

# ÁLGEBRA SUPERIOR

Càrdenes • Lluís • Raggi • Tomàs

- Conjuntos y combinatoria
- Introducción al álgebra lineal
- Estructuras numéricas
- Polinomios y ecuaciones



# ÁLGEBRA SUPERIOR

- Cárdenas
- Lluis
- Raggi
- Tomás

La presente obra está enfocada a los cursos de álgebra en los primeros semestres de facultades, escuelas profesionales e institutos técnicos.

El texto se ha elaborado de manera que pueda servir como:

- a) Un estudio de las estructuras numéricas básicas: números naturales, enteros, racionales, reales y complejos (capítulos 6, 8 y 9).
- b) Una introducción al álgebra lineal: espacios vectoriales, matrices, determinantes y sistemas de ecuaciones lineales (capítulos 3, 4 y 5).
- c) Una introducción a la teoría de los números: números enteros y divisibilidad (capítulos 6 y 7).
- d) Un curso de teoría de las ecuaciones: los números complejos, polinomios y ecuaciones (capítulos 9 y 10).

No obstante el enfoque antes mencionado de la obra y su secuencia funcional para los cursos de álgebra en los primeros semestres, existe una interdependencia de los capítulos.

Al principio de la obra se incluyen las nociones básicas acerca de lenguaje de



**ÁLGEBRA  
SUPERIOR**

**BIBLIOTECA DE MATEMÁTICA SUPERIOR**

# **ÁLGEBRA SUPERIOR**

- **Conjuntos y combinatoria**
- **Introducción al álgebra lineal**
- **Estructuras numéricas**
- **Polinomios y ecuaciones**

• **Humberto Càrdenas** • **Emilio Lluis**  
• **Francisco Raggi** • **Francisco Tomàs**

**EDITORIAL**  
**TRILLAS**

México. Argentina. España.  
Colombia. Puerto Rico. Venezuela



### Catalogación en la fuente

Álgebra superior : conjuntos y combinatoria,  
Introducción al álgebra lineal, estructuras  
numéricas, polinomios y ecuaciones /  
Humberto Cárdenas ... [et al.] -- 2a ed. -- México  
Trillas, 1990 (reimp. 1995).  
323 p. ; 23 cm. -- (Biblioteca de matemáticas  
superior)  
Incluye índices  
ISBN 968-24-3783-0

1. Álgebra. I. Cárdenas, Humberto. II. Ser.

LC - QA155'A4

D-512.9044'A669

331

**La presentación y disposición en conjunto de  
ÁLGEBRA SUPERIOR**

son propiedad del editor. Ninguna parte de esta obra  
puede ser reproducida o transmitida, mediante ningún sistema  
o método, electrónico o mecánico (incluyendo el fotocopiado,  
la grabación o cualquier sistema de recuperación y almacenamiento  
de información), sin consentimiento por escrito del editor

**Derechos reservados**

© 1973, Editorial Trillas, S. A. de C. V.,  
Av. Río Churubusco 385, Col. Pedro María Anaya,  
C. P. 03340, México, D. F.

División Comercial, Calz. de la Viga 1132, C. P. 09439  
México, D. F. Tel. 6330995, FAX 6330870

Miembro de la Cámara Nacional de la  
Industria Editorial. Reg. núm. 158

Primera edición, 1973 (ISBN 968-24-0247-6)  
Reimpresiones, 1974, 1976, 1978, 1979, 1981, 1982  
1983, 1984, 1986 y 1988  
Segunda edición, 1990 (ISBN 968-24-3783-0)  
Reimpresión, 1991

---

**Segunda reimpresión, enero 1995\***

---

Impreso en México  
Printed in Mexico

# Prólogo

Esta obra está basada en los cursos de álgebra superior que los autores han impartido en la Facultad de Ciencias de la UNAM y en otros centros educativos. Puede usarse como texto en los cursos de álgebra de los primeros semestres de facultades, escuelas profesionales e institutos tecnológicos.

Algunos de los capítulos aparecieron publicados previamente en la monografía *Temas de álgebra\** y otros como notas de clase.

El texto se ha elaborado de manera que pueda servir como:

- Un estudio de las estructuras numéricas básicas: números naturales, enteros, racionales, reales y complejos (capítulos 6, 8 y 9).
- Una introducción al álgebra lineal: espacios vectoriales, matrices, determinantes y sistemas de ecuaciones lineales (capítulos 3, 4 y 5).
- Una introducción a la teoría de los números: números enteros y divisibilidad (capítulos 6 y 7).
- Un curso de teoría de las ecuaciones: los números complejos, polinomios y ecuaciones (capítulos 9 y 10).

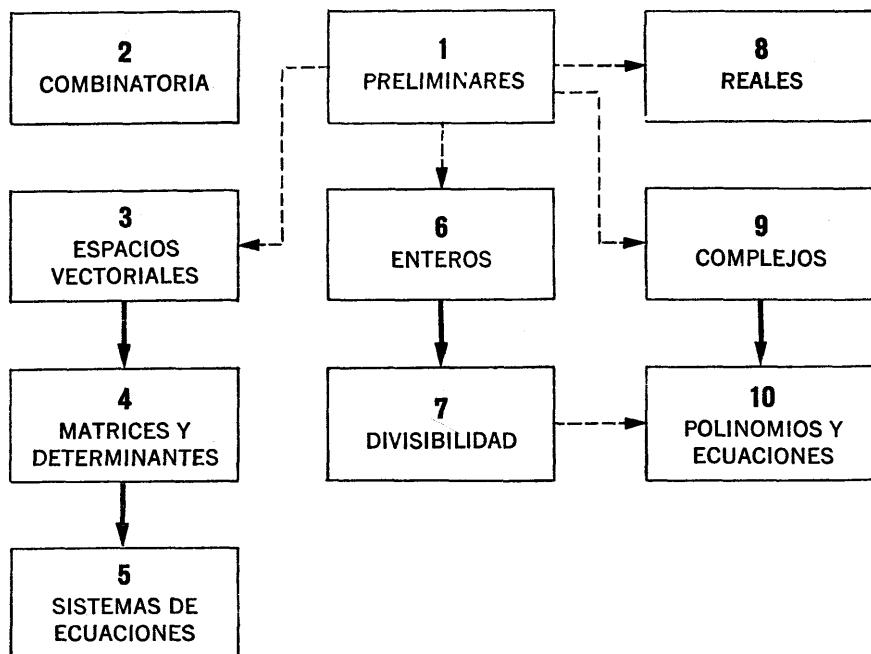
La interdependencia de los capítulos se muestra en el diagrama que aparece en la página siguiente.

El capítulo 1, de carácter introductorio, se incluye tanto para uniformar el lenguaje como para recordar algunos conceptos muchas veces ya bien conocidos del alumno que ingresa al primer año de estudios superiores. Para muchos estudiantes no será necesaria su lectura.

El capítulo 2 es independiente de los demás. El cálculo combinatorio ofrece la oportunidad de que el alumno se familiarice con el concepto de función y, al mismo tiempo, aprenda a resolver problemas que serán de gran interés en el cálculo de probabilidades.

El capítulo 8 es también independiente de los restantes. No cabe duda que un conocimiento correcto de lo que son los números reales, base del

\* Cárdenas, Humberto; Lluis, Emilio; Raggi, Francisco y Tomás, Francisco. *Temas de álgebra*. Editorial Trillas, México, 1971; preedición.



cálculo diferencial e integral y de muchas otras ramas de las matemáticas, es de fundamental interés. Sin embargo, ya que la enseñanza de este tema ofrece siempre ciertas dificultades, se suele omitir en la mayoría de los cursos a este nivel.

El libro puede usarse como texto para dos cursos semestrales. El programa mínimo de uno de ellos constaría de los capítulos 2, 3 (parte), 4 y 5; el del otro, de los capítulos 6, 7, 9 y parte del 10. Ahora bien, como se infiere del esquema (o tabla) anterior, estos dos cursos pueden ofrecerse en cualquier orden.

LOS AUTORES

# Índice general

## Capítulo 1

<b>CONCEPTOS PRELIMINARES</b>	<b>13</b>
-------------------------------	-----------

1. Conjuntos [13]
2. Subconjuntos [15]
3. Operaciones con conjuntos [16]
4. Producto cartesiano [18]
5. Relaciones [20]
6. Funciones [21]
7. Composición de funciones [22]
8. Funciones inyectivas, suprayectivas y biyectivas [24]
9. Cardinalidad y conjuntos finitos [27]
10. Inducción matemática [29]
11. El teorema del binomio [31]
12. Relaciones de equivalencia y particiones [33]
13. Estructuras numéricas [36]

## Capítulo 2

<b>CÁLCULO COMBINATORIO</b>	<b>39</b>
-----------------------------	-----------

1. Ejemplos ilustrativos [39]
2. Funciones [47]
3. Funciones inyectivas, suprayectivas y biyectivas [54]
4. Ordenaciones, permutaciones y combinaciones [57]
5. Problemas [64]

**Capítulo 3****ESPACIOS VECTORIALES**

73

1. El espacio vectorial  $\mathbf{R}^2$  [73]
2. El espacio vectorial  $\mathbf{R}^n$  [80]
3. Subespacios vectoriales [82]
4. Combinaciones lineales. Dependencia e independencia lineal [84]
5. Bases de subespacios vectoriales. Dimensión [89]

**Capítulo 4****MATRICES Y DETERMINANTES**

97

1. Matrices [97]
2. El rango de una matriz [101]
3. Permutaciones [108]
4. Determinantes [113]
5. Propiedades básicas de los determinantes [117]
6. Más propiedades de los determinantes [123]
7. Cálculo de determinantes [131]
8. Caracterización del rango de una matriz mediante determinantes [133]

**Capítulo 5****SISTEMAS DE ECUACIONES LINEALES**

137

1. Definiciones [137]
2. Existencia de soluciones [140]
3. Sistemas de  $n$  ecuaciones con  $n$  incógnitas [144]
4. Sistemas homogéneos [148]
5. Sistema homogéneo asociado [152]
6. Resolución de sistemas [154]

**Capítulo 6****EL ANILLO DE LOS NÚMEROS ENTEROS**

163

1. Propiedades básicas de las operaciones en  $\mathbf{Z}$  [163]
2. Anillos [164]

3. Propiedades de anillos de los enteros [167]
4. Dominios enteros [170]
5. El orden en  $\mathbf{Z}$  [171]
6. Unidades en  $\mathbf{Z}$  [173]
7. El principio de inducción [174]
8. El principio de buen orden [177]

**Capítulo 7****DIVISIBILIDAD****179**

1. Definiciones y propiedades elementales [179]
2. El algoritmo de la división [184]
3. El máximo común divisor [187]
4. El algoritmo de Euclides y ecuaciones diofantinas [193]
5. Factorización única [198]
6. Congruencias [202]

**Capítulo 8****LOS NÚMEROS REALES****209**

1. Los números racionales [209]
2. El conjunto  $\mathbf{R}$  de los reales. Orden en  $\mathbf{R}$  [217]
3. Cotas y fronteras [219]
4. Suma y producto de reales [222]
5. Propiedades de la suma, el producto y el orden en  $\mathbf{R}$  [224]
6. Racionales y reales [233]
7. Raíces de reales positivos. Exponentes fraccionarios [238]
8. Valor absoluto [241]
9. Aproximación [242]

**Capítulo 9****EL CAMPO DE LOS NÚMEROS COMPLEJOS****245**

1. Módulo y argumento de vectores de  $\mathbf{R}^2$  [245]
2. Los números complejos [253]
3. Propiedades de las operaciones [259]
4. Raíz cuadrada [266]

5. Raíces  $n$ -ésimas de números complejos [271]
6. El campo de los números complejos [273]

## Capítulo 10

### POLINOMIOS Y TEORÍA DE ECUACIONES

277

1. Polinomios [277]
2. Los polinomios como funciones [279]
3. Suma y producto de polinomios [280]
4. División con residuo [283]
5. Raíces de polinomios. Teorema del residuo.  
Todo polinomio de grado positivo tiene  
raíces [286]
6. Ecuaciones de segundo grado [288]
7. División sintética. Expresión de un polinomio  
en la forma  $\sum a_i(x-a)^i$  [290]
8. Cálculo de una raíz aislada en un intervalo en  
cuyos extremos el polinomio tiene signos  
contrarios [293]
9. Factorización de un polinomio. Raíces  
múltiples [297]
10. Derivadas y multiplicidad [300]
11. Coeficientes y raíces [303]
12. Polinomios con coeficientes reales [304]
13. El algoritmo de Euclides con polinomios [306]
14. Aislamiento de las raíces reales de un polinomio  
con coeficientes reales (teorema de Sturm) [308]
15. Fracciones racionales. Descomposición en  
fracciones parciales [312]
16. Ecuaciones de tercero y cuarto grados con  
coeficientes reales [318]

Índice analítico [321]

Índice de símbolos [323]

- Conjuntos y combinatoria
- Introducción al álgebra lineal
- Estructuras numéricas
- Polinomios y ecuaciones



# 1

CAPÍTULO

# Conceptos preliminares

ESTE capítulo es de carácter introductorio. En la actualidad, muchos de los alumnos que llegan a las facultades están ya familiarizados con el lenguaje de conjuntos y funciones y conocen sus operaciones y propiedades básicas. Sin embargo, tanto para uniformar el lenguaje como para recordar los conocimientos aprendidos en cursos previos y, en ocasiones, para profundizar un poco, incluimos aquí las nociones básicas acerca de estos temas.

Según sus conocimientos, el alumno puede omitir o simplemente leer superficialmente algunos de los párrafos de este capítulo.

## 1. CONJUNTOS

Es posible definir, con una axiomática, los conceptos “conjunto, elemento y pertenencia”. Sin embargo, para las finalidades de este libro, es suficiente considerar como primitivos dichos conceptos y manejarlos en la forma intuitiva usual; es decir, los elementos pertenecen a conjuntos y un conjunto está formado por todos sus elementos. Así pues, dos conjuntos son iguales si y solo si, tienen los mismos elementos.

En general, usaremos letras mayúsculas  $A, B, C$ , etc., para representar conjuntos y minúsculas  $a, b, c$ , etc., para representar a los elementos. Para especificar los elementos de un conjunto, usaremos la escritura entre llaves; si  $A$  es el conjunto que consta de las letras  $a, b$  y  $c$ , escribimos

$$A = \{a, b, c\}.$$

No escribiremos un mismo elemento repetidas veces. Por ejemplo, el conjunto de las cifras que aparecen en el número 1 212 212 es {1, 2}.

El orden en que aparecen los elementos de un conjunto, cuando están enlistados, es irrelevante. Por ejemplo, {1, 2, 3} = {2, 3, 1} = {2, 1, 3}.

Un conjunto muy importante en matemáticas es el conjunto  $\mathbb{N}$  de los *números naturales*

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, \dots\}.$$

También es importante el conjunto  $\mathbb{Z}$  de los *números enteros*

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

Para denotar que un elemento  $x$  pertenece a un conjunto  $A$  escribiremos  $x \in A$  y cuando un elemento  $x$  no pertenezca al conjunto  $A$  escribiremos  $x \notin A$ .

### Ejemplos:

1. Sea  $A = \{1, 3, 5, 7\}$ . Entonces

$$5 \in A \quad y \quad 2 \notin A.$$

2. Sea  $A = \{1, 4, 9, 16, \dots, n^2, \dots\}$ , es decir,  $A$  es el conjunto de los cuadrados de los números naturales. Entonces  $1\ 024 \in A$  y  $50 \notin A$ .

## EJERCICIOS

1. Enlistese la familia de los números naturales que son múltiplos de tres y menores que 17.

2. Enlistense las cifras que aparecen en el número  $2^{12}$  cuando se escribe en notación decimal.

3. ¿Cuál es el conjunto de las letras en la palabra *Parangaricutirimícuaro*?

4. Sea  $P = \{2, 3, 5, 7, 11, 13, \dots\}$  el conjunto de los números naturales primos (es decir, aquellos cuyos únicos factores son él mismo y la unidad). Indíquense cuáles de los siguientes números pertenecen a  $P$ :

$$11, 111, 1\ 111, 11\ 111, 37, 27.$$

5. Sean  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{2, 4, 6, 8\}$  y  $C = \{3, 6, 9\}$ .

Enlistense los elementos tales que:

- i) pertenecen a  $A$  y a  $B$ ;
- ii) pertenecen a  $A$  y a  $C$ ;
- iii) pertenecen a  $A$ ,  $B$  y  $C$ .

Usaremos el símbolo  $\phi$  para denotar al conjunto vacío, es decir, el conjunto que no tiene elementos.

Por medio de condiciones podemos también describir conjuntos. Por ejemplo si  $A$  es el conjunto  $\{2, 4, 6, 8\}$  escribiremos

$$A = \{n \in \mathbb{N} \mid n \text{ es par y } n \leq 8\}.$$

6. Procediendo como en el ejemplo anterior, describanse, mediante condiciones apropiadas, los siguientes conjuntos:

- a)  $\{1, 3, 5, 7, 9\};$
- b)  $\{1, 4, 9, 25, 36, \dots, n^2, \dots\};$
- c)  $\{11, 12, 13, 14, \dots\};$
- d)  $\{2, 6, 10, 14, 18, 22, \dots\}.$

## 2. SUBCONJUNTOS

**DEFINICIÓN:** Sean  $A$  y  $B$  dos conjuntos. Decimos que  $B$  es un subconjunto de  $A$ , si cada elemento de  $B$  es también un elemento de  $A$ .

Usemos la notación  $B \subset A$  siempre que  $B$  sea un subconjunto de  $A$ .

Así pues,  $B \subset A$  si y solo si,  $x \in B$  implica que  $x \in A$ .

Si  $B$  no es subconjunto de  $A$  empleamos la notación  $B \not\subset A$ .

### Ejemplos:

1. Sean  $B$  el conjunto de los pájaros y  $A$  el conjunto de los bípedos. Entonces  $B \subset A$  y  $A \not\subset B$ .

2. Sean  $A$  el conjunto de los seres del reino animal y  $B$  el conjunto de los seres del reino vegetal. Entonces  $A \not\subset B$  y  $B \not\subset A$ .

3. Sean  $A = \{n \mid n \in \mathbb{N}, n \leq 10\}$ ,  $B = \{1, 3, 5, 7\}$  y  $C = \{2, 4, 8\}$ . Entonces  $B \subset A$ ,  $C \subset A$ ,  $B \not\subset C$ ,  $C \not\subset B$  y  $A \not\subset C$ .

4. En geometría euclíadiana, es bien sabido que todo punto del segmento  $\overline{AB}$ , pertenece a la recta determinada por  $A$  y  $B$ , que denotaremos  $\overleftrightarrow{AB}$ . Esto se puede expresar así  $\overline{AB} \subset \overleftrightarrow{AB}$ .

5. La misma afirmación anterior se puede escribir del siguiente modo:

Sea  $\mathcal{R}$  una recta con puntos  $A$  y  $B$  en ella. Entonces  $\overline{AB} \subset \mathcal{R}$ . En otras palabras

$$A \in \mathcal{R} \text{ y } B \in \mathcal{R} \text{ implica } \overline{AB} \subset \mathcal{R}.$$

### EJERCICIO

1. Sea  $B(P, r)$  el círculo del plano con centro  $P$  y radio  $r$ . Esto es,

$$B(P, r) = \{x \mid d(P, x) \leq r\}$$

donde  $d(P, x)$  denota la distancia de  $P$  a  $x$ .

Demuéstrese que

- a)  $B(P, r) \subset B(P, r')$  si y solo si,  $r \leq r'$ ;
- b)  $s \leq r - d(Q, P)$  implica  $B(Q, s) \subset B(P, R)$ .

### 3. OPERACIONES CON CONJUNTOS

En situaciones que se presentan con frecuencia, todos los conjuntos considerados son subconjuntos de uno fijo. A tal conjunto lo llamamos *conjunto universal*.

**DEFINICIÓN:** *La unión de dos conjuntos A y B es el conjunto*

$$A \cup B = \{x | x \in A \text{ o } x \in B\}.$$

Las propiedades

- i)  $A \subset A \cup B, B \subset A \cup B$ ;
- ii)  $A \cup B = B \cup A$  (comutatividad);
- iii)  $(A \cup B) \cup C = A \cup (B \cup C)$  (asociatividad),

se verifican inmediatamente a partir de la definición.

Podemos entonces, sin ambigüedad, hacer uso del símbolo  $A \cup B \cup C$ , para denotar al conjunto  $A \cup (B \cup C) = (A \cup B) \cup C$ .

**DEFINICIÓN:** *La intersección de dos conjuntos A y B es el conjunto*

$$A \cap B = \{x | x \in A \text{ y } x \in B\}.$$

Las propiedades

- iv)  $A \cap B \subset A, A \cap B \subset B$ ;
- v)  $A \cap B = B \cap A$  (comutatividad);
- vi)  $A \cap (B \cap C) = (A \cap B) \cap C$  (asociatividad),

se verifican inmediatamente a partir de la definición.

Usamos el símbolo  $A \cap B \cap C$ , para denotar al conjunto  $(A \cap B) \cap C = A \cap (B \cap C)$ .

**PROPOSICIÓN 1:** Sean A, B y C conjuntos. Entonces las propiedades

- vii)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;
- viii)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ,

son válidas. Estas son llamadas *leyes distributivas*.

Demostraremos la propiedad (vii).

Sea  $x \in A \cap (B \cup C)$ . Entonces  $x \in A$  y  $x \in B \cup C$  de donde,  $x \in A$  y  $(x \in B \text{ o } x \in C)$ . Si  $x \in B$ , tenemos  $x \in A \cap B$ ; luego  $x \in (A \cap B) \cup (A \cap C)$ .

Si  $x \in C$ , tenemos  $x \in A \cap C$ ; luego  $x \in (A \cap B) \cup (A \cap C)$ .

Esto demuestra que  $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$ .

La contención en el otro sentido se demuestra como sigue:

Ya que  $A \cap B \subset A$  y  $A \cap C \subset A$ , se tiene  $(A \cap B) \cup (A \cap C) \subset A$ .

Análogamente,  $A \cap B \subset B \cup C$  y  $A \cap C \subset B \cup C$ , por lo que  $(A \cap B) \cup (A \cap C) \subset B \cup C$ .

Se tiene entonces,  $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$ , lo que termina la demostración.

La demostración de la propiedad (viii) queda a cargo del lector.

**DEFINICIÓN:** Sea  $X$  el conjunto universal y  $A$  un conjunto arbitrario. El complemento del conjunto  $A$  es el conjunto

$$A^c = \{x | x \in X, x \notin A\}.$$

Nótese que el complemento de un conjunto se define respecto al conjunto universal del cual se están tomando los conjuntos.

Son propiedades básicas de la complementación las siguientes:

ix)  $(A^c)^c = A$ ;

x)  $A \cup A^c = X$ ;

xi)  $A \cap A^c = \emptyset$ .

La demostración de estas propiedades se deja a cargo del lector.

**PROPOSICIÓN 2** (leyes de De Morgan): Para cualquier pareja de conjuntos  $A$  y  $B$  valen las propiedades

xii)  $(A \cup B)^c = A^c \cap B^c$ ;

xiii)  $(A \cap B)^c = A^c \cup B^c$ .

Demostraremos la propiedad (xiii).

Sea  $x \in (A \cap B)^c$ . Entonces  $x \notin A \cap B$ , de donde  $x \notin A$  o  $x \notin B$ ; esto es  $x \in A^c$  o  $x \in B^c$ , de donde,  $x \in A^c \cup B^c$ . Esto prueba que  $(A \cap B)^c \subset A^c \cup B^c$ .

Ahora,  $A \cap B \subset A$  y  $A \cap B \subset B$ , por lo que  $(A \cap B)^c \supset A^c$  y  $(A \cap B)^c \supset B^c$ . De donde,  $(A \cap B)^c \supset A^c \cup B^c$ .

Esto termina la demostración.

**DEFINICIÓN:** La diferencia entre dos conjuntos  $A$  y  $B$ , es el conjunto

$$A - B = \{x | x \in A \text{ y } x \notin B\}.$$

Se tiene entonces que  $A - B = A \cap B^c$ .

Tenemos la siguiente propiedad:

$$\text{xiv)} \quad A - (B \cap C) = (A - B) \cup (A - C).$$

*Demostración:*

$$\begin{aligned} A - (B \cap C) &= A \cap (B \cap C)^c = (A^c \cup (B \cap C))^c \\ &= ((A^c \cup B) \cap (A^c \cup C))^c = (A^c \cup B)^c \cup (A^c \cup C)^c \\ &= (A \cap B^c) \cup (A \cap C^c) = (A - B) \cup (A - C). \end{aligned}$$

Se sugiere al lector que verifique qué propiedades y definiciones se usaron en cada paso de esta demostración.

#### 4. PRODUCTO CARTESIANO

**DEFINICIÓN:** Sean  $a, b \in X$ , definimos la pareja ordenada formada por  $a$  y  $b$  [y la denotamos  $(a, b)$ ] por

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

Nótese que lo que se quiere recalcar es la distinción entre el primer lugar y el segundo lugar en la pareja; esta definición nos lleva a tal distinción ya que

$$(a, b) = (c, d) \quad \text{si y solo si} \quad a = c \quad \text{y} \quad b = d.$$

*Demostración.* Existen dos posibilidades, a saber

- i)  $\{a\} = \{c\}$  y  $\{a, b\} = \{c, d\}$ ;
- ii)  $\{a\} = \{c, d\}$  y  $\{a, b\} = \{c\}$ .

En el caso (i) se tiene  $a = c$  por lo que  $\{a, b\} = \{a, d\}$  y entonces  $b = d$ .

En el caso (ii) se tiene  $a = c = d$  y entonces  $\{a, b\} = \{a\}$  por lo que  $b = a$ .

Ilustraremos el concepto de pareja ordenada con algunos ejemplos:

1. Sea  $A = \{1, 2\}$ , hay entonces cuatro parejas ordenadas de elementos de  $A$ ,

$$(1, 1), (1, 2), (2, 1) \text{ y } (2, 2).$$

2. Sean  $A = \{a, b\}$ ,  $B = \{c, d\}$ , hay cuatro parejas ordenadas tales que el primer elemento pertenezca a  $A$  y el segundo a  $B$ , a saber

$$(a, c), (a, d), (b, c) \text{ y } (b, d).$$

3. Sea  $A = \{1, 2, 3\}$ . Hay nueve parejas ordenadas de elementos de  $A$ . El lector debe escribirlas todas.

4. Si  $A$  es un conjunto infinito, entonces el conjunto de parejas ordenadas  $(a, b)$  con  $a, b \in A$  es también infinito.

**DEFINICIÓN:** Sean  $A$  y  $B$  conjuntos. El producto cartesiano de  $A$  y  $B$ ,  $A \times B$ , es el conjunto de parejas ordenadas

$$A \times B = \{(a, b) | a \in A \text{ y } b \in B\}.$$

**Ejemplos:**

5. Sean  $A = \{1, 2, 3\}$ ,  $B = \{a, b\}$ . Entonces

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

6. Sea  $A = \{1, 2\}$ . Entonces

$$A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}.$$

7. Sea  $\mathbb{N}$  el conjunto de los números naturales. Entonces

$$\mathbb{N} \times \mathbb{N} = \{(n, m) | n \in \mathbb{N}, m \in \mathbb{N}\}.$$

8. Sea  $\mathbb{Z}$  el conjunto de los números enteros. Entonces

$$\mathbb{Z} \times \mathbb{Z} = \{(n, m) | n \in \mathbb{Z}, m \in \mathbb{Z}\}.$$

9. Sea  $\mathbf{R}$  el conjunto de los números reales. Entonces  $\mathbf{R} \times \mathbf{R} = \{(x, y) | x \in \mathbf{R}, y \in \mathbf{R}\}$  es el plano real.

En el caso que tomamos el producto cartesiano de un conjunto  $A$  por sí mismo usamos la notación  $A \times A = A^2$ .

## EJERCICIOS

1. Compruebe que  $A \times B$  tiene seis elementos si  $A$  tiene tres elementos y  $B$  tiene dos.

2. Dé la lista de los elementos de  $A \times B$  donde  $A = \{1, 2, 3, 4\}$  y  $B = \{1, 2\}$ .

3. Verifique que el conjunto  $\mathbb{N} \times A$  con  $A = \{a, b\}$  es infinito.

*Sugerencia.* Si  $a \in A$ , los elementos de la forma  $(n, a)$  con  $n \in \mathbb{N}$  están en  $\mathbb{N} \times A$  y forman un subconjunto infinito.

**4.** Describa  $A^2$ , donde:

- i)  $A = \{1, 2\}$
- ii)  $A = \{a, b, c\}$
- iii)  $A = \{2, 4, 6, 8\}$ .

## 5. RELACIONES

**DEFINICIÓN:** Sean  $A$  y  $B$  conjuntos. Una relación entre  $A$  y  $B$  es un subconjunto del producto cartesiano  $A \times B$ .

### Ejemplos:

1. Sea  $A = \phi$ ,  $B$  arbitrario, entonces  $A \times B = \phi$  y por lo tanto la única posible relación entre  $A$  y  $B$  es la vacía.

Análogamente si  $B = \phi$ .

2. Si  $A = \{a\}$  y  $B = \{b\}$  entonces  $A \times B = \{(a, b)\}$  y existen dos relaciones entre  $A$  y  $B$ , la vacía y la total.

3. Si  $A$  y  $B$  son arbitrarios siempre se tienen al menos dos relaciones entre  $A$  y  $B$  (no necesariamente distintas), la vacía y la total.

4. Si  $A = \{a, b\}$  y  $B = \{1, 2\}$  existen dieciséis relaciones entre  $A$  y  $B$ .

## EJERCICIOS

**1.** Enlístense las relaciones en el ejemplo 4.

Sea  $R \subset A \times B$  una relación.

El dominio  $D_R$  de la relación  $R$ , está definida por:

$$D_R = \{a \in A \mid \text{existe } b \in B, (a, b) \in R\}.$$

Por ejemplo, si  $A = \{a, b\}$ ,  $B = \{1, 2, 3\}$  y  $R = \{(a, 1), (a, 3)\}$ , entonces  $a \in D_R$  y  $b \notin D_R$ .

Por la definición de dominio tenemos que  $D_R \subset A$ .

**2.** Dígase cuál es el dominio en cada una de las dieciséis relaciones del ejercicio anterior.

La imagen  $I_R$  de la relación  $R$ , está dada por:

$$I_R = \{b \in B \mid \text{existe } a \in A, (a, b) \in R\}.$$

**3.** Dígase cuál es la imagen en cada una de las relaciones del ejemplo (4).

El codominio de una relación  $R \subset A \times B$  es el conjunto  $B$ .

**4.** En el ejemplo (4) díganse cuáles relaciones tienen la propiedad de que su imagen y su codominio coinciden.

## 6. FUNCIONES

Sean  $A$  y  $B$  conjuntos. Una función  $f:A \rightarrow B$  es una relación  $R$  en  $A \times B$  que satisface:

- $D_R = A$ ; es decir, para toda  $x \in A$  existe una pareja  $(x, y) \in R$ .
- Cada elemento  $x \in A$  tiene asociado uno solo de  $B$ ; es decir,  $(x, y_1) \in R$  y  $(x, y_2) \in R$  implica  $y_1 = y_2$ .

Una notación alternativa para una función  $f:A \rightarrow B$  es  $A \xrightarrow{f} B$ .

El conjunto  $A$  es llamado el *dominio* de la función, el conjunto  $B$  es llamado el *codominio* de la función y para cada  $x \in A$ , denotamos con  $f(x)$  al elemento de  $B$  que le corresponde; es decir,  $(x, f(x)) \in R$ . Llamamos a  $f(x)$  la *imagen* del elemento  $x$ .

### Ejemplos:

- Sea  $A$  un conjunto y sea  $f:A \rightarrow A$  la función dada por  $f(x) = x$  para toda  $x \in A$ .
- Sean  $A$  el conjunto de las personas y  $B$  el conjunto de las naciones. La relación  $R \subset A \times B$  de las parejas  $(x, y)$  tales que, “ $x$  tiene nacionalidad correspondiente a  $y$ ”, es una función  $f:A \rightarrow B$ .
- Sean  $f:\mathbb{Z} \rightarrow \mathbb{N}$  dada por  $f(n) = n^2 + 1$  para toda  $n \in \mathbb{Z}$ .

Es inmediato de la definición que dos funciones  $f:A \rightarrow B$  y  $g:C \rightarrow D$  son iguales si y solo si,

- $A = C$ ;
- $B = D$ ;
- $f(x) = g(x)$  para toda  $x \in A$ .

### EJERCICIOS

- Díganse por qué las funciones  $f:\mathbb{Z} \rightarrow \mathbb{N}$  y  $g:\mathbb{Z} \rightarrow \mathbb{Z}$  dadas por  $f(n) = n^2 + 1 = g(n)$  no son iguales.
- Lo mismo para  $f:\mathbb{Z} \rightarrow \mathbb{Z}$  y  $g:\mathbb{N} \rightarrow \mathbb{Z}$  dadas por  $f(n) = 2n = g(n)$ .

**DEFINICIÓN:** La *imagen* de una función  $f:A \rightarrow B$  es

$$Imf = \{b \in B \mid \text{existe } a \in A \text{ con } f(a) = b\}.$$

Se tiene que  $Imf$  es un subconjunto del codominio de la función.

## EJERCICIOS

Dése la imagen de la función para cada uno de los siguientes ejemplos:

3.  $f: \mathbf{Z} \rightarrow \mathbf{Z}$  dada por  $f(n) = 2n$ .
4.  $f: \mathbf{Z} \rightarrow \mathbf{N}$  dada por  $f(n) = n^2 + 1$ .
5.  $f: \mathbf{N} \rightarrow \mathbf{N}$  dada por  $f(n) = n^2 + 1$ .
6.  $I_A: A \rightarrow A$  dada por  $I_A(x) = x$ .

Sea  $f: A \rightarrow B$  una función en donde el conjunto  $A$  es finito.

Si  $A = \{a_1, \dots, a_n\}$  y  $f(a_i) = b_i$ , emplearemos la siguiente notación:

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_r \end{pmatrix}.$$

Es decir, en esta notación, en el primer renglón se escriben todos los elementos del dominio y debajo de cada uno de ellos el elemento que le corresponde según la función.

Esta notación, salvo por la descripción del codominio, nos dice cuál es la función.

### Ejemplo:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 9 & 16 & 25 \end{pmatrix},$$

es una función  $f: A \rightarrow B$  en donde  $A = \{n \in \mathbf{N} | n \leq 5\}$  y  $f(x) = x^2$  para toda  $x \in A$ .

## EJERCICIO

7. Dé la lista completa de las funciones  $f: A \rightarrow B$  donde  $A = \{a, b, c\}$  y  $B = \{1, 2\}$ , usando el método antes descrito.

## 7. COMPOSICIÓN DE FUNCIONES

Sean  $f: A \rightarrow B$  y  $g: B \rightarrow C$  dos funciones. Definimos la composición de  $f$  y  $g$ , denotada por  $g \circ f$ , como la función  $g \circ f: A \rightarrow C$  dada por

$$(g \circ f)(x) = g(f(x)) \quad \text{para toda } x \in A.$$

### Ejemplos:

1. Sean  $f: \mathbf{R} \rightarrow \mathbf{R}$  y  $g: \mathbf{R} \rightarrow \mathbf{R}$  definidas por  $f(x) = x^2 + 1$  y  $g(x) = 3x + 2$ . Entonces la composición  $g \circ f: \mathbf{R} \rightarrow \mathbf{R}$  está dada por

$$(g \circ f)(x) = g(f(x)) = g(x^2 + 1) = 3(x^2 + 1) + 2 = 3x^2 + 5.$$

2. Sean  $A = \{a_1, a_2, a_3\}$ ,  $B = \{b_1, b_2\}$ ,  $C = \{c_1, c_2, c_3\}$   $f:A \rightarrow B$  y  $g:B \rightarrow C$  dadas por

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_1 & b_2 \end{pmatrix} \quad g = \begin{pmatrix} b_1 & b_2 \\ c_2 & c_3 \end{pmatrix}$$

entonces la composición  $g \circ f:A \rightarrow C$  está dada por

$$g \circ f = \begin{pmatrix} a_1 & a_2 & a_3 \\ c_2 & c_2 & c_3 \end{pmatrix}$$

ya que  $(g \circ f)(a_1) = g(f(a_1)) = g(b_1) = c_2$ , etc.

3. Sean  $A = \{a_1, a_2, a_3\}$ ,  $B = \{b_1, b_2, b_3, b_4\}$ ,  $f:A \rightarrow B$  y  $g:B \rightarrow C$  dadas por

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_4 & b_3 & b_2 \end{pmatrix} \quad g = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ a_3 & a_3 & a_2 & a_1 \end{pmatrix}$$

entonces  $g \circ f:A \rightarrow A$  está dada por

$$g \circ f = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix} = I_A.$$

4. Sea  $A = \{1, 2\}$  y  $f:A \rightarrow A$  la función dada por

$$f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

entonces  $f \circ f:A \rightarrow A$  es

$$f \circ f = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = I_A.$$

5. Sean  $A = \{1, 2, 3\}$  y  $f, g, h:A \rightarrow A$  dadas por

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \end{pmatrix} \quad h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}$$

Entonces  $h \circ f, h \circ g:A \rightarrow A$  son

$$h \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix} = h \quad h \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix} = h$$

es decir  $h \circ f = h \circ g = h$ .

**TEOREMA 1:** *Sea  $f:A \rightarrow B$  una función. Entonces*

$$I_B \circ f = f \quad f \circ I_A = f$$

donde  $I_B, I_A$  son las identidades en  $B$  y  $A$  respectivamente.

La demostración de este teorema se deja a cargo del lector.

**TEOREMA 2:** Sean  $f:A \rightarrow B$ ,  $g:B \rightarrow C$  y  $h:C \rightarrow D$  funciones. Entonces

$$h \circ (g \circ f) = (h \circ g) \circ f$$

es decir, la composición de funciones es asociativa.

*Demostración.* Sea  $x \in A$ , entonces

$$\begin{aligned}[h \circ (g \circ f)](x) &= h[(g \circ f)(x)] = h[g(f(x))] \\ [(h \circ g) \circ f](x) &= (h \circ g)(f(x)) = h[g(f(x))]\end{aligned}$$

y como las dos funciones tienen dominio  $A$  y codominio  $D$  la demostración queda completa.

Sea  $f:A \rightarrow B$  una función.

**DEFINICIÓN:** Un inverso derecho (izquierdo) de  $f$  es una función  $g:B \rightarrow A$  tal que

$$g \circ f = I_A \quad (f \circ g = I_B).$$

Si  $g$  es inverso derecho e izquierdo de  $f$  entonces  $g$  se llama inverso de  $f$  y en caso de que  $f$  tenga inverso se dice que  $f$  es invertible.

**TEOREMA 3:** Si  $f$  tiene inverso derecho  $g_1$  e inverso izquierdo  $g_2$  entonces  $g_1 = g_2$  y  $f$  es invertible.

*Demostración.* Por definición  $g_1 \circ f = I_A$  y  $f \circ g_2 = I_B$  de donde

$$g_1 = g_1 \circ I_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2.$$

**COROLARIO:** Si  $f:A \rightarrow B$  es invertible, entonces su inverso  $g:B \rightarrow A$  es único.

El ejemplo siguiente nos ilustra que una función puede tener inverso por un lado y sin embargo no ser invertible. También comprueba que, aunque las composiciones  $g \circ f$  y  $f \circ g$  tengan sentido, no son necesariamente iguales; es decir la composición de funciones no es una operación commutativa.

Denotemos por  $[x]$  a la parte entera de cualquier número real  $x$ , es decir,  $[x]$  es el entero máximo, menor o igual que  $x$ .

Sean  $f:\mathbf{Z} \rightarrow \mathbf{Z}$  y  $g:\mathbf{Z} \rightarrow \mathbf{Z}$  dadas por  $f(n) = 2n$  y  $g(n) = \left[ \frac{n}{2} \right]$  entonces  $g \circ f = I_{\mathbf{Z}}$  pero  $f \circ g \neq I_{\mathbf{Z}}$  (el lector deberá comprobar estas afirmaciones).

## 8. FUNCIONES INYECTIVAS, SUPRAYECTIVAS Y BIYEKTIVAS

**DEFINICIÓN 1:** Una función  $f:A \rightarrow B$  se llama inyectiva si para toda pareja  $a_1, a_2 \in A$  con  $a_1 \neq a_2$  se tiene  $f(a_1) \neq f(a_2)$ .

Esto equivale a

$$f(a_1) = f(a_2) \text{ implica } a_1 = a_2.$$

**DEFINICIÓN 2:** Una función  $f:A \rightarrow B$  se llama suprayectiva si  $\text{Im}f = B$ ; es decir, si para toda  $b \in B$  existe  $a \in A$  tal que  $f(a) = b$ .

**DEFINICIÓN 3:** Una función  $f:A \rightarrow B$  se llama biyectiva si es inyectiva y suprayectiva.

### Ejemplos:

1. Sea  $f:\mathbf{R} \rightarrow \mathbf{R}$  dada por  $f(x) = x^2$ , entonces  $f$  no es inyectiva ya que  $f(1) = f(-1)$ ; tampoco es suprayectiva ya que  $f(x) \geq 0$  y por lo tanto ningún elemento negativo está en la imagen de  $f$ .

2. Sea  $f:\mathbf{Z} \rightarrow \mathbf{Z}$  dada por  $f(n) = 2n$ , entonces  $f$  es inyectiva porque  $f(n) = f(m)$  implica  $2n = 2m$  implica  $n = m$ .

La función no es suprayectiva ya que los números enteros impares no están en la imagen de  $f$ .

3. Sea  $f:\mathbf{Z} \rightarrow \mathbf{Z}$  dada por  $f(n) = \left[ \frac{n}{2} \right]$  entonces  $f$  es suprayectiva ya que si  $m \in \mathbf{Z}$  tenemos  $m = \left[ \frac{2m}{2} \right] = f(2m)$ ; la función no es inyectiva puesto que  $f(2n) = \left[ \frac{2n}{2} \right] = n = \left[ \frac{2n+1}{2} \right] = f(2n+1)$ .

4. Sea  $A$  un conjunto arbitrario. La función idéntica  $I_A:A \rightarrow A$  es biyectiva.

### EJERCICIOS

1. Compruébese la afirmación del ejemplo 4.

2. Sea  $f:\mathbf{N} \rightarrow \mathbf{Z}$  dada por  $f(n) = (-1)^n \left[ \frac{n}{2} \right]$ . Demuéstrese que  $f$  es biyectiva.

3. Sea  $f:\mathbf{Z} \rightarrow \mathbf{Q}$  la inclusión natural, donde  $\mathbf{Q}$  es el conjunto de los números racionales o fraccionarios. Demuéstrese que  $f$  es inyectiva.

4. Sea  $f:\mathbf{Q} \rightarrow \mathbf{Z}$  dada por  $f\left(\frac{n}{m}\right) = 2^n 3^m$  donde  $\left(\frac{n}{m}\right)$  fracción simplificada (es decir,  $n$  y  $m$  no tienen factores comunes). Demuéstrese que  $f$  es inyectiva.

Demostraremos a continuación varias proposiciones interesantes:

**PROPOSICIÓN 1:**  $f:A \rightarrow B$  es invertible si y solo si, es biyectiva.

**PROPOSICIÓN 2:** La composición de dos funciones inyectivas es inyectiva.

**PROPOSICIÓN 3:** La composición de dos funciones suprayectivas es suprayectiva.

**COROLARIO.** La composición de dos funciones biyectivas es biyectiva.

*Demostraciones:*

1. Sea  $f:A \rightarrow B$  biyectiva. Definimos  $g:B \rightarrow A$  como sigue:

Si  $b \in B$  entonces existe  $a \in A$  tal que  $f(a) = b$  por ser  $f$  suprayectiva y dicha  $a$  es única por ser  $f$  inyectiva; sea  $g(b) = a$ .

Tenemos entonces, para cualquier  $b \in B$ ,  $g(b) = a$  donde  $f(a) = b$ , luego

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

por lo tanto  $f \circ g = I_B$ .

Para cualquier  $a \in A$  tenemos: si  $f(a) = b$ , que  $g(b) = a$  y entonces

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

por lo que  $g \circ f = I_A$ .

Esto demuestra que si  $f$  es biyectiva entonces es invertible.

Supongamos ahora que  $f$  es invertible, es decir, existe  $g:B \rightarrow A$  tal que

$$f \circ g = I_B \quad y \quad g \circ f = I_A.$$

*Demostraremos primero que  $f$  es inyectiva:*

Si  $a_1 \in A$ ,  $a_2 \in A$  y  $f(a_1) = f(a_2)$  tenemos  $a_1 = I_A(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2) = I_A(a_2) = a_2$ .

Veamos ahora que  $f$  es suprayectiva:

Sea  $b \in B$  arbitrario. Entonces

$$b = I_B(b) = (f \circ g)(b) = f(g(b))$$

es decir,  $b$  es la imagen de  $g(b)$  bajo  $f$ .

Esto termina la demostración de la proposición 1.

Demostremos ahora la proposición 2. Suponemos que  $f:A \rightarrow B$  y  $g:B \rightarrow C$  son inyectivas.

Sean  $a_1, a_2 \in A$  tales que  $(g \circ f)(a_1) = (g \circ f)(a_2)$ ; de la definición de composición obtenemos

$$g(f(a_1)) = g(f(a_2))$$

y como  $g$  es inyectiva concluimos que

$$f(a_1) = f(a_2);$$

acto seguido podemos concluir que  $a_1 = a_2$  por ser  $f$  inyectiva. Esto muestra que  $g \circ f$  es inyectiva.

Veamos la proposición 3. Supongamos que  $f:A \rightarrow B$  y  $g:B \rightarrow C$  son funciones suprayectivas.

Sea  $c \in C$ . Entonces  $c = g(b)$  para algún  $b \in B$  puesto que  $g$  es suprayectiva. Pero a su vez  $b = f(a)$  para algún  $a \in A$ , por ser  $f$  suprayectiva, así que

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

Esto muestra que  $g \circ f$  es suprayectiva.

## EJERCICIOS

5. Sean  $f:A \rightarrow B$  y  $g:B \rightarrow C$  funciones tales que  $g \circ f$  es inyectiva. Demuéstrese que  $f$  es inyectiva.

6. Sean  $f:A \rightarrow B$  y  $g:B \rightarrow C$  funciones tales que  $g \circ f$  es suprayectiva. Demuéstrese que  $g$  es suprayectiva.

7. Dense funciones  $f:A \rightarrow B$  y  $g:B \rightarrow C$  tales que  $f$  es inyectiva y  $g \circ f$  no lo es.

8. Dense funciones  $f:A \rightarrow B$  y  $g:B \rightarrow C$  tales que  $g$  es suprayectiva y  $g \circ f$  no lo es.

9. Dense funciones  $f:A \rightarrow B$  y  $g:B \rightarrow C$  tales que  $f$  es inyectiva,  $g$  es suprayectiva y  $g \circ f$  no es inyectiva ni suprayectiva.

10. Dense funciones  $f:A \rightarrow B$  y  $g:B \rightarrow C$  tales que  $f$  no es suprayectiva,  $g$  no es inyectiva y  $g \circ f$  es biyectiva.

## 9. CARDINALIDAD Y CONJUNTOS FINITOS

Decimos que dos conjuntos  $A$  y  $B$  tienen la misma cardinalidad si existe alguna función biyectiva  $f:A \rightarrow B$ .

### EJERCICIO

1. Demuéstrese que los siguientes conjuntos tienen todos la misma cardinalidad:

- i)  $\mathbb{N}$  el conjunto de los números naturales;
- ii)  $\mathbb{Z}$  el conjunto de los números enteros;
- iii)  $\{n^2 | n \in \mathbb{Z}\}$ ;
- iv)  $\{2n | n \in \mathbb{Z}\}$ ;
- v)  $\{3n | n \in \mathbb{Z}\}$ .

Sea  $I_n$  el conjunto de los  $n$  primeros naturales:

$$I_n = \{1, 2, 3, \dots, n\} = \{a | a \in \mathbb{Z}, 1 \leq a \leq n\}.$$

Decimos que un conjunto  $A \neq \emptyset$  es finito si para algún  $n \in \mathbb{N}$  existe una función biyectiva

$$f: I_n \rightarrow A.$$

En otras palabras,  $A$  es finito si podemos “contar” sus elementos.

Definimos el número cardinal o número de elementos de un conjunto finito  $A \neq \emptyset$  como el natural  $n$  para el cual existe una función biyectiva  $f: I_n \rightarrow A$ .

Al dar esta definición, hemos admitido, tácitamente, que sólo hay un número natural  $n$  para el cual existe tal función biyectiva. Admitir esto, no es otra cosa que admitir que cada vez que contemos los elementos de un conjunto no vacío sin equivocarnos obtendremos el mismo resultado.

Denotamos el cardinal del conjunto finito  $A \neq \emptyset$  por  $\#A$ .

Completamos la definición con  $\#\emptyset = 0$ .

Si  $\#A = n$  sabemos que existe una biyección (que, en general, no es única)  $J: I_n \rightarrow A$ . Se acostumbra utilizar la notación

$$a_i = J(i) \quad \text{para } i = 1, 2, \dots, n.$$

Así que  $A = \{a_1, a_2, \dots, a_n\}$ .

A los conjuntos que no son finitos se les llama infinitos.

**LEMÁ 1:** Si  $A$  y  $B$  son conjuntos finitos y  $f: A \rightarrow B$  es una función inyectiva entonces  $\#A \leq \#B$ .

*Demostración.* Supongamos que  $\#A = n$ . Sea  $A = \{a_1, \dots, a_n\}$  con todas las  $a_i$  distintas entre sí. Los  $n$  elementos  $f(a_1), \dots, f(a_n) \in B$  son todos distintos ya que si  $i \neq j$  y  $f(a_i) = f(a_j)$  por ser  $f$  inyectiva tendríamos  $a_i = a_j$  lo cual es una contradicción, por lo que  $B$  tiene al menos  $n$  elementos, es decir,  $\#B \geq n$ .

**LEMÁ 2:** Si  $A$  y  $B$  son conjuntos finitos y  $f: A \rightarrow B$  es una función suprayectiva, entonces  $\#A \geq \#B$ .

*Demostración.* Supongamos que  $\#B = m$ . Sea  $B = \{b_1, \dots, b_m\}$  con todas las  $b_i$  distintas entre sí. Sea  $a_i \in A$  tal que  $f(a_i) = b_i$  para  $i = 1, 2, \dots, m$  (esta  $a_i$  existe debido a que  $f$  es suprayectiva). Los  $m$  elementos  $a_1, \dots, a_m$  son todos distintos ya que si  $a_i = a_j$  se tendría  $f(a_i) = f(a_j)$  y entonces  $b_i = b_j$  que contradice la elección de las  $b_i$ , por lo que  $A$  tiene al menos  $m$  elementos, es decir,  $\#A \geq m$ .

**COROLARIO:** Si  $A$  y  $B$  son conjuntos finitos y  $f: A \rightarrow B$  es biyectiva entonces  $\#A = \#B$ .

**TEOREMA:** Sean  $A$  y  $B$  conjuntos finitos tales que  $\#A = \#B$  y  $f: A \rightarrow B$  una función. Las tres siguientes condiciones son equivalentes:

- i)  $f$  es inyectiva;
- ii)  $f$  es suprayectiva;
- iii)  $f$  es biyectiva.

*Demostración.* Basta demostrar la equivalencia entre i) y ii).

Supongamos i). Sea  $A = \{a_1, \dots, a_n\}$ ,  $\#A = n = \#B$  entonces como  $f$  es inyectiva  $Imf = \{f(a_1), \dots, f(a_n)\}$  tiene  $n$  elementos distintos de  $B$ ; pero  $\#B = n$  por lo que  $Imf \subset B$  y  $\#Imf = \#B$ , de donde  $Imf = B$  y  $f$  es suprayectiva.

Supongamos ahora ii). Sea  $A = \{a_1, \dots, a_n\}$ , es decir,  $\#A = n$ . Si  $f$  no fuese inyectiva existirían elementos  $a_i, a_j \in A$  distintos tales que  $f(a_i) = f(a_j)$ . Sin pérdida de generalidad podemos suponer que,  $f(a_{n-1}) = f(a_n)$ , se tendría entonces

$$Imf = \{f(a_1), \dots, f(a_{n-1})\}$$

ya que  $f(a_n)$  es  $f(a_{n-1})$ . Pero como  $f$  es suprayectiva  $Imf = B$ . Por otro lado  $\#Imf \leq n-1$ , es decir,  $\#B \leq n-1$ , lo cual contradice la hipótesis  $\#A = \#B$ .

Así pues,  $f$  debe ser inyectiva y el teorema queda demostrado.

Nótese que la hipótesis  $A$  y  $B$  finitos es necesaria, pues los ejemplos (2) y (3) de 7. son contraejemplos al teorema en el caso infinito.

## 10. INDUCCIÓN MATEMÁTICA

Cuando una propiedad requiere ser demostrada y es concerniente a los números naturales, hay un tipo de demostración, llamada inducción matemática, que se lleva al cabo de la siguiente forma.

Supongamos que se quiere demostrar la propiedad  $P(n)$  donde  $n \in \mathbb{N}$ . Los dos pasos siguientes son necesarios y suficientes:

- i) Se demuestra la validez de  $P(1)$ ; es decir, que la propiedad vale cuando  $n = 1$ .
- ii) Se supone que  $P(n)$  es válida y a partir de esto se demuestra la validez de  $P(n+1)$ ; es decir, se supone que la propiedad es válida para  $n$  y a partir de esto se demuestra que es válida para  $n + 1$ .

Una vez llevados al cabo estos pasos, la conclusión es que la propiedad es válida para todos los números naturales.

Más adelante justificaremos la validez lógica de este tipo de demostración, por ahora solo daremos algunos ejemplos en los que puede ser usada.

Supongamos que queremos averiguar si la fórmula

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}$$

es válida para todos los números naturales.

Procedemos de acuerdo con lo descrito.

**Ejemplos:**

Si  $n = 1$  el miembro izquierdo de la fórmula consta de un solo sumando que es 1 y el miembro derecho es  $\frac{1(1+1)}{2}$  y como este es también 1 se tiene que la fórmula es válida para  $n = 1$ . Supongamos ahora que

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad (*)$$

y tratemos de probar la fórmula correspondiente para  $n + 1$ .

El miembro izquierdo en la fórmula para  $n + 1$  es  $1 + 2 + \cdots + n + (n+1)$  y si usamos (\*) tenemos

$$\begin{aligned} 1 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + n + 1 = \frac{n^2 + n + 2n + 2}{2} = \\ &= \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2} \end{aligned}$$

lo que prueba la validez de la fórmula para  $n + 1$ .

Un segundo ejemplo es el siguiente:

Supongamos que queremos probar que

$$2^n < n!$$

para  $n \geq 4$  ( $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$  para  $n \geq 1$ ).

Es equivalente esto a

$$2^{n+3} \leq (n+3)!$$

para  $n \in \mathbb{N}$ , así que demostraremos la segunda desigualdad:

$$\text{Si } n = 1, 2^{1+3} = 16 \text{ y } (1+3)! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

y como  $16 < 24$  queda probado este caso.

$$\text{Supongamos ahora que } 2^{n+3} < (n+3)! \quad (*)$$

y como  $n \geq 1$  se tiene  $2 < n + 4$ . Multiplicando (\*) por esta desigualdad se obtiene

$$2^{n+3} \cdot 2 < (n+3)!(n+4)$$

de donde

$$2^{n+4} < (n+4)!$$

que es lo que se quería probar.

Un tercer ejemplo es el siguiente:

Deseamos demostrar que  $n^3 - n$  es un múltiplo de 6 para todo natural  $n$ .

Si  $n = 1$  entonces  $n^3 - n = 0$  y 0 es múltiplo de 6 (ya que  $0 = 6 \cdot 0$ ).

Supongamos que  $n^3 - n$  es múltiplo de 6, es decir  $n^3 - n = 6k$  para alguna  $k \in \mathbb{Z}$ .

$$\begin{aligned} \text{Ahora } (n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 - n + 3(n^2 + n) \\ &= 6k + 3(n^2 + n) \end{aligned}$$

pero  $n^2 + n$  es par para toda  $n \in \mathbb{N}$  por lo que  $n^2 + n = 2s$  y  $(n+1)^3 - (n+1) = 6k + 3 \cdot 2s = 6(k+s)$ .

## EJERCICIOS

1. Supóngase que  $a_{i+1} - a_i = r$  para toda  $i$ . Demuéstrese que

$$a_1 + \cdots + a_n = \frac{(a_1 + a_n)n}{2}.$$

2. Demuéstrese, para  $q \neq 1$ , que

$$1 + q + \cdots + q^{n-1} = \frac{q^n - 1}{q - 1}.$$

3. Supóngase que  $a_{i+1} = a_i q$  para todo  $i$ . Demuéstrese que si  $q \neq 1$ ,

$$a_1 + \cdots + a_n = \frac{a_{n+1} - a_1}{q - 1}.$$

## 11. EL TEOREMA DEL BINOMIO

**DEFINICIÓN:** Sea  $n \in \mathbb{Z}$  tal que  $n \geq 0$ . Definimos el factorial de  $n$ , denotado por  $n!$ , por inducción, como sigue:

- i)  $0! = 1$ ;
- ii)  $n! = (n-1)! n$     $n \geq 1$ .

**PROPOSICIÓN 1:** Si  $n \geq 1$  entonces

$$n! = n(n-1) \cdots 2 \cdot 1.$$

*Demostración.* Si  $n = 1$  entonces el miembro derecho de la igualdad se reduce a un solo factor, que es la unidad, mientras que  $1! = 0! \cdot 1 = 1 \cdot 1 = 1$ .

Sea  $n > 1$  y continuamos la demostración por inducción.

Se tiene  $(n-1)! = (n-1) \cdots 2 \cdot 1$ , de donde

$$n! = (n-1)! \cdot n = n \cdot (n-1) \cdots 2 \cdot 1$$

lo que termina la demostración.

Denotamos  $C_n^m = \frac{n!}{m!(n-m)!}$ .

**TEOREMA 1** (teorema de Pascal):

$$C_{n-1}^m + C_{n-1}^{m-1} = C_n^m.$$

La demostración se deja a cargo del lector. (Véase también la pág. 63.)

**PROPOSICIÓN 2:** El número  $C_n^m$  es un número natural.

*Demostración.* Inducción sobre  $n$ . Si  $n = 0$  entonces  $C_0^0 = \frac{0!}{0! 0!} = 1$ .

Sea  $n > 1$  y supongamos el resultado válido para  $n-1$ . Entonces  $C_{n-1}^m$  y  $C_{n-1}^{m-1}$  son números naturales y por lo tanto lo es  $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$ .

**Teorema del binomio.** Sean  $a$  y  $b$  números reales y  $n \in \mathbb{Z}$ ,  $n \geq 0$ ; entonces

$$\begin{aligned} (a+b)^n &= C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^n b^n \\ &= \sum_{i=0}^n C_n^i a^{n-i} b^i. \end{aligned}$$

*Demostración.* Inducción sobre  $n$ .

Si  $n = 0$  entonces  $(a+b)^0 = 1$  y  $C_0^0 a^0 b^0 = 1$ .

Sea  $n > 0$  y

$$(a+b)^{n-1} = \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} b^i$$

entonces

$$\begin{aligned} (a+b)^n &= (a+b)(a+b)^{n-1} = (a+b) \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} b^i \\ &= \sum_{i=0}^{n-1} C_{n-1}^i a^{n-i} b^i + \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} b^{i+1} \end{aligned}$$

Por tanto

$$\begin{aligned}
 (a+b)^n &= \sum_{i=0}^{n-1} C_{n-1}^i a^{n-i} b^i + \sum_{i=1}^n C_{n-1}^{i-1} a^{n-i} b^i \\
 &= \sum_{i=0}^n (C_{n-1}^i + C_{n-1}^{i-1}) a^{n-i} b^i \\
 &= \sum_{i=0}^n C_n^i a^{n-i} b^i
 \end{aligned}$$

En el último paso se usa el teorema de Pascal y se conviene que  $C_{n-1}^{-1} = 0$  y  $C_{n-1}^n = 0$ , es claro que  $C_{n-1}^{-1} + C_{n-1}^0 = C_n^0$  y  $C_{n-1}^{n-1} + C_{n-1}^n = C_n^n$ .

## 12. RELACIONES DE EQUIVALENCIA Y PARTICIONES

**DEFINICIÓN:** Una relación  $R \subset A \times A$  se llama de equivalencia si satisface:

- i)  $(a, a) \in R$  para toda  $a \in A$ ;
- ii)  $(a, b) \in R$  implica  $(b, a) \in R$ ;
- iii)  $(a, b) \in R, (b, c) \in R$  implica  $(a, c) \in R$ .

Estas tres propiedades son llamadas reflexividad, simetría y transitividad, respectivamente.

Nótese que la propiedad de reflexividad implica que  $D_R = A = I_R$ , es decir, en una relación de equivalencia, dominio, codominio e imagen coinciden.

### Ejemplos:

1. Si  $A$  es un conjunto arbitrario, entonces la mínima relación de equivalencia en  $A$  es  $R = \{(a, a) | a \in A\}$ ; esta es llamada la diagonal de  $A \times A$  y se tiene que toda relación de equivalencia debe contener a la diagonal debido a la propiedad de reflexividad.

2. Consideremos la familia  $A$  de los triángulos en el plano geométrico. Vamos a dar una relación  $R$  en  $A \times A$ .

Decimos que  $(a, b)$  está en  $R$  si  $a$  y  $b$  son triángulos semejantes; es decir, si los ángulos correspondientes son iguales.

Es claro que todo triángulo es semejante a sí mismo, lo que demuestra que la relación  $R$  es reflexiva. Así mismo podemos ver fácilmente que la relación es simétrica y transitiva, por lo que  $R$  es una relación de equivalencia.

3. Sea  $A = \{1, 2, 3\}$  y  $R \subset A \times A$  dada por

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2)\}.$$

El lector puede verificar que  $R$  es simétrica y transitiva. Sin embargo, la pareja  $(3, 3) \notin R$  y por tanto  $R$  no es reflexiva.

## EJERCICIOS

1. Dese un ejemplo de relación para la cual valgan las propiedades de reflexividad y simetría, pero no la de transitividad.
2. Dese un ejemplo de relación para la cual valgan las propiedades de reflexividad y transitividad, pero no la de simetría.
3. Sea  $k \in \mathbb{N}$ . Definimos una relación  $R \subset \mathbb{Z} \times \mathbb{Z}$  como sigue:

$$(n, m) \in R \text{ si } n - m = ks \text{ para algún } s \in \mathbb{Z}.$$

Demuéstrese que  $R$  es una relación de equivalencia.

**DEFINICIÓN:** Una partición de un conjunto  $A$  es una familia de subconjuntos de  $A$ ,  $\{A_\alpha\}_{\alpha \in I}$ , tal que:

- i) Si  $A_\alpha \neq A_\beta$  entonces  $A_\alpha \cap A_\beta = \emptyset$ ;
- ii)  $A_\alpha \neq \emptyset$  para toda  $\alpha \in I$ ;
- iii)  $A = \bigcup_{\alpha \in I} A_\alpha$ .

### Ejemplos:

4. Si  $A = \{a\}$  entonces hay una y solo una partición de  $A$ , es decir,  $\{A\}$  la familia con un solo conjunto.
5. Para cualquier conjunto  $A \neq \emptyset$  siempre existen al menos dos particiones (que coinciden si  $A$  tiene menos de dos elementos) que son:
  - i) la partición  $\{A\}$  cuya familia consta de un solo conjunto;
  - ii) la partición  $\{\{a\}\}_{a \in A}$  cuya familia consta de todos los subconjuntos de  $A$  que tienen un solo elemento.

## EJERCICIOS

4. Verifíquese que las familias de los ejemplos (4) y (5) son particiones.
5. Si  $A = \{1, 2, 3\}$  considérese la familia  $\{1, 2\}, \{3\}$ . Demuéstrese que es una partición de  $A$ .
6. Enlístese la colección de particiones de:
  - a)  $A = \{1\}$ .
  - b)  $A = \{1, 2\}$ .
  - c)  $A = \{1, 2, 3\}$ .
  - d)  $A = \{1, 2, 3, 4\}$ .
  - e)  $A = \{1, 2, 3, 4, 5\}$ .
7. Si  $P_n$  denota el número de particiones de un conjunto con  $n$  elementos, dígase cuánto vale  $P_1, P_2, P_3, P_4$  y  $P_5$ .

Sea  $A$  un conjunto arbitrario; denotamos por  $R_A$  a la familia de relaciones de equivalencia en  $A \times A$  y por  $P_A$  a la familia de particiones de  $A$ .

Para cada relación de equivalencia en  $A \times A$  vamos a definir una partición de  $A$ , es decir, vamos a dar una función

$$\varphi: R_A \rightarrow P_A$$

como sigue:

Si  $R \in R_A$  para cada  $x \in A$  definimos

$$Ax = \{y \in A \mid (x, y) \in R\}.$$

**LEMÁ:** La familia  $\{Ax\}_{x \in A}$  es una partición  $P$  de  $A$  ya que:

- i)  $Ax \neq \emptyset$  para toda  $x \in A$ ;
- ii)  $Ax = Ay$  si  $(x, y) \in R$  y  $Ax \cap Ay = \emptyset$  si  $(x, y) \notin R$ ;
- iii)  $A = \bigcup_{x \in A} Ax$ .

*Demostración:* i) Es inmediata de la reflexividad de  $R$ .

Para probar ii) supongamos primero que  $(x, y) \in R$ ; sea  $z \in Ax$ ; por definición tenemos  $(x, z) \in R$  y como  $(x, y) \in R$  entonces  $(y, x) \in R$  tenemos  $(y, z) \in R$ ,  $(x, z) \in R$  por lo que  $(y, z) \in R$ , es decir,  $z \in Ay$  de donde  $Ax \subset Ay$ .

Análogamente se verifica que  $Ay \subset Ax$  y entonces  $Ax = Ay$ .

Ahora supongamos que  $(x, y) \notin R$  y que  $z \in Ax \cap Ay$ ; tenemos  $(x, z), (y, z) \in R$  y por la simetría de  $R$   $(z, y) \in R$ ; finalmente por la transitividad tenemos  $(x, y) \in R$  que contradice la hipótesis. Entonces  $Ax \cap Ay \neq \emptyset$ .

Es claro que  $\bigcup Ax \subset A$  ya que  $A$  es el conjunto universal.

Si  $y \in A$  entonces  $y \in Ay$ ; por tanto  $y \in \bigcup_{x \in A} Ax$  de donde  $A = \bigcup_{x \in A} Ax$ .

Hemos definido una función  $\varphi: R_A \rightarrow P_A$  dada por  $\varphi(R) = P$ .

Vamos ahora a definir una función  $\psi: P_A \rightarrow R_A$ .

Sea  $P \in P_A$  con la familia asociada  $\{A_\alpha\}$  y consideremos la relación  $R \subset A \times A$  dada como sigue:

$(x, y) \in R$  si existe  $A_\alpha$  subconjunto de la partición  $P$  tal que  $x, y \in A_\alpha$ .

**LEMÁ:** La relación  $R$  así definida es una relación de equivalencia.

*Demostración.* Sea  $x \in A$ , entonces por ser  $P$  partición existe  $A_\alpha$  en  $P$  tal que  $x \in A_\alpha$ , y ahora por la definición de  $R$ , ya que  $x \in A_\alpha$ , tenemos  $(x, x) \in R$ ; es decir  $R$  es reflexiva.

Sean  $x, y \in A$  tales que  $(x, y) \in R$ , es decir, existe  $A_\alpha$  en  $P$  tal que  $x, y \in A_\alpha$  pero esto es equivalente a  $y, x \in A_\alpha$ , es decir,  $(y, x) \in R$ , por tanto  $R$  es simétrica.

