos de cero, donde $a * b$ es a/b.
13. En $\mathbb{R}$, donde $a * b$ es el mínimo de a y b.
14. En el conjunto de todas las matrices booleanas $n \times n$, donde $\mathbf{A} * \mathbf{B}$ es $\mathbf{A} \odot \mathbf{B}$ (véase la sección 1.5).
15. En $\mathbb{R}$, donde $a * b$ es $ab/3$.
16. En $\mathbb{R}$, donde $a * b$ es $ab + 2b$.
17. En una retícula A, donde $a * b$ es $a \vee b$.
18. Complete la siguiente tabla de modo que la operación binaria * sea conmutativa.

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

19. Considere la operación binaria * definida sobre el conjunto $A = \{a, b, c, d\}$ mediante la tabla siguiente.

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

Calcule
(a) $c * d$ y $d * c$.
(b) $b * d$ y $d * b$.
(c) $a * (b * c)$ y $(a * b) * c$.
(d) ¿Es * conmutativa? ¿Es asociativa?

En los ejercicios 20 *y* 21, *complete la tabla dada de modo que la operación binaria * sea asociativa.*

20.

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

21.

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

22. Sea A un conjunto con n elementos.
(a) ¿Cuántas operaciones binarias pueden ser definidas sobre A?
(b) ¿Cuántas operaciones binarias conmutativas pueden ser definidas sobre A?

23. Sea $A = \{a, b\}$.
(a) Cree una tabla para cada una de las 16 operaciones binarias que pueden definirse sobre A.
(b) Utilice la parte (a) para identificar las operaciones binarias sobre A que sean conmutativas.
(c) Utilice la parte (a) para identificar las operaciones binarias sobre A que sean asociativas.
(d) Utilice la parte (a) para identificar las operaciones binarias sobre A que satisfagan la propiedad idempotente.

24. Sea * una operación binaria sobre un conjunto A, suponiendo que * satisface las propiedades idempotente, conmutativa y asociativa, como se analizó en el ejemplo 16. Defina una relación $\leq$ sobre A como $a \leq b$ si y sólo si $b = a * b$. Muestre que $(A, \leq)$ es un conjunto parcialmente ordenado y que, para toda a y b, LUB$(a, b) = a * b$.

25. Describa la forma en que difiere la definición de una operación binaria sobre un conjunto A de la definición de una operación binaria dada en la sección 1.6. Explique también si una operación binaria sobre un conjunto es o no una operación binaria, según la definición anterior.

9.2. Semigrupos

En esta sección se define un sistema matemático sencillo, que consta de un conjunto y una operación binaria, y que tiene muchas aplicaciones importantes.

Un **semigrupo** es un conjunto no vacío S junto con una operación binaria asociativa * definida en S. Se denotará el semigrupo como $(S, *)$, o bien, si queda claro cuál es la operación *, sólo como S. También se hará referencia a $a * b$ como el **producto** de a y b. El semigrupo $(S, *)$ es conmutativo si * es una operación conmutativa.

Ejemplo 1. La sección 9.1 implica que $(Z, +)$ es un semigrupo conmutativo. ◆

Ejemplo 2. El conjunto $P(S)$, donde S es un conjunto, junto con la operación de unión es un semigrupo conmutativo. ◆

Ejemplo 3. El conjunto Z con la operación binaria de resta no es un semigrupo, pues la resta no es asociativa. ◆

Ejemplo 4. Sea S un conjunto fijo no vacío, y sea S^S el conjunto de todas las funciones $f: S \to S$. Si f y g son elementos de S^S, se define $f * g$ como $f \circ g$, la composición. Entonces * es una operación binaria sobre S^S, y la sección 4.7 implica que * es asociativa. Por lo tanto, $(S^S, *)$ es un semigrupo. El semigrupo S^S no es conmutativo. ◆

Ejemplo 5. Sea $(L, \leq)$ una retícula. Se define una operación binaria en L como $a * b = a \vee b$. Entonces L es un semigrupo. ◆

Ejemplo 6. Sea $A = \{a_1, a_2, \ldots, a_n\}$ un conjunto no vacío. Recuérdese según lo visto en la sección 1.3 que A^* es el conjunto de todas las secuencias finitas de elementos de A. Es decir, A^* consta de todas las palabras que es posible formar con el alfabeto A. Sean α y β elementos de A^*. Observe que la concatenación es una operación binaria $\cdot$ sobre A^*. Recuérdese que si $\alpha = a_1a_2 \cdots a_n$ y $\beta = b_1b_2 \cdots b_k$, entonces $\alpha \cdot \beta = a_1a_2 \cdots a_nb_1b_2 \cdots b_k$. Es fácil ver que si α, β y γ son elementos de A^*, entonces

$$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

de modo que $\cdot$ es una operación binaria asociativa y $(A^*, \cdot)$ es un semigrupo, llamado **semigrupo libre generado por** A. ◆

En un semigrupo $(S, *)$ puede establecerse la siguiente generalización de la propiedad asociativa; se omitirá la demostración.

Teorema 1. *Si $a_1, a_2, \ldots, a_n$, $n \geq 3$, son elementos arbitrarios de un semigrupo, entonces todos los productos de los elementos $a_1, a_2, \ldots, a_n$ que puede formarse insertando paréntesis con sentido de manera arbitraria son iguales.* ●

Si $a_1, a_2, \ldots, a_n$ son elementos en un semigrupo $(S, *)$, se escribirá su producto como

$$a_1 * a_2 * \cdots * a_n,$$

sin escribir los paréntesis.

Ejemplo 7. El teorema 1 muestra que los productos

$$((a_1 * a_2) * a_3) * a_4, \qquad a_1 * (a_2 * (a_3 * a_4)), \qquad (a_1 * (a_2 * a_3)) * a_4$$

son todos iguales. ◆

Un elemento e de un semigrupo $(S, *)$ es un elemento **identidad** si

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

para toda $a \in S$. Como muestra el teorema 1 de la sección 1.6, un elemento identidad debe ser único.

Ejemplo 8. El número 0 es una identidad en el semigrupo $(Z, +)$. ◆

Ejemplo 9. El semigrupo $(Z^+, +)$ no tiene elemento identidad. ◆

Un **monoide** es un semigrupo $(S, *)$ que tiene una identidad.

Ejemplo 10. El semigrupo $P(S)$ definido en el ejemplo 2, tiene la identidad $\varnothing$, pues

$$\varnothing * A = \varnothing \cup A = A = A \cup \varnothing = A * \varnothing$$

para cualquier elemento $A \in P(S)$. Por lo tanto, $P(S)$ es un monoide. ♦

Ejemplo 11. El semigrupo S^S definido en el ejemplo 4 tiene la identidad 1_S, pues

$$1_S * f = 1_S \circ f = f = f \circ 1_S = f * 1_S$$

para cualquier elemento $f \in S^S$, por lo tanto S^S es un monoide. ♦

Ejemplo 12. El semigrupo A^* definido en el ejemplo 6 es en realidad un monoide con identidad Λ, la secuencia vacía, pues $\alpha \cdot \Lambda = \Lambda \cdot \alpha = \alpha$ para toda $\alpha \in A^*$. ♦

Ejemplo 13. El conjunto de todas las relaciones sobre un conjunto A es un monoide bajo la operación de composición. El elemento identidad es la relación de igualdad Δ (véase la sección 4.7). ♦

Sea $(S, *)$ un semigrupo y T un subconjunto de S. Si T es cerrado bajo la operación $*$ (es decir, $a * b \in T$ siempre que a y b sean elementos de T), entonces $(T, *)$ es un **subsemigrupo** de $(S, *)$. De manera análoga, sea $(S, *)$ un monoide con identidad e, y sea T un subconjunto no vacío de S. Si T es cerrado bajo la operación $*$ y $e \in T$, entonces $(T, *)$ es un **submonoide** de $(S, *)$.

Observe que la propiedad asociativa es válida en cualquier subconjunto de un semigrupo, de modo que un subsemigrupo $(T, *)$ de un semigrupo $(S, *)$ es en sí un semigrupo. De manera análoga, un submonoide de un monoide es a su vez un monoide.

Ejemplo 14. Si $(S, *)$ es un semigrupo, entonces $(S, *)$ es un subsemigrupo de $(S, *)$. De manera similar, sea $(S, *)$ un monoide. Entonces $(S, *)$ es un submonoide de $(S, *)$ y si $T = \{e\}$, entonces $(T, *)$ es también un submonoide de $(S, *)$. ♦

Supóngase que $(S, *)$ es un semigrupo y que $a \in S$. Para $n \in Z^+$, se define las potencias de a^n de manera recursiva, de la siguiente manera:

$$a^1 = a, \qquad a^n = a^{n-1} * a, \qquad n \geq 2.$$

Además, si $(S, *)$ es un monoide, también se define

$$a^0 = e.$$

Se puede demostrar que si m y n son enteros no negativos, entonces

$$a^m * a^n = a^{m+n}.$$

Ejemplo 15

(a) Si $(S, *)$ es un semigrupo, $a \in S$ y

$$T = \{a^i \mid i \in Z^+\},$$

entonces $(T, *)$ es un subsemigrupo de $(S, *)$.

(b) Si $(S, *)$ es un monoide, $a \in S$ y

$$T = \{a^i \mid i \in Z^+ \text{ o } i = 0\},$$

entonces $(T, *)$ es un submonoide de $(S, *)$. ♦

Ejemplo 16. Si T es el conjunto de los enteros pares, entonces $(T, \times)$ es un subsemigrupo del monoide $(Z, \times)$, donde $\times$ es la multiplicación ordinaria, pero no es un submonoide, pues la identidad de Z, el número 1, no pertenece a T. ♦

Isomorfismo y homomorfismo

En la sección 7.1 se define un isomorfismo entre dos conjuntos parcialmente ordenados como una correspondencia biunívoca que preserva las relaciones de orden, que son la característica distintiva de los conjuntos parcialmente ordenados. Ahora se define un isomorfismo entre dos semigrupos que preserve las operaciones binarias. En general, un isomorfismo entre dos estructuras matemáticas del mismo tipo debe preservar las características distintivas de las estructuras.

Sean $(S, *)$ y $(T, *')$ dos semigrupos. Una función $f: S \to T$ es un **isomorfismo** de $(S, *)$ en $(T, *')$ si es una correspondencia biunívoca de S a T, y si

$$f(a * b) = f(a) *' f(b)$$

para toda a y b en S.

Si f es un isomorfismo de $(S, *)$ en $(T, *')$, entonces, como f es una correspondencia biunívoca, el teorema 1 de la sección 5.1 implica que f^{-1} existe y es una correspondencia biunívoca de T a S. Ahora se mostrará que f^{-1} es un isomorfismo de $(T, *')$ en $(S, *)$. Sean a' y b' elementos cualesquiera de T. Como f es sobre, es posible encontrar elementos a y b en S tales que $f(a) = a'$ y $f(b) = b'$. Entonces, $a = f^{-1}(a')$ y $b = f^{-1}(b')$. Ahora,

$$\begin{aligned} f^{-1}(a' *' b') &= f^{-1}(f(a) *' f(b)) \\ &= f^{-1}(f(a * b)) \\ &= (f^{-1} \circ f)(a * b) \\ &= a * b = f^{-1}(a') * f^{-1}(b'). \end{aligned}$$

Por lo tanto, f^{-1} es un isomorfismo.

Sólo se dirá que los semigrupos $(S, *)$ y $(T, *')$ son **isomorfos** y se escribe $S \simeq T$.

Para mostrar que los semigrupos $(S, *)$ y $(T, *')$ son isomorfos, se debe utilizar el siguiente procedimiento:

PASO 1. Se define una función $f: S \to T$ con $\mathrm{Dom}(f) = S$.

PASO 2. Se muestra que f es biunívoca.

PASO 3. Se muestra que f es sobre.

PASO 4. Se muestra que $f(a * b) = f(a) *' f(b)$.

Ejemplo 17. Sea T el conjunto de todos los enteros pares. Muestre que los semigrupos $(Z, +)$ y $(T, +)$ son isomorfos.