Para terminar supongamos que  $(x, y), (y, z) \in R$  entonces existen  $A_\alpha$  y  $A_\beta$  en  $P$  tales que  $x, y \in A_\alpha$  y  $y, z \in A_\beta$ . Entonces  $y \in A_\alpha \cap A_\beta$  por lo tanto

$A_\alpha = A_\beta$ , es decir,  $x, z \in A_\alpha$  y de aquí  $(x, z) \in R$ ; lo que prueba que  $R$  es transitiva. Lo cual concluye la demostración.

**TEOREMA:**  $\psi \circ \varphi = I_{RA}$  y  $\varphi \circ \psi = I_{PA}$ .

*Demostración.* Sea  $R \in R_A$ ,  $x, y \in A$  tal que  $(x, y) \in (\psi \circ \varphi)R$ . Entonces existe  $A_\alpha$  en la partición  $\varphi R$  tal que  $x, y \in A_\alpha$  por la definición de  $\psi$ . Ahora los subconjuntos de la partición  $\varphi R$  son aquellos de la forma  $Az = \{t \in A \mid (z, t) \in R\}$ ; por lo tanto existe  $z \in A$  tal que  $A_\alpha = Az$ , es decir,  $x, y \in Az$ ; por lo tanto,  $(z, x), (z, y) \in R$ ; por ser  $R$  de equivalencia obtenemos  $(x, y) \in R$ ; esto prueba que  $(\psi \circ \varphi)R \subset R$ .

Sea  $(x, y) \in R$  implica  $x, y \in Ax$ ,  $Ax$  subconjunto de  $\varphi R$  implica  $(x, y) \in (\psi \circ \varphi)R$  por la definición de  $\psi$ .

Hemos probado que  $R = (\psi \circ \varphi)R$ , es decir,  $\psi \circ \varphi = I_{RA}$ .

La demostración de  $\varphi \circ \psi = I_{PA}$  es análoga y la dejamos como ejercicio.

El teorema nos demuestra que existe correspondencia biunívoca entre particiones y relaciones de equivalencia, la conclusión del teorema es que podemos usar indistintamente un concepto o el otro; o sea podemos identificar cada relación de equivalencia con su partición asociada.

Algunos ejemplos ilustrativos del teorema son los que a continuación damos:

Si  $A$  es un conjunto arbitrario y  $R$  es la relación diagonal en  $A \times A$ , es decir  $R = \{(x, x) \mid x \in A\}$  entonces  $\varphi R$  está dada por la familia  $\{\{x\}\}_{x \in A}$ .

Sea  $A = \{1, 2, 3\}$ ,  $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$  entonces  $\varphi R = \{\{1, 2\}, \{3\}\}$ .

Sea  $A = \mathbf{Z}$ ,  $k \in \mathbf{N}$  y  $R \subset \mathbf{Z} \times \mathbf{Z}$  dada por  $(n, m) \in R$  si  $n - m = ks$  para alguna  $s \in \mathbf{Z}$ .

Entonces la partición  $\varphi R$  está dada por la familia  $\{[0], [1], \dots, [k-1]\}$  donde

$$[i] = \{m \in \mathbf{Z} \mid m - i = ks, s \in \mathbf{Z}\}$$

$$i = \{0, \dots, k-1\}.$$

Es fácil demostrar que  $\varphi R$  es la descrita y con esto vemos que en  $\mathbf{Z}$  podemos obtener particiones finitas con cualquier número de subconjuntos (existen  $k$  subconjuntos en la partición obtenida). Más adelante estudiaremos en detalle este tipo de particiones.

### 13. ESTRUCTURAS NUMÉRICAS

En este párrafo describiremos las estructuras numéricas fundamentales. Estas son:

Los números naturales

$$\mathbf{N} = \{1, 2, \dots\};$$

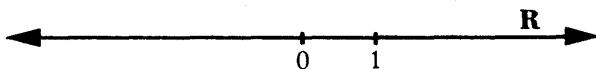
el anillo de los números enteros

$$\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\};$$

el campo de los números racionales

$$\mathbf{Q} = \left\{ \frac{b}{a} \mid a, b \in \mathbf{Z}, b \neq 0 \right\};$$

el campo de los números reales  $\mathbf{R}$  cuyos elementos son los números decimales; este se puede poner en correspondencia biyectiva con el conjunto de puntos de una recta



y el campo de los números complejos

$$\mathbf{C} = \{a + bi \mid a, b \in \mathbf{R}, i^2 = -1\}.$$

Las operaciones de suma y producto en estas estructuras satisfacen las siguientes propiedades:

1. La suma es conmutativa:  $a + b = b + a$  para todo  $a, b$ .
2. La suma es asociativa:  $(a + b) + c = a + (b + c)$  para todo  $a, b, c$ .
3. Vale la ley de la cancelación para la suma:  $a + c = b + c$  implica  $a = b$  para todo  $a, b, c$ .
4. El producto es conmutativo:  $ab = ba$  para todo  $a, b$ .
5. El producto es asociativo:  $(ab)c = a(bc)$  para todo  $a, b, c$ .
6. Vale la ley de la cancelación para el producto:  $ac = bc$  y  $c \neq 0$  implican  $a = b$  para todo  $a, b, c$ .
7. Existe un elemento neutral para el producto, 1, tal que

$$1a = a \text{ para todo } a.$$

8. El producto distribuye la suma  $a(b + c) = ab + ac$  para todo  $a, b, c$ . Excepción hecha de los números naturales, para las restantes estructuras se cumplen:

9. Existe un elemento neutral para la suma, cero, tal que

$$0 + a = a \text{ para todo } a.$$

10. Para cada  $a$  existe un inverso aditivo,  $-a$ , tal que

$$-a + a = 0.$$

Para **Q**, **R** y **C** se cumple también:

11. Para cada  $a$  existe un inverso multiplicativo,  $a^{-1}$ , tal que

$$a^{-1} \cdot a = 1.$$

En estas estructuras (excepto para los números complejos) existe también una relación de orden,  $<$ , que satisface:

12. El orden es transitivo:  $a < b$  y  $b < c$  implican  $a < c$  para todo  $a, b, c$ .

13. Vale la tricotomía para el orden:

Dados  $a$  y  $b$  se satisface una y solo una de las condiciones:

- i)  $a < b$ ;
- ii)  $a = b$ ;
- iii)  $b < a$ .

14. El orden es compatible con la suma:  $a < b$  implica  $a + c < b + c$  para todo  $a, b, c$ .

15. El orden es compatible con el producto:  $a < b$  y  $0 < c$  implican  $ac < bc$  para todo  $a, b, c$ .

Una estructura algebraica con dos operaciones que satisfacen las propiedades (1) a (10) es llamada anillo conmutativo con unitario. Si además se satisface la propiedad (11), entonces la estructura es llamada campo. Estructuras como las anteriores en las que además existe un orden que satisface las propiedades (12) a (15) se llaman anillo ordenado y campo ordenado.



# Cálculo combinatorio

ESTE capítulo consta, en primer lugar, de una presentación intuitiva de los conceptos de ordenaciones con repetición, ordenaciones, permutaciones y combinaciones.

A continuación se habla de funciones entre conjuntos finitos y se interpretan los conceptos anteriores a la luz de estas ideas. Esta exposición no requiere la lectura previa del capítulo uno.

Se termina el capítulo con el planteamiento de gran número de problemas típicos y la resolución de algunos de ellos.

## 1. EJEMPLOS ILUSTRATIVOS

Este párrafo está dedicado a ilustrar, mediante varios ejemplos, problemas y ejercicios, los conceptos de ordenaciones con repetición, ordenaciones, permutaciones y combinaciones.

**Ordenaciones con repetición.** Iniciaremos la exposición con varios ejemplos:

1. Consideremos las letras  $a, b, c$ . A cada una de las “palabras” de dos letras que se puedan formar usando exclusivamente las letras consideradas se le llama *ordenación con repetición de las letras  $a, b, c$  tomadas de dos en dos*. Aquí “palabra” no tiene el sentido usual; “palabra” quiere decir sim-

plemente una lista de letras sin que estas tengan necesariamente algún sentido o sigan alguna regla. Por ejemplo:

$$aa \quad ac \quad cb,$$

se consideran palabras. Un procedimiento útil para escribir todas estas palabras consiste en formar una tabla:

<i>c</i>	<i>ac</i>	<i>bc</i>	<i>cc</i>
<i>b</i>	<i>ab</i>	<i>bb</i>	<i>cb</i>
<i>a</i>	<i>aa</i>	<i>ba</i>	<i>ca</i>
	<i>a</i>	<i>b</i>	<i>c</i>

Es fácil convencernos que, de esta manera, hemos obtenido *todas* las palabras de dos letras con el "pequeño alfabeto" *a, b, c*. O sea, podemos afirmar que el número de ordenaciones con repetición de las letras *a, b, c* tomadas de dos en dos es nueve.

2. Supongamos que para ciertas transmisiones de tipo telegráfico se dispone de dos sonidos, uno corto, llamado punto y uno largo, llamado raya. Con estos podemos formar señales de un solo sonido, señales de dos sonidos, etc. A las señales de un sonido les llamaremos ordenaciones con repetición de los sonidos, punto, raya, tomados de uno en uno. Estas son dos:

punto                      raya  
o, simbólicamente,

— — — — — — — — — —

En forma análoga, las ordenaciones con repetición de los sonidos ., — tomados de dos en dos serán las señales de dos sonidos

. . — — . — — — —

las cuales podríamos obtener mediante una tabla como la del ejemplo 1:

<i>—</i>	<i>. —</i>	<i>— —</i>
<i>.</i>	<i>..</i>	<i>— .</i>
	<i>.</i>	<i>—</i>

Las señales de tres sonidos son las ordenaciones con repetición de ., — tomados de tres en tres. Para escribirlos todos, podríamos hacer una tabla

en la cual en un lado hemos puesto todas las señales de dos sonidos y abajo los sonidos . y —:

— —	· — —	— — —
— .	· — .	— — .
· —	· · —	— . —
..	...	— ..
	·	—

¿Por qué estas ocho señales son todas las de tres sonidos? Esto es claro, pues si consideramos una señal arbitraria de tres sonidos pueden ocurrir dos cosas: que empiece con un punto o con una raya. Si empieza con un punto los dos sonidos restantes serán una señal de dos sonidos y por lo tanto estará en la lista del lado izquierdo (pues ahí figuran todas las de dos sonidos); luego, la señal dada estará en la primera columna de la tabla. Si empieza con una raya, un razonamiento análogo indica que la señal estará forzosamente en la segunda columna.

Hemos visto así que hay ocho ordenaciones con repetición de los sonidos ., — tomados de tres en tres.

Para formar las señales de cuatro sonidos, es decir, las ordenaciones de ., — tomados de cuatro en cuatro podríamos proceder en forma análoga partiendo de las de tres sonidos (véase el ejercicio 3).

## EJERCICIOS

1. Escríbanse todas las ordenaciones con repetición de los objetos del conjunto {1, 2, 3} tomados de dos en dos.
2. ¿Cuáles son las ordenaciones con repetición de los objetos del conjunto anterior tomados de uno en uno?
3. Díganse todas las ordenaciones con repetición de los sonidos ., — tomados de cuatro en cuatro. ¿Cuántas son?
4. Escríbanse todos los números de tres cifras que se pueden formar con los dígitos 1, 2, 3. ¿Cuántos hay?
5. Escríbanse todos los números de dos cifras que se pueden formar con los dígitos 1, 2, 3, 4, 5. ¿Cuántos hay?

**OR<sub>n</sub><sup>m</sup>.** Usaremos el símbolo  $OR_n^m$  para indicar el número de ordenaciones con repetición de  $n$  objetos tomados de  $m$  en  $m$ . En los ejemplos y ejercicios anteriores puede verse que

$$OR_3^2 = 3^2, OR_4^2 = 4^2, OR_2^3 = 2^3, OR_3^3 = 3^3, OR_5^2 = 5^2.$$

Se demostrará más adelante que

$$OR_n^m = n^m.$$

**Ordenaciones.** Como antes, se ilustrará el concepto con varios ejemplos.

3. Alterando ahora la situación del párrafo anterior supongamos que con las letras  $a, b, c$  queremos formar palabras de dos letras *distintas*. Estas palabras serán

$$ab \quad ac \quad ba \quad bc \quad ca \quad cb$$

y recibirán el nombre de *ordenaciones de los objetos  $a, b, c$  tomados de dos en dos*.

4. Consideremos ahora un alfabeto de cuatro letras:  $a, b, c, d$  y formemos todas las palabras que consten de dos letras distintas. Estas serán las ordenaciones de los objetos  $a, b, c, d$  tomados de dos en dos. Obsérvese que para obtener estas basta omitir aquellas palabras del ejemplo 2 en que figuren letras repetidas. Obtenemos:

$$ab \quad ac \quad ad \quad ba \quad bc \quad bd \quad ca \quad cb \quad cd \quad da \quad db \quad dc.$$

De las  $OR_4^2$  ordenaciones con repetición que se tenían se omitieron  $aa, bb, cc, dd$ . Por consiguiente el número de ordenaciones de cuatro objetos tomados de dos en dos es  $4^2 - 4 = 4(4-1) = 4 \cdot 3 = 12$ .

Cuando se hable de las ordenaciones de los objetos de un conjunto con  $n$  elementos tomados de  $m$  en  $m$  se supondrá siempre que  $m \leq n$  pues en caso contrario no habría ninguno, ya que una lista con  $m$  elementos tomados de un conjunto de  $n$  elementos tiene necesariamente repeticiones si  $m > n$ .

**$O_n^m$ .** Usaremos el símbolo  $O_n^m$  para indicar el número de ordenaciones de  $n$  elementos tomados de  $m$  en  $m$ . Así pues, en los dos ejemplos anteriores se tiene que

$$O_3^2 = 3^2 - 3 = 3 \cdot 2 = 6, \quad O_4^2 = 4 \cdot 3 = 12.$$

Se demostrará más adelante que

$$O_n^m = n(n-1)(n-2) \cdots (n-m+1)$$

(este símbolo,  $O_n^m$ , está definido únicamente cuando  $n \geq m$ ).

La fórmula anterior debe interpretarse como sigue:  $O_n^m$  es el producto de todos los números naturales entre  $n$  y  $(n-m+1)$  inclusivo; es decir, de los  $m$  factores de la forma  $n-i$  en donde  $i = 0, 1, 2, \dots, m-1$ .

Por ejemplo,  $O_5^1 = 5$ ,  $O_5^2 = 5 \cdot 4$ ,  $O_5^3 = 5 \cdot 4 \cdot 3$ ,  $O_5^4 = 5 \cdot 4 \cdot 3 \cdot 2$ ,  $O_5^5 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ .

Como casos especiales, se tiene

$$O_n^1 = n, O_n^n = n(n-1) \cdots 2 \cdot 1.$$

## EJERCICIOS

**6.** Escríbanse todas las palabras de tres letras distintas que se pueden formar con las letras  $a, b, c, d$ . ¿Cuántas hay? Verifíquese la fórmula para este caso.

**7.** Escríbanse todos los números de dos cifras distintas que se pueden formar con los dígitos  $1, 2, 3, 4, 5$ . Cuéntense cuántos hay y verifíquese el valor de  $O_5^2$ .

**8.** ¿Qué señales de tres símbolos distintos pueden formarse con los elementos de  $\{., —, \sim\}$ ? Compruébese que hay  $O_3^3$  señales.

**9.** ¿Cuáles son los números de tres cifras distintas que se pueden formar con los dígitos  $1, 2, 3, 4$ ? Compruébese la validez de la fórmula para este caso.

**10.** ¿De cuántas formas ordenadas puede llenarse un estante de tres lugares si se dispone de cuatro libros distintos? Escríbanse todas las ordenaciones de estos. Contéstese la misma pregunta si el estante tiene 7 lugares y se dispone de 11 libros.

**11.** Si disponemos de cuatro lienzos de diferente color y queremos formar banderas bicolores, ¿cuántas banderas es posible obtener?

**12.** Usando la relación  $OR_n^2 = n^2$  demuéstrese que  $O_n^2 = n(n-1)$ . (Recuérdese el ejemplo 4 de este párrafo).

**13.** Calcúlese

$$O_6^2, O_7^5, O_4^4, O_{100}^3, O_{1002}^3, O_n^3, O_q^5.$$

**14.** Compruébese que

$$O_7^4 O_3^3 = O_7^7,$$

$$O_9^5 O_4^2 O_2^2 = O_9^9,$$

$$O_n^{n-1} = O_n^n.$$

**15.** Encuéntrese el valor de  $n$  si:

a)  $O_n^2 = 42$ .

b)  $O_n^3 = 120$ .

c)  $O_7^n = 210$ .

**Permutaciones.** A las ordenaciones de un conjunto de  $n$  elementos, tomados de  $n$  en  $n$ , se les llama *permutaciones* de los  $n$  elementos. Por ejemplo:

5. Las permutaciones de  $\{a, b, c\}$  son las palabras de tres letras en las que no haya repetición de letras. Estas son:

$$abc \quad acb \quad bac \quad bca \quad cab \quad cba.$$

6. Las banderas bicolores que se pueden hacer con los colores blanco y verde son las permutaciones de los colores blanco y verde:

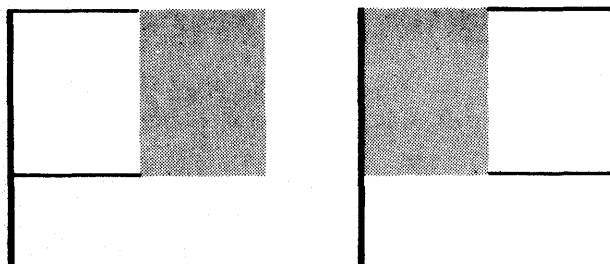


Figura 2.1

**P<sub>n</sub>, n!** El símbolo  $P_n$  denotará el número de permutaciones de un conjunto de  $n$  elementos. De la fórmula dada para el número de ordenaciones se obtiene

$$P_n = O_n^n = n(n-1) \dots 2 \cdot 1 = 1 \cdot 2 \dots n.$$

Es decir,  $P_n$  es el producto de los  $n$  primeros números naturales. Este producto se acostumbra denotar por  $n!$ , es decir, se tiene que

$$P_n = n! = 1 \cdot 2 \cdot 3 \dots n$$

y recibe el nombre de *factorial de n*. Por ejemplo,

$$\begin{aligned} 1! &= 1, 2! = 2, 3! = 6, 4! = 24, 5! = 120 \\ 6! &= 720, 7! = 5\,040, 8! = 40\,329, 9! = 326\,880. \end{aligned}$$

Obsérvese que

$$n! = (n-1)! \cdot n.$$

## EJERCICIOS

16. Escríbanse todas las palabras de tres letras distintas que se pueden formar con las letras  $a, b, c$ .

17. Escríbanse todos los números de cuatro cifras distintas que se pueden formar con los dígitos 2, 4, 6, 8.

18. El número de permutaciones de los elementos de  $\{a, b, c, d, e\}$  es 120. Escríbanse 10 de ellas.

**19.** ¿De cuántas maneras podemos colocar diez libros distintos en un estante que tiene 10 lugares?

**20.** En los ejercicios 16, 17 y 18 compruébese la validez de la fórmula para  $P_n$ .

**21.** ¿De cuántas maneras se pueden distribuir 15 libros diferentes entre 15 alumnos?

**22.** Un matemático tiene lugar en su casa para guardar 5 automóviles. Si tiene un Bentley, un Ferrari, un Aston Martin, un Maserati y un Stutz, ¿de cuántas maneras puede guardarlos?

**23.** Calcúlese

$$P_{11}, P_{29}/P_{27}, P_4 P_{12}/P_{16}, (n-1)!/n!, n!/(n-2)!$$

**24.** Compruébese que

$$O_7^4 P_3 = P_7 \quad 7! + 8! = 7! \cdot 9$$

$$1\ 003! + 1\ 004! + 1\ 005! = 1\ 003! \cdot 1\ 005^2.$$

**25.** a) ¿Cuál es el valor de  $n$  si  $n! = 39\ 916\ 800$ ?

b) ¿Existe un número natural  $n$  tal que  $n! = 5\ 820$ ?

c) Demuéstrese que

$$n! + (n+1)! = n!(n+2),$$

$$n! + (n+1)! + (n+2)! = n!(n+2)^2.$$

**Combinaciones.** Si  $A$  es un conjunto con  $n$  elementos, los subconjuntos de  $A$  que constan de  $m$  elementos se llaman también *combinaciones de los  $n$  elementos de  $A$  tomados de  $m$  en  $m$* .

Ilustraremos esta definición con ejemplos.

7. Las combinaciones de los elementos del conjunto  $\{a, b, c\}$  tomados de dos en dos son los subconjuntos de  $\{a, b, c\}$  que tienen dos elementos. Es decir, son:

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

Las combinaciones de los mismos tomados de uno en uno son

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

y tomados de 3 en 3 hay una sola, que es  $\{a, b, c\}$ .

8. Una situación típica en donde aparece el concepto de combinación se presenta al considerar las comisiones que consten, por ejemplo, de tres personas que se puedan elegir entre cinco candidatos. Cada una de estas comisiones es, en efecto, un subconjunto de tres elementos, del conjunto formado por los cinco candidatos.

Denotando con 1, 2, 3, 4, 5 a los candidatos, las comisiones posibles son

$$\begin{aligned} &\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \\ &\{1, 4, 5\}, \{2, 3, 4\}, \{2, 3, 5\}, \{2, 4, 5\}, \{3, 4, 5\}. \end{aligned}$$

Así pues, el número de combinaciones de 5 elementos tomados de 3 en 3 es 10.

9. Si en el ejemplo anterior suponemos que uno de los candidatos no es elegible, para obtener todas las comisiones posibles de tres personas, basta considerar aquellas de la lista anterior en que no figure la persona no elegible. Si la no elegible es, por ejemplo la 5, las comisiones posibles son

$$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}.$$

Por tanto la respuesta es el número de combinaciones de cuatro elementos tomados de 3 en 3 que es 4.

**C<sub>n</sub><sup>m</sup>.** El número de combinaciones de  $n$  elementos tomados de  $m$  en  $m$ ; es decir, el número de subconjuntos con  $m$  elementos de un conjunto de  $n$  elementos se denota con  $C_n^m$ . Se probará más adelante que

$$C_n^m P_m = O_n^m$$

o bien, explícitamente,

$$C_n^m = \frac{n(n-1) \dots (n-m+1)}{1 \cdot 2 \dots m},$$

o también,

$$C_n^m = \frac{n!}{m!(n-m)!}.$$

Nótese que al hablar de combinaciones de  $n$  elementos tomados de  $m$  en  $m$ , el número  $m$  es menor o igual que  $n$ .

## EJERCICIOS

26. ¿Cuántos equipos de basquetbol se pueden formar de un grupo de 9 jugadores? (Un equipo consta de cinco jugadores.)

27. Sea  $A = \{a, b, c, d, e\}$ . Escríbanse todos los subconjuntos de  $A$  y dedúzcanse los valores  $C_5^1, C_5^2, C_5^3, C_5^4$  y  $C_5^5$ .

28. El juego de dominó consta de 28 fichas y una mano consta de 7 fichas. ¿De cuántas formas se puede seleccionar una mano?

29. ¿De cuántas maneras puede seleccionarse una patrulla de 3 entre 10 soldados?

30. Una mano de póker consta de cinco cartas. ¿Cuántas manos de póker diferentes hay? (La baraja tiene 52 cartas.)

31. Una mano de bridge consta de 13 cartas. ¿Cuántas manos posibles hay?

32. Calcúlese

$$C_9^4, C_9^5, C_{15}^3, C_{15}^{12}, C_{1002}^2, C_{1002}^{1000}.$$

**33.** Compruébese que

$$C_{11}^7 = C_{11}^4 \quad C_{11}^7 = \frac{11!}{7!4!}$$

$$C_6^1 + C_6^2 + C_6^3 + C_6^4 + C_6^5 + C_6^6 = 2^6 - 1.$$

**34.** Compruébese que

$$C_8^3 + C_8^4 = C_9^4, \quad C_{10}^4 + C_{10}^5 = C_{11}^5,$$

$$C_7^3 + C_7^2 + C_8^2 = C_9^3.$$

**35.** Encuéntrense los valores de  $n$  si

$$C_n^3 = 220 \quad C_{n-1}^4 = 15 \quad C_n^3 = 364 \quad 5C_{n+1}^5 = 8C_n^4.$$

## 2. FUNCIONES

LA GRAN importancia que el concepto de función juega en las matemáticas se debe a que casi cada situación de la experiencia diaria es susceptible de ser interpretada como una función. Citaremos a continuación varios ejemplos simples en los cuales se exhibe la forma en que se pueden lograr tales interpretaciones y obtener funciones de ciertos conjuntos en otros. Al mismo tiempo iremos recordando la terminología y notación usuales.

### Ejemplos:

1. Sea  $A$  el conjunto de los alumnos de cierto grupo de una escuela, y  $B$  el conjunto de bancas que hay en su salón. Supongamos que a cada alumno se le ha asignado un lugar en el salón. Esto puede interpretarse como una función  $A \rightarrow B$  en que a cada alumno (es decir, a cada elemento del conjunto  $A$ ) se le asocia una determinada banca (es decir, un elemento del conjunto  $B$ ). Convenimos que a varios alumnos se les puede asociar la misma banca, pero que a un mismo alumno no se le pueden asignar dos bancas distintas. (Si esto último ocurriera no diríamos que se trata de una función de  $A$  en  $B$ .)

2. Si llamamos ahora  $A$  al conjunto de las once casas que hay en el Callejón del Sapo y  $N$  es el conjunto de los números naturales, cierta oficina del Departamento Central se ocupa de establecer una función  $f: A \rightarrow N$  al asignar a cada casa (es decir, a cada elemento del conjunto  $A$ ) su "número oficial" (un elemento de  $N$ ). Aun cuando en dicha oficina se equivocaran y a dos o más casas distintas les dieran el mismo número seguiríamos diciendo que se trata de una función de  $A$  en  $B$ . Pero si la

equivocación consistiera en asignarle dos o más números a una misma casa, entonces diríamos que dicha asignación no es una función de  $A$  en  $B$ .

3. El encargado de un equipo de beisbol debe, al principiar cada partido, decidir qué posiciones ocuparán sus jugadores en el campo. Las posiciones son las de lanzador ( $p$ ), receptor ( $c$ ), primera base ( $1b$ ), segunda base ( $2b$ ), parador en corto ( $ss$ ), tercera base ( $3b$ ), jardinero izquierdo, ( $lf$ ), jardinero central ( $cf$ ) y jardinero derecho ( $rf$ ). Supongamos que el equipo consta de 17 jugadores identificables por sus números del 1 al 17. Si llamamos  $A$  al conjunto de las posiciones, es decir,

$$A = \{p, c, 1b, 2b, ss, 3b, lf, cf, rf\}$$

y  $B = \{1, 2, \dots, 17\}$  al de los jugadores, lo que hace el encargado es establecer una función de  $A$  en  $B$ . Por ejemplo, la siguiente lista o tabla nos da una de estas funciones:

posiciones	jugadores
$p$	15
$c$	13
$1b$	10
$2b$	1
$ss$	9
$3b$	12
$lf$	3
$cf$	6
$rf$	8

4. Es frecuente tener que formar parejas (ordenadas) de objetos de cierto conjunto, por ejemplo parejas de números enteros como  $(2, 5)$ ,  $(-7, 3)$ ,  $(3, 0)$ . Veamos cómo cada pareja puede interpretarse como una función. Sea  $A$  el conjunto que conste de dos objetos:

$$A = \{\text{primer lugar, segundo lugar}\}$$

y  $\mathbf{Z}$  el conjunto de los enteros. La pareja  $(2, 5)$  puede interpretarse como la función que asigna al primer lugar el 2 y al segundo el 5; la pareja  $(-7, 3)$  es la función que asocia  $-7$  al primer lugar y 3 al segundo.

Observemos en estos ejemplos que la pareja  $(7, 7)$  es la función que al primer lugar le asocia el 7 y al segundo lugar también le asocia el mismo número 7. Es decir, a dos elementos distintos de  $A$  podemos asociar un mismo elemento de  $B$ . Lo que no podemos hacer es asociar a un elemento

de  $A$  dos o más elementos de  $B$ . Lo que obtendríamos no se llamaría función; no sería una pareja.

5. *El producto cartesiano de dos conjuntos.* Recordemos que el producto cartesiano  $A \times B$  de dos conjuntos  $A$  y  $B$  es el conjunto de parejas [ordenadas]  $(a, b)$  tales que  $a$  es un elemento de  $A$  y  $b$  un elemento de  $B$ , es decir,

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

Si designamos ahora con  $C$  el conjunto {primer lugar, segundo lugar} o, por abreviar  $C = \{1, 2\}$ , vemos que los elementos del producto cartesiano, es decir las parejas  $(a, b)$  mencionadas, pueden interpretarse como funciones

$$f: C \rightarrow A \times B$$

tales que  $f(1) \in A$  y  $f(2) \in B$ . De esta forma, los elementos de un producto cartesiano pueden pensarse como funciones.

6. Como último ejemplo podemos dar la función de  $\mathbf{Z}$  en  $\mathbf{Z}$  que a cada entero asocia un cuadrado, es decir, dada por

$$n \mapsto n^2.$$

**Funciones; notación.** Observemos que en todos los ejemplos anteriores, al hablar de una función hemos dispuesto siempre de un conjunto  $A$  (alumnos en el primero, casas en el segundo, posiciones en el tercero, primero y segundo lugares en el cuarto y  $\mathbf{Z}$  en el quinto) y cierta forma en que a cada elemento de  $A$  se le ha asociado un elemento de  $B$ . Como se mencionó en el capítulo primero, al primer conjunto se le acostumbra llamar el *dominio* de la función, al segundo el *codominio* y es usual la notación

$$f: A \rightarrow B$$

para indicar que  $f$  es una función de  $A$  en  $B$ , es decir, con dominio  $A$  y codominio  $B$ . Si al elemento  $a$  de  $A$  le corresponde el elemento  $b$  de  $B$  escribimos  $f(a) = b$  o también  $a \mapsto b$ . Por ejemplo, si  $f$  es la función de la tabla del ejemplo 3, podemos escribir  $f(p) = 15$ ,  $f(c) = 13$ ,  $f(1b) = 10$ , etcétera. En el caso de la pareja  $(-7, 3)$  del ejemplo 4 si  $f$  es la función que determina esta pareja, podríamos escribir

$$f(\text{primer lugar}) = -7. \quad f(\text{segundo lugar}) = 3.$$

Dos funciones  $f$  y  $g$  se consideran iguales si tienen el mismo dominio y el mismo codominio, es decir, si las dos son funciones de un mismo conjunto  $A$  en un mismo conjunto  $B$  y para todo elemento  $a$  de  $A$ ,  $f(a) = g(a)$ .

En el cálculo combinatorio y sus numerosas aplicaciones [y muy en especial en el cálculo de probabilidades (caso discreto)] se trabaja constantemente con funciones de conjuntos finitos en conjuntos finitos. También en otras ramas de las matemáticas, como por ejemplo, la teoría de grupos y sus importantes aplicaciones, el papel que juega este tipo de funciones es de singular interés.

### Más ejemplos:

Daremos a continuación varios ejemplos más y una notación que se usará a lo largo de este capítulo.

7. Sea  $A$  el conjunto que consta de los elementos 1, 2, 3 y  $B$  el formado por las letras  $a, b, c, d$ . Es decir,

$$A = \{1, 2, 3\} \quad B = \{a, b, c, d\}.$$

Si, como ejemplo, la función  $f: A \rightarrow B$  está dada por

$$f(1) = a, \quad f(2) = d, \quad f(3) = c,$$

o bien por la tabla

$A$	$B$
1	$a$
2	$d$
3	$c$

será muy cómoda, en lo que sigue, la notación

$$f = \begin{pmatrix} 1 & 2 & 3 \\ a & d & c \end{pmatrix}.$$

Es decir, en el primer renglón escribimos (no importa en qué orden) todos los elementos del dominio y debajo de cada uno de ellos los elementos del codominio que les corresponden según la función. O sea, la función anterior la podemos escribir también en las formas

$$f = \begin{pmatrix} 2 & 1 & 3 \\ d & a & c \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ c & d & a \end{pmatrix} = \dots$$

Una expresión de la forma

$$\begin{pmatrix} 1 & 2 & 2 & 3 \\ a & c & b & d \end{pmatrix}$$

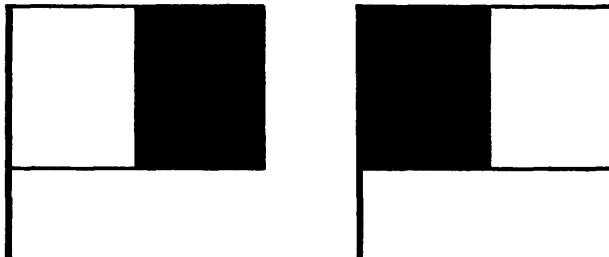
no representa función alguna pues al mismo elemento 2 de  $A$  se le han asociado dos elementos distintos de  $B$ . Si recordamos lo dicho en el capítulo uno, esta expresión representa una relación (que no es función), a saber, la formada con las parejas  $(1, a)$ ,  $(2, c)$ ,  $(2, b)$  y  $(3, d)$ . Tampoco

$$\begin{pmatrix} 2 & 3 \\ d & a \end{pmatrix}$$

representa una función de  $A$  en  $B$ , pues no hemos dicho qué elemento de  $B$  debe asociársele al elemento 1 de  $A$  (es, de nuevo, simplemente una relación). Esta última expresión define, sin embargo, una función del conjunto  $\{2, 3\}$  en  $B$ .

8. Muchas veces en el cálculo combinatorio y en el cálculo de probabilidades necesitaremos contar cuántas funciones de cierto tipo podemos definir de un conjunto en otro. Por ejemplo, supongamos que se nos pide encontrar cuántas señales en forma de banderas bicolores podemos formar si disponemos de tres colores, digamos, blanco, verde y rojo.

Creemos conveniente aquí observar que en este tipo de problemas lo primero que se debe hacer es aclarar bien los datos del enunciado. Por ejemplo, en este caso debemos especificar que por "banderas bicolores" entendemos que sean con dos colores *distintos*. Además debemos aclarar si dos banderas como las siguientes



**Figura 2.2**

las consideramos iguales o no (por ejemplo, para cierto tipo de señales, en donde el asta no se pueda observar bien desde lejos y donde el aire pueda "voltear" la bandera), ambas señales convendría considerarlas como la misma. Para los efectos de este ejemplo supondremos que estas son distintas.

¿Cómo interpretar cada bandera de estas como una función?

Sea  $A = \{1, 2\}$  indicando con 1 (para abreviar la notación) el lugar de la bandera junto al asta y con 2 el otro lugar. Sea  $B = \{b, v, r\}$  indicando los colores con sus iniciales. Las banderas dibujadas antes se pueden interpretar como las funciones

$$\begin{pmatrix} 1 & 2 \\ v & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ b & v \end{pmatrix}$$

respectivamente. Las funciones

$$\begin{pmatrix} 1 & 2 \\ r & v \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ b & b \end{pmatrix}$$

representarían la rojiverde y la blanca-blanca, pero hemos convenido en no considerar esta última como bandera bicolor. Podemos hacer fácilmente la lista de *todas* las funciones de  $A$  en  $B$ :

$$\begin{pmatrix} 1 & 2 \\ b & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ b & v \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ b & r \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ v & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ v & v \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ v & r \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ r & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ r & v \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ r & r \end{pmatrix}.$$

De estas, las que representan banderas bicolors, según los convenios que hemos hecho, son

$$\begin{pmatrix} 1 & 2 \\ b & v \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ b & r \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ v & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ v & r \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ r & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ r & v \end{pmatrix},$$

o sea

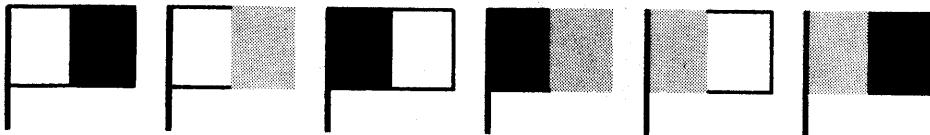


Figura 2.3

Es decir, hay seis banderas.

Este ejemplo, aun cuando pueda parecer demasiado sencillo, es típico del cálculo combinatorio y nos servirá además para iniciar la discusión, en el próximo párrafo, de ciertos tipos especiales y muy importantes de funciones.

## EJERCICIOS

1. La mesa directiva de un club que tiene 50 socios consta de un presidente, un secretario y un tesorero. Interprétese como función la elección de una mesa directiva. ¿Cuál es el dominio y el codominio? Déñese ejemplos de algunas de estas funciones.

**2.** Interprétese como función el resultado de un examen en un grupo de alumnos. Si las calificaciones son del 0 al 10 y el grupo consta de 15 alumnos describáse el dominio, el codominio y dése un ejemplo.

**3.** Utilizando el símbolo introducido en el ejemplo 7 para denotar funciones de conjuntos finitos en conjuntos finitos, escríbanse todas las funciones del conjunto  $A = \{x, y, z\}$  en el conjunto  $B = \{a, b\}$ . Escríbanse también todas las funciones del conjunto  $B$  en el conjunto  $A$ .

**4.** Bajo las mismas condiciones del ejemplo 8 interprétese como funciones las banderas tricolores. ¿Pueden dibujarse todas y decirse cuántas hay?

(Los ejercicios siguientes puede omitirlos el lector que haya estudiado el capítulo uno.)

**5.** Si  $A = \{1, 2, 3, 4\}$  y  $B = \{x, y, z\}$ , ¿cuáles de los símbolos siguientes representan funciones de  $A$  en  $B$ ? Explíquese por qué.

$$\begin{pmatrix} 2 & 3 & 4 \\ x & y & z \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ x & y & z & z \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ x & y & z & t \end{pmatrix} \quad \begin{pmatrix} 3 & 1 & 2 & 4 \\ z & x & y & z \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ x & x & x & x \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 1 \\ x & y & y & z & z \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & x & y & x \end{pmatrix}$$

¿Hay dos funciones iguales en esta lista?

**6.** Una función  $f: A \rightarrow B$  se llama *constante* si a todos los elementos de  $A$  se les asocia un mismo elemento de  $B$ . Por ejemplo si  $A = \{1, 2, 3, 4\}$  y  $B = \{a, b, c, d, e\}$ , la función

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ c & c & c & c \end{pmatrix}$$

es una función constante. ¿Cuántas funciones constantes de  $A$  en  $B$  hay en este ejemplo? ¿Cuántas funciones constantes hay de  $B$  en  $A$ ?

**7.** Sea  $A$  un conjunto arbitrario no vacío y  $B$  un conjunto con  $n$  elementos. ¿Cuántas funciones constantes hay de  $A$  en  $B$ ?

**8.** Dénsese ejemplos de funciones constantes de un conjunto arbitrario no vacío  $A$  en  $\mathbf{N}$  y de  $A$  en  $\mathbf{Z}$ . Obsérvese que cada función constante queda determinada por un número de  $\mathbf{N}$  o de  $\mathbf{Z}$ , respectivamente.

**9.** Es frecuente, para funciones, usar figuras como la que sigue para describir la función de  $A = \{1, 2, 3, 4, 5\}$  en  $B = \{a, b, c, d\}$  dada por

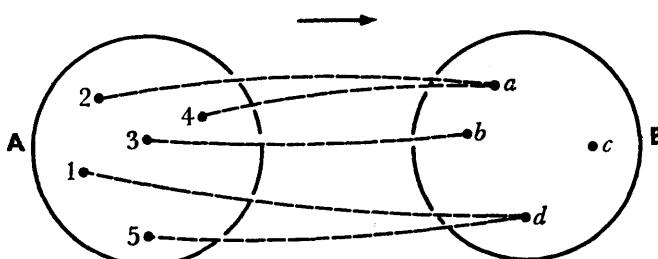


Figura 2.4

$f(1) = d, f(2) = a, f(3) = b, f(4) = a, f(5) = d$ . ¿Cuáles de las figuras siguientes representan funciones de  $A$  en  $B$ ? Explíquese por qué. ¿Es alguna de ellas constante?

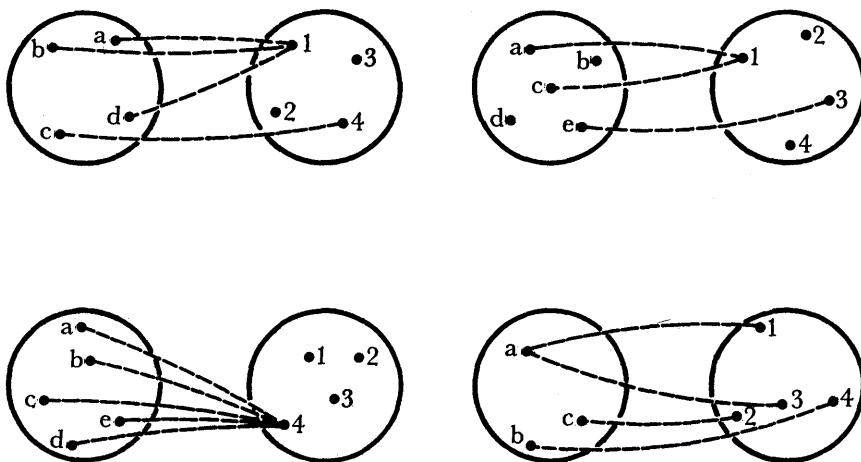


Figura 2.5

10. Escríbanse todos los elementos del producto cartesiano  $A \times B$  si  $A = \{1, 2\}$ ,  $B = \{a, b, c\}$ . Lo mismo para  $A = \{1, 2, 3, 4\}$ ,  $B = \{a, b\}$ .

11. Extiéndase el ejemplo 5 al caso del producto cartesiano  $A \times B \times C$  de tres conjuntos  $A$ ,  $B$  y  $C$ .

### 3. FUNCIONES INYECTIVAS, SUPRAYECTIVAS Y BIYEKTIVAS \*

**Definiciones.** Sea  $f: A \rightarrow B$  una función de un conjunto  $A$  en un conjunto  $B$ . Se tienen las siguientes definiciones:

*La función  $f$  es inyectiva si, dados dos elementos arbitrarios  $a, a'$  en  $A$  tales que  $a \neq a'$ , entonces  $f(a) \neq f(a')$ .*

*La función  $f$  es suprayectiva si dado un elemento arbitrario  $b$  en  $B$  existe un elemento  $a$  en  $A$  tal que  $f(a) = b$ .*

*Si una función es inyectiva y suprayectiva entonces se dice que es biyectiva.*

A continuación daremos ejemplos que aclaren estas tres definiciones y mencionaremos varios problemas, en cuya solución se empleen:

\* Este párrafo puede omitirse si ya se ha estudiado previamente el capítulo uno.

1. Empecemos analizando con más detenimiento el ejemplo 8 del párrafo anterior. Hay 9 funciones del conjunto  $A = \{1, 2\}$  de los lugares en el conjunto  $B = \{b, v, r\}$  de los colores. De ellas, las siguientes tres

$$\begin{pmatrix} 1 & 2 \\ b & b \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ v & v \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ r & r \end{pmatrix},$$

no son inyectivas, pues a los lugares 1 y 2 les corresponde, en cada caso, un mismo color. No así las seis funciones restantes del ejemplo. En ellas a los lugares distintos 1 y 2 les corresponden, en cada caso, colores distintos.

O sea, hablando en los nuevos términos, en el problema del ejemplo 8, lo que se trata es de encontrar todas las funciones *inyectivas* del conjunto  $A$  en el conjunto  $B$ .

Siguiendo, podemos preguntarnos: ¿qué funciones de las 9 ahí dadas son suprayectivas? La respuesta es que ninguna de ellas. Por ejemplo en la función

$$\begin{pmatrix} 1 & 2 \\ r & b \end{pmatrix}$$

el elemento  $v$  de  $B$  no es imagen ni de 1 ni de 2. Es claro que si hay tres colores y las banderas son bicolores siempre sobrará un color.

2. En el ejercicio 3 del párrafo anterior se vio que hay 8 funciones de un conjunto  $A = \{x, y, z\}$  de tres elementos en un conjunto  $B = \{a, b\}$  de los elementos. Estas son

$$\begin{pmatrix} x & y & z \\ a & a & a \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ a & a & b \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ a & b & a \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ b & a & a \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ a & b & b \end{pmatrix} \\ \begin{pmatrix} x & y & z \\ b & a & b \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ b & b & a \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ b & b & b \end{pmatrix}.$$

Ninguna de estas es inyectiva. Por ejemplo en la tercera, a los elementos  $x, z$  les corresponde un mismo elemento  $a$ .

¿Cuáles de las funciones anteriores son suprayectivas? Todas, menos

$$\begin{pmatrix} x & y & z \\ a & a & a \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ b & b & b \end{pmatrix},$$

pues en cada una de las restantes tanto  $a$  como  $b$  son siempre imágenes de algún elemento de  $A$ .

Es conveniente, antes de continuar con los ejemplos, decir en otras palabras, qué significa que una función sea inyectiva y, respectivamente, suprayectiva.

Una función es *inyectiva* si *a elementos distintos del dominio le corresponden elementos distintos del codominio*. Dicho aun de otra manera, *si dos elementos  $x, y$  del dominio se transforman en un mismo elemento del codominio*, es decir, si  $f(x) = f(y)$  entonces forzosamente  $x = y$ .

Que una función sea *suprayectiva* significa que *todo elemento del codominio es imagen de algún elemento del dominio* (puede serlo de más de uno).

Por tanto, podemos decir que una función es *biyectiva* si *todo elemento del codominio es imagen de uno y solamente un elemento del dominio*.

Continuemos con los ejemplos.

3. La función  $f: \mathbf{Z} \rightarrow \mathbf{Z}$  dada por  $f(n) = 2n$  es inyectiva. En efecto, si  $m, n \in \mathbf{Z}$  y  $f(m) = f(n)$  entonces  $2m = 2n$ , de donde  $m = n$ .

Esta función no es suprayectiva. Por ejemplo, 7 no es imagen de ningún elemento de  $\mathbf{Z}$ , pues si  $f(m) = 7$ ,  $2m = 7$  y  $m = 7/2$  sería un entero, lo cual no es cierto. De hecho, ningún entero impar es imagen bajo  $f$  de algún elemento de  $\mathbf{Z}$ .

4. Si  $A = \{a, b, c\}$ ,  $B = \{x, y, z\}$ , la función

$$\begin{pmatrix} a & b & c \\ z & x & y \end{pmatrix}$$

es inyectiva y suprayectiva. Podemos decir entonces que esta función es *biyectiva*. (Como comentario podemos afirmar que las funciones de los ejemplos 1, 2 y 3 no son biyectivas, pues o bien no son inyectivas o no son suprayectivas.)

5. La función  $f: \mathbf{Z} \rightarrow \mathbf{Z}$  dada por  $f(n) = n + 1$  es biyectiva.

En efecto,  $f$  es inyectiva, pues si  $f(m) = f(n)$ , entonces  $m + 1 = n + 1$ , de donde  $m = n$ . Además es suprayectiva, pues si  $n$  es un elemento arbitrario del codominio, es decir, si  $n \in \mathbf{Z}$ , existe un elemento en el dominio, a saber,  $n - 1 \in \mathbf{Z}$  tal que  $f(n - 1) = (n - 1) + 1 = n$ .

6. La función  $f: \mathbf{N} \rightarrow \mathbf{N}$  dada por la misma fórmula del ejemplo anterior, es decir, por  $f(n) = n + 1$  es inyectiva pero no suprayectiva. La demostración de que es inyectiva es igual que antes. No es suprayectiva, pues siendo  $\mathbf{N} = \{1, 2, 3, \dots\}$ , no hay en  $\mathbf{N}$  ningún elemento de  $n$  tal que  $f(n) = 1$ .

7. Si  $A$  es un conjunto arbitrario, podemos siempre definir una función de  $A$  en  $A$ , llamada la función idéntica y que se denota por  $1_A: A \rightarrow A$  asociando a cada elemento de  $A$  el mismo, es decir,  $1_A(a) = a$  para toda  $a \in A$ . Esta función es evidentemente biyectiva.

Si  $f: A \rightarrow B$  es una función de  $A$  en  $B$  es usual llamar *imagen* de  $f$  al conjunto de todos los elementos de  $B$  que sean imagen, bajo  $f$ , de algún

elemento de  $A$ . Por ejemplo si  $f: \mathbf{Z} \rightarrow \mathbf{Z}$  es la función dada por  $f(n) = 2n$ , la imagen de  $f$  es el conjunto de todos los números pares.

Con este lenguaje podemos decir que una función es *suprayectiva* si su imagen es igual a todo el codominio.

## EJERCICIOS

1. Sea  $A = \{a, b, c, d\}$ ,  $B = \{1, 2, 3, 4\}$ . ¿Cuáles de las funciones siguientes son inyectivas, suprayectivas o biyectivas?

$$\begin{pmatrix} a & b & c & d \\ 1 & 3 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} a & b & c & d \\ 1 & 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} a & b & c & d \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} a & b & c & d \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

2. Para los conjuntos  $A$  y  $B$  del ejercicio anterior, ¿se puede encontrar una función que sea inyectiva pero no suprayectiva?

3. Sean  $A$  un conjunto con  $m$  elementos y  $B$  un conjunto con  $n$  elementos tales que existe una función inyectiva  $f:A \rightarrow B$ . ¿Qué relación de orden existe entre  $m$  y  $n$ ?

4. Sean  $A$  y  $B$  como en el ejercicio anterior, pero tales que existe ahora una función suprayectiva  $f:A \rightarrow B$ . ¿Qué relación de orden hay entre  $m$  y  $n$ ?

5. Si  $A$  y  $B$  son como en los dos ejercicios anteriores y existe una función biyectiva  $f:A \rightarrow B$ , ¿cómo son  $m$  y  $n$ ?

6. Sea  $f: \mathbf{Z} \rightarrow \mathbf{Z}$  la función dada por  $f(n) = 2n - 3$ . ¿Es inyectiva esta función? ¿Es suprayectiva?

7. Sea  $f: \mathbf{N} \rightarrow \mathbf{N}$  la función dada por  $f(n) = n + 5$ . ¿Es inyectiva esta función? ¿Es suprayectiva?

8. Sea  $f: \mathbf{Z} \rightarrow \mathbf{Z}$  la función dada por  $f(n) = n + 5$ . ¿Es inyectiva esta función?

## 4. ORDENACIONES, PERMUTACIONES Y COMBINACIONES

En el primer párrafo de este capítulo se introdujeron, de una manera un tanto informal, los conceptos de ordenaciones con repetición, ordenaciones, etc. Ahora definiremos estos conceptos y además demostraremos las fórmulas para calcular los números  $OR_n^m$ ,  $O_n^m$  y  $C_n^m$ .

**Ordenaciones con repetición.** Designaremos de aquí en adelante con  $I_m$  al conjunto de los  $m$  primeros números naturales, es decir,

$$I_m = \{1, 2, \dots, m\}.$$

Sea  $A$  un conjunto con  $n$  elementos. Las ordenaciones con repetición de los elementos de  $A$  tomados de  $m$  en  $m$  son las funciones  $f:I_m \rightarrow A$ .

Revisemos algunos ejemplos:

1. En el ejemplo 2 del párrafo 1 se consideraron las señales formadas con los sonidos ., —. Estas señales pueden considerarse como ordenaciones con repetición de los objetos ., —. Por ejemplo, las señales de tres sonidos serán las ordenaciones con repetición de dichos sonidos tomados de tres en tres. Escritos en forma de funciones, estas son:

$$\begin{array}{c} \left( \begin{matrix} 1 & 2 & 3 \\ . & . & . \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 & 3 \\ . & . & - \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 & 3 \\ . & - & . \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 & 3 \\ . & - & - \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 & 3 \\ - & . & . \end{matrix} \right) \\ \left( \begin{matrix} 1 & 2 & 3 \\ - & . & - \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 & 3 \\ - & - & . \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 & 3 \\ - & - & - \end{matrix} \right) \end{array}$$

2. Las ordenaciones con repetición de los elementos del conjunto  $\{x, y, z\}$  tomados de dos en dos son las funciones de  $I_2$  en  $A$ , es decir,

$$\begin{array}{c} \left( \begin{matrix} 1 & 2 \\ x & x \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ x & y \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ x & z \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ y & x \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ y & y \end{matrix} \right) \\ \left( \begin{matrix} 1 & 2 \\ y & z \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ z & x \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ z & y \end{matrix} \right) \quad \left( \begin{matrix} 1 & 2 \\ z & z \end{matrix} \right) \end{array}$$

Estas ordenaciones con repetición no son otra cosa, más que las parejas ordenadas de elementos de  $A$ . Ellas constituyen el producto cartesiano  $A \times A$  y se les acostumbra denotar simplemente con  $(x, x)$ ,  $(x, y)$ , etcétera.

En forma análoga, a las ordenaciones con repetición de los elementos de  $A$  tomados de tres en tres se les suele llamar *ternas* (ordenadas, desde luego) de elementos de  $A$ .

En general, a las ordenaciones con repetición de elementos de  $A$  tomados de  $m$  en  $m$  se les llama *familias de  $m$  elementos* de  $A$  o también *sucesiones finitas* de  $m$  elementos (de  $A$ ).

Cuando se usa esta terminología, es frecuente escribir, en lugar de la función

$$\left( \begin{matrix} 1 & 2 & 3 & \cdots & n \\ a & b & c & \cdots & . \end{matrix} \right)$$

simplemente  $(a, b, c, \dots)$ .

El *producto cartesiano*  $A \times \cdots \times A = A^m$  de  $m$  veces  $A$  consta de todas las familias de  $m$  elementos de  $A$ .

**OR<sub>n</sub><sup>m</sup>**. Como en la sección 1, este símbolo denota el número de ordenaciones con repetición de un conjunto  $A$  de  $n$  elementos tomados de  $m$  en  $m$ , es decir, el número de elementos del producto cartesiano  $A^m$ .

Demostraremos aquí que  $OR_n^m = n^m$ . Para que sea más clara la demostración conviene analizar primero un ejemplo.

3. Sea  $A$  un conjunto, digamos, de 10 elementos y  $a, b$  dos elementos de  $A$ . Nos preguntamos lo siguiente: ¿Cuántas funciones  $f: I_3 \rightarrow A$  hay, tales que

$$f(1) = a, f(2) = b?$$

Cada una de estas funciones que buscamos tiene ya su valor determinado para 1 y para 2 y por lo tanto queda únicamente por determinar su valor para 3; pero ya que a 3 podemos asociarle cualquier valor de  $A$  y  $A$  tiene 10 elementos, habrá exactamente 10 de estos.

Esto podemos expresarlo diciendo que hay 10 funciones de  $I_3$  en  $A$  que extienden a la función de  $I_2$  en  $A$  dada por  $1 \mapsto a, 2 \mapsto b$ . (También decimos que la función de  $I_3 \rightarrow A$  restringida a  $I_2 \subset I_3$  es  $1 \mapsto a, 2 \mapsto b$ .)

Demostraremos ahora que:

$$OR_n^m = n OR_n^{m-1}.$$

En efecto, si  $A$  tiene  $n$  elementos y  $f: I_{n-1} \rightarrow A$  es una función, como en el ejemplo de antes, habrá  $n$  funciones de  $I_n \rightarrow A$  que extienden a  $f$ . Es decir, por cada función de  $I_{n-1}$  en  $A$  hay  $n$  funciones diferentes de  $I_n$  en  $A$ , lo cual demuestra la fórmula.

La demostración de que  $OR_n^m = n^m$  es ahora muy fácil. En primer lugar,  $OR_n^1 = n$  pues  $I_1 = \{1\}$  y cada función queda determinada por un elemento de  $A$ . Supongamos la fórmula cierta para  $m-1$ , es decir, que  $OR_n^{m-1} = n^{m-1}$ . Entonces  $OR_n^m = n OR_n^{m-1} = nn^{m-1} = n^m$ .

**Ordenaciones.** Como antes, sea  $I_m = \{1, 2, \dots, m\}$  y  $A$  un conjunto con  $n$  elementos. Las ordenaciones de los elementos de  $A$  tomados de  $m$  en  $m$  son las funciones inyectivas de  $I_m$  en  $A$ .

Las ordenaciones son casos especiales de las ordenaciones con repetición pero no recíprocamente, pues estas últimas son funciones no necesariamente inyectivas.

Un ejemplo ilustrativo:

4. Las palabras de tres letras *distintas* formadas con el alfabeto  $A = \{a, b, c, d, e\}$  son las ordenaciones de  $A$  tomadas de tres en tres, pues cada una de ellas es, en efecto, una función inyectiva de  $I_3$  en  $A$ . Por ejemplo la palabra *eda* es la función

$$\begin{pmatrix} 1 & 2 & 3 \\ e & d & a \end{pmatrix}.$$

**O<sub>n</sub><sup>m</sup>.** Para demostrar que el número de ordenaciones de un conjunto  $A$  con  $n$  elementos tomados de  $m$  en  $m$  es

$$O_n^m = n(n-1) \cdots (n-m+1)$$

seguiremos un razonamiento análogo al utilizado para probar la fórmula de la sección anterior.

Empecemos, como antes, con un ejemplo.

5. Sea, como en el ejemplo 4,  $A = \{a, b, c, d, e\}$ . Consideremos una función inyectiva  $f: I_2 \rightarrow A$ , por ejemplo

$$\begin{pmatrix} 1 & 2 \\ e & d \end{pmatrix}.$$

Nos preguntamos ahora: ¿Cuántas funciones *inyectivas* hay de  $I_3 \rightarrow A$  tales que en 1 y 2 coincidan con  $f$ ?

Si

$$\begin{pmatrix} 1 & 2 & 3 \\ e & d & x \end{pmatrix}$$

es una función inyectiva de  $I_3$  en  $A$ ,  $x$  puede ser cualquier elemento de  $A$ , excepto  $e, d$ , es decir cualquiera de las  $5 - 2 = 3$  letras restantes:

$$\begin{pmatrix} 1 & 2 & 3 \\ e & d & a \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ e & d & b \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ e & d & c \end{pmatrix}.$$

Resumiendo, por cada función inyectiva de  $I_2 \rightarrow A$  hay 3 funciones inyectivas de  $I_3 \rightarrow A$ .

Este ejemplo nos sirve para ilustrar la demostración de que

$$O_n^m = (n-m+1) O_n^{m-1}.$$

En efecto, si  $f: I_{m-1} \rightarrow A$  es una función inyectiva, esta puede extenderse a una función inyectiva de  $I_m \rightarrow A$  de  $n - (m-1)$  maneras distintas, pues al elemento  $n$  de  $I_m$  le podemos asociar cualquier elemento de  $A$ , excepto los elementos  $m-1$  de  $A: f(1), f(2), \dots, f(m-1)$ ; (estos son distintos, pues  $f$  es inyectiva). Así pues, por cada función inyectiva de  $I_{m-1}$  en  $A$  hay  $n - (m-1) = n - m + 1$  funciones inyectivas distintas de  $I_m$  en  $A$ , lo cual prueba la fórmula.

Finalmente, es evidente que  $O_n^1 = n$ . Entonces, según la fórmula anterior,  $O_n^2 = (n-2+1) O_n^1 = (n-1)n = n(n-1)$ . Si suponemos, inductivamente, que

$$\begin{aligned} O_n^{m-1} &= n(n-1) \cdots (n-(m-1)+1) = \\ &= n(n-1) \cdots (n-m+2), \end{aligned}$$

tenemos que

$$O_n^m = (n-m+1) O_n^{m-1},$$

de donde

$$O^m = n(n-1) \dots (n-m+2)(n-m+1),$$

que es la fórmula que se quería probar.

**Permutaciones.** *Las permutaciones de un conjunto A son las funciones biyectivas de A en A.*

Si A es un conjunto finito, toda función inyectiva de A en A es biyectiva.\*

Sea A = {a<sub>1</sub>, ..., a<sub>n</sub>} y f: A → A una permutación de A. Entonces podemos identificar la permutación f con la ordenación g: I<sub>n</sub> → A dada por

$$g(1) = f(a_1), \dots, g(n) = f(a_n).$$

Por ejemplo, si A = {a, b, c}, las 6 permutaciones de A son

$$\begin{array}{cccc} \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} & \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} & \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} & \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \\ \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} & \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} & & \end{array}$$

las cuales pueden identificarse con las ordenaciones de A tomadas de 3 en 3:

$$\begin{array}{cccc} \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ a & c & b \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ b & a & c \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ b & c & a \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ c & a & b \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ c & b & a \end{pmatrix} & & \end{array}$$

Si P<sub>n</sub> indica el número de permutaciones de un conjunto con n elementos, se tiene entonces

$$P_n = O_n^n = 1 \cdot 2 \cdots n = n!$$

**Combinaciones.** Como se dijo en el párrafo 1, si A es un conjunto con n elementos, las combinaciones de los elementos de A tomados de m en m son los subconjuntos de A que consten de m elementos. (Suponemos 0 ≤ m ≤ n.)

Si C<sub>n</sub><sup>m</sup> indica el número de combinaciones de los elementos de A tomados de m en m probaremos ahora que

$$C_n^m P_m = O_n^m.$$

\* Esta propiedad puede tomarse como característica de los conjuntos finitos. (Véase el ejemplo 4 pág. 56 y los ejercicios 1, 2, 3, 4, 5 y 7 de la pág. 57.)

Sea  $S$  el conjunto de todas las ordenaciones de los elementos de  $A$  tomados de  $m$  en  $m$  y  $T$  el conjunto de todas las combinaciones de los elementos de  $A$  tomados también de  $m$  en  $m$ . (El número de elementos de  $S$  es  $O_n^m$  y el de  $T$  es  $C_n^m$ .) Asociemos ahora a cada ordenación una combinación en la forma siguiente:

$$\begin{pmatrix} 1 & 2 & \cdots & m \\ a_1 & a_2 & \cdots & a_m \end{pmatrix} \rightarrow \{a_1, a_2, \dots, a_m\}.$$

Esto determina una función  $S \rightarrow T$  que es evidentemente suprayectiva. Además hay exactamente  $P_m$  ordenaciones a las que corresponde la misma combinación. Por ejemplo, si  $m = 3$ , a las seis ordenaciones

$$\begin{matrix} \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ a & c & b \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ b & a & c \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ b & c & a \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ c & a & b \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ c & b & a \end{pmatrix} \end{matrix}$$

les corresponde la combinación  $\{a, b, c\}$ . Por tanto, el número de elementos de  $S$  es igual a  $P_m$  veces el número de elementos de  $T$ , lo que quiere decir que  $O_n^m = C_n^m P_m$ .

De esta fórmula se obtiene

$$C_n^m = \frac{n(n-1) \cdots (n-m+1)}{m!},$$

pues  $O_n^m = n(n-1) \cdots (n-m+1)$  y  $P_m = m!$

A los números de la forma  $C_n^m$  se les acostumbra llamar *coeficientes binomiales* pues aparecen como coeficientes en el desarrollo de la fórmula del binomio de Newton:

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

( $C_n^0 = 1$ ), pues es el número de subconjuntos de  $A$  que no tienen elementos de los cuales hay uno solo, el conjunto vacío  $\phi$ .

$C_n^m = C_n^{n-m}$ . Para demostrar esta relación consideremos un conjunto  $A$  con  $n$  elementos. Sea  $S$  el conjunto de todas las combinaciones de los elementos de  $A$  tomados de  $m$  en  $m$  y  $T$  el conjunto de todas las combinaciones de los elementos de  $A$  tomados de  $n-m$  en  $n-m$ . La función de  $S$  en  $T$  que asocia a cada combinación su complemento es claramente biyectiva. Por consiguiente, el número de elementos de  $S$ , es decir,  $C_n^m$ , es igual al de elementos de  $T$ , que es  $C_n^{n-m}$ , con lo cual queda probada la fórmula.

$C_n^0 + C_n^1 + C_n^2 + \cdots + C_n^n = 2^n$ . Observemos primero que la suma del lado izquierdo de la igualdad es el número total de subconjuntos de un conjunto  $A$  con  $n$  elementos, pues  $C_n^m$  es el número de subconjuntos de  $A$  con  $m$  elementos y  $m$  varía de 0 a  $n$ .

Para demostrar esta relación consideremos el conjunto  $A = \{1, 2, \dots, n\}$ . A cada subconjunto  $B$  de  $A$  asociemos una función,

$$f_B: A \rightarrow \{\in, \notin\}$$

en la forma siguiente:

$$f_B(x) = \begin{cases} \in & \text{si } x \in B \\ \notin & \text{si } x \notin B \end{cases}$$

( $f_B$  se llama la *función característica* del subconjunto  $B$ , pues dada la función, el conjunto  $B$  queda ya determinado). Esto establece una correspondencia biyectiva entre los subconjuntos de  $A$  y las funciones de  $A$  en  $\{\in, \notin\}$ . Por lo tanto el número total de subconjuntos de  $A$ , es decir,  $C_n^0 + C_n^1 + \cdots + C_n^n$  es igual al número de funciones de  $A$  en  $\{\in, \notin\}$  que es  $2^n$ , con lo cual queda probada la fórmula.

### Fórmula del triángulo de Pascal.

Esta fórmula es:

$$C_n^{r-1} + C_n^r = C_{n+1}^r.$$

Para su demostración consideremos el conjunto con  $n+1$  elementos  $A = \{1, 2, \dots, n, n+1\}$ . Los  $C_{n+1}^r$  subconjuntos de  $A$  con  $r$  elementos podemos clasificarlos en dos tipos:

- a) los que no contienen al elemento  $n+1$ , de los cuales hay  $C_n^r$ ;
- .. b) los que contienen a  $n+1$ . Estos están determinados por los subconjuntos de  $A' = \{1, 2, \dots, n\}$  con  $r-1$  elementos, de los cuales hay  $C_n^{r-1}$ .

Por consiguiente  $C_{n+1}^r = C_n^r + C_n^{r-1}$ .

Esta fórmula permite escribir el triángulo de Pascal,

$$\begin{array}{ccccccc} C_0^0 & & & & & & \\ C_1^0 & C_1^1 & & & & & \\ C_2^0 & C_2^1 & C_2^2 & & & & \\ C_3^0 & C_3^1 & C_3^2 & C_3^3 & & & \\ C_4^0 & C_4^1 & C_4^2 & C_4^3 & C_4^4 & & \\ & & & & & \ddots & \end{array}$$

en el cual cada número  $C_{n+1}^r$  es igual a la suma de  $C_n^r$  que se encuentra en el renglón anterior y en la misma columna, y de  $C_{n-1}^{r-1}$  que se encuentra a la izquierda de  $C_n^r$ . Por ejemplo,  $C_3^2 = C_2^2 + C_2^1$ ,  $C_4^2 = C_3^2 + C_3^1$ . (Los de la primera columna,  $C_n^0$  valen todos 1 y el último número de cada renglón, es decir,  $C_n^n$  vale 1 también.) Podemos de esta manera escribir el triángulo de Pascal:

1
1    1
1    2    1
1    3    3    1
1    4    6    4    1
1    5    10    10    5    1
1    6    15    20    15    6    1
.....

## 5. PROBLEMAS

1. ¿Cuántos números telefónicos de seis cifras hay que comiencen con 1, 2, 3, 4 o 6?

*Respuesta:* 500 000.

2. ¿Cuántas banderas tricolores pueden formarse con siete colores distintos?

*Respuesta:* 210.

3. ¿Cuántas placas de automóvil pueden hacerse que consten de dos letras y tres cifras? (Considérense 27 letras.)

*Respuesta:* 729 000.

4. ¿Cuántas placas de automóvil hay que consten de dos letras y tres cifras si la primera letra es la *A* y la segunda una letra de la *A* a la *F*?

*Respuesta:* 6 000.

5. Entre un grupo de 30 personas se debe elegir una comisión formada por cuatro. ¿De cuántas maneras se puede seleccionar dicha comisión?

*Respuesta:* 27 405.