Solución

PASO 1. Se define la función $f: Z \to T$ como $f(a) = 2a$.

PASO 2. Ahora se mostrará que f es biunívoca, de la siguiente manera. Supóngase que $f(a_1) = f(a_2)$. Entonces $2a_1 = 2a_2$, de modo que $a_1 = a_2$. Por lo tanto, f es biunívoca.

PASO 3. A continuación se mostrará que f es sobre. Supóngase que b es un entero par. Entonces $a = b/2 \in Z$ y

$$f(a) = f(b/2) = 2(b/2) = b,$$

de modo que f es sobre.

PASO 4. Se tiene

$$\begin{aligned} f(a+b) &= 2(a+b) \\ &= 2a + 2b = f(a) + f(b). \end{aligned}$$

Por lo tanto, $(Z, +)$ y $(T, +)$ son semigrupos isomorfos. ◆

En general, resulta casi directo verificar que una función dada $f: S \to T$ es o no un isomorfismo. Sin embargo, por lo general es difícil mostrar que dos semigrupos son isomorfos, dado que se debe crear el isomorfismo f.

Como en el caso de los isomorfismos de conjuntos parcialmente ordenados o de retículas, cuando dos semigrupos $(S, *)$ y $(T, *')$ son isomorfos, sólo pueden diferir por la naturaleza de sus elementos; sus estructuras como semigrupos son idénticas. Si S y T son semigrupos finitos, sus operaciones binarias respectivas pueden darse mediante tablas. Entonces S y T son isomorfos si es posible reordenar y re-etiquetar los elementos de S de modo que su tabla coincida con la de T.

Ejemplo 18. Sean $S = \{a, b, c\}$ y $T = \{x, y, z\}$. Es fácil verificar que las siguientes tablas de operaciones dan estructura de semigrupo a S y T, respectivamente.

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

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

Sea

$$\begin{aligned} f(a) &= y \\ f(b) &= x \\ f(c) &= z. \end{aligned}$$

Al reemplazar los elementos en S por sus imágenes y reordenar la tabla, se obtiene, precisamente, la tabla para T. Así, S y T son isomorfos. ◆

Teorema 2. *Sean $(S, *)$ y $(T, *')$ monoides con identidades e y e', respectivamente. Sea $f: S \to T$ un isomorfismo. Entonces $f(e) = e'$.*

Demostración: Sea b cualquier elemento de T. Como f es sobre, existe un elemento a en S tal que $f(a) = b$. Entonces

$$\begin{aligned} a &= a * e \\ b = f(a) &= f(a * e) = f(a) *' f(e) \\ &= b *' f(e). \end{aligned}$$

De manera análoga, como $a = e * a$, $b = f(e) *' b$. Así, para cualquier $b \in T$,

$$b = b *' f(e) = f(e) *' b.$$

lo que significa que $f(e)$ es una identidad para T. Esto implica que $f(e) = e'$. ●

Si $(S, *)$ y $(T, *')$ son semigrupos tales que S tiene una identidad y T no, el teorema 2 implica que $(S, *)$ y $(T, *')$ no pueden ser isomorfos.

Ejemplo 19. Sea T el conjunto de los enteros pares y $\times$ la multiplicación ordinaria. Entonces los semigrupos $(Z, \times)$ y $(T, \times)$ no son isomorfos, pues Z tiene una identidad y T no. ◆

Si se elimina las condiciones de ser biunívoca y sobre en la definición de un isomorfismo de dos semigrupos, se obtiene otro método importante para comparar las estructuras algebraicas de los dos semigrupos.

Sean $(S, *)$ y $(T, *')$ dos semigrupos. Una función definida para todo punto $f: S \to T$ es un **homomorfismo** de $(S, *)$ en $(T, *')$ si

$$f(a * b) = f(a) *' f(b)$$

para toda a y b en S. Además, si f es sobre T es una **imagen homomorfa** de S.

Ejemplo 20. Sea $A = \{0, 1\}$ y considérese los semigrupos $(A^*, \cdot)$ y $(A, +)$, donde $\cdot$ es la operación de concatenación y + se define mediante la tabla

+	0	1
0	0	1
1	1	0

Se define la función $f: A^* \to A$ como

$$f(\alpha) = \begin{cases} 1 & \text{si } \alpha \text{ tiene un número impar de unos} \\ 0 & \text{si } \alpha \text{ tiene un número par de unos.} \end{cases}$$

Es fácil verificar que si α y β son elementos arbitrarios de A^*, entonces

$$f(\alpha \cdot \beta) = f(\alpha) + f(\beta).$$

Así, f es un homomorfismo. La función f es sobre, pues

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \end{aligned}$$

pero f no es un isomorfismo, pues no es biunívoca. ◆

La diferencia entre un isomorfismo y un homomorfismo es que un isomorfismo debe ser biunívoca y sobre. Para un isomorfismo y un homomorfismo, la imagen de un producto debe ser el producto de las imágenes.

La demostración del siguiente teorema, que se deja como ejercicio para el lector, es completamente análoga a la demostración del teorema 2.

Teorema 3. *Sean $(S, *)$ y $(T, *')$ monoides con identidades e y e', respectivamente. Sea $f: S \to T$ un homomorfismo de $(S, *)$ sobre $(T, *')$. Entonces $f(e) = e'$.* ●

El teorema 3, junto con los dos teoremas siguientes, muestra que, si un semigrupo $(T, *')$ es una imagen homomorfa del semigrupo $(S, *)$, entonces $(T, *')$ tiene una gran semejanza algebraica con $(S, *)$.

Teorema 4. *Sea f un homomorfismo de un semigrupo $(S, *)$ al semigrupo $(T, *')$. Si S' es un subsemigrupo de $(S, *)$, entonces*

$$f(S') = \{t \in T \mid t = f(s) \text{ para algún } s \in S'\},$$

la imagen de S' bajo f, es un subsemigrupo de $(T, *')$.

Demostración: Si t_1 y t_2 son elementos arbitrarios de $f(S')$, entonces existen s_1 y s_2 en S' tales que

$$t_1 = f(s_1) \quad \text{y} \quad t_2 = f(s_2).$$

Entonces

$$\begin{aligned} t_1 *' t_2 &= f(s_1) *' f(s_2) \\ &= f(s_1 * s_2) \\ &= f(s_3), \end{aligned}$$

donde $s_3 = s_1 * s_2 \in S'$. Por lo tanto, $t_1 *' t_2 \in f(S')$.

Así, $f(S')$ es cerrado bajo la operación $*'$. Como la propiedad asociativa es válida en $f(S')$, se tiene que $f(S')$ es un subsemigrupo de $(T, *')$. ●

Teorema 5. *Si f es un homomorfismo de un semigrupo conmutativo $(S, *)$ sobre un semigrupo $(T, *')$, entonces $(T, *')$ también es conmutativo.*

Demostración: Sean t_1 y t_2 elementos de T. Entonces existen s_1 y s_2 en S tales que

$$t_1 = f(s_1) \quad \text{y} \quad t_2 = f(s_2).$$

Por consiguiente,

$$\begin{aligned} t_1 *' t_2 &= f(s_1) *' f(s_2) \\ &= f(s_1 * s_2) \\ &= f(s_2 * s_1) \\ &= f(s_2) *' f(s_1) \\ &= t_2 *' t_1. \end{aligned}$$

Por lo tanto, $(T, *')$ también es conmutativo. ●

GRUPO DE EJERCICIOS 9.2

1. Sea $A = \{a, b\}$. ¿Cuáles de las tablas siguientes definen un semigrupo en A? ¿Cuáles definen un monoide en A?

*	a	b
a	a	b
b	a	a

(a)

*	a	b
a	a	b
b	b	b

(b)

*	a	b
a	b	a
b	a	b

(c)

*	a	b
a	a	b
b	b	a

(d)

*	a	b
a	a	a
b	b	b

(e)

*	a	b
a	b	b
b	a	a

(f)

En los ejercicios 2 al 12, determine si el conjunto junto con la operación binaria es un semigrupo, un monoide o ninguno de los dos. Si es un monoide, especifique la identidad. Si es un semigrupo o un monoide, determine si es conmutativo.

2. Z^+, donde $*$ se define como la multiplicación ordinaria.

3. Z^+, donde $a * b$ se define como máx$\{a, b\}$.

4. Z^+, donde $a * b$ se define como MCD$\{a, b\}$.

5. Z^+, donde $a * b$ se define como a.

6. Los números reales distintos de cero, donde $*$ es la multiplicación ordinaria.

7. $P(S)$, con S un conjunto, donde $*$ se define como la intersección.

8. Un álgebra booleana B, donde $a * b$ se define como $a \wedge b$.

9. $S = \{1, 2, 3, 6, 12\}$, donde $a * b$ se define como MCD(a, b).

10. $S = \{1, 2, 3, 6, 9, 18\}$, donde $a * b$ se define como MCM(a, b).

11. Z, donde $a * b = a + b - ab$.

12. Los enteros pares, donde $a * b$ se define como $\dfrac{ab}{2}$.

13. ¿Cuáles de las tablas siguientes definen un semigrupo?

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

(a)

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

(b)

14. Complete la tabla siguiente para obtener un semigrupo.

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

15. Sea $S = \{a, b\}$. Escriba la tabla de operación para el semigrupo S^S. ¿Es conmutativo el semigrupo?

16. Sea $S = \{a, b\}$. Escriba la tabla de operación para el semigrupo $(P(S), \cup)$.

17. Sea $A = \{a, b, c\}$ y considérese el semigrupo $(A^*, \cdot)$, donde $\cdot$ es la operación de concatenación. Si $\alpha = abac$, $\beta = cba$ y $\gamma = babc$, calcule (a) $(\alpha \cdot \beta) \cdot \gamma$ (b) $\gamma \cdot (\alpha \cdot \alpha)$ (c) $(\gamma \cdot \beta) \cdot \alpha$.

18. Demuestre que la intersección de dos subsemigrupos de un semigrupo $(S, *)$ es un subsemigrupo de $(S, *)$.

19. Demuestre que la intersección de dos submonoides de un monoide $(S, *)$ es un submonoide de $(S, *)$.

20. Sea $A = \{0, 1\}$ y considérese el semigrupo $(A^*, \cdot)$, donde $\cdot$ es la operación de concatenación. Sea T el subconjunto de A^* que consta de todas las sucesiones con un número impar de unos. ¿Es $(T, \cdot)$ un subsemigrupo de $(A, \cdot)$?

21. Sea $A = \{a, b\}$. ¿Existen dos semigrupos $(A, *)$ y $(A, *')$ que no sean isomorfos?

22. Un elemento x en un monoide es **idempotente** si $x^2 = x * x = x$. Muestre que el conjunto de todos los elementos idempotentes en un monoide conmutativo S es un submonoide de S.

23. Sean $(S_1, *_1)$, $(S_2, *_2)$ y $(S_3, *_3)$ semigrupos y $f: S_1 \to S_2$ y $g: S_2 \to S_3$ homomorfismos. Demuestre que $g \circ f$ es un homomorfismo de S_1 a S_3.

24. Sean $(S_1, *)$, $(S_2, *')$ y $(S_3, *'')$ semigrupos y $f: S_1 \to S_2$ y $g: S_2 \to S_3$ isomorfismos. Demuestre que $g \circ f$ es un isomorfismo de S_1 a S_3.

25. Sea R^+ el conjunto de los números reales positivos. Muestre que la función $f: R^+ \to R$ definida por $f(x) = \ln x$ es un isomorfismo del semigrupo $(R^+, \times)$ con el semigrupo $(R, +)$, donde $\times$ y $+$ son la multiplicación y la suma ordinarias, respectivamente.

9.3. Semigrupos productos y cocientes

En esta sección se obtendrán nuevos semigrupos a partir de semigrupos existentes.

Teorema 1. *Si $(S, *)$ y $(T, *')$ son semigrupos, entonces $(S \times T, *'')$ es un semigrupo, donde $*''$ se define como $(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$.*

Demostración: Se deja como ejercicio. ●

El teorema 1 implica de inmediato que si S y T son monoides con identidades e_S y e_T, respectivamente, entonces $S \times T$ es un monoide con identidad (e_S, e_T).