6. Entre un grupo de 30 personas se debe elegir una mesa directiva que conste de un presidente, un secretario, un tesorero y un vocal. ¿De cuántas maneras se puede hacer la selección?

*Respuesta:* 657 720.

7. Entre un grupo de 30 personas se debe elegir una mesa directiva que conste de un presidente, un secretario y dos vocales. ¿Cuántas maneras hay de hacer la selección?

*Respuesta:* 328 860.

8. ¿Cuántas placas de 7 cifras distintas pueden formarse si la primera, la cuarta y la séptima deben ser cifras impares?

*Respuesta:* 50 400.

9. ¿Cuántos subconjuntos con 3 elementos hay del conjunto  $A = \{a, b, c, d, e\}$ , tales que contengan al elemento  $a$ ? Escríbalos.

*Respuesta:* 6.

*Observación al problema 9.* Una forma conveniente de resolver este problema es la siguiente:

El número de subconjuntos  $B \subset A$  tales que

- a)  $B$  tenga 3 elementos, y
- b)  $a \in B$

es igual al número de subconjuntos  $B' \subset A' = \{b, c, d, e\}$  tales que  $B'$  tenga 2 elementos. Este último es  $C_4^2$  y por consiguiente el resultado del problema es  $C_4^2 = 6$ .

10. ¿Cuántos subconjuntos hay del conjunto  $A = \{a, b, c, d, e\}$  tales que contengan al elemento  $a$ ?

*Respuesta:* 16.

*Observación al problema 10.* Como en el problema 9, los subconjuntos de  $A$  que contienen al elemento  $a$  son los subconjuntos de  $A' = \{b, c, d, e\}$  a los que se ha agregado el elemento  $a$ .

11. Sea  $A$  un conjunto con  $n$  elementos ( $n \geq 4$ ) y  $a$  un elemento de  $A$ . ¿Cuántos subconjuntos de  $A$  con 4 elementos hay tales que contengan al elemento  $a$ ?

*Respuesta:*  $C_{n-1}^3$

12. ¿Cuántos subconjuntos con cuatro elementos habrán del conjunto  $A = \{a, b, c, d, e\}$  tales que contengan a los elementos  $a$  y  $b$ ? Escríbalos todos.

$$\text{Respuesta: } C_3^2.$$

13. Sea  $A$  un conjunto con  $n$  elementos y  $B$  un subconjunto de  $A$  con  $r$  elementos. ¿Cuántos subconjuntos  $S$  de  $A$  hay con  $m$  elementos, tales que  $S$  contenga a  $B$ ? ( $n \geq m \geq r$ )

$$\text{Respuesta: } C_{n-r}^{m-r}.$$

14. ¿Cuántos subconjuntos con 3 elementos hay del conjunto  $\{a, b, c, d, e\}$  tales que contengan al elemento  $a$  o al elemento  $b$  (pero no a ambos)?

$$\text{Respuesta: } 6.$$

**SOLUCIÓN.** Según se vio en los problemas anteriores, hay 6 subconjuntos que contienen a  $a$ , de los cuales tres contienen a  $\{a, b\}$ . Por lo tanto, hay  $6 - 3 = 3$  que contienen a  $a$  pero no a  $b$ . Análogamente, hay 3 que contienen a  $b$  pero no a  $a$ . Por lo tanto el resultado es  $3 + 3 = 6$ .

15. De un grupo de 30 personas debe “elegirse” un comité de cuatro miembros. Pero, por ciertas razones, en él debe figurar forzosamente Don Perpetuo o su hermano, pero no los dos, pues “se vería mal”. ¿Cuántos comités pueden resultar “electos”?

$$\text{Respuesta: } 2(C_{29}^3 - C_{28}^2).$$

16. Consideremos una baraja simplificada con seis cartas numeradas del 1 al 3 y con dos palos únicamente: corazones y diamantes. ¿Cuántas manos de tres cartas hay que no tengan dos cartas con el mismo número?

$$\text{Respuesta: } 8.$$

**OBSERVACIONES Y SOLUCIÓN.** Esta baraja puede considerarse como el producto cartesiano de los conjuntos  $S = \{1, 2, 3\}$  y  $T = \{\heartsuit, \diamondsuit\}$ .

Una mano de 3 cartas sin cartas del mismo número es un subconjunto de 3 elementos de  $S \times T$ , tal que no tiene dos elementos en la misma columna. Contemos primero cuantas “manos ordenadas” hay, es decir, cuántas funciones  $f: I_3 = \{1, 2, 3\} \rightarrow S \times T$  hay cuya imagen satisfaga las condiciones del problema. El valor  $f(1)$  puede ser cualquiera de las 6 cartas. Para que

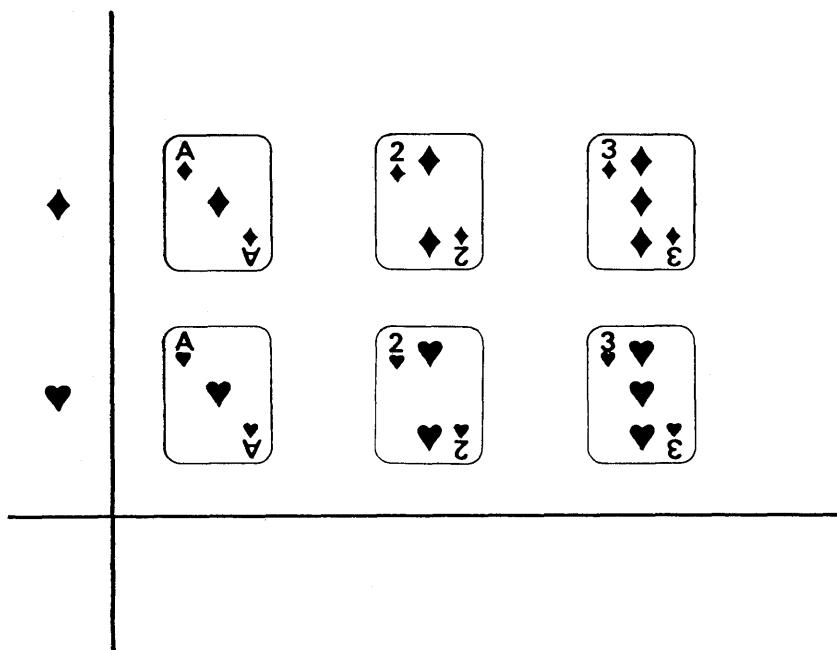


Figura 2.6

la condición del problema se satisfaga,  $f(2)$  puede ser una de las 4 cartas que no estén en la columna en donde está  $f(1)$  (pues en caso contrario habría 2 cartas con el mismo número).  $f(3)$  puede después ser cualquiera de las 2 cartas que no estén en la columna en donde se encuentran las cartas  $f(1)$  y  $f(2)$ . Por tanto el número de "manos ordenadas" es  $6 \times 4 \times 2$ . Ahora bien, por cada mano de 3 cartas se pueden formar  $3!$  "manos ordenadas" de 3 cartas, por lo cual la solución del problema es  $\frac{6 \times 4 \times 2}{1 \times 2 \times 3} = 8$ .

17. Sean  $S$  y  $T$  dos conjuntos con  $s$  y  $t$  elementos, respectivamente. Sea  $p:S \times T \rightarrow S$  la proyección [es decir, la función dada por  $p(x, y) = x$ , en donde  $(x, y) \in S \times T$ ]. Sea, como antes,  $I_m = \{1, 2, \dots, m\}$  y supongamos que  $m \leq s$ . ¿Cuántas funciones  $f:I_m \rightarrow S \times T$  hay tales que la composición

$$I_m \xrightarrow{f} S \times T \xrightarrow{p} S$$

sea inyectiva?

**SOLUCIÓN.** El razonamiento es análogo al del cálculo de las "manos ordenadas" del ejercicio anterior. En efecto,  $f(1) = (x_1, y_1)$  puede ser cual-

quiera de los  $rs$  elementos de  $S \times T$ .  $f(2) = (x_2, y_2)$  puede ser cualquier elemento de  $S \times T$  excepto aquellos para los que  $x_2 = x_1$  [pues en caso contrario, ya que  $p_f(1) = p(x_1, y_1) = x_1$ ,  $p_f(2) = p(x_2, y_2) = x_2$ ,  $p_f(1)$  sería igual a  $p_f(2)$ , contra la hipótesis de que  $p_f$  es inyectiva]. Por lo tanto  $f(2)$  puede tomar  $ts - t = t(s-1)$  valores. Continuando el procedimiento obtenemos finalmente que  $f(m)$  puede tomar  $t(s-m+1)$  valores. Por consiguiente la solución es  $tst(s-1)t(s-2)\cdots t(s-m+1) = t^m O_s^m$ .

18. Con las barajas del ejercicio 16, ¿cuántas manos de 3 cartas hay que tengan dos cartas del mismo número?

$$\text{Respuesta: } C_6^3 - 8 = 12.$$

**SUGERENCIA.** Réstese del total de manos posibles de 3 cartas aquellas en las que no haya números repetidos.

19. Con las mismas barajas, ¿cuántas manos de tres cartas hay que tengan exactamente un par?

$$\text{Respuesta: } 12.$$

**SOLUCIÓN.** Sea  $M$  el conjunto de manos que tienen exactamente un par y  $S = \{1, 2, 3\}$ . Consideremos la función  $F: M \rightarrow S$  que asocia a cada una de estas manos el número de las cartas que forman el par en dicha mano. [Por ejemplo, a la mano  $(1, \heartsuit), (3, \heartsuit), (3, \diamondsuit)$  le asociamos el 3.]  $F$  es evidentemente suprayectiva. ¿Cuántas manos hay que bajo  $F$  les corresponde el mismo número? Evidentemente 4. Por tanto, el número de elementos de  $M$  es igual al número de elementos de  $S$  multiplicado por 4, es decir,  $3 \times 4 = 12$ .

20. La baraja completa consta de 52 cartas (13 "números": 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K y 4 palos:  ,  ,  ,  ). Una mano de póker consta de cinco cartas. ¿Cuántas manos posibles de póker hay?

$$\text{Respuesta: } C_{52}^5 = 2\,598\,960.$$

21. ¿Cuántas manos de póker hay que no tengan dos cartas del mismo número?

$$\text{Respuesta: } 4^5 C_{13}^5 = 1\,317\,888.$$

**22.** ¿Cuántas manos de póker habrá en las que aparezcan por lo menos dos cartas del mismo número?

$$\text{Respuesta: } C_{52}^5 - 4^5 C_{13}^5 = 1\,281\,072.$$

**23.** ¿Cuántas manos de póker hay que tengan exactamente un par? (Es decir, que tengan dos cartas y solamente dos de un mismo número.) (Véase el ejercicio 19.)

$$\text{Respuesta: } 13C_4^2 \cdot 4C_{12}^3 = 68\,640.$$

**24.** ¿Cuántas manos de póker hay que tengan exactamente dos pares (distintos)?

$$\text{Respuesta: } 44 (C_4^2)^2 \cdot C_{13}^2 = 44\,928.$$

**25.** ¿Cuántas manos de póker hay que tengan al menos tres cartas del mismo número?

$$\text{Respuesta: } 13C_4^3 C_{48}^2 + 13C_{48}^1 = 52\,280.$$

**26.** Cuántas manos de póker hay que tengan exactamente una tercia (y que no sea ful)?

$$\text{Respuesta: } 13C_4^3 4^2 C_{12}^2 = 54\,912.$$

**27.** ¿Cuántas manos de póker hay que tengan ful? (Es decir, un par y una tercia.)

$$\text{Respuesta: } 13C_4^3 12C_4^2 = 3\,744.$$

**28.** ¿Cuántas manos de póker hay que tengan póker? (Es decir, que haya 4 cartas del mismo número.)

$$\text{Respuesta: } 13C_{48}^1 = 624.$$

**29.** ¿Cuántas manos de póker hay en que las cinco cartas sean del mismo palo? (Se llama flor o "flux".)

$$\text{Respuesta: } 4C_{13}^5 = 5\,148.$$

**30.** ¿Cuántas manos de póker hay en que las cinco cartas tengan números consecutivos? (Se llama "corrida". OBSERVACIÓN: la numeración 10, J, Q, K, 1 se considera también una corrida.)

$$\text{Respuesta: } 10 \times 4^5 = 10\,240.$$

31. ¿Cuántas manos de póker hay que sean "flor imperial"? (Es decir, que sea flor y corrida.)

*Respuesta:* 40.

32. ¿Cuántas diagonales se pueden trazar en un pentágono regular?

*Respuesta:* 5.

33. ¿Cuántas diagonales se pueden trazar en un polígono regular de  $n$  lados?

$$\text{Respuesta: } C_n^2 - n = \frac{n^2 - 3n}{2}.$$

34. En el dominó hay 28 fichas, de las cuales 7 son dobles. Una mano consta de 7 fichas. ¿Cuántas manos posibles de dominó hay?

35. ¿Cuántas manos de dominó hay que tengan exactamente cuatro fichas dobles?

$$\text{Respuesta: } C_7^4 C_{21}^3 = 46\,550.$$

36. ¿Cuántas manos de dominó hay que tengan por lo menos tres fichas dobles?

$$\text{Respuesta: } C_7^3 C_{24}^4 = 260\,543.$$

37. Pruébese que si la composición  $fg$  de dos funciones

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ & & \xrightarrow{f} C \\ & fg & \end{array}$$

es inyectiva, entonces  $g$  es inyectiva.

SOLUCIÓN. Si  $g$  no fuera inyectiva existirían dos elementos distintos  $x, x'$  en  $A$  tales que  $g(x) = g(x')$ . Pero entonces  $f(g(x)) = f(g(x'))$ , es decir,  $(fg)(x) = (fg)(x')$  con  $x \neq x'$  y la composición  $fg$  no sería inyectiva, contra la hipótesis.

38. Pruébese que si la composición  $fg$  de dos funciones, como en el ejercicio anterior, es suprayectiva, entonces  $f$  es también suprayectiva.

39. Sea  $f:A \rightarrow B$  una función suprayectiva y  $g, h:B \rightarrow C$  dos funciones. Demuéstrese que si  $gf = hf$ , entonces  $g = h$ .

SOLUCIÓN. Sea  $b \in B$  arbitrario. Por ser  $f$  suprayectiva, existe un elemento de  $A$  tal que  $b = f(a)$ . Ya que  $gf = hf$ , se tiene que  $(gf)(a) = (hf)(a)$ , es decir,  $g(f(a)) = h(f(a))$ , de donde  $g(b) = h(b)$ . Por lo tanto  $g = h$ .

40. Sean  $g, h:A \rightarrow B$  dos funciones y  $f:B \rightarrow C$  una función inyectiva. Demuéstrese que si  $fg = fh$  entonces  $g = h$ .



# 3

CAPÍTULO

# Espacios vectoriales

## 1. EL ESPACIO VECTORIAL $\mathbb{R}^2$

El concepto de espacio vectorial puede ilustrarse en el plano cartesiano. Llamamos plano cartesiano real al plano “de la geometría analítica”, es decir, al producto cartesiano  $\mathbb{R} \times \mathbb{R}$  de los reales por sí mismos. Los elementos de  $\mathbb{R} \times \mathbb{R}$  son las parejas ordenadas  $(a, b)$  de números reales. Estas se representan como puntos:

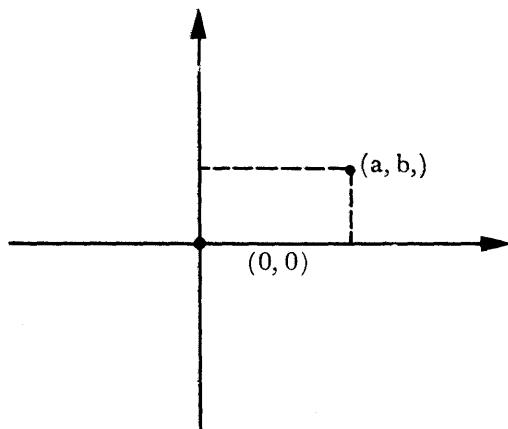


Figura 3.1

Escribimos  $\mathbf{R}^2$  en lugar de  $\mathbf{R} \times \mathbf{R}$  y, en general,  $\mathbf{R}^n$  en lugar de  $\mathbf{R} \times \mathbf{R} \times \cdots \times \mathbf{R}$  ( $n$  factores).

A los elementos de  $\mathbf{R}^2$ , es decir, a los puntos del plano les llamaremos ahora *vectores* y, para seguir la costumbre, a los números reales les llamaremos *escalares*.

En  $\mathbf{R}^2$  introducimos las operaciones siguientes:

### Suma de vectores:

$$(a, b) + (c, d) = (a+c, b+d), \quad ((a, b), (c, d) \in \mathbf{R}^2).$$

### Producto de un escalar por un vector:

$$\lambda(a, b) = (\lambda a, \lambda b). \quad (\lambda \in \mathbf{R}, (a, b) \in \mathbf{R}^2).$$

Al referirnos a un vector  $(a, b)$  diremos que  $a$  es la primera coordenada (o abscisa) de  $(a, b)$  y que  $b$  es la segunda coordenada (u ordenada) del mismo. Con este lenguaje, las operaciones que acabamos de definir pueden describirse así:

La suma de dos vectores es el vector cuyas coordenadas son la suma de las coordenadas respectivas de los sumandos.

El producto de un escalar por un vector es el vector cuyas coordenadas son el producto del escalar por las coordenadas del vector dado.

Por ejemplo:

$$\begin{array}{ll} (1, 2) + (-1, 3) = (0, 5) & 3(1, 2) = (3, 6) \\ (0, 0) + (2, 3) = (2, 3) & (-1)(3, -2) = (-3, 2) \\ (-1, 2) + (1, -2) = (0, 0) & a(1, 0) = (a, 0) \\ (1, 0) + (0, 1) = (1, 1) & b(0, 1) = (0, b) \\ (a, 0) + (0, b) = (a, b) & 0(a, b) = (0, 0). \end{array}$$

Tenemos también que

$$(a, b) = a(1, 0) + b(0, 1).$$

### Interpretación geométrica de la adición.

Recordemos los dos siguientes resultados:

1. Si las diagonales de un cuadrilátero se intersecan en su punto medio, entonces el cuadrilátero es un paralelogramo:

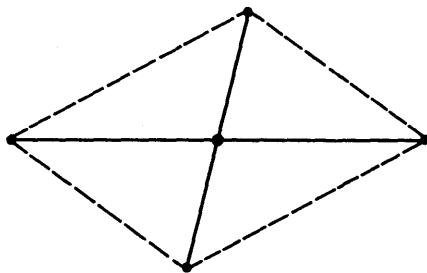


Figura 3.2

2. Si  $A_1 = (x_1, y_1)$  y  $A_2 = (x_2, y_2)$  son dos puntos del plano, entonces el punto medio del segmento  $\overline{A_1A_2}$  es

$$M = \left( \frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2} \right).$$

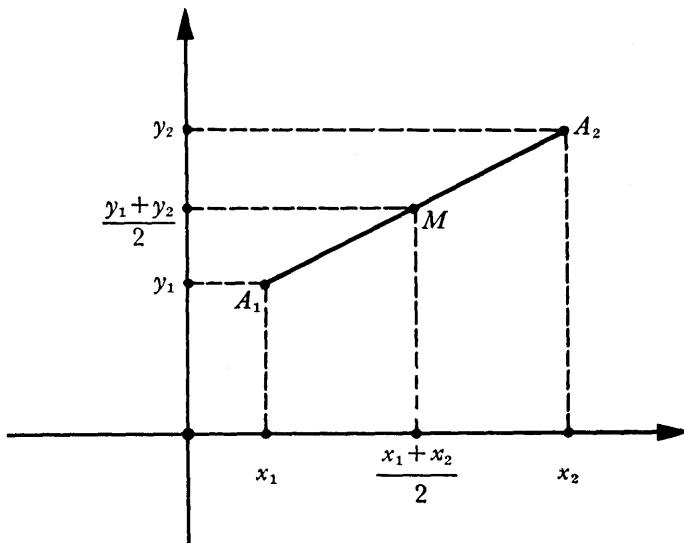


Figura 3.3

Veremos ahora la interpretación geométrica de la adición de vectores. Sean  $P = (a, b)$ ,  $Q = (c, d)$  y  $R = P + Q$ , es decir,  $R = (a+c, b+d)$ . Consideremos el cuadrilátero  $OPRQ$ :

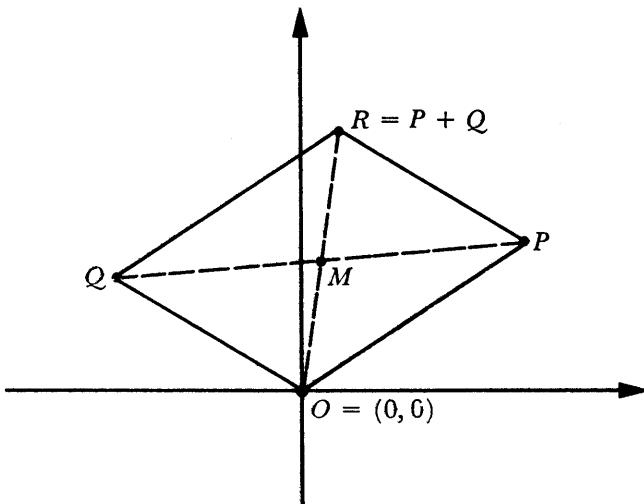


Figura 3.4

El punto medio de  $\overline{OR}$  es  $\left(\frac{a+c+0}{2}, \frac{b+d+0}{2}\right)$ . El punto medio de  $\overline{PQ}$  es  $\left(\frac{a+c}{2}, \frac{b+d}{2}\right)$ , por lo que vemos que las diagonales tienen el mismo punto medio. Por tanto, el cuadrilátero es un paralelogramo.

Si al representar los vectores en el plano dibujamos flechas que vayan del origen  $O$  al punto respectivo, como se ilustra en la siguiente figura,

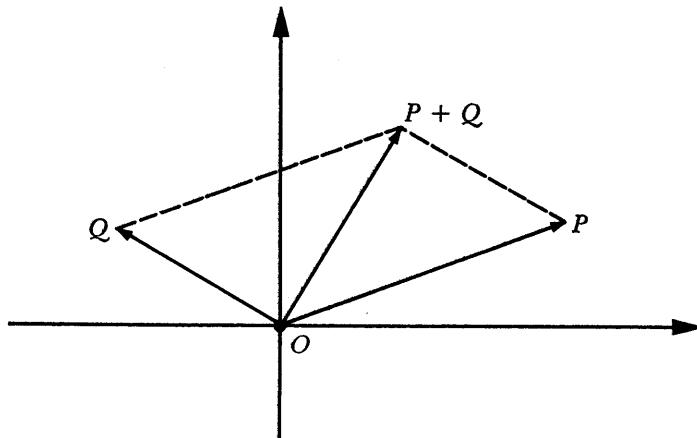


Figura 3.5

entonces podemos describir la adición diciendo que *la suma* de dos vectores  $P$  y  $Q$  es el vector determinado por la diagonal del paralelogramo de lados  $\overrightarrow{OP}$  y  $\overrightarrow{OQ}$ .

### Interpretación del producto de un escalar por un vector.

Recordemos dos resultados:

1. La distancia  $d(A_1, A_2)$  entre los puntos  $A_1 = (x_1, y_1)$  y  $A_2 = (x_2, y_2)$  es

$$d(A_1, A_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

2. Si  $A$ ,  $B$  y  $C$  son tres puntos del plano, entonces  $B$  está en el segmento  $\overline{AC}$  si y solamente si

$$d(A, B) + d(B, C) = d(A, C).$$

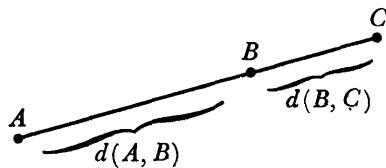


Figura 3.6

Veremos ahora el significado geométrico del producto de un escalar  $\lambda$  por un vector  $P = (a, b)$ .

Si  $P = O = (0, 0)$ , entonces  $\lambda O = O$  para toda  $\lambda$ .

Supongamos ahora que  $P \neq O$  y sea  $Q = \lambda P$ . Demostraremos que

1. Si  $\lambda \geq 1$ ,  $Q$  está en el segmento  $\overline{OQ}$ .
2. Si  $0 \leq \lambda \leq 1$ ,  $Q$  está en el segmento  $\overline{OP}$ .
3. Si  $\lambda \leq 0$ ,  $Q$  está en el segmento  $\overline{PQ}$ .

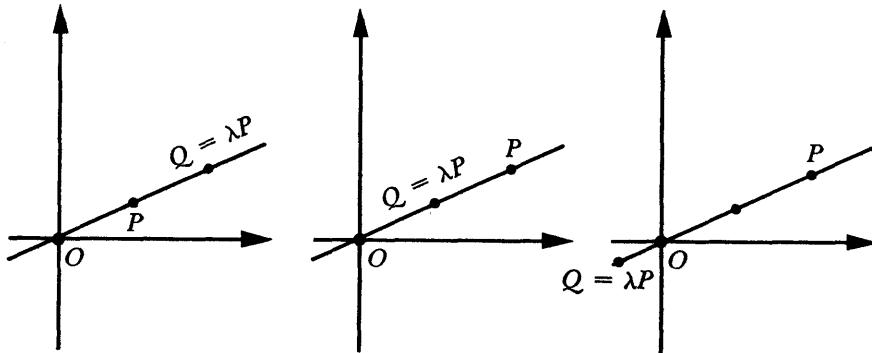


Figura 3.7

Denotemos con  $c$  a la distancia  $d(O, P)$ , es decir,

$$d(O, P) = \sqrt{a^2 + b^2} = c.$$

Entonces

$$\begin{aligned} d(O, Q) &= d(O, \lambda P) = \sqrt{(\lambda a)^2 + (\lambda b)^2} = \sqrt{\lambda^2(a^2 + b^2)} = \\ &= |\lambda| \sqrt{a^2 + b^2} = |\lambda|c \\ d(P, Q) &= \sqrt{(a - \lambda a)^2 + (b - \lambda b)^2} = \sqrt{(1 - \lambda)^2(a^2 + b^2)} \\ &= |1 - \lambda| \sqrt{a^2 + b^2} = |1 - \lambda|c. \end{aligned}$$

Veamos ahora los tres casos:

*Caso 1.* Por ser  $\lambda \geq 1$ ,  $|\lambda| = \lambda$  y  $|1 - \lambda| = \lambda - 1$ . Entonces

$$d(O, P) + d(P, Q) = c + (\lambda - 1)c = \lambda c = d(O, Q),$$

de donde,  $P \in \overleftrightarrow{OQ}$ .

*Caso 2.* Si  $0 \leq \lambda \leq 1$ ,  $|\lambda| = \lambda$  y  $|1 - \lambda| = 1 - \lambda$ . Por consiguiente,

$$d(O, Q) + d(Q, P) = \lambda c + (1 - \lambda)c = c = d(O, P),$$

de donde,  $Q \in \overleftrightarrow{OP}$ .

*Caso 3.* Si  $\lambda \leq 0$ ,  $|\lambda| = -\lambda$  y  $|1 - \lambda| = 1 - \lambda$ . Por consiguiente,

$$d(Q, O) + d(O, P) = \lambda c + c = (1 - \lambda)c = d(P, Q),$$

de donde,  $O \in \overleftrightarrow{QP}$ .

En todos los casos tenemos que el punto  $\lambda P$  pertenece a la recta  $\overleftrightarrow{OP}$ .

## EJERCICIOS

**1.** Encuéntrense las sumas de los vectores indicados y máquense en el plano los vectores sumandos, así como el vector suma:

$$\begin{array}{ll} (-1, -2) + (-3, 4) & (3, 2) + (-1, -3) + (-2, 1) \\ \left(\frac{3}{2}, \frac{4}{3}\right) + \left(-\frac{1}{2}, \frac{2}{3}\right) & \left(-\frac{2}{3}, \frac{1}{5}\right) + \left(\frac{1}{3}, \frac{3}{5}\right) + \left(\frac{5}{3}, \frac{1}{5}\right). \end{array}$$

**2.** Compruébese que si  $P = (-1, 2)$  y  $Q = (3, 5)$  entonces  $P + Q = Q + P$ . Demuéstrese que esta propiedad conmutativa es cierta para cualquier pareja de vectores  $P = (a, b)$  y  $Q = (c, d)$ .

**3.** Demuéstrese que si  $P$ ,  $Q$  y  $R$  son tres vectores arbitrarios entonces  $(P+Q) + R = P + (Q+R)$ .

**4.** Resuélvanse las ecuaciones

$$(3, 1) + (x, y) = (2, 3) \quad (a, b) + (x, y) = (c, d) \\ (a, 1) + (x, y) = (-3, b) \quad (x, y) + (a, b) = (0, 0)$$

**5.** Si  $\square OPRQ$  es un paralelogramo y  $P = (1, 2)$ ,  $R = (-1, 3)$ , calcúlense las coordenadas de  $Q$ .

**6.** Sean  $P_1 = \overset{\leftrightarrow}{(-1, 2)}$ ,  $P_2 = \overset{\leftrightarrow}{(-1, -1)}$ ,  $L_1$  la recta que pasa por  $P_1$  paralela a la recta  $\overleftrightarrow{OP_2}$  y  $L_2$  la recta que pasa por  $P_2$  paralela a la recta  $\overleftrightarrow{OP_1}$ . ¿En qué punto se intersecan las rectas  $L_1$  y  $L_2$ ? Hágase una figura.

**7.** Calcúlese

$$\sqrt{2} \left( \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} \right) + 3(-1, -1) \quad \tan \alpha (\cos \alpha, \csc \alpha)$$

$$\sqrt{3} \left( \frac{1}{2}, \frac{\sqrt{3}}{2} \right) + (-1)(2, 4) \quad (-1)(a, b) + (a, b).$$

**8.** Pruébese que si  $P$  es un vector cualquiera y  $O = (0, 0)$ , entonces

$$P + (-1)P = O.$$

Al vector  $(-1)P$  se le denota simplemente  $-P$ . Por lo anterior  $-P$  tiene la propiedad de que

$$P + (-P) = O.$$

**9.** Pruébese que

$$-(P+Q) = (-P) + (-Q).$$

**10.** Si  $P = (2, -1)$ ,  $Q = (-3, 2)$ ,  $\lambda = 2$ ,  $\mu = -1$  compruébese que

$$\lambda(P+Q) = \lambda P + \lambda Q$$

$$(\lambda + \mu)P = \lambda P + \mu P$$

$$(\lambda\mu)P = \lambda(\mu P).$$

Demuéstrese que estas tres propiedades son válidas para  $P$ ,  $Q$ ,  $\lambda$  y  $\mu$  arbitrarios.

**11.** Si  $E_1 = (1, 0)$ ,  $E_2 = (0, 1)$  y  $P = (a, b)$  pruébese que

$$P = aE_1 + bE_2.$$

**12.** Dibújese en el plano  $\mathbf{R}^2$  los vectores

$$3E_1 + 5E_2 \quad -\frac{1}{2}E_1 + 2E_2 \quad -2E_1 - 3E_2.$$

**13.** Pruébese que el eje de las abscisas consiste de todos los vectores de la forma  $aE_1$  con  $a$  en  $\mathbf{R}$ . ¿Qué puede decirse del eje de las ordenadas?

**14.** Si  $P = (1, -2)$  indíquense en el plano los puntos  $\lambda P$  para los siguientes valores de  $\lambda$ :

$$\lambda = 0, \quad \lambda = \frac{1}{2}, \quad \lambda = 3, \quad \lambda = -2, \quad \lambda = 1, \quad \lambda = -1.$$

**15.** Si  $P = (4, -2)$  y  $Q = (-2, 1)$  encuéntrese  $\lambda$  tal que  $Q = \lambda P$ . Si  $P = (4, -2)$  y  $Q = (1, 2)$  ¿puede encontrarse  $\lambda$  tal que  $Q = \lambda P$ ? Explíquese por qué.

16. Encuéntrese un número real  $\lambda$  tal que

$$\lambda(\sqrt{2}, -\sqrt{2}) = \left(-\frac{2}{\sqrt{2}}, \frac{2}{\sqrt{2}}\right).$$

17. Resuélvanse las ecuaciones:

$$\begin{aligned} 3(x, y) + (-1, -2) &= (-4, 1) \\ a(x, y) + (a^2, ab) &= (a, b) \quad (a \neq 0) \\ aX + B = C & \quad (a \neq 0, X, B \text{ y } C \text{ vectores}). \end{aligned}$$

18. Resuélvase la ecuación:

$$x(3, 1) + y(2, 4) = (-3, 2) \quad (x, y \in \mathbf{R})$$

19. ¿Tiene solución la ecuación siguiente?

$$x(6, 3) + y(2, 4) = (1, 1).$$

## 2. EL ESPACIO VECTORIAL $\mathbf{R}^n$

Ahora generalizaremos lo que acabamos de estudiar.

**DEFINICIÓN:** *El espacio vectorial  $\mathbf{R}^n$  consta del conjunto de todas las colecciones ordenadas de  $n$  números reales*

$$(a_1, a_2, \dots, a_n)$$

y las operaciones siguientes:

$$\begin{aligned} (a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \\ \lambda(a_1, a_2, \dots, a_n) &= (\lambda a_1, \lambda a_2, \dots, \lambda a_n). \quad (\lambda \in \mathbf{R}) \end{aligned}$$

A los elementos  $(a_1, a_2, \dots, a_n)$  de  $\mathbf{R}^n$  los llamaremos *vectores* y, como antes, a los números reales, *escalares*.

Observemos que, como en el caso especial de  $\mathbf{R}^2$  que antes analizamos, la suma de vectores se efectúa sumando las coordenadas correspondientes y el producto de un escalar por un vector se obtiene multiplicando el escalar por cada una de las coordenadas del vector.

Estas operaciones, como en el caso de  $\mathbf{R}^2$ , cumplen una serie de propiedades, entre las cuales mencionaremos las básicas:

1. La adición es *asociativa*, es decir, si  $A, B$  y  $C$  son vectores en  $\mathbf{R}^n$ , entonces

$$(A + B) + C = A + (B + C).$$

2. La adición es *comutativa*, es decir, si  $A$  y  $B$  son vectores en  $\mathbf{R}^n$ , entonces

$$A + B = B + A.$$

3. Existe un *elemento neutro* (único) en  $\mathbf{R}^n$  para la adición. Este es el vector  $(0, 0, \dots, 0)$  que, cuando no haya confusión, denotaremos simplemente con 0. Este tiene la propiedad de que

$$0 + A = A$$

para cualquier  $A$  en  $\mathbf{R}^n$ .

4. Existe en  $\mathbf{R}^n$  el *inverso aditivo* (también llamado el *negativo*) de cada vector de  $\mathbf{R}^n$ . Si  $A$  es un vector, al inverso aditivo se le denota  $-A$ . Si  $A = (a_1, a_2, \dots, a_n)$  entonces  $-A = (-a_1, -a_2, \dots, -a_n)$ . La propiedad de  $-A$  es que

$$A + (-A) = 0$$

[en donde, como en la propiedad 3,  $0 = (0, 0, \dots, 0)$ ].

5. Si  $A \in \mathbf{R}^n$  y  $\lambda, \mu \in \mathbf{R}$ ,

$$\lambda(\mu A) = (\lambda\mu)A.$$

6. Si  $A$  y  $B \in \mathbf{R}^n$  y  $\lambda \in \mathbf{R}$ ,

$$\lambda(A+B) = \lambda A + \lambda B.$$

7. Si  $A \in \mathbf{R}^n$  y  $\lambda, \mu \in \mathbf{R}$ ,

$$(\lambda+\mu)A = \lambda A + \mu A.$$

8.  $1A = A$  y  $(-1)A = -A$  para todo  $A \in \mathbf{R}^n$ .

9.  $0A = 0$  (aquí el primer 0 es el cero de  $\mathbf{R}$  y el segundo es el vector  $0 = (0, 0, \dots, 0)$ ).

10.  $\lambda A = 0$  implica  $\lambda = 0$ , o bien  $A = 0$ .

La demostración de estas propiedades es directa y se deja como ejercicio. Como ejemplo, demostrarímos aquí dos de ellas, la 7 y la 10.

$$\begin{aligned} (\lambda+\mu)A &= (\lambda+\mu)(a_1, a_2, \dots, a_n) \\ &= ((\lambda+\mu)a_1, (\lambda+\mu)a_2, \dots, (\lambda+\mu)a_n) \\ &= (\lambda a_1 + \mu a_1, \lambda a_2 + \mu a_2, \dots, \lambda a_n + \mu a_n) \\ &= (\lambda a_1, \lambda a_2, \dots, \lambda a_n) + (\mu a_1, \mu a_2, \dots, \mu a_n) \\ &= \lambda(a_1, a_2, \dots, a_n) + \mu(a_1, a_2, \dots, a_n) \\ &= \lambda A + \mu A. \end{aligned}$$

Para probar la propiedad 10 supongamos que  $\lambda A = 0$ , o sea que  $\lambda(a_1, a_2, \dots, a_n) = (0, 0, \dots, 0)$ . Entonces  $(\lambda a_1, \lambda a_2, \dots, \lambda a_n) = (0, 0, \dots, 0)$ , de donde

$$\lambda a_1 = 0, \lambda a_2 = 0, \dots, \lambda a_n = 0,$$

por lo que o bien  $\lambda = 0$ , o en caso contrario,  $a_1 = 0, a_2 = 0, \dots, a_n = 0$ , es decir,  $A = (0, 0, \dots, 0)$ .

**OBSERVACIÓN.** En todo lo anterior y en lo que sigue de este capítulo se puede tomar en lugar de  $\mathbf{R}$  cualquier otro campo  $K$ , como por ejemplo, el campo  $\mathbf{Q}$  de los números racionales o el campo  $\mathbf{C}$  de los números complejos y todo lo que se haga para  $\mathbf{R}$  seguirá siendo válido para cualquier campo pues de  $\mathbf{R}$  solamente utilizaremos la estructura de campo.

### EJERCICIOS

1. Si  $A = (2, -1, 1, 3), B = (-5, 2, -3, 1), C = (0, 1, 1, 0), \lambda = -1, \mu = 2, \nu = -3, \tau = 0$ , encuéntrese

$$\begin{array}{lll} \lambda A & \mu C & \tau B \\ \lambda A + \mu B & \nu B + \tau A & \nu A + \mu B + \lambda A \end{array}$$

2. Si en  $\mathbf{R}^n$

$$E_1 = (1, 0, 0, \dots, 0)$$

$$E_2 = (0, 1, 0, \dots, 0)$$

.....

$$E_n = (0, 0, 0, \dots, 1)$$

encuéntrense las coordenadas del vector

$$A = \lambda_1 E_1 + \lambda_2 E_2 + \dots + \lambda_n E_n.$$

3. Si en  $\mathbf{R}^4$   $D_1 = (1, 0, 0, 0), D_2 = (1, 1, 0, 0), D_3 = (1, 1, 1, 0)$  y  $D_4 = (1, 1, 1, 1)$  y

$$A = a_1 D_1 + a_2 D_2 + a_3 D_3 + a_4 D_4$$

encuéntrense las coordenadas de  $A$ . Generalícese este ejercicio a  $\mathbf{R}^n$ .

4. Demuéstrense las propiedades 1, 2, ..., 6, 8 y 9.

5. Con las notaciones del ejercicio 1 encuéntrese el vector  $X$  si

$$a) \lambda X + A = B \quad b) \mu X + B = C.$$

### 3. SUBESPACIOS VECTORIALES

Se dice que un subconjunto  $W$  de  $\mathbf{R}^n$  es un **subespacio vectorial** de  $\mathbf{R}^n$  si cumple las tres condiciones siguientes:

1. El vector 0 de  $\mathbf{R}^n$  pertenece a  $W$ .
2. Si  $A$  y  $B$  son vectores de  $W$ , su suma  $A + B$  pertenece también a  $W$ .
3. Si  $A$  pertenece a  $W$  y  $\lambda$  es un escalar arbitrario, entonces  $\lambda A$  pertenece a  $W$ .

### Ejemplos:

1. Sea  $W$  el conjunto de todos los vectores de  $\mathbf{R}^2$  "sobre el eje de las abscisas", es decir, las de la forma  $(a, 0)$ . Afirmando que  $W$  es un subespacio vectorial de  $\mathbf{R}^2$ . En primer lugar,  $0 = (0, 0) \in W$ . Además, si  $A$  y  $B$  están en  $W$ , se tiene que  $A = (a, 0)$  y  $B = (b, 0)$ . Entonces

$$A + B = (a + b, 0)$$

por lo que  $A + B \in W$  y se cumple la condición 2. Finalmente, si  $A$  está en  $W$  y  $\lambda$  en  $\mathbf{R}$  se tiene que  $A = (a, 0)$  y  $\lambda A = (\lambda a, 0)$ . Por lo tanto  $\lambda A$  pertenece también a  $W$ , lo cual prueba que se cumple la condición 3.

2. Consideremos en  $\mathbf{R}^2$  el conjunto  $W$  de los vectores de la forma  $\lambda A$  en donde  $A$  es un vector fijo y  $\lambda$  un real arbitrario.  $W$  es un subespacio vectorial de  $\mathbf{R}^2$ .

Se cumple la condición 1, pues el vector 0 es igual a  $0A$ . Ahora bien, si tomamos dos vectores de  $W$ , estos son de la forma  $\lambda A$  y  $\mu A$  y su suma es  $\lambda A + \mu A = (\lambda + \mu)A$ , el cual es también un vector de  $W$ , por lo que se cumple la condición 2. Finalmente, si  $\lambda A \in W$  y  $\mu \in \mathbf{R}$ ,  $\mu(\lambda A) = (\mu\lambda)A \in W$ , por lo que se cumple la condición 3.

3. Como en el ejemplo 1, pero en el espacio, se tiene que el conjunto  $W$  de los vectores sobre uno de los ejes, digamos el de las abscisas, o sea, los de la forma

$$(a, 0, 0)$$

es un subespacio vectorial de  $\mathbf{R}^3$ .

4. En  $\mathbf{R}^3$  el conjunto de vectores de la forma

$$(a, b, 0)$$

es un subespacio vectorial de  $\mathbf{R}^3$  (un plano del sistema de coordenadas).

5. Si  $A$  y  $B$  son dos vectores de  $\mathbf{R}^3$ , el conjunto

$$W = \{\lambda A + \mu B \mid \lambda \in \mathbf{R}, \mu \in \mathbf{R}\}$$

es un subespacio vectorial de  $\mathbf{R}^3$ .

6. En  $\mathbf{R}^n$  el conjunto  $\{0\}$  que consta solamente del vector 0 es un subespacio vectorial de  $\mathbf{R}^n$ .

7.  $\mathbf{R}^n$  es un subespacio vectorial de  $\mathbf{R}^n$ . (Los subespacios  $\{0\}$  y  $\mathbf{R}^n$  se llaman respectivamente subespacios trivial e impropio de  $\mathbf{R}^n$ .)

### EJERCICIOS

1. Compruébese que los conjuntos definidos en los ejemplos 3, 4, 5, 6 y 7 son efectivamente subespacios vectoriales.

2. Si  $A$  y  $B$  son dos vectores de  $\mathbf{R}^n$  demuéstrese que

$$W = \{\lambda A + \mu B | \lambda \in \mathbf{R}, \mu \in \mathbf{R}\}$$

es un subespacio vectorial de  $\mathbf{R}^n$ .

3. Demuéstrese que

$$\{(x, y) \in \mathbf{R}^2 | 2x - 3y = 0\}$$

es un subespacio vectorial de  $\mathbf{R}^2$ .

4. Pruébese que

$$\{(x, y, z) \in \mathbf{R}^3 | x - y + z = 0\}$$

es un subespacio vectorial de  $\mathbf{R}^3$ .

5. Pruébese que en  $\mathbf{R}^3$

$$\{(x, y, z) | x + y - z = 0, x + 2y + 3z = 0\}$$

es un subespacio vectorial de  $\mathbf{R}^3$ .

6. Demuéstrese que

$$\{(x_1, x_2, \dots, x_n) \in \mathbf{R}^n | x_1 + x_2 + \dots + x_n = 0\}$$

es un subespacio vectorial de  $\mathbf{R}^n$ .

7. Demuéstrese que si  $W$  es un subespacio vectorial de  $\mathbf{R}^3$  y  $A \in W$  (con  $A \neq 0$ ) entonces  $W$  contiene a la recta  $\overset{\leftrightarrow}{OA}$ .

8. Demuéstrese que en  $\mathbf{R}^2$  los vectores que están sobre una recta forman un subespacio vectorial si y sólo si la recta pasa por el origen.

9. En  $\mathbf{R}^3$  los vectores que están en un plano forman un subespacio vectorial si y sólo si el plano pasa por el origen.

10. En  $\mathbf{R}^3$  los vectores que están en una recta forman un subespacio vectorial si y sólo si la recta pasa por el origen.

11. Demuéstrese que los únicos subespacios vectoriales de  $\mathbf{R}^2$  son  $\{0\}$ , las rectas que pasan por 0 y  $\mathbf{R}^2$ . ¿Qué ocurre en  $\mathbf{R}^3$ ?

#### 4. COMBINACIONES LINEALES. DEPENDENCIA E INDEPENDENCIA LINEAL

En el espacio vectorial  $\mathbf{R}^n$  se llama **combinación lineal de los vectores**  $A_1, A_2, \dots, A_h$  a cualquier vector  $C$  que se exprese en la forma

$$C = \lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_h A_h,$$

en donde  $\lambda_1, \lambda_2, \dots, \lambda_h$  son escalares.

##### Ejemplos:

1. En  $\mathbf{R}^2$ , si  $A_1 = (1, 1)$ ,  $A_2 = (2, -1)$ , el vector  $C = (-4, 5)$  es combinación lineal de  $A_1$  y  $A_2$  pues  $C = 2A_1 + (-3)A_2$ .

2. En  $\mathbf{R}^2$ , el vector  $(2, 1)$  no es combinación lineal de los vectores  $(1, 0)$  y  $(-2, 0)$ . En efecto, toda combinación lineal  $\lambda(1, 0) + \mu(-2, 0)$  tiene ordenada 0.

3. En  $\mathbf{R}^3$ , todo vector  $C = (x_1, x_2, x_3)$  es combinación lineal de los vectores  $E_1 = (1, 0, 0)$ ,  $E_2 = (0, 1, 0)$  y  $E_3 = (0, 0, 1)$ . En efecto, se comprueba directamente que

$$C = x_1E_1 + x_2E_2 + x_3E_3.$$

4. En  $\mathbf{R}^n$ , todo vector  $C = (x_1, x_2, \dots, x_n)$  es combinación lineal de los vectores

$$E_1 = (1, 0, 0, \dots, 0)$$

$$E_2 = (0, 1, 0, \dots, 0)$$

$$\dots$$

$$E_n = (0, 0, 0, \dots, 1)$$

pues  $C = x_1E_1 + x_2E_2 + \dots + x_nE_n$ .

5. Dados varios vectores  $A_1, A_2, \dots, A_h$  podemos afirmar que cualquiera de ellos, por ejemplo  $A_1$ , es combinación lineal de  $A_1, A_2, \dots, A_h$ . En efecto, tenemos que

$$A_1 = 1A_1 + 0A_2 + \dots + 0A_h.$$

6. El vector 0 es combinación lineal de cualquier conjunto de vectores:  $\{A_1, A_2, \dots, A_h\}$ . En efecto,

$$0 = 0A_1 + 0A_2 + \dots + 0A_h.$$

7. Si  $C$  y  $D$  son combinaciones lineales de los vectores  $A_1, A_2, \dots, A_h$  entonces  $C + D$  también lo es. En efecto, por hipótesis

$$C = \lambda_1A_1 + \lambda_2A_2 + \dots + \lambda_hA_h$$

$$D = \mu_1A_1 + \mu_2A_2 + \dots + \mu_hA_h,$$

de donde obtenemos

$$C + D = (\lambda_1 + \mu_1)A_1 + (\lambda_2 + \mu_2)A_2 + \dots + (\lambda_h + \mu_h)A_h.$$

Esto prueba que  $C + D$  es combinación lineal de  $A_1, A_2, \dots, A_h$ .

## EJERCICIOS

1. Si  $A = (a_1, a_2, a_3)$ ,  $B = (b_1, b_2, b_3)$ ,  $C = (c_1, c_2, c_3)$  y  $D = (d_1, d_2, d_3)$  escríbase en términos de las  $a_i, b_i, c_i, d_i$  las coordenadas del vector

$$P = \lambda A + \mu B + \nu C + \tau D.$$

2. Si en  $\mathbf{R}^m$ 

$$A_1 = (a_{11}, a_{21}, \dots, a_{m1})$$

$$A_2 = (a_{12}, a_{22}, \dots, a_{m2})$$

.....

$$A_n = (a_{1n}, a_{2n}, \dots, a_{mn})$$

y

$$B = x_1 A_1 + x_2 A_2 + \cdots + x_n A_n$$

escribanse las coordenadas de  $B = (b_1, b_2, \dots, b_m)$  en términos de las  $x_i$ , y de las coordenadas de los vectores  $A_i$ .

3. Demuéstrese que en  $\mathbf{R}^2$  todo vector  $(x, y)$  es combinación lineal de los vectores  $(1, 0)$  y  $(1, 1)$ .

4. Demuéstrese que en  $\mathbf{R}^3$  todo vector  $(x, y, z)$  es combinación lineal de los vectores  $(1, 0, 0)$ ,  $(1, 1, 0)$  y  $(1, 1, 1)$ .

5. Generalícese a  $\mathbf{R}^n$  las afirmaciones de los dos ejercicios anteriores.

6. Exprésese el vector  $(8, -1)$  como combinación de  $(2, 1)$  y  $(3, -1)$ .  
SUGERENCIA: Plantéese un sistema de dos ecuaciones con dos incógnitas y resuélvalo.

7. ¿Es  $(1, 0)$  combinación lineal de los vectores  $(1, 2)$  y  $(-2, -4)$ ?

8. Demuéstrese que en  $\mathbf{R}^3$  hay vectores que no son combinación lineal de los vectores  $(1, 1, 0)$  y  $(2, -1, 0)$ .

### Subespacio vectorial generado por un conjunto de vectores.

Consideremos un conjunto  $\{A_1, A_2, \dots, A_r\}$  de vectores de  $\mathbf{R}^n$  y el conjunto  $W \subset \mathbf{R}^n$  que estará formado con todas las combinaciones lineales de  $\{A_1, A_2, \dots, A_r\}$ .

Afirmamos que  $W$  es un subespacio vectorial de  $\mathbf{R}^n$ .

En efecto,  $0 \in W$  (véase el ejemplo 6, de este párrafo). Además, si  $B$  y  $C$  están en  $W$ , es decir, si  $B$  y  $C$  son combinaciones lineales de  $\{A_1, A_2, \dots, A_r\}$  entonces  $B + C$  también lo es (véase el ejemplo 7 de este párrafo), es decir,  $B + C \in W$ . Finalmente, si  $\lambda$  es un escalar y  $C = \mu_1 A_1 + \mu_2 A_2 + \cdots + \mu_r A_r$ , entonces  $\lambda C = (\lambda \mu_1) A_1 + (\lambda \mu_2) A_2 + \cdots + (\lambda \mu_r) A_r \in W$ . Por lo tanto,  $W$  es un subespacio vectorial de  $\mathbf{R}^n$ , pues cumple las tres condiciones de la definición (véase el párrafo 3).

Así pues, hemos demostrado que

*El conjunto de todas las combinaciones lineales de un conjunto  $\{A_1, A_2, \dots, A_r\}$  de vectores de  $\mathbf{R}^n$  es un subespacio vectorial de  $\mathbf{R}^n$ .*

A este subespacio se le llama **subespacio generado por  $A_1, A_2, \dots, A_r$** . Es decir,

*Un subespacio vectorial  $W$  está generado por los vectores  $A_1, A_2, \dots, A_r$ , de  $\mathbf{R}^n$  si  $W$  consta de todas las combinaciones lineales de estos vectores.*

Conviene observar que este subespacio contiene a los vectores  $A_1, A_2, \dots, A_r$ . ¿Por qué? (Véase el ejemplo 5.)

### Dependencia lineal.

**DEFINICIÓN 1:** Se dice que un vector  $C$  depende linealmente del conjunto de vectores  $\{A_1, A_2, \dots, A_r\}$  si  $C$  es una combinación lineal de  $\{A_1, A_2, \dots, A_r\}$  o, lo que es lo mismo, si  $C$  pertenece al subespacio vectorial  $W$  generado por  $\{A_1, A_2, \dots, A_r\}$ .

**DEFINICIÓN 2:** Se dice que un conjunto  $\{A_1, A_2, \dots, A_r\}$  de vectores de  $\mathbf{R}^n$  es linealmente dependiente si al menos uno de ellos depende linealmente de los restantes.

En otras palabras, si al menos uno de ellos, digamos  $A_k$  es combinación lineal de los restantes, o sea, de  $\{A_1, \dots, A_{k-1}, A_{k+1}, \dots, A_r\}$ .

**PROPOSICIÓN 1.** El conjunto  $\{A_1, A_2, \dots, A_r\}$  de vectores de  $\mathbf{R}^n$  es linealmente dependiente si y solamente si existe una combinación lineal de ellos igual a cero

$$\lambda_1 A_1 + \lambda_2 A_2 + \cdots + \lambda_r A_r = 0$$

con algún coeficiente  $\lambda_i$  distinto de cero.

Antes de proceder a la demostración de esta proposición haremos dos observaciones.

**Observaciones.** 1. Cuando, en la definición anterior, decimos que “al menos uno de ellos depende linealmente de los demás”, esto no significa, desde luego, que *cada uno* de ellos se pueda expresar como combinación lineal de los restantes. Por ejemplo, los vectores

$$A = (1, 1, 0), \quad B = (2, 2, 0), \quad C = (0, 0, 1)$$

son linealmente dependientes pues, por ejemplo,

$$B = 2A + 0C.$$

También  $A$  es combinación lineal de  $B$  y  $C$ :

$$A = \frac{1}{2}B + 0C.$$

Pero  $C$  no es combinación lineal de  $A$  y  $B$  como puede verse fácilmente.

2. En la proposición anterior, la condición de que *al menos una de las  $\lambda_i$  sea distinta de cero* es completamente indispensable. Si quitáramos esa condición, todo conjunto de vectores resultaría linealmente dependiente pues ya sabemos que 0 es combinación lineal de cualquier conjunto de vectores.

Demostraremos ahora la proposición.

Supongamos que  $\{A_1, A_2, \dots, A_r\}$  es un conjunto linealmente dependiente de vectores. Esto significa que alguno de ellos, digamos  $A_i$ , depende linealmente de los demás:

$$A_i = \lambda_1 A_1 + \dots + \lambda_{i-1} A_{i-1} + \lambda_{i+1} A_{i+1} + \dots + \lambda_r A_r.$$

Por consiguiente,

$$\lambda_1 A_1 + \dots + \lambda_{i-1} A_{i-1} + (-1) A_i + \lambda_{i+1} A_{i+1} + \dots + \lambda_r A_r = 0,$$

es decir, existe una combinación lineal igual a cero con al menos un coeficiente distinto de cero, a saber,  $\lambda_i = -1$ .

Inversamente, supongamos ahora que hay una combinación lineal con algún coeficiente, digamos  $\lambda_i \neq 0$ :

$$\lambda_1 A_1 + \dots + \lambda_{i-1} A_{i-1} + \lambda_i A_i + \lambda_{i+1} A_{i+1} + \dots + \lambda_r A_r = 0.$$

De aquí obtenemos

$$A_i = -\frac{\lambda_1}{\lambda_i} A_1 - \dots - \frac{\lambda_{i-1}}{\lambda_i} A_{i-1} - \frac{\lambda_{i+1}}{\lambda_i} A_{i+1} - \dots - \frac{\lambda_r}{\lambda_i} A_r,$$

lo cual prueba que los vectores son linealmente dependientes.

Se dice que un conjunto de vectores es **linealmente independiente** si no es linealmente dependiente, es decir, si *ninguno de ellos es combinación lineal de los restantes*.

De la proposición anterior resulta que:

**PROPOSICIÓN 2:** *El conjunto  $\{A_1, A_2, \dots, A_r\}$  de vectores es linealmente independiente si la relación*

$$\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_r A_r = 0$$

*sólo es posible cuando  $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0$ .*

## EJERCICIOS

9. El conjunto formado por el vector 0 es linealmente dependiente.
10. El conjunto  $\{A\}$  formado con un solo vector  $A$  es linealmente independiente si y solamente si  $A \neq 0$ .
11. Si en un conjunto de vectores uno de ellos es 0 entonces el conjunto es linealmente dependiente.
12. Si un conjunto  $\{A_1, A_2, \dots, A_r\}$  es linealmente dependiente, entonces cualquier conjunto que lo contenga, digamos  $\{A_1, A_2, \dots, A_r, A_{r+1}, \dots, A_{r+s}\}$  es también linealmente dependiente. Usando esto y el ejercicio 9, demuéstrese nuevamente el ejercicio 11.

**13.** Cualquier subconjunto de un conjunto linealmente independiente de vectores es linealmente independiente.

**14.** Demuéstrese que los vectores  $(1, 0, 0)$ ,  $(0, 1, 0)$  y  $(0, 0, 1)$  en  $\mathbf{R}^3$  forman un conjunto linealmente independiente. Lo mismo para los vectores de  $\mathbf{R}^n$

$$E_1 = (1, 0, 0, \dots, 0)$$

$$E_2 = (0, 1, 0, \dots, 0)$$

.....

$$E_n = (0, 0, 0, \dots, 1)$$

**15.** Demuéstrese que los vectores  $D_1 = (1, 0, 0)$ ,  $D_2 = (1, 1, 0)$  y  $D_3 = (1, 1, 1)$  forman un conjunto linealmente independiente en  $\mathbf{R}^3$ . Generalícese el resultado a  $\mathbf{R}^n$ .

**16.** Pruébese que en  $\mathbf{R}^2$  los vectores  $(1, 0)$ ,  $(0, 1)$  y  $(3, 2)$  forman un conjunto linealmente dependiente.

**17.** Pruébese que en  $\mathbf{R}^2$  los vectores  $(-1, 1)$ ,  $(2, 3)$  y  $(5, -2)$  forman un conjunto linealmente dependiente.

**18.** En  $\mathbf{R}^3$  los vectores  $D_1$ ,  $D_2$ ,  $D_3$  y  $A = \{a_1, a_2, a_3\}$  forman un conjunto linealmente dependiente.

**19.** Generalícese el ejercicio 18 a  $\mathbf{R}^n$ .

## 5. BASES DE SUBESPACIOS VECTORIALES. DIMENSIÓN

Para definir la dimensión de un subespacio vectorial  $W$  de  $\mathbf{R}^n$  nos será útil el concepto de base.

**DEFINICIÓN 1:** Un conjunto  $\{A_1, A_2, \dots, A_r\}$  de vectores de  $\mathbf{R}^n$  es una base del subespacio vectorial  $W$  de  $\mathbf{R}^n$  si

- a)  $\{A_1, A_2, \dots, A_r\}$  es linealmente independiente.
- b)  $\{A_1, A_2, \dots, A_r\}$  genera a  $W$ .

**OBSERVACIÓN.** El conjunto  $\{0\}$  formado únicamente con el vector 0 de  $\mathbf{R}^n$  sabemos que es un subespacio vectorial de  $\mathbf{R}^n$ . Convenimos en que  $\phi$  es una base de  $\{0\}$  y, de aquí en adelante, cuando hablemos de bases de subespacios  $W$  supondremos siempre que  $W \neq \{0\}$ .

### Ejemplos:

1. Si  $E_1 = (1, 0)$  y  $E_2 = (0, 1)$ ,  $\{E_1, E_2\}$  es una base de  $\mathbf{R}^2$  pues sabemos ya que  $E_1, E_2$  forman un conjunto linealmente independiente y que genera a  $\mathbf{R}^2$ .

2.  $D_1 = (1, 0)$  y  $D_2 = (1, 1)$  forman también una base de  $\mathbf{R}^2$ .

3. En  $\mathbf{R}^n$ , los vectores

$$E_1 = (1, 0, 0, \dots, 0)$$

$$E_2 = (0, 1, 0, \dots, 0)$$

.....

$$E_n = (0, 0, 0, \dots, 1)$$

forman una base de  $\mathbf{R}^n$  que se acostumbra llamar la base canónica.

4. También

$$D_1 = (1, 0, 0, \dots, 0)$$

$$D_2 = (1, 1, 0, \dots, 0)$$

$$D_3 = (1, 1, 1, \dots, 0)$$

.....

$$D_n = (1, 1, 1, \dots, 1)$$

forman una base de  $\mathbf{R}^n$ .

5. Consideremos en  $\mathbf{R}^3$  el conjunto

$$W = \{(x, y, z) | 2x + 3y - z = 0\}.$$

$W$  es un subespacio vectorial (pruébese que se satisfacen las tres condiciones necesarias) de  $\mathbf{R}^3$ . Afirmamos que los vectores

$$P = (1, 0, 2) \quad \text{y} \quad Q = (0, 1, 3)$$

forman una base de  $W$ . En efecto si  $\lambda P + \mu Q = 0$ , tenemos

$$\lambda(1, 0, 2) + \mu(0, 1, 3) = (\lambda, \mu, 2\lambda + 3\mu) = (0, 0, 0),$$

de donde  $\lambda = \mu = 0$ , es decir,  $P$  y  $Q$  son linealmente independientes. Veremos que  $\{P, Q\}$  genera a  $W$ . Sea  $A = (x, y, z)$  en  $W$ . Entonces  $2x + 3y - z = 0$ , de donde  $z = 2x + 3y$ . Veremos que  $A = xP + yQ$ . En efecto,

$$\begin{aligned} xP + yQ &= x(1, 0, 2) + y(0, 1, 3) = \\ &= (x, 0, 2x) + (0, y, 3y) = \\ &= (x, y, 2x + 3y) = (x, y, z) = A. \end{aligned}$$

6. Si  $A \in \mathbf{R}^n$ , el conjunto  $W = \{\lambda A | \lambda \in \mathbf{R}\}$  es un subespacio vectorial de  $\mathbf{R}^n$ . Si  $A \neq 0$ ,  $W \neq \{0\}$  y entonces  $\{A\}$  es una base de  $W$ .

7. En  $\mathbf{R}^2$  el eje de las abscisas es un subespacio vectorial,  $E_1 = (1, 0)$  forma una base de éste.

8. En  $\mathbf{R}^3$  el plano  $z = 0$ , es decir, el conjunto

$$W = \{(x, y, 0)\}$$

es un subespacio vectorial de  $\mathbf{R}^3$ . Los vectores  $(1, 0, 0)$  y  $(0, 1, 0)$  forman una base de  $W$ .

## EJERCICIOS

**1.** En  $\mathbf{R}^3$ ,  $W = \{(x, y, z) | 2x - y + 5z = 0\}$  es un subespacio vectorial (demuéstrese). Pruébese que  $A = (1, 2, 0)$  y  $B = (0, 5, 1)$  forman una base de  $W$ .

**2.** Lo mismo para  $W = \{(x, y, z) | 2x - 3y + 6z = 0\}$  y  $A = (-3, 0, 1)$  y  $B = (0, 2, 1)$ .

**3.** Demuéstrese que si  $\{A, B\}$  es un conjunto linealmente independiente de vectores de  $\mathbf{R}^n$  entonces es una base de  $W = \{\lambda A + \mu B | \lambda, \mu \in \mathbf{R}\}$ .

**4.** Sea

$$W = \{(x_1, x_2, \dots, x_n) \in \mathbf{R}^n | x_1 = x_2 = \dots = x_r = 0 \ (r < n)\}.$$

Encuéntrese una base de  $W$ .

**5.** Consideremos en  $\mathbf{R}^4$

$$W = \{(x, y, z, t) | x + y + z + t = 2, x + y - z - t = 0\}.$$

Demuéstrese que  $W$  es un subespacio vectorial de  $\mathbf{R}^4$  y que

$$A = (1, 0, 1, 0) \quad y \quad B = (0, 1, 0, 1)$$

forman una base de  $W$ .

Es fácil ver geométricamente que si tomamos tres vectores en el plano  $\mathbf{R}^2$  siempre son linealmente dependientes. Veremos a continuación un resultado que generaliza esto.

**PROPOSICIÓN 1:** *Si un subespacio vectorial  $W$  de  $\mathbf{R}^n$  está generado por  $r$  vectores, entonces cualquier conjunto de  $r+1$  vectores de  $W$  es linealmente dependiente.*

**DEMOSTRACIÓN:** Por inducción sobre  $r$ . Suponemos primero que  $r = 1$  y que  $W$  está generado por  $A \neq 0$ , es decir,  $W = \{\lambda A | \lambda \in \mathbf{R}\}$ . Necesitamos demostrar que si tomamos dos vectores distintos  $B_1$  y  $B_2$  en  $W$ , estos forman un conjunto linealmente dependiente. Sea  $B_1 = \lambda_1 A$  y  $B_2 = \lambda_2 A$ . Como  $\lambda_1 \neq \lambda_2$ , alguna de estas  $\lambda_i$  es distinta de cero, digamos  $\lambda_1 \neq 0$ . Entonces

$$B_2 = \frac{\lambda_2}{\lambda_1} B_1,$$

lo cual prueba la dependencia lineal.

Supongamos ahora cierto el resultado para  $r$ . Lo probaremos para  $r+1$ . Supongamos que  $A_1, A_2, \dots, A_r, A_{r+1}$  generan  $W$  y que  $B_1, B_2, \dots, B_{r+1}, B_{r+2} \in W$ . Debemos probar que estos últimos son linealmente dependientes. Podemos escribir

$$B_1 = \alpha_{11}A_1 + \cdots + \alpha_{1r}A_r + \gamma_1 A_{r+1}$$

$$B_2 = \alpha_{21}A_1 + \cdots + \alpha_{2r}A_r + \gamma_2 A_{r+1}$$

.....

$$B_{r+2} = \alpha_{r+21}A_1 + \cdots + \alpha_{r+2r}A_r + \gamma_{r+2} A_{r+1}.$$

Supongamos que alguna  $\gamma_i$ , digamos  $\gamma$ , es distinta de cero. Los vectores  $B'_1, \dots, B'_{r+1}$  definidos por

$$B'_1 = B_2 - \frac{\gamma_2}{\gamma_1} B_1, \dots, B'_{r+1} = B_{r+2} - \frac{\gamma_{r+2}}{\gamma_1} B_1$$

pertenecen al espacio vectorial  $W'$  generado por  $\{A_1, A_2, \dots, A_r\}$  (pruébelo) y entonces, por hipótesis de inducción  $\{B'_1, \dots, B'_{r+1}\}$  es linealmente dependiente. Luego, existe una combinación lineal

$$\lambda_1 B'_1 + \cdots + \lambda_{r+1} B'_{r+1} = 0$$

con alguna  $\lambda_i \neq 0$ . Sustituyendo, obtenemos

$$\lambda_1 B_2 + \cdots + \lambda_{r+1} B_{r+2} + \left( -\frac{\lambda_1 \gamma_2}{\gamma_1} - \cdots - \frac{\lambda_{r+1} \gamma_{r+2}}{\gamma_1} \right) B_1 = 0$$

lo cual prueba que  $\{B_1, B_2, \dots, B_{r+2}\}$  es linealmente dependiente pues alguna  $\lambda_i \neq 0$ .

El caso  $\gamma_1 = \gamma_2 = \cdots = \gamma_{r+2} = 0$  se deja como ejercicio.

**COROLARIO 1:** Si un subespacio vectorial  $W$  de  $\mathbf{R}^n$  está generado por  $r$  vectores, entonces cualquier conjunto de más de  $r$  vectores de  $W$  es linealmente dependiente.

Esto es consecuencia de la proposición anterior y de que cualquier conjunto que contenga a un subconjunto linealmente dependiente es linealmente dependiente.

**COROLARIO 2:** En  $\mathbf{R}^n$  cualquier conjunto de más de  $n$  vectores es linealmente dependiente.

En efecto, en  $\mathbf{R}^n$  hay conjuntos con  $n$  vectores que generan  $\mathbf{R}^n$ , por ejemplo, la base canónica.

**Existencia de bases.** Demostraremos a continuación que todo conjunto linealmente independiente de vectores de  $W$  puede “extenderse” a una base de  $W$ . Para ello demostraremos primero el siguiente

**LEMA:** Sea  $\{B_1, B_2, \dots, B_r\}$  un conjunto linealmente independiente de vectores de  $\mathbf{R}^n$  y  $W$  el subespacio vectorial que genera. Si  $B$  es un vector

de  $\mathbf{R}^n$  que no está en  $W$ , entonces  $\{B_1, B_2, \dots, B_r, B\}$  es linealmente independiente.

**DEMOSTRACIÓN:** Supongamos que

$$\lambda_1 B_1 + \dots + \lambda_r B_r + \lambda B = 0. \quad (*)$$

En primer lugar, tenemos que  $\lambda = 0$  pues en caso contrario tendríamos que

$$B = \left( -\frac{\lambda_1}{\lambda} \right) B_1 + \dots + \left( -\frac{\lambda_r}{\lambda} \right) B_r,$$

lo cual no es posible ya que  $B \notin W$ . Entonces la relación (\*) queda

$$\lambda_1 B_1 + \dots + \lambda_r B_r = 0$$

y como  $\{B_1, \dots, B_r\}$  es linealmente independiente tenemos  $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0$ . En resumen, la condición (\*) implica que todas las  $\lambda$  son cero, es decir,  $\{B_1, \dots, B_r, B\}$  es linealmente independiente.

**TEOREMA 1:** Sea  $W$  un subespacio vectorial de  $\mathbf{R}^n$  y  $\{B_1, \dots, B_r\}$  un conjunto linealmente independiente de vectores de  $W$ . Entonces existen vectores  $B_{r+1}, B_{r+2}, \dots, B_{r+s}$  en  $W$  tales que

$$\{B_1, \dots, B_r, B_{r+1}, \dots, B_{r+s}\}$$

es una base de  $W$ .

*Demostración.* Si  $\{B_1, \dots, B_r\}$  genera a  $W$  no hay nada que demostrar pues, en este caso, en una base de  $W$ . En el caso contrario, si  $W_1$  es el subespacio generado por  $\{B_1, \dots, B_r\}$ ,  $W_1 \subset W$  y  $W_1 \neq W$ . Entonces podemos tomar un vector  $B_{r+1} \in W - W_1$ . Por el lema anterior,  $\{B_1, \dots, B_r, B_{r+1}\}$  es linealmente independiente.

Ahora bien, si este último genera  $W$ , es una base de  $W$  y queda probado el teorema. En caso contrario, procediendo en igual forma obtenemos un conjunto linealmente independiente  $\{B_1, \dots, B_r, B_{r+1}, B_{r+2}\}$ .

Este proceso debe terminar antes de que  $r+s$  sea mayor que  $n$  pues de lo contrario obtendríamos más de  $n$  vectores linealmente independientes en  $\mathbf{R}^n$ .

Luego existe una  $s$  tal que  $\{B_1, \dots, B_r, B_{r+1}, \dots, B_{r+s}\}$  es una base de  $W$  y el teorema queda probado.

Lo anterior demuestra la existencia de bases:

**PROPOSICIÓN 2:** Todo subespacio vectorial de  $\mathbf{R}^n$  tiene base.

*Demostración.* Si  $W = \{0\}$  convenimos que tiene como base al conjunto vacío. Sea pues  $W \neq \{0\}$ . Entonces hay en  $W$  vectores distintos de

cero. Sea  $B_1 \in W$ ,  $B_1 \neq 0$ .  $\{B_1\}$  es linealmente independiente y la proposición se sigue del teorema anterior.

**Dimensión.** Veremos ahora el concepto de dimensión de un subespacio vectorial.

**TEOREMA 2:** *Todas las bases de un subespacio  $W$  de  $\mathbf{R}^n$  tienen el mismo número de elementos.*

**DEMOSTRACIÓN:** Sean  $\{A_1, \dots, A_r\}$  y  $\{B_1, \dots, B_s\}$  dos bases de  $W$ . Demostaremos que  $r=s$ .

En primer lugar, ya que  $\{A_1, \dots, A_r\}$  genera a  $W$  y  $\{B_1, \dots, B_s\}$  es linealmente independiente, por el corolario 1 de 4.2, resulta que  $s \leq r$ . Invirtiendo los papeles resulta que  $r \leq s$ , de donde,  $r=s$ .

**DEFINICIÓN 2:** *La dimensión de un subespacio vectorial  $W$  de  $\mathbf{R}^n$  es el número de elementos de cualquier base de  $W$ .*

### Ejemplos:

9.  $\mathbf{R}^n$  es de dimensión  $n$  puesto que la base canónica tiene  $n$  vectores. Por ello se dice que la recta  $\mathbf{R}^1 = \mathbf{R}$  es de dimensión 1, el plano  $\mathbf{R}^2$  es de dimensión 2 y que  $\mathbf{R}^3$  es un espacio tridimensional.

10. Cualquier recta en  $\mathbf{R}^2$  (que pase por el origen) es de dimensión 1.
11.  $\{0\}$  es de dimensión 0 (= número de elementos de  $\emptyset$ ).
12. En  $\mathbf{R}^3$  las rectas (a través de 0) son subespacios de dimensión 1 y los planos (a través de 0) son subespacios de dimensión 2.
13. En  $\mathbf{R}^n$  se llaman rectas a los subespacios de dimensión 1, es decir, a los generados por un vector no nulo.
14. En  $\mathbf{R}^n$  se llaman hiperplanos a los subespacios de dimensión  $n-1$ , es decir, a los generados por  $n-1$  vectores linealmente independientes.

### EJERCICIOS

6. Demuéstrese que en  $\mathbf{R}^2$  dos vectores linealmente independientes constituyen una base de  $\mathbf{R}^2$ . Generalícese y demuéstrese el resultado para  $\mathbf{R}^n$ .
7. Demuéstrese que en  $\mathbf{R}^2$  dos vectores que generen  $\mathbf{R}^2$  constituyen una base de  $\mathbf{R}^2$ . Generalícese y demuéstrese el resultado para  $\mathbf{R}^n$ .
8. Si  $W$  es un subespacio de dimensión  $r$  entonces
  - a) cualquier conjunto linealmente independiente de  $r$  vectores de  $W$  es una base de  $W$ ;
  - b) cualquier conjunto de  $r$  vectores que genere a  $W$  es una base de  $W$ .
9. Examíñese la dimensión en los ejemplos 1 a 8 y en los ejercicios 1 a 5 de este párrafo.
10. Demuéstrese que todo conjunto  $\{B_1, \dots, B_r\}$  de generadores de un subespacio vectorial contiene una base de  $W$ .

**SUGERENCIA:** Considérense todos los subconjuntos linealmente independientes de  $\{B_1, \dots, B_r\}$ . Tómese uno que tenga un número máximo de elementos y pruebe que es base.

**11.** Si  $V$  y  $W$  son dos subespacios de la misma dimensión y  $V \subset W$ , entonces  $V = W$ .

**SUGERENCIA:** Sea  $\{B_1, \dots, B_r\}$  una base de  $V$  y  $a \in W$ . Entonces  $\{B_1, \dots, B_r, A\}$  es un conjunto linealmente dependiente de vectores de  $W$ .





# Matrices y determinantes

## 1. MATRICES

EN el estudio de algunos temas de matemáticas y en muchas aplicaciones aparecen arreglos rectangulares de elementos. Por ejemplo, al estudiar sistemas de ecuaciones lineales, es decir, sistemas de la forma

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{array} \right.$$

podemos formar, con los coeficientes de  $x_1, x_2, \dots, x_n$ , el siguiente arreglo:

$$\left[ \begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array} \right].$$

A este tipo de arreglos les llamaremos **matrices**. Hablaremos de **renglones** y **columnas** de una matriz. Así, diremos que la matriz anterior tiene  $m$  renglones y  $n$  columnas. A veces, para abreviar, diremos que es una matriz de  $m \times n$ .

Con los términos libres del sistema de ecuaciones mencionado podemos formar una matriz de  $m \times 1$ :

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Veamos un ejemplo; con los coeficientes y con los términos libres del sistema

$$\begin{aligned} 3x + 2y - z &= 1 \\ x - y &= 3 \\ x - 2y + 3z &= -1 \end{aligned}$$

podemos formar las matrices

$$\begin{bmatrix} 3 & 2 & -1 \\ 1 & -1 & 0 \\ 1 & -2 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 3 \\ -1 \end{bmatrix}.$$

En general, los elementos con que se forman matrices son elementos de un cierto campo. En este capítulo consideraremos matrices formadas con números reales pero todo lo que se diga será válido para matrices formadas con números complejos o con elementos de un campo cualquiera.

Como lo hicimos al escribir la matriz del sistema de ecuaciones con el que iniciamos nuestra discusión, se acostumbra denotar con  $a_{ij}$  al elemento que ocupa el renglón  $i$  y la columna  $j$ . Así, por ejemplo,  $a_{24}$  es el elemento que ocupa el segundo renglón en la cuarta columna y  $a_{42}$  el que ocupa el cuarto renglón y la segunda columna.

Así, una matriz como la anterior la denotaremos a veces

$$(a_{ij}), \quad (1 \leq i \leq m, \quad 1 \leq j \leq n)$$

indicando el número de renglones y el de columnas o bien, si estos se sobreentienden, simplemente escribiremos  $(a_{ij})$ .

A las matrices de  $n \times n$  las llamaremos matrices **cuadradas**.

En una matriz cuadrada, a los elementos de la forma  $a_{ii}$  los llamaremos **elementos diagonales** y diremos que  $a_{11}, a_{22}, \dots, a_{nn}$  es la diagonal principal.

Si en una matriz cuadrada todos los elementos no diagonales son cero diremos que la matriz es **diagonal**. Por ejemplo

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 2 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

son matrices diagonales.

Los elementos  $a_{ij}$ , con  $i > j$  diremos que están **debajo de la diagonal** y los  $a_{ij}$ , con  $i < j$  diremos que están **arriba de la diagonal**.

Una matriz cuadrada se dice que es **triangular** si todos los elementos debajo (o arriba) de la diagonal son cero. Por ejemplo,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ -1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 5 & 3 \end{pmatrix}$$

son matrices triangulares.

A las matrices que constan de ceros se les llama matrices nulas o matrices 0.

Las matrices de  $1 \times 1$ , ( $a_{11}$ ), se pueden identificar con los números reales  $a_{11}$ .

Con frecuencia será conveniente pensar en los renglones de una matriz de  $m \times n$ :

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

como vectores del espacio vectorial  $\mathbf{R}^n$ :

$$\begin{aligned} R_1 &= (a_{11}, a_{12}, \dots, a_{1n}) \\ R_2 &= (a_{21}, a_{22}, \dots, a_{2n}) \\ &\dots \\ R_m &= (a_{m1}, a_{m2}, \dots, a_{mn}). \end{aligned}$$

También podemos pensar en las columnas de la matriz  $A$  como vectores del espacio vectorial  $\mathbf{R}^m$ :

$$\begin{aligned} C_1 &= (a_{11}, a_{21}, \dots, a_{m1}) \\ C_2 &= (a_{12}, a_{22}, \dots, a_{m2}) \\ &\dots \\ C_n &= (a_{1n}, a_{2n}, \dots, a_{mn}). \end{aligned}$$

Si la matriz  $B$  se obtiene suprimiendo cualquier número de renglones y de columnas de cierta matriz  $A$  se dirá que  $B$  es una **submatriz** de la matriz  $A$ . Por ejemplo, si

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \\ 3 & 1 & 3 & 1 & 3 \end{pmatrix} \text{ y } B = \begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix},$$

$B$  es una submatriz de  $A$ , pues se obtiene de  $A$  al eliminar el primer renglón y la primera, tercera y quinta columnas.

## EJERCICIOS

1. Escríbanse las matrices formadas con los coeficientes de las incógnitas y las formadas con los términos libres de los siguientes sistemas:

$$\left\{ \begin{array}{l} x + y + z + t = 1 \\ x + 2y + 3z + 4t = 2 \\ y + 2z + 3t = 3 \\ z + 2t = 4 \\ t = 5 \end{array} \right. \quad \left\{ \begin{array}{l} ax_1 + bx_2 + cx_3 = 0 \\ cx_1 + ax_2 + bx_3 = 0 \\ bx_1 + cx_2 + ax_3 = 0 \end{array} \right.$$

Sean

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix} = \begin{pmatrix} 2 & -1 & -4 & -3 \\ 0 & -1 & 0 & -1 \\ -1 & 2 & -2 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} = \begin{pmatrix} -1 & 0 & -2 \\ 2 & 2 & 0 \\ 3 & 0 & -2 \end{pmatrix}.$$

2. Escríbase la matriz  $(c_{ij})$  ( $i = 1, 2, 3; j = 1, 2, 3$ ) tal que

$$c_{ij} = b_{ji}.$$

3. Escríbase la matriz  $d_{ij}$  ( $i = 1, 2, 3, 4; j = 1, 2, 3$ ) tal que

$$d_{ij} = a_{ji}.$$

[Las matrices  $(c_{ij})$  y  $(d_{ij})$  se llaman **transpuestas** de las matrices  $B$  y  $A$ , respectivamente.]

4. Escríbase la matriz  $(e_{ij})$  ( $i = 1, 2, 3; j = 1, 2, 3$ ) tal que

$$\begin{aligned} e_{ij} &= b_{ij} & \text{si } i \geq j \\ e_{ij} &= 0 & \text{si } i < j. \end{aligned}$$

5. Escríbase la matriz  $(f_{ij})$  ( $i, j = 1, 2, 3$ ) tal que

$$f_{ii} = b_{ii} \quad \text{y} \quad f_{ij} = 0 \quad \text{si} \quad i \neq j.$$

6. Escríbase la matriz que se obtiene de  $A$  intercambiando las dos primeras columnas.

7. Escríbase la matriz  $(g_{ij})$  ( $i = 1, 2, 3; j = 1, 2, 3, 4$ ) tal que para  $i = 1, 2, 3$ ,

$$g_{i1} = a_{i2}, g_{i2} = a_{i1}, g_{i3} = a_{i3}, g_{i4} = a_{i4}.$$

(Compárense los resultados de los ejercicios 6 y 7).

8. Escríbase la matriz que se obtiene de  $A$  intercambiando el segundo y el tercer renglón. Si se llama  $(h_{ij})$  a esta matriz relacionese  $h_{ij}$  con  $a_{ij}$  tal como se hizo en el ejercicio 7.

9. Escríbase la matriz  $(p_{ij})$  ( $i = 1, 2, 3; j = 1, 2, 3, 4$ ) tal que para  $j = 1, 2, 3, 4$ ,

$$p_{1j} = a_{1j}, p_{2j} = a_{1j} + a_{2j}, p_{3j} = a_{3j}.$$

**10.** Escríbase la matriz que se obtiene de  $A$  al sumar al segundo renglón el primero. Compárese con el ejercicio anterior.

**11.** Escríbase la matriz que se obtiene de  $B$  al sumar a la tercera columna la primera. Si se llama  $(q_{ij})$  a esta escribanse las relaciones que hay entre  $p_{ij}$  con  $b_{ij}$  tal como se hizo en el ejercicio 10.

**12.** Escríbase la matriz  $(r_{ij})$  ( $i = 1, 2, 3; j = 1, 2, 3, 4$ ) tal que  $r_{2j} = 3a_{2j}$  ( $j = 1, 2, 3, 4$ ) y en todos los demás casos  $r_{ii} = a_{ij}$ . Describáse lo hecho.

## 2. EL RANGO DE UNA MATRIZ

Se dice que el rango de una matriz

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

es  $r$  si  $r$  es la dimensión del subespacio vectorial de  $\mathbf{R}^n$  generado por los renglones

$$\begin{aligned} R_1 &= (a_{11}, a_{12}, \dots, a_{1n}) \\ R_2 &= (a_{21}, a_{22}, \dots, a_{2n}) \\ &\dots \dots \dots \dots \dots \\ R_m &= (a_{m1}, a_{m2}, \dots, a_{mn}). \end{aligned}$$

En el último párrafo de este capítulo se demostrará que el rango es igual también a la dimensión del subespacio vectorial de  $\mathbf{R}^m$  generado por las columnas

$$\begin{aligned} C_1 &= (a_{11}, a_{21}, \dots, a_{m1}) \\ C_2 &= (a_{12}, a_{22}, \dots, a_{m2}) \\ &\dots \dots \dots \dots \\ C_n &= (a_{1n}, a_{2n}, \dots, a_{mn}). \end{aligned}$$

Evidentemente se tiene que  $r \leq m$ . Además, ya que  $R_1, R_2, \dots, R_m$  pertenecen a  $\mathbf{R}^n$ , la dimensión  $r$  del subespacio que generan es menor o igual que  $n$ . Es decir,

$$r \leq m \quad y \quad r \leq n.$$

## EJERCICIOS

**1.** Encuéntrese el rango de las siguientes matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 0 \\ i & i & i & \cdots & i \end{pmatrix}$$

(de  $n \times n$ )(de  $n \times n$ )

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2. Sean  $A = (a_1, a_2, a_3)$ ,  $B = (b_1, b_2, b_3)$  dos vectores de  $\mathbf{R}^3$  linealmente independientes. Encuéntrese el rango de las siguientes matrices:

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ 2a_1 & 2a_2 & 2a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \quad \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix} \quad \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ a_1 + b_1 & a_2 + b_2 & a_3 + b_3 \end{pmatrix} \quad \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ 2a_1 + 3b_1 & 2a_2 + 3b_2 & 2a_3 + 3b_3 \end{pmatrix}.$$

**Operaciones elementales.** Para encontrar el rango de una matriz nos serán útiles las llamadas **operaciones elementales** (por renglones) en matrices. Estas son:

1. Intercambio de renglones.
2. Multiplicación de un renglón por un número *distinto de cero*.
3. Sumar a un renglón otro renglón.

Diremos que dos matrices son equivalentes si se puede obtener una de la otra mediante un número finito de operaciones elementales. Si dos matrices  $A$  y  $B$  son equivalentes escribiremos  $A \sim B$ .

### Ejemplo:

1. Las dos matrices siguientes son equivalentes porque la segunda se obtuvo de la primera intercambiando el primer y el tercer renglón:

$$\begin{pmatrix} 1 & 3 & 2 & 4 \\ 0 & 1 & 2 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Las dos matrices siguientes son equivalentes pues la segunda se obtuvo de la primera multiplicando el tercer renglón por  $-1$ :

$$\begin{bmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{bmatrix} \sim \begin{bmatrix} a & b & c \\ a' & b' & c' \\ -a'' & -b'' & -c'' \end{bmatrix}.$$

Las dos matrices siguientes son equivalentes pues la segunda se obtuvo de la primera sumando al tercer renglón el segundo

$$\begin{bmatrix} 1 & 3 & 2 & 4 \\ 0 & 1 & 2 & 3 \\ 2 & 1 & 3 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 2 & 4 \\ 0 & 1 & 2 & 3 \\ 2 & 2 & 5 & 7 \end{bmatrix}.$$

### EJERCICIO

3. Dígase qué operaciones elementales se han efectuado para obtener las siguientes matrices equivalentes:

$$\begin{aligned} \begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} &\sim \begin{pmatrix} 2a & 2b & 2c & 2d \\ a' & b' & c' & d' \end{pmatrix} \\ &\sim \begin{pmatrix} 2a & 2b & 2c & 2d \\ a' + 2a & b' + 2b & c' + 2c & d' + 2d \end{pmatrix} \\ &\sim \begin{pmatrix} a & b & c & d \\ a' + 2a & b' + 2b & c' + 2c & d' + 2d \end{pmatrix} \\ \begin{pmatrix} a & b \\ a' & b' \\ a'' & b'' \end{pmatrix} &\sim \begin{pmatrix} a & b \\ 2a' & 2b' \\ a'' & b'' \end{pmatrix} \sim \begin{pmatrix} a + 2a' & b + 2b' \\ 2a' & 2b' \\ a'' & b'' \end{pmatrix} \sim \begin{pmatrix} a + 2a' & b + 2b' \\ a' & b' \\ a'' & b'' \end{pmatrix} \sim \\ &\sim \begin{pmatrix} a + 2a' & b + 2b' \\ a' & b' \\ -3a'' & -3b'' \end{pmatrix} \sim \begin{pmatrix} a + 2a' - 3a'' & b + 2b' - 3b'' \\ a' & b' \\ -3a'' & -3b'' \end{pmatrix} \\ &\sim \begin{pmatrix} a + 2a' - 3a'' & b + 2b' - 3b'' \\ a' & b' \\ a'' & b'' \end{pmatrix}. \end{aligned}$$

El ejercicio anterior indica cómo podemos obtener una matriz equivalente sumando a un renglón un múltiplo (no nulo) de otro renglón o también, en general, sumando a un renglón una combinación lineal de los demás renglones.

En forma parecida, el siguiente ejemplo nos indica cómo proceder para obtener una matriz equivalente sumando a cada renglón un múltiplo (no nulo) de un renglón fijo (en este ejemplo, el primero),

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix} &\sim \begin{pmatrix} 2a & 2b \\ c & d \\ e & f \end{pmatrix} \sim \begin{pmatrix} 2a & 2b \\ c+2a & d+2b \\ e & f \end{pmatrix} \sim \\ &\sim \begin{pmatrix} a & b \\ c+2a & d+2b \\ e & f \end{pmatrix} \sim \begin{pmatrix} 3a & 3b \\ c+2a & d+2b \\ e+3a & f+3b \end{pmatrix} \sim \begin{pmatrix} a & b \\ c+2a & d+2b \\ e+3a & f+3b \end{pmatrix}. \end{aligned}$$

Así, podemos escribir directamente

$$\begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix} \sim \begin{pmatrix} a & b \\ c+2a & d+2b \\ e+3a & f+3b \end{pmatrix}.$$

Esto nos permite “hacer ceros” debajo de un elemento distinto de cero. Por ejemplo, se trata de encontrar una matriz equivalente a

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

y tal que “debajo” del 1 haya cero y cero. Podemos proceder así:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ -3 & -4 & -5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 2+(-2)(1) & 3+(-2)(2) & 4+(-2)(3) \\ -3+3(1) & -4+3(2) & -5+3(3) \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 2 & 4 \end{pmatrix}.$$

### EJERCICIO

4. Encuéntrense matrices equivalentes a cada una de las siguientes matrices y que tengan ceros en la primera columna, a partir del segundo renglón:

$$\begin{array}{ccc} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 3 & 1 & 3 & 1 \end{pmatrix} & \begin{pmatrix} -1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \begin{pmatrix} 2 & 3 & 4 \\ 6 & 8 & 10 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 3 & 1 & 3 & 1 \\ 2 & 2 & 2 & 2 \end{pmatrix} & \begin{pmatrix} -1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 5 \\ 3 & 3 & 3 & 0 \end{pmatrix} & \begin{pmatrix} 2 & 3 & 4 & 6 \\ 6 & 8 & 10 & 0 \\ -4 & 3 & 0 & 8 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 6 \end{pmatrix} & \begin{pmatrix} -1 & 0 & -1 \\ 2 & -1 & 2 \\ -3 & 2 & -3 \\ 4 & 3 & 4 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 \\ 1 & 3 & 2 \\ 0 & 1 & 2 \\ 3 & 1 & 3 \end{pmatrix}. \end{array}$$

En el teorema siguiente enunciamos una propiedad importante relativa a las operaciones elementales.

**TEOREMA:** *Las operaciones elementales no alteran el rango.*

De aquí, se sigue que

**COROLARIO:** *Si dos matrices son equivalentes entonces tienen el mismo rango.*

*Demostración del teorema.* Sean  $R_1, R_2, \dots, R_m$  los renglones de una matriz  $A$ . El rango de  $A$  es, por definición, la dimensión del subespacio vectorial generado por  $\{R_1, R_2, \dots, R_m\}$ . Si intercambiamos dos renglones, por ejemplo el primero y el segundo, obtenemos una matriz  $A'$  cuyos renglones son  $R_2, R_1, R_3, \dots, R_m$ . Pero, como conjuntos,

$$\{R_1, R_2, R_3, \dots, R_m\} = \{R_2, R_1, R_3, \dots, R_m\}$$

por lo que los renglones de  $A$  y  $A'$  generan *el mismo* subespacio vectorial, por lo que  $A$  y  $A'$  tienen el mismo rango.

La demostración de que las operaciones elementales 2 y 3 no alteran el rango es análoga a la anterior y se basa en los ejercicios siguientes.

## EJERCICIOS

5. Si  $R_1, R_2$  y  $R_3$  son vectores de  $\mathbf{R}^n$  demuéstrese que  $\{R_1, R_2, R_3\}$  y  $\{\lambda R_1, R_2, R_3\}$  ( $\lambda \neq 0$ ) generan el mismo subespacio vectorial. [Pruébese que todo vector que sea combinación lineal de  $\{R_1, R_2, R_3\}$  es también combinación lineal de  $\{\lambda R_1, R_2, R_3\}$  e inversamente.]

6. Si  $R_1, R_2$  y  $R_3$  son vectores de  $\mathbf{R}^n$  demuéstrese que  $\{R_1, R_2, R_3\}$  y  $\{R_1 + R_2, R_2, R_3\}$  generan el mismo subespacio vectorial.

Lo que trataremos ahora es, dada una matriz  $A$ , encontrar otra equivalente  $A'$  para la cual sea fácil encontrar su rango. Como  $A$  y  $A'$  tienen el mismo rango (corolario anterior), con esto resolveremos el problema de calcular el rango de una matriz arbitraria  $A$ .

Las matrices para las que será fácil encontrar el rango son las matrices escalonadas.

Diremos que una matriz es **escalonada** si *el primer elemento distinto de cero de cada renglón está más a la derecha del primer elemento distinto de cero del renglón anterior*.

Por ejemplo, las siguientes matrices son escalonadas:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Las tres siguientes no lo son

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Es fácil ver que *el rango de una matriz escalonada es igual al número de renglones de ella distintos de cero*.

Para esto basta ver que los renglones distintos de cero de la matriz escalonada son linealmente independientes pues entonces su número es precisamente la dimensión del espacio vectorial que generan, es decir, el rango de la matriz.

Nada mejor que un ejemplo para que nos demos cuenta de esto. Consideremos la siguiente matriz escalonada:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Los renglones distintos de cero son

$$R_1 = (1, 2, 3, 4, 5) \quad R_2 = (0, 1, 1, 1, 1) \quad y \quad R_3 = (0, 0, 0, 1, 1).$$

Supongamos que  $\lambda_1 R_1 + \lambda_2 R_2 + \lambda_3 R_3 = 0$ , es decir, que

$$(\lambda_1, 2\lambda_1 + \lambda_2, 3\lambda_1 + \lambda_2, 4\lambda_1 + \lambda_2 + \lambda_3, 5\lambda_1 + \lambda_2 + \lambda_3) = 0.$$

Entonces  $\lambda_1 = 0$ ,  $2\lambda_1 + \lambda_2 = 0$ ,  $3\lambda_1 + \lambda_2 = 0$ ,  $4\lambda_1 + \lambda_2 + \lambda_3 = 0$  y  $5\lambda_1 + \lambda_2 + \lambda_3 = 0$ . Esto implica que  $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = 0$ , lo cual demuestra que  $\{R_1, R_2, R_3\}$  es linealmente independiente.

La demostración del caso general es la misma que la de este ejemplo, excepto por complicaciones de notación. La omitiremos.

Finalmente veremos cómo encontrar una matriz escalonada que sea equivalente a una matriz dada. Lo más simple es analizar varios ejemplos.

### Ejemplos:

2. Para encontrar el rango de la matriz

$$A = \begin{pmatrix} 1 & -1 & 3 & -5 \\ 2 & -3 & 4 & -10 \\ -3 & 3 & -9 & 15 \\ 3 & -3 & -6 & -4 \end{pmatrix}$$

hacemos, como en el ejercicio 4, que debajo del número 1 de la primera columna haya ceros:

$$A \sim \begin{pmatrix} 1 & -1 & 3 & -5 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -15 & 11 \end{pmatrix}$$

y para llegar a una matriz escalonada basta intercambiar los dos últimos renglones, obteniendo

$$A \sim \begin{pmatrix} 1 & -1 & 3 & -5 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & -15 & 11 \\ 0 & 0 & 0 & 0 \end{pmatrix} = A'$$

Como  $A'$  es escalonada y tiene tres renglones distintos de cero, su rango es 3 y como  $A$  es equivalente a  $A'$ , el rango de  $A$  es también 3.

3.

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 1 & 0 \\ 0 & -1 & -2 & -4 & 2 & 1 \\ 0 & 0 & 0 & 2 & 0 & -1 \\ 0 & 1 & 2 & 2 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 0 & -1 & 3 & 1 \\ 0 & 0 & 0 & 2 & 0 & -1 \\ 0 & 1 & 2 & 2 & 4 & 1 \end{pmatrix} \sim \\ \sim \begin{pmatrix} 0 & 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 0 & -1 & 3 & 1 \\ 0 & 0 & 0 & 2 & 0 & -1 \\ 0 & 0 & 0 & -1 & 3 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 0 & -1 & 3 & 1 \\ 0 & 0 & 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = A'$$

$A'$  es de rango 3;  $A$  es equivalente a  $A'$ ; por lo tanto el rango de  $A$  es 3.

### EJERCICIOS

Procediendo como en los ejemplos anteriores encuéntrense los rangos de las siguientes matrices:

7.

$$\begin{pmatrix} 1 & -1 & 2 & 0 \\ 2 & -1 & -3 & 1 \\ 0 & 1 & -1 & 1 \\ 1 & 0 & -1 & 1 \\ 1 & 2 & 1 & 3 \end{pmatrix}$$

8.

$$\begin{pmatrix} 1 & -1 & -1 & 0 \\ 2 & -1 & 1 & 0 \\ 3 & -2 & 1 & -1 \\ 1 & 1 & 5 & 0 \\ 2 & 1 & 7 & 0 \end{pmatrix}$$

9.

$$\begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & 1 & -3 & -1 \\ 2 & 1 & -3 & 1 \\ 1 & 2 & -2 & 1 \end{pmatrix}$$

10.

$$\begin{pmatrix} 1 & 1 & 1 & -2 & -2 & 5 \\ 2 & -1 & 0 & -1 & -2 & 0 \\ 2 & 0 & -1 & -2 & -1 & 0 \\ 0 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$

11.

$$\begin{pmatrix} 2 & 1 & -1 & 1 & 3 \\ 1 & 2 & 1 & -1 & 3 \\ 1 & 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 3 & 1 & -2 & 2 & 4 \\ 1 & 3 & 2 & -2 & 4 \end{pmatrix}$$

12.

$$\begin{pmatrix} 1 & -1 & 1 & 1 & 2 & -1 \\ -1 & 1 & 1 & 1 & -4 & 3 \\ -1 & -1 & 1 & 1 & -2 & 3 \\ 1 & -2 & 1 & 2 & 3 & -1 \\ 0 & -4 & 1 & 5 & 3 & 1 \end{pmatrix}$$

### 3. PERMUTACIONES

En el estudio de los determinantes que haremos en los siguientes párrafos, nos serán útiles algunos resultados concernientes a las permutaciones. A estas dedicaremos este párrafo.

Recordemos que una permutación de un conjunto  $I_n = \{1, 2, \dots, n\}$  es una función biyectiva  $\sigma: I_n \rightarrow I_n$ . Biyectiva significa que todo elemento de  $I_n$  es imagen, bajo  $\sigma$ , de uno y solamente un elemento de  $I_n$ .

Denotaremos con  $S_n$  al conjunto de todas las permutaciones de  $I_n$ . Sabemos que hay  $n!$  Por ejemplo, las permutaciones de  $I_2 = \{1, 2\}$  son

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

y las de  $I_3 = \{1, 2, 3\}$  son

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

[No debemos confundir esta notación para las funciones con la notación para matrices. Aquí, por ejemplo,

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

es la función  $\sigma: I_3 \rightarrow I_3$  dada por  $\sigma(1) = 2$ ,  $\sigma(2) = 3$  y  $\sigma(3) = 1$ .]

Si  $\sigma: I_n \rightarrow I_n$  es una permutación, acostumbramos escribir

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

y, a veces, simplemente el segundo renglón:

$$\sigma = (\sigma(1), \sigma(2), \dots, \sigma(n)).$$

**Permutaciones pares e impares.** Para definir cuándo una permutación es par o impar nos será útil el concepto de inversión. Empecemos con un ejemplo.

En la permutación

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

diremos que los elementos 7 y 1 (del segundo renglón) forman una inversión. También los elementos 3 y 1; también 6 y 2. En cambio 3 y 7 no forman inversión, ni 1 y 5, ni 3 y 6.

Siguiendo esta idea diremos que 2 números (del segundo renglón) forman inversión si el mayor está antes que el menor. Si el menor está a la izquierda diremos que no forman inversión.

Más precisamente,  $\sigma(i)$ ,  $\sigma(j)$  forman inversión si

$$i < j \text{ y } \sigma(i) > \sigma(j).$$

Examinemos ahora cuántas inversiones hay en la permutación que dimos como ejemplo. Forman inversión:

- 1 con 3, 1 con 7;
- 2 con 3, 2 con 7, 2 con 5 y 2 con 6;
- 4 con 5, 4 con 6 y 4 con 7;
- 5 con 7;
- 6 con 7.

Así pues en la permutación  $\sigma$  hay 11 inversiones.

Obsérvese que para contar cuántas inversiones hay en una permutación basta contar cuántos números mayores que 1 preceden a 1, cuántos mayores que 2 preceden a 2, etc., hasta  $n - 1$ .

## EJERCICIOS

1. Encuéntrense todas las inversiones en cada una de las permutaciones siguientes:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

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

2. Encuéntrese el número de inversiones en cada una de las permutaciones siguientes (para abreviar escribimos solamente el segundo renglón):

$$(2, 1, 3, 4, 5) \quad (3, 2, 1, 4, 5) \quad (4, 2, 3, 1, 5) \quad (5, 2, 3, 4, 1)$$

$$(7, 2, 6, 3, 5, 4, 1) \quad (1, 3, 4, 2) \quad (1, 4, 3, 2) \quad (3, 2, 1)$$

*Se dice que una permutación es par si tiene un número par de inversiones y que es impar si tiene un número impar de inversiones.*

Por ejemplo, la permutación  $(1, 2, 3, 4, 5)$  es par pues tiene cero inversiones. La permutación  $(2, 1, 3, 4, 5)$  es impar pues tiene una inversión.  $(2, 3, 1)$  es par pues tiene dos inversiones. La permutación que antes examinamos,

$$\sigma = (3, 7, 1, 5, 6, 2, 4),$$

es impar pues tiene 11 inversiones.

## EJERCICIOS

3. Encuéntrese la paridad de las permutaciones de los dos ejercicios anteriores.

4. Escríbanse las  $3!$  permutaciones de  $I_3$  y encuéntrense cuáles son pares y cuáles impares.

5. Lo mismo para  $I_4$  (debe haber 12 pares y 12 impares).

**Transposiciones.** Consideremos una permutación  $\sigma$  de  $I_n$ ; al **transponer** (intercambiar) dos de los elementos del segundo renglón se obtiene otra permutación. Por ejemplo, al transponer 2 y 3 en  $\sigma$  obtenemos  $\tau$ :

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

al transponer 1 y 5 en  $\sigma'$  obtenemos  $\tau'$ :

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 1 & 5 & 6 & 2 & 4 \end{pmatrix}, \quad \tau' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}.$$

En estos casos diremos que la permutación que resulta se ha obtenido de la permutación dada, mediante una transposición.

Veamos cómo afectan las transposiciones a la paridad de una permutación. Al examinar la permutación  $\sigma'$  de arriba y la permutación  $\tau'$  obtenida mediante una transposición vemos que  $\sigma'$  es impar (tiene 11 inversiones) y  $\tau'$  es par (tiene una más, 12). ¿Por qué tiene una más? Al contar las inversiones de 1 con los demás elementos en  $\sigma$  y en  $\tau$  vemos que hay las mismas, excepto la de 1 con 5 que en  $\sigma'$  no forman inversión y en  $\tau'$  sí. Todas las demás inversiones son las mismas.

Este análisis sugiere el siguiente resultado:

**LEMA.** Si  $\tau$  es una permutación obtenida de la permutación  $\sigma$  mediante la transposición de dos números consecutivos, entonces  $\sigma$  y  $\tau$  tienen distinta paridad.

**Demostración.** Veremos que si  $\sigma$  tiene  $r$  inversiones entonces  $\tau$  tiene  $r + 1$  o  $r - 1$  inversiones. Sea

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i) & \sigma(i+1) & \dots & \sigma(n) \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i+1) & \sigma(i) & \dots & \sigma(n) \end{pmatrix}.$$

Todas las parejas de números que forman inversión en  $\sigma$ , la forman también en  $\tau$ , excepto  $\sigma(i)$  y  $\sigma(i+1)$ . Si  $\sigma(i)$ ,  $\sigma(i+1)$  no forman inversión en

$\sigma$ , en  $\tau$  sí la forman, e inversamente. Por ello, el número  $r$  de inversiones en  $\sigma$  aumenta o disminuye en 1 al pasar a  $\tau$ .

**TEOREMA:** Si  $\tau$  es una permutación obtenida de la permutación  $\sigma$  mediante la transposición de dos números, entonces  $\sigma$  y  $\tau$  tienen distinta paridad.

**Demostración.** Si los números que se transponen ocupan lugares consecutivos estamos en el caso del lema. Supongamos pues que los números que se transponen están separados por  $s$  lugares:

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & \dots & r & \dots & r+s & \dots & n \\ \sigma(1) & \dots & \sigma(r) & \dots & \sigma(r+s) & \dots & \sigma(n) \end{pmatrix} \\ \tau &= \begin{pmatrix} 1 & \dots & r & \dots & r+s & \dots & n \\ \sigma(1) & \dots & \sigma(r+s) & \dots & \sigma(r) & \dots & \sigma(n) \end{pmatrix}.\end{aligned}$$

Podemos pasar de  $\sigma$  a  $\tau$  haciendo  $s$  transposiciones de elementos consecutivos, cambiando  $\sigma(r)$  por cada uno de los de su derecha, hasta llegar a

$$\sigma' = \begin{pmatrix} 1 & \dots & r & \dots & r+s & \dots & n \\ \sigma(1) & \dots & \sigma(r+1) & \dots & \sigma(r) & \dots & n \end{pmatrix}$$

y después  $s-1$  transposiciones de elementos consecutivos, cambiando  $\sigma(r+s)$  [que ahora está a la izquierda de  $\sigma(r)$ ] con cada uno de los anteriores hasta llegar a  $\tau$ . Por tanto, podemos pasar de  $\sigma$  a  $\tau$  con  $2s-1$  transposiciones de elementos consecutivos. Como en cada paso se cambia la paridad, al hacer un número impar ( $2s-1$ ) de pasos, la paridad cambiará también.

**Inversa de una permutación.** Sea  $\sigma$  una permutación de  $I_n = \{1, 2, \dots, n\}$ , es decir, una función biyectiva  $\sigma: I_n \rightarrow I_n$ . Entonces la función inversa  $\sigma^{-1}: I_n \rightarrow I_n$  es también una función biyectiva, es decir,  $\sigma^{-1}$  es también una permutación.

En otras palabras, si  $\sigma \in S_n$  (en donde  $S_n$  denota el conjunto de todas las permutaciones de  $I_n$ ) entonces  $\sigma^{-1} \in S_n$  también.

Recordemos cómo se define la inversa de una función biyectiva:

$$\sigma(i) = k \quad \text{si y solamente si} \quad \sigma^{-1}(k) = i.$$

En particular, si escribimos  $\sigma$  en la forma

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

entonces

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma^{-1}(1) & \sigma^{-1}(2) & \dots & \sigma^{-1}(n) \end{pmatrix}.$$

Por ejemplo, si

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

entonces

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

**Ejemplo.** Escribiremos a continuación todas las permutaciones de  $I_3$  y sus inversas:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_2^{-1} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_3^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_4^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_5^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_6^{-1} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Vemos que  $\sigma_1^{-1} = \sigma_1$ ;  $\sigma_2^{-1} = \sigma_2$ ;  $\sigma_3^{-1} = \sigma_3$ ;  $\sigma_4^{-1} = \sigma_5$ ;  $\sigma_5^{-1} = \sigma_4$  y  $\sigma_6^{-1} = \sigma_6$ . Por lo tanto,  $S_3 = \{\sigma_1, \sigma_2, \dots, \sigma_6\} = \{\sigma_1^{-1}, \sigma_2^{-1}, \dots, \sigma_6^{-1}\}$ .

## EJERCICIO

6. Repítase el ejemplo anterior para las  $4! = 24$  permutaciones de  $I_4$ . Compruébese que

$$S_4 = \{\sigma_1, \sigma_2, \dots, \sigma_{24}\} = \{\sigma_1^{-1}, \sigma_2^{-1}, \dots, \sigma_{24}^{-1}\}.$$

Lo observado en el ejemplo y en el ejercicio anteriores es cierto en general. En efecto, podemos asociar a cada permutación  $\sigma$ , su inversa  $\sigma^{-1}$ , con lo que obtenemos una función de  $S_n$  en  $S_n$ . Además, si dos permutaciones  $\sigma$  y  $\tau$  son distintas, entonces  $\sigma^{-1}$  y  $\tau^{-1}$  son distintas y toda permutación  $\tau$  es inversa de una permutación [a saber  $\tau = (\tau^{-1})^{-1}$ ]. Por lo tanto la función de  $S_n$  en  $S_n$  que a cada permutación asocia su inversa es biyectiva.

Es fácil comprobar en el ejemplo anterior que  $\sigma_i$  es par si y solamente si  $\sigma_i^{-1}$  es par.

## EJERCICIO

7. Compruébese en  $S_4$  que  $\sigma$  es par si y solamente si  $\sigma^{-1}$  es par.

Esto es cierto en general:

**PROPOSICIÓN:**  $\sigma \in S_n$  es par si y solo si  $\sigma^{-1}$  es par.

*Demostración.* La función de  $S_n$  en  $S_n$  que a cada permutación  $\sigma$  asocia su inversa, que es biyectiva, puede extenderse al conjunto de parejas y esta extensión preserva inversiones. En efecto, si

$$\begin{aligned} i < j \quad y \quad r = \sigma(i) > \sigma(j) = s \\ \text{entonces} \quad s < r \quad y \quad j = \sigma^{-1}(s) > \sigma^{-1}(r) = i. \end{aligned}$$

## 4. DETERMINANTES

En la solución de sistemas de ecuaciones lineales y en otros muchos temas de las matemáticas aparecen en forma natural y, a la vez, juegan un importante papel, los determinantes.

En este párrafo veremos cómo se asocia a cada matriz cuadrada un número que se llama *el determinante de la matriz*. Empecemos con las matrices de  $2 \times 2$  y de  $3 \times 3$ .

A cada matriz (formada con números reales) de  $2 \times 2$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

se le asocia el número (real)  $ad - bc$ , al que se llama el determinante de  $A$  y se denota con  $|A|$  o con

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

Así pues, el determinante de la matriz  $A$  es el número

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

El determinante de una matriz de  $3 \times 3$

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

es, por definición, el número

$$|A| = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1b_2c_3 + b_1c_2a_3 + c_1a_2b_3 - c_1b_2a_3 - b_1a_2c_3 - a_1c_2b_3.$$

Una forma gráfica de recordar los seis términos de la expresión anterior es:

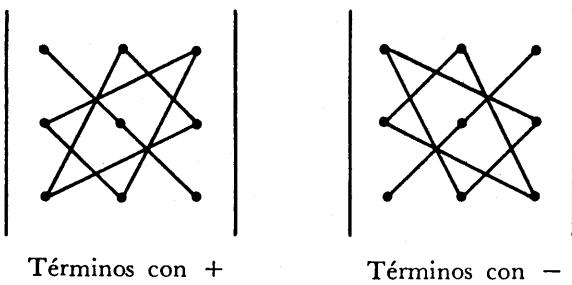


Figura 4.1

### EJERCICIOS

1. Encuéntrense los determinantes de las siguientes matrices, usando las definiciones anteriores:

$$\begin{array}{ccccccc} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} & \begin{pmatrix} a & b \\ a & b \end{pmatrix} & \begin{pmatrix} a & a \\ b & b \end{pmatrix} & \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} & \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 1 \\ 3 & -2 & 3 \\ -2 & 1 & -2 \end{pmatrix} & \begin{pmatrix} a & b & c \\ a & b & c \\ d & e & f \end{pmatrix} & \begin{pmatrix} a & d & e \\ 0 & b & f \\ 0 & 0 & c \end{pmatrix} & \begin{pmatrix} a & 0 & b \\ c & 0 & d \\ e & 0 & f \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \end{array}$$

Con el fin de extender las definiciones anteriores al caso general de matrices de  $n \times n$  conviene reescribir las definiciones anteriores en la forma siguiente:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Consideremos uno de los sumandos de la expresión anterior, digamos  $a_{13}a_{21}a_{32}$ . Asociado a este, podemos formar la permutación  $\sigma: \{1, 2, 3\} \rightarrow \{1, 2, 3\}$  dada por  $\sigma(1) = 3$ ,  $\sigma(2) = 1$  y  $\sigma(3) = 2$ , o sea, escrita en otra forma

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

En palabras: a cada término de la expresión para el determinante podemos asociar la permutación que asocia al primer índice, el segundo. A conti-

nuación escribiremos los seis términos y las permutaciones asociadas, indicando además la paridad de la permutación:

$$\begin{aligned}
 & + a_{11} a_{22} a_{33} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{par (hay 0 inversiones)} \\
 & + a_{12} a_{23} a_{31} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{par (hay 2 inversiones)} \\
 & + a_{13} a_{21} a_{32} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{par (hay 2 inversiones)} \\
 & - a_{13} a_{22} a_{31} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{impar (hay 3 inversiones)} \\
 & - a_{12} a_{21} a_{33} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{impar (hay 1 inversión)} \\
 & - a_{11} a_{23} a_{32} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \text{impar (hay 1 inversión).}
 \end{aligned}$$

Aquí podemos observar que los 6 términos corresponden a las 6 permutaciones de  $I_3$  y que, además, los términos que llevan signo + corresponden a las permutaciones pares y los que llevan signo - a las impares.

Lo mismo ocurre para el caso  $2 \times 2$ :

$$\begin{aligned}
 & + a_{11} a_{22} \quad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{par} \\
 & - a_{12} a_{21} \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \text{impar.}
 \end{aligned}$$

Otra forma de escribir el determinante de la matriz de  $2 \times 2$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

es, según lo que acabamos de observar, la siguiente:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \sum_{\sigma \in S_2} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)}$$

Aquí  $\Sigma$  significa que sumamos los términos correspondientes a cada  $\sigma \in S_2$ . (Recordemos que  $S_2$  es el conjunto de las permutaciones de  $I_2 = \{1, 2\}$ ;

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

y  $\epsilon(\sigma) = 1$  si  $\sigma$  es par y  $\epsilon(\sigma) = -1$  si  $\sigma$  es impar.

Para el caso  $3 \times 3$  tenemos una expresión análoga:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_{\sigma \in S_3} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} a_{3\sigma(3)}.$$

Aquí  $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$ , es el conjunto (con  $3!$  elementos) de todas las permutaciones de  $I_3 = \{1, 2, 3\}$ . El significado de  $\sum$  es el mismo, es decir, sumamos todos los términos correspondientes a cada  $\sigma$  en  $S_3$ . Como antes,  $\varepsilon(\sigma) = 1$  si  $\sigma$  es par y  $\varepsilon(\sigma) = -1$  si  $\sigma$  es impar.

Esta forma de expresar el determinante, utilizando el símbolo  $\sum$  para indicar "suma", puede parecer más complicado que el que dimos inicialmente. Sin embargo tiene la gran ventaja de que puede generalizarse al caso de matrices de  $n \times n$ .

### Definición de determinante; caso general.

**DEFINICIÓN:** A cada matriz (formada con números reales)

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

le asociamos el número (real), llamado su determinante, dado por la expresión

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

en donde  $S_n$  es el conjunto de todas las permutaciones de  $\{1, 2, \dots, n\}$  y  $\varepsilon(\sigma) = 1$  si  $\sigma$  es par y  $\varepsilon(\sigma) = -1$  si  $\sigma$  es impar.

Observemos que cada sumando en la expresión anterior es un producto

$$\varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

Aquí  $\varepsilon(\sigma) = \pm 1$  según  $\sigma$  sea par o impar. Los demás factores son

$$a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

y hay uno de cada renglón (pues los primeros índices son  $1, 2, \dots, n$ ) y uno de cada columna [pues los segundos índices son  $\sigma(1), \sigma(2), \dots, \sigma(n)$  y  $\sigma$  es una permutación de  $\{1, 2, \dots, n\}$ ].

Por ejemplo, al escribir la expresión para el determinante de una matriz de  $4 \times 4$

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

aparecen todos los sumandos del tipo

$$\epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} a_{3\sigma(3)} a_{4\sigma(4)}$$

en donde  $\sigma$  es una permutación de  $\{1, 2, 3, 4\}$ . Si por ejemplo,

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

entonces  $\epsilon(\sigma) = 1$ , pues  $\sigma$  es par (hay 2 inversiones) y el término correspondiente es

$$a_{12} a_{23} a_{31} a_{44}.$$

## EJERCICIOS

2. Encuéntrese el signo  $\epsilon(\sigma)$  en los siguientes términos de la expresión del determinante de una matriz de  $7 \times 7$ :

$$a_{13} a_{22} a_{31} a_{44} a_{55} a_{66} a_{77}, \quad a_{17} a_{26} a_{35} a_{44} a_{53} a_{62} a_{71}.$$

3. Escríbase la expresión para el determinante de una matriz de  $4 \times 4$  (24 sumandos).

4. Utilizando la observación que sigue a la definición de determinante demuéstrese que si un renglón o una columna de una matriz es cero, entonces el determinante es cero.

5. Utilizando la definición, demuéstrese que el determinante de una matriz diagonal es igual al producto de los elementos de la diagonal.

6. El mismo resultado que el del ejercicio anterior para matrices triangulares.

## 5. PROPIEDADES BÁSICAS DE LOS DETERMINANTES

En este párrafo analizaremos y demostraremos algunas propiedades básicas de los determinantes. A partir de ellas, en el párrafo siguiente demostraremos otras propiedades y más adelante veremos cómo aplicar estas para simplificar el cálculo de los determinantes.

Empezaremos estudiando las propiedades básicas en determinantes de matrices de  $2 \times 2$  y de  $3 \times 3$ .

Al calcular el determinante de una matriz de la forma

$$\begin{pmatrix} a + a' & b + b' \\ c & d \end{pmatrix}$$

vemos que

$$\begin{vmatrix} a + a' & b + b' \\ c & d \end{vmatrix} = (a + a')d - (b + b')c = ad - bc + a'd - b'c$$

$$= \begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} a' & b' \\ c & d \end{vmatrix}$$

Para matrices de  $3 \times 3$  ocurre lo mismo. Si un renglón, digamos el segundo,  $R_2$  de una matriz  $A$  está expresado como suma de dos renglones  $R_2' + R_2''$ :

$$(a_2, b_2, c_2) = (a'_2, b'_2, c'_2) + (a''_2, b''_2, c''_2) =$$

$$= (a'_2 + a''_2, b'_2 + b''_2, c'_2 + c''_2),$$

tenemos que

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & a'_1 & b_1 & c_1 \\ a'_2 + a''_2 & b'_2 + b''_2 & c'_2 + c''_2 & \\ a_3 & b_3 & c_3 & \end{vmatrix} =$$

$$= a_1(b'_2 + b''_2)c_3 + b_1(c'_2 + c''_2)a_3 + c_1(a'_2 + a''_2)b_3 -$$

$$- c_1(b'_2 + b''_2)a_3 - b_1(a'_2 + a''_2)c_3 - a_1(c'_2 + c''_2)b_3 =$$

$$= a_1b'_2c_3 + b_1c'_2a_3 + c_1a'_2b_3 - c_1b'_2a_3 - b_1a'_2c_3 - a_1c'_2b_3 +$$

$$+ a_1b''_2c_3 + b_1c''_2a_3 + c_1a''_2b_3 - c_1b''_2a_3 - b_1a''_2c_3 - a_1c''_2b_3 =$$

$$= \begin{vmatrix} a_1 & b_1 & c_1 \\ a'_2 & b'_2 & c'_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} a_1 & b_1 & c_1 \\ a''_2 & b''_2 & c''_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

Así pues, para matrices de  $2 \times 2$  y de  $3 \times 3$  vemos que:

**PROPIEDAD 1:** Si el renglón  $R_i$  de una matriz  $A$  se expresa como suma de dos vectores

$$R_i = R'_i + R''_i,$$

entonces

$$|A| = |A'| + |A''|$$

en donde  $A'$  y  $A''$  son matrices tales que su renglón  $i$  es  $R'_i$  y  $R''_i$  respectivamente y los demás renglones son los mismos que los de la matriz  $A$ .

Más adelante demostraremos que esta propiedad vale para matrices de  $n \times n$ .

### Ejemplos:

1.

$$\begin{aligned} \begin{vmatrix} a & b \\ c & d \end{vmatrix} &= \begin{vmatrix} a+0 & 0+b \\ c & d \end{vmatrix} = \begin{vmatrix} a & 0 \\ c & d \end{vmatrix} + \begin{vmatrix} 0 & b \\ c & d \end{vmatrix} = \\ &= \begin{vmatrix} a & 0 \\ c+0 & 0+d \end{vmatrix} + \begin{vmatrix} 0 & b \\ c+0 & 0+d \end{vmatrix} = \\ &= \begin{vmatrix} a & 0 \\ c & 0 \end{vmatrix} + \begin{vmatrix} a & 0 \\ 0 & d \end{vmatrix} + \begin{vmatrix} 0 & b \\ c & 0 \end{vmatrix} + \begin{vmatrix} 0 & b \\ 0 & d \end{vmatrix} \end{aligned}$$

2.

$$\begin{aligned} \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} &= \begin{vmatrix} a_1+0 & b_1+0 & 0+c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \\ &= \begin{vmatrix} a_1 & b_1 & 0 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} 0 & 0 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \\ &= \begin{vmatrix} a_1+0 & 0+b_1 & 0+0 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} 0 & 0 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \\ &= \begin{vmatrix} a_1 & 0 & 0 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} 0 & b_1 & 0 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} 0 & 0 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}. \end{aligned}$$

### EJERCICIOS

1. Demuéstrese la propiedad 1 para los casos de  $2 \times 2$  y de  $3 \times 3$  que faltan, es decir, para las matrices

$$\left( \begin{matrix} a & b \\ c+c' & d+d' \end{matrix} \right) \left[ \begin{matrix} a'_1+a''_1 & b'_1+b''_1 & c'_1+c''_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{matrix} \right] \quad \left[ \begin{matrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a'_3+a''_3 & b'_3+b''_3 & c'_3+c''_3 \end{matrix} \right]$$

2. Demuéstrese que si  $(a_1, b_1, c_1) = (a'_1, b'_1, c'_1) + (a''_1, b''_1, c''_1) + (a'''_1, b'''_1, c'''_1)$ ,

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a'_1 & b'_1 & c'_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} a''_1 & b''_1 & c''_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} a'''_1 & b'''_1 & c'''_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

3. Procediendo como en el ejemplo 2 anterior pruébese que

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & 0 & 0 \end{vmatrix} + \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ 0 & b_3 & 0 \end{vmatrix} + \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ 0 & 0 & c_3 \end{vmatrix}.$$

4. Utilizando ahora el ejercicio 2 anterior pruébese nuevamente el ejercicio 3.

5. Pruébese que

$$\begin{vmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} + \begin{vmatrix} a_1 & b_1 \\ c_2 & d_2 \end{vmatrix} + \begin{vmatrix} a_2 & b_2 \\ c_1 & d_1 \end{vmatrix} + \begin{vmatrix} a_2 & b_2 \\ c_2 & d_2 \end{vmatrix}.$$

Para matrices de  $2 \times 2$  y  $3 \times 3$  es fácil ver que vale la siguiente propiedad que más adelante demostraremos para el caso general:

**PROPIEDAD 2:** Si el renglón  $R_i$  de la matriz  $A$  es de la forma  $R_i = \lambda R'_i$ , entonces

$$|A| = \lambda |A'|,$$

en donde  $A'$  es la matriz que se obtiene de  $A$  cambiando el renglón  $R_i$  por  $R'_i$ .

### Ejemplos:

3.

$$\begin{vmatrix} \lambda a & \lambda b \\ c & d \end{vmatrix} = \lambda ad - \lambda bc = \lambda(ad - bc) = \lambda \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

4.

$$\begin{vmatrix} \lambda a_1 & \lambda b_1 & \lambda c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} =$$

$$= \lambda a_1 b_2 c_3 + \lambda b_1 c_2 a_3 + \lambda c_1 a_2 b_3 - \lambda c_1 b_2 a_3 - \lambda b_1 a_2 c_3 - \lambda a_1 c_2 b_3 =$$

$$= \lambda(a_1 b_2 c_3 + b_1 c_2 a_3 + c_1 a_2 b_3 - c_1 b_2 a_3 - b_1 a_2 c_3 - a_1 c_2 b_3) =$$

$$= \lambda \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

### EJERCICIO

6. En los ejemplos anteriores demostramos la propiedad 2 para matrices de  $2 \times 2$  y  $3 \times 3$  y para  $i = 1$ . Demuéstrese la misma propiedad para  $i = 2$  en el caso  $2 \times 2$  y para  $i = 2, i = 3$  en el caso  $3 \times 3$ .

Analicemos una propiedad más. Supongamos que en la matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

intercambiamos los dos renglones. Obtenemos la matriz

$$A' = \begin{pmatrix} c & d \\ a & b \end{pmatrix}.$$

Tenemos que

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \quad \begin{vmatrix} c & d \\ a & b \end{vmatrix} = cb - da;$$

de donde,

$$|A'| = - |A|.$$

### EJERCICIO

7. Demuéstrese que si en una matriz de  $3 \times 3$  intercambiamos dos renglones, entonces el determinante de la matriz obtenida es igual a menos el determinante de la matriz dada. (Examínense los tres casos posibles.)

Más adelante demostraremos que esta propiedad vale en general.

**PROPIEDAD 3:** Si la matriz  $A'$  se obtiene de una matriz  $A$  intercambiando dos renglones, entonces

$$|A'| = - |A|.$$

Observemos, finalmente, que

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \quad \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1.$$

Veremos que, en general, se tiene:

**PROPIEDAD 4:**

$$\begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix} = 1.$$

En lo que resta de este párrafo nos ocuparemos de demostrar las propiedades 1, 2, 3 y 4 en el caso general. (En una primera lectura pueden omitirse estas demostraciones.)

*Demostración de la propiedad 1.* Sea

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}.$$

Supongamos que el renglón  $R_i$  de  $A$  es suma de dos vectores:

$$R_i = R'_i + R''_i.$$

Así, tenemos que

$$\begin{aligned} (a_{i1}, a_{i2}, \dots, a_{in}) &= (a'_{i1}, a'_{i2}, \dots, a'_{in}) + (a''_{i1}, a''_{i2}, \dots, a''_{in}) = \\ &= (a'_{i1} + a''_{i1}, a'_{i2} + a''_{i2}, \dots, a'_{in} + a''_{in}). \end{aligned}$$

Entonces

$$\begin{aligned} |A| &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{i\sigma(i)} \cdots a_{n\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots (a'_{i\sigma(i)} + a''_{i\sigma(i)}) \cdots a_{n\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a'_{i\sigma(i)} a_{n\sigma(n)} + \\ &\quad + \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a''_{i\sigma(i)} \cdots a_{n\sigma(n)} = \\ &= |A'| + |A''|. \end{aligned}$$

*Demostración de la propiedad 2.* Sea  $A$  como antes y supongamos que  $R_i = \lambda R'_i$ :

$$\begin{aligned} (a_{i1}, a_{i2}, \dots, a_{in}) &= \lambda (a'_{i1}, a'_{i2}, \dots, a'_{in}) \\ &= (\lambda a'_{i1}, \lambda a'_{i2}, \dots, \lambda a'_{in}). \end{aligned}$$

Entonces

$$\begin{aligned} |A| &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{i\sigma(i)} \cdots a_{n\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots \lambda a'_{i\sigma(i)} \cdots a_{n\sigma(n)} = \\ &= \lambda \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a'_{i\sigma(i)} \cdots a_{n\sigma(n)} = \\ &= \lambda |A'|. \end{aligned}$$

*Demostración de la propiedad 3.* Sean

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \qquad A' = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

con

$$\begin{aligned} b_{ij} &= a_{ij} \text{ para toda } i, j \text{ e } i \neq r, i \neq s \\ b_{rj} &= a_{sj} \text{ para toda } j \\ b_{sj} &= a_{rj} \text{ para toda } j. \end{aligned}$$

En palabras,  $A'$  es la matriz obtenida de  $A$  intercambiando los renglones  $r$  y  $s$  (suponemos, desde luego, que  $r \neq s$ ). Para cada  $\sigma \in S_n$  definimos  $\tau \in S_n$  como sigue:

$$\begin{aligned}\tau(i) &= \sigma(i) \text{ para toda } i \neq r, i \neq s \\ \tau(r) &= \sigma(s) \\ \tau(s) &= \sigma(r).\end{aligned}$$

Evidentemente, si  $\sigma$  es una permutación par (respectivamente, impar) entonces  $\tau$  es una permutación impar (respectivamente par) pues  $\tau$  se obtiene de  $\sigma$  mediante una transposición. Entonces

$$\begin{aligned}|A| &= \sum \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{r\sigma(r)} \cdots a_{s\sigma(s)} \cdots a_{n\sigma(n)} \\ &= \sum \varepsilon(\sigma) b_{1\sigma(1)} \cdots b_{s\sigma(r)} \cdots b_{r\sigma(s)} \cdots b_{n\sigma(n)} \\ &= \sum -\varepsilon(\sigma) b_{1\tau(1)} \cdots b_{s\tau(s)} \cdots b_{r\tau(r)} \cdots b_{n\tau(n)} \\ &= -|A'|.\end{aligned}$$

*Demostración de la propiedad 4.* En la matriz

$$I = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

tenemos que

$$\begin{aligned}a_{ij} &= 0 \quad \text{si } i \neq j \\ a_{ii} &= 1.\end{aligned}$$

Por consiguiente todos los sumandos  $a_{1\sigma(1)}a_{2\sigma(2)} \cdots a_{n\sigma(n)}$  son cero excepto  $a_{11}a_{22} \cdots a_{nn}$  que vale 1. Y como la permutación correspondiente a ese término es par, tenemos que  $|I| = 1$ .

## 6. MÁS PROPIEDADES DE LOS DETERMINANTES

Las propiedades 5, 6 y 7 y sus corolarios que a continuación veremos, se demostrarán utilizando las propiedades básicas demostradas en el párrafo anterior.

**PROPIEDAD 5:** *Si una matriz cuadrada tiene dos renglones iguales entonces su determinante es cero.*

*Demostración.* Sea  $A$  dicha matriz y  $A'$  la que se obtiene de  $A$  intercambiando los dos renglones que son iguales. Entonces  $A = A'$  por lo que  $|A| = |A'|$ . Pero, según la propiedad 3, tenemos también que  $|A'| = -|A|$ , de donde  $|A| = -|A|$ . Luego  $2|A| = 0$ , por lo que  $|A| = 0$ .

**PROPIEDAD 6:** Si una matriz cuadrada tiene un renglón de ceros, entonces su determinante es cero.

*Demostración.* Se sigue inmediatamente de la propiedad 2 tomando  $\lambda = 0$  y  $R'_i$  arbitrario.

### EJERCICIOS

**8.** Pruébese directamente la propiedad 5 para determinantes de matrices de  $2 \times 2$ .

**9.** Lo mismo para matrices de  $3 \times 3$  para el caso en que sean iguales el segundo y el tercer renglones.

Antes de analizar la siguiente propiedad conviene ver el caso de  $2 \times 2$  y de  $3 \times 3$ , lo que haremos en los siguientes ejercicios.

### EJERCICIOS

**10.** Pruébese que

$$\begin{vmatrix} a & b \\ c + \lambda a & d + \lambda b \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

**11.** Pruébese que

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 + \lambda a_3 & b_2 + \lambda b_3 & c_2 + \lambda c_3 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

**12.** Pruébese que

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 + \lambda a_1 + \mu a_2 & b_3 + \lambda b_1 + \mu b_2 & c_3 + \lambda c_1 + \mu c_2 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

Los ejercicios anteriores pueden resolverse calculando directamente los determinantes a partir de la definición; pero es mejor resolverlos utilizando propiedades demostradas antes. En efecto, por la propiedad 1, tenemos que

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 + \lambda a_3 & b_2 + \lambda b_3 & c_2 + \lambda c_3 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} a_1 & b_1 & c_1 \\ \lambda a_3 & \lambda b_3 & \lambda c_3 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

y, por la propiedad 2, el segundo sumando de esta expresión es

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ \lambda a_3 & \lambda b_3 & \lambda c_3 \\ a_3 & b_3 & c_3 \end{vmatrix} = \lambda \begin{vmatrix} a_1 & b_1 & c_1 \\ a_3 & b_3 & c_3 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

Finalmente y según la propiedad 5, este último determinante es cero pues tiene dos renglones iguales, con lo que queda demostrada la propiedad.

## EJERCICIO

**13.** Resuélvase nuevamente el ejercicio 1 utilizando ahora el razonamiento que acabamos de exponer.

[Esta propiedad es válida en general.]

**PROPIEDAD 7:** *Si la matriz  $A'$  se obtiene de la matriz cuadrada  $A$  sumando a un renglón un múltiplo de otro, entonces  $|A| = |A'|$ .*

*Demostración.* Se hace como en los casos de  $3 \times 3$  y de  $2 \times 2$  que acabamos de ver. En efecto, si al renglón  $R_i$  le hemos sumado  $\lambda$  veces el renglón  $k$ , entonces, utilizando las propiedades 1 y 2 obtenemos

$$|A'| = |A| + \lambda|B|$$

en donde  $B$  es una matriz que tiene los renglones que ocupan los **lugares**  $i$  y  $k$  iguales. Por lo tanto  $|B| = 0$ , de donde  $|A'| = |A|$ .

Aplicando repetidas veces la propiedad 7 obtenemos el

**COROLARIO 1:** *Si a un renglón de una matriz cuadrada  $A$  le sumamos una combinación lineal de los demás renglones, entonces el determinante de la matriz obtenida es igual al determinante de  $A$ .*

**COROLARIO 2:** *Si los renglones de una matriz cuadrada son linealmente dependientes, entonces su determinante es cero.*

*Demostración.* Si los renglones de la matriz  $A$  son linealmente dependientes entonces alguno de ellos es combinación lineal de los demás. Restando a dicho renglón la combinación lineal obtenemos una matriz  $A'$  que tiene un renglón de ceros y tal que (por el corolario 1)  $|A'| = |A|$ . Como  $|A'| = 0$  se obtiene el resultado.

## Ejemplo

1. En la matriz

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 6 & 9 & 12 \end{pmatrix}$$

los renglones son linealmente dependientes pues, por ejemplo,

$$(6, 9, 12) = 2(1, 2, 3) + (4, 5, 6).$$

Si a (6, 9, 12) le restamos esta combinación lineal obtenemos

$$A' = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Tenemos que  $|A| = |A'|$  y  $|A'| = 0$ , de donde,  $|A| = 0$ .