Ahora se analizará las relaciones de equivalencia en un semigrupo $(S, *)$. Como un semigrupo no es simplemente un conjunto, ciertas relaciones de equivalencia en un semigrupo proporcionan información adicional acerca de la estructura del semigrupo.

Una relación de equivalencia R sobre el semigrupo $(S, *)$ es una **relación de congruencia** si

$$a\,R\,a' \quad \text{y} \quad b\,R\,b' \quad \text{implican que} \quad (a * b)\,R\,(a' * b').$$

Ejemplo 1. Considérese el semigrupo $(Z, +)$ y la relación de equivalencia R en Z definida por

$$a\,R\,b \quad \text{si y sólo si} \quad a \equiv b \pmod 2.$$

Recuérdese que esta relación de equivalencia fue analizada en la sección 4.5. Observe que si a y b proporcionan el mismo residuo al dividirse entre 2, entonces $2 \mid (a - b)$. Ahora se mostrará que ésta es una relación de congruencia, de la siguiente manera.

Si

$$a \equiv b \pmod 2 \quad \text{y} \quad c \equiv d \pmod 2,$$

entonces 2 divide a $a - b$ y 2 divide a $c - d$, de modo que

$$a - b = 2m \quad \text{y} \quad c - d = 2n,$$

donde m y n están en Z. Al sumar, se obtiene

$$(a - b) + (c - d) = 2m + 2n$$

o

$$(a + c) - (b + d) = 2(m + n),$$

de modo que

$$a + c \equiv b + d \pmod 2.$$

Por lo tanto, ésta es una relación de congruencia. ◆

Ejemplo 2. Sea $A = \{0, 1\}$ y considérese el semigrupo libre $(A^*, \cdot)$ generado por A. Se define la siguiente relación sobre A:

$$\alpha\,R\,\beta \quad \text{si y sólo si} \quad \alpha \text{ y } \beta \text{ tienen el mismo número de unos.}$$

Muestre que R es una relación de congruencia en $(A^*, \cdot)$.

Solución: Primero se mostrará que R es una relación de equivalencia. Se tiene que

1. $\alpha\,R\,\alpha$ para toda $\alpha \in A^*$.
2. Si $\alpha\,R\,\beta$, entonces α y β tienen el mismo número de unos, de modo que $\beta\,R\,\alpha$.
3. Si $\alpha\,R\,\beta$ y $\beta\,R\,\gamma$, entonces α y β tienen el mismo número de unos y β y γ tienen el mismo número de unos, de modo que α y γ tienen el mismo número de unos. Por lo tanto, $\alpha\,R\,\gamma$.

A continuación se mostrará que R es una relación de congruencia. Supóngase que $\alpha\,R\,\alpha'$ y $\beta\,R\,\beta'$. Entonces α y α' tienen el mismo número de unos y β y β' tienen el mismo número de unos. Como el número de unos en $\alpha \cdot \beta$ es la suma de los números de unos en α y en β, se concluye que el número de unos en $\alpha \cdot \beta$ es igual al número de unos en $\alpha' \cdot \beta'$. Por lo tanto,

$$(\alpha \cdot \beta)\,R\,(\alpha' \cdot \beta')$$

y entonces R es una relación de congruencia. ◆

Ejemplo 3. Considérese el semigrupo $(Z, +)$, donde $+$ es la suma ordinaria. Sea $f(x) = x^2 - x - 2$. Ahora se definirá la siguiente relación sobre Z:

$$a\,R\,b \quad \text{si y sólo si} \quad f(a) = f(b).$$

Se verifica de manera directa que R es una relación de equivalencia sobre Z. Sin embargo, R no es una relación de congruencia, pues se tiene

$$-1\,R\,2 \qquad (f(-1) = f(2) = 0)$$

y

$$-2\,R\,3 \qquad (f(-2) = f(3) = 4)$$

pero

$$-3 \not R\, 5,$$

ya que $f(-3) = 10$ y $f(5) = 18$. ◆

Recuerde de la sección 4.5 que una relación de equivalencia R sobre el semigrupo $(S, *)$ determina una partición de S. Sean $[a] = R(a)$ la clase de equivalencia que contiene a a y S/R el conjunto de todas las clases de equivalencia. La notación $[a]$ es más tradicional en este contexto y produce cálculos menos confusos.

Teorema 2. *Sea R una relación de congruencia sobre el semigrupo $(S, *)$. Considérese la relación $\circledast$ de $S/R \times S/R$ a S/R en la que la pareja ordenada $([a], [b])$ se relaciona con $[a * b]$, donde a y b están en S.*

(a) *$\circledast$ es una función de $S/R \times S/R$ en S/R, y como es usual, denotamos $\circledast([a], [b])$ por $[a] \circledast [b]$. Así, $[a] \circledast [b] = [a * b]$.*
(b) *$(S/R, \circledast)$ es un semigrupo.*

Demostración: Supóngase que $([a], [b]) = ([a'], [b'])$. Entonces $a\,R\,a'$ y $b\,R\,b'$, de modo que debe tenerse $a * b\,R\,a' * b'$, ya que R es una relación de congruencia. Así, $[a * b] = [a' * b']$; es decir, $\circledast$ es una función. Esto significa que $\circledast$ es una operación binaria sobre S/R.

A continuación, se debe verificar si ⊛ es una operación asociativa. Se tiene que

$$\begin{aligned}[a] \circledast ([b] \circledast [c]) &= [a] \circledast [b * c]\\ &= [a * (b * c)]\\ &= [(a * b) * c] \quad \text{por la propiedad asociativa de } * \text{ en } S\\ &= [a * b] \circledast [c]\\ &= ([a] \circledast [b]) \circledast [c]\end{aligned}$$

Por lo tanto, S/R es un semigrupo, llamado **semigrupo cociente** o **semigrupo factor**. Observe que ⊛ es un tipo de "relación binaria cociente" sobre S/R que se construye a partir de la relación binaria original $*$ en S mediante la relación de congruencia R. ●

Corolario 1. *Sea R una relación de congruencia sobre el monoide $(S, *)$. Si se define la operación ⊛ en S/R como $[a] \circledast [b] = [a * b]$, entonces $(S/R, \circledast)$ es un monoide.*

Demostración: Si e es la identidad en $(S, *)$, entonces es fácil verificar que $[e]$ es la identidad en $(S/R, \circledast)$. ●

Ejemplo 4. Considérese la situación del ejemplo 2. Como R es una relación de congruencia sobre el monoide $S = (A^*, \cdot)$, se concluye que $(S/R, \odot)$ es un monoide, donde

$$[\alpha] \odot [\beta] = [\alpha \cdot \beta].$$ ♦

Ejemplo 5. Como ya se señaló en la sección 4.5, se puede repetir el ejemplo 4 de esa sección con el entero positivo n en vez de 2. Es decir, se define la siguiente relación sobre el semigrupo $(Z, +)$:

$$a\,R\,b \quad \text{si y sólo si} \quad a \equiv b \pmod{n}.$$

Con el mismo método utilizado en el ejemplo 4 de la sección 4.5, se puede mostrar que R es una relación de equivalencia y que, como en el caso de $n = 2$, $a \equiv b$ (mód n) implica que $n \mid (a - b)$. Así, si n es 4, entonces

$$2 \equiv 6 \quad (\text{mód } 4)$$

y 4 divide a $(2 - 6)$. También quedará como ejercicio para el lector mostrar que $\equiv$ (mód n) es una relación de congruencia en Z.

Ahora, sea $n = 4$ y calcule las clases de equivalencia determinadas por la relación de congruencia $\equiv$ (mód 4) sobre Z. Se obtiene

$$\begin{aligned}[0] &= \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\} = [4] = [8] = \cdots\\ [1] &= \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\} = [5] = [9] = \cdots\\ [2] &= \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\} = [6] = [10] = \cdots\\ [3] &= \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\} = [7] = [11] = \cdots\end{aligned}$$

Éstas son todas las clases de equivalencia distintas que forman el conjunto cociente $Z/\equiv$ (mód 4). Se acostumbra denotar el conjunto cociente $Z/\equiv$ (mód n) por Z_n; Z_n es un monoide con operación ⊕ e identidad [0]. Ahora se determinará la tabla de sumar para el semigrupo Z_4 con operación ⊕.

⊕	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Se obtienen las entradas de esta tabla de

$$[a] \oplus [b] = [a + b].$$

Así,

$$\begin{aligned}[1] \oplus [2] &= [1 + 2] = [3]\\ [1] \oplus [3] &= [1 + 3] = [4] = [0]\\ [2] \oplus [3] &= [2 + 3] = [5] = [1]\\ [3] \oplus [3] &= [3 + 3] = [6] = [2].\end{aligned}$$

Se puede mostrar que Z_n tiene las n clases de equivalencia

$$[0], [1], [2], \ldots, [n - 1]$$

y que

$$[a] \oplus [b] = [r],$$

donde r es el residuo obtenido al dividir $a + b$ entre n. Así, si n es 6,

$$\begin{aligned}[2] \oplus [3] &= [5]\\ [3] \oplus [5] &= [2]\\ [3] \oplus [3] &= [0].\end{aligned}$$ ♦

Ahora se examinará la conexión entre la estructura de un semigrupo $(S, *)$ y el semigrupo cociente $(S/R, \circledast)$, donde R es una relación de congruencia en $(S, *)$.

Teorema 3. *Sea R una relación de congruencia sobre un semigrupo $(S, *)$ y $(S/R, \circledast)$ el semigrupo cociente correspondiente. Entonces la función $f_R : S \to S/R$ definida por*

$$f_R(a) = [a]$$

es un homomorfismo sobre, llamado **homomorfismo natural**.

Demostración: Si $[a] \in S/R$, entonces $f_R(a) = [a]$, de modo que f_R es una función sobre. Además, si a y b son elementos de S, entonces

$$\begin{aligned}f_R(a * b) &= [a * b]\\ &= [a] \circledast [b]\\ &= f_R(a) \circledast f_R(b),\end{aligned}$$

de modo que f_R es un homomorfismo. ●

Teorema 4 (teorema fundamental de los homomorfismos). *Sea $f : S \to T$ un homomorfismo del semigrupo $(S, *)$ sobre el semigrupo $(T, *')$. Sea R la relación sobre S definida por*

$a\,R\,b$ si y sólo si $f(a)=f(b)$, para a y b en S. Entonces

(a) *R es una relación de congruencia.*

(b) *$(T, *')$ y el semigrupo cociente $(S/R, \circledast)$ son isomorfos.*

Demostración: (a) Se mostrará que R es una relación de equivalencia. En primer lugar, $a\,R\,a$ para toda $a \in S$, pues $f(a)=f(a)$. Ahora, si $a\,R\,b$, entonces $f(a)=f(b)$, de modo que $b\,R\,a$. Por último, si $a\,R\,b$ y $b\,R\,c$, entonces $f(a)=f(b)$ y $f(b)=f(c)$, de modo que $f(a)=f(c)$ y $a\,R\,c$. Por lo tanto, R es una relación de equivalencia. Ahora, supóngase que $a\,R\,a_1$ y $b\,R\,b_1$. Entonces

$$f(a)=f(a_1) \quad \text{y} \quad f(b)=f(b_1).$$

Al multiplicar en T, se obtiene

$$f(a) *' f(b) = f(a_1) *' f(b_1).$$

Como f es un homomorfismo, esta última ecuación puede volverse a escribir como

$$f(a * b) = f(a_1 * b_1).$$

Por lo tanto,

$$(a * b)\; R\; (a_1 * b_1)$$

y R es una relación de congruencia.

(b) Ahora, considérese la relación $\bar{f}$ de S/R a T definida de la siguiente manera:

$$\bar{f} = \{([a], f(a)) \mid [a] \in S/R\}.$$

Primero se mostrará que $\bar{f}$ es una función. Supóngase que $[a] = [a']$. Entonces $a\,R\,a'$, de modo que $f(a)=f(a')$, lo que implica que $\bar{f}$ es una función. Ahora se puede escribir $\bar{f} : S/R \to T$, donde $\bar{f}([a])=f(a)$ para $[a] \in S/R$.