Recordemos que la transpuesta de una matriz  $A$  es la matriz  $A^t$  cuyos renglones son (en el orden respectivo) las columnas de  $A$ . Por ejemplo,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad A^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

En general, si

$$A = (a_{ij}) \quad (1 \leq i \leq n, 1 \leq j \leq n)$$

entonces

$$A^t = (b_{ij})$$

en donde

$$b_{ij} = a_{ji}.$$

Veamos lo que pasa con los determinantes de  $A$  y de  $A^t$ . En el caso  $2 \times 2$  tenemos:

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

$$|A^t| = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc$$

por lo que vemos que  $|A| = |A^t|$ .

## EJERCICIO

**14.** Calculando directamente demuéstrese que

$$|A| = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} = |A^t|.$$

**PROPIEDAD 8:** El determinante de una matriz cuadrada  $A$  es igual al determinante de su matriz transpuesta  $A^t$ .

**Demostración.** Sea, como escribimos antes,  $A = (a_{ij})$ ,  $A^t = (b_{ij})$  en donde  $b_{ij} = a_{ji}$ . Tenemos que

$$\begin{aligned} |A| &= \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} \epsilon(\sigma) b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n}. \end{aligned}$$

Ahora bien, si  $\sigma(i) = j$ , entonces, por definición de  $\sigma^{-1}$ , tenemos que  $\sigma^{-1}(j) = i$ . Por lo tanto,

$$b_{\sigma(i)i} = b_{j\sigma^{-1}(j)}.$$

Ya que, además, por ser  $\sigma$  una permutación

$$\{\sigma(1), \sigma(2), \dots, \sigma(n)\} = \{1, 2, \dots, n\},$$

podemos reordenar los factores en cada sumando y escribir

$$b_{\sigma(1)1}b_{\sigma(2)2} \cdots b_{\sigma(n)n} = b_{1\sigma^{-1}(1)}b_{2\sigma^{-1}(2)} \cdots b_{n\sigma^{-1}(n)}.$$

Ya que si  $\sigma$  recorre  $S_n$ ,  $\sigma^{-1}$  recorre también  $S_n$  (véase el final del párrafo 3) y que  $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ , tenemos que

$$|A| = \sum_{\sigma^{-1} \in S_n} \varepsilon(\sigma^{-1}) b_{1\sigma^{-1}(1)}b_{2\sigma^{-1}(2)} \cdots b_{n\sigma^{-1}(n)} = |A^t|,$$

con lo que queda demostrada la propiedad 8.

Esta propiedad permite enunciar el siguiente resultado:

*Todas las propiedades que hemos demostrado para los renglones, valen también para las columnas.* En particular, las propiedades 1, 2, ..., 7.

**Desarrollos por menores.** Finalmente veremos una propiedad que permite expresar un determinante de orden  $n$  como suma de  $n$  determinantes de orden  $n - 1$ . Esta puede servir para dar otra definición, de tipo inductivo, de determinante.

Si  $A$  es la matriz

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

con  $A_{ij}$  denotaremos la submatriz de  $A$  que se obtiene omitiendo el renglón  $i$  y la columna  $j$  en  $A$ . Por ejemplo, si

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

$$A_{11} = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}, \quad A_{32} = \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \quad A_{23} = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}, \quad A_{33} = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}, \text{ etc.}$$

Al determinante  $|A_{ij}|$  se le llama *el menor del elemento  $a_{ij}$* . Por ejemplo, para el caso anterior, el menor de  $a_{11}$  es

$$|A_{11}| = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} = -3,$$

y el de  $a_{33}$  es

$$|A_{33}| = \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} = -3.$$

Sea

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Un simple cálculo prueba que

$$|A| = a_{11}|A_{11}| - a_{12}|A_{12}| + a_{13}|A_{13}|.$$

En efecto,

$$\begin{aligned} |A| &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} = \\ &= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}) = \\ &= a_{11}|A_{11}| - a_{12}|A_{12}| + a_{13}|A_{13}|. \end{aligned}$$

## EJERCICIO

15. Demuéstrese que, para esa matriz,

$$\begin{aligned} |A| &= -a_{21}|A_{21}| + a_{22}|A_{22}| - a_{23}|A_{23}| \\ &= a_{31}|A_{31}| - a_{32}|A_{32}| + a_{33}|A_{33}| \\ &= a_{11}|A_{11}| - a_{21}|A_{21}| + a_{31}|A_{31}| \\ &= -a_{12}|A_{12}| + a_{22}|A_{22}| - a_{32}|A_{32}| \\ &= a_{13}|A_{13}| - a_{23}|A_{23}| + a_{33}|A_{33}|. \end{aligned}$$

A las expresiones del ejemplo y del ejercicio anteriores se les suele llamar *desarrollo del determinante* con respecto al renglón o a la columna respectiva.

Para demostrar la validez de estos desarrollos en el caso general nos serán útiles los dos lemas siguientes:

**LEMA 1:** *Si en la matriz*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

$$a_{n1} = a_{n2} = \cdots = a_{nn-1} = 0, \text{ entonces}$$

$$|A| = a_{nn}|A_{nn}|.$$

Por ejemplo,

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 \\ 0 & 0 & 0 & 9 \end{vmatrix} = 9 \begin{vmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 8 & 7 & 6 \end{vmatrix}.$$

*Demostración del lema.* Tenemos que

$$|A| = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

Como  $a_{n\sigma(n)} = 0$  para  $\sigma(n) \neq n$ , tenemos que

$$|A| = \sum_{\sigma \in S_{n-1}} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n-1\sigma(n-1)} a_{nn} = |A_{nn}|.$$

**LEMA 2:** Si en una matriz cuadrada  $A$  todos los elementos distintos de  $a_{ij}$ , en el renglón  $i$  son cero, entonces

$$|A| = (-1)^{i+j} a_{ij} |A_{ij}|.$$

*Demostración.* Observemos primero las matrices

$$A = \left[ \begin{array}{cccc|ccccc} a_{11} & \dots & a_{1 j-1} & a_{ij} & a_{1 j+1} & \dots & a_{1 n} \\ \dots & & \dots & \dots & \dots & & \dots \\ a_{i-1 1} & \dots & a_{i-1 j-1} & a_{i-1 j} & a_{i-1 j+1} & \dots & a_{i-1 n} \\ \hline a_{i 1} & \dots & a_{i j-1} & a_{ij} & a_{i j+1} & \dots & a_{i n} \\ a_{i+1 1} & \dots & a_{i+1 j-1} & a_{i+1 j} & a_{i+1 j+1} & \dots & a_{i+1 n} \\ \dots & & \dots & \dots & \dots & & \dots \\ a_{n 1} & \dots & a_{n j-1} & a_{nj} & a_{n j+1} & \dots & a_{n n} \end{array} \right]$$

y

$$A' = \left[ \begin{array}{cccc|ccccc} a_{11} & \dots & a_{1 j-1} & a_{1 j+1} & \dots & a_{1 n} & a_{ij} \\ \dots & & \dots & \dots & & \dots & \dots \\ a_{i-1 1} & \dots & a_{i-1 j-1} & a_{i-1 j+1} & \dots & a_{i-1 n} & a_{i-1 j} \\ a_{i+1 1} & \dots & a_{i+1 j-1} & a_{i+1 j+1} & \dots & a_{i+1 n} & a_{i+1 j} \\ \dots & & \dots & \dots & & \dots & \dots \\ a_{n 1} & \dots & a_{n j-1} & a_{n j+1} & \dots & a_{n n} & a_{nj} \\ \hline a_{i 1} & \dots & a_{i j-1} & a_{i j+1} & \dots & a_{i n} & a_{ij} \end{array} \right]$$

Es fácil ver que podemos obtener  $A'$  de  $A$  intercambiando el renglón  $i$  por el  $i+1$ , después por el  $i+2$ , etc., hasta intercambiarlo con el renglón  $n$  y, después, la columna  $j$  por la  $j+1$ , luego por la  $j+2$ , etc., hasta intercambiarla con la columna  $n$ . Habremos hecho, en total  $(n-i)+(n-j)$  intercambios de renglones o columnas. Como en cada intercambio, los determinantes de las matrices correspondientes difieren sólo en el factor  $(-1)$ , tendremos que

$$|A| = (-1)^{n-i+n-j} |A'|$$

y como

$$(-1)^{n-i+n-j} = (-1)^{i+j}$$

resulta que

$$|A| = (-1)^{i+j} |A'|.$$

Ahora bien, según la hipótesis, en el último renglón hay ceros excepto, posiblemente,  $a_{ij}$ . Por lo tanto, por el lema anterior tenemos que

$$|A'| = a_{ij}|A_{ij}|$$

(obsérvese que los menores del elemento  $a_{ij}$  en  $A$  y en  $A'$  son iguales). Por consiguiente sustituyendo la última igualdad en la penúltima, se obtiene

$$|A| = (-1)^{i+j} a_{ij}|A_{ij}|.$$

**Ejemplos:**

$$\begin{vmatrix} a & b & c \\ 0 & 0 & c' \\ a'' & b'' & c'' \end{vmatrix} = (-1)^{2+3} \begin{vmatrix} a & b \\ a'' & b'' \end{vmatrix} = - \begin{vmatrix} a & b \\ a'' & b'' \end{vmatrix}.$$

$$\begin{vmatrix} 1 & 3 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 5 & 1 \\ 1 & 0 & 0 & 1 \end{vmatrix} = (-1)^{3+3} \cdot 5 \begin{vmatrix} 1 & 3 & 2 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} = 5(-1)^{2+2} \cdot 1 \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = -5.$$

**PROPIEDAD 9.** Si  $A$  es una matriz de  $n \times n$ , entonces

$$\begin{aligned} |A| &= (-1)^{i+1} a_{i1}|A_{i1}| + (-1)^{i+2} a_{i2}|A_{i2}| + \cdots + (-1)^{i+n} a_{in}|A_{in}|. \\ &= (-1)^{1+j} a_{1j}|A_{1j}| + (-1)^{2+j} a_{2j}|A_{2j}| + \cdots + (-1)^{n+j} a_{nj}|A_{nj}|. \end{aligned}$$

En palabras, podemos encontrar el determinante de una matriz  $A$  desarrollándolo con respecto a cualquier renglón  $i$  o también con respecto a cualquier columna  $j$ .

*Demostración.* La segunda parte es consecuencia de la primera debido a que el determinante de una matriz es igual al de su transpuesta.

La demostración de la primera parte quedará clara si examinamos, por ejemplo, el desarrollo de un determinante de orden 3 con respecto a un renglón, digamos el segundo. Tenemos, debido a la propiedad básica 1, que

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & 0 & 0 \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{21} & 0 \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix},$$

de donde, tomando en cuenta el lema anterior, resulta que

$$|A| = (-1)^{2+1} a_{21}|A_{21}| + (-1)^{2+2} a_{22}|A_{22}| + (-1)^{2+3} a_{23}|A_{23}|.$$

La demostración del caso general sigue, paso a paso, la del ejemplo anterior.

## 7. CÁLCULO DE DETERMINANTES

Para calcular el determinante de una matriz de  $n \times n$ , utilizando la expresión que dimos en la definición, hay que encontrar  $n!$  productos de  $n$  factores cada uno y después su suma, con el signo correspondiente. Para los casos de  $2 \times 2$  y  $3 \times 3$ , e incluso de  $4 \times 4$ , esto no presenta serios problemas. En efecto,  $2! = 2$ ,  $3! = 6$ ,  $4! = 24$ . Pero para valores mayores de  $n$  este método es totalmente impracticable. Por ejemplo, si quisieramos calcular así el determinante de una matriz de  $7 \times 7$  deberíamos efectuar 5 040 productos de 7 factores cada uno. Para matrices de  $11 \times 11$ , casi 40 millones de productos.

Los desarrollos por menores son igualmente largos. Por ejemplo, para un determinante de  $11 \times 11$  hay que calcular 11 determinantes de  $10 \times 10$ , cada uno de los cuales conduce a 10 de  $9 \times 9$ , etc.

Sin embargo, el uso apropiado de algunas propiedades de los determinantes puede abreviar enormemente los cálculos. Daremos a continuación unos cuantos ejemplos. Las propiedades que se usan son, principalmente, las que permiten agregar a un renglón (o columna) un múltiplo de otro renglón (o columna), o bien el intercambio de renglones (o columnas) cambiando el signo convenientemente o, finalmente, "sacar" un factor de un renglón (o columna).

### Ejemplos:

1.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 2 & -1 & 2 & -1 \\ 1 & 2 & -1 & -2 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & -2 \\ 0 & -3 & 0 & -3 \\ 0 & 1 & -2 & -3 \end{vmatrix} = 6 \begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -2 & -3 \end{vmatrix} = \\ = -6 \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & -2 & -4 \end{vmatrix} = -6 \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{vmatrix} = 12.$$

2.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 5 & 9 \\ 0 & 3 & 9 & 19 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 5 & 9 \\ 3 & 9 & 19 \end{vmatrix} \\ = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 3 \\ 0 & 3 & 10 \end{vmatrix} = \begin{vmatrix} 1 & 3 \\ 0 & 1 \end{vmatrix} = 1.$$

3.

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{vmatrix} = \begin{vmatrix} 10 & 2 & 3 & 4 \\ 10 & 3 & 4 & 1 \\ 10 & 4 & 1 & 2 \\ 10 & 1 & 2 & 3 \end{vmatrix} = 10 \begin{vmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & -3 \\ 0 & 2 & -2 & -2 \\ 0 & -1 & -1 & -1 \end{vmatrix}$$

$$= 20 \begin{vmatrix} 1 & 1 & -3 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \end{vmatrix} = 20 \begin{vmatrix} 1 & 1 & -3 \\ 0 & -2 & 2 \\ 0 & 0 & -4 \end{vmatrix} = 160.$$

4.

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & b-a & b^2-ab \\ 1 & c-a & c^2-ac \end{vmatrix} =$$

$$= (b-a)(c-a) \begin{vmatrix} 1 & b \\ 1 & c \end{vmatrix} = (b-a)(c-a)(c-b)$$

5.

$$\begin{vmatrix} 1 & a & a^2 & a^3 \\ 1 & b & b^2 & b^3 \\ 1 & c & c^2 & c^3 \\ 1 & d & d^2 & d^3 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & b-a & b^2-ab & b^3-ab^2 \\ 1 & c-a & c^2-ac & c^3-ac^2 \\ 1 & d-a & d^2-ad & d^3-ad^2 \end{vmatrix} =$$

$$= (b-a)(c-a)(d-a) \begin{vmatrix} 1 & b & b^2 \\ 1 & c & c^2 \\ 1 & d & d^2 \end{vmatrix}$$

$$= (b-a)(c-a)(d-a)(c-b)(d-b)(d-c).$$

## EJERCICIOS

1.

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{vmatrix}$$

2.

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 2 \end{vmatrix}$$

3.

$$\begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}$$

4.

$$\begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{vmatrix}$$

5.

$$\begin{vmatrix} a & b & c & d \\ b & c & d & a \\ c & d & a & b \\ d & a & b & c \end{vmatrix}$$

6.

$$\begin{vmatrix} 1 & -3 & 4 & 6 \\ -2 & 4 & 1 & 7 \\ 3 & -1 & 2 & 5 \\ -1 & 2 & 3 & 7 \end{vmatrix}$$

7.

$$\begin{vmatrix} 1 & 3 & 0 & 0 \\ 2 & 1 & 3 & 0 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 2 & 1 \end{vmatrix}$$

8.

$$\begin{vmatrix} 1 & 3 & 0 & 0 & 0 \\ 2 & 1 & 3 & 0 & 0 \\ 0 & 2 & 1 & 3 & 0 \\ 0 & 0 & 2 & 1 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{vmatrix}$$

9.

$$\begin{vmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

10.

$$\begin{vmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{vmatrix}$$

11. Pruébese que si

$$M_n = \begin{vmatrix} 1 & a_1 & a_1^2 \cdots a_1^{n-1} \\ 1 & a_2 & a_2^2 \cdots a_2^{n-1} \\ \dots & \dots & \dots \\ 1 & a_n & a_n^2 \cdots a_n^{n-1} \end{vmatrix}$$

entonces

$$M_n = (a_n - a_1)(a_{n-1} - a_1) \cdots (a_2 - a_1) M_{n-1}.$$

$M_n$  se llama el determinante de Van der Monde. Utilizando lo anterior pruébese, por inducción que

$$M_n = \prod_{j>i} (a_j - a_i) \quad (1 \leq i, j \leq n).$$

## 8. CARACTERIZACIÓN DEL RANGO DE UNA MATRIZ MEDIANTE DETERMINANTES

En el segundo párrafo de este capítulo definimos el rango de una matriz como la dimensión del espacio vectorial generado por los renglones. Demostaremos ahora que el rango es igual también a la dimensión del espacio vectorial generado por las columnas. Esto será consecuencia del teorema 2.

Empecemos demostrando lo siguiente:

**TEOREMA 1:** *Un conjunto  $\{A_1, A_2, \dots, A_s\}$  de vectores de  $\mathbf{R}^n$  ( $s \leq n$ ) es linealmente dependiente si y solamente si todos los determinantes de  $s \times s$  formados con las coordenadas de los vectores son cero.*

(Durante la demostración se precisa el significado de la expresión “formado con las coordenadas”).

Consideremos primero el caso  $s = 2$ . Sean

$$\begin{aligned} A &= (a_1, a_2, a_3, \dots, a_n) \\ B &= (b_1, b_2, b_3, \dots, b_n). \end{aligned}$$

Supongamos que son linealmente dependientes es decir, que

$$\alpha A + \beta B = 0$$

con  $\alpha$  o  $\beta$  distintos de cero. Digamos que  $\beta \neq 0$ . Para cada  $i = 1, 2, \dots, n$  tenemos que

$$\alpha a_i + \beta b_i = 0.$$

Entonces

$$0 = \begin{vmatrix} a_i & a_j \\ 0 & 0 \end{vmatrix} = \begin{vmatrix} a_i & a_j \\ \alpha a_i + \beta b_i & \alpha a_j + \beta b_j \end{vmatrix} = \beta \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix}$$

y como  $\beta \neq 0$ , tenemos que

$$\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} = 0,$$

es decir, todos los determinantes de  $2 \times 2$  formados con las coordenadas de  $A$  y  $B$  son cero.

Inversamente, supongamos que para toda pareja

$$\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} = 0.$$

Veremos que entonces  $A$  y  $B$  son linealmente dependientes. Si  $A = 0$ , no hay nada que demostrar. Supongamos pues que  $A \neq 0$ , por lo que alguna coordenada de  $A$  es distinta de cero. Supongamos, para facilitar la escritura que  $a_1 \neq 0$ . Entonces

$$(-b_1)A + a_1B = (-b_1)(a_1, a_2, \dots, a_n) + a_1(b_1, b_2, \dots, b_n) = 0$$

pues, por hipótesis  $a_i b_j - a_j b_i = 0$ . Ahora bien, ya que  $a_1 \neq 0$ , la relación  $(-b_1)A + a_1B = 0$  prueba la dependencia lineal.

La demostración del teorema se hace por inducción. Para evitar una notación complicada, solamente señalaremos cómo del caso  $s = 2$  se deduce el caso  $s = 3$ .

Sean

$$\begin{aligned} A &= (a_1, a_2, \dots, a_n) \\ B &= (b_1, b_2, \dots, b_n) \\ C &= (c_1, c_2, \dots, c_n). \end{aligned}$$

Supongamos primero que  $\{A, B, C\}$  es linealmente dependiente. Entonces hay una combinación lineal

$$\alpha A + \beta B + \gamma C = 0$$

con algún coeficiente distinto de cero. Supongamos que  $\gamma \neq 0$ . Tenemos entonces que, para toda  $i$ ,

$$\alpha a_i + \beta b_i + \gamma c_i = 0.$$

Por lo tanto,

$$\begin{aligned} 0 &= \begin{vmatrix} a_i & a_j & a_k \\ b_i & b_j & b_k \\ \alpha a_i + \beta b_i + \gamma c_i & \alpha a_j + \beta b_j + \gamma c_j & \alpha a_k + \beta b_k + \gamma c_k \end{vmatrix} = \\ &= \gamma \begin{vmatrix} a_i & a_j & a_k \\ b_i & b_j & b_k \\ c_i & c_j & c_k \end{vmatrix} \end{aligned}$$

y como  $\gamma \neq 0$  resulta que todos los determinantes de  $3 \times 3$  formados con las coordenadas de  $A, B$  y  $C$  son cero.

Inversamente, supongamos ahora que todos esos determinantes son cero. Si  $\{A, B\}$  es linealmente dependiente, también  $\{A, B, C\}$  lo es y no hay nada que probar. Supondremos pues que  $\{A, B\}$  es linealmente independiente. Entonces por hipótesis de inducción, algún determinante

$$\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix}$$

es distinto de cero. Sin pérdida de generalidad supondremos que

$$\gamma = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \neq 0.$$

Llamemos

$$\beta = - \begin{vmatrix} a_1 & a_2 \\ c_1 & c_2 \end{vmatrix} \quad y \quad \alpha = \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix}.$$

Tenemos que, para toda  $k$ ,

$$0 = \begin{vmatrix} a_1 & a_2 & a_k \\ b_1 & b_2 & b_k \\ c_1 & c_2 & c_k \end{vmatrix} = \alpha a_k + \beta b_k + \gamma c_k,$$

de donde

$$\alpha A + \beta B + \gamma C = 0$$

y como  $\gamma \neq 0$ ,  $\{A, B, C\}$  es linealmente dependiente, con lo que queda probado el teorema.

**TEOREMA 2:** *El rango de una matriz  $A$  es  $r$  si y solo si existe una submatriz de  $r \times r$  de  $A$  cuyo determinante es distinto de cero y, además, los determinantes de todas las submatrices de  $s \times s$  con  $s > r$  son cero.*

**Demostración.** Si  $r$  es el rango de  $A$ , por definición existen  $r$  renglones linealmente independientes. Por el teorema anterior hay una submatriz de  $r \times r$  cuyo determinante es distinto de cero. Ahora bien, si  $s > r$ ,  $s$  renglones son siempre linealmente dependientes. Luego, según el teorema anterior todos los determinantes de las submatrices de  $s \times s$  son cero.

**COROLARIO 1:** *El rango de una matriz es igual a la dimensión del subespacio vectorial generado por las columnas.*

**COROLARIO 2:** *Una matriz de  $n \times n$  es de rango  $n$  si y solo si su determinante es distinto de cero.*

# 5

CAPÍTULO

# Sistemas de ecuaciones lineales

## 1. DEFINICIONES

SE estudiarán ahora sistemas de  $m$  ecuaciones lineales con  $n$  incógnitas, es decir, sistemas del tipo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = k_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = k_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = k_m. \end{cases}$$

Los coeficientes  $a_{ij}$  de las incógnitas  $x_j$  y los términos libres  $k_i$  se supondrá que son números reales aunque todo lo que se diga valdrá para el caso en que dichos números se tomen del campo de los números complejos o, en general, de un campo arbitrario.

Al sistema anterior se le asocian dos matrices, la matriz del sistema, de  $m$  renglones y  $n$  columnas

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

y la matriz aumentada con los términos libres, de  $m$  por  $n+1$

$$A' = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & k_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & k_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & k_m \end{bmatrix}.$$

Denotaremos con  $B_1, B_2, \dots, B_n$  a las columnas de  $A$ :

$$\begin{aligned} B_1 &= (a_{11}, a_{21}, \dots, a_{m1}) \\ B_2 &= (a_{12}, a_{22}, \dots, a_{m2}) \\ &\cdots \cdots \cdots \cdots \cdots \\ B_n &= (a_{1n}, a_{2n}, \dots, a_{mn}). \end{aligned}$$

Con  $K$  denotaremos la columna de los términos libres:

$$K = (k_1, k_2, \dots, k_m).$$

Las  $B_i$  y  $K$  son vectores de  $\mathbf{R}^m$ . Entonces el sistema puede escribirse, en forma vectorial, con una sola ecuación:

$$x_1B_1 + x_2B_2 + \cdots + x_nB_n = K.$$

Diremos que un vector  $S = (s_1, s_2, \dots, s_n)$  de  $\mathbf{R}^n$  es solución del sistema si  $S$  es solución de cada una de las ecuaciones del sistema, es decir, si

$$\begin{cases} a_{11}s_1 + a_{12}s_2 + \cdots + a_{1n}s_n = k_1 \\ a_{21}s_1 + a_{22}s_2 + \cdots + a_{2n}s_n = k_2 \\ \cdots \cdots \cdots \cdots \cdots \\ a_{m1}s_1 + a_{m2}s_2 + \cdots + a_{mn}s_n = k_m. \end{cases}$$

En otras palabras,  $S = (s_1, s_2, \dots, s_n)$  es solución si y solo si

$$s_1B_1 + s_2B_2 + \cdots + s_nB_n = K,$$

y en este caso  $K$  pertenece al subespacio vectorial de  $\mathbf{R}^m$  generado por  $\{B_1, B_2, \dots, B_n\}$ .

Un sistema se llama *homogéneo* si  $K = 0$ , es decir, si  $k_1 = k_2 = \cdots = k_n = 0$ .

Como sabemos de cursos elementales de matemáticas hay sistemas que tienen muchas soluciones, otros tienen una solución única y otros no tienen solución.

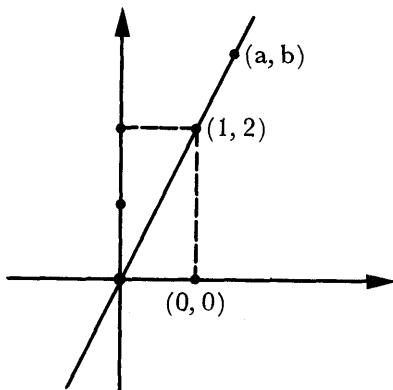
Por ejemplo, el sistema

$$\begin{cases} x + y = 3 \\ x - y = 1 \end{cases}$$

tiene una sola solución:  $(2, 1)$ . El sistema de una sola ecuación

$$\{2x - y = 0$$

tiene una infinidad de soluciones, a saber, todos los puntos  $(a, b)$  de la recta que pasa por  $(0, 0)$  y  $(1, 2)$ .



**Figura 5.1**

El sistema

$$\begin{cases} x + y = 2 \\ x + y = 3 \end{cases}$$

no tiene solución.

## EJERCICIOS

1. Díganse cuáles de los siguientes vectores son solución del sistema:

$$\begin{cases} x_1 - 2x_2 + x_3 - 3x_4 = -2 \\ 2x_1 + x_2 - x_3 + 2x_4 = -1 \\ x_1 + 3x_2 - 2x_3 + 5x_4 = 1 \end{cases}$$

$$S_1 = (1, 7, 8, -1), S_2 = (1, 1, -1, 1), \bar{S} = (3, 3, 1, 0), \\ S' = (-1, 2, 1, 0), T = (2, 9, 14, 0).$$

2. Un sistema homogéneo de ecuaciones lineales siempre tiene solución.  
3. Díganse cuáles de los sistemas siguientes:

- a) Que tenga una infinidad de soluciones.
- b) Que tenga una sola solución.
- c) Que no tenga soluciones.

4. Pruébese que  $S = (1, 2, 3)$  es solución del sistema

$$x_1B_1 + x_2B_2 + x_3B_3 = K,$$

en donde

$$\begin{aligned} B_1 &= (-2, 1, 3, -1) & B_3 &= (2, 1, 1, -1) \\ B_2 &= (2, 0, -1, 0) & K &= (8, 4, 4, -4). \end{aligned}$$

5. Pruébese que  $S = (s_1, s_2, \dots, s_n) = (1, 1, \dots, 1)$  es solución del sistema

$$\begin{cases} x_1 + x_2 + \cdots + x_n = n \\ x_1 - x_2 + \cdots - x_n = 0. \quad (n \text{ par}) \end{cases}$$

6. Pruébese que  $(1, 2, \dots, n)$  es solución de

$$\begin{cases} 2x_1 + 2x_2 + \cdots + 2x_n = n^2 + n \\ -2x_1 + 2x_2 - \cdots + 2x_n = n. \quad (n \text{ par}) \end{cases}$$

7. Demuéstrese que  $S = (-1, 2, 1)$  es solución de

$$\begin{cases} x_1 + x_2 + 4x_3 = 5 \\ 2x_1 + x_2 + 3x_3 = 3 \\ 3x_1 + x_2 + 2x_3 = 1 \\ 4x_1 + x_2 + x_3 = -1. \end{cases}$$

Usando esto, exprérese  $K$  como combinación lineal de  $B_1$ ,  $B_2$  y  $B_3$ , en donde

$$\begin{aligned} B_1 &= (1, 2, 3, 4) & B_3 &= (4, 3, 2, 1) \\ B_2 &= (1, 1, 1, 1) & K &= (5, 3, 1, -1). \end{aligned}$$

8. Encuéntrese la solución del sistema

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n = n \\ x_2 + x_3 + \cdots + x_n = n-1 \\ x_3 + \cdots + x_n = n-2 \\ \dots \\ x_n = 1. \end{cases}$$

Usando esto, exprérese  $K = (n, n-1, n-2, \dots, 1)$  como combinación lineal de los vectores

$$\begin{aligned} D_1 &= (1, 0, 0, \dots, 0) \\ D_2 &= (1, 1, 0, \dots, 0) \\ D_3 &= (1, 1, 1, \dots, 0) \\ \dots \\ D_n &= (1, 1, 1, \dots, 1). \end{aligned}$$

## 2. EXISTENCIA DE SOLUCIONES

Lo que hemos estudiado acerca del rango nos permite dar un criterio sobre cuándo un sistema tiene o no soluciones.

**TEOREMA:** *Un sistema de ecuaciones lineales tiene solución si y solo si el rango de la matriz del sistema es igual al rango de la matriz aumentada.*

*Demostración.* Que el sistema

$$x_1B_1 + x_2B_2 + \cdots + x_nB_n = K$$

tenga solución significa que existe  $S = (s_1, s_2, \dots, s_n)$  tal que

$$s_1B_1 + s_2B_2 + \cdots + s_nB_n = K.$$

Esto equivale a decir que  $K$  pertenece al subespacio  $V$  de  $\mathbf{R}^m$  generado por  $\{B_1, B_2, \dots, B_n\}$ , lo cual ocurre si y solo si  $V$  es igual al subespacio generado por  $\{B_1, \dots, B_n, K\}$ . Y como  $V \subset U$ , esto ocurre si y solo si  $V$  y  $U$  tienen la misma dimensión, o sea, si y solo si los rangos de la matriz del sistema y de la matriz aumentada son iguales.

Así pues, usando el método descrito en el capítulo anterior para calcular el rango de una matriz resulta fácil conocer cuándo un sistema tiene o no solución.

### Ejemplos:

1. Consideremos el sistema

$$\begin{cases} x + y - w = 0 \\ x + z - w = -1 \\ -x + y - 2z + w = 3. \end{cases}$$

Su matriz aumentada es

$$\begin{pmatrix} 1 & 1 & 0 & -1 & 0 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & -2 & 1 & 3 \end{pmatrix},$$

la cual es equivalente a

$$\begin{pmatrix} 1 & 1 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 & -1 \\ 0 & 2 & -2 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Esta última es escalonada y tiene los 3 renglones distintos de cero. Por lo tanto su rango  $r' = 3$ . La matriz del sistema, como submatriz de la aumentada, es equivalente, según podemos observar, a

$$\begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

la cual es de rango  $r = 2$ . Como  $r \neq r'$ , según el teorema el sistema *no tiene solución*.

## 2. Analicemos el sistema

$$\begin{cases} x - y + 2z = 1 \\ y - z = 1 \\ 3x + y - z = 0 \\ 4x + y = 2. \end{cases}$$

Su matriz aumentada es

$$\left[ \begin{array}{cccc} 1 & -1 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 3 & 1 & -1 & 0 \\ 4 & 1 & 0 & 2 \end{array} \right]$$

que es equivalente a

$$\left[ \begin{array}{cccc} 1 & -1 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 4 & -7 & -3 \\ 0 & 5 & -8 & -2 \end{array} \right] \sim \left[ \begin{array}{cccc} 1 & -1 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & -3 & -7 \\ 0 & 0 & -3 & -7 \end{array} \right] \sim \left[ \begin{array}{cccc} 1 & -1 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & -3 & -7 \\ 0 & 0 & 0 & 0 \end{array} \right].$$

Vemos que la matriz del sistema es equivalente a

$$\left[ \begin{array}{ccc} 1 & -1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & -3 \\ 0 & 0 & 0 \end{array} \right]$$

Así pues, las dos matrices son de rango 3, por lo que el sistema tiene solución.

3. Un sistema de  $n$  ecuaciones con  $n$  incógnitas tal que el determinante sea distinto de cero tiene solución. En efecto, la matriz aumentada es de  $n \times (n+1)$  y su rango no puede ser mayor que  $n$ . Además es  $n$  porque contiene como submatriz a la matriz del sistema que es de rango  $n$  pues su determinante es distinto de cero.

4. Todo sistema homogéneo tiene solución, pues el rango de la matriz aumentada es igual al rango de la matriz del sistema. [Es claro que este resultado es más fácil de ver observando simplemente que  $(0, 0, \dots, 0)$  es solución.]

5. Un sistema de  $m$  ecuaciones con  $n$  incógnitas con  $m < n$  y rango  $r = m$  tiene siempre solución. En efecto, el rango de la matriz aumentada no puede ser mayor que  $m$  pues esta es de  $m \times (n+1)$ .

## EJERCICIOS

1. Llevando las matrices a la forma escalonada díganse si los sistemas siguientes tienen o no solución:

$$\begin{cases} x - y = 1 \\ x + y = 1 \end{cases}$$

$$\begin{cases} -x + 2y - 3z = -10 \\ 2x - 4y + 6z = 15 \end{cases}$$

$$\begin{cases} x + y + z = 1 \\ -x + z = -1 \\ x - y = 1 \end{cases} \quad \begin{cases} x + z = 1 \\ 2x + y + 3z + t = 2 \\ 4x + y + 5z + t = 4 \end{cases}$$

$$\begin{cases} x + y = 1 \\ ax + by = c \\ (a+1)x + (b+1)y = c+1 \end{cases} \quad (a \neq 0, a \neq b)$$

$$\begin{cases} x + y + z = 1 \\ ax + by + cz = 1 \\ a^2x + b^2y + c^2z = 1 \end{cases} \quad (a \neq b, a \neq c, b \neq c).$$

2. ¿Para qué valores de  $k$  tienen solución los siguientes sistemas?

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 1 \\ x_1 + x_3 = 1 \\ x_2 + x_4 = k \end{cases}$$

$$\begin{cases} x + y - w = 0 \\ x + z - w = k \\ -x + y - 2z + w = -4. \end{cases}$$

3. Para los siguientes vectores  $K$  y  $B_1, B_2, \dots, B_r$ , dígase si  $K$  pertenece o no al subespacio vectorial generado por  $\{B_1, B_2, \dots, B_r\}$ :

a)  $B_1 = (1, 2, 1, 1)$   
 $B_2 = (1, 1, 1, 2)$   
 $B_3 = (-3, -2, 1, -3)$        $K = (-1, 1, 3, 1)$

b)  $B_1 = (2, 1, 1, 2)$   
 $B_2 = (1, 3, 1, 3)$   
 $B_3 = (1, 1, 5, -3)$        $K = (2, 5, -7, 14)$

c)  $B_1 = (1, 2, 3, 4, 5)$   
 $B_2 = (2, 3, 4, 5, 1)$   
 $B_3 = (3, 4, 5, 1, 2)$   
 $B_4 = (4, 5, 1, 2, 3)$   
 $B_5 = (5, 1, 2, 3, 4)$        $K = (3, -1, 5, 1, 7)$

d)  $B_1 = (1, 1, 1, 0, 2)$   
 $B_2 = (-2, 2, -1, 0, 3)$   
 $B_3 = (3, -1, 2, -1, -1)$   
 $B_4 = (-4, 0, -3, 1, 1)$   
 $B_5 = (2, -1, 0, -2, 4)$        $K = (-2, -3, 10, -5, 1)$

4. ¿Es  $K$  combinación lineal de  $\{B_1, B_2, \dots, B_r\}$ ?

a)  $B_1 = (2, 3, 5, 2)$   
 $B_2 = (1, -2, 1, -1)$   
 $B_3 = (-1, 2, -1, 1)$   
 $B_4 = (1, -3, 2, -3)$        $K = (1, 2, -1, 4)$

b)  $B_1 = (1, 1, 2, 2)$   
 $B_2 = (3, 1, 3, 1)$   
 $B_3 = (1, 5, 3, 1)$        $K = (5, -7, 14, 2)$

5. Un sistema de  $n$  ecuaciones y de rango  $n$  tiene solución.

### 3. SISTEMAS DE $n$ ECUACIONES CON $n$ INCÓGNITAS

En este párrafo estudiaremos los sistemas en los cuales el número de incógnitas es igual al número de ecuaciones:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = k_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = k_2 \\ \dots \dots \dots \dots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = k_n \end{cases}$$

En este caso la matriz del sistema es cuadrada y podemos hablar de su determinante

$$d = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \dots \dots \dots \dots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} \quad (*)$$

el cual supondremos que es distinto de cero. Según el teorema 2 del párrafo 8 del capítulo anterior esto equivale a suponer que el rango de la matriz del sistema (y también de la matriz aumentada) es también  $n$ . Lo demostrado en el párrafo 2 de este capítulo nos asegura que el sistema tiene solución.

Nos serán útiles los determinantes  $d_i$  ( $1 \leq i \leq n$ ) que se obtienen sustituyendo en (\*) la columna formada con los términos libres, en lugar de la columna  $i$ . Por ejemplo,

$$d_1 = \begin{vmatrix} k_1 & a_{12} & \cdots & a_{1n} \\ k_2 & a_{22} & \cdots & a_{2n} \\ \dots \dots \dots \dots \\ k_n & a_{n2} & \cdots & a_{nn} \end{vmatrix}, \quad d_2 = \begin{vmatrix} a_{11} & k_1 & a_{13} & \cdots & a_{1n} \\ a_{21} & k_2 & a_{23} & \cdots & a_{2n} \\ \dots \dots \dots \dots \\ a_{n1} & k_n & a_{n3} & \cdots & a_{nn} \end{vmatrix}, \text{ etc.}$$

Supongamos que  $S = (s_1, s_2, \dots, s_n)$  es una solución del sistema, es decir, que

$$\begin{aligned} a_{11}s_1 + a_{12}s_2 + \cdots + a_{1n}s_n &= k_1 \\ a_{21}s_1 + a_{22}s_2 + \cdots + a_{2n}s_n &= k_2 \\ \dots \dots \dots \dots \\ a_{n1}s_1 + a_{n2}s_2 + \cdots + a_{nn}s_n &= k_n. \end{aligned} \quad (**)$$

Encontremos  $d_1$ :

$$\begin{aligned} d_1 &= \begin{vmatrix} k_1 & a_{12} & \cdots & a_{1n} \\ k_2 & a_{22} & \cdots & a_{2n} \\ \dots \dots \dots \dots \\ k_n & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11}s_1 + a_{12}s_2 + \dots + a_{1n}s_n & a_{12} \cdots a_{1n} \\ a_{21}s_1 + a_{22}s_2 + \dots + a_{2n}s_n & a_{22} \cdots a_{2n} \\ \dots \dots \dots \dots \\ a_{n1}s_1 + a_{n2}s_2 + \dots + a_{nn}s_n & a_{n2} \cdots a_{nn} \end{vmatrix} = \\ &= \begin{vmatrix} a_{11}s_1 & a_{12} \cdots a_{1n} \\ a_{21}s_1 & a_{22} \cdots a_{2n} \\ \dots \dots \dots \dots \\ a_{n1}s_1 & a_{n2} \cdots a_{nn} \end{vmatrix} = s_1 \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \dots \dots \dots \dots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = s_1 d. \end{aligned}$$

[En el primer paso simplemente hemos sustituido  $k_1$  por su valor según (\*\*). Después hemos restado de la primera columna la segunda multiplicada por  $s_2$ , la tercera multiplicada por  $s_3$ , etc., y la última multiplicada por  $s_n$ . Finalmente hemos “sacado”  $s_1$  de la primera columna.]

Un razonamiento completamente análogo demuestra que  $d_2 = s_2 d$ ,  $d_3 = s_3 d$ , ...,  $d_n = s_n d$ . Ya que hemos supuesto que  $d \neq 0$ , podemos escribir

$$s_1 = \frac{d_1}{d}, s_2 = \frac{d_2}{d}, \dots, s_n = \frac{d_n}{d}.$$

Con esto hemos demostrado que hay una sola solución, pues toda solución  $(s_1, s_2, \dots, s_n)$  debe ser igual a esta última. Tal resultado se conoce como la regla de Cramer o las fórmulas de Cramer. Lo enunciaremos como un teorema.

**TEOREMA:** *Un sistema de  $n$  ecuaciones lineales en  $n$  incógnitas con el determinante distinto de cero tiene una y sólo una solución, la cual está dada por  $S = (s_1, s_2, \dots, s_n)$  con*

$$s_1 = \frac{d_1}{d}, s_2 = \frac{d_2}{d}, \dots, s_n = \frac{d_n}{d}.$$

**COROLARIO.** *Si un sistema homogéneo de  $n$  ecuaciones con  $n$  incógnitas tiene el determinante distinto de cero, entonces la única solución es  $(0, 0, \dots, 0)$ .*

*Demostración.* Por el teorema, sabemos que hay una sola solución, dada por  $s_1 = \frac{d_1}{d}, \dots, s_n = \frac{d_n}{d}$ . Pero  $d_1 = d_2 = \dots = d_n = 0$ , pues las matrices correspondientes tienen una columna de ceros (la de los términos libres).

### Ejemplos:

$$1. \quad \begin{cases} x + y = a \\ x - y = b \end{cases} \quad d = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} = -2; \quad d_1 = \begin{vmatrix} a & 1 \\ b & -1 \end{vmatrix} = -a - b;$$

$$d_2 = \begin{vmatrix} 1 & a \\ 1 & b \end{vmatrix} = b - a; \quad x = \frac{a+b}{2} \quad y = \frac{a-b}{2}.$$

La solución es  $\left( \frac{a+b}{2}, \frac{a-b}{2} \right)$ .

$$2. \quad \begin{cases} x \operatorname{sen} \alpha + y \cos \alpha = \operatorname{sen} 2\alpha \\ x \cos \alpha - y \operatorname{sen} \alpha = \cos 2\alpha \end{cases} \quad d = \begin{vmatrix} \operatorname{sen} \alpha & \cos \alpha \\ \cos \alpha & -\operatorname{sen} \alpha \end{vmatrix} = -1$$

$$\begin{aligned}
 d_1 &= \begin{vmatrix} \sin 2\alpha & \cos \alpha \\ \cos 2\alpha & -\sin \alpha \end{vmatrix} = -(\sin 2\alpha \sin \alpha + \cos 2\alpha \cos \alpha) = \\
 &= -(2 \sin^2 \alpha \cos \alpha + \cos^3 \alpha - \sin^2 \alpha \cos \alpha) = \\
 &= -(\cos^3 \alpha + \sin^2 \alpha \cos \alpha) = -\cos \alpha
 \end{aligned}$$

$$\begin{aligned}
 d_2 &= \begin{vmatrix} \sin \alpha & \sin 2\alpha \\ \cos \alpha & \cos 2\alpha \end{vmatrix} = \sin \alpha \cos 2\alpha - \cos \alpha \sin 2\alpha = \\
 &= \sin \alpha \cos^2 \alpha - \sin^3 \alpha - 2 \sin \alpha \cos^2 \alpha = -(\sin^3 \alpha + \sin \alpha \cos^2 \alpha) \\
 &= -\sin \alpha.
 \end{aligned}$$

Por lo tanto,  $x = \cos \alpha$ ,  $y = \sin \alpha$ , es decir, la solución es  $(\cos \alpha, \sin \alpha)$ .

3.

$$\begin{aligned}
 &\left\{ \begin{array}{l} x + y + z = 1 \\ ax + by + cz = k \\ a^2x + b^2y + c^2z = k^2 \end{array} \right. \quad (a \neq b, a \neq c, b \neq c) \\
 d &= \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & b^2-ba & c^2-ca \end{vmatrix} = \begin{vmatrix} b-a & c-a \\ b(b-a) & c(c-a) \end{vmatrix} \\
 &= (b-a)(c-a) \begin{vmatrix} 1 & 1 \\ b & c \end{vmatrix} = (b-a)(c-a)(c-b) \neq 0.
 \end{aligned}$$

$d_1$ ,  $d_2$  y  $d_3$  se encuentran sustituyendo en esta última expresión  $k$  en lugar de  $a$ ,  $b$  y  $c$  respectivamente. Por lo tanto la solución es

$$\left( \frac{(b-k)(c-k)(c-b)}{(b-a)(c-a)(c-b)}, \frac{(k-a)(c-a)(c-k)}{(b-a)(c-a)(c-b)}, \frac{(b-a)(k-a)(k-b)}{(b-a)(c-a)(c-b)} \right)$$

o bien,

$$\left( \frac{(b-k)(c-k)}{(b-a)(c-a)}, \frac{(k-a)(c-k)}{(b-a)(c-b)}, \frac{(k-a)(k-b)}{(c-a)(c-b)} \right).$$

4. Exprésese  $K = (5, 1, 11)$  como combinación lineal de  $B_1 = (3, 2, 2)$ ,  $B_2 = (2, 3, 1)$  y  $B_3 = (1, 1, 3)$ .

Queremos encontrar números  $s_1, s_2, s_3$  tales que

$$s_1 B_1 + s_2 B_2 + s_3 B_3 = K,$$

es decir, se trata de resolver el sistema

$$x_1 B_1 + x_2 B_2 + x_3 B_3 = K,$$

o bien,

$$\begin{aligned} 3x_1 + 2x_2 + x_3 &= 5 \\ 2x_1 + 3x_2 + x_3 &= 1 \\ 2x_1 + x_2 + 3x_3 &= 11. \end{aligned}$$

La solución es  $(2, -2, 3)$  y por consiguiente

$$K = 2B_1 - 2B_2 + 3B_3.$$

5. ¿Son linealmente independientes los vectores  $B_1 = (1, 5, 3)$ ,  $B_2 = (2, 1, -1)$ ,  $B_3 = (4, 2, 1)$ ?

Supongamos que una combinación lineal de ellos es cero, es decir, que

$$s_1B_1 + s_2B_2 + s_3B_3 = 0.$$

Entonces  $(s_1, s_2, s_3)$  es solución del sistema homogéneo

$$x_1B_1 + x_2B_2 + x_3B_3 = 0$$

es decir, de

$$\begin{cases} x_1 + 2x_2 + 4x_3 = 0 \\ 5x_1 + x_2 + 2x_3 = 0 \\ 3x_1 - x_2 + x_3 = 0. \end{cases}$$

Como

$$d = \begin{vmatrix} 1 & 2 & 4 \\ 5 & 1 & 2 \\ 3 & -1 & 1 \end{vmatrix} = -27 \neq 0,$$

la única solución es  $(0, 0, 0)$ . Por lo tanto

$$s_1B_1 + s_2B_2 + s_3B_3 = 0$$

implica  $s_1 = s_2 = s_3 = 0$ , por lo que los vectores son linealmente independientes.

## EJERCICIOS

1. Resuélvanse con las fórmulas de Cramer los sistemas siguientes:

$$\begin{array}{ll} \begin{cases} 2x - 3y + 2z = 0 \\ x + y + z = 2 \\ 3x - y - 3z = 4 \end{cases} & \begin{cases} x \operatorname{sen} \alpha + y \cos \alpha = \operatorname{sen} \alpha \\ x \cos \alpha - y \operatorname{sen} \alpha = -\cos \alpha \end{cases} \\ \left\{ \begin{array}{l} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ x_2 + x_3 + x_4 + x_5 = 2 \\ x_3 + x_4 + x_5 = 3 \\ x_4 + x_5 = 3 \\ x_5 = 2 \end{array} \right. & \left\{ \begin{array}{l} 2x_1 + 3x_3 - 5x_4 = 12 \\ -2x_2 + x_3 + 3x_4 = 4 \\ 3x_1 - 5x_2 + 4x_3 = 5 \\ x_1 - 3x_2 - 4x_4 = -5. \end{array} \right. \end{array}$$

**2.** Exprésese  $K$  como combinación de  $B_1, B_2, \dots, B_r$  en los siguientes casos:

- a)  $K = (-1, -4, -2)$ ,  $B_1 = (1, 2, 4)$ ,  $B_2 = (1, -1, 1)$ ,  $B_3 = (2, 2, 4)$ .  
 b)  $K = (-5, -, 12, 5)$ ,  $B_1 = (0, 1, 3, 4)$ ,  $B_2 = (1, 0, 2, 3)$ ,  $B_3 = (-3, -2, 0, -5)$ ,  $B_4 = (4, 3, -5, 0)$ .

**3.** ¿Son linealmente independientes  $\{B_1, B_2, \dots, B_r\}$  en los siguientes casos?

- a)  $B_1 = (1, 1, 1, 1)$ ,  $B_2 = (1, 2, 3, 4)$ ,  $B_3 = (1, 3, 6, 10)$ ,  $B_4 = (1, 4, 10, 20)$ .  
 b)  $B_1 = (2, 3, 3)$ ,  $B_2 = (-1, 4, -2)$ ,  $B_3 = (-1, -2, 4)$ ,  
 c)  $B_1 = (2, 3, 3, 3)$ ,  $B_2 = (-1, 3, -1, -1)$ ,  $B_3 = (3, 3, -1, 3)$ ,  
 $B_4 = (2, 2, 2, -1)$ .

**SUGERENCIA.** Demuéstrese que si  $\lambda_1 B_1 + \lambda_2 B_2 + \dots + \lambda_r B_r = 0$ , entonces  $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0$ .

#### 4. Desarrollando los determinantes

$$0 = \begin{vmatrix} a_{11} & a_{12} & a_{13} & k_1 \\ a_{21} & a_{22} & a_{23} & k_2 \\ a_{31} & a_{32} & a_{33} & k_3 \\ a_{i1} & a_{i2} & a_{i3} & k_i \end{vmatrix} \quad (i = 1, 2, 3)$$

dése otra demostración (para  $n = 3$ ) de la parte del teorema que asegura que

$$\left( \frac{d_1}{d}, \frac{d_2}{d}, \frac{d_3}{d} \right)$$

es solución del sistema

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = k_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = k_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = k_3. \end{cases} \quad (d \neq 0).$$

#### 4. SISTEMAS HOMOGÉNEOS

Ahora estudiaremos los sistemas homogéneos, es decir, sistemas del tipo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0. \end{cases}$$

Si, como antes, denotamos con  $B_1, B_2, \dots, B_n$  a los vectores de  $\mathbf{R}^m$  cuyas coordenadas son las columnas de la matriz del sistema, este se puede escribir en la forma

$$x_1 B_1 + x_2 B_2 + \dots + x_n B_n = 0.$$

Observemos antes que nada, que los sistemas homogéneos siempre tienen a  $(0, 0, \dots, 0)$  como solución, pues

$$0B_1 + 0B_2 + \dots + 0B_n = 0.$$

Denotemos con  $W$  el subconjunto de  $\mathbf{R}^n$  formado por todos los vectores  $S = (s_1, s_2, \dots, s_n)$  que sean solución del sistema. En símbolos,

$$S \in W \text{ si y solo si } s_1B_1 + s_2B_2 + \dots + s_nB_n = 0.$$

Es muy fácil probar que:

**PROPOSICIÓN 1:** *El conjunto  $W$  de todas las soluciones de un sistema homogéneo de ecuaciones lineales*

$$x_1B_1 + x_2B_2 + \dots + x_nB_n = 0$$

*es un subespacio vectorial de  $\mathbf{R}^n$ .*

*Demostración.* Veremos que  $W$  cumple las tres condiciones de la definición de subespacio vectorial:

Sean  $S = (s_1, s_2, \dots, s_n) \in W$  y  $T = (t_1, t_2, \dots, t_n) \in W$ . Entonces

$$\begin{aligned} s_1B_1 + s_2B_2 + \dots + s_nB_n &= 0 \\ t_1B_1 + t_2B_2 + \dots + t_nB_n &= 0, \end{aligned}$$

de donde,

$$(s_1 + t_1)B_1 + (s_2 + t_2)B_2 + \dots + (s_n + t_n)B_n = 0.$$

Luego  $S + T \in W$ .

Evidentemente, como antes observamos,  $0 \in W$ .

Además, si  $S \in W$  y  $\lambda \in \mathbf{R}$ , tenemos que

$$s_1B_1 + s_2B_2 + \dots + s_nB_n = 0,$$

de donde,

$$\lambda(s_1B_1 + s_2B_2 + \dots + s_nB_n) = 0,$$

por lo que

$$(\lambda s_1)B_1 + (\lambda s_2)B_2 + \dots + (\lambda s_n)B_n = 0.$$

Por consiguiente  $(\lambda s_1, \lambda s_2, \dots, \lambda s_n) = \lambda S \in W$ , con lo que terminamos de demostrar la proposición.

El teorema que a continuación demostraremos nos servirá para relacionar la dimensión del subespacio  $W$  de soluciones con el rango del sistema y con el número de incógnitas. Analizaremos el caso no necesariamente homogéneo, pues este mismo teorema nos servirá para encontrar todas las soluciones de un sistema arbitrario.

**TEOREMA 1:** *Sea  $\{B_1, B_2, \dots, B_r\}$  una base del subespacio vectorial  $V$  de  $\mathbf{R}^n$  generado por las columnas  $\{B_1, B_2, \dots, B_n\}$  del sistema*

$$x_1 B_1 + x_2 B_2 + \dots + x_n B_n = K$$

*que supondremos que tiene solución. Entonces, dados  $n-r$  números  $s_{r+1}, s_{r+2}, \dots, s_n$  existen  $r$  números, únicos,  $s_1, s_2, \dots, s_r$  tales que*

$$S = (s_1, s_2, \dots, s_r, s_{r+1}, \dots, s_n)$$

*es una solución del sistema.*

**Demostración.** Formemos el vector

$$C = s_{r+1} B_{r+1} + s_{r+2} B_{r+2} + \dots + s_n B_n.$$

Ya que  $\{B_1, \dots, B_r\}$  generan a  $V$ , lo anterior indica que  $C \in V$ . Como también  $K \in V$ , pues suponemos que el sistema tiene solución, resulta que  $K - C \in V$ . Por consiguiente  $K - C$  es combinación lineal de  $\{B_1, \dots, B_r\}$ , es decir, existen números  $s_1, \dots, s_r$  tales que

$$K - C = s_1 B_1 + \dots + s_r B_r,$$

de donde,

$$s_1 B_1 + \dots + s_r B_r + s_{r+1} B_{r+1} + \dots + s_n B_n = K,$$

lo cual demuestra que  $S = (s_1, \dots, s_r, s_{r+1}, \dots, s_n)$  es solución.

Probaremos la unicidad de los números  $s_1, \dots, s_r$ . Si hubiera otros números  $s'_1, \dots, s'_r$  tales que

$$S' = (s'_1, \dots, s'_r, s_{r+1}, \dots, s_n)$$

fuerá también solución, entonces  $S - S' = K - K = 0$ , de donde,

$$(s_1 - s'_1) B_1 + (s_2 - s'_2) B_2 + \dots + (s_r - s'_r) B_r = 0$$

lo cual implica que  $s_1 - s'_1 = 0, s_2 - s'_2 = 0, \dots, s_r - s'_r = 0$ , puesto que  $\{B_1, B_2, \dots, B_r\}$  es linealmente independiente por ser base. Luego

$$s_1 = s'_1, s_2 = s'_2, \dots, s_r = s'_r.$$

Según la unicidad que acabamos de demostrar bajo las hipótesis anteriores, para que dos soluciones sean iguales, basta que tengan iguales las últimas  $n-r$  coordenadas.

Aplicaremos ahora este resultado a sistemas homogéneos.

**TEOREMA 2:** Si  $V$  es el subespacio vectorial de  $\mathbf{R}^m$  generado por las columnas de la matriz de un sistema homogéneo

$$x_1B_1 + x_2B_2 + \dots + x_nB_n = 0$$

y  $W$  es el subespacio de  $\mathbf{R}^m$  formado con todas las soluciones del sistema, entonces

$$\dim V + \dim W = n.$$

*Demostración.* Consideremos las siguientes  $n-r$  soluciones correspondientes a los valores de  $s_{r+1}, s_{r+2}, \dots, s_n$  que consten de un 1 y 0 los demás (su existencia queda asegurada por el teorema 1) :

$$S_1 = (s_{11}, s_{12}, \dots, s_{1r}, 1, 0, \dots, 0)$$

$$S_2 = (s_{21}, s_{22}, \dots, s_{2r}, 0, 1, \dots, 0)$$

.....

$$S_{n-r} = (s_{n-r,1}, s_{n-r,2}, \dots, s_{n-r,r}, 0, 0, \dots, 1).$$

Demostraremos que  $\{S_1, S_2, \dots, S_{n-r}\}$  es una base de  $W$ . En primer lugar, es linealmente independiente, pues uno de los determinantes formados con sus coordenadas es distinto de cero:

$$\left| \begin{array}{cccc|c} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{array} \right| = 1.$$

Veremos ahora que  $\{S_1, S_2, \dots, S_{n-r}\}$  genera a  $W$ . Sea  $S = (s_1, \dots, s_r, s_{r+1}, \dots, s_n)$  una solución cualquiera. El vector

$$S' = s_{r+1}S_1 + s_{r+2}S_2 + \dots + s_nS_{n-r}$$

(construido usando las últimas  $n-r$  coordenadas de  $S$ ) pertenece a  $W$ , pues  $S_1, \dots, S_{n-r} \in W$ . Un cálculo directo prueba que  $S'$  es de la forma

$$S' = (s'_1, s'_2, \dots, s'_r, s_{r+1}, s_{r+2}, \dots, s_n).$$

Así pues,  $S$  y  $S'$  tienen sus últimas  $n-r$  coordenadas iguales, por lo que (véase la unicidad en el teorema 1)  $S = S'$  y  $S \in W$ , con lo que queda probado el teorema.

En el párrafo 6 se ilustrará este teorema.

**COROLARIO:** La dimensión del subespacio  $W$  de soluciones de un sistema homogéneo de ecuaciones lineales es

$$\dim W = n-r$$

en donde  $n$  es el número de incógnitas y  $r$  el rango.

## 5. SISTEMA HOMOGÉNEO ASOCIADO

Dado un sistema de ecuaciones lineales

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = k_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = k_2 \\ \dots \dots \dots \dots \dots \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = k_m \end{array} \right. \quad (1)$$

podemos asociarle el sistema homogéneo

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \dots \dots \dots \dots \dots \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0. \end{array} \right. \quad (2)$$

En notación vectorial, al sistema

$$x_1B_1 + x_2B_2 + \dots + x_nB_n = K \quad (1)$$

se le asocia el sistema homogéneo

$$x_1B_1 + x_2B_2 + \dots + x_nB_n = 0. \quad (2)$$

Supondremos que (1), tiene solución. Sea  $\bar{S}$  una solución de (1). En el siguiente teorema se describen todas las soluciones de (1) a partir de  $\bar{S}$  y del subespacio de soluciones de (2).

**TEOREMA:** *Toda solución  $T$  del sistema (1) es de la forma*

$$T = S + \bar{S},$$

*en donde  $\bar{S}$  es una solución fija de (1) y  $S$  recorre todas las soluciones de (2).*

**Demostración.** Sea  $S = (s_1, s_2, \dots, s_n)$  una solución de (2) y  $\bar{S} = (\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$  la solución dada de (1). Entonces  $S + \bar{S}$  es solución de (1), pues

$$\begin{aligned} & (s_1 + \bar{s}_1)B_1 + (s_2 + \bar{s}_2)B_2 + \dots + (s_n + \bar{s}_n)B_n = \\ & = (s_1B_1 + s_2B_2 + \dots + s_nB_n) + (\bar{s}_1B_1 + \bar{s}_2B_2 + \dots + \bar{s}_nB_n) = \\ & = 0 + K = K. \end{aligned}$$

Inversamente, si  $T = (t_1, t_2, \dots, t_n)$  es solución de (1), tenemos que  $t_1B_1 + t_2B_2 + \dots + t_nB_n = K$ , de donde,

$$\begin{aligned} & (t_1 - \bar{s}_1)B_1 + (t_2 - \bar{s}_2)B_2 + \dots + (t_n - \bar{s}_n)B_n = \\ &= (t_1B_1 + t_2B_2 + \dots + t_nB_n) - (\bar{s}_1B_1 + \bar{s}_2B_2 + \dots + \bar{s}_nB_n) = \\ &= K - K = 0; \end{aligned}$$

o sea,  $T - \bar{S}$  es solución de (2). Si llamamos  $S = T - \bar{S}$  a esta solución, tenemos que  $T = S + \bar{S}$ , con lo que queda probado el teorema.

Este teorema sirve para describir convenientemente al conjunto de soluciones de un sistema. En efecto, basta dar un vector  $\bar{S}$  [una solución particular de (1)] y un subespacio vectorial  $W$  [el de las soluciones de (2)]. Todas las soluciones del sistema son entonces de la forma  $S + \bar{S}$  con  $S \in W$ .

**Ejemplo.** Consideremos el sistema

$$x + y = 2 \quad (3)$$

de una sola ecuación con dos incógnitas. El sistema homogéneo asociado es

$$x + y = 0. \quad (4)$$

Una solución particular de (3) es, por ejemplo,  $\bar{S} = (1, 1)$ . La solución de (4) es el subespacio vectorial  $W$ :

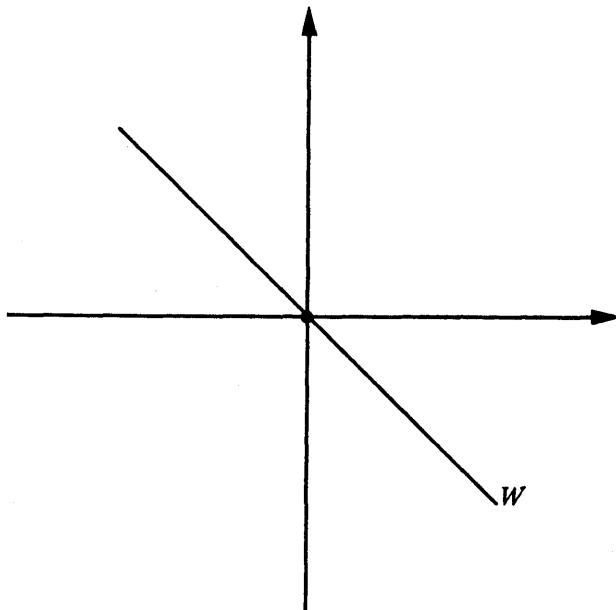
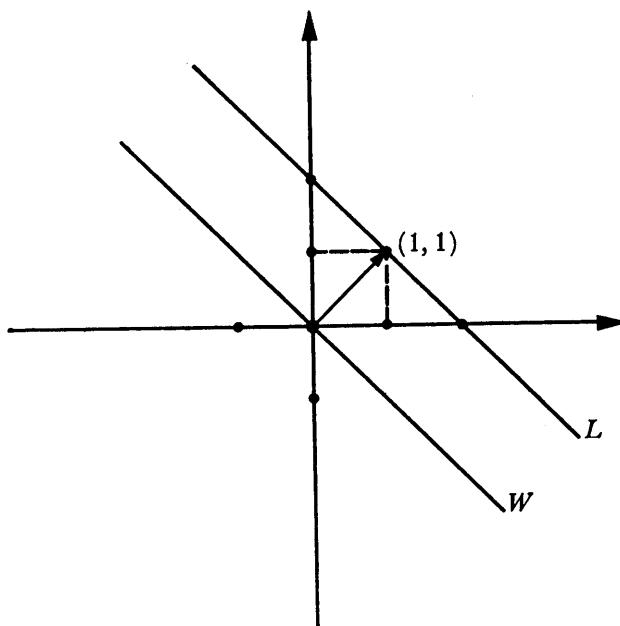


Figura 5.2

Según el teorema, toda solución de (1) es de la forma  $T = S + \bar{S}$  con  $S \in W$ . Es decir, el conjunto de soluciones de (3) es una “traslación” de  $W$ , a saber, la recta  $L$ :



**Figura 5.3**

El teorema de este párrafo se ilustrará ampliamente en los ejemplos y ejercicios del párrafo siguiente.

## 6. RESOLUCIÓN DE SISTEMAS

Las operaciones elementales (por renglones) que se definieron para matrices, pueden efectuarse también en sistemas de ecuaciones lineales. Por ejemplo, consideremos un sistema de ecuaciones lineales y la matriz aumentada del sistema:

$$\begin{cases} x - 2y + 3z = 2 \\ 2x + 3y - 4z = 1 \\ 3x + y - z = 3 \end{cases} \quad \left( \begin{array}{ccc|c} 1 & -2 & 3 & 2 \\ 2 & 3 & -4 & 1 \\ 3 & 1 & -1 & 3 \end{array} \right). \quad (1)$$

Analicemos las tres operaciones elementales.

1. Intercambiar dos renglones en la matriz se traduce en el intercambio de dos ecuaciones del sistema. Por ejemplo, intercambiemos el primer renglón con el tercero (respectivamente, la primera ecuación con la tercera) :

$$\left\{ \begin{array}{l} 3x + y - z = 3 \\ 2x + 3y - 4z = 1 \\ x - 2y + 3z = 2 \end{array} \right. \quad \left( \begin{array}{cccc} 3 & 1 & -1 & 3 \\ 2 & 3 & -4 & 1 \\ 1 & -2 & 3 & 2 \end{array} \right).$$

Es evidente que al hacer esta operación elemental no alteramos las soluciones, es decir, obtenemos un sistema que tiene las mismas soluciones que (1).

2. Multiplicar un renglón de la matriz por un número distinto de cero se traduce en multiplicar una ecuación por dicho número. Por ejemplo, en (1) multipliquemos por  $-2$  el segundo renglón (respectivamente, la segunda ecuación) :

$$\left\{ \begin{array}{l} x - 2y + 3z = 2 \\ -4x - 6y + 8z = -2 \\ 3x + y - z = 3 \end{array} \right. \quad \left( \begin{array}{cccc} 1 & -2 & 3 & 2 \\ -4 & -6 & 8 & -2 \\ 3 & 1 & -1 & 3 \end{array} \right).$$

Observemos que al hacer esta operación elemental no cambiamos las soluciones, es decir, obtenemos otro sistema que tiene las mismas soluciones que el sistema inicial. Esto se debe a que el número por el que multiplicamos es *distinto de cero*.

3. Sumar a un renglón otro renglón significa sumar a una ecuación, otra. Por ejemplo, sumemos al tercer renglón el primero [en (1)] (respectivamente, sumemos a la tercera, la primera ecuación) :

$$\left\{ \begin{array}{l} x - 2y + 3z = 2 \\ 2x + 3y - 4z = 1 \\ 4x - y + 2z = 5 \end{array} \right. \quad \left( \begin{array}{cccc} 1 & -2 & 3 & 2 \\ 2 & 3 & -4 & 1 \\ 4 & -1 & 2 & 5 \end{array} \right). \quad (2)$$

Observemos que, tampoco en este caso, se alteran las soluciones. Veamos los detalles. Si  $(a, b, c)$  es solución de (1), tenemos que

$$\begin{aligned} a - 2b + 3c &= 2 \\ 2a + 3b - 4c &= 1 \\ 3a + b - c &= 3. \end{aligned}$$

Entonces  $(a, b, c)$  satisface las dos primeras ecuaciones de (2), pues son las mismas. Ya que

$$4x - y + 2z = 5$$

se obtuvo sumando  $x - 2y + 3z = 2$  y  $3x + y - z = 3$ , vemos que

$$4a - b + 2c = (a - 2b + 3c) + (3a + b - c) = 2 + 3 = 5,$$

con lo que probamos que  $(a, b, c)$  es solución de (2).

## EJERCICIO

Pruébese que si  $(a, b, c)$  es solución de (2) entonces es también solución de (1).

Con esto queda probada la observación.

Lo que aquí hemos ilustrado en un ejemplo es cierto en general (y las demostraciones son las mismas).

Siguiendo la misma terminología que en matrices diremos que dos sistemas de ecuaciones son equivalentes si puede obtenerse uno del otro mediante transformaciones elementales. Según lo observado, tenemos que

**PROPOSICIÓN 1:** *Si un sistema de ecuaciones lineales se obtiene de otro mediante transformaciones elementales, entonces ambos sistemas tienen las mismas soluciones.*

Es decir, si dos sistemas son equivalentes, entonces tienen las mismas soluciones. (El inverso es también cierto, es decir, si dos sistemas tienen las mismas soluciones, entonces son equivalentes. Este resultado no lo necesitaremos por lo que omitimos su demostración.)

El método que estudiamos en el párrafo 2 de este capítulo para ver si el sistema tiene o no solución demuestra que:

**PROPOSICIÓN 2:** *Si el sistema*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = k_1 \\ \dots \dots \dots \dots \dots \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = k_m \end{cases}$$

*tiene solución, entonces es equivalente a un sistema*

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n = l_1 \\ \dots \dots \dots \dots \dots \dots \\ b_{r1}x_1 + b_{r2}x_2 + \dots + b_{rn}x_r = l_r \end{cases}$$

*con  $r$  ecuaciones (y, además, escalonado), en donde  $r \leq m$  es el rango de la matriz del sistema (y de la matriz aumentada).*

### Ejemplos:

1. Consideremos el siguiente sistema y su matriz aumentada:

$$\begin{cases} x + y - 2z &= 1 \\ 2x - y - z - 3t &= -4 \\ x + 2y - 3z + t &= 3 \\ 2x + y - 3z - t &= 0 \end{cases} \quad \left( \begin{array}{ccccc|c} 1 & 1 & -2 & 0 & 1 \\ 2 & -1 & -1 & -3 & -4 \\ 1 & 2 & -3 & 1 & 3 \\ 2 & 1 & -3 & -1 & 0 \end{array} \right)$$

Llevemos la matriz a la forma escalonada:

$$\sim \left[ \begin{array}{ccccc} 1 & 1 & -2 & 0 & 1 \\ 0 & -3 & 3 & -3 & -6 \\ 0 & 1 & -1 & 1 & 2 \\ 0 & -1 & 1 & -1 & -2 \end{array} \right] \sim \left[ \begin{array}{ccccc} 1 & 1 & -2 & 0 & 1 \\ 0 & 1 & -1 & 1 & 2 \\ 0 & 1 & -1 & 1 & 2 \\ 0 & -1 & 1 & -1 & -2 \end{array} \right]$$

$$\sim \left[ \begin{array}{ccccc} 1 & 1 & -2 & 0 & 1 \\ 0 & 1 & -1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right].$$

Aquí vemos que la matriz del sistema y la matriz aumentada tienen ambas rango 2, por lo que el sistema tiene solución. Además el sistema es equivalente al sistema

$$\begin{cases} x + y - 2z = 1 \\ y - z + t = 2 \end{cases}$$

que, como se dijo en la proposición 2, consta de 2 ecuaciones. Por lo tanto, para resolver el sistema original, bastará resolver este sistema con 2 ecuaciones.

2. Analicemos el sistema

$$\begin{cases} x - y + z + 2t = 0 \\ 2x + y - z - 5t = -6 \\ x - 2y + z + 4t = -1 \\ x + y + 2z - t = 5. \end{cases}$$

Calculemos los rangos:

$$\sim \left[ \begin{array}{ccccc} 1 & -1 & 1 & 2 & 0 \\ 2 & 1 & -1 & -5 & -6 \\ 1 & -2 & 1 & 4 & -1 \\ 1 & 1 & 2 & -1 & 5 \end{array} \right] \sim \left[ \begin{array}{ccccc} 1 & -1 & 1 & 2 & 0 \\ 0 & 3 & -3 & -9 & -6 \\ 0 & -1 & 0 & 2 & -1 \\ 0 & 2 & 1 & -3 & 5 \end{array} \right]$$

$$\sim \left[ \begin{array}{ccccc} 1 & -1 & 1 & 2 & 0 \\ 0 & -1 & 0 & 2 & -1 \\ 0 & 3 & -3 & -9 & -6 \\ 0 & 2 & 1 & -3 & 5 \end{array} \right] \sim \left[ \begin{array}{ccccc} 1 & -1 & 1 & 2 & 0 \\ 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & -3 & -3 & -9 \\ 0 & 0 & 1 & 1 & 3 \end{array} \right]$$

$$\sim \left[ \begin{array}{ccccc} 1 & -1 & 1 & 2 & 0 \\ 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 1 & 3 \end{array} \right].$$

Los dos rangos son 3 y el sistema original es equivalente al sistema con tres ecuaciones

$$\begin{cases} x - y + z + 2t = 0 \\ -y + 2t = -1 \\ z + t = 3 \end{cases}$$

el cual es ya fácil de resolver.

Veremos ahora cómo encontrar todas las soluciones de un sistema. Podemos suponer que, si el sistema tiene solución y es de rango  $r$ , tiene  $r$  ecuaciones (según la proposición anterior). Además, si es necesario podemos intercalar la numeración de las incógnitas de tal forma que  $\{B_1, B_2, \dots, B_r\}$  sea linealmente independiente. El sistema será de la forma

$$\begin{cases} a_{11}x_1 + \dots + a_{1r}x_r + \dots + a_{1n}x_n = k_1 \\ a_{21}x_1 + \dots + a_{2r}x_r + \dots + a_{2n}x_n = k_2 \\ \dots \dots \dots \dots \dots \dots \dots \\ a_{r1}x_1 + \dots + a_{rr}x_r + \dots + a_{rn}x_n = k_r \end{cases}$$

Con las hipótesis de que  $\{B_1, B_2, \dots, B_r\}$  es linealmente independiente podemos, según el teorema 2 del párrafo 4, dar arbitrariamente  $n-r$  números reales  $s_{r+1}, \dots, s_n$  y asegurar que existen  $s_1, \dots, s_r$  únicos, tales que

$$(s_1, \dots, s_r, s_{r+1}, \dots, s_n)$$

es solución. Para encontrar  $s_1, \dots, s_r$  sustituimos en el sistema,  $x_{r+1} = s_{r+1}, \dots, x_n = s_n$  y obtenemos un sistema de  $r$  ecuaciones en  $r$  incógnitas:

$$\begin{cases} a_{11}x_1 + \dots + a_{1r}x_r = k_1 - a_{1, r+1}s_{r+1} - \dots - a_{1n}s_n \\ a_{21}x_1 + \dots + a_{2r}x_r = k_2 - a_{2, r+1}s_{r+1} - \dots - a_{2n}s_n \\ \dots \dots \dots \dots \dots \dots \dots \\ a_{r1}x_1 + \dots + a_{rr}x_r = k_r - a_{r, r+1}s_{r+1} - \dots - a_{rn}s_n \end{cases}$$

Al resolver éste obtenemos  $s_1, \dots, s_r$ . Este sistema puede resolverse, en particular, con las fórmulas de Cramer, pues el determinante es distinto de cero.

### Ejemplos:

3. Reconsideremos el ejemplo 1 anterior:

$$\begin{cases} x + y - 2z = 1 \\ y - z + t = 2 \end{cases}$$

Como  $B_1 = (1, 0)$ ,  $B_2 = (1, 1)$ ,  $\{B_1, B_2\}$  es linealmente independiente, o, lo que es lo mismo,

$$\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} \neq 0.$$

Luego, podemos escribir  $z = s$ ,  $t = s'$ , y

$$\begin{cases} x + y = 1 + 2s \\ y = 2 + s - s' \end{cases}$$

en donde  $s$  y  $s'$  son números arbitrarios.

Tenemos entonces que

$$d = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1,$$

$$d_1 = \begin{vmatrix} 1+2s & 1 \\ 2+s-s' & 1 \end{vmatrix} = 1+2s-2-s+s' = -1+s+s',$$

$$d_2 = \begin{vmatrix} 1 & 1+2s \\ 0 & 2+s-s' \end{vmatrix} = 2+s-s'.$$

Por lo tanto,

$$x = d_1/d = -1 + s + s'; \quad y = 2 + s - s', \quad z = s, \quad t = s'.$$

O sea, las soluciones son

$$(-1 + s + s', 2 + s - s', s, s')$$

con  $s$  y  $s'$  números arbitrarios.

En relación con el teorema del párrafo 5 podemos observar que  $\bar{S} = (-1, 2, 0, 0)$  es una solución particular del sistema y que el espacio  $W$  de soluciones del sistema homogéneo asociado consta de los vectores de la forma  $(s + s', s - s', s, s')$ . Si llamamos  $S = (1, 1, 1, 0)$  y  $S' = (1, -1, 0, 1)$  entonces  $\{S, S'\}$  es una base de  $W$ , pues son independientes y

$$(s + s', s - s', s, s') = sS + s'S'.$$

Así pues, el conjunto de soluciones del sistema es

$$\{\bar{S} + sS + s'S' \mid s, s' \in \mathbf{R}\}$$

con  $\bar{S} = (-1, 2, 0, 0)$ ,  $S = (1, 1, 1, 0)$  y  $S' = (1, -1, 0, 1)$ .

4. Revisemos ahora el sistema del ejemplo 2. Vimos que el sistema es equivalente a

$$\begin{cases} x - y + z + 2t = 0 \\ -y + 2t = -1 \\ z + t = 3 \end{cases}$$

Como

$$\begin{vmatrix} 1 & -1 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \neq 0,$$

las primeras 3 columnas de coeficientes son linealmente independientes. Entonces podemos tomar  $t = s$ , un número arbitrario, y escribir

$$\begin{cases} x - y + z = -2s \\ -y = -1 - 2s \\ z = 3 - s. \end{cases}$$

Y aquí podríamos usar las fórmulas de Cramer para acabar de resolver el sistema, pero resulta más práctico simplemente sustituir.

Las soluciones son

$$(-2 + s, 1 + 2s, 3 - s),$$

con  $s$  un número cualquiera.

Aquí podemos ilustrar nuevamente el teorema del párrafo 5. En efecto,  $\bar{S} = (-2, 1, 3, 0)$  es una solución particular [también lo son  $(-1, 3, 2, 1)$ ,  $(-3, -1, 4, -1)$ , etc.]. El espacio  $W$  de soluciones del sistema homogéneo asociado está generado por  $S = (1, 2, -1, 1)$ . Por lo tanto el conjunto de soluciones del sistema es

$$\{\bar{S} + sS \mid s \in \mathbf{R}, \bar{S} = (-2, 1, 3, 0), S = (1, 2, -1, 1)\}.$$

5. Analicemos finalmente el ejemplo 2 del párrafo 2. Se vio que el sistema

$$\begin{cases} x - y + 2z = 1 \\ y - z = 1 \\ 3x + y - z = 0 \\ 4x + y = 2 \end{cases}$$

es equivalente a

$$\begin{cases} x - y + 2z = 1 \\ y - z = 1 \\ 3z = 7. \end{cases}$$

Como  $r = n$  hay una sola solución, la cual se obtiene fácilmente sustituyendo:

$$z = \frac{7}{3}, \quad y = 1 + z = 1 + \frac{7}{3} = \frac{10}{3}, \quad x = 1 + y - 2z = -\frac{1}{3}.$$

La solución es  $\left(\frac{7}{3}, \frac{10}{3}, -\frac{1}{3}\right)$ . (En este caso, el subespacio de soluciones  $W$  del sistema homogéneo asociado consta únicamente del vector 0.)

**OBSERVACIÓN.** En los ejemplos anteriores hemos visto que no es necesario utilizar las fórmulas de Cramer al llegar al sistema de  $r$  ecuaciones con  $r$  incógnitas, pues el hecho de que la matriz esté en forma escalonada permite despejar muy fácilmente las incógnitas.

De hecho, el método de Cramer es muy poco práctico, pues exige el cálculo de  $n + 1$  determinantes de matrices de  $n \times n$ . Se ve que el cálculo de uno de ellos es más o menos igual de laborioso que llevar una matriz a la forma escalonada. Veremos esto en el siguiente ejemplo.

### Ejemplos:

#### 6. Consideraremos el sistema

$$\begin{cases} x + y + z + t = 10 \\ x + y - z - t = -4 \\ 2x - y + 2z - t = 2 \\ x + 2y - z - 2t = -6. \end{cases}$$

Escribimos

$$\begin{aligned} & \left[ \begin{array}{ccccc} 1 & 1 & 1 & 1 & 10 \\ 1 & 1 & -1 & -1 & -4 \\ 2 & -1 & 2 & -1 & 2 \\ 1 & 2 & -1 & -2 & -6 \end{array} \right] \sim \left[ \begin{array}{ccccc} 1 & 1 & 1 & 1 & 10 \\ 0 & 0 & -2 & -2 & -14 \\ 0 & -3 & 0 & -3 & -18 \\ 0 & 1 & -2 & -3 & -16 \end{array} \right] \sim \\ & \sim \left[ \begin{array}{ccccc} 1 & 1 & 1 & 1 & 10 \\ 0 & 1 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 7 \\ 0 & 1 & -2 & -3 & -16 \end{array} \right] \sim \left[ \begin{array}{ccccc} 1 & 1 & 1 & 1 & 10 \\ 0 & 1 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 7 \\ 0 & 0 & -2 & -4 & -22 \end{array} \right] \sim \\ & \sim \left[ \begin{array}{ccccc} 1 & 1 & 1 & 1 & 10 \\ 0 & 1 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 7 \\ 0 & 0 & 0 & -2 & -8 \end{array} \right] \sim \left[ \begin{array}{ccccc} 1 & 1 & 1 & 1 & 10 \\ 0 & 1 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 7 \\ 0 & 0 & 0 & 1 & 4 \end{array} \right] \sim \end{aligned}$$

El sistema original es equivalente a

$$\begin{cases} x + y + z + t = 10 \\ y + t = 6 \\ z + t = 7 \\ t = 4, \end{cases}$$

de donde, la solución (única) es  $(1, 2, 3, 4)$ .

Con el método de Cramer se hubiera necesitado el cálculo de 5 determinantes de  $4 \times 4$ .

## EJERCICIOS

Resuélvanse los siguientes sistemas de ecuaciones:

1.

$$\begin{cases} x - y - 2z = 0 \\ 2x - y - 3z = 1 \\ y - z = 1 \\ x - z = 1 \\ x + 2y + z = 3 \end{cases}$$

2.

$$\begin{cases} x - y - z = 0 \\ 2x - y + z = 0 \\ 3x - 2y + z = -1 \\ x + y + 5z = 0 \\ 2x + y + 7z = 0 \end{cases}$$

3.

$$\begin{cases} x_1 + x_2 + x_3 = 3 \\ x_1 + x_2 - 3x_3 = -1 \\ 2x_1 + x_2 - 3x_3 = 1 \\ x_1 + 2x_2 - 2x_3 = 1 \end{cases}$$

4.

$$\begin{cases} x_1 + x_2 + x_3 - 2x_4 - 2x_5 = 5 \\ 2x_1 - x_2 - x_4 - 2x_5 = 0 \\ 2x_1 - x_3 - 2x_4 - x_5 = 0 \\ x_2 - x_3 - x_4 + x_5 = 0 \end{cases}$$

5.

$$\begin{cases} x + y + z + t = 0 \\ x - y + z - t = 0 \\ x + y - z - t = 0 \\ x + 2y + 2z + t = 3 \\ 2x + y + z + 2t = -3 \end{cases}$$

6.

$$\begin{cases} x_1 - 3x_2 + 4x_3 + 6x_4 = 0 \\ -2x_1 + 4x_2 + x_3 + 7x_4 = 0 \\ 3x_1 - x_2 + 2x_3 + 5x_4 = 0 \\ -x_1 + 2x_2 + 3x_3 + 7x_4 = 0 \end{cases}$$

7.

$$\begin{cases} 2x_1 + x_2 - x_3 + x_4 = 3 \\ x_1 + 2x_2 + x_3 - x_4 = 3 \\ x_1 - x_3 + x_4 = 0 \\ x_2 + x_3 - x_4 = 0 \\ 3x_1 + x_2 - 2x_3 + 2x_4 = 4 \\ x_1 + 3x_2 + 2x_3 - 2x_4 = 4 \end{cases}$$

8.

$$\begin{cases} x_1 + x_2 + 3x_3 - 2x_4 - x_5 = 1 \\ 5x_1 - 2x_2 + 3x_3 + 7x_4 + 8x_5 = 3 \\ -3x_1 - x_2 + 2x_3 + 7x_4 + 5x_5 = 2 \\ 5x_1 + 3x_2 + x_3 - 2x_4 - 7x_5 = 3 \end{cases}$$

9.

$$\begin{cases} x_1 - x_2 + x_3 + x_4 + 2x_5 = -1 \\ -x_1 + x_2 + x_3 + x_4 - 4x_5 = 3 \\ -x_1 - x_2 + x_3 + x_4 - 2x_5 = 3 \\ x_1 - 2x_2 + x_3 + 2x_4 + 3x_5 = -1 \\ -4x_2 + x_3 + 5x_4 + 3x_5 = 1 \end{cases}$$

# 6

CAPÍTULO

## El anillo de los números enteros

Todos estamos bien familiarizados con los números enteros. En este capítulo empezaremos destacando las propiedades básicas de las operaciones de adición y multiplicación de números enteros y veremos cómo a partir de ellas se demuestran otras propiedades que ya conocemos. Después estudiaremos la relación de orden y el principio de inducción.

Como es costumbre  $\mathbf{Z}$  denotará el conjunto de los números enteros:

$$\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}.$$

### 1. PROPIEDADES BÁSICAS DE LAS OPERACIONES EN $\mathbf{Z}$

Los números enteros constan del conjunto  $\mathbf{Z}$  y dos operaciones binarias, la adición y la multiplicación que satisfacen los siguientes axiomas:

**AXIOMA 1.** *La suma de números enteros es conmutativa*, es decir, si  $a, b \in \mathbf{Z}$ , entonces

$$a + b = b + a.$$

**AXIOMA 2.** *La suma de números enteros es asociativa*, es decir, si  $a, b, c \in \mathbf{Z}$ , entonces

$$(a + b) + c = a + (b + c).$$

**AXIOMA 3.** Existe en  $\mathbf{Z}$  un elemento neutro para la suma, el 0. Es decir, si  $a \in \mathbf{Z}$ ,

$$a + 0 = 0 + a = a.$$

**AXIOMA 4.** Para cada  $a$  en  $\mathbf{Z}$  existe en  $\mathbf{Z}$  su inverso aditivo que se denota por  $-a$ . Esto es,

$$a + (-a) = (-a) + a = 0.$$

**AXIOMA 5.** El producto de números enteros es commutativo, es decir, si  $a, b \in \mathbf{Z}$  entonces

$$ab = ba.$$

**AXIOMA 6.** El producto en  $\mathbf{Z}$  es asociativo, es decir, si  $a, b, c \in \mathbf{Z}$  entonces

$$(ab)c = a(bc).$$

**AXIOMA 7.** Existe en  $\mathbf{Z}$  un elemento neutro para la multiplicación, el 1. Es decir, si  $a \in \mathbf{Z}$

$$a1 = 1a = a.$$

**AXIOMA 8.** En  $\mathbf{Z}$  el producto distribuye a la suma, es decir, si  $a, b, c \in \mathbf{Z}$  entonces

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc. \end{aligned}$$

## 2. ANILLOS

En matemáticas aparecen con mucha frecuencia conjuntos en los cuales se tienen dos operaciones que cumplen los axiomas 1, 2, ..., 8 que acabamos de mencionar. En estos casos se dice que dichos conjuntos, con las operaciones respectivas, constituyen un *anillo commutativo, con elemento unitario* (el 1).

Así pues, podemos decir que el conjunto  $\mathbf{Z}$  de los números enteros, con las operaciones  $+$  y  $\times$  forman un anillo.

Cuando valen todos los axiomas menos (posiblemente) el 5 y el 7, a dichas estructuras se les llama simplemente anillos.

A continuación daremos varios ejemplos de anillos.

Sea  $A$  un conjunto con dos elementos:

$$A = \{a, b\}$$

y definamos dos operaciones, que por comodidad seguiremos llamando suma y producto y denotándolas con  $+$  y  $\times$ , mediante las tablas siguientes:

$+ \begin{array}{c cc} & a & b \\ \hline a & a & b \\ b & b & a \end{array}$	$\times \begin{array}{c cc} & a & b \\ \hline a & a & a \\ b & a & b \end{array}$
--	---

Según vemos en la tabla

$$a + b = b \quad y \quad b + a = b,$$

de donde  $a + b = b + a$ , es decir, la suma es commutativa.

Para ver que la suma es asociativa, debemos considerar todas las ternas posibles de elementos de  $A$  y probar que al sumarlos en las dos formas indicadas en el axioma 2 obtenemos el mismo elemento. Algunas de las posibles ternas son

$$\begin{aligned} &a, a, a \\ &a, a, b \\ &a, b, a \\ &a, b, b. \end{aligned}$$

En el ejercicio 1 se pide encontrar las ternas restantes. Ahora bien, para la primera terna tenemos

$$\begin{aligned} (a + a) + a &= a + a = a \\ a + (a + a) &= a + a = a. \end{aligned}$$

Para la segunda, tenemos

$$\begin{aligned} (a + a) + b &= a + b = b \\ a + (a + b) &= a + b = b. \end{aligned}$$

Una vez resuelto el ejercicio 1 quedará probado que la suma en  $A$  es asociaitiva.

Es fácil ver que en  $A$  hay un elemento que es neutro con respecto a la adición. En efecto, ya que

$$a + a = a \quad y \quad a + b = b,$$

resulta que  $a$  es dicho elemento.

Vemos en la tabla que  $a + a = a$ , de donde el inverso aditivo de  $a$  es  $a$ . Es decir,  $-a = a$ . Análogamente, ya que  $b + b = 0$ , tenemos que  $-b = b$ . O sea, los dos elementos tienen inverso aditivo y se cumple el axioma 4.

En el ejercicio 2 se pide probar que en  $A$  se cumplen los axiomas 5, 6 y 7 para la multiplicación y en el 3 se pide probar la asociatividad.

De esta manera, quedará demostrado que  $A$  es un anillo.

Podemos dar ahora un ejemplo de anillo con 3 elementos. Sea

$$B = \{\bar{0}, \bar{1}, \bar{2}\}$$

con las operaciones siguientes:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Según se verá en el ejercicio 4,  $B$  es un anillo. Consideraremos finalmente un ejemplo más. Denotemos con  $P$  al conjunto de todos los enteros pares:

$$P = \{\dots, -4, -2, 0, 2, 4, \dots\}.$$

Este conjunto, con las operaciones usuales de adición y multiplicación satisface todos los axiomas menos uno. ¿Cuál es?

Más adelante, en este mismo curso, veremos muchos ejemplos de anillos. En particular, estudiaremos con detalle el anillo de los polinomios en una indeterminada. También estudiaremos los números racionales, los números reales y los números complejos; estos son anillos con ciertas propiedades adicionales por lo que reciben el nombre de campos.

## EJERCICIOS

1. Encuéntrense todas las ternas posibles de elementos de  $A = \{a, b\}$  y pruebe que la adición antes definida en este conjunto es asociativa.
2. Pruébese que en  $A$  valen los axiomas 5, 6 y 7. (El elemento unitario es  $b$ .) Para la asociatividad aprovechense las ternas encontradas en el ejercicio anterior.
3. Pruébese que en  $A$  vale la ley distributiva.
4. Pruébese que  $B = \{\bar{0}, \bar{1}, \bar{2}\}$  con las operaciones antes definidas es un anillo conmutativo con elemento unitario (el  $\bar{1}$ ).
5. El conjunto  $C = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  con las operaciones definidas en las tablas siguientes,

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

es un anillo. Encuéntrese el neutro para la adición, el neutro para la multiplicación y el inverso aditivo de cada elemento de  $C$ .

6. Encuéntrense dos elementos en el anillo  $C$  del ejercicio anterior que sean distintos de 0 y cuyo producto sea 0.

### 3. PROPIEDADES DE ANILLO DE LOS ENTEROS

Veremos ahora cómo, a partir de las propiedades básicas de las operaciones con los números enteros, pueden demostrarse otras muchas de las que conocemos. La importancia de proceder en esta forma es que estas propiedades no solo serán válidas en los enteros, sino en cualquier conjunto con dos operaciones que cumplan los axiomas 1, 2, ..., 8, es decir en cualquier anillo conmutativo con elemento unitario.

Así, cuando nos encontremos con un anillo de esos, no habrá necesidad de demostrar nuevamente para él dichas propiedades pues, debido a que para la demostración de estas únicamente se usan los axiomas mencionados, podemos asegurar que todas ellas serán válidas en él.

**PROPOSICIÓN 1:** (Ley de cancelación.) *Si  $a$ ,  $b$  y  $c$  son enteros y  $a + b = a + c$ , entonces  $b = c$ .*

*Demostración.* Supongamos que  $a + b = a + c$ . Según el axioma 4 existe un entero,  $-a$ , tal que  $(-a) + a = 0$ . Tenemos entonces que

$$(-a) + (a+b) = (-a) + (a+c).$$

Por la propiedad asociativa (axioma 2), podemos escribir

$$((-a)+a)+b = ((-a)+a)+c,$$

de donde,

$$0 + b = 0 + c$$

y como 0 es el elemento neutro aditivo (axioma 3), obtenemos que  $b = c$ .

Esta propiedad podríamos llamarla, con más precisión, ley de cancelación por la izquierda.

No todas las propiedades se demostrarán utilizando directamente los axiomas 1, 2, ..., 8. En ocasiones utilizaremos propiedades ya demostradas anteriormente a partir de ellos. (Así, de todas formas, las propiedades que demostremos serán consecuencia de los axiomas.)

Por ejemplo, utilizando la ley de cancelación por la izquierda y la propiedad conmutativa para la adición podemos demostrar fácilmente la ley de cancelación por la derecha.

**COROLARIO 1:** *Si  $a$ ,  $b$ , y  $c$  son enteros y  $a + c = b + c$ , entonces  $a = b$ .*

*Demostración.* Ya que  $a + c = b + c$ , por el axioma 1 obtenemos  $c + a = c + b$  y por la ley de cancelación demostrada anteriormente, resulta que  $a = b$ .

**COROLARIO 2:** Si  $a$  y  $b$  son enteros y  $a + b = a$ , entonces  $b = 0$ .

*Demostración.* Por hipótesis, ya que  $a = a + 0$ , tenemos que

$$a + b = a + 0,$$

de donde, por la ley de cancelación, obtenemos  $b = 0$ .

**PROPOSICIÓN 2:** Para todo entero  $a$ , se tiene que  $0a = 0$ .

*Demostración.* Ya que  $0 = 0 + 0$  (según el axioma 3) tenemos, por la propiedad asociativa; que

$$0a = (0+0)a = 0a + 0a.$$

Por lo tanto, según el corolario anterior, resulta que  $0a = 0$ .

Usando la ley de cancelación podemos demostrar fácilmente que

**COROLARIO 2:** El inverso aditivo del inverso aditivo de un número entero  $a$  es  $a$ . Es decir,

$$-(-a) = a.$$

*Demostración.* Por definición de inverso aditivo de un entero sabemos que

$$(-a) + a = 0 \tag{1}$$

y también que

$$-(-a) + (-a) = 0. \tag{2}$$

Por la propiedad conmutativa, (1) nos da

$$a + (-a) = 0, \tag{3}$$

por lo que, de (2) y (3) obtenemos

$$a + (-a) = -(-a) + (-a).$$

Ahora bien, usando la propiedad de cancelación obtenemos que  $a = -(-a)$  que es lo que se quería demostrar.

Podemos ahora demostrar las a veces llamadas “reglas de los signos”.

**PROPOSICIÓN 3:** Si  $a, b \in \mathbf{Z}$ , entonces

$$(-a)b = -(ab)$$

$$(-a)(-b) = ab.$$

*Demostración.* Tenemos que

$$(-a)b + ab = ((-a) + a)b = 0b = 0,$$

y también, por definición de inverso aditivo,

$$-(ab) + ab = 0.$$

Por consiguiente

$$(-a)b + ab = -(ab) + ab$$

y por la ley de cancelación resulta que

$$(-a)b = -(ab)$$

con lo que queda demostrada la primera parte.

Se tiene que

$$(-a)b + (-a)(-b) = (-a)(b + (-b)) = (-a)0 = 0$$

y también, como vimos antes,

$$(-a)b + ab = 0.$$

Por consiguiente,

$$(-a)b + (-a)(-b) = (-a)b + ab$$

y, cancelando, obtenemos

$$(-a)(-b) = ab$$

con lo que queda probada la segunda parte.

**COROLARIO 3:**

$$(-1)a = -a \quad (a \in \mathbf{Z})$$

$$(-1)(-1) = 1.$$

La diferencia de dos números enteros se puede definir utilizando la adición y los inversos aditivos.

**DEFINICIÓN:** Si  $a, b \in \mathbf{Z}$  la diferencia  $a - b$  es el entero

$$a - b = a + (-b).$$

**PROPOSICIÓN 4:** Si  $a, b, c \in \mathbf{Z}$ , entonces

$$a(b - c) = ab - ac.$$

En efecto,

$$a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac.$$

Como caso particular resulta que:

COROLARIO 4:  $-(a+b) = -a - b$ .

En efecto

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

### EJERCICIOS

1. Demuéstrese que si  $a + b = c$  ( $a, b, c$  enteros), entonces  $a = c - b$ .

2. Demuéstrese que si  $a - b = c$ , entonces  $a = c + b$ .

No todas las propiedades de las operaciones en los enteros son consecuencia de los axiomas de anillo. Por ejemplo, en  $\mathbf{Z}$  se tiene la propiedad siguiente:

**AXIOMA 9:** *Si  $a, b$  son números enteros diferentes de cero, entonces su producto  $ab$  es diferente de cero.*

Es fácil ver que esta propiedad no es consecuencia de los axiomas 1, 2, ..., 8. La forma de hacerlo es exhibir un anillo commutativo, con 1 en donde podemos encontrar dos elementos distintos de cero, cuyo producto sea cero. Pero esto ya lo hicimos en los ejercicios 5 y 6. En efecto, en el anillo  $C = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  que ahí se construyó se tiene que  $\bar{2} \neq \bar{0}$  y  $\bar{2} \cdot \bar{2} = \bar{0}$ .

A los elementos  $a, b$  cuyo producto es cero se les llama divisores de cero. Con esta terminología, el axioma 9 dice que *en  $\mathbf{Z}$  no hay divisores de cero distintos de cero*.

## 4. DOMINIOS ENTEROS

**DEFINICIÓN:** *Si  $A$  es un anillo commutativo con 1 en el cual se cumple el axioma 9 se dirá que  $A$  es un dominio entero.*

Así pues, podemos decir que  $\mathbf{Z}$  es un dominio entero. Más adelante estudiaremos otros dominios enteros que juegan un importante papel en matemáticas, en particular los anillos de polinomios.

**PROPOSICIÓN:** *En un dominio entero vale la ley de cancelación para la multiplicación. Es decir, si  $a, b, c \in \mathbf{Z}$  y  $a \neq 0$  entonces  $ab = ac$  implica  $b = c$ .*

*Demostración.* Ya que  $ab = ac$  tenemos que  $ab - ac = 0$ , de donde  $a(b - c) = 0$  y como  $a \neq 0$  forzosamente  $b - c = 0$ , es decir,  $b = c$ .

La conveniencia de demostrar esta y otras propiedades para dominios enteros en general es que cada vez que tengamos un dominio entero podremos asegurar que en él valen estas propiedades. Por ejemplo, ya que  $\mathbf{Z}$  es un dominio entero, *en  $\mathbf{Z}$  vale la ley de cancelación*.

Es necesario observar que en esta propiedad el factor que podemos cancelar debe ser *distinto de cero*. En efecto, si  $a = 0$  puede ser que  $ab = ac$  sin que  $b$  y  $c$  sean iguales.

## EJERCICIOS

1. Demuéstrese que el anillo que consta de dos elementos y las operaciones definidas en la sección 1 de este capítulo es un dominio entero.
2. Lo mismo para el anillo con 3 elementos de dicha sección.
3. El anillo del ejercicio 5 de la sección 1 no es un dominio entero. ¿Por qué?
4. Pruébese que si en un anillo conmutativo con elemento unitario vale la ley de cancelación para la multiplicación, entonces es un dominio entero.

Según el ejercicio 4, podemos decir que un dominio entero es un anillo conmutativo con elemento unitario en el cual no hay divisores de cero distintos de cero.

## 5. EL ORDEN EN $\mathbf{Z}$

Otro aspecto muy importante en el anillo de los números enteros es el orden. Sabemos cuándo un número es mayor que otro. Ahora precisaremos este concepto.

Los números naturales  $\mathbf{N}$  forman un subconjunto de los números enteros:

$$\mathbf{N} = \{1, 2, 3, \dots\} \subset \mathbf{Z}.$$

Destacaremos las tres propiedades básicas siguientes:

**AXIOMA 10:** *La suma de dos números naturales es un número natural.*

**AXIOMA 11:** *El producto de dos números naturales es un número natural.*

**AXIOMA 12:** *Si  $a$  es un número entero se cumple una y solamente una de las tres condiciones siguientes:*

- i)  $a$  es un número natural;
- ii)  $a = 0$ ;
- iii)  $-a$  es un número natural.

Dicho de otra manera, un entero puede ser o bien natural, o bien cero, o bien su inverso aditivo es natural.

Usando el subconjunto  $\mathbf{N}$  de  $\mathbf{Z}$  y estas tres propiedades, podemos definir el orden y demostrar las propiedades básicas del orden y las que de ellas se deduzcan.

**DEFINICIÓN:** Si  $a$  y  $b$  son números enteros, decimos que  $a$  es mayor que  $b$  si  $a - b$  es un número natural.

En símbolos,

$$a > b \iff a - b \in \mathbf{N}.$$

Observemos que, de esta definición se sigue que

$$a > 0 \iff a \in \mathbf{N},$$

pues  $a - 0 = a$ .

A los números  $a$  tales que  $a > 0$  se les llama *positivos*. Así pues, *los números naturales son los enteros positivos*.

Demostraremos ahora, usando los axiomas 10, 11 y 12 las propiedades de la relación de orden “mayor que”.

**PROPOSICIÓN 1** (propiedad transitiva): Si  $a$ ,  $b$  y  $c$  son enteros tales que  $a > b$  y  $b > c$  entonces  $a > c$ .

*Demostración.*  $a > b$  significa, según la definición, que  $a - b \in \mathbf{N}$ . Análogamente, como  $b > c$ , sabemos que  $b - c \in \mathbf{N}$ . Por el axioma 10, como  $a - b \in \mathbf{N}$  y  $b - c \in \mathbf{N}$  tenemos que su suma  $(a - b) + (b - c) \in \mathbf{N}$ . Pero  $(a - b) + (b - c) = a - c$ . Por lo tanto  $a - c \in \mathbf{N}$ , lo que, según la definición significa que  $a > c$ .

Como es costumbre, la notación  $a < b$  equivale a  $b > a$  y  $a \geq b$  significa que  $a > b$  o que  $a = b$ . Análogamente  $a \leq b$  significa  $a < b$ , o bien  $a = b$ .

El axioma 12 podemos enunciarlo ahora como sigue:

**PROPOSICIÓN 2:** Si  $a$  es un número entero, se cumple una y solamente una de las condiciones siguientes:

- i)  $a > 0$ ;
- ii)  $a = 0$ ;
- iii)  $a < 0$ .

**PROPOSICIÓN 3:** Si  $a$ ,  $b$  y  $c$  son enteros y  $a > b$ , entonces  $a + c > b + c$ .

*Demostración.* Puesto que  $a > b$ , sabemos que  $a - b \in \mathbf{N}$ . Ya que  $a - b = (a + c) - (b + c)$  tenemos que  $(a + c) - (b + c) \in \mathbf{N}$ .

## EJERCICIOS

1. Demuéstrese que el cuadrado de cualquier entero distinto de cero es positivo.

2. Demuéstrese que si  $a, b \in \mathbf{Z}$ ,  $a^2 + b^2 \geq 0$ .  
 3. Demuéstrese que si  $a < b$ , entonces  $-a > -b$ . (Esto será consecuencia del ejercicio 4, pero aquí se pide probarlo directamente a partir de las definiciones.)

**PROPOSICIÓN 4:** *Si  $a, b$  y  $c$  son enteros tales que  $a > b$  y  $c > 0$ , entonces  $ac > bc$ .*

*Demostración.* Por hipótesis  $a - b \in \mathbf{N}$  y  $c \in \mathbf{N}$ . Luego, por el axioma 11,  $(a - b)c \in \mathbf{N}$ , es decir,  $ac - bc$  es natural, de donde,  $ac > bc$ .

4. Demuéstrese que si  $a > b$  y  $c < 0$  entonces  $ac < bc$ .

**PROPOSICIÓN 5:** *Si  $a$  y  $b$  son enteros positivos y  $b > 1$ , entonces  $ab > a$ .*

En efecto,  $b > 1$  y  $a > 0$ . Por lo tanto, según la proposición 6, tenemos que  $ba > 1a$ , es decir,  $ab > a$ .

## EJERCICIOS

5. Demuéstrese que si  $a$  y  $b$  son naturales y  $a < b$ , entonces  $a^2 < b^2$ .  
 6. Encuéntrense ejemplos de números enteros tales que  $a < b$  y  $a^2 > b^2$  (lo cual indica que es necesario suponer en el ejercicio 5 que  $a$  y  $b$  son positivos).  
 7. Demuéstrese que si  $a$  y  $b$  son enteros positivos entonces  $a^2 < b^2$  implica que  $a < b$ .  
 8. Con ejemplos, pruébese que la condición de que los enteros del ejercicio anterior sean positivos no se puede omitir.  
 9. Demuéstrese que si  $a > b$  y  $c > d$ , entonces  $a + c > b + d$ . (Utilícese dos veces la proposición 3.)

## 6. UNIDADES EN $\mathbf{Z}$

Uno de los axiomas que se cumplen para los enteros (el que hemos numerado con 4), asegura la existencia de un inverso aditivo para cada elemento de  $\mathbf{Z}$ . Podríamos ahora preguntarnos qué ocurre con los inversos multiplicativos de los números enteros.

**PROPOSICIÓN:** *Los únicos elementos de  $\mathbf{Z}$  que tienen inverso multiplicativo (en  $\mathbf{Z}$ ) son 1 y -1.*

*Demostración.* 0 no tiene inverso multiplicativo pues  $0a = 0 \neq 1$  para cualquier  $a$ :

- 1 tiene a 1 por inverso multiplicativo, pues  $1 \cdot 1 = 1$ .  
 -1 tiene a -1 como inverso multiplicativo, pues  $(-1)(-1) = 1$ .

Supongamos ahora que  $a > 1$ . Si  $a$  tuviera inverso multiplicativo, digamos  $a^{-1} \in \mathbf{Z}$  entonces, ya que  $aa^{-1} = 1$ ,  $a^{-1}$  no puede ser negativo. Por lo

tanto  $a^{-1} > 0$ . También  $a^{-1} \neq 1$ , pues si  $a^{-1} = 1$ ,  $a = 1$  (porque  $aa^{-1} = 1$ ). Por lo tanto  $a^{-1} > 1$ . Pero como  $a > 1$  y  $a^{-1} > 1$ ,  $aa^{-1} > 1$  también, lo cual contradice que  $aa^{-1} = 1$ .

Para  $a < 0$ , véase el ejercicio 2.

En un anillo, a los elementos que tienen inverso multiplicativo se les llama *unidades*.

Así, en el anillo de los números enteros, 1 y  $-1$  son las únicas unidades.

## EJERCICIOS

1. Demuéstrese que  $a$  es unidad si y solamente si  $-a$  es una unidad.
2. Usando el ejercicio anterior complétense la demostración de la proposición.

## 7. EL PRINCIPIO DE INDUCCIÓN

En los números naturales vale la siguiente propiedad:

**Principio de inducción.** *Sea  $M$  un subconjunto de  $\mathbb{N}$  tal que se cumplen las condiciones*

- i)  $1 \in M$ ;
- ii) si  $n \in M$ , luego  $n + 1 \in M$ .

*Entonces  $M = \mathbb{N}$ .*

En otras palabras, si un conjunto  $M$  de números naturales contiene al 1 y contiene a  $n + 1$  cada vez que contenga a  $n$ , entonces  $M$  es el conjunto de *todos* los números naturales.

Esta propiedad sirve para demostrar muchas proposiciones. Veremos algunos ejemplos.

Supongamos que queremos demostrar que *para cualquier número natural  $n$ ,*

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

es decir, la suma de todos los números impares desde 1 hasta  $2n-1$  es  $n^2$ . (Por ejemplo,  $1 = 1^2$ ,  $1 + 3 = 2^2$ ,  $1 + 3 + 5 = 3^2$ ,  $1 + 3 + 5 + 7 = 4^2$ , etcétera.)

Sea  $M$  el conjunto de números naturales para los cuales la fórmula (\*) es cierta.

Vemos que

- i)  $1 \in M$ , pues, como ya dijimos,  $1 = 1^2$ ;
- ii) si  $n \in M$ , entonces  $n+1 \in M$ .

En efecto, que  $n \in M$  (lo que llamamos hipótesis de inducción) significa que vale (\*). Calculemos pues

$$1 + 3 + 5 + \dots + (2(n+1)-1).$$

Tenemos que, según la hipótesis de inducción,

$$\begin{aligned} 1 + 3 + 5 + \dots + (2n-1) + (2(n+1)-1) = \\ n^2 + (2n+1) = (n+1)^2, \end{aligned}$$

es decir, vale la fórmula para  $n+1$ , o sea  $n+1 \in M$ .

Luego, por el principio de inducción, podemos afirmar que  $M = \mathbb{N}$  y como  $M$  es el conjunto de  $n$  para los cuales vale (\*) podemos asegurar que dicha fórmula vale para todo  $n \in \mathbb{N}$ , que es lo que queríamos demostrar.

Veamos otro ejemplo. Para demostrar que para todo número natural  $n$  vale la relación

$$2^0 + 2^1 + 2^2 + \dots + 2^{n-1} = 2^n - 1 \quad (**)$$

podemos proceder como sigue:

Sea  $M$  el conjunto de todos los números naturales para los cuales (\*\*) es cierta. [Queremos demostrar que (\*\*) es cierta para todo natural, es decir, queremos demostrar que  $M = \mathbb{N}$ .]

i) Si  $n = 1$ , la fórmula (\*\*) es cierta, pues

$$2^0 = 2^1 - 1;$$

ii) supongamos ahora que  $n \in M$ , es decir, vale (\*\*) para  $n$ . Vamos a demostrar que (\*\*) vale para  $n+1$ :

$$\begin{aligned} 2^0 + 2^1 + 2^2 + \dots + 2^{n-1} + 2^n = \\ 2^n - 1 + 2^n = 2^{n+1} - 1. \end{aligned}$$

(En el primer paso usamos la hipótesis de inducción.)

Entonces, por el principio de inducción tenemos que  $M = \mathbb{N}$ , es decir, (\*\*) vale para cualquier número natural  $n$ .

## EJERCICIOS

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

2.  $1 + 5 + 5^2 + \dots + 5^{n-1} = \frac{5^n - 1}{4}.$

$$3. \quad 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$4. \quad \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Podemos acortar un poco la escritura de estas demostraciones examinando un caso general.

Sea  $P_1, P_2, \dots, P_n, \dots$  una sucesión de proposiciones. Para demostrar que son todas ciertas se puede proceder así:

Sea  $M$  el conjunto de números naturales  $n$  para los que sea cierta la proposición  $P_n$ .

Si logramos demostrar que:

- i)  $P_1$  es cierta (es decir, que  $1 \in M$ );
- ii) si  $P_n$  es cierta, entonces  $P_{n+1}$  es cierta (es decir, que si  $n \in M$  entonces  $n+1 \in M$ ),

entonces podemos afirmar, por el principio de inducción, que  $M = \mathbb{N}$ , es decir, que  $P_n$  es cierta para cualquier número entero  $n$ .

Por ejemplo, queremos demostrar que

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left( \frac{n(n+1)}{2} \right)^2. \quad (***)$$

Esta fórmula vale para  $n = 1$  pues

$$1^3 = \left( \frac{1 \cdot 2}{2} \right)^2.$$

Supongamos que vale para  $n$ . Para  $n+1$  obtenemos:

$$\begin{aligned} & 1^3 + 2^3 + \dots + n^3 + (n+1)^3 = \\ & = \left( \frac{n(n+1)}{2} \right)^2 + (n+1)^3 = (n+1)^2 \left( \frac{n^2}{2^2} + (n+1) \right) = \\ & = (n+1)^2 \frac{n^2 + 4n + 4}{2^2} = \frac{(n+1)^2(n+2)^2}{2^2} = \left( \frac{(n+1)(n+2)}{2} \right)^2, \end{aligned}$$

es decir, vale para  $n+1$ .

Por consiguiente la fórmula es cierta para cualquier número natural  $n$ .

## EJERCICIOS

Demuéstrense por inducción las siguientes igualdades:

$$5. \frac{1}{1 \cdot 2 \cdot 3} + \frac{1}{2 \cdot 3 \cdot 4} + \dots + \frac{1}{n(n+1)(n+2)} = \frac{n(n+3)}{4(n+1)(n+2)}.$$

$$6. \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{1}{2n+1}.$$

$$7. 1 \cdot 4 + 4 \cdot 7 + \dots + (3n-2)(3n+1) = n(3n^2+3n-2).$$

$$8. x^n + x^{n-1} + \dots + 1 = \frac{x^n - 1}{x - 1}.$$

$$9. 1^4 + 2^4 + \dots + n^4 = \frac{6n^5 + 15n^4 + 10n^3 - n}{30}.$$

Para ciertas demostraciones es a veces conveniente utilizar una modificación del principio de inducción que es equivalente al principio de inducción.

**Principio de inducción (modificado).** Si  $M$  es un subconjunto de  $\mathbb{N}$  tal que

- i)  $1 \in M$ ;
- ii) Si  $1, 2, \dots, n \in M$  entonces  $n+1 \in M$ ,

entonces  $M = \mathbb{N}$ .

## EJERCICIO

**10.** Demuéstrese que los dos principios de inducción son equivalentes.

## 8. EL PRINCIPIO DE BUEN ORDEN

En los números naturales se cumple también una propiedad que recibe el nombre de principio de buen orden. Como veremos más adelante, esta propiedad es equivalente al principio de inducción que acabamos de examinar.

**Principio de buen orden.** Si  $A$  es un subconjunto no vacío de números naturales entonces  $A$  tiene un elemento que es menor que todos los demás elementos de  $A$ .

**PROPOSICIÓN 1:** El principio de inducción implica el del buen orden.

*Demostración.* Sea  $A$  un subconjunto no vacío de  $\mathbb{N}$  y supongamos que  $A$  no tiene ningún elemento menor que todos los demás de  $A$ . Construyamos un conjunto  $B$  con todos los números naturales  $b$  tales que  $b < a$  para todo  $a$  en  $A$ . Como ningún elemento es menor que sí mismo,  $B$  está contenido en el complemento  $A'$  de  $A$ :

$$\overbrace{\begin{array}{ccccccccc} 1 & 2 & 3 & & & b & b+1 \\ & & & & & \hline & & & & & B & \end{array}} \quad (* \text{ elementos de } A).$$

Ahora bien, tenemos que:

i)  $1 \in B$ . En efecto,  $1 \notin A$  pues de lo contrario en  $A$  habría un elemento, el 1, menor que todos los demás de  $A$ . Además 1 es menor que todos los demás naturales, 1 es menor que todos los elementos de  $A$ . Luego  $1 \in B$ .

ii) Supongamos que  $b \in B$  (es decir  $b < a$  para toda  $a$  en  $A$ ). Entonces  $b + 1 \in B$  también. En efecto, si  $b + 1 \notin B$ ,  $b + 1 \geq a$  para cierta  $a \in A$ . Y como  $b < a$ ,  $b + 1 \leq a$ , de donde  $b + 1 = a \in A$ . Entonces  $b + 1$  sería un elemento de  $A$  menor que todos los demás de  $A$ , contra lo supuesto.

Por lo anterior, según el principio de inducción,  $B = \mathbb{N}$  y como  $B \subset A'$ , resulta que  $A' = \mathbb{N}$ , de donde  $A = \emptyset$ , contra la hipótesis, con lo que queda demostrada la proposición.

**PROPOSICIÓN 2:** *El principio del buen orden implica el principio de inducción.*

*Demostración.* Sea  $M$  un subconjunto de  $\mathbb{N}$  tal que  $1 \in M$  y si  $n \in M$  entonces  $n + 1 \in M$ . Suponiendo el principio del buen orden demostraremos que  $M = \mathbb{N}$ . Sea  $M'$  el complemento de  $M$  en  $\mathbb{N}$ . Si  $M'$  es no vacío,  $M'$  tiene un elemento mínimo  $m'$ . Por consiguiente ya que  $m' - 1 < m'$ ,  $m' - 1 \notin M'$ , es decir,  $m' - 1 \in M$ . Pero por hipótesis  $(m' - 1) + 1$  pertenece también a  $M$ , es decir,  $m' \in M$ , lo cual es una contradicción. Luego  $M' = \emptyset$  y  $M = \mathbb{N}$ .

# 7

CAPÍTULO

## Divisibilidad

### 1. DEFINICIONES Y PROPIEDADES ELEMENTALES

Hasta aquí hemos estudiado propiedades simples de los números enteros. Ahora analizaremos propiedades relativas a la divisibilidad, cuyo estudio es parte de una rama de las matemáticas llamada Teoría de los números.

Recordemos primero que si consideramos a los enteros como parte de los números racionales, al formar el cociente  $\frac{a}{b}$  de dos enteros  $a$  y  $b$ , con  $b \neq 0$ , este cociente no es necesariamente un número entero. Por ejemplo, si  $a = 5$ ,  $b = 7$ ,  $\frac{a}{b} = \frac{5}{7}$  que no es un entero. En otros casos este cociente sí es un número entero; por ejemplo, si  $a = 12$ ,  $b = 6$ ,  $\frac{a}{b} = \frac{12}{6} = 2$ . Cuando el cociente de dos enteros  $a$  y  $b$  ( $b \neq 0$ ) es número entero decimos que  $b$  divide a  $a$ .

Es conveniente, sin embargo, tener una definición intrínseca de divisibilidad, en la que no se haga referencia al concepto de cociente.

Para ello expresamos la definición anterior en la forma siguiente:

**DEFINICIÓN:** *Si  $a$  y  $b$  son números enteros, decimos que  $b$  divide a  $a$  si existe un entero  $q$  tal que  $a = bq$ .*

Es claro que si suponemos que  $b \neq 0$ , esta definición es equivalente a la mencionada anteriormente.

Otras formas de expresar que " $b$  divide a  $a$ " son:

- " $b$  es un divisor de  $a$ "
- " $b$  es un factor de  $a$ "
- " $a$  es un múltiplo de  $b$ "
- " $a$  es divisible entre  $b$ ".

**Notación.** Para expresar que  $b$  divide a  $a$  utilizamos la notación

$$b | a$$

y  $b \nmid a$  significa que  $b$  no divide a  $a$ .

Demostraremos a continuación algunas de las propiedades elementales de la divisibilidad.

En lo sucesivo, aunque no se haga mención explícita, se supondrá que las letras que usamos para representar números denotan siempre números enteros.

**PROPOSICIÓN 1 (propiedad reflexiva):** Para todo número entero  $a$ , se tiene que  $a$  divide a  $a$ .

Esto es claro, pues

$$a = a1.$$

**PROPOSICIÓN 2 (propiedad transitiva):** Si  $a$ ,  $b$  y  $c$  son números enteros tales que  $a$  divide a  $b$  y  $b$  divide a  $c$ , entonces  $a$  divide a  $c$ .

*Demostración.* De la definición de divisibilidad y de las hipótesis se sigue que existen enteros  $q$  y  $r$  tales que

$$b = aq, \quad c = br;$$

por lo tanto,

$$c = (aq)r = a(qr),$$

lo que indica que  $a$  divide a  $c$ .

En la primera parte vimos que las unidades del anillo de los enteros son 1,  $-1$ . Al estudiar la divisibilidad entre enteros veremos que ésta se preserva al multiplicar estos por unidades. Más precisamente:

**PROPOSICIÓN 3:** Si  $a$  y  $b$  son números enteros y  $u$ ,  $u'$  son unidades, entonces las dos condiciones siguientes son equivalentes:

- i)  $a$  divide a  $b$ ;
- ii)  $ua$  divide a  $u'b$ .

*Demostración.* Veamos primero que i) implica ii). Supongamos, pues, que

$$b = aq;$$

ahora bien, ya que  $u$  es unidad, existe  $u_1$  tal que  $uu_1 = 1$ ; por consiguiente,

$$b = (uu_1)b = (uu_1)aq = ua(u_1q),$$

lo que prueba que  $ua \mid b$ . Pero claramente  $b \mid u'b$ ; por consiguiente, por la transitividad tenemos  $ua \mid u'b$ .

Veamos ahora que ii) implica i). En este caso tenemos

$$u'b = uar;$$

pero como  $u'$  es unidad, existe  $u'_1$  tal que  $u'_1u' = 1$ ; por consiguiente,

$$b = (u'_1u')b = u'_1(uar) = a(u'_1ur)$$

lo que prueba que  $a \mid b$ .

Ahora bien, ya que las unidades de los enteros son 1, -1 la proposición anterior nos indica que al considerar la divisibilidad en los números enteros basta referirse a los enteros no negativos.

Como consecuencia de la proposición anterior tenemos el siguiente  
**COROLARIO:** *Si  $a$  y  $b$  son enteros, las condiciones siguientes son equivalentes:*

- i)  $a$  divide a  $b$ ;
- ii)  $|a|$  divide a  $|b|$ .

Esto es claro, pues si  $a$  es un entero  $|a| = ua$  en donde  $u$  es una unidad.

Otra proposición relativa a la divisibilidad y las unidades es:

**PROPOSICIÓN 4 (propiedad de simetría):** *Si  $a$  y  $b$  son dos enteros distintos de cero tales que  $a \mid b$  y  $b \mid a$  entonces  $a = bu$  en donde  $u$  es una unidad.*  
**Demostración.** Por hipótesis,

$$b = ar, \quad a = bq;$$

por consiguiente,

$$a = (ar)q = arq.$$

Ya que  $a \neq 0$ , cancelando obtenemos

$$1 = rq,$$

lo que prueba que  $q$  es unidad.

Otros resultados simples relativos a la divisibilidad aparecen en los siguientes:

## EJERCICIOS

1. Demuéstrese que todo número entero divide a cero.
2. Demuéstrese que si 0 es divisor de  $a$ , entonces  $a = 0$ .
3. Demuéstrese que las unidades de  $\mathbb{Z}$ , es decir 1, -1, son divisores de cualquier entero.
4. Demuéstrese que si  $u$  es un entero que divide a todos los enteros, entonces  $u$  es una unidad.
5. Demuéstrese que las condiciones siguientes son equivalentes:

- i)  $a$  divide a  $b$ ;
- ii)  $-a$  divide a  $b$ ;
- iii)  $a$  divide a  $-b$ ;
- iv)  $-a$  divide a  $-b$ .

Daremos ahora una propiedad que relaciona el orden y la divisibilidad en  $\mathbb{Z}$ .

**PROPOSICIÓN 5:** Si  $a$  y  $b \neq 0$  son enteros y  $a | b$  entonces  $|a| \leq |b|$ .

*Demuestração.* Por el corolario de la proposición 3 tenemos que  $|a| | |b|$ , es decir,  $|b| = |a|q$ , con  $q \geq 1$ . Si  $q = 1$ ,  $|b| = |a|$ . Si  $q \neq 1$ ,  $q = 1 + q'$  con  $q'$  positivo. Por lo tanto,

$$|b| = |a|(1 + q') = |a| + |a|q',$$

de donde

$$|b| - |a| = |a|q' \geq 1,$$

es decir,  $|b| > |a|$ .

Trataremos ahora algunas propiedades que relacionan la divisibilidad con las operaciones en  $\mathbb{Z}$ .

**PROPOSICIÓN 6:** Si  $a | b$  y  $a | c$  entonces  $a | (b + c)$ .

*Demuestração.* Las hipótesis implican que

$$b = aq, \quad c = ar.$$

Por lo tanto,

$$b + c = aq + ar = a(q + r),$$

es decir,  $a$  divide a  $b + c$ .

**PROPOSICIÓN 7:** Si  $a | b$  y  $c$  es un entero arbitrario, entonces  $a | bc$ .

En efecto, ya que

$$b = aq,$$

se tiene que

$$bc = a(qc).$$

Como consecuencia de las dos proposiciones anteriores tenemos el siguiente:

**COROLARIO:** Si  $a$ ,  $b$  y  $c$  son enteros tales que  $c \mid a$  y  $c \mid b$ , entonces

$$c \mid ar + bs$$

para enteros arbitrarios  $r$  y  $s$ .

Cuando se tienen, como en el corolario anterior, dos números  $a$  y  $b$ , a los enteros de la forma

$$ar + bs$$

con  $r$  y  $s$  enteros, se les llama *combinaciones lineales de  $a$  y  $b$* .

Utilizando esta nomenclatura tenemos el siguiente

**COROLARIO:** Un entero  $c$  divide a los enteros  $a$  y  $b$  si y solo si  $c$  divide a cualquier combinación lineal de  $a$  y  $b$ .

**Demostración.** El corolario anterior asegura que si  $c$  divide a  $a$  y  $b$ , entonces  $c$  divide a cualquier combinación lineal de  $a$  y  $b$ .

Inversamente, ya que  $a = a_1 + b_0$  y  $b = a_0 + b_1$ ,  $a$  y  $b$  son combinaciones lineales de  $a_1$  y  $b_0$ ; por lo tanto si  $c$  divide a cualquier combinación lineal de  $a$  y  $b$ ,  $c \mid a$  y  $c \mid b$ .

Es claro que, en general, dados dos enteros, no cualquier otro entero es combinación lineal de ellos. Por ejemplo, 6 no es combinación lineal de 15 y 20, pues si

$$6 = 15r + 20s,$$

ya que  $5 \mid 15$  y  $5 \mid 20$  se tendría que  $5 \mid 6$ , lo cual es falso.

El corolario anterior asegura que una condición necesaria para que un número  $g$  sea combinación lineal de  $a$  y  $b$  es que  $g$  sea divisible entre todo divisor común de  $a$  y  $b$ .

Dicho de otra manera, si hay un número  $e$  tal que  $e \mid a$  y  $e \mid b$  pero  $e \nmid g$ , entonces  $g$  no es combinación lineal de  $a$  y  $b$ .

## EJERCICIOS

6. Pruébese que 52 no es combinación lineal de 20 y 15.
7. Encuéntrese un número que no sea combinación lineal de 30 y 70.
8. Pruébese que si  $c$  es un entero impar, entonces  $c$  no es combinación lineal de 98 y 102.
9. Pruébese que si  $c = 3n \pm 1$  ( $n$  entero), entonces  $c$  no es combinación lineal de 45 y 1 251.
10. Pruébese que si  $c = 30n + 6$  ( $n$  entero), entonces  $c$  no es combinación lineal de 1 020 y 210.
11. Pruébese que si  $c$  es combinación lineal de  $a$  y  $b$ , entonces  $rc$  lo es también.
12. Pruébese que si  $d$  es combinación lineal de  $a$  y  $b$ , y  $b$  es combinación lineal de  $a$  y  $c$ , entonces  $d$  es combinación lineal de  $a$  y  $c$ .

Cuando se tiene una sucesión de enteros,  $b_1, b_2, \dots, b_n$ , a los enteros de la forma

$$c_1b_1 + c_2b_2 + \dots + c_nb_n$$

con  $c_1, c_2, \dots, c_n$  enteros, se les llama *combinaciones lineales* de  $b_1, b_2, \dots, b_n$ . Obsérvese que cada uno de los enteros  $b_i$  es combinación lineal de  $b_1, b_2, \dots, b_n$ . Por ejemplo,

$$b_1 = 1b_1 + 0b_2 + \dots + 0b_n.$$

### EJERCICIO

13. Demuéstrese que si  $a$  divide a los enteros  $b_1, b_2, \dots, b_n$  entonces  $a$  divide a cualquier combinación lineal de  $b_1, b_2, \dots, b_n$  e inversamente.

## 2. EL ALGORITMO DE LA DIVISIÓN

Dados dos números enteros  $a$  y  $b \neq 0$ , no siempre  $a$  es divisible entre  $b$ , es decir, no siempre existe otro entero  $q$  tal que  $a = bq$ . Sin embargo, en todos los casos podemos “dividir”  $a$  entre  $b$  y obtener un cociente y un residuo. Este proceso ya lo conocemos desde la enseñanza elemental. Aquí lo precisaremos y daremos una demostración.

**TEOREMA 1:** *Si  $a$  y  $b$  son enteros y  $b \neq 0$ , existen dos enteros  $q$  y  $r$ , únicos, tales que*

$$a = bq + r, \text{ con } 0 \leq r < |b|.$$

*Demostración.* Haremos primero la demostración para el caso  $a > 0$ ,  $b > 0$ .

Consideraremos el conjunto de números enteros *no negativos* que sean de la forma

$$a - bs$$

con  $s$  entero. Este conjunto, según las hipótesis hechas, no es vacío, pues  $a - b \cdot 0 > 0$ .

Por el principio del buen orden dicho conjunto tiene un elemento menor que todos los demás. Sea

$$r = a - bq \geq 0$$

dicho elemento. De aquí obtenemos que

$$a = bq + r,$$

y lo único que resta por demostrar es que  $r < |b| = b$ . Si  $r \geq b$ , ya que  $r = a - bq$  obtenemos

$$r - b = a - b(q + 1)$$

y puesto que  $r - b \geq 0$ , resulta que

$$a - b(q + 1) \geq 0,$$

lo cual contradice que  $r = a - bq$  es menor que todas las expresiones no negativas de la forma  $a - bs$ , pues

$$a - b(q + 1) = r - b < r = a - bq$$

con lo cual queda terminada la demostración de este caso.

Si  $a > 0$  y  $a < b$ , la expresión

$$a = b \cdot 0 + a$$

demuestra el teorema en este caso, pues  $a < |b| = b$ .

Los casos en que  $a$  o  $b$  o ambos sean negativos se deducen muy fácilmente de los casos anteriores como se verá en los ejemplos que siguen y en los ejercicios.

Por lo tanto nos ocuparemos solamente de demostrar la unicidad de  $q$  y  $r$ .

Supongamos que

$$\begin{aligned} a &= bq + r \quad \text{con} \quad 0 \leq r < |b| \\ a &= bq' + r' \quad \text{con} \quad 0 \leq r' < |b|. \end{aligned}$$

Obtenemos

$$b(q - q') = (r' - r),$$

de donde

$$|b| |q - q'| = |r - r'|.$$

Pero  $|r - r'| < |b|$ , de donde la igualdad anterior implica (prop. 5)

$$|b| |q - q'| = 0 \quad \text{y} \quad |r - r'| = 0.$$

Como  $|b| \neq 0$ , de aquí obtenemos

$$q = q' \quad \text{y} \quad r = r'.$$

En los siguientes ejemplos veremos cómo pueden tratarse los casos en que  $a$  o  $b$  sean negativos.

Supongamos primero que, por ejemplo,  $a = 436$ ,  $b = 17$ . Tenemos que

$$436 = 17 \times 25 + 11,$$

es decir, en este caso  $q = 25$  y  $0 \leq r = 11 < |17| = 17$ .

Si tuviéramos  $a = -436$ ,  $b = -17$  podríamos aprovechar la igualdad anterior y escribir

$$-436 = (-17) \times 25 - 11.$$

Pero  $-11$  no sirve como residuo, pues es negativo. Luego,

$$-436 = (-17) \times 25 - 17 + 17 - 11$$

$$-436 = (-17) \times 26 + 6.$$

O sea,  $q = 26$  y  $0 \leq r = 6 < |-17| = 17$ .

En el caso  $a = -436$ ,  $b = 17$  podemos, en forma análoga, escribir

$$-436 = 17 \times (-25) - 11 = 17 \times (-25) + 17 \times (-1) + 17 - 11$$

$$-436 = 17 \times (-26) + 6,$$

o sea,  $q = -26$ ,  $0 \leq r = 6 < |-17| = 17$ .

Finalmente, en el caso  $a = 436$ ,  $b = -17$ , vemos que

$$436 = (-17) \times (-25) + 11,$$

o sea,  $q = -25$ ,  $r = 11$ .

## EJERCICIOS

**1.** Encuéntrense  $q$  y  $r$  para las siguientes parejas de números  $a$ ,  $b$ :

- |                         |  |
|-------------------------|--|
| a) $a = 0$ , $b = -3$   | f) $a = -59$ , $b = -12$                                   |
| b) $a = 12$ , $b = 59$  | g) $a = 8611$ , $b = -37$                                  |
| c) $a = 59$ , $b = 12$  | h) $a = -8611$ , $b = -37$                                 |
| d) $a = -59$ , $b = 12$ | i) $a = -37$ , $b = 8611$                                  |
| e) $a = 59$ , $b = -12$ | j) $a = p^3 + 2p^2 + 2p + 2$ ,<br>$b = p + 1$ ( $p > 0$ ). |

**2.** Siguiendo el ejemplo del texto, termínese la demostración del teorema, considerando los casos

- i)  $a < 0$ ,  $b < 0$ ; ii)  $a < 0$ ,  $b > 0$ ; iii)  $a > 0$ ,  $b < 0$ .

Observemos finalmente que este proceso nos permite encontrar *todos* los divisores de un número dado. En efecto, para encontrar todos los divisores de un número  $a \neq 0$ , basta encontrar todos los divisores positivos de  $|a|$ .

Ahora bien, como cualquier divisor positivo de  $|a|$  es menor que  $|a|$  y solamente hay un número finito de enteros positivos menores que  $|a|$ , en un número finito de pasos se pueden encontrar todos los divisores positivos de  $|a|$  y por lo dicho antes, de todos los divisores de  $a$ . (Claro está que éste no es el método conveniente de hacerlo. Esto simplemente demuestra que *se puede* hacer.)

**OBSERVACIÓN:** Para una mayor comprensión hemos demostrado la proposición anterior en el caso en que  $a$  y  $b$  son positivos y después hemos visto, con ejemplos, cómo puede adaptarse al caso general. Sin embargo, utilizando la misma idea es posible hacer una demostración que abarque todos los casos. La única dificultad que se presenta es demostrar que el conjunto de todos los enteros no negativos de la forma  $a - bq$  es no vacío. Esto se puede analizar considerando los distintos casos  $a$  y  $b$ .

### 3. EL MÁXIMO COMÚN DIVISOR

Ya hemos visto que el conjunto de divisores de cualquier número entero es finito. Por lo tanto, dados dos números enteros  $a$  y  $b$ , el conjunto de divisores comunes de  $a$  y  $b$  es también un conjunto finito pues éste es la intersección del conjunto de divisores de  $a$  con el conjunto de divisores de  $b$ . Por consiguiente, podemos hablar del máximo de los divisores comunes de  $a$  y  $b$ . Al mcd de  $a$  y  $b$  lo denotaremos  $(a, b)$ .

Por ejemplo, el conjunto de divisores comunes de 24 y 18 es

$$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\} \cap \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9\} = \\ = \{\pm 1, \pm 2, \pm 3, \pm 6\},$$

por lo que el mcd de 24 y 18 es

$$(24, 18) = 6.$$

#### EJERCICIOS

**1.** Demuéstrese que

- a)*  $(a, 0) = a$  [en particular  $(0, 0) = 0$ ].
- b)*  $(a, b) = 0$  implica  $a = 0$  y  $b = 0$ .

**2.** Demuéstrese que si  $a$  y  $b$  son enteros, su máximo común divisor es igual al máximo común divisor de sus valores absolutos  $|a|$  y  $|b|$ . En símbolos,

$$(a, b) = (|a|, |b|).$$

Debido a lo anterior, al hablar del mcd de dos números  $a$  y  $b$  nos podremos restringir al caso  $a > 0$  y  $b > 0$ .