A continuación se mostrará que $\bar{f}$ es biunívoca. Supóngase que $\bar{f}([a]) = \bar{f}([a'])$. Entonces

$$f(a) = f(a').$$

Así, $a\,R\,a'$, lo que implica que $[a] = [a']$. Por lo tanto, $\bar{f}$ es biunívoca.

Ahora se mostrará que $\bar{f}$ es sobre. Supóngase que $b \in T$. Como f es sobre, $f(a) = b$ para algún elemento a en S. Entonces

$$\bar{f}([a]) = f(a) = b.$$

Así, $\bar{f}$ es sobre.

Por último,

$$\begin{aligned}\bar{f}([a] \circledast [b]) &= \bar{f}([a * b]) \\ &= f(a * b) = f(a) *' f(b) \\ &= \bar{f}([a]) *' \bar{f}([b]).\end{aligned}$$

Por lo tanto, $\bar{f}$ es un isomorfismo. ●

Ejemplo 6. Sea $A = \{0, 1\}$ y considérese el semigrupo libre A^* generado por A bajo la operación de concatenación. Observe que A^* es un monoide, con la cadena vacía Λ como identidad. Sea N el conjunto de enteros no negativos. Entonces N es un semigrupo bajo la operación de suma ordinaria, denotado como $(N, +)$. Se puede verificar fácilmente que

la función $f : A^* \to N$ dada por

$$f(\alpha) = \text{el número de unos en } \alpha$$

es un homomorfismo. Sea R la siguiente relación en A^*:

$$\alpha\,R\,\beta \quad \text{si y sólo si} \quad f(\alpha)=f(\beta).$$

Es decir, $\alpha\,R\,\beta$ si y sólo si α y β tienen la misma cantidad de unos. El teorema 4 implica que $A^*/R \simeq N$ bajo el isomorfismo $\bar{f} : A^*/R \to N$ definido por

$$\bar{f}([\alpha]) = f(\alpha) = \text{el número de unos en } \alpha.$$ ◆

Es posible describir el teorema 4(b) mediante el diagrama de la figura 9.2. En este caso, f_R es el homomorfismo natural. Las definiciones de f_R y $\bar{f}$ implican que

$$\bar{f} \circ f_R = f$$

$$\begin{tikzcd} S \arrow[rr, "f"] \arrow[dr, "f_R"'] & & T \\ & S/R \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Figura 9.2

ya que

$$\begin{aligned}(\bar{f} \circ f_R)(a) &= \bar{f}(f_R(a)) \\ &= \bar{f}([a]) = f(a).\end{aligned}$$

GRUPO DE EJERCICIOS 9.3

1. Sean $(S, *)$ y $(T, *')$ semigrupos conmutativos. Muestre que $S \times T$ (véase el teorema 1) es también un semigrupo conmutativo.

2. Sean $(S, *)$ y $(T, *')$ monoides. Muestre que $S \times T$ es también un monoide. Muestre que la identidad de $S \times T$ es (e_S, e_T).

3. Sean $(S, *)$ y $(T, *')$ semigrupos. Muestre que la función $f : S \times T \to S$ dada por

$$f(s, t) = s$$

es un homomorfismo del semigrupo $S \times T$ sobre el semigrupo S.

4. Sean $(S, *)$ y $(T, *')$ semigrupos. Muestre que $S \times T$ y $T \times S$ son semigrupos isomorfos.

En los ejercicios 5 al 14, determine si la relación R sobre el semigrupo S es una relación de congruencia.

5. $S = Z$ bajo la operación de suma ordinaria; $a\,R\,b$ si y sólo si 2 no divide a $a - b$.

6. $S = Z$ bajo la operación de suma ordinaria; $a\,R\,b$ si y sólo si $a + b$ es par.

7. S = cualquier semigrupo; $a\ R\ b$ si y sólo si $a = b$.

8. S = el conjunto de los números racionales bajo la operación de suma; $a/b\ R\ c/d$ si y sólo si $ad = bc$.

9. S = el conjunto de números racionales bajo la operación de multiplicación; $a/b\ R\ c/d$ si y sólo si $ad = bc$.

10. $S = Z$ bajo la operación de suma ordinaria; $a\ R\ b$ si y sólo si $a \equiv b$ (mód 3).

11. $S = Z$ bajo la operación de suma ordinaria; $a\ R\ b$ si y sólo si a y b son ambos pares o a y b son ambos nones.

12. $S = Z^+$ bajo la operación de multiplicación ordinaria; $a\ R\ b$ si y sólo si $|a - b| \leq 2$.

13. $A = \{0, 1\}$ y $S = A^*$, el semigrupo generado por A bajo la operación de concatenación; $\alpha\ R\ \beta$ si y sólo si ambos tienen un número par de unos o si ambos tienen un número impar de unos.

14. $S = \{0, 1\}$ bajo la operación $*$ definida mediante la tabla

*	0	1
0	0	1
1	1	0

$a\ R\ b$ si y sólo si $a * a = b * b = b$. (*Sugerencia*: Observe que si x es cualquier elemento de S, entonces $x * x = 0$.)

15. Muestre que la intersección de dos relaciones de congruencia sobre un semigrupo es una relación de congruencia.

16. Muestre que la composición de dos relaciones de congruencia sobre un semigrupo no necesariamente es una relación de congruencia.

17. Describa el semigrupo cociente para S y R dado en el ejercicio 9.

18. Considere el semigrupo $S = \{a, b, c, d\}$ con la siguiente tabla de operación.

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

Considere la relación de congruencia $R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, d), (d, c), (d, d)\}$ en S.

(a) Escriba la tabla de operación del semigrupo cociente S/R.

(b) Describa el homomorfismo natural $f_R : S \to S/R$.

19. Considere el monoide $S = \{e, a, b, c\}$ con la siguiente tabla de operación:

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

Considere la relación de congruencia $R = \{(e, e), (e, a), (a, e), (a, a), (b, b), (b, c), (c, b), (c, c)\}$ en S.

(a) Escriba la tabla de operación del monoide cociente S/R.

(b) Describa el homomorfismo natural $f_R : S \to S/R$.

20. Sea $A = \{0, 1\}$ y considérese el semigrupo libre A^* generado por A bajo la operación de concatenación. Sea N el semigrupo de enteros no negativos bajo la operación de suma ordinaria.

(a) Verifique que la función $f : A^* \to N$, definida como $f(\alpha)$ = el número de dígitos en α, es un homomorfismo.

(b) Sea R la siguiente relación en A^*: $\alpha\ R\ \beta$ si y sólo si $f(\alpha) = f(\beta)$. Muestre que R es una relación de congruencia en A^*.

(c) Muestre que A^*/R y N son isomorfos.

9.4. Grupos

En esta sección se analizará un tipo particular de monoide, llamado grupo, que tiene aplicaciones en todas las áreas donde aparece una simetría. Las aplicaciones de los grupos pueden ser encontradas en las matemáticas, la física y la química, así como en áreas menos evidentes como la sociología. Recientemente, han surgido aplicaciones excitantes de la teoría de grupos en campos como la física de partículas y la solución de pasatiempos como el cubo de Rubik. En este libro se presenta una importante aplicación de la teoría de grupos a los códigos binarios, en la sección 11.2.

Un **grupo** $(G, *)$ es un monoide con identidad e con la propiedad adicional de que para cada elemento $a \in G$ existe un elemento $a' \in G$ tal que $a * a' = a' * a = e$. Así, un grupo es un conjunto G junto con una operación binaria $*$ en G tal que

1. $(a * b) * c = a * (b * c)$ para cualquiera de los elementos a, b y c en G.
2. Existe un único elemento e en G tal que

$$a * e = e * a = a \quad \text{para cada } a \in G.$$

3. Para cada $a \in G$, existe un elemento $a' \in G$, llamado **inverso** de a, tal que

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

Observe que si $(G, *)$ es un grupo, entonces $*$ es una operación binaria, de modo que G debe ser cerrado bajo $*$; es decir,

$$a * b \in G \quad \text{para cualesquiera elementos } a \text{ y } b \text{ en } G.$$

Para simplificar la notación, de aquí en adelante, cuando sólo se esté considerando un grupo $(G, *)$ y no haya posibilidad de confusión se escribirá el producto $a * b$ de los elementos a y b en el grupo $(G, *)$ sólo como ab, y también se hará referencia a $(G, *)$ sólo como G.

Un grupo G es **abeliano** si $ab = ba$ para todos los elementos a y b en G.

Ejemplo 1. El conjunto de todos los enteros Z con la operación de suma ordinaria es un grupo abeliano. Si $a \in Z$, entonces un inverso de a es su negativo $-a$. ◆

Ejemplo 2. El conjunto Z^+ bajo la operación de multiplicación ordinaria no es un grupo, pues el elemento 2 en Z^+ no tiene un inverso. Sin embargo, este conjunto, junto con la operación dada, es un monoide. ◆

Ejemplo 3. El conjunto de los números reales distintos de cero bajo la operación de multiplicación ordinaria es un grupo. Un inverso de $a \neq 0$ es $1/a$. ◆

Ejemplo 4. Sea G el conjunto de los números reales distintos de cero y sea

$$a * b = \frac{ab}{2}.$$

Muestre que $(G, *)$ es un grupo abeliano.

Solución: Primero se verifica que * es una operación binaria. Si a y b son elementos de G, entonces $ab/2$ es un número real distinto de cero y que por tanto pertenece a G. A continuación se verifica la asociatividad. Como

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

y

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{(ab)c}{4},$$

la operación * es asociativa.

El número 2 es la identidad en G, ya que si $a \in G$, entonces

$$a * 2 = \frac{(a)(2)}{2} = a = \frac{(2)(a)}{2} = 2 * a.$$

Por último, si $a \in G$, entonces $a' = 4/a$ es un inverso de a, ya que

$$a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)(a)}{2} = \frac{4}{a} * a = a' * a.$$

Como $a * b = b * a$ para toda a y b en G, se concluye que G es un grupo abeliano. ◆

Antes de presentar más ejemplos de grupos, se desarrollarán varias propiedades importantes satisfechas en cualquier grupo G.

Teorema 1. *Sea G un grupo. Cada elemento a en G tiene un único inverso en G.*

Demostración: Sean a' y a'' inversos de a. Entonces

$$a'(aa'') = a'e = a'$$

y

$$(a'a)a'' = ea'' = a''.$$

Por lo tanto, por la asociatividad,

$$a' = a''.$$ ●

De aquí en adelante, se denotará el inverso de a por a^{-1}. Así, en un grupo G se tiene que

$$aa^{-1} = a^{-1}a = e.$$

Teorema 2. *Sea G un grupo y sean a, b y c elementos de G. Entonces*

(a) *$ab = ac$ implica que $b = c$* (**propiedad de cancelación por la izquierda**).

(b) *$ba = ca$ implica que $b = c$* (**propiedad de cancelación por la derecha**).

Demostración: (a) Supóngase que

$$ab = ac.$$

Al multiplicar ambos lados de esta ecuación por a^{-1} por la izquierda, se obtiene

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) & \\ (a^{-1}a)b &= (a^{-1}a)c & &\text{por asociatividad} \\ eb &= ec & &\text{por la definición de un inverso} \\ b &= c & &\text{por la definición de una identidad} \end{aligned}$$

(b) La demostración es similar a la de la parte (a). ●

Teorema 3. *Sea G un grupo y sean a y b elementos de G. Entonces*

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

(b) $(ab)^{-1} = b^{-1}a^{-1}$.

Demostración: (a) Se mostrará que a actúa como un inverso de a^{-1}:

$$aa^{-1} = a^{-1}a = e.$$

Como el inverso de un elemento es único, se concluye que $(a^{-1})^{-1} = a$.