Con objeto de caracterizar de otra manera el mcd de dos enteros veremos cómo se relaciona este concepto con el de combinación lineal de dichos enteros.

Recordemos que las combinaciones lineales de dos enteros  $a$  y  $b$  son los números  $c$  que se pueden expresar en la forma

$$c = ar + bs$$

con  $r$  y  $s$  enteros.

En la sección anterior vimos que una condición necesaria para que un número  $c$  sea combinación lineal de  $a$  y  $b$  es que  $c$  sea divisible entre cualquier divisor común de  $a$  y  $b$ ; en particular, entre el mcd de  $a$  y  $b$ . El corolario 2 de la siguiente proposición demostrará que esta condición es también suficiente.

**PROPOSICIÓN 1:** *Si  $a$  y  $b$  son enteros positivos y  $d = as + bt$  es su combinación lineal positiva mínima, entonces todo divisor de  $d$  es divisor también de  $a$  y  $b$ .*

*Demostración.* Por la transitividad de la divisibilidad basta demostrar que  $d \mid a$  y  $d \mid b$ .

Según el algoritmo de la división, tenemos:

$$a = dq + r \quad \text{con} \quad 0 \leq r < d.$$

Pero ya que  $d = as + bt$ , obtenemos  $a = (as + bt)q + r$ , de donde se ve que  $r$  es combinación lineal de  $a$  y  $b$ :

$$r = a(1 - sq) - btq.$$

Pero como  $0 \leq r < d$  y  $d$  es la combinación lineal *positiva mínima* de  $a$  y  $b$ , resulta que  $r = 0$ , es decir, que  $d \mid a$ .

En forma semejante se prueba que  $d \mid b$ .

**COROLARIO 1:** *El mcd de dos enteros  $a$  y  $b$  es la combinación lineal positiva mínima de  $a$  y  $b$ .*

*Demostración.* Sea  $d' = (a, b)$  el mcd de  $a$  y  $b$  y  $d = as + bt$  la combinación lineal mínima de  $a$  y  $b$ . Por la proposición 1,  $d$  es un divisor común de  $a$  y  $b$  y como  $d'$  es el mcd, resulta que  $d \leq d'$ . Ahora bien, como  $d' \mid a$  y  $d' \mid b$  entonces  $d' \mid d$  por ser  $d$  combinación lineal de  $a$  y  $b$ . Por lo tanto,  $d' \leq d$ . Las dos desigualdades implican que  $d = d'$ .

**COROLARIO 2:** *Un entero  $c$  es combinación lineal de  $a$  y  $b$  si y solo si el mcd ( $d$ ) de  $a$  y  $b$ , divide a  $c$ .*

*Demostración.* Sabemos que si  $c = am + bn$ ,  $d \mid c$ . Inversamente, por el corolario anterior el mcd de  $a$  y  $b$  es combinación lineal de  $a$  y  $b$ :  $d = as + bt$ . Si  $d \mid c$ ,  $c = dk$ , de donde  $c = ask + btk$ .

Lo anterior permite dar varias definiciones equivalentes de mcd.

**TEOREMA 1:** *Si  $a, b$  y  $d > 0$  son enteros, las cuatro condiciones siguientes son equivalentes:*

- i)  $d = (a, b)$
- ii)  $d = as + bt$  es la combinación lineal positiva mínima de  $a$  y  $b$ .
- iii)  $d \mid a$ ,  $d \mid b$ , y si  $c \mid a$  y  $c \mid b$ , entonces  $c \mid d$ .
- iv)  $d \mid a$ ,  $d \mid b$ , y  $d$  es combinación lineal de  $a$  y  $b$ .

*Demostración.* El corolario 1 de la proposición 1 asegura que (i) y (ii) son equivalentes.

Demostraremos ahora que (i) y (iii) son equivalentes. Sea  $d' = (a, b)$  y  $d$  entero que satisface la condición (iii). Como  $d$  es divisor común y  $d'$  el máximo común divisor tenemos que  $d \leq d'$ . Además, como  $d' \mid a$  y  $d' \mid b$ , por (iii)  $d' \mid d$  y como  $d > 0$ ,  $d' \leq d$ . Las dos desigualdades muestran que  $d = d'$ .

## EJERCICIO

3. Demuéstrese que (iv) es equivalente a la condición (ii).

Con esto queda probado el teorema.

Conviene observar que las definiciones de mcd dadas por las condiciones (iii) y (iv) no utilizan el concepto de orden en  $\mathbb{Z}$ . Por ello estas definiciones serán útiles en aquellas generalizaciones del concepto de mcd a anillos en los que no se tenga el concepto de orden.

Cuando los únicos divisores comunes de dos números  $a$  y  $b$  son 1 y  $-1$ , los números se llaman primos entre sí. Es decir,

**DEFINICIÓN:** *Se dice que dos enteros  $a$  y  $b$  son primos entre sí (o primos relativos) si su máximo común divisor es 1.*

Como 1 es el menor entero positivo, resulta que

**PROPOSICIÓN 2:**  *$a$  y  $b$  son primos entre sí, si y solo si,*

$$1 = as + bt.$$

Mencionaremos ahora algunos resultados relativos a números primos entre sí.

Observemos primero que cuando un número  $a$  divide a un producto  $bc$ , no necesariamente  $a$  divide a alguno de los factores. Por ejemplo,  $8 \mid 6 \times 12$  y sin embargo  $8 \nmid 6$  y  $8 \nmid 12$ . Pero en el caso en que  $a$  y  $b$  sean primos relativos tenemos que:

**PROPOSICIÓN 3:** Si  $a \mid bc$  y  $(a, b) = 1$  entonces  $a \mid c$ .

*Demostración.* Por hipótesis,

$$1 = as + bt,$$

de donde,

$$c = asc + bct.$$

Ahora bien, como  $a \mid a$  y  $a \mid bc$  (hipótesis),  $a$  divide a la combinación lineal  $a(sc) + (bc)t = c$ , lo que prueba la proposición.

En los ejercicios siguientes, supondremos  $a \neq 0$ ,  $b \neq 0$ .

## EJERCICIOS

4. Pruébese que si  $d = (a, b)$  y  $d = ar + bs$ , entonces  $r$  y  $s$  son primos entre sí.
5. Si  $d = (a, b)$  y  $a = a'd$ ,  $b = b'd$  pruébese que  $a'$  y  $b'$  son primos entre sí.
6. Pruébese que si  $c \mid a$  y  $(a, b) = 1$  entonces  $(b, c) = 1$ .
7. Si  $d \mid a$ ,  $d \mid bc$  y  $(a, b) = 1$  pruébese que  $d \mid c$ .
8. Si  $a$  y  $b$  son primos entre sí, pruébese que el mcd de  $a$  y  $bc$  es igual al mcd de  $a$  y  $c$ . (Pruébese que el conjunto de los divisores comunes de  $a$  y  $bc$  es el mismo que el conjunto de divisores comunes de  $a$  y  $c$ . Úsese el ejercicio 7.)

Los conceptos y resultados anteriores permiten encontrar soluciones enteras de ciertas ecuaciones lineales.

**PROPOSICIÓN 4:** Las soluciones enteras de la ecuación

$$ax + by = 0 \text{ con } (a, b) = 1 \text{ y } a, b \neq 0$$

son  $x = -bt$ ,  $y = at$  con  $t$  entero arbitrario.

*Demostración.* Evidentemente  $x = -bt$ ,  $y = at$  es solución, cualquiera que sea el entero  $t$ . Queda solamente probar que toda solución es de esta forma. En efecto, si  $(x, y)$  es una solución de la ecuación  $ax + by = 0$ , tenemos que  $ax = -by$ , de donde,  $a \mid by$ . Como  $(a, b) = 1$ , por la proposición anterior tenemos que  $a \mid y$ , por lo que  $y = at$  para cierto entero  $t$ . Por consiguiente,  $ax = -bat$ , de donde  $x = -bt$ .

Sean  $a$  y  $b$  dos enteros distintos de cero. El conjunto de múltiplos comunes positivos de  $a$  y  $b$  no es vacío pues, por ejemplo, el producto  $|ab|$  es un

múltiplo común positivo. Por el axioma del buen orden este conjunto tiene un elemento mínimo, el cual se llama el mínimo común múltiplo de  $a$  y  $b$ . Lo denotaremos con  $[a, b]$ .

Por ejemplo, si  $a = 6$ ,  $b = 10$ , los múltiplos comunes positivos de 6 y 10 son

$$\begin{aligned} \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, \dots\} \cap \\ \cap \{10, 20, 30, 40, 50, 60, 70, \dots\} = \\ = \{30, 60, 90, \dots\}, \end{aligned}$$

por lo que el mínimo común múltiplo es

$$[6, 10] = 30.$$

**PROPOSICIÓN 5:** Sean  $a$  y  $b$  enteros distintos de cero. El mcm,  $m = [a, b]$  divide a cualquier múltiplo común de  $a$  y  $b$ . Inversamente si  $m' > 0$  es un múltiplo común de  $a$  y  $b$  que divide a todos los múltiplos comunes de  $a$  y  $b$  entonces  $m' = m$ .

En otras palabras, el mcm de  $a$  y  $b$  queda caracterizado como aquel entero positivo  $m'$  tal que:

- i)  $a \mid m'$ ,  $b \mid m'$ ;
- ii) si  $a \mid m''$  y  $b \mid m''$  entonces  $m' \mid m''$ .

*Demostración.* Sea  $m''$  un múltiplo común de  $a$  y  $b$ . Por el algoritmo de la división,

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

Como  $a \mid m''$  y  $a \mid m$  entonces  $a \mid r$ . Análogamente,  $b \mid r$ . Por lo tanto  $r$  es un múltiplo común no negativo de  $a$  y  $b$  y si  $r$  fuera distinto de cero se tendría que  $m \leq r$  lo cual es falso. Por tanto  $r = 0$ . Es decir,  $m$  divide a cualquier múltiplo común.

## EJERCICIO

9. Pruébese la segunda parte de la proposición 5.

Si  $a = 12$  y  $b = 8$  entonces  $(a, b) = 4$  y  $[a, b] = 24$ . Tenemos que  $12 \times 8 = 4 \times 24$ , o sea, en este ejemplo,  $ab = (a, b)[a, b]$ . Esto es cierto en general.

**PROPOSICIÓN 6:** Si  $a$  y  $b$  son enteros positivos entonces su producto  $ab$  es igual al producto de su mcd y mcm. En símbolos,

$$ab = (a, b)[a, b].$$

*Demostración.* Sea  $m = [a, b]$ . Entonces, como  $ab$  es un múltiplo común,  $m \mid ab$ . Sea  $d$  tal que

$$md = ab.$$

i) Demostraremos primero que  $d$  es un divisor común de  $a$  y  $b$ . Ya que  $m$  es múltiplo común, tenemos que

$$m = ar = bs,$$

de donde,

$$md = ard = bsd = ab.$$

Por lo tanto, como  $a \neq 0$  y  $b \neq 0$  obtenemos

$$rd = b, \quad sd = a,$$

lo cual prueba (i).

ii) Veremos ahora que  $d$  es divisible entre cualquier divisor común de  $a$  y  $b$ .

Sea  $d'$  tal que  $d' \mid a$  y  $d' \mid b$ . Entonces

$$a = d'a', \quad b = d'b'.$$

Tenemos que el entero  $m'$  definido como sigue

$$m' = a'b'd' = ab' = ba'$$

es un múltiplo común de  $a$  y  $b$ . Por lo tanto  $m' = mt$ . Entonces

$$mtd' = m'd' = a'd'b'd' = md$$

y como  $m \neq 0$ ,  $td' = d$ , es decir,  $d' \mid d$ .

Las condiciones (i) y (ii) implican (véase el teorema 1) que  $d = (a, b)$ . Por lo tanto  $ab = (a, b) [a, b]$ .

## EJERCICIOS

**10.** Pruébese que el mcm de dos números primos entre sí es igual a su producto.

Los dos siguientes ejercicios nos dan otra demostración de la proposición:

**11.** Si  $a$  y  $b$  son primos entre sí y  $a \mid c$  y  $b \mid c$ , entonces  $ab \mid c$ .

**12.** Sea  $d = (a, b)$  y  $a = a'd$ ,  $b = b'd$ . Si  $a \mid c$  y  $b \mid c$  pruébese que  $a'b'd \mid c$ . (Utilícese el ejercicio anterior.)

**13.** Utilizando los dos ejercicios anteriores dése una nueva demostración de la proposición 6.

14. Si  $k > 0$  demuéstrese que

$$\begin{aligned}(ka, kb) &= k(a, b) \\ [ka, kb] &= k[a, b].\end{aligned}$$

Los conceptos de mcd y mcm se pueden extender a conjuntos de más de dos enteros. Por ejemplo, el mcm  $(a_1, a_2, \dots, a_n)$  de los enteros  $a_1, a_2, \dots, a_n$  es la intersección de los conjuntos de divisores de cada uno de los enteros  $a_i$ .

15. Si  $a_1, a_2, \dots, a_n$  son enteros y  $d_i = (a_1, a_2, \dots, a_n)$  para  $2 \leq i \leq n$ , demuéstrese que

$$d_i = (d_{i-1}, a_i).$$

16. Pruébese la afirmación análoga a la del ejercicio anterior para el mcm para enteros  $a_1, a_2, \dots, a_n$  distintos de cero.

#### 4. EL ALGORITMO DE EUCLIDES Y ECUACIONES DIOFANTINAS

En el párrafo anterior definimos el mcd de dos números. Veremos ahora un procedimiento, llamado algoritmo de Euclides que permite calcularlo.

Sean  $a, b$  dos enteros que supondremos positivos y tales que  $a$  no sea múltiplo de  $b$ . Podemos aplicar iteradamente el algoritmo de la división en la forma siguiente:

$$\begin{aligned}a &= bq + r_1, & 0 < r_1 < b \\ b &= r_1 q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2 \\ \dots && \dots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n.\end{aligned}$$

Ya que  $0 < r_n < r_{n-1} < \dots < r_2 < r_1 < b$  es claro que después de aplicar el algoritmo de la división un número finito de veces obtenemos un residuo cero (como lo indica  $r_{n-1} = r_n q_n$ ).

Este proceso es el llamado *algoritmo de Euclides*.

**PROPOSICIÓN 1:** Si  $a, b$  son enteros positivos y  $b \nmid a$ , entonces el último residuo distinto de cero en el algoritmo de Euclides es el mcd de  $a$  y  $b$ . Con la notación anterior tenemos

$$r_n = (a, b).$$

Para la demostración de esto basta aplicar el siguiente lema a cada uno de los pasos del proceso.

**LEMA 1:** Si  $a = bq + r$ , entonces  $(a, b) = (b, r)$ .

## EJERCICIO

1. Pruébese el lema anterior.

**SUGERENCIA:** Demuéstrese que el conjunto de divisores comunes de  $a$  y  $b$  es el mismo que el conjunto de divisores comunes de  $b$  y  $r$ .

### Ejemplo:

Calculemos el mcd de 60 y 42:

$$\begin{aligned} 60 &= 42 \times 1 + 18 \\ 42 &= 18 \times 2 + 6 \\ 18 &= 6 \times 3 \end{aligned}$$

Por lo tanto,  $(60, 42) = 6$ .

## EJERCICIOS

2. Aplicando el algoritmo de Euclides encuéntrese el mcd de las siguientes parejas de números:

- a) 329, 1 005;
- b) 1 302, 1 224;
- c) 1 816, -1 789;
- d) -666, -12 309.

3. Encuéntrese el mcd de los siguientes conjuntos de enteros:

- a) 2 784, 4 988, 8 444;
- b) 103 224, 31 416, 3 432, 840.

(Recuérdese lo demostrado en el ejercicio 16 del párrafo 3.)

El algoritmo de Euclides no sólo permite calcular el mcd de dos números enteros sino también nos da un procedimiento para expresar este como combinación lineal de ellos. Esto es consecuencia de un resultado demostrado anteriormente en un ejercicio y que aquí enunciamos nuevamente:

**LEMA 2:** Si  $c$  es combinación lineal de  $a$  y  $b$  y  $c'$  es combinación lineal de  $c$  y  $b$ , entonces  $c'$  es combinación lineal de  $a$  y  $b$ .

Veamos un ejemplo; supongamos que  $a$  y  $b$  son tales que

$$\begin{aligned} a &= bq + r_1, & 0 < r_1 < b \\ b &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_2. \end{aligned}$$

tenemos que

$$\begin{aligned} r_2 &= b - r_1q_1 \\ r_1q_1 &= aq_1 - bqq_1, \end{aligned}$$

de donde,

$$\begin{aligned} r_2 &= b - (aq_1 - bq_1) = \\ &= a(-q_1) + b(1 + qq_1), \end{aligned}$$

que expresa  $r_2$  como combinación lineal de  $a$  y  $b$ .

### EJERCICIOS

4. Utilizando el algoritmo de Euclides exprésese el mcd como combinación lineal:

- a) 228, 348;
- b) 15, 21;
- c)  $2n + 1, 4n$ ;
- d)  $4n^2 + 2n - 40, 2n + 7$ .

Los resultados de divisibilidad que hemos visto, pueden aplicarse para encontrar las soluciones en números enteros de ecuaciones como

$$ax + by = c$$

en donde  $a$ ,  $b$  y  $c$  son números enteros. A este tipo de ecuaciones se les llama ecuaciones diofantinas.

El corolario 2 de la proposición 1 del párrafo anterior podemos enunciarlo también como sigue:

**PROPOSICIÓN 2:** Una condición necesaria y suficiente para que la ecuación

$$ax + by = c \quad (a, b, c \text{ enteros})$$

tenga solución en enteros es que el máximo común divisor de  $a$  y  $b$  divide a  $c$ .

### EJERCICIOS

5. Determínense cuáles de las siguientes ecuaciones tienen solución en enteros:

- a)  $35x + 17y = 14$ ;
- b)  $1\,242x + 1\,476y = 49$ ;
- c)  $15x + 21y = 10$ .

El algoritmo de Euclides que permite expresar el mcd de dos números como combinación lineal de estos nos da un procedimiento para encontrar soluciones a ecuaciones diofantinas.

En efecto, consideremos la ecuación

$$ax + by = c \quad (a, b, c \text{ enteros}),$$

sea  $d = (a, b)$  y supongamos que  $d \mid c$ . Aplicando el algoritmo de Euclides podemos escribir

$$ar + bs = d.$$

Sea  $c = dc'$ ; entonces

$$arc' + bsc' = dc' = c$$

por consiguiente

$$x_0 = rc', \quad y_0 = sc'$$

es una solución de la ecuación.

### EJERCICIOS

6. Aplicando el algoritmo de Euclides encuéntrese una solución en enteros para cada una de las siguientes ecuaciones:

- a)  $696x + 408y = 48$
- b)  $(6n + 1)x + 3ny = 12$ .

Veamos ahora como conociendo una solución entera se pueden encontrar *todas* las soluciones en enteros de una ecuación diofantina.

**PROPOSICIÓN 3:** *El conjunto de soluciones enteras  $x, y$  de la ecuación*

$$ax + by = c \quad (a, b, c \text{ enteros})$$

*es de la forma*

$$x = x_0 + u; \quad y = y_0 + v$$

*en donde  $x_0, y_0$  es una solución particular de la ecuación  $ax + by = c$  y  $u, v$  son soluciones arbitrarias de la ecuación homogénea asociada*

$$ax + by = 0.$$

*Demostración.* Sea  $x_0, y_0$  una solución particular de  $ax + by = c$  y  $x_1, y_1$  otra solución. Entonces

$$u = x_1 - x_0, \quad v = y_1 - y_0$$

es solución de  $ax + by = 0$ . En efecto

$$\begin{aligned} au + bv &= a(x_1 - x_0) + b(y_1 - y_0) \\ &= ax_1 + by_1 - (ax_0 + by_0) \\ &= c - c = 0. \end{aligned}$$

Por lo tanto

$$x_1 = x_0 + u, \quad y_1 = y_0 + v$$

en donde  $u, v$  es solución de

$$ax + by = 0.$$

Sea ahora  $u, v$  una solución de

$$ax + by = 0.$$

Entonces

$$x_1 = x_0 + u; \quad y_1 = y_0 + v$$

es solución de la ecuación original. En efecto

$$\begin{aligned} ax_1 + by_1 &= a(x_0 + u) + b(y_0 + v) \\ &= ax_0 + by_0 + au + bv = c + 0 = c. \end{aligned}$$

Recordemos como encontramos todas las soluciones de la ecuación homogénea

$$ax + by = 0 \quad (a, b \text{ enteros}).$$

Si  $a = 0, b = 0$ , entonces toda pareja de enteros es solución.

Supongamos ahora que  $a \neq 0$ , o bien  $b \neq 0$ . Sea  $d = (a, b)$ ; escribimos

$$a = da', \quad b = db'.$$

Ya que  $d \neq 0$ , la ecuación

$$a'x + b'y = 0$$

tiene las mismas soluciones que la anterior. Ahora bien, las soluciones de esta última son, según la proposición 4 de la sección anterior

$$x = -b't, \quad y = a't \quad (t \text{ entero arbitrario}).$$

Combinando estos resultados con la proposición anterior obtenemos el

**COROLARIO:** Sean  $a, b, c$  enteros tales que  $a$  y  $b$  no son ambos ceros; supongamos además que  $d = (a, b)$  divide a  $c$ . Sea  $a = da'$ ,  $b = db'$ . Entonces el conjunto  $x, y$  de soluciones enteras de la ecuación

$$ax + by = c$$

es  $x = x_0 - b't$ ,  $y = y_0 + a't$  en donde  $t$  es un entero arbitrario y  $x_0, y_0$  es una solución particular entera de  $ax + by = c$ .

Es claro que el caso  $a = 0, b = 0, c \neq 0$  no tiene solución. Si  $c = 0$  entonces, evidentemente, toda pareja de enteros es solución.

## EJERCICIOS

7. Calcúlense todas las soluciones enteras de las siguientes ecuaciones diofantinas:

- a)  $15x + 21y = 300$
- b)  $228x - 348y = 1\,368$
- c)  $1\,242x + 1\,476y = 90$
- d)  $(4n+1)x + 2ny = n$
- e)  $(2n+1)x + 4ny = n.$

## 5. FACTORIZACIÓN ÚNICA

Ya en la enseñanza elemental de las matemáticas se ha tratado la descomposición de los números naturales en producto de primos. Por ejemplo, escribimos

$$36 = 2^2 3^2, \quad 1\,400 = 2^3 5^2 7, \quad 187 = 11 \times 17.$$

En esta sección analizaremos este tema con mayor detalle.

Recordemos primero que

**DEFINICIÓN:** Se dice que un número entero  $p$  distinto de  $\pm 1$  es primo si sus únicos divisores son  $\pm 1$  y  $\pm p$ .

Evidentemente un número  $p$  es primo si y solo si  $-p$  lo es.

Los primeros números primos positivos son

$$\begin{array}{ccccccccccccccccc} 2 & 3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47 & 53 & 59 & 61 & 67 \\ & & & & & & & & & & & & & & & & & & & \\ 71 & 73 & 79 & 83 & 89 & 97 & 101 & 103 & 107 & 109 & 113, & \cdots \end{array}$$

Observemos que si  $p$  es primo y  $a$  un entero entonces el mcd de  $p$  y  $a$  puede ser o bien  $p$  o bien 1. Por tanto  $(p, a) = p$  si y solo si  $p$  divide a  $a$ .

**PROPOSICIÓN 1:** Si un número primo  $p$  divide al producto  $ab$  de dos enteros, entonces  $p$  divide a  $a$  o bien  $p$  divide a  $b$ .

En símbolos,

$$p | ab \Rightarrow p | a \text{ o bien } p | b.$$

**Demostración.** Si  $p | a$  no hay nada que demostrar. Si  $p \nmid a$  entonces  $(p, a) = 1$  y por lo tanto, según la proposición 3 del párrafo 3 tenemos que  $p | b$ .

## EJERCICIOS

1. Utilizando la expresión de 1 como combinación lineal de  $p$  y  $a$  demuéstrese la proposición anterior directamente.
2. Si  $p$  y  $q$  son primos distintos entonces  $(p, q) = 1$ .
3. Demuéstrese que si un primo  $p$  divide a un producto  $a_1 a_2 \dots a_n$  entonces  $p$  divide al menos a uno de los factores  $a_i$ .
4. Demuéstrese que si un primo  $p$  divide a  $b^n$  ( $n \in \mathbb{N}$ ) entonces  $p$  divide a  $b$ .
5. Mediante ejemplos pruébese que las afirmaciones de los ejercicios 3 y 4 son falsas si  $p$  no es primo.
6. Usando el principio de buen orden demuéstrese que todo entero mayor que 1 es divisible entre un número primo.

**SUGERENCIA:** Considérese el conjunto  $M$  de enteros mayores que 1 que no tienen un factor primo. Si  $M \neq \emptyset$ ,  $M$  tiene un elemento mínimo  $a$ , el cual no puede ser primo. Al descomponer  $a$  como producto de dos enteros positivos mayores que 1 estos sí tienen factores primos.

7. Demuéstrese que hay una infinidad de números primos. Más precisamente, que dado un número natural  $n$ , hay más de  $n$  primos.

**SUGERENCIA:** Supóngase que hay  $n$  primos, digamos  $p_1, p_2, \dots, p_n$ . Demuéstrese que el número

$$p_1 p_2 \cdots p_n + 1$$

tiene un factor primo distinto de los  $n$  primos mencionados.

8. Pruébese que si  $a$  es un entero positivo y  $a$  no es primo, entonces hay un divisor primo  $p$  de  $a$  tal que  $p \leq \sqrt{a}$ .

9. Usando el ejercicio 8 encuéntrense los números primos positivos menores que 150 y mayores que los mencionados en la lista del principio de esta sección.

Es conveniente observar, para futuras generalizaciones, que la propiedad de la proposición 1 caracteriza a los números primos. En efecto,

**PROPOSICIÓN 2:** *Si  $p$  es un entero distinto de  $\pm 1$  con esta propiedad:*

*Si  $a, b \in \mathbb{Z}$  y  $p \mid ab$  entonces  $p \mid a$  o  $p \mid b$ ,*  
*entonces  $p = 0$  o  $p$  es un número primo.* (\*)

**Demostración.** Podemos, desde luego, suponer que  $p \geq 0$ . Examinemos primero el caso  $p > 1$ . Si  $p$  no fuera primo entonces

$$p = ab \text{ con } 1 < a < p, \quad 1 < b < p.$$

La igualdad anterior prueba que  $p \mid ab$  y las desigualdades indican que  $p \nmid a$  y  $p \nmid b$ , es decir,  $p$  no cumpliría la propiedad (\*). Luego, si  $p > 1$  cumple (\*) entonces  $p$  es primo.

Observemos finalmente que 0 cumple la propiedad (\*). En efecto, si  $0 \mid ab$  entonces  $ab = 0$ , por lo que, según sabemos,  $a = 0$  o  $b = 0$ . Esto equivale a  $0 \mid a$  o  $0 \mid b$ .

**OBSERVACIÓN:** Debido a la propiedad de la proposición 2 es conveniente considerar que en  $\mathbf{Z}$ , 0 es primo. Sin embargo, para facilitar los enunciados, en lo que sigue hablaremos únicamente de números primos *distintos* de 0.

**Teorema de factorización única.** *Todo número entero  $a$ , distinto de  $\pm 1$  se puede expresar en la forma*

$$a = up_1p_2 \dots p_h \quad (*)$$

en donde  $u = \pm 1$  y  $p_1, p_2, \dots, p_h$  son primos positivos.

Además, si  $a \neq 0$  la expresión (\*) es única, excepto el orden de los factores.

**Demostración.** Si  $a = 0$ , hacemos  $u = 1$ ,  $h = 1$ ,  $p_1 = 0$  y obtenemos  $a = up_1$ .

Por lo tanto, bastará demostrar que todo entero  $a > 1$  puede expresarse en la forma (\*).

Sea  $M$  el conjunto de enteros mayores que 1 que no se pueden expresar en la forma (\*). Nuestro propósito es demostrar que  $M = \emptyset$ .

Para ello, veremos que si suponemos que  $M \neq \emptyset$  se llega a una contradicción.

Supongamos pues que  $M \neq \emptyset$ . Por el principio de buen orden,  $M$  tiene un elemento mínimo  $a$ . Ahora bien, si  $a$  fuera primo, haciendo  $h = 1$ ,  $u = 1$  y  $a = p_1$  obtendríamos  $a = up$ , lo cual contradice que  $a$  pertenezca a  $M$ . Por consiguiente  $a$  no es primo. Entonces

$$a = bc, \quad (1 < b < a, \quad 1 < c < a).$$

Por ser  $a$  elemento mínimo de  $M$ , las desigualdades anteriores indican que  $b$  y  $c$  no pertenecen a  $M$  y, por lo tanto se pueden expresar en la forma (\*):

$$b = p_1p_2 \dots p_n; \quad c = q_1q_2 \dots q_r.$$

Pero como  $a = bc$ , obtenemos la descomposición

$$a = p_1p_2 \dots p_nq_1q_2 \dots q_r$$

en primos positivos, que es una expresión de la forma (\*). Esto contradice nuevamente el hecho de que  $a$  esté en  $M$ , con lo que queda probada la primera parte del teorema.

Demostraremos ahora la unicidad (excepto el orden de los factores) de las descomposiciones en primos positivos. Supongamos que hay dos tales descomposiciones para un número  $a \neq 0$ :

$$\begin{aligned} a &= up_1p_2 \dots p_h \\ a &= u'q_1q_2 \dots q_t. \end{aligned}$$

Desde luego,  $u = u'$ , por lo que

$$p_1 p_2 \cdots p_h = q_1 q_2 \cdots q_t.$$

Como  $p_1$  divide al miembro de la izquierda,  $p_1$  debe dividir al producto  $q_1 q_2 \cdots q_t$  y como  $p_1$  es primo,  $p_1$  debe dividir a alguna de las  $q_i$ , digamos a  $q_1$ . Pero como  $q_1$  es también primo, resulta que  $p_1 = q_1$ . Simplificando, obtenemos la expresión

$$p_2 p_3 \cdots p_h = q_2 q_3 \cdots q_t.$$

Procediendo en forma análoga, llegamos a que  $p_2 = q_2$ ,  $p_3 = q_3, \dots$ . Si  $h$  fuera menor que  $t$  llegaríamos finalmente a una expresión de la forma  $1 = q_{h+1} \cdots q_t$  lo cual no es posible. Análogamente, si  $t < h$ . Por lo tanto  $t = h$ , con lo que queda probada la unicidad.

En una descomposición de primos como la del teorema anterior podemos juntar los primos iguales que en ella figuren y entonces ésta quedará en la forma

$$a = \pm p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \quad (m_i > 0)$$

y si, además, ordenamos los primos en la forma  $p_1 < p_2 < \cdots < p_h$  entonces la expresión es, según lo demostrado, única.

A veces, dados dos enteros conviene escribir descomposiciones en las que figuren los *mismos* primos. Por ejemplo, si

$$\begin{aligned} a &= 2^8 5^2 7 \\ b &= 3^2 5 \times 11 \end{aligned}$$

podemos escribir

$$\begin{aligned} a &= 2^8 3^0 5^2 7^1 (11)^0 \\ a &= 2^0 3^2 5^1 7^0 (11)^1. \end{aligned}$$

En general, si  $a$  y  $b$  son dos enteros, existe una colección de primos tales que

$$a = \pm p_1^{m_1} p_2^{m_2} \cdots p_h^{m_h} \quad (m_i \geq 0)$$

$$b = \pm p_1^{n_1} p_2^{n_2} \cdots p_h^{n_h} \quad (n_i \geq 0).$$

## EJERCICIOS

**10.** Si  $a$  y  $b$  son dos enteros y los escribimos como acabamos de ver, demuéstrese que

i)  $(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_h^{r_h}$  con  $r_i = \min \{m_i, n_i\}$ .

ii)  $[a, b] = p_1^{s_1} p_2^{s_2} \cdots p_h^{s_h}$  con  $s_i = \max\{m_i, n_i\}$ .

**11.** Si  $m$  y  $n$  son dos enteros demuéstrese que

$$m + n = \min\{m, n\} + \max\{m, n\}.$$

**12.** Utilizando lo demostrado en los dos ejercicios anteriores demuéstrese que si  $a$  y  $b$  son dos enteros, entonces

$$ab = (a, b)[a, b].$$

## 6. CONGRUENCIAS

La divisibilidad permite definir ciertas relaciones de equivalencia en  $\mathbb{Z}$  que son de mucha importancia. En particular, éstas nos permitirán construir valiosos ejemplos de anillos que servirán como punto de partida en el estudio de varios temas del álgebra.

Sea  $m$  un número natural mayor que 1.

**DEFINICIÓN:** Se dice que dos enteros  $a$  y  $b$  son congruentes, módulo  $m$ , si  $m$  divide a la diferencia  $a - b$ .

En símbolos escribiremos

$$a \equiv b \pmod{m} \text{ si y solo si } m | a - b.$$

Por ejemplo, dos números pares arbitrarios  $a$  y  $b$  son congruentes, módulo 2, pues su diferencia  $a - b$  es divisible entre 2. Análogamente, dos números impares  $c$  y  $d$  son también congruentes módulo 2. Si  $e$  es par y  $f$  impar entonces  $e$  y  $f$  no son congruentes módulo 2.

Veamos otro ejemplo: si  $m$  y  $n$  son enteros arbitrarios, los números  $a = 5m - 3$  y  $5n - 3$  son congruentes módulo 5, pues su diferencia  $a - b = 5(m - n)$  es divisible entre 5. Los números  $c = 5m - 1$  y  $d = 5n - 4$  no son congruentes módulo 5 pues su diferencia  $c - d = 5(m - n) + 3$  no es divisible entre 5.

La relación de congruencia que acabamos de definir es *reflexiva, simétrica y transitiva*, o sea, es una relación de equivalencia. En efecto,

**PROPOSICIÓN 1:** Para  $a, b, c$  en  $\mathbb{Z}$ , se tiene que

- i)  $a \equiv a \pmod{m}$ ;
- ii) si  $a \equiv b \pmod{m}$  entonces  $b \equiv a \pmod{m}$ ;
- iii) si  $a \equiv b \pmod{m}$  y  $b \equiv c \pmod{m}$ , entonces  $a \equiv c \pmod{m}$ .

**Demostración:** i) Ya que  $m | 0$ ,  $m | a - a$ , de donde  $a \equiv a \pmod{m}$ .  
ii) Por hipótesis  $m | a - b$ . Luego  $m | b - a$ , de donde  $b \equiv a \pmod{m}$ .

## EJERCICIOS

1. Demuestre (iii).
2.  $a \equiv 0 \pmod{m}$  si y solo si  $m \mid a$ .

La relación de congruencia es compatible con las operaciones de adición y multiplicación en  $\mathbf{Z}$ . Esto significa lo siguiente:

**PROPOSICIÓN 2:** *Para  $a, b, c$  en  $\mathbf{Z}$  se tiene que*

- i) si  $a \equiv b \pmod{m}$  entonces  $a + c \equiv b + c \pmod{m}$ ;
- ii) si  $a \equiv b \pmod{m}$  entonces  $ac \equiv bc \pmod{m}$ .

Demostración. i) Por hipótesis  $m \mid a - b$  y como  $a - b = (a + c) - (b + c)$  se tiene que  $m \mid (a + c) - (b + c)$ , de donde  $a + c \equiv b + c \pmod{m}$ .

3. Demuéstrese (ii).
4. Demuéstrese que si  $a + c \equiv b + c \pmod{m}$ , entonces  $a \equiv b \pmod{m}$ .

Para congruencias, vale también la siguiente ley de cancelación:

5. Demuéstrese que si  $ac \equiv bc \pmod{m}$  y  $m$  y  $c$  son primos entre sí entonces  $a \equiv b$ .
6. Demuéstrese, con ejemplos, que sin la condición de que  $m$  y  $c$  sean primos entre sí la afirmación del ejercicio anterior es falsa.

El siguiente resultado nos da una condición necesaria y suficiente para que dos números sean congruentes.

7. Demuéstrese que si

$$\begin{aligned} a &= mq_1 + r_1 & 0 \leq r_1 < m \\ b &= mq_2 + r_2 & 0 \leq r_2 < m \end{aligned}$$

entonces

$$a \equiv b \pmod{m} \text{ si y solo si } r_1 = r_2.$$

8. Demuéstrese que, módulo 5, todo número es congruente con 0, 1, 2, 3 ó 4.

9. Demuéstrese que si  $p$  es un primo positivo entonces  $ab \equiv 0 \pmod{p}$  implica  $a \equiv 0 \pmod{p}$  o bien  $b \equiv 0 \pmod{p}$ .

10. Dénse varios ejemplos en los que  $ab \equiv 0 \pmod{m}$ , con  $a \not\equiv 0 \pmod{m}$  y  $b \not\equiv 0 \pmod{m}$ .

11. Demuéstrese que si  $a \equiv b \pmod{m}$  y  $c \equiv d \pmod{m}$  entonces  $a \pm c \equiv b \pm d \pmod{m}$  y  $ac \equiv bd \pmod{m}$ .

12. Pruébese que si  $a \equiv b \pmod{m}$  entonces  $b$  es la forma  $b = a + km$  para cierto entero  $k$ .

13. Si  $a \equiv b \pmod{m}$  con  $0 \leq a < m$ ,  $0 \leq b < m$ , entonces  $a = b$ .

Analizaremos ahora la resolución de congruencias lineales en una incógnita. Consideremos la congruencia

$$23x - 11 \equiv 0 \pmod{19}.$$

Como 23 y 19 son primos entre sí, podemos expresar 1 como combinación de 23 y 19 (por ejemplo, usando el algoritmo de Euclides):

$$1 = 5 \times 23 - 6 \times 19.$$

De aquí obtenemos

$$23 \times 5 - 1 = 6 \times 19$$

y multiplicando por 11 resulta que

$$23 \times 55 - 11 = 66 \times 19,$$

de donde,

$$23 \times 55 - 11 \equiv 0 \pmod{19}.$$

En esta forma hemos encontrado la solución  $x = 55$ .

Esta no es la única solución. Por ejemplo  $x = 17$  es también solución como puede comprobarse fácilmente.

La siguiente proposición aclara esto:

**PROPOSICIÓN 3:** *Si  $a$  y  $m$  son primos entre sí entonces la congruencia*

$$ax + b \equiv 0 \pmod{m}$$

*tiene solución. Además si  $x_1$  y  $x_2$  son soluciones, entonces*

$$x_1 \equiv x_2 \pmod{m}.$$

*Demostración.* Por ser  $(a, m) = 1$  existen enteros  $r$  y  $s$  tales que

$$1 = ar + ms.$$

De ahí obtenemos

$$ar - 1 = -ms$$

y multiplicando por  $-b$ , resulta que

$$a(-br) + b = m(bs),$$

de donde

$$a(-br) + b \equiv 0 \pmod{m}.$$

Es decir,  $x = -br$  es una solución.

## EJERCICIOS

**14.** Demuéstrese la segunda parte de la proposición.

**SUGERENCIA.** Supóngase que  $x_1$  y  $x_2$  son soluciones. Entonces

$$ax_1 + b \equiv 0 \pmod{m}$$

$$ax_2 + b \equiv 0 \pmod{m}.$$

Réstense las dos congruencias (ejercicio 11) y úsese la hipótesis  $(a, m) = 1$  y el ejercicio 5.

**15.** Demuéstrese que la congruencia  $ax + b \equiv 0 \pmod{m}$  tiene solución si y solo si el mcd de  $a$  y  $m$  divide a  $b$ .

El resultado siguiente se refiere a soluciones de sistemas de dos congruencias y se conoce como:

**El teorema chino del residuo.** Si  $m$  y  $n$  son primos entre sí, entonces las congruencias

$$\begin{aligned}x &\equiv a \pmod{m} \\x &\equiv b \pmod{n}\end{aligned}$$

tienen solución común.

*Demostración.* Por la proposición anterior, la congruencia  $x \equiv a \pmod{m}$  tiene solución, digamos  $r$  y cualquier otra solución es de la forma (véase el ejercicio 12)  $s = r + km$  con  $k \in \mathbb{Z}$ . Ahora bien, lo que queremos es que alguna de estas soluciones lo sea también de la congruencia  $x \equiv b \pmod{n}$ . Es decir, necesitamos encontrar una  $k$  tal que

$$r + km \equiv (mod n)$$

o, lo que es lo mismo, tal que

$$mk + (r - b) \equiv 0 \pmod{n}.$$

Esto se puede hacer, pues  $(m, n) = 1$ .

## EJERCICIOS

**16.** Si  $x_1$  y  $x_2$ , son soluciones del sistema del teorema anterior entonces  $x_1 \equiv x_2 \pmod{mn}$ . Por lo tanto hay una sola solución  $t$  tal que  $0 \leq t < rs$ .

**17.** Si  $m_1, m_2, \dots, m_h$  son primos relativos dos a dos, entonces las congruencias

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_h \pmod{m_h}$$

tienen solución común.

**18.** Resuélvanse las siguientes congruencias:

- a)  $16x - 9 \equiv 0 \pmod{35}$ ;
- b)  $200x + 315 \equiv 0 \pmod{441}$ ;
- c)  $(2n + 1)x + 7 \equiv 0 \pmod{4n}$ ;
- d)  $(3n - 2)x + 5n \equiv 0 \pmod{9n - 9}$ .

**19.** Resuélvanse los siguientes sistemas de congruencias:

<i>a)</i> $x \equiv 0 \pmod{3}$	<i>b)</i> $x \equiv 1 \pmod{25}$	<i>c)</i> $x \equiv 3 \pmod{17}$
$x \equiv 0 \pmod{8}$	$x \equiv 7 \pmod{35}$	$x \equiv 4 \pmod{21}$
		$x \equiv 5 \pmod{25}$ .

Lo estudiado hasta aquí permite construir más ejemplos de anillos. En efecto, para cada número natural  $m$  daremos un anillo, denotado con  $\mathbf{Z}_m$ , que llamaremos *el anillo de los enteros módulo m*. Todos ellos son anillos con un número finito de elementos cada uno. Veremos un ejemplo.

Como vimos en el ejercicio 8, módulo 5, todo número es congruente con 0, 1, 2, 3 o 4. Estos números son los únicos residuos posibles que se obtienen al dividir un número entre 5. Definamos ahora dos operaciones nuevas con estos residuos. Por comodidad, a las operaciones las seguiremos denotando con + y  $\times$  y las llamaremos suma y producto (módulo 5) :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

La simple observación de las tablas nos indica cómo las podemos elaborar. Por ejemplo, al sumar 3 y 4, primero los sumamos con la suma en  $\mathbf{Z}$ , obteniendo 7 y escribimos en la tabla el residuo que obtenemos al dividir 7 entre 5, o sea 2. Análogamente para el producto. Por ejemplo,  $4 \times 4 = 16$  y, módulo 5, obtenemos 1. Es decir, con la operación de  $\mathbf{Z}_5$ ,  $4 \times 4 = 1$ .

En general, dados dos elementos  $a$  y  $b$  en  $\mathbf{Z}_5$ , su suma y su producto se calculan así:

Escribimos

$$\begin{aligned} a + b &= 5q + r \quad 0 \leq r < 5 \\ ab &= 5q' + s \quad 0 \leq s < 5. \end{aligned}$$

Entonces, en  $\mathbf{Z}_5$ ,  $a + b = r \in \mathbf{Z}_5$  y  $ab = s \in \mathbf{Z}_5$ .

## EJERCICIOS

20. Compruébense las dos tablas anteriores.
21. Constrúyanse, en forma análoga las tablas de multiplicación para  $\mathbf{Z}_2$ ,  $\mathbf{Z}_3$ ,  $\mathbf{Z}_4$  y  $\mathbf{Z}_6$ .
22. Dése la forma de definir las operaciones de suma y producto en  $\mathbf{Z}_m$ .

El conjunto  $\mathbf{Z}_m = \{0, 1, 2, \dots, m-1\}$  con las operaciones obtenidas en un anillo conmutativo con elemento unitario. Para demostrar esto debemos comprobar que se satisfacen los axiomas 1 a 8 mencionados en la sección 1 del capítulo anterior.

Como ejemplo, probaremos que vale la propiedad distributiva.

Sean  $a, b, c$  en  $\mathbf{Z}_m$ . Si

$$a(b+c) = mq_1 + r \quad (0 \leq r < m)$$

sabemos, por lo anterior, que en  $\mathbf{Z}_m$   $a(b+c) = r$ . Análogamente, si

$$ab+ac = mq_2 + s, \quad (0 \leq s < m)$$

en  $\mathbf{Z}_m$ ,  $ab+ac = s$ . Por lo tanto, en  $\mathbf{Z}$ ,

$$r \equiv a(b+c) = ab+ac \equiv s \pmod{m}$$

en donde (ejercicio 13),  $r = s$ . Es decir, en  $\mathbf{Z}_m$  tenemos que

$$a(b+c) = ab+ac.$$

### EJERCICIOS

- 23. Compruébese que en  $\mathbf{Z}_m$  valen los demás axiomas antes mencionados.
- 24. Demuéstrese que  $\mathbf{Z}_2$ ,  $\mathbf{Z}_3$  y  $\mathbf{Z}_5$  son dominios enteros. Lo mismo para  $\mathbf{Z}_p$  con  $p$  primo.
- 25. Demuéstrese que  $\mathbf{Z}_4$  y  $\mathbf{Z}_6$  no son dominios enteros.



# 8

CAPÍTULO

# Los números reales

**NOTA IMPORTANTE:** Por la naturaleza de su tema este capítulo (con la excepción del párrafo 1) es más difícil que los demás. Convendrá excluirlo de la mayoría de los cursos en que se use este libro como texto. Esto no impedirá al estudiante comprender los demás capítulos.

El párrafo 1, relativo a los números racionales, puede incluirse en cualquier curso.

## 1. LOS NÚMEROS RACIONALES

En este párrafo construiremos los números *racionales* (o fraccionarios) a partir de los enteros. Destacaremos únicamente las propiedades de los racionales que se usarán en los párrafos siguientes.

Consideremos el conjunto  $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ , cuyos elementos son las parejas  $(a, b)$  de enteros tales que  $b \neq 0$ .

Definimos una relación  $\sim$ :

$$(a, b) \sim (a', b') \text{ si } ab' = ba'.$$

**PROPOSICIÓN 1:**  $\sim$  es una relación de equivalencia.

*Demostración:*

- i)  $\sim$  es reflexiva puesto que  $ab = ba$ ;
- ii)  $\sim$  es simétrica:

$$(a, b) \sim (a', b') \iff ab' = ba' \iff a'b = b'a \iff (a', b') \sim (a, b)$$

iii)  $\sim$  es transitiva:

$$\text{si } (a, b) \sim (a', b') \text{ y } (a', b') \sim (a'', b'') \text{ se cumplen} \\ ab' = ba' \text{ y } a'b'' = b'a'',$$

de donde

$$ab'b'' = ba'b'' \text{ y } a'b''b = b'a''b.$$

De estas igualdades obtenemos  $ab'b'' = b'a''b$  y, puesto que  $b' \neq 0$ ,  $ab'' = a''b$ . Pero esto último significa que  $(a, b) \sim (a'', b'')$ , como se quería demostrar.

Usaremos la notación siguiente:

$$\frac{a}{b} = \{(x, y) | (a, b) \sim (x, y)\}.$$

Es decir que  $\frac{a}{b}$  denota el conjunto de todos los  $(x, y) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$  tales que  $(a, b) \sim (x, y)$ .

Estos conjuntos pueden ser denotados de varias maneras diferentes. En efecto:

**PROPOSICIÓN 2:**

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba'.$$

*Demostración.* Supóngase que  $a/b = a'/b'$ . Como

$$(a', b') \in \frac{a'}{b'}$$

tenemos que

$$(a', b') \in \frac{a}{b},$$

esto es,  $(a, b) \sim (a', b')$ . Por la definición de  $\sim$  esto significa que  $ab' = ba'$ . Hemos demostrado la implicación de izquierda a derecha.

Supongamos ahora que  $ab' = ba'$ , lo que significa que  $(a, b) \sim (a', b')$ . Sea

$$(x, y) \in \frac{a}{b}.$$

Entonces  $(a, b) \sim (x, y)$  y, por ser  $\sim$  una relación de equivalencia,  $(a', b') \sim (x, y)$ . Con esto hemos demostrado que

$$\frac{a}{b} \subset \frac{a'}{b'}.$$

De manera análoga se demuestra la inclusión en el sentido contrario, lo que termina la demostración.

**COROLARIO 1:**

$$\frac{a}{b} = \frac{ar}{br} \text{ si } r \neq 0.$$

Los conjuntos  $a/b$  son, por definición, los *números racionales*. El conjunto de los racionales se denota **Q**.

**Suma y producto en Q.** Para definir estas operaciones necesitamos dos lemas.

**LEMA 1:**

$$\left( \frac{a}{b} = \frac{a'}{b'} \text{ y } \frac{c}{d} = \frac{c'}{d'} \right) \Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}.$$

*Demostración.* Por hipótesis  $ab' = ba'$  y  $cd' = dc'$ . Entonces

$$\begin{aligned} (ad + bc)b'd' &= adb'd' + bcb'd' = bda'd' + bdb'c' \\ &= bd(a'd' + b'c'), \end{aligned}$$

que, según la proposición 2, es lo que se quería demostrar.

**LEMA 2:**

$$\left( \frac{a}{b} = \frac{a'}{b'} \text{ y } \frac{c}{d} = \frac{c'}{d'} \right) \Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

*Demostración.* La hipótesis es la misma del lema anterior. Tendremos, pues,

$$acb'd' = bda'c',$$

como se quería demostrar.

Ahora podemos definir

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Los lemas anteriores muestran que estas son definiciones auténticas. Si denotamos  $a/b$  y  $c/d$  de otras maneras, la suma y el producto que se obtienen con las fórmulas anteriores son los mismos.

**OBSERVACIÓN:**

$$\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d}.$$

En efecto,

$$\frac{a}{d} + \frac{b}{d} = \frac{ad+db}{d^2} = \frac{(a+b)d}{d^2} = \frac{a+b}{d},$$

por el corolario 1.

Se deja a cargo del lector la comprobación de cada una de las propiedades de la suma y el producto en  $\mathbf{Q}$  que aparecen en la proposición siguiente. En las comprobaciones es necesario usar las propiedades que son válidas en  $\mathbf{Z}$ .

**PROPOSICIÓN 3:** En  $\mathbf{Q}$ :

- i) La suma es conmutativa.
- ii) La suma es asociativa.
- iii)  $0/1$  es idéntico aditivo. Es decir,  $(m/n) + (0/1) = m/n$  para todo  $m/n$ .
- iv) Todo racional tiene inverso aditivo (otro racional que al ser sumado con él da  $0/1$  como resultado). El único inverso aditivo de  $m/n$  es  $-m/n$ , también denotado por  $-(m/n)$ .
- v) El producto es conmutativo.
- vi) El producto es asociativo.
- vii)  $1/1$  es idéntico aditivo. Es decir,  $(m/n) \cdot (1/1) = m/n$  para todo  $m/n$ .
- viii) Todo racional  $\neq 0/1$  tiene inverso multiplicativo (otro racional que al ser multiplicado por él da el producto  $1/1$ ). El único inverso multiplicativo de  $m/n$  es  $n/m$ , también denotado por  $(m/n)^{-1}$ .
- ix) El producto distribuye a la suma.

El inciso vi), por ejemplo, se demuestra así:

$$\begin{aligned} \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} &= \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f} \\ &= \frac{a(ce)}{b(df)} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right). \end{aligned}$$

**Racionales positivos. Orden en  $\mathbf{Q}$ .** Sea  $\mathbf{Z}^+$  el conjunto de los enteros positivos.

**LEMA 3:** Supóngase que

$$\frac{a}{b} = \frac{a'}{b'}.$$

Entonces  $ab \in \mathbf{Z}^+ \iff a'b' \in \mathbf{Z}^+$ .

*Demostración.* Por hipótesis  $ab' = ba'$ , de donde  $abb'^2 = a'b'b^2$ . Supóngase que  $ab \in \mathbf{Z}^+$ . Como  $b'^2 \in \mathbf{Z}^+$  tenemos  $abb'^2 \in \mathbf{Z}^+$ , esto es,  $a'b'b^2 \in \mathbf{Z}^+$ . Como  $b^2 \in \mathbf{Z}^+$  debe tenerse  $a'b' \in \mathbf{Z}^+$ , ya que el producto de un entero positivo por un entero no positivo no es positivo. Esto muestra que  $ab \in \mathbf{Z}^+ \implies a'b' \in \mathbf{Z}^+$ . El recíproco se demuestra de manera análoga.

Este lema nos permite definir el conjunto  $\mathbf{Q}^+$  de los *racionales positivos*:

$$\mathbf{Q}^+ = \left\{ \frac{a}{b} \middle| \frac{a}{b} \in \mathbf{Q}, ab \in \mathbf{Z}^+ \right\}.$$

**PROPOSICIÓN 4:** Para cada  $a/b \in \mathbf{Q}$  es verdadera una y solo una de las afirmaciones siguientes:

i)  $\frac{a}{b} \in \mathbf{Q}^+$ ;

ii)  $\frac{a}{b} = \frac{0}{1}$ ;

iii)  $-\frac{a}{b} \in \mathbf{Q}^+$ .

**PROPOSICIÓN 5:** Las sumas y los productos de racionales positivos son positivos.

De las afirmaciones contenidas en las dos proposiciones anteriores demostraremos únicamente que la suma de positivos es positiva. Supongamos que

$$\frac{a}{b} \in \mathbf{Q}^+, \frac{c}{d} \in \mathbf{Q}^+.$$

Definimos

$$a' = \begin{cases} a & \text{si } b \in \mathbf{Z}^+ \\ -a & \text{si } b \notin \mathbf{Z}^+ \end{cases}$$

$$b' = \begin{cases} b & \text{si } b \in \mathbf{Z}^+ \\ -b & \text{si } b \notin \mathbf{Z}^+ \end{cases}$$

Entonces

$$\frac{a'}{b'} = \left\{ \begin{array}{l} \frac{a}{b} \text{ si } b \in \mathbf{Z}^+ \\ \frac{-a}{b} \text{ si } b \notin \mathbf{Z}^+ \end{array} \right\} = \frac{a}{b}.$$

Además,  $b' \in \mathbf{Z}^+$ . Como consecuencia de  $a'b' \in \mathbf{Z}^+$  se tiene también  $a' \in \mathbf{Z}^+$ .

Definimos análogamente  $c'$  y  $d'$  a partir de  $c$  y  $d$ , que cumplen las condiciones

$$\frac{c'}{d'} = \frac{c}{d}, \quad c' \in \mathbf{Z}^+, \quad d' \in \mathbf{Z}^+.$$

Entonces

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'}$$

y es claro que  $(a'd' + b'c') / (b'd') \in \mathbf{Z}^+$ , de donde concluimos que

$$\frac{a}{b} + \frac{c}{d} \in \mathbf{Z}^+.$$

A continuación definiremos el orden en  $\mathbf{Q}$ :

$$\frac{a}{b} > \frac{c}{d} \text{ si } \frac{a}{b} + \frac{-c}{d} \in \mathbf{Q}^+.$$

OBSERVACIÓN:

$$\frac{a}{b} \in \mathbf{Q}^+ \iff \frac{a}{b} > \frac{0}{1}.$$

PROPOSICIÓN 6: Dados  $a/b$  y  $c/d$  en  $\mathbf{Q}$  se cumple una y solo una de las afirmaciones siguientes:

i)  $\frac{a}{b} > \frac{c}{d}$ ;

ii)  $\frac{a}{b} = \frac{c}{d}$ ;

iii)  $\frac{c}{d} > \frac{a}{b}$ .

PROPOSICIÓN 7: La relación  $>$  es transitiva:

$$\left( \frac{a}{b} > \frac{c}{d} \text{ y } \frac{c}{d} > \frac{e}{f} \right) \Rightarrow \frac{a}{b} > \frac{e}{f}.$$

PROPOSICIÓN 8:

i)  $\left( \frac{a}{b} > \frac{a'}{b'} \text{ y } \frac{c}{d} > \frac{c'}{d'} \right) \Rightarrow \frac{a}{b} + \frac{c}{d} > \frac{a'}{b'} + \frac{c'}{d'};$

ii)  $\frac{a}{b} > \frac{a'}{b'} \Rightarrow \frac{a}{b} + \frac{c}{d} > \frac{a'}{b'} + \frac{c}{d};$

$$\text{iii}) \left( \frac{a}{b} > \frac{a'}{b'} \geq \frac{0}{1} \text{ y } \frac{c}{d} > \frac{c'}{d'} \geq \frac{0}{1} \right) \Rightarrow \frac{a}{b} \cdot \frac{c}{d} > \frac{a'}{b'} \cdot \frac{c'}{d'};$$

$$\text{iv}) \left( \frac{a}{b} > \frac{a'}{b'} \text{ y } \frac{c}{d} > \frac{0}{1} \right) \Rightarrow \frac{a}{b} \cdot \frac{c}{d} > \frac{a'}{b'} \cdot \frac{c}{d}.$$

$$\text{v}) \frac{a}{b} > \frac{c}{d} \Leftrightarrow -\frac{c}{d} > -\frac{a}{b}.$$

Las demostraciones quedan como ejercicio.

**Los enteros como racionales.** Consideremos la función

$$i: \mathbf{Z} \rightarrow \mathbf{Q}$$

definida como

$$i(a) = \frac{a}{1}.$$

Esta función es inyectiva ( $i(a) = i(b) \Rightarrow a/1 = b/1 \Rightarrow a = b$ ). Convenimos en cambiar el significado de  $\mathbf{Z}$ , que de ahora en adelante denotará al conjunto  $Im(i)$  que consta de los racionales que pueden expresarse en la forma  $a/1$ . Pero convenimos también en que el símbolo  $a$  es otra notación admisible para el racional  $a/1$ . Así que escribiremos, por ejemplo, 0 y 1 en lugar de  $0/1$  y  $1/1$ , respectivamente. Podríamos expresar esta convención de otro modo diciendo que identificamos  $\mathbf{Z}$  con un subconjunto de  $\mathbf{Q}$  por medio de la función inyectiva  $i$ . Al hacer esta identificación se preservan las operaciones. Es decir:

$$\begin{aligned} i(a) + i(b) &= i(a+b) \\ i(a) \cdot i(b) &= i(ab). \end{aligned}$$

**El subconjunto  $\mathbf{D}$  de  $\mathbf{Q}$ .** Los números racionales de la forma

$$\frac{a}{10^n}$$

constituyen un subconjunto de  $\mathbf{Q}$  que denotaremos  $\mathbf{D}$ . El elemento  $a/10^n$  se acostumbra representar escribiendo  $a$  en la forma usual, con base 10, y poniendo un punto a  $n$  lugares del extremo derecho:

$$\frac{325}{100} = 3.25$$

$$\frac{4}{10000} = 0.0004.$$

También se utilizará la notación

$$10^{-n} = \frac{1}{10^n} = 0.\underbrace{0\cdots 0}_n 1$$

Las sumas y productos de elementos de  $\mathbf{D}$  pertenecen a  $\mathbf{D}$ . Sea

$$\mathbf{D}^+ = \mathbf{D} \cap \mathbf{Q}^+, \quad \mathbf{D}^- = \mathbf{D} \cap \mathbf{Q}^-.$$

Los elementos de  $\mathbf{D}^+$  son los

$$A.a_1a_2\cdots a_n,$$

donde  $A$  es un entero no negativo, los  $a_i$  son cifras  $a_i \in \{0, 1, \dots, 9\}$ , y  $n$  es tan grande como se quiera, porque podemos agregar ceros a la derecha de la última cifra:

$$3.25 = 3.250 = 3.2500 = \dots$$

Los elementos de  $\mathbf{D}^-$  son los

$$-A.a_1a_2\cdots a_n.$$

**PROPOSICIÓN 9:**

- i)  $0 > x$  para todo  $x \in \mathbf{D}^-$ ,
- ii)  $x > y$  siempre que  $x \in \mathbf{D}^+$ ,  $y \in \mathbf{D}^-$ ,
- iii)  $x > 0$  para todo  $x \in \mathbf{D}^+$ ,
- iv) dados dos elementos cualquiera de  $\mathbf{D}^+$ ,

$$x = A.a_1a_2\cdots a_n,$$

$$y = B.b_1b_2\cdots b_n,$$

$x > y$  en cualquiera de los dos casos siguientes:

- iv') Si  $A > B$ .
- iv'') Si  $A = B$  y existe algún entero no negativo  $m \leq n$  tal que  $a_i = b_i$  para  $i < n$  y  $a_m > b_m$ .
- v) Dados  $x \in \mathbf{D}^+$ ,  $y \in \mathbf{D}^+$ ,

$$-x > -y \quad \text{si} \quad y > x.$$

**PROPOSICIÓN 10:** La regla de los signos es válida en  $\mathbf{D}$ . Esto es:

$$(-A.a_1\cdots a_n) \times B.b_1\cdots b_n = -(A.a_1\cdots a_n \times B.b_1\cdots b_n)$$

$$A.a_1\cdots a_n \times (-B.b_1\cdots b_n) = -(A.a_1\cdots a_n \times B.b_1\cdots b_n)$$

$$(-A.a_1\cdots a_n) \times (-B.b_1\cdots b_n) = A.a_1\cdots a_n \times B.b_1\cdots b_n.$$

## 2. EL CONJUNTO $\mathbf{R}$ DE LOS REALES. ORDEN EN $\mathbf{R}$

Consideremos las expresiones

$$A \cdot a_1 a_2 a_3 \dots,$$

donde  $A$  es un entero no negativo expresado en base 10 y los  $a_i \in \{0, 1, 2, \dots, 9\}$ . Los puntos suspensivos indican que hay una infinidad de cifras  $a_i$ . De esas expresiones admitimos únicamente las que no tienen colas de 9, o sea las que satisfacen la condición siguiente:

*Para ningún natural  $n$  se cumple que  $a_i = 9$  para todos los índices  $i \geq n$ .*

A estas expresiones, con la excepción de

$$0.000\dots$$

las llamamos *números reales positivos*. Su conjunto se denota  $\mathbf{R}^+$ .

El conjunto  $\mathbf{R}^-$  de los *reales negativos* consta de los reales positivos con el signo  $-$  antepuesto.

El conjunto  $\mathbf{R}$  de los *números reales* es la unión de  $\mathbf{R}^+$ ,  $\mathbf{R}^-$  y  $\{0.000\dots\}$ .

Identificamos  $\mathbf{D}$  con un subconjunto de  $\mathbf{R}$  siguiendo la última cifra de cada elemento de  $\mathbf{D}$  con una infinidad de ceros:

$$3.25 = 3.250000\dots$$

Tenemos, pues,  $\mathbf{Z} \subset \mathbf{D} \subset \mathbf{R}$ ,  $\mathbf{Z}^+ = \mathbf{D}^+ \cap \mathbf{Z}$ ,  $\mathbf{Z}^- = \mathbf{D}^- \cap \mathbf{Z}$ ,  $\mathbf{D}^+ = \mathbf{R}^+ \cap \mathbf{D}$ ,  $\mathbf{D}^- = \mathbf{R}^- \cap \mathbf{D}$ .

**Orden en  $\mathbf{R}$ .** Un *orden total* en un conjunto  $S$  es una relación  $>$  en  $S$  que satisface las condiciones:

- a) Para cualesquiera  $r, s, t \in S$ ,  $(r > s \text{ y } s > t) \Rightarrow r > t$  (Transitividad).
- b) Para cualesquiera  $r, s \in S$  se cumple una y solo una de las afirmaciones siguientes:

$$r = s, \quad r > s, \quad s > r \quad (\text{Tricotomía}).$$

Describiremos ahora el orden total  $>$  de  $\mathbf{R}$ :

- i)  $0 > x$  para todo  $x \in \mathbf{R}^-$ ,
- ii)  $x > y$  siempre que  $x \in \mathbf{R}^+$ ,  $y \in \mathbf{R}^-$ ,
- iii)  $x > 0$  para todo  $x \in \mathbf{R}^+$ ,
- iv) dados dos reales positivos cualesquiera,

$$x = A \cdot a_1 a_2 \dots,$$

$$y = B \cdot b_1 b_2 \dots,$$

$x > y$  en cualquiera de los dos casos siguientes:

- iv') Si  $A > B$ .
- iv'') Si  $A = B$  y existe algún entero no negativo  $n$  tal que  $a_i = b_i$  para  $i < n$  y  $a_n > b_n$ .
- v) Para  $x \in \mathbf{R}^+$ ,  $y \in \mathbf{R}^+$ ,

$$-x > -y \quad \text{si } y > x.$$

**Ejemplo:**

$$\begin{aligned} 0 &> -0.0001 \\ 0.002 \dots &> -2.539 \\ 3.25 &> 0 \\ 1 &> 0.99872 \\ 2.1234608 \dots &> 2.123459812 \dots \\ -2.123459812 \dots &> -2.1234608 \dots \end{aligned}$$

El lector puede comprobar que las reglas i) a v) son suficientes para decidir si  $x = y$ ,  $x > y$  o  $y > x$ , y para demostrar que solo se da una de esas posibilidades. También puede comprobar que  $>$  es transitiva.

Observamos (véase proposición 9 del párrafo 1) que el orden que acabamos de definir en  $\mathbf{R}$  al ser restringido a  $\mathbf{D}$  coincide con el orden que ya habíamos definido para este conjunto en el párrafo 1. O sea que hemos extendido el orden de  $\mathbf{D}$  a  $\mathbf{R}$ .

**PROPOSICIÓN 1:** Entre cada dos elementos de  $\mathbf{R}$  hay uno de  $\mathbf{D}$ . Esto es, si  $\alpha < \beta$  existe  $c \in \mathbf{D}$  tal que  $\alpha < c < \beta$ .

*Demostración.* Se hará la demostración en el caso  $0 < \alpha < \beta$  y el lector la completará. Supóngase que

$$\begin{aligned} \alpha &= A \cdot a_1 a_2 \dots \\ \beta &= B \cdot b_1 b_2 \dots \end{aligned}$$

Si  $A < B$  sea  $n$  tal que  $a_n \neq 9$  y sea  $a_n^* = a_n + 1$ . Tomando  $c = A \cdot a_1 \dots a_{n-1} a_n^* \in \mathbf{D}$  vemos que

$$\alpha < c < \beta.$$

Si  $A = B$  sea  $n$  tal que  $a_i = b_i$  para  $i < n$  y  $a_n < b_n$ . Tomemos  $m > n$  tal que  $a_m \neq 9$  y sea  $a_m^* = a_m + 1$ . Sea  $c = A \cdot a_1 \dots a_{m-1} a_m^* \in \mathbf{D}$ . Entonces

$$\alpha < c < \beta.$$

**PROPOSICIÓN 2:** Para cada  $\alpha \in \mathbf{R}$  y cada entero positivo  $n$  existe  $a \in \mathbf{D}$  tal que  $a < \alpha < a + 10^{-n}$ . Si  $\alpha > 0$  puede tomarse  $a > 0$ .

*Demostración:*

i) Supongamos que  $\alpha \notin \mathbf{D}$ .

Si  $\alpha$  es positivo, sea  $\alpha = A \cdot a_1 a_2 \dots$ . Tomamos  $a = A \cdot a_1 \dots a_n$  y tenemos  $a < \alpha < a + 10^{-n}$ .

Si  $\alpha$  es negativo, sea  $\alpha = -A \cdot a_1 a_2 \dots$ . Tenemos, si  $a = A \cdot a_1 \dots a_n$ ,

$$-(a + 10^{-n}) < \alpha < -a = -(a + 10^{-n}) + 10^{-n}.$$

ii) Supongamos que  $\alpha \in \mathbf{D}$ . Tomamos

$$a = \alpha - 10^{-n-1} \in \mathbf{D}$$

y tenemos

$$a = \alpha - 10^{-n-1} < \alpha < \alpha + 10^{-n-1} = a + 2 \times 10^{-n-1} < a + 10^{-n}.$$

### 3. COTAS Y FRONTERAS

Las nociones de *cota* y *frontera (superiores e inferiores)* que se introducen en esta sección son indispensables para el resto del capítulo.