(b) Se verifica fácilmente que

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

y, de manera análoga,

$$(b^{-1}a^{-1})(ab) = e,$$

de modo que

$$(ab)^{-1} = b^{-1}a^{-1}.$$ ●

Teorema 4. *Sea G un grupo y sean a y b elementos de G. Entonces*

(a) *La ecuación $ax = b$ tiene una única solución en G.*

(b) *La ecuación $ya = b$ tiene una única solución en G.*

Demostración: (a) El elemento $x = a^{-1}b$ es una solución de la ecuación $ax = b$, pues

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Supóngase ahora que x_1 y x_2 son dos soluciones de la ecuación $ax = b$. Entonces

$$ax_1 = b \quad \text{y} \quad ax_2 = b.$$

Por lo tanto,

$$ax_1 = ax_2.$$

El teorema 2 implica que $x_1 = x_2$.

(b) La demostración es análoga a la de la parte (a). ●

Por el análisis anterior de los monoides, se sabe que si un grupo G tiene un número finito de elementos, entonces es posible proporcionar su operación binaria mediante una tabla, que por lo general se llama **tabla de multiplicar**. La tabla de multiplicar de un grupo $G = \{a_1, a_2, \ldots, a_n\}$ bajo la operación binaria * debe satisfacer las siguientes propiedades:

1. La fila etiquetada con e debe contener los elementos

$$a_1, a_2, \ldots, a_n$$

y la columna etiquetada con e debe contener a los elementos

$$a_1$$
$$a_2$$
$$\vdots$$
$$a_n.$$

2. Por el teorema 4, cada elemento b del grupo debe aparecer exactamente una vez en cada fila y columna de la tabla. Así, cada fila y columna es una permutación de los elementos $a_1, a_2, \ldots, a_n$ de G y cada fila (y cada columna) determina una permutación diferente.

Si G es un grupo con un número finito de elementos, G es un **grupo finito** y el **orden** de G es el número de elementos $|G|$ en G. A continuación, se determinará las tablas de multiplicar de todos los grupos no isomorfos de órdenes 1, 2, 3 y 4.

Si G es un grupo de orden 1, entonces $G = \{e\}$ y se tiene que $ee = e$. Ahora, sea $G = \{e, a\}$ un grupo de orden 2. Entonces se obtiene una tabla de multiplicar (tabla 9.1) donde se debe llenar el espacio en blanco.

Tabla 9.1

	e	a
e	e	a
a	a	

Puede ocuparse el espacio con e o a. Como no pueden existir repeticiones en las filas ni las columnas, se debe escribir e en el espacio en blanco. La tabla de multiplicar de la tabla 9.2 satisface la propiedad asociativa y las demás propiedades de un grupo, de modo que es la tabla de multiplicar de un grupo de orden 2.

Tabla 9.2

	e	a
e	e	a
a	a	e

Ahora, sea $G = \{e, a, b\}$ un grupo de orden 3. Se tiene una tabla de multiplicar (tabla 9.3) donde se debe llenar cuatro espacios.

Tabla 9.3

	e	a	b
e	e	a	b
a	a		
b	b		

Tabla 9.4

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Algunos intentos muestran que sólo es posible completar la tabla como se muestra en la tabla 9.4. Se puede demostrar (pero es una tarea tediosa) que la tabla 9.4 satisface la propiedad asociativa y las demás propiedades de un grupo. Así, es la tabla de multiplicar de un grupo de orden 3. Observe que los grupos de órdenes 1, 2 y 3 también son abelianos y que sólo existe un grupo de cada orden, una vez fijas las etiquetas de los elementos.

A continuación, se tiene un grupo $G = \{e, a, b, c\}$ de orden 4. No es difícil mostrar que la posible tabla de multiplicar para G se puede completar como se muestra en las tablas 9.5 a la 9.8. Se puede mostrar que cada una de estas tablas satisface la propiedad asociativa y las demás propiedades de un grupo. Así, existen cuatro posibles tablas de multiplicar para un grupo de orden 4. De nuevo, observe que un grupo de orden 4 es abeliano. Se regresará a los grupos de orden 4 al final de esta sección, donde se verá que sólo existen dos, y no cuatro, grupos distintos, no isomorfos, de orden 4.

Tabla 9.5

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabla 9.6

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Tabla 9.7

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Tabla 9.8

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Ejemplo 5. Sea $B = \{0, 1\}$ y sea $+$ la operación definida en B de la siguiente manera:

$+$	0	1
0	0	1
1	1	0

Entonces B es un grupo. En este grupo, cada elemento es su propio inverso. ◆

Ahora se analizará un ejemplo importante de un grupo.

Ejemplo 6. Considérese el triángulo equilátero de la figura 9.3, con vértices 1, 2 y 3. Una **simetría** del triángulo (o de cualquier figura geométrica) es una correspondencia biunívoca del conjunto de puntos que forman el triángulo (la figura geométrica) en sí mismo que preserve la distancia entre los puntos adyacentes. Como el triángulo queda determinado por sus vértices, una simetría del triángulo es sólo una permutación de los vértices que preserve la distancia entre los puntos adyacentes. Sean l_1, l_2 y l_3 las bisectrices de los ángulos correspondientes, como muestra la figura 9.3, y sea O su punto de intersección.

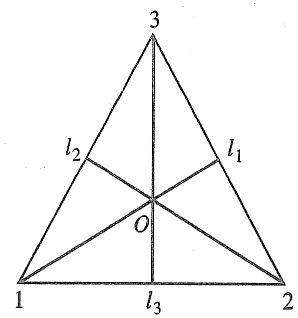


Figura 9.3

Ahora se describirá las simetrías de este triángulo. En primer lugar, existe una rotación en sentido contrario al de las manecillas del reloj f_2 del triángulo, en torno de O, con un ángulo de 120°. Entonces se puede escribir f_2 (véase la sección 5.3) como la permutación

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

A continuación se obtiene una rotación en sentido contrario al de las manecillas del reloj f_3, en torno de O, con un ángulo de 240°, que se puede escribir como la permutación

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Por último, existe una rotación en sentido contrario al de las manecillas del reloj f_1, en torno de O, con un ángulo de 360°, que se puede escribir como la permutación

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Por supuesto, también se puede ver a f_1 como el resultado de girar el triángulo en torno de O un ángulo de 0°.

También es posible obtener otras tres simetrías del triángulo, g_1, g_2 y g_3, reflejando con respecto de las líneas l_1, l_2 y l_3, respectivamente. Es posible denotar estas reflexiones como las siguientes permutaciones:

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Observe que el conjunto de todas las simetrías del triángulo queda descrito por el conjunto de permutaciones del conjunto $\{1, 2, 3\}$, estudiado en la sección 5.3 y denotado como S_3. Así,

$$S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}.$$

Ahora se puede presentar la operación *, seguido de, sobre el conjunto S_3, y se obtiene la tabla de multiplicar de la tabla 9.9.

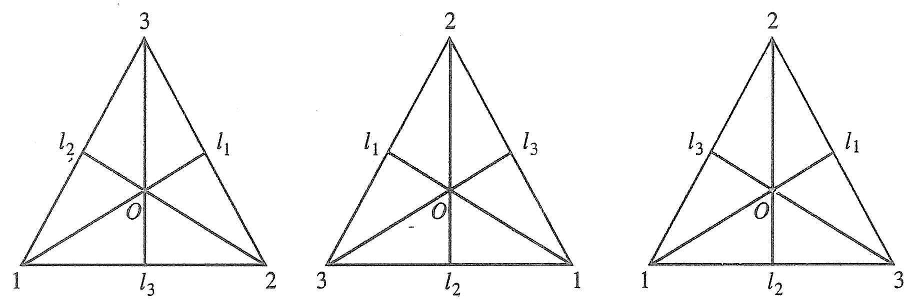
Tabla 9.9

*	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Se puede obtener cada una de las entradas de esta tabla de dos formas: algebraica o geométrica. Por ejemplo, suponga que se desea calcular $f_2 * g_2$. En forma algebraica, se tiene

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1.$$

En forma geométrica, se procede como en la figura 9.4. Como la composición de funciones siempre es asociativa, se ve que * es una operación asociativa sobre S_3. Observe que f_1 es la identidad en S_3 y que cada elemento de S_3 tiene un único inverso en S_3. Por ejemplo, $f_2^{-1} = f_3$. Por lo tanto, S_3 es un grupo, llamado **grupo de simetrías del triángulo**. Observe que S_3 es el primer ejemplo que se ha dado de un grupo que no es abeliano. ◆



Triángulo dado — Triángulo resultante después de aplicar f_2 — Triángulo resultante después de aplicar g_2 al triángulo de la izquierda

Figura 9.4

Ejemplo 7. El conjunto de todas las permutaciones de n elementos es un grupo de orden $n!$ bajo la operación de composición. Este grupo es el **grupo simétrico sobre n letras** y se denota S_n. Se ha visto que S_3 también representa al grupo de simetrías del triángulo equilátero. ◆

Como en el ejemplo 6, también es posible considerar el grupo de simetrías de un cuadrado. Sin embargo, puede verse que este grupo es de orden 8, de modo que no coincide con el grupo S_4, cuyo orden es $4! = 24$.

Ejemplo 8. En la sección 9.3 se analizó el monoide Z_n. Ahora se mostrará que Z_n es un grupo, se la siguiente manera. Sea $[a] \in Z_n$. Entonces es posible suponer que $0 \leq a < n$. Además, $[n - a] \in Z_n$, y como

$$[a] \oplus [n - a] = [a + n - a] = [n] = [0],$$

se concluye que $[n - a]$ es el inverso de $[a]$. Así, si n es 6, entonces [2] es el inverso de [4]. Observe que Z_n es un grupo abeliano. ◆

A continuación, se analizará los subconjuntos importantes de un grupo. Sea H un subconjunto de un grupo G tal que

(a) La identidad e de G pertenece a H.
(b) Si a y b pertenecen a H, entonces $ab \in H$.
(c) Si $a \in H$, entonces $a^{-1} \in H$.

Entonces H es un **subgrupo** de G. La parte (b) dice que H es un subsemigrupo de G. Así, un subgrupo de G se puede ver como un subsemigrupo que tiene las propiedades (a) y (c).

Observe que si G es un grupo y H es un subgrupo de G, entonces H también es un grupo con respecto de la operación en G, pues la propiedad asociativa en G también es válida en H.

Ejemplo 9. Sea G un grupo. Entonces G y $H = \{e\}$ son subgrupos de G, llamados subgrupos **triviales** de G. ◆

Ejemplo 10. Considérese S_3, el grupo de simetrías del triángulo equilátero, cuya tabla de multiplicar aparece en la tabla 9.9. Es fácil verificar que $H = \{f_1, f_2, f_3\}$ es un subgrupo de S_3. ◆

Ejemplo 11. Sea A_n el conjunto de las permutaciones pares (véase la sección 5.3) en el grupo S_n. Se puede mostrar, a partir de la definición de una permutación par, que A_n es un subgrupo de S_n, llamado **grupo alternante sobre *n* letras**. ◆

Ejemplo 12. Sea G un grupo y $a \in G$. Como un grupo es un monoide, ya se ha definido (sección 9.2) a^n para $n \in Z^+$ como $aa \cdots a$ (n factores) y a^0 como e. Si n es un entero negativo, a^{-n} se define como $a^{-1}a^{-1} \cdots a^{-1}$ (n factores). Entonces, si n y m son enteros arbitrarios, resulta que

$$a^n a^m = a^{n+m}.$$

Es fácil mostrar que

$$H = \{a^i \mid i \in Z\}$$

es un subgrupo de G. ◆

Sean $(G, *)$ y $(G', *')$ dos grupos. Como los grupos también son semigrupos, se puede considerar los isomorfismos y homomorfismos de $(G, *)$ en $(G', *')$.

Como un isomorfismo debe ser una función biunívoca y sobre, dos grupos cuyos órdenes no sean iguales no pueden ser isomorfos.

Ejemplo 13. Sea G el grupo de números reales bajo la suma, y sea G' el grupo de números reales positivos bajo la multiplicación. Sea $f: G \to G'$ definida por $f(x) = e^x$. Ahora se mostrará que f es un isomorfismo.

Si $f(a) = f(b)$, de modo que $e^a = e^b$, entonces $a = b$. Así, f es biunívoca. Si $c \in G'$, entonces $\ln c \in G$ y

$$f(\ln c) = e^{\ln c} = c,$$

de modo que f es sobre. Por último,

$$f(a + b) = e^{a+b} = e^a e^b = f(a)f(b).$$

Por lo tanto, f es un isomorfismo. ◆

Ejemplo 14. Sea G el grupo simétrico de n letras, y sea G' el grupo B definido en el ejemplo 5. Sea $f: G \to G'$ definida de la siguiente manera: para $p \in G$,

$$f(p) = \begin{cases} 0 & \text{si } p \in A_n \quad \text{(el subgrupo de permutaciones pares en } G\text{)} \\ 1 & \text{si } p \notin A_n. \end{cases}$$

Entonces f es un homomorfismo. ◆

Ejemplo 15. Sea G el grupo de los enteros bajo la suma y sea G' el grupo Z_n analizado en el ejemplo 8. Sea $f: G \to G'$ definida de la siguiente manera: Si $m \in G$, entonces $f(m) = [r]$, donde r es el residuo cuando m se divide entre n. A continuación se mostrará que f es un homomorfismo de G sobre G'.

Sea $[r] \in Z_n$. Entonces puede suponerse que $0 \leq r < n$, de modo que

$$r = 0 \cdot n + r,$$

lo que significa que el residuo al dividir r entre n es r. Por lo tanto,

$$f(r) = [r]$$

por lo que f es sobre.

Ahora, sean a y b elementos de G expresados como

$$a = q_1 n + r_1, \quad \text{donde } 0 \leq r_1 < n \text{ y } r_1 \text{ y } q_1 \text{ son enteros} \qquad (1)$$

$$b = q_2 n + r_2, \quad \text{donde } 0 \leq r_2 < n \text{ y } r_2 \text{ y } q_2 \text{ son enteros} \qquad (2)$$

de modo que

$$f(a) = [r_1] \quad \text{y} \quad f(b) = [r_2].$$

Entonces

$$f(a) + f(b) = [r_1] + [r_2] = [r_1 + r_2].$$

Para determinar $[r_1 + r_2]$, se necesita el residuo cuando se divide $r_1 + r_2$ entre n. Se escribe

$$r_1 + r_2 = q_3 n + r_3, \quad \text{donde } 0 \leq r_3 < n \text{ y } r_3 \text{ y } q_3 \text{ son enteros.}$$

Así,

$$f(a) + f(b) = [r_3].$$

Al sumar se obtiene

$$a + b = q_1 n + q_2 n + r_1 + r_2$$
$$= (q_1 + q_2 + q_3)n + r_3,$$

de modo que

$$f(a + b) = [r_1 + r_2] = [r_3].$$

Por lo tanto,

$$f(a + b) = f(a) + f(b),$$

lo que implica que f es un homomorfismo.

Cuando n es 2, f asigna cada entero par a [0] y cada entero impar a [1]. ◆

Teorema 5. *Sean $(G, *)$ y $(G', *')$ dos grupos y sea $f: G \to G'$ un homomorfismo de G en G'.*

(a) *Si e es la identidad en G y e' es la identidad en G', entonces $f(e) = e'$.*

(b) *Si $a \in G$, entonces $f(a^{-1}) = (f(a))^{-1}$.*

(c) *Si H es un subgrupo de G, entonces*

$$f(H) = \{f(h) \mid h \in H\}$$

es un subgrupo de G'.

Demostración: (a) Sea $x = f(e)$. Entonces

$$x *' x = f(e) *' f(e) = f(e * e) = f(e) = x,$$

de modo que $x *' x = x$. Al multiplicar ambos lados por x^{-1} a la derecha, se obtiene

$$x = x *' x *' x^{-1} = x *' x^{-1} = e'$$

Así, $f(e) = e'$.

(b)

$$a * a^{-1} = e,$$

de modo que

$$f(a * a^{-1}) = f(e) = e' \quad \text{por la parte (a)}$$

bien

$$f(a) *' f(a^{-1}) = e' \quad \text{ya que } f \text{ es un homomorfismo.}$$

De igual manera,

$$f(a^{-1}) *' f(a) = e'.$$

Por lo tanto, $f(a^{-1}) = (f(a))^{-1}$.

(c) Esto es consecuencia del teorema 4 de la sección 9.2 y de las partes (a) y (b). ●

Ejemplo 16. Los grupos S_3 y Z_6 son ambos de orden 6. Sin embargo, S_3 no es abeliano pero Z_6 sí lo es. Por lo tanto, no son isomorfos. Recuerde que un isomorfismo preserva todas las propiedades definidas en términos de las operaciones de grupo. ◆

Ejemplo 17. En esta sección ya se había determinado cuatro posibles tablas de multiplicar (las tablas 9.5 a 9.8) para un grupo de orden 4. A continuación se mostrará que los grupos con las tablas de multiplicar 9.6, 9.7 y 9.8 son isomorfos, de la manera siguiente. Sea $G = \{e, a, b, c\}$ el grupo cuya tabla de multiplicar es la tabla 9.6, y sea $G' = \{e', a', b', c'\}$ el grupo cuya tabla de multiplicar es la tabla 9.7, donde se ha colocado apóstrofos en cada entrada de esta última tabla. Sea $f: G \to G'$ definida por $f(e) = e'$, $f(a) = b'$, $f(b) = a'$, $f(c) = c'$. Entonces es posible verificar que, con este cambio de nombres a los elementos, las dos tablas son idénticas, de modo que los grupos correspondientes son isomorfos. De manera análoga, sea $G'' = \{e'', a'', b'', c''\}$ el grupo cuya tabla de multiplicar es la tabla 9.8, donde se ha colocado comillas dobles en cada entrada de esta última tabla. Sea $g: G \to G''$ definida por $g(e) = e''$, $g(a) = c''$, $g(b) = b''$, $g(c) = a''$. Entonces se puede verificar que, con este cambio de nombres a los elementos, las dos tablas son idénticas, de modo que los grupos correspondientes son isomorfos. Es decir, los grupos dados por las tablas 9.6, 9.7 y 9.8 son isomorfos.

Ahora, ¿cómo es posible asegurarse de que las tablas 9.5 y 9.6 no producen grupos isomorfos? Observe que si x es cualquier elemento en el grupo determinado por la tabla 9.5, entonces $x^2 = e$. Si los grupos fuesen isomorfos, entonces el grupo determinado por la tabla 9.6 tendrían la misma propiedad. Como no la tiene, se concluye que estos grupos no son isomorfos. Así, existen exactamente dos grupos no isomorfos de orden 4.

El grupo con la tabla de multiplicar 9.5 es llamado **grupo 4 de Klein** y se denota con V. El grupo con tabla de multiplicar 9.6, 9.7 o 9.8 es Z_4, pues al volver a etiquetar los elementos de Z_4 se produce esta tabla de multiplicar. ◆

GRUPO DE EJERCICIOS 9.4

En los ejercicios 1 *al* 11, *determine si el conjunto junto con la operación binaria es un grupo. Si es un grupo, determine si es abeliano; especifique la identidad y el inverso de un elemento a.*

1. Z, donde $*$ es la multiplicación ordinaria.

2. Z, donde $*$ es la resta.

3. Q, el conjunto de los números racionales bajo la operación de suma.

4. Q, el conjunto de números racionales bajo la operación de multiplicación.

5. $\mathbb{R}$, bajo la operación de multiplicación.

6. $\mathbb{R}$, donde $a * b = a + b + 2$.

7. Z^+, bajo la operación de suma.

8. Los números reales que no son iguales a -1, donde $a * b = a + b + ab$.

9. El conjunto de enteros impares bajo la operación de multiplicación.

10. El conjunto de las matrices $m \times n$ bajo la operación de suma de matrices.

11. Si S es un conjunto no vacío, el conjunto $P(S)$, donde $A * B = A \oplus B$ (véase la sección 1.2).

12. Sea $S = \{x \mid x \text{ es un número real y } x \neq 0, x \neq -1\}$. Considere las siguientes funciones $f_i: S \to S$, $i = 1, 2, \ldots, 6$:

$$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{1}{x}$$
$$f_4(x) = \frac{1}{1 - x}, \quad f_5(x) = 1 - \frac{1}{x}, \quad f_6(x) = \frac{x}{x - 1}.$$

Muestre que $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ es un grupo bajo la operación de composición. Proporcione la tabla de multiplicar de G.

13. Sea G un grupo con identidad e. Muestre que si $x^2 = x$ para algún x en G, entonces $x = e$.

14. Muestre que un grupo G es abeliano si y sólo si $(ab)^2 = a^2b^2$ para todos los elementos a y b en G.

15. Sea G el grupo definido en el ejemplo 4. Resuelva las siguientes ecuaciones: (a) $3 * x = 4$; (b) $y * 5 = -2$.

16. Sea G un grupo con identidad e. Muestre que si $a^2 = e$ para toda a en G, entonces G es abeliano.

17. Considere el cuadrado de la figura 9.5. Las simetrías del cuadrado son

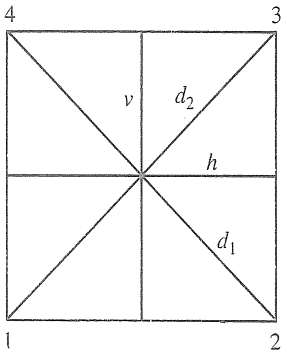


Figura 9.5

Las rotaciones f_1, f_2, f_3 y f_4 con ángulos de 0°, 90°, 180° y 270°, respectivamente.
f_5 y f_6, las reflexiones con respecto de las rectas v y h, respectivamente.
f_7 y f_8, las reflexiones con respecto de las diagonales d_1 y d_2, respectivamente.

Escriba la tabla de multiplicar de D_4, el grupo de simetrías del cuadrado.

18. Sea G un grupo. Muestre por inducción matemática que si $ab = ba$, entonces $(ab)^n = a^nb^n$ para $n \in Z^+$.

19. Sea G un grupo finito con identidad e, y sea a un elemento arbitrario de G. Demuestre que existe un entero no negativo n tal que $a^n = e$.

20. Sea G el grupo de enteros bajo la operación de suma. ¿Cuáles de los siguientes subconjuntos de G son subgrupos de G? (a) el conjunto de todos los enteros pares; (b) el conjunto de todos los enteros impares.

21. ¿Es el conjunto de racionales positivos un subgrupo del grupo de números reales bajo la operación de suma?

22. Sea G el grupo de los enteros distintos de cero bajo la operación de multiplicación, y sea $H = \{3^n \mid n \in Z\}$. ¿Es H un subgrupo de G?

23. Sea G el grupo de los enteros bajo la operación de suma, y sea $H = \{3k \mid k \in Z\}$. ¿Es H un subgrupo de G?

24. Sea G un grupo abeliano con identidad e y sea $H = \{x \mid x^2 = e\}$. Muestre que H es un subgrupo de G.

25. Sea G un grupo y sea $H = \{x \mid x \in G \text{ y } xy = yx \text{ para toda } y \in G\}$. Demuestre que H es un subgrupo de G.

26. Sea G un grupo y $a \in G$. Se define $H_a = \{x \mid x \in G \text{ y } xa = ax\}$. Demuestre que H_a es un subgrupo de G.

27. Sea A_n el conjunto de permutaciones pares en S_n. Muestre que A_n es un subgrupo de S_n.

28. Sean H y K subgrupos de un grupo G.
(a) Demuestre que $H \cap K$ es un subgrupo de G.
(b) Muestre que $H \cup K$ no necesariamente es un subgrupo de G.

29. Determine todos los subgrupos del grupo dado en el ejercicio 17.

30. Sea G un grupo abeliano y n un entero fijo. Demuestre que la función $f: G \to G$ definida por $f(a) = a^n$ para $a \in G$ es un homomorfismo.

31. Demuestre que la función $f(x) = |x|$ es un homomorfismo del grupo G de los números reales distintos de cero bajo la multiplicación con el grupo G' de números reales positivos bajo la multiplicación.

32. Sea G un grupo con identidad e. Muestre que la función $f: G \to G$ definida por $f(a) = e$ para toda $a \in G$ es un homomorfismo.

33. Sea G un grupo. Muestre que la función $f: G \to G$ dada por $f(a) = a^2$ es un homomorfismo si y sólo si G es abeliano.

34. Muestre que el grupo del ejercicio 12 es isomorfo a S_3.

35. Muestre que si $f: G \to G'$ es un isomorfismo, entonces $f^{-1}: G' \to G$ también es un isomorfismo.

36. Sea S el conjunto de todos los grupos finitos y defínase la siguiente relación R en S: $G \mathrel{R} G'$ si y sólo si G y G' son isomorfos. Demuestre que R es una relación de equivalencia. (*Sugerencia*: Utilice el ejercicio 35.)

37. Sea G el grupo de los enteros bajo la operación de suma, y sea G' el grupo de los enteros pares bajo la operación de suma. Muestre que la función $f: G \to G'$ dada por $f(a) = 2a$ es un isomorfismo.

38. Sea G un grupo. Muestre que la función $f: G \to G$ dada por $f(a) = a^{-1}$ es un isomorfismo si y sólo si G es abeliano.

39. Sea G un grupo y a un elemento fijo de G. Muestre que la función $f_a: G \to G$ definida por $f_a(x) = axa^{-1}$, para $x \in G$, es un isomorfismo.

40. Sea $G = \{e, a, a^2, a^3, a^4, a^5\}$ un grupo bajo la operación $a^ia^j = a^r$, donde $i + j \equiv r$ (mód 6). Demuestre que G y Z_6 son isomorfos.

9.5. Grupos productos y cocientes

En esta sección se obtendrá nuevos grupos a partir de otros, utilizando las ideas de producto y cociente. Como un grupo tiene más estructura que un semigrupo, nuestro resultado será más profundo que los resultados análogos para semigrupos analizados en la sección 9.3.

Teorema 1. *Si G_1 y G_2 son grupos, entonces $G = G_1 \times G_2$ es un grupo con la operación definida por*

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2).$$

●

Ejemplo 1. Sean G_1 y G_2 el grupo Z_2. Para simplificar la notación, se escribirá los elementos de Z_2 como $\bar{0}$ y $\bar{1}$, respectivamente, en vez de $[0]$ y $[1]$. Entonces la tabla de multiplicar de $G = G_1 \times G_2$ aparece en la tabla 9.10.

Tabla 9.10 Tabla de multiplicar de $Z_2 \times Z_2$

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

Como G es un grupo de orden 4, debe ser isomorfo a V o a Z_4 (véase la sección 9.4), los únicos grupos de orden 4. Al analizar las tablas de multiplicar, se observa que la función $f: V \to Z_2 \times Z_2$ definida por $f(e) = (0, 0)$, $f(a) = (1, 0)$, $f(b) = (0, 1)$ y $f(c) = (1, 1)$ es un isomorfismo.

◈

Si se repite el ejemplo 1 con Z_2 y Z_3, se verá que $Z_2 \times Z_3 \simeq Z_6$. En general, se puede mostrar que $Z_m \times Z_n \simeq Z_{mn}$ si y sólo si MCD$(m, n) = 1$, es decir, si y sólo si m y n son primos relativos.

Es claro que es posible extender el teorema 1 para mostrar que si $G_1, G_2, \ldots, G_n$ son grupos, entonces $G = G_1 \times G_2 \times \cdots \times G_n$ también es un grupo.

Ejemplo 2. Sea $B = \{0, 1\}$ el grupo definido en el ejemplo 5 de la sección 9.4, donde + se define de la siguiente manera:

+	0	1
0	0	1
1	1	0

Entonces $B^n = B \times B \times \cdots \times B$ (n factores) es un grupo con operación $\oplus$ definida por

$$(x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

La identidad de B^n es $(0, 0, \ldots, 0)$ y cada elemento es su propio inverso. Este grupo es esencialmente igual al álgebra booleana B_n definida en la sección 7.4, pero la operación binaria es muy diferente de $\wedge$ y $\vee$. ♦

Una relación de congruencia sobre un grupo es sólo una relación de congruencia sobre el grupo, visto como semigrupo. Ahora se analizará las estructuras cociente determinadas por una relación de congruencia sobre un grupo.

Teorema 2. *Sea R una relación de congruencia sobre el grupo $(G, *)$. Entonces el semigrupo $(G/R, \circledast)$ es un grupo, donde la operación $\circledast$ se define en G/R como*

$$[a] \circledast [b] = [a * b] \quad (\textit{véase la sección } 9.3).$$

Demostración: Como un grupo es un monoide, el corolario 1 de la sección 9.3 implica que G/R es un monoide. Se necesita saber si cada elemento de G/R tiene un inverso. Sea $[a] \in G/R$. Entonces $[a^{-1}] \in G/R$, y

$$[a] \circledast [a^{-1}] = [a * a^{-1}] = [e].$$

De modo que $[a]^{-1} = [a^{-1}]$. Por lo tanto, $(G/R, \circledast)$ es un grupo. ●

Como las definiciones de homomorfismo, isomorfismo y congruencia para grupos sólo implican la estructura de semigrupo y monoide, el siguiente corolario es una consecuencia inmediata de los teoremas 3 y 4 de la sección 9.3.

Corolario 1

(a) *Si R es una relación de congruencia en un grupo G, entonces la función $f_R: G \to G/R$ dada por $f_R(a) = [a]$ es un homomorfismo de grupo.*

(b) *Si $f: G \to G'$ es un homomorfismo del grupo $(G, *)$ sobre el grupo $(G', *')$ y R es la relación definida en G como $a\,R\,b$ si y sólo si $f(a) = f(b)$, para a y b en G, entonces*

1. *R es una relación de congruencia.*
2. *La función [illegible]$/R \to G'$, dada por $\bar{f}([a]) = f(a)$, es un isomorfismo del grupo $(G/R, \circledast)$ sobre el grupo $(G', *')$.* ●

Las relaciones de congruencia sobre los grupos tienen una forma muy especial, que se desarrollará a continuación. Sea H un subgrupo de un grupo G, y sea $a \in G$. La **clase izquierda** (o clase lateral izquierda) de H en G determinada por a es el conjunto $aH = \{ah \mid h \in H\}$. La **clase derecha** (o clase lateral derecha) de H en G determinada por a es el conjunto $Ha = \{ha \mid h \in H\}$. Por último, un subgrupo H de G es **normal** si $aH = Ha$ para toda a en G.

ADVERTENCIA. Si $Ha = aH$, esto *no* implica que para $h \in H$, y $a \in G$, $ha = ah$. Implica que $ha = ah'$, donde h' es algún elemento en H.

Si H es un subgrupo de G, se necesitan calcular todas las clases izquierdas de H en G. En primer lugar, supóngase que $a \in H$. Entonces $aH \subseteq H$, ya que H es un subgrupo de G; además, si $h \in H$, entonces $h = ah'$, donde $h' = a^{-1}h \in H$, de modo que $H \subseteq aH$. Así, si $a \in H$, entonces $aH = H$. Esto significa que, al determinar todas las clases de H, no se tiene que calcular aH para $a \in H$, pues siempre será igual a H.

Ejemplo 3. Sea G el grupo simétrico S_3 analizado en el ejemplo 6 de la sección 9.4. El subconjunto $H = \{f_1, g_2\}$ es un subgrupo de G. Calcule todas las clases izquierdas distintas de H en G.

Solución: Si $a \in H$, entonces $aH = H$. Así,

$$f_1H = g_2H = H.$$

Además,

$$\begin{aligned} f_2H &= \{f_2, g_1\} \\ f_3H &= \{f_3, g_3\} \\ g_1H &= \{g_1, f_2\} = f_2H \\ g_3H &= \{g_3, f_3\} = f_3H. \end{aligned}$$

Las clases izquierdas distintas de H en G son H, f_2H y f_3H. ♦

Ejemplo 4. Sean G y H como en el ejemplo 3. Entonces la clase derecha $Hf_2 = \{f_2, g_3\}$. En el ejemplo 3 se vio que $f_2H = \{f_2, g_1\}$. Esto implica que H no es un subgrupo normal de G. ♦

Ejemplo 5. Muestre que si G es un grupo abeliano, entonces todo subgrupo de G es un subgrupo normal.

Solución: Sea H un subgrupo de G y sean $a \in G$ y $h \in H$. Entonces $ha = ah$, de modo que $Ha = aH$, lo que implica que H es un subgrupo normal de G. ♦

Teorema 3. *Sea R una relación de congruencia en un grupo G y sea $H = [e]$, la clase de equivalencia que contiene a la identidad. Entonces H es un subgrupo normal de G y para cada $a \in G$, $[a] = aH = Ha$.*

Demostración: Sean a y b elementos arbitrarios en G. Como R es una relación de equivalencia, $b \in [a]$ si y sólo si $[b] = [a]$. Además, por el teorema 2 G/R es un grupo. Por lo tanto, $[b] = [a]$ si y sólo si $[e] = [a]^{-1}[b] = [a^{-1}b]$. Así, $b \in [a]$ si y sólo si $H = [e] = [a^{-1}b]$. Es decir, $b \in [a]$ si y sólo si $a^{-1}b \in H$ o $b \in aH$. Esto demuestra que $[a] = aH$ para cada $a \in G$. Puede demostrarse, de manera análoga, que $b \in [a]$ si y sólo si $H = [e] = [b][a]^{-1} = [ba^{-1}]$. Esto es equivalente a la proposición $[a] = Ha$. Así, $[a] = aH = Ha$, y H es normal. ●

Al combinar el teorema 3 con el corolario 1, se observa que en este caso, el grupo cociente G/R consta de todas las clases izquierdas de $N = [e]$. La operación en G/R está dada por

$$(aN)(bN) = [a] \circledast [b] = [ab] = abN$$

y la función $f_R : G \to G/R$, definida por $f_R(a) = aN$, es un homomorfismo de G sobre G/R. Por esta razón, se escribirá con frecuencia G/R como G/N.

A continuación se considerará la cuestión de si todo subgrupo normal de un grupo G es la clase de equivalencia de la identidad de G bajo alguna relación de congruencia.

Teorema 4. *Sea N un subgrupo normal de un grupo G, y sea R la siguiente relación en G:*

$$a\,R\,b \quad \text{si y sólo si} \quad a^{-1}b \in N.$$

Entonces

(a) *R es una relación de congruencia en G.*
(b) *N es la clase de equivalencia $[e]$ con respecto de R, donde e es la identidad de G.*

Demostración: (a) Sea $a \in G$. Entonces $a\,R\,a$, ya que $a^{-1}a = e \in N$, de modo que R es reflexiva. A continuación, supóngase que $a\,R\,b$, de modo que $a^{-1}b \in N$. Entonces $(a^{-1}b)^{-1} = b^{-1}a \in N$, por lo que $b\,R\,a$. Por lo tanto, R es simétrica. Por último, supóngase que $a\,R\,b$ y $b\,R\,c$. Entonces $a^{-1}b \in N$ y $b^{-1}c \in N$. Entonces $(a^{-1}b)(b^{-1}c) = a^{-1}c \in N$, de modo que $a\,R\,c$. Por lo tanto, R es transitiva. Así, R es una relación de equivalencia en G.

A continuación, se demostrará que R es una relación de congruencia en G. Supóngase que $a\,R\,b$ y $c\,R\,d$. Entonces $a^{-1}b \in N$ y $c^{-1}d \in N$. Como N es normal, $Nd = dN$; es decir, para cada $n_1 \in N$, $n_1 d = dn_2$ para alguna $n_2 \in N$. En particular, como $a^{-1}b \in N$, se tiene que $a^{-1}bd = dn_2$ para algún $n_2 \in N$. Entonces $(ac)^{-1}bd = (c^{-1}a^{-1})(bd) = c^{-1}(a^{-1}b)d = (c^{-1}d)n_2 \in N$, de modo que $ac\,R\,bd$. Por lo tanto, R es una relación de congruencia sobre G.

(b) Supóngase que $x \in N$. Entonces $x^{-1}e = x^{-1} \in N$ ya que N es un subgrupo, de modo que $x\,R\,e$ y por lo tanto, $x \in [e]$. Así, $N \subseteq [e]$. Recíprocamente, si $x \in [e]$, entonces $x\,R\,e$, de modo que $x^{-1}e = x^{-1} \in N$. Entonces $x \in N$ y $[e] \subseteq N$. Por lo tanto, $N = [e]$. ●

Gracias a los teoremas 3 y 4, se observa que si G es cualquier grupo, entonces las clases de equivalencia con respecto de una relación de congruencia en G son siempre las clases de algún subgrupo normal de G. Recíprocamente, las clases de cualquier subgrupo normal de G son precisamente las clases de equivalencia con respecto de alguna relación de congruencia en G. Por lo tanto, es posible traducir el corolario 1 (b) de la siguinte manera: Sea f un homomorfismo de un grupo $(G, *)$ en un grupo $(G', *')$, y sea $\ker(f)$ el **núcleo** de f, definido por

$$\ker(f) = \{a \in G \mid f(a) = e'\}.$$

Entonces

(a) $\ker(f)$ es un subgrupo normal de G.
(b) El grupo cociente $G/\ker(f)$ es isomorfo a G'.

Esto es consecuencia del corolario 1 y el teorema 3, pues si R es la relación de congruencia sobre G dada por

$$a\,R\,b \quad \text{si y sólo si} \quad f(a) = f(b),$$

entonces es fácil verificar que $\ker(f) = [e]$.

Ejemplo 6. Considérese el homomorfismo de Z en Z_n definido por

$$f(m) = [r],$$

donde r es el residuo al dividir m entre r. (Véase el ejemplo 15 de la sección 9.4.) Determine $\ker(f)$.

Solución: El entero m en Z pertenece a $\ker(f)$ si y sólo si $f(m) = [0]$; es decir, si y sólo si m es un múltiplo de n. Por lo tanto, $\ker(f) = nZ$. ◆

GRUPO DE EJERCICIOS 9.5

1. Escriba la tabla de multiplicar del grupo $Z_2 \times Z_3$.

2. Demuestre que si G y G' son grupos abelianos, entonces $G \times G'$ es un grupo abeliano.

3. Sean G_1 y G_2 dos grupos. Demuestre que $G_1 \times G_2$ y $G_2 \times G_1$ son isomorfos.

4. Sean G_1 y G_2 grupos. Muestre que la función $f: G_1 \times G_2 \to G_1$ dada por $f(a, b) = a$, para $a \in G_1$ y $b \in G_2$, es un homomorfismo.

5. Determine la tabla de multiplicar del grupo cociente $Z/3Z$, donde Z tiene la operación $+$.

6. Sea Z el grupo de enteros bajo la operación de suma. Demuestre que la función $f: Z \times Z \to Z$ dada por $f(a, b) = a + b$ es un homomorfismo.

7. Sea $G = Z_4$. Para cada uno de los siguientes subgrupos H de G, determine todas las clases izquierdas de H en G.
   (a) $H = \{[0]\}$ (b) $H = \{[0], [2]\}$
   (c) $H = \{[0], [1], [2], [3]\}$

8. Sea $G = S_3$. Para cada uno de los siguientes subgrupos H de G, determine todas las clases izquierdas de H en G.
   (a) $H = \{f_1, g_1\}$ (b) $H = \{f_1, g_3\}$
   (c) $H = \{f_1, f_2, f_3\}$ (d) $H = \{f_1\}$
   (e) $H = \{f_1, f_2, f_3, g_1, g_2, g_3\}$

9. Sea $G = Z_8$. Para cada uno de los siguientes subgrupos H de G, determine todas las clases izquierdas de H en G.
   (a) $H = \{[0], [4]\}$
   (b) $H = \{[0], [2], [4], [6]\}$

10. Sea G el grupo de los números reales distintos de cero bajo la operación de multiplicación y considere el subgrupo $H = \{3^n \mid n \in Z\}$ de G. Determine todas las clases izquierdas de H en G.

11. Sea Z el grupo de los enteros bajo la operación de suma y sea $G = Z \times Z$. Considere el subgrupo $H = \{(x, y) \mid x = y\}$ de G. Determine las clases izquierdas de H en G.

12. Sea N un subgrupo de un grupo G y sea $a \in G$. Defina
$$a^{-1}Na = \{a^{-1}na \mid n \in N\}.$$
Demuestre que N es un subgrupo normal de G si y sólo si $a^{-1}Na = N$ para toda $a \in G$.

13. Sea N un subgrupo de un grupo G. Demuestre que N es un subgrupo normal de G si y sólo si $a^{-1}Na \subseteq N$ para toda $a \in G$.

14. Determine todos los subgrupos normales de S_3.

15. Determine todos los subgrupos normales de D_4. (Ver ejercicio 17 de la sección 9.4.)

16. Sea G un grupo y $H = \{x \mid x \in G \text{ y } xa = ax \text{ para toda } a \in G\}$. Muestre que H es un subgrupo normal de G.

17. Sea H un subgrupo de un grupo G. Demuestre que toda clase izquierda aH de H tiene el mismo número de elementos que H, mostrando que la función $f_a : H \to aH$ definida por $f_a(h) = ah$, para $h \in H$, es biunívoca y sobre.

18. Sean H y K subgrupos normales de G. Muestre que $H \cap K$ es un subgrupo normal de G.

19. Sea G un grupo y H un subgrupo de G. Sea S el conjunto de las clases izquierdas de H en G, y sea T el conjunto de las clases derechas de H en G. Demuestre que la función $f: S \to T$ definida por $f(aH) = Ha^{-1}$ es biunívoca y sobre.

20. Sean G_1 y G_2 grupos. Sea $f: G_1 \times G_2 \to G_2$ el homomorfismo de $G_1 \times G_2$ en G_2 dado por $f((g_1, g_2)) = g_2$. Calcule $\ker(f)$.

21. Sea f un homomorfismo de un grupo G_1 sobre un grupo G_2 y suponga que G_2 es abeliano. Muestre que $\ker(f)$ contiene a todos los elementos de G_1 de la forma $aba^{-1}b^{-1}$, donde a y b son arbitrarios en G_1.

22. Sea G un grupo abeliano y N un subgrupo de G. Demuestre que G/N es un grupo abeliano.

23. Sea H un subgrupo del grupo finito G y suponga que sólo existen dos clases izquierdas de H en G. Demuestre que H es un subgrupo normal de G.

24. Sean H y N subgrupos del grupo G. Demuestre que si N es un subgrupo normal de G, entonces $H \cap N$ es un subgrupo normal de H.

25. Sea $f: G \to G'$ un homomorfismo de grupos. Demuestre que f es biunívoca si y sólo si $\ker(f) = \{e\}$.

IDEAS CLAVE PARA REPASO

- Operación binaria sobre A: función $f: A \times A \to A$ definida en todo punto.
- Operación binaria conmutativa: $a * b = b * a$.
- Operación binaria asociativa: $a * (b * c) = (a * b) * c$.
- Semigrupo: conjunto no vacío S junto con una operación binaria asociativa $*$ definida en S.
- Monoide: semigrupo que tiene una identidad.
- Subsemigrupo $(T, *)$ de un semigrupo $(S, *)$: T es un subconjunto no vacío de S y $a * b \in T$ siempre que a y b estén en T.
- Submonoide $(T, *)$ de un monoide $(S, *)$: T es un subconjunto no vacío de S, $e \in T$ y $a * b \in T$ siempre que a y b estén en T.
- Isomorfismo: véase la página 337.
- Homomorfismo: véase la página 339.
- Teorema: Sean $(S, *)$ y $(T, *')$ monoides con identidades e y e', respectivamente. Sea $f: S \to T$ un isomorfismo. Entonces $f(e) = e'$.
- Teorema: Si $(S, *)$ y $(T, *')$ son semigrupos, entonces $(S \times T, *'')$ es un semigrupo, donde $*''$ se define como

$$(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2).$$

- Relación de congruencia R sobre el semigrupo $(S, *)$: relación de equivalencia R tal que $a\ R\ a'$ y $b\ R\ b'$ implican que $(a * b)\ R\ (a' * b')$.
- Teorema: Sea R una relación de congruencia sobre el semigrupo $(S, *)$. Defina la operación $\circledast$ en S/R de la siguiente manera:

$$[a] \circledast [b] = [a * b].$$

Entonces $(S/R, \circledast)$ es un semigrupo.
- Semigrupo cociente o semigrupo factor S/R: véase la página 344.
- Z_n: véase la página 344.
- Teorema (Teorema fundamental de los homomorfismos). Sea $f: S \to T$ un homomorfismo del semigrupo $(S, *)$ sobre el semigrupo $(T, *')$. Sea R la relación sobre S definida por $a\ R\ b$ si y sólo si $f(a) = f(b)$, para a y b en S. Entonces
  (a) R es una relación de congruencia.
  (b) T es isomorfo a S/R.
- Grupo $(G, *)$: monoide con identidad e tal que para cada $a \in G$ existe $a' \in G$ con la propiedad de que $a * a' = a' * a = e$.
- Teorema: Sea G un grupo y sean a, b y c elementos de G. Entonces
  (a) $ab = ac$ implica que $b = c$ (propiedad de cancelación por la izquierda).
  (b) $ba = ca$ implica que $b = c$ (propiedad de cancelación por la derecha).
- Teorema: Sea G un grupo y sean a y b elementos de G. Entonces
  (a) $(a^{-1})^{-1} = a$.
  (b) $(ab)^{-1} = b^{-1}a^{-1}$.
- Orden de un grupo G: $|G|$, el número de elementos de G.
- S_n: el grupo simétrico de n letras.
- Subgrupo: véase la página 356.
- Teorema: Sea R una relación de congruencia sobre el grupo $(G, *)$. Entonces el semigrupo $(G/R, \circledast)$ es un grupo, donde la operación $\circledast$ se define en G/R como

$$[a] \circledast [b] = [a * b].$$

- Clase izquierda aH de H en G determinada por a: $\{ah \mid h \in H\}$.
- Subgrupo normal: subgrupo H tal que $aH = Ha$ para toda a en G.
- Teorema: Sea R una relación de congruencia en un grupo G y sea $H = [e]$, la clase de equivalencia que contiene a la identidad. Entonces H es un subgrupo normal de G y para cada $a \in G$, $[a] = aH = Ha$.
- Teorema: Sea N un subgrupo normal de un grupo G, y sea R la siguiente relación en G:

$$a\ R\ b \quad \text{si y sólo si} \quad a^{-1}b \in N.$$

Entonces
  (a) R es una relación de congruencia en G.
  (b) N es la clase de equivalencia $[e]$ con respecto de R, donde e es la identidad de G.

EJERCICIOS DE CODIFICACIÓN

Para cada uno de los siguientes ejercicios, escriba el programa o subrutina solicitado en seudocódigo (según lo descrito en el apéndice A) o en un lenguaje de programación conocido por usted. Verifique su código mediante una prueba con lápiz y papel o con una ejecución en la computadora.

Sea Z_n el grupo definido en la sección 9.3.

1. Escriba una función SUM que considere dos elementos de Z_n, $[x]$ y $[y]$ y regrese su suma $[x] \oplus [y]$. El usuario debe poder introducir una opción para n.

2. Sea $H = \{[0], [2]\}$. Escriba una subrutina que calcule las clases izquierdas de H en Z_6.

3. Sea $H = \{[0], [2], [4], [6]\}$. Escriba una subrutina que calcule las clases derechas de H en Z_8.

4. Escriba un programa tal que, dada una tabla finita de operación, determine si la operación satisface la propiedad asociativa.

5. Escriba un programa tal que, dado un grupo finito G y un subgrupo H, determine si H es un subgrupo normal de G.