Cada una de las definiciones siguientes contiene, en realidad, una pareja de definiciones. La primera, al ignorar lo que está entre paréntesis. La segunda al poner las palabras y fórmulas que están entre paréntesis en lugar de las que les preceden.

**DEFINICIÓN 1:** Sea  $S \subset \mathbf{R}$ . Decimos que  $\alpha \in \mathbf{R}$  es una *cota superior (inferior)* de  $S$  si  $\alpha \geqslant x$  ( $\alpha \leqslant x$ ) para todo  $x \in S$ .

**DEFINICIÓN 2:** Sea  $S \subset \mathbf{R}$ . Decimos que  $S$  es *acotado superiormente (inferiormente)* si existe algún  $\alpha \in \mathbf{R}$  que es cota superior (inferior) de  $S$ .

**DEFINICIÓN 3:** Sea  $S \subset \mathbf{R}$ . Decimos que  $\alpha$  es *frontera superior (inferior)* de  $S$  si:

i)  $\alpha$  es cota superior (inferior) de  $S$ .

ii) Si  $x$  es cualquier otra cota superior (inferior) de  $S$ , entonces  $x > \alpha$  ( $x < \alpha$ ).

Si  $\alpha$  es frontera superior (inferior) de  $S$  escribimos

$$\alpha = \sup S \quad (\alpha = \inf S).$$

Esta notación solo quedará plenamente justificada cuando demostremos la unicidad de las fronteras. De otro modo tendríamos un mismo símbolo para denotar objetos diferentes.

**TEOREMA 1:** Todo subconjunto no vacío de  $\mathbf{R}$  acotado superiormente (inferiormente) tiene frontera superior (inferior).

*Demostración:*

a) Demostraremos primero que todo  $S$  acotado superiormente y tal que  $S \cap \mathbf{R}^+ \neq \emptyset$  tiene frontera superior.

Sea  $C$  el conjunto de todas las cotas superiores de  $S$ . Entonces  $C \neq \emptyset$  y  $C \subset \mathbf{R}^+$ .

Sea  $C_0$  el conjunto de todos los enteros no negativos que son la parte entera de algún elemento de  $C$  (decimos que  $B$  es la parte entera de  $B.b_1b_2\ldots$ ). Entonces  $C_0 \neq \emptyset$ . Sea  $A$  el mínimo de los elementos de  $C_0$ .  $A$  es un entero no negativo.

Sea  $C_1$  el conjunto de todas las cifras que aparecen como primera cifra decimal de algún elemento de  $C$  cuya parte entera es  $A$ . Sea  $a_1$  el mínimo de los elementos de  $C_1$ .

Sea  $C_2$  el conjunto de todas las cifras que aparecen como segunda cifra decimal de algún elemento de  $C$  de la forma  $A.a_1x_2x_3\ldots$ . Sea  $a_2$  el mínimo de los elementos de  $C_2$ .

Sea  $C_3$  el conjunto de todas las cifras que aparecen como tercera cifra decimal de algún elemento de  $C$  de la forma  $A.a_1a_2x_3x_4\ldots$ , y sea  $a_3$  el mínimo de los elementos de  $C_3$ , y así sucesivamente.

Obtenemos así un entero no negativo  $A$  y una sucesión de cifras  $a_1, a_2, a_3, \dots$

Observemos que no existe ningún entero positivo  $n$  tal que  $a_i = 9$  para todo  $i \geq n$ . Comprobaremos, en efecto, que siempre que  $a_n = 9$  existe algún  $m > n$  tal que  $a_m \neq 9$ : si  $a_n = 9$  existe algún elemento de  $C$  de la forma

$$A \cdot a_1 \dots a_n x_{n+1} x_{n+2} \dots$$

Pero existe algún  $r > n$  tal que  $x_r \neq 9$ , por la restricción hecha en el párrafo 2. Y vemos entonces que alguna  $a_m$  posterior a  $a_n$  es  $\neq 9$ , ya que la suposición  $a_{n+1} = \dots = a_{r-1} = 9$  implica que  $a_r = \text{mínimo elemento de } C_r \leq x_r < 9$ .

Vemos así que hemos formado un real

$$\alpha = A \cdot a_1 a_2 a_3 \dots$$

Demostraremos que  $\alpha$  es frontera superior de  $S$ :

a.1) Veamos en primer lugar que  $\alpha$  es cota superior de  $S$ .

Sea cualquier  $\beta = B.b_1b_2\ldots \in S$ . Por la manera como se ha obtenido  $A$  existe algún real  $A \cdot x_1x_2\ldots \geq \beta$ . Por lo tanto  $A \geq B$ .

Si  $A > B$  queda comprobado que  $\alpha > \beta$ . Si  $A = B$  existe algún  $A \cdot a_1 \cdot x_2 x_3 \dots \geq \beta$ . Por lo tanto  $a_1 \geq b_1$ .

Si  $a_1 > b_1$  queda comprobado que  $\alpha > \beta$ . Si  $a_1 = b_1$  existe algún  $A \cdot a_1 a_2 x_3 x_4 \dots \geq \beta$ . Por lo tanto  $a_2 \geq b_2$ , etcétera.

Vemos así que, o bien  $A = B$ ,  $a_i = b_i$  para  $i < n$  y  $a_n > b_n$ , en cuyo caso  $\alpha > \beta$ , o bien  $A = B$  y  $a_i = b_i$  para todo  $i$ , en cuyo caso  $\alpha = \beta$ . En todo caso  $\alpha \geq \beta$ , como se quería demostrar.

a.2) Veamos, finalmente, para terminar la parte (a) de la demostración, que  $\alpha \leq \beta = B \cdot b_1 b_2 \dots$  para cualquier  $\beta$  que sea cota superior de  $S$ .

Si  $A < B$  se tiene  $\alpha < \beta$ . Si  $A = B$  se tiene  $a_1 \leq b_1$ .

Si  $a_1 < b_1$  se tiene  $\alpha < \beta$ . Si  $a_1 = b_1$  se tiene  $a_2 \leq b_2$ , etcétera.

Vemos así que  $\alpha \leq \beta$ .

b) Demostraremos ahora que todo  $S \subset \mathbf{R}^+$  tiene frontera inferior ( $S \neq \phi$ ).

Sea  $C_0$  el conjunto de las partes enteras de los elementos de  $S$  y sea  $A$  el mínimo de los elementos de  $C_0$ , que es un entero no negativo.

Sea  $C_1$  el conjunto de las primeras cifras decimales de los elementos de  $S$  cuya parte entera es  $A$ , y sea  $a_1$  el mínimo de los elementos de  $C_1$ .

Sea  $C_2$  el conjunto de las segundas cifras decimales de los elementos de  $S$  de la forma  $A \cdot a_1 x_2 x_3 \dots$ , y sea  $a_2$  el mínimo de los elementos de  $C_2$ , etcétera.

Obtenemos así un real  $\alpha = A \cdot a_1 a_2 \dots$ , que el lector podrá demostrar que es frontera inferior de  $S_3$  con procedimientos análogos a los usados en la parte (a) de la demostración.

c) Demostraremos que todo subconjunto  $S$  de  $\mathbf{R}$  no vacío y acotado superiormente tiene frontera superior.

Si  $S \cap \mathbf{R}^+ \neq \phi$  estamos en el caso (a) de la demostración.

Si  $S \cap \mathbf{R}^+ \neq \phi$  pero  $0 \notin S$ , es muy fácil demostrar que  $0 = \sup S$ .

El único caso restante es si  $S \cap \mathbf{R}^+ = \phi$  y  $0 \notin S$ . En este caso  $S \subset \mathbf{R}^-$ .

Sea

$$S' = \{X \cdot x_1 x_2 \dots \mid -X \cdot x_1 x_2 \dots \in S\}.$$

Es claro que  $S' \subset \mathbf{R}^+$ . Por la parte (b) de la demostración  $S'$  tiene frontera inferior. Sea

$$\alpha' = A \cdot a_1 a_2 \dots = \inf S'.$$

Comprobaremos que  $\alpha = -\alpha' = \sup S$ :

$$\begin{aligned} \beta = -B \cdot b_1 b_2 \dots \in S &\implies B \cdot b_1 b_2 \dots \in S' \implies B \cdot b_1 b_2 \dots \geq \alpha' \\ &\implies -B \cdot b_1 b_2 \dots \leq -\alpha' \implies B \leq \alpha. \end{aligned}$$

Con esto queda demostrado que  $\alpha$  es cota superior de  $S$ . Veamos que es menor o igual que cualquier otra cota superior:

$$\begin{aligned}
 & \beta = -B \cdot b_1 b_2 \dots \text{ es cota superior de } S \Rightarrow \\
 \Rightarrow & -B \cdot b_1 b_2 \dots \geq -X \cdot x_1 x_2 \dots \text{ para todo } -X \cdot x_1 x_2 \dots \in S \Rightarrow \\
 \Rightarrow & B \cdot b_1 b_2 \dots \leq X \cdot x_1 x_2 \dots \text{ para todo } X \cdot x_1 x_2 \dots \in S' \Rightarrow \\
 \Rightarrow & B \cdot b_1 b_2 \dots \text{ es cota inferior de } S' \Rightarrow B \cdot b_1 b_2 \dots \leq \alpha' \Rightarrow \\
 \Rightarrow & \beta = -B \cdot b_1 b_2 \dots \geq -\alpha' = \alpha.
 \end{aligned}$$

d) Demostraremos que todo subconjunto  $S$  de  $\mathbf{R}$  no vacío y acotado inferiormente tiene frontera inferior:

Si  $S \subset \mathbf{R}^+$  estamos en el caso (b).

Si  $S \cap \mathbf{R}^- = \emptyset$  y  $0 \in S$  es claro que  $0 = \inf S$ .

Si  $S \cap \mathbf{R}^- \neq \emptyset$  sea  $S_1 = S \cap \mathbf{R}^-$ , y sea

$$S'_1 = \{X \cdot x_1 x_2 \dots \mid -X \cdot x_1 x_2 \dots \in S_1\}.$$

El lector puede demostrar que

$$\inf S = \inf S_1 = -\inf S'_1.$$

El teorema que acabamos de demostrar se complementa con el siguiente:

**TEOREMA 2:** Un subconjunto no vacío de  $\mathbf{R}$  acotado superiormente tiene una sola frontera superior. Si es acotado inferiormente tiene una sola frontera inferior.

En efecto, si  $\alpha$  y  $\beta$  son fronteras superiores de  $S$  se tiene:

- i)  $\alpha$  es cota superior de  $S$ ;
- ii)  $x$  es cota superior de  $S \Rightarrow x \geq \alpha$ ;
- iii)  $\beta$  es cota superior de  $S$ ;
- iv)  $x$  es cota superior de  $S \Rightarrow x \geq \beta$ .

De (ii) y (iii) concluimos que  $\beta \geq \alpha$ . De (i) y (iv), que  $\alpha \geq \beta$ . Por lo tanto  $\alpha = \beta$ .

La unicidad de la frontera inferior se demuestra de manera parecida.

#### 4. SUMA Y PRODUCTO DE REALES

Para sumar y multiplicar elementos de  $\mathbf{D}$  se usan algoritmos bien conocidos:

$$\begin{array}{r}
 3.25 \\
 + 0.0004 \\
 \hline
 3.2504
 \end{array}
 \quad
 \begin{array}{r}
 3.25 \\
 \times 0.024 \\
 \hline
 1300 \\
 650 \\
 \hline
 0.07800
 \end{array}$$

Estos procedimientos no son aplicables en general a elementos de  $\mathbf{R}$ . Si queremos calcular el producto de los reales  $3.1415926535 \dots$  y  $2.71828\dots$ , por ejemplo, debemos contentarnos con tomar elementos de  $\mathbf{D}$  que los aproximen, tales como  $3.14159$  y  $2.71828$ , y tomar el producto de estos últimos como una “aproximación” al verdadero producto. Para definir el producto de los dos números originales requerimos la noción de frontera. Lo mismo sucede con la suma.

### Suma de reales.

Dados  $\alpha \in \mathbf{R}$ ,  $\beta \in \mathbf{R}$ , sean

$$\begin{aligned}\mathcal{A} &= \{x \mid x \in \mathbf{D}, x \leq \alpha\} \\ \mathcal{B} &= \{x \mid x \in \mathbf{D}, x \leq \beta\} \\ \mathcal{C} &= \{x + y \mid x \in \mathcal{A}, y \in \mathcal{B}\}.\end{aligned}$$

Definimos

$$\alpha + \beta = \sup \mathcal{C}.$$

Pero esta no es una definición a menos que comprobemos que  $\mathcal{C}$  es acotado superiormente, lo que haremos en seguida.

Si  $\alpha = A \cdot a_1 a_2 \dots \in \mathbf{R}^+ \cup \{0\}$  es claro que  $\alpha < A + 1 \in \mathbf{D}$ . Si  $\alpha \in \mathbf{R}^-$ ,  $\alpha < 0 \in \mathbf{D}$ . En todo caso existe  $a \in \mathbf{D}$  tal que  $\alpha < a$ . De igual modo existe  $b \in \mathbf{D}$  tal que  $\beta < b$ . Tenemos entonces

$$x \in \mathcal{A} \Rightarrow x < a, \quad x \in \mathcal{B} \Rightarrow x < b.$$

Teniendo en cuenta que podemos sumar desigualdades del mismo sentido entre elementos de  $\mathbf{D}$  (proposición 8 del párrafo 1), vemos que

$$(x \in \mathcal{A}, y \in \mathcal{B}) \Rightarrow x + y < a + b,$$

lo que muestra que  $a + b$  es una cota superior de  $\mathcal{C}$ .

**Producto de reales positivos.** Dados  $\alpha \in \mathbf{R}^+$ ,  $\beta \in \mathbf{R}^+$ , sean

$$\begin{aligned}\mathcal{D} &= \{x \mid x \in \mathbf{D}, 0 \leq x \leq \alpha\} \\ \mathcal{E} &= \{x \mid x \in \mathbf{D}, 0 \leq x \leq \beta\} \\ \mathcal{F} &= \{xy \mid x \in \mathcal{D}, y \in \mathcal{E}\}.\end{aligned}$$

Definimos

$$\alpha\beta = \sup \mathcal{F}.$$

Lo mismo que en el caso de la suma debemos comprobar que  $\mathcal{F}$  es acotado superiormente para poder hablar de  $\sup \mathcal{F}$ .

**Producto de reales cualesquiera.** Dados  $\alpha \in \mathbf{R}^+$ ,  $\beta \in \mathbf{R}^+$ , definimos

$$\left. \begin{array}{l} (-\alpha)\beta = \alpha(-\beta) = -\alpha\beta \\ (-\alpha)(-\beta) = \alpha\beta \\ 0 \cdot \alpha = 0 \cdot (-\alpha) = (-\alpha) \cdot 0 = \alpha \cdot 0 = 0 \cdot 0 = 0 \end{array} \right\} \text{(Regla de los signos)}$$

**NOTA:** Si  $\alpha$  y  $\beta$  son elementos de  $\mathbf{D}$  podemos pensar en la posibilidad de que su suma, definida como  $\sup \mathcal{C}$  al considerarlos como elementos de  $\mathbf{R}$ , no coincida con la suma definida en el párrafo 1 para racionales. Pero esto no sucede, sino que podemos demostrar que

$$\alpha + \beta = \sup \mathcal{C}$$

donde la suma del primer miembro es la definida en el párrafo 1. En efecto,

$$\begin{aligned} \alpha \in \mathcal{A} &= \{x \mid x \in \mathbf{D}, x \leq \alpha\} \\ \beta \in \mathcal{B} &= \{x \mid x \in \mathbf{D}, x \leq \beta\} \\ \alpha + \beta \in \mathcal{C} &= \{x + y \mid x \in \mathcal{A}, y \in \mathcal{B}\}. \end{aligned}$$

Como  $\alpha$  es cota superior de  $\mathcal{A}$  y  $\beta$  es cota superior de  $\mathcal{B}$  sabemos que  $\alpha + \beta$  es cota superior de  $\mathcal{C}$  [proposición 8 inciso (i) del párrafo 1]. Como  $\alpha + \beta \in \mathcal{C}$  es claro que  $\alpha + \beta = \sup \mathcal{C}$ .

De manera parecida podemos comprobar que  $\alpha\beta = \sup \mathcal{J}$ , para  $\alpha \in \mathbf{D}^+$ ,  $\beta \in \mathbf{D}^+$ . Esto significa que el producto que se ha definido en  $\mathbf{R}^+$  se extiende al que estaba definido en  $\mathbf{D}^+$ . Como ese producto se extiende a  $\mathbf{R}$  de acuerdo con la regla de los signos y dicha regla es válida en  $\mathbf{D}$  vemos que el producto definido en  $\mathbf{R}$  es una extensión del producto definido en  $\mathbf{D}$  en el párrafo 1.

## 5. PROPIEDADES DE LA SUMA, EL PRODUCTO Y EL ORDEN EN $\mathbf{R}$

En este párrafo se demuestran las propiedades básicas de  $\mathbf{R}$ . Para demostrarlas usaremos libremente las propiedades de  $\mathbf{Q}$  demostradas en el párrafo 1, todas ellas válidas en  $\mathbf{D}$ , con la excepción de la que se refiere a la existencia de inversos multiplicativos. También usaremos con mucha frecuencia las proposiciones 1 y 2 del párrafo 2 y, claro está, deberemos tener presentes las definiciones de orden (párrafo 2) y de suma y producto (párrafo 4). Además, utilizaremos en varias ocasiones el lema siguiente:

**LEMA 1.**

$$-10^{-n} < \alpha < 10^{-n} \text{ para todo } n \geq 0 \Rightarrow \alpha = 0.$$

*Demostración:* Supongamos  $\alpha \neq 0$ . Tendremos

$$\alpha = A \cdot a_1 a_2 \dots$$

Supongamos  $\alpha \in \mathbf{R}^+$ . Si  $A \neq 0$  es claro que  $\alpha \geq 10^0 = 1$ . Si  $A = 0$  existirá  $n$  tal que  $a_1 = \dots = a_{n-1} = 0$ ,  $a_n \neq 0$ , y entonces  $\alpha \geq 10^{-n}$ . Supongamos ahora que  $\alpha \in \mathbf{R}^-$ . Si  $A \neq 0$  es claro que  $\alpha < -10^0 = -1$ . Si  $A = 0$  existirá  $n$  tal que  $a_1 = \dots = a_{n-1} = 0$  y  $a_n \neq 0$ , y entonces  $\alpha \leq -10^{-n}$ .

PROPOSICIÓN 1. En  $\mathbf{R}$ :

- i)  $(\alpha > \alpha' \text{ y } \beta > \beta') \Rightarrow \alpha + \beta > \alpha' + \beta'$ ;
- ii)  $\alpha > \alpha' \Rightarrow \alpha + \beta > \alpha' + \beta$ ;
- iii)  $(\alpha > \alpha' \geq 0 \text{ y } \beta > \beta' \geq 0) \Rightarrow \alpha\beta > \alpha'\beta'$ ;
- iv)  $(\alpha > \alpha' \text{ y } \beta > 0) \Rightarrow \alpha\beta > \alpha'\beta$ .

*Demostración:*

a) Sea  $c_1 \in \mathbf{D}$  tal que  $\alpha > c_1 > \beta$ . Sea  $c'_1 \in \mathbf{D}$  tal que  $c_1 > c'_1 > \beta$ . Entonces

$$\alpha > c_1 > c'_1 > \beta$$

Sean  $c_2$  y  $c'_2$  en  $\mathbf{D}$  tales que

$$\beta > c_2 > c'_2 > \beta$$

Sean

$$\begin{aligned}\mathcal{A} &= \{x | x \in \mathbf{D}, x \leq \alpha\} \\ \mathcal{B} &= \{x | x \in \mathbf{D}, x \leq \beta\} \\ \mathcal{A}' &= \{x | x \in \mathbf{D}, x \leq \alpha'\} \\ \mathcal{B}' &= \{x | x \in \mathbf{D}, x \leq \beta'\} \\ \mathcal{C} &= \{x+y | x \in \mathcal{A}, y \in \mathcal{B}\} \\ \mathcal{C}' &= \{x+y | x \in \mathcal{A}', y \in \mathcal{B}'\}.\end{aligned}$$

Entonces, por definición,

$$\begin{aligned}\alpha + \beta &= \sup \mathcal{C} \\ \alpha' + \beta' &= \sup \mathcal{C}'\end{aligned}$$

Ahora bien,

$$\begin{aligned}c_1 + c_2 &\in \mathcal{C}, \text{ de donde } \sup \mathcal{C} \geq c_1 + c_2 > c'_1 + c'_2 \\ c'_1 &> \alpha' \geq x \text{ para todo } x \in \mathcal{A}' \\ c'_2 &> \beta' \geq y \text{ para todo } y \in \mathcal{B}'\end{aligned}$$

de donde  $c'_1 + c'_2 \geq \sup \mathcal{C}'$ .

Por lo tanto

$$\alpha + \beta = \sup C \geq c_1 + c_2 > c'_1 + c'_2 \geq \sup C' = \alpha' + \beta'$$

b) Sean  $c$  y  $c'$  en  $\mathbf{D}$  tales que

$$\alpha > c > c' > \alpha'.$$

Sea  $n$  tal que  $c - c' > 10^{-n}$  y sea  $b \in \mathbf{D}$  tal que

$$b < \beta < b + 10^{-n}.$$

Entonces, por (a),

$$\alpha + \beta > b + c = b + (c - c') + c' > (b + 10^{-n}) + c' > \alpha' + \beta.$$

c) Si  $\alpha' = 0$  o  $\beta' = 0$  la afirmación es obvia. En caso contrario la demostración es muy parecida a la de (i), usando la definición de producto de reales positivos.

d) Lo demostrarímos para el caso  $\alpha' > 0$  y el lector completará la demostración.

Sean  $c$  y  $c'$  en  $\mathbf{D}$  tales que

$$\alpha > c > c' > \alpha'.$$

Sea  $n$  tal que  $c - c' > 10^{-n}$ .

Sea  $N$  entero positivo tal que  $10^{-N} < \beta$ . Existe un entero positivo  $m > N + 1$  tal que  $10^{m-N-n-1} > c'$ .

Sea  $b \in \mathbf{D}$  tal que

$$0 < b < \beta < b + 10^{-m}.$$

Entonces

$$b > 10^{-N-1},$$

porque en caso contrario se tendría  $b \leq 10^{-N-1}$  y

$$b + 10^{-m} \leq 10^{-N-1} + 10^{-m} < 10^{-N-1} + 10^{-N-1} < 10^{-N} < \beta$$

que es una contradicción.

Tenemos entonces

$$\begin{aligned} \alpha\beta &> bc = (b + 10^{-m})c' + b(c - c') - 10^{-m}c' \\ &> (b + 10^{-m})c' + 10^{-n}b - 10^{-m}c' \\ &> (b + 10^{-m})c' + 10^{-N-n-1} - 10^{-m}c' \\ &= (b + 10^{-m})c' + 10^{-m}(10^{-m-N-n-1} - c') \\ &> (b + 10^{-m})c' > \alpha'\beta. \end{aligned}$$

**PROPOSICIÓN 2:** La suma en **R** es conmutativa.

Es consecuencia inmediata de la definición de suma y de la conmutatividad de la suma en **D**.

**PROPOSICIÓN 3:** La suma en **R** es asociativa.

*Demostración.* Dados  $\alpha, \beta$  y  $\gamma$ , existen, para cada natural  $n$ , elementos  $a, b$  y  $c$  en **D** tales que

$$a < \alpha < a + 10^{-n-1}, \quad b < \beta < b + 10^{-n-1}, \quad c < \gamma < c + 10^{-n-1}.$$

Entonces

$$\begin{aligned} a + b &< \alpha + \beta < a + b + 2 \times 10^{-n-1} \\ a + b + c &< (\alpha + \beta) + \gamma < a + b + c + 3 \times 10^{-n-1} \end{aligned} \quad (1)$$

$$\begin{aligned} b + c &< \beta + \gamma < b + c + 2 \times 10^{-n-1} \\ a + b + c &< \alpha + (\beta + \gamma) < a + b + c + 3 \times 10^{-n-1}. \end{aligned} \quad (2)$$

Supongamos por un momento que  $(\alpha + \beta) + \gamma \neq \alpha + (\beta + \gamma)$ ; por ejemplo que la primera suma es mayor que la segunda. Entonces habrán elementos  $d_1$  y  $d_2$  de **D** tales que  $\alpha + (\beta + \gamma) < d_1 < d_2 < (\alpha + \beta) + \gamma$ . Usando (1) y (2),

$$a + b + c < d_1 < d_2 < a + b + c + 3 \times 10^{-n-1},$$

de donde

$$\begin{aligned} a + b + c &< d_1 < a + b + c + 10^{-n} \\ -(a + b + c + 10^{-n}) &< -d_2 < -(a + b + c) \\ -10^{-n} &< d_1 - d_2 < 10^{-n} \text{ para todo } n, \end{aligned}$$

lo que implica  $d_1 = d_2$ , en contradicción con  $d_1 < d_2$ .

**PROPOSICIÓN 4:**  $\alpha + 0 = \alpha$  para todo  $\alpha \in \mathbf{R}$ .

*Demostración.* Para cada  $n$  existe  $a \in \mathbf{D}$  tal que

$$a < \alpha < a + 10^{-n}.$$

Por la proposición 1, inciso (ii),

$$\alpha = \alpha + 0 < \alpha + 0 < a + 10^{-n} + 0 = a + 10^{-n}.$$

Si se tuviera  $\alpha \neq \alpha + 0$ , por ejemplo  $\alpha < \alpha + 0$ , existirían  $d_1$  y  $d_2$  en **D** tales que

$$a < \alpha < d_1 < d_2 < \alpha + 0 < a + 10^{-n},$$

de donde

$$\begin{aligned} a &< d_1 < a + 10^{-n} \\ -(a + 10^{-n}) &< -d_2 < -a \end{aligned}$$

y finalmente,

$$-10^{-n} < d_1 - d_2 < 10^{-n}$$

para todo  $n$ , lo que da una contradicción.

**PROPOSICIÓN 5:**  $A \cdot a_1 a_2 \dots + (-A \cdot a_1 a_2 \dots) = 0$ .

*Demostración.* Para cada  $n$  existe  $a \in \mathbf{D}^+$  tal que

$$a < A \cdot a_1 a_2 \dots < a + 10^{-n}.$$

Por la definición del orden en  $\mathbf{R}$  tenemos

$$-(a + 10^{-n}) < -A \cdot a_1 a_2 \dots < -a.$$

Por la proposición 1,

$$-10^{-n} < A \cdot a_1 a_2 \dots + (-A \cdot a_1 a_2 \dots) < 10^{-n}$$

para todo  $n$ , lo que implica la proposición.

**COROLARIO 1:** Todo real tiene un inverso aditivo que es único.

En efecto, todo real positivo es de la forma  $A \cdot a_1 a_2 \dots$  y tiene a  $-A \cdot a_1 a_2 \dots$  por inverso. Todo real negativo  $-A \cdot a_1 a_2 \dots$  tiene al real  $A \cdot a_1 a_2 \dots$  por inverso. El real 0 tiene a 0 por inverso, según la proposición 4.

La unicidad se comprueba como sigue: Si  $\alpha'$  y  $\alpha''$  son inversos de  $\alpha$  tenemos  $\alpha + \alpha' = 0$  y  $\alpha + \alpha'' = 0$ , de donde

$$\begin{aligned} \alpha + \alpha' &= \alpha + \alpha'' \\ \alpha' + (\alpha + \alpha') &= \alpha' + (\alpha + \alpha'') \\ (\alpha' + \alpha) + \alpha' &= (\alpha' + \alpha) + \alpha'' \\ 0 + \alpha' &= 0 + \alpha'' \\ \alpha' &= \alpha''. \end{aligned}$$

**Notación.** El inverso de  $A \cdot a_1 a_2 \dots$  es  $-A \cdot a_1 a_2 \dots$ . Extendemos esta notación escribiendo  $-\alpha$  para denotar al inverso de  $\alpha$ . Así tendremos

$$\begin{aligned} -(-A \cdot a_1 a_2 \dots) &= A \cdot a_1 a_2 \dots \\ -0 &= 0 \\ -(-\alpha) &= \alpha. \end{aligned}$$

**PROPOSICIÓN 6:**  $\alpha > \beta \iff \alpha + (-\beta) \in \mathbf{R}^+$ .

*Demostración.* Observemos que  $\gamma > 0$  equivale a  $\gamma \in \mathbf{R}^+$ . Entonces

$$\alpha > \beta \implies \alpha + (-\beta) > \beta + (-\beta) = 0 \implies \alpha = \alpha + (-\beta) + \beta > \beta.$$

**PROPOSICIÓN 7:**  $\alpha > \beta \iff -\beta > -\alpha$ .

*Demostración:*

$$\alpha > \beta \iff \alpha + (-\beta) > 0 \iff -\beta + (-(-\alpha)) > 0 \iff -\beta > -\alpha.$$

**PROPOSICIÓN 8:** El producto en  $\mathbf{R}$  es conmutativo.

*Demostración.* Para reales positivos es consecuencia inmediata de la definición de producto de reales y de la conmutatividad del producto en  $\mathbf{D}$ . Si  $\alpha$  y  $\beta$  son reales positivos tenemos, por la regla de los signos,

$$\begin{aligned} (-\alpha)\beta &= -(\alpha\beta) = -(\beta\alpha) = \beta(-\alpha) \\ \alpha(-\beta) &= -(\alpha\beta) = -(\beta\alpha) = (-\beta)\alpha \\ (-\alpha)(-\beta) &= \alpha\beta = \beta\alpha = (-\beta)(-\alpha). \end{aligned}$$

Además,  $0 \cdot \alpha = 0 = \alpha \cdot 0$  para todo  $\alpha \in \mathbf{R}$ .

**PROPOSICIÓN 9:** El producto en  $\mathbf{R}$  es asociativo.

*Demostración.* Lo demostrarímos para reales positivos. La demostración se puede completar usando la regla de los signos. Sean  $\alpha$ ,  $\beta$  y  $\gamma$  positivos,

$$\begin{aligned} \alpha &= A \cdot a_1 a_2 \dots \\ \beta &= B \cdot b_1 b_2 \dots \\ \gamma &= C \cdot c_1 c_2 \dots \end{aligned}$$

Sea  $N$  un natural mayor que  $A$ ,  $B$  y  $C$ , que será mayor que  $\alpha$ ,  $\beta$  y  $\gamma$ . Para cada entero positivo  $n$  sean  $a$ ,  $b$  y  $c$  en  $\mathbf{D}$  tales que

$$\begin{aligned} 0 < a < \alpha < a + 10^{-n} \\ 0 < b < \beta < b + 10^{-n} \\ 0 < c < \gamma < c + 10^{-n}. \end{aligned}$$

Tenemos

$$\begin{aligned} ab &< \alpha\beta < ab + 10^{-n}(a+b) \\ abc &< (\alpha\beta)\gamma < abc + 10^{-n}(ab+ac+bc) + 10^{-2n}(a+b+c) \quad (1) \end{aligned}$$

$$\begin{aligned} bc &< \beta\gamma < bc + 10^{-n}(b+c) \\ abc &< \alpha(\beta\gamma) < abc + 10^{-n}(ab+ac+bc) + 10^{-2n}(a+b+c). \quad (2) \end{aligned}$$

Observemos que

$$10^{-n}(ab+ac+bc) + 10^{-2n}(a+b+c) < 10^{-n} \times 3(N^2+N) < 10^{m-n}$$

para un  $m$  suficientemente grande.

De (1) concluimos

$$abc < (\alpha\beta)\gamma < abc + 10^{m-n}.$$

De (2) y la proposición 7 concluimos

$$-(abc + 10^{m-n}) < -\alpha(\beta\gamma) < -abc.$$

De las dos últimas series de desigualdades:

$$-10^{m-n} < (\alpha\beta)\gamma + (-\alpha(\beta\gamma)) < 10^{m-n},$$

para todo  $n$ , lo que implica que

$$(\alpha\beta)\gamma + (-\alpha(\beta\gamma)) = 0.$$

Por la unicidad del inverso aditivo tendremos

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

**PROPOSICIÓN 10:**  $\alpha \cdot 1 = \alpha$  para todo  $\alpha \in \mathbf{R}$ .

*Demuestração.* Para cada  $n \in \mathbf{Z}^+$  existe  $a \in \mathbf{D}$  tal que  $a < \alpha < a + 10^{-n}$ . Por el inciso (iv) de la proposición 1,

$$a = a \cdot 1 < \alpha \cdot 1 < (a + 10^{-n}) \times 1 = a + 10^{-n},$$

de donde

$$-(a + 10^{-n}) < -\alpha \cdot 1 < -a$$

y

$$10^{-n} < \alpha + (-\alpha \cdot 1) < 10^{-n}$$

para todo  $n$ , de donde  $\alpha = \alpha \cdot 1$ .

**PROPOSICIÓN 11:**  $(-1) \alpha = -\alpha$ .

*Demuestração.*

Si  $\alpha = A \cdot a_1 a_2 \dots$ ,

$$(-1) \alpha = -A \cdot a_1 a_2 \dots = -\alpha,$$

por la regla de los signos.

Si  $\alpha = 0$ ,  $(-1)\alpha = (-1) \cdot 0 = 0 = \alpha$ .

Si  $\alpha = -A \cdot a_1 a_2 \dots$ ,

$$(-1)\alpha = A \cdot a_1 a_2 \dots = -\alpha.$$

**LEMÁ 2.**  $(-1)(\alpha + \beta) = (-1)\alpha + (-1)\beta$ .

*Demuestração.* Es claro que  $-(\alpha + \beta) = (-\alpha) + (-\beta)$ , puesto que  $[(-\alpha) + (-\beta)] + (\alpha + \beta) = ((-\alpha) + \alpha) + ((-\beta) + \beta) = 0 + 0 = 0$ .

Por la proposición anterior

$$(-1)(\alpha + \beta) = -(\alpha + \beta) = (-\alpha) + (-\beta) = (-1)\alpha + (-1)\beta.$$

**PROPOSICIÓN 12:** El producto distribuye a la suma en  $\mathbf{R}$ .

*Demuestração.* Si uno de los reales  $\alpha, \beta, \gamma$  es cero es fácil verificar que  $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ . Supondremos que  $\alpha \neq 0, \beta \neq 0, \gamma \neq 0$ .

a) Si  $\alpha > 0, \beta > 0$  y  $\gamma > 0$ . Tomemos  $a, b, c \in \mathbf{D}$  tales que

$$\begin{aligned} 0 < a < \alpha < a + 10^{-n} \\ 0 < b < \beta < b + 10^{-n} \\ 0 < c < \gamma < c + 10^{-n}. \end{aligned}$$

De estas desigualdades podemos deducir

$$\begin{aligned} -10^{-n}(2a+b+c+2 \times 10^{-n}) &< -\alpha(\beta+\gamma) + (\alpha\beta+\alpha\gamma) \\ &< 10^{-n}(2a+b+c+2 \times 10^{-n}). \end{aligned}$$

Pero

$$2a+b+c+2 \times 10^{-n} < 2\alpha+\beta+\gamma+1 < 10^N$$

para algún  $N$ , de donde

$$-10^{-n+N} < -\alpha(\beta+\gamma) + (\alpha\beta+\alpha\gamma) < 10^{-n+N}$$

para todo  $n$ , que implica que  $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$ .

b) Si  $\alpha < 0, \beta > 0, \gamma > 0$ . Entonces

$$\alpha(\beta+\gamma) = (-(-\alpha))(\beta+\gamma) = (-1)(-\alpha)(\beta+\gamma).$$

Como  $-\alpha \in \mathbf{R}^+$  tenemos, por (a),

$(-\alpha)(\beta+\gamma) = (-\alpha)\beta + (-\alpha)\gamma = (-1)\alpha\beta + (-1)\alpha\gamma = (-1)(\alpha\beta + \alpha\gamma)$ ,  
de donde

$$\alpha(\beta+\gamma) = (-1)^2(\alpha\beta + \alpha\gamma) = \alpha\beta + \alpha\gamma.$$

c) Si  $\beta < 0$  y  $\gamma < 0$ ,  $\alpha$  cualquiera:

$$\begin{aligned}\alpha(\beta + \gamma) &= (-1)\alpha(-1)(\beta + \gamma) = (-1)\alpha((-1)\beta + (-1)\gamma) \\ &= (-1)^2\alpha\beta + (-1)^2\alpha\gamma = \alpha\beta + \alpha\gamma.\end{aligned}$$

d) Hemos tratado todos los casos posibles en que  $\beta$  y  $\gamma$  tienen el mismo signo. Supongamos ahora que tienen signo contrario, por ejemplo  $\beta > 0$  y  $\gamma = -\gamma' < 0$ . Hay dos casos:

d') Si  $\beta \geq \gamma'$ . Entonces  $\beta + (-\gamma') \geq 0$

$$\alpha\beta = \alpha((\beta + (-\gamma')) + \gamma') = \alpha(\beta + (-\gamma')) + \alpha\gamma',$$

de donde

$$\begin{aligned}\alpha\beta + (-\alpha\gamma') &= \alpha(\beta + (-\gamma')) \\ \alpha\beta + (-1)\alpha\gamma' &= \alpha(\beta + \gamma) \\ \alpha\beta + \alpha\gamma &= \alpha(\beta + \gamma).\end{aligned}$$

d'') Si  $\beta < \gamma'$ . Queda como ejercicio.

**PROPOSICIÓN 13:** Todo real no nulo tiene inverso multiplicativo, que es único.

*Demuestração.* Supongamos primero que  $\alpha > 0$ . Sea

$$\mathcal{R}' = \{x | x \in \mathbf{D}^+, x\alpha \leq 1\}.$$

Demostraremos que  $\alpha \sup \mathcal{R}' = 1$ . Sean

$$\begin{aligned}\alpha &= A \cdot a_1 a_2 \dots \\ \sup \mathcal{R}' &= A' \cdot a'_1 a'_2 \dots\end{aligned}$$

Para cada entero positivo  $n$  existe  $b \in \mathcal{R}'$  tal que

$$b = A' \cdot a'_1 \dots a'_n b_{n+1} \dots$$

Entonces

$$\begin{aligned}A' \cdot a'_1 \dots a'_n \times \alpha &\leq b\alpha \leq 1 < (A \cdot a_1 \dots a_n + 10^{-n})\alpha, \\ A' \cdot a'_1 \dots a'_n \times \alpha &\leq \sup \mathcal{R}' \cdot \alpha \leq (A \cdot a_1 \dots a_n + 10^{-n})\alpha,\end{aligned}$$

de donde

$$-10^{-n}(A' + 1) < 1 - \sup \mathcal{R}' \cdot \alpha < 10^{-n}(A' + 1)$$

para todo  $n$ , lo que implica que  $1 = \sup \mathcal{R}' \cdot \alpha$ .

Para el real negativo  $-\alpha$  tenemos

$$(-\alpha)(-\sup \mathcal{A}') = \alpha \sup \mathcal{A}' = 1.$$

Falta demostrar la unicidad.

OBSERVACIÓN.  $\alpha \in \mathbf{R}^+ \iff \alpha^{-1} \in \mathbf{R}^+$ .

RESUMEN: Las proposiciones 2, 3, 4, el corolario 1 y las proposiciones 8, 9, 10, 12 y 13 muestran que  $\mathbf{R}$  es un campo.

La proposición 6 muestra que el orden en  $\mathbf{R}$ , que originalmente (párrafo 2) se habría definido lexicográficamente, es el orden determinado por  $\mathbf{R}^+$ . Es decir,

$$\alpha > \beta \text{ si } \alpha - \beta \in \mathbf{R}^+.$$

Esta proposición, junto con los incisos (i) y (iii) de la proposición 1, nos muestra que sumas y productos de elementos de  $\mathbf{R}^+$  pertenecen a  $\mathbf{R}^+$ .

De la proposición 5 se deduce la tricotomía: una y sólo una de las afirmaciones

$$\alpha \in \mathbf{R}^+, \alpha = 0, -\alpha \in \mathbf{R}^+$$

es verdadera.

La otra propiedad importante de  $\mathbf{R}$  es la existencia de fronteras de conjuntos acotados, demostrada en el párrafo 3.

## 6. RACIONALES Y REALES

Recordemos que  $\mathbf{Z} \subset \mathbf{D} \subset \mathbf{R}$ . Veremos cómo identificar  $\mathbf{Q}$  con una parte de  $\mathbf{R}$ , con lo que tendremos  $\mathbf{Z} \subset \mathbf{D} \subset \mathbf{Q} \subset \mathbf{R}$ .

Definimos

$$j : \mathbf{Q} \rightarrow \mathbf{R}$$

como

$$j\left(\frac{a}{b}\right) = ab^{-1}$$

$j$  está bien definida porque

$$\frac{a}{b} = \frac{c}{d} \implies ad = bc \implies ad(bd)^{-1} = bc(bd)^{-1} \implies ab^{-1} = cd^{-1}.$$

Observamos:

a)  $j$  es inyectiva:

$$\begin{aligned} j\left(\frac{a}{b}\right) = j\left(\frac{c}{d}\right) &\implies ab^{-1} = cd^{-1} \implies ad = bc \\ &\implies \frac{a}{b} = \frac{c}{d}. \end{aligned}$$

b)  $j$  preserva sumas:

$$\begin{aligned} j\left(\frac{a}{b}\right) + j\left(\frac{c}{d}\right) &= ab^{-1} + cd^{-1} = (ad+bc)(bd)^{-1} \\ &= j\left(\frac{ad+bc}{bd}\right) \\ &= j\left(\frac{a}{b} + \frac{c}{d}\right); \end{aligned}$$

c)  $j$  preserva productos:

$$\begin{aligned} j\left(\frac{a}{b}\right) \cdot j\left(\frac{c}{d}\right) &= (ab^{-1})(cd^{-1}) = ac(bd)^{-1} = j\left(\frac{ac}{bd}\right) \\ &= j\left(\frac{a}{b} \cdot \frac{c}{d}\right); \end{aligned}$$

d)  $j$  preserva el orden:

$$\begin{aligned} j\left(\frac{a}{b}\right) > j\left(\frac{c}{d}\right) &\iff ab^{-1} > cd^{-1} \iff ab^{-1} - cd^{-1} \in \mathbf{R}^+ \\ &\iff (ad-bc)(bd)^{-1} \in \mathbf{R}^+ \\ &\iff (ad-bc)(bd) \in \mathbf{R}^+ \\ &\iff \frac{ad-bc}{bd} \in \mathbf{Q}^+ \iff \frac{a}{b} - \frac{c}{d} \in \mathbf{Q}^+ \\ &\iff \frac{a}{b} > \frac{c}{d}. \end{aligned}$$

Identificamos  $\mathbf{Q}$  con  $j(\mathbf{Q})$  y admitimos, para reales  $\beta \neq 0$  y  $\alpha$ , la notación

$$\frac{\alpha}{\beta} = \alpha\beta^{-1}.$$

El lector puede demostrar las fórmulas

$$\frac{\alpha}{\beta} = \frac{\alpha\gamma}{\beta\gamma} \text{ para } \gamma \neq 0$$

$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \beta\gamma}{\beta\delta}$$

$$\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta}$$

NOTA: La proposición 1 del párrafo 2 afirma que entre cada dos reales hay un racional. Esto se suele expresar con la frase

$$\mathbf{Q} \text{ es denso en } \mathbf{R}.$$

**Representación decimal de los racionales.** El problema que abordamos es el de encontrar, dados los enteros positivos  $m$  y  $n$ , el entero  $A$  y las cifras decimales  $a_i$  tales que

$$A.a_1a_2\dots = \frac{m}{n}.$$

El procedimiento es simple. Consiste en dividir  $m$  entre  $n$  por el algoritmo bien conocido de la división con decimales. Como ejemplo, obtengamos la expresión decimal de  $3/7$ :

$$\begin{array}{r} 0.42857142\dots \\ \hline 7 / 3 \\ 30 \\ 20 \\ 60 \\ 40 \\ 50 \\ 10 \\ 30 \\ 20 \\ 6 \\ \dots \\ \dots \\ \dots \end{array}$$

Afirmamos que

$$\frac{3}{7} = 0.42857142\dots$$

Justificaremos esta afirmación.

Al dividir  $m$  entre  $n$  obtenemos un cociente  $A \cdot a_1a_2\dots$ . El entero  $A$  y las cifras  $a_i$  se van obteniendo de manera que se cumplan las desigualdades

$$\begin{aligned} nA &\leq m < n(A+1) \\ n \times A \cdot a_1 &\leq m < n(A \cdot a_1 + 10^{-1}) \\ n \times A \cdot a_1a_2 &\leq m < n(A \cdot a_1a_2 + 10^{-2}). \end{aligned}$$

$$\begin{array}{c} \dots \\ \dots \\ \dots \end{array}$$

De estas desigualdades obtenemos

$$\begin{aligned} 0 &\leq m - nA < n \\ 0 &\leq m - n \times A \cdot a_1 < 10^{-1} n \\ 0 &\leq m - n \times A \cdot a_1 a_2 < 10^{-2} n \end{aligned}$$

. . . . .  
. . . . .  
. . . . .

o bien

$$\begin{aligned} 0 &\leq \frac{m}{n} - A < 1 \\ 0 &\leq \frac{m}{n} - A \cdot a_1 < 10^{-1} \\ 0 &\leq \frac{m}{n} - A \cdot a_1 a_2 < 10^{-2}. \end{aligned}$$

. . . . .  
. . . . .  
. . . . .

Supóngase que

$$\frac{m}{n} = B.b_1 b_2 \dots$$

De las desigualdades anteriores concluimos sucesivamente que  $B = A$ ,  $b_i = a_i$  para  $i = 1, 2, \dots$ , lo que muestra que  $m/n = A \cdot a_1 a_2 \dots$ , como se quería.

**Decimales periódicos y números racionales.** Al calcular  $3/7$  hemos podido observar que el decimal que se obtiene es “periódico”:

$$\frac{3}{7} = 0.428571428571428571\dots$$

Si calculamos las expresiones decimales de otros racionales encontraremos siempre el mismo fenómeno:

$$\frac{8}{3} = 2.66666\dots$$

$$\frac{2}{5} = 0.400000\dots$$

$$\frac{5561}{4950} = 1.12343434\dots$$

Usaremos una notación que describiremos con ejemplos:

$$35.78128198173737373\dots = 35.781281981\overbrace{73}$$

$$0.35555\dots = 0.\overline{35}$$

$$12312.3123123123123\dots = 12312.\overbrace{312}.$$

A los reales de este tipo les llamaremos periódicos.

De acuerdo con la notación,

$$\frac{3}{7} = 0.\overbrace{428571}$$

$$\frac{8}{3} = 2.\widehat{6}$$

$$\frac{2}{5} = 0.4$$

$$\frac{5561}{4950} = 1.12\overbrace{34}.$$

**PROPOSICIÓN 1:** Un real es periódico si y solo si es racional.

*Demostración.* Dividamos  $m$  entre  $n$ . Cuando entramos en la parte decimal del cociente los restos que van apareciendo son siempre menores que  $n$ . Como solo hay un número finito de enteros no negativos menores que  $n$  debe suceder que, o bien uno de los restos es cero, en cuyo caso todas las cifras decimales que siguen son cero, o bien un resto se repite. Cuando sucede esto todas las cifras decimales que se obtuvieron a partir del momento en que apareció por primera vez este resto (dentro del cálculo de la parte decimal) se repiten en el mismo orden, así como los restos, y la división se convierte en la repetición exacta de un mismo proceso, obteniéndose un decimal periódico.

Supongamos ahora que

$$\alpha = A \cdot a_1 \dots a_m \overbrace{a_{m+1} \dots a_n}.$$

Queremos demostrar que  $\alpha \in \mathbf{Q}$ . Para ello necesitamos un resultado auxiliar.

**LEMA:** Multiplicar por 10 un elemento de  $\mathbf{R}$  equivale a correr el punto decimal un lugar hacia la derecha.

La afirmación es obvia para elementos de  $\mathbf{D}$  pero no lo es para elementos de  $\mathbf{R}$ , aunque no es difícil de demostrar. La demostración se deja como ejercicio.

Aplicando el lema tenemos

$$\begin{aligned} 10^m \alpha &= 10^m A + 10^{m-1} a_1 + \dots + 10 a_{m-1} + a_m + 0 \cdot \overbrace{a_{m+1} \dots a_n} \\ 10^n \alpha &= 10^n A + 10^{n-1} a_1 + \dots + 10 a_{n-1} + a_n + 0 \cdot \overbrace{a_{n+1} \dots a_n} \\ (10^n - 10^m) \alpha &= 10^n A + 10^{n-1} a_1 + \dots + a_n - (10^m A + 10^{m-1} a_1 + \dots + a_m) \\ &= B \in \mathbf{Z} \\ \alpha &= \frac{B}{10^n - 10^m} \in \mathbf{Q}. \end{aligned}$$

## 7. RAÍCES DE REALES POSITIVOS. EXPONENTES FRACCIONARIOS

**TEOREMA 1:** Para cada  $\alpha \in \mathbf{R}^+$  y cada  $n \in \mathbf{Z}^+$  existe un único  $\beta \in \mathbf{R}^+$  tal que  $\beta^n = \alpha$ . Este real  $\beta$  se denota por  $\sqrt[n]{\alpha}$ .

*Demostración.* Sea

$$\beta = \sup \{x | x \in \mathbf{R}, x^n < \alpha\}.$$

Veremos que  $\beta^n = \alpha$ .

Sea  $\beta = B.b_1 b_2 \dots$

Para cada  $r \in \mathbf{Z}^+$  hay un índice  $m \geq r$  tal que  $b_m \neq 9$ . Sea  $b_m^* = b_m + 1$ .

Si revisamos la demostración del teorema de existencia de fronteras superiores (sección 3), recordaremos que hay una cota superior del conjunto

$$\mathcal{B} = \{x | x \in \mathbf{R}^+, x^n < \alpha\},$$

que es de la forma  $B.b_1 \dots b_m b'_{m+1} b'_{m+2} \dots$ . Entonces  $B.b_1 \dots b_{m-1} b_m^*$  es mayor que cualquier elemento de  $\mathcal{B}$  y, por lo tanto, no pertenece a  $\mathcal{B}$ , de donde

$$(B.b_1 \dots b_{m-1} b_m^*)^n \geq \alpha.$$

Podemos además suponer que el índice  $m$  es tan grande que  $\beta - 10^{-m} > 0$ . Es claro que  $\beta - 10^{-m}$ , por no ser cota superior de  $\mathcal{B}$ , debe ser menor que algún  $x$  tal que  $x^n < \alpha$ , de donde

$$(\beta - 10^{-m})^n < \alpha.$$

Tenemos entonces

$$(\beta + 10^{-r})^n \geq (\beta + 10^{-m})^n \geq (B.b_1 \dots b_{m-1} b_m^*)^n \geq \alpha > (\beta - 10^{-m})^n \geq (\beta - 10^{-r})^n,$$

En consecuencia para toda  $r \in \mathbb{Z}^+$ ,

$$(\beta + 10^{-r})^n \geq \alpha > (\beta - 10^{-r})^n.$$

Pero

$$\begin{aligned} (\beta + 10^{-r})^n &= \sum_{j=0}^n \binom{n}{j} \frac{\beta^{n-j}}{10^{jr}} \leq \beta^n + \frac{(\max(1, \beta))^{n-1}}{10^r} \sum_{j=1}^n \binom{n}{j} \\ &\leq \beta^n + \frac{(\max(1, \beta))^{n-1} 2^n}{10^r} \\ (\beta - 10^{-r})^n &\geq \beta^n - \frac{(\max(1, \beta))^{n-1} 2^n}{10^r}. \end{aligned}$$

Sea  $N$  tal que

$$10^N \geq \frac{(\max(1, \beta))^{n-1} 2^n}{10^r}$$

Entonces, para todo  $r$ ,

$$\beta^n + \frac{1}{10^{r-N}} \geq \alpha > \beta^n - \frac{1}{10^{r-N}},$$

o sea que

$$\frac{1}{10^r} \geq \alpha - \beta^n \geq -\frac{1}{10^r}$$

para todo  $r$ , lo que implica  $\alpha = \beta^n$ . La unicidad de  $\beta$  se comprueba fácilmente:

$$\begin{aligned} \beta' > \beta &\Rightarrow \beta'^n > \beta^n = \alpha \\ \beta > \beta' &\geq 0 \Rightarrow \alpha = \beta^n > \beta'^n. \end{aligned}$$

**Exponentes fraccionarios.** Para todo  $\alpha \in \mathbf{R} - \{0\}$  y  $n \in \mathbb{Z}^+$  definimos

$$\begin{aligned} \alpha^n &= \underbrace{\alpha \alpha \cdots \alpha}_{n \text{ factores}} \\ \alpha^{-n} &= (\alpha^n)^{-1}. \end{aligned}$$

Convenimos además en que

$$\alpha^0 = 1.$$

Es claro, para enteros  $m$  y  $n$ , que

$$\begin{aligned} \alpha^m \alpha^n &= \alpha^{m+n} \\ (\alpha^m)^n &= \alpha^{mn}. \end{aligned}$$

PROPOSICIÓN 1: Para  $\alpha, \beta \in \mathbf{R}^+$ ,  $n \in \mathbf{Z}^+$ ,  $m \in \mathbf{Z}$ ,

$$a) \sqrt[n]{\alpha} \sqrt[n]{\beta} = \sqrt[n]{\alpha \beta}$$

$$b) \sqrt[m]{\sqrt[n]{\alpha}} = \sqrt[mn]{\alpha}$$

$$c) (\sqrt[n]{\alpha})^m = \sqrt[n]{\alpha^m}$$

$$d) \sqrt[n]{\alpha^m} = \sqrt[s]{\alpha^r} \iff \frac{m}{n} = \frac{r}{s}$$

Demostración:

$$a) (\sqrt[n]{\alpha} \sqrt[n]{\beta})^n = (\sqrt[n]{\alpha})^n (\sqrt[n]{\beta})^n = \alpha \beta$$

$$b) (\sqrt[m]{\sqrt[n]{\alpha}})^{mn} = ((\sqrt[m]{\sqrt[n]{\alpha}})^m)^n = (\sqrt[n]{\alpha})^n = \alpha$$

$$c) ((\sqrt[n]{\alpha})^m)^n = ((\sqrt[n]{\alpha})^n)^m = \alpha^m$$

$$d) \sqrt[n]{\alpha^m} = \sqrt[s]{\alpha^r} \iff (\sqrt[n]{\alpha^m})^{ns} = (\sqrt[s]{\alpha^r})^{ns} \iff$$

$$\iff ((\sqrt[n]{\alpha^m})^s)^n = ((\sqrt[s]{\alpha^r})^s)^n \iff (\alpha^m)^s = (\alpha^r)^n$$

$$\iff \alpha^{ms} = \alpha^{rn} \iff \frac{m}{n} = \frac{r}{s}.$$

DEFINICIÓN 1: Para todo  $\alpha \in \mathbf{R}^+$  y  $m/n \in \mathbf{Q}$  tal que  $n \in \mathbf{Z}^+$ , definimos

$$\alpha^n = \sqrt[n]{\alpha^m} = (\sqrt[n]{\alpha})^m.$$

El inciso (d) de la proposición anterior muestra que la definición no depende de la manera en que se expresa  $m/n$ , siempre que el denominador sea positivo.

TEOREMA 2: Para  $\alpha, \beta \in \mathbf{R}^+$ ,  $m/n \in \mathbf{Q}$ ,  $r/s \in \mathbf{Q}$ ,  $n \in \mathbf{Z}^+$ ,  $s \in \mathbf{Z}^+$ :

$$a) \alpha^{m/n} \beta^{m/n} = (\alpha \beta)^{m/n}.$$

$$b) \alpha^{m/n} \alpha^{r/s} = \alpha^{m/n + r/s}.$$

$$c) (\alpha^{m/n})^{r/s} = \alpha^{m/n \cdot r/s}.$$

Demostración:

$$a) \alpha^{m/n} \beta^{m/n} = \sqrt[n]{\alpha^m} \sqrt[n]{\beta^m} = \sqrt[n]{\alpha^m \beta^m} = \sqrt[n]{(\alpha \beta)^m} = (\alpha \beta)^{m/n}.$$

$$b) \alpha^{m/n} \alpha^{r/s} = \alpha^{ms/ns} \alpha^{nr/ns} = \sqrt[ns]{\alpha^{ms}} \sqrt[ns]{\alpha^{nr}} \\ = \sqrt[ns]{\alpha^{ms+nr}} = \alpha^{(ms+nr)/ns} = \alpha^{m/n+r/s}.$$

$$c) (\alpha^{m/n})^{r/s} = (\sqrt[s]{\sqrt[n]{\alpha^m}})^r = (\sqrt[ns]{\alpha^m})^r = \\ = (\sqrt[ns]{\alpha})^{mr} = \alpha^{mr/ns} = \alpha^{m/n \cdot r/s}.$$

## 8. VALOR ABSOLUTO

Definimos el valor absoluto de un real  $\alpha$ , denotado por  $|\alpha|$ :

$$|\alpha| = \begin{cases} \alpha & \text{si } \alpha \geq 0 \\ -\alpha & \text{si } \alpha < 0. \end{cases}$$

Así que

$$\begin{aligned} |A.a_1a_2 \dots| &= A.a_1a_2 \dots \\ |-A.a_1a_2 \dots| &= A.a_1a_2 \dots \end{aligned}$$

OBSERVACIÓN:  $|- \alpha| = |\alpha|$ .

El valor absoluto tiene las propiedades siguientes:

- I.  $|\alpha| \geq 0$ , y  $|\alpha| = 0$  sólo si  $\alpha = 0$
- II.  $|\alpha\beta| = |\alpha| |\beta|$
- III.  $|\alpha + \beta| \leq |\alpha| + |\beta|$ .

La propiedad I es consecuencia inmediata de la definición. La propiedad II se puede demostrar fácilmente usando la regla de los signos. Demostraremos la propiedad III:

Si  $\alpha = 0$  o  $\beta = 0$  la afirmación es obvia.

Si  $\alpha > 0$  y  $\beta > 0$  tenemos,

$$|\alpha + \beta| = \alpha + \beta = |\alpha| + |\beta|,$$

y queda comprobada la afirmación.

Si  $\alpha < 0$  y  $\beta < 0$ ,  $\alpha + \beta < 0$  y

$$|\alpha + \beta| = -|\alpha + \beta| = (-\alpha) + (-\beta) = |\alpha| + |\beta|.$$

Queda por considerar el caso en que  $\alpha$  y  $\beta$  tengan signos contrarios. Supongamos  $\alpha > 0$  y  $\beta < 0$ ,  $\alpha = \alpha'$  y  $\beta = -\beta'$ , siendo  $\alpha' > 0$  y  $\beta' > 0$ . Debemos demostrar que

$$|\alpha' + (-\beta')| \leq |\alpha'| + |-\beta'|,$$

es decir, que

$$|\alpha' - \beta'| \leq |\alpha'| + |\beta'|.$$

Si  $\alpha' = \beta'$  la desigualdad es clara.

Si  $\alpha' > \beta'$  tenemos  $\alpha' - \beta' > 0$ ,  $\alpha' > \alpha' - \beta'$ , de donde

$$|\alpha' - \beta'| = \alpha' - \beta' < \alpha' < \alpha' + \beta' = |\alpha'| + |\beta'|.$$

Si  $\alpha' < \beta'$  tenemos

$$|\alpha' - \beta'| = |-(\alpha' - \beta')| = |\beta' - \alpha'| \leq |\beta'| + |\alpha'|,$$

por el caso anterior.

Una consecuencia interesante es

$$\text{III}' \quad |\alpha - \beta| \geq ||\alpha| - |\beta||.$$

*Demostración:*

$$|\alpha| = |(\alpha - \beta) + \beta| \leq |\alpha - \beta| + |\beta|,$$

de donde

$$|\alpha| - |\beta| \leq |\alpha - \beta|.$$

Análogamente,  $|\beta| - |\alpha| \leq |\beta - \alpha| = |\alpha - \beta|$ , esto es,

$$-(|\alpha| - |\beta|) \leq |\alpha - \beta|.$$

Por lo tanto

$$|\alpha - \beta| \geq \max(|\alpha| - |\beta|, -(|\alpha| - |\beta|)) = ||\alpha| - |\beta||.$$

## 9. APROXIMACIÓN

Frecuentemente los números reales se manejan por medio de aproximaciones. Este es el caso, por ejemplo, cuando escribimos  $\sqrt{2} = 1.414$ . El número real  $\sqrt{2}$  se puede calcular con tantas cifras decimales como se quiera, obteniéndose

$$\sqrt{2} = 1.414 \dots,$$

de manera que

$$1.414 \leq \sqrt{2} \leq 1.414 + 10^{-3}$$

$$0 \leq \sqrt{2} - 1.414 \leq 10^{-3}.$$

Otro ejemplo: como

$$\pi = 3.1415926535 \dots$$

sabemos que

$$0 < 3.1416 - \pi < 10^{-5}.$$

Estas relaciones de aproximación se pueden expresar en la forma

$$\begin{aligned} |\sqrt{2} - 1.414| &\leq 10^{-3} \\ |\pi - 3.1416| &< 10^{-5}. \end{aligned}$$

Podemos ahora preguntar cuál es la aproximación con que el producto  $1.414 \times 3.1416 = 4.4422224$  nos da el real  $\sqrt{2}\pi$ . Para saberlo procederemos así:

$$\begin{aligned} & |\sqrt{2}\pi - 4.4422224| = |\sqrt{2}\pi - 1.414 \times 3.1416| = \\ & = |\sqrt{2}\pi - \sqrt{2} \times 3.1416 + \sqrt{2} \times 3.1416 - 1.414 \times 3.1416| \\ & \leq |\sqrt{2}| |\pi - 3.1416| + |\sqrt{2} - 1.414| |3.1416| \\ & \leq \sqrt{2} \times 10^{-5} + 10^{-3} \times 3.1416 \leq 1.415 \times 10^{-5} + 0.0031416 \\ & = 0.00315575 \leq 0.004. \end{aligned}$$

Entonces  $\sqrt{2}\pi = 4.4422224$  con aproximación de 4 milésimas o bien

$$\begin{aligned} -0.004 & < \sqrt{2}\pi - 4.4422224 < 0.004 \\ -0.01 & < -0.0017776 < \sqrt{2}\pi - 4.44 < 0.0062224 < 0.01 \end{aligned}$$

de donde  $\sqrt{2}\pi = 4.44$  con aproximación  $10^{-2}$ .

### EJERCICIOS

1. Supóngase que los reales  $\alpha$  y  $\beta$  están aproximados respectivamente por  $a$  y  $b$  de manera que

$$\begin{aligned} |\alpha - a| & < \epsilon \\ |\beta - b| & < \epsilon. \end{aligned}$$

Demuéstrese que

$$|\alpha\beta - ab| \leq |\epsilon^2 + \epsilon(|\alpha| + |\beta|)|.$$

2. Supóngase que  $\alpha$ ,  $\beta$  y  $\gamma$  están dados con aproximación  $10^{-3}$  y que son, en valor absoluto, menores que 10. ¿Con qué aproximación podemos obtener

$$\alpha^2 + \alpha\beta + \alpha\gamma + \beta^2 + \beta\gamma + \gamma^2?$$

3. Calcúlese  $\sqrt{\sqrt{5} - 1}$  con aproximación  $10^{-3}$ .



# 9

CAPÍTULO

## El campo de los números complejos

Con objeto de despojar a los números complejos de su aspecto “irreal” o “complejo” con el que se fueron abriendo paso en las matemáticas a través de la historia, hemos querido destacar, desde el principio y a lo largo de toda la exposición, el aspecto geométrico de los números complejos.

Aquí, los números complejos serán los puntos del plano real  $\mathbf{R}^2$  con dos operaciones convenientemente definidas.

Este capítulo es independiente de todos los anteriores, *excepto el primer párrafo del capítulo tercero* (págs. 73 a 80), cuyo conocimiento es indispensable para iniciar el estudio de éste.

### 1. MÓDULO Y ARGUMENTO DE VECTORES DE $\mathbf{R}^2$

**Módulo de un vector.** El módulo de un vector  $P = (a, b)$  del plano se define como la distancia de  $P$  al origen y se denota por  $|P|$ . O sea,

$$|P| = d(P, O) = \sqrt{a^2 + b^2}.$$

El módulo de un vector  $P$  es un número real no negativo. Además es evidente que el único vector cuyo módulo es cero, es el origen. En símbolos,

$$|P| \geq 0 \quad \text{y} \quad |P| = 0 \quad \text{si y solo si} \quad P = O.$$

Así como para definir el módulo de un vector hemos utilizado el concepto de distancia se puede, inversamente, determinar la distancia entre dos puntos  $P$  y  $Q$  como el módulo de su diferencia:

$$|P - Q| = d(P, Q).$$

En efecto, si  $P = (a, b)$  y  $Q = (c, d)$ ,  $P - Q = (a - c, b - d)$  y

$$|P - Q| = \sqrt{(a - c)^2 + (b - d)^2} = d(P, Q).$$

Otras propiedades que conviene mencionar son las siguientes:

$$|rP| = |r| |P|,$$

$$|P + Q| \leq |P| + |Q|, \quad (\text{desigualdad del triángulo}).$$

En la primera fórmula,  $|r|$  denota, como es usual, el valor absoluto del número real  $r$ . La demostración es directa.

Para demostrar la segunda, consideremos el triángulo de vértices  $O$ ,  $P$ ,  $P + Q$ :

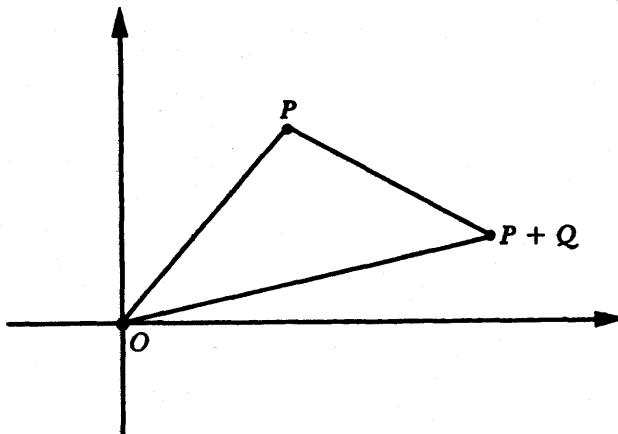


Figura 9.1

Ya que en un triángulo, la longitud de un lado es menor o igual que la suma de las longitudes de los otros dos, se tiene que  $d(O, P + Q) \leq d(O, P) + d(P, P + Q)$ , de donde

$$|P + Q| \leq |P| + |P + Q - P| = |P| + |Q|.$$

## EJERCICIOS

1. Calcúlense los módulos de los siguientes vectores:

$$(3, 4)$$

$$(-3, -4)$$

$$(\cos t, \operatorname{sen} t)$$

$$(\sqrt{2}, \sqrt{2})$$

$$\left( \frac{1}{2}, -\frac{\sqrt{3}}{2} \right)$$

$$(-3, 0).$$

2. El módulo de un punto sobre el eje de las abscisas es igual al valor absoluto de su abscisa:

$$|(a, 0)| = |a|.$$

3. Si  $r$  es un número real mayor que cero, el conjunto de vectores  $P$  tales que  $|P| = r$  es la circunferencia de centro en el origen y radio  $r$ . ¿Cuál es el conjunto de todos los puntos  $P$  del plano tales que  $|P| \leq r$ ?

4. Si  $r$  es un número real mayor que cero y  $P_0$  un punto fijo del plano, cuáles son los conjuntos de puntos del plano determinados por

a)  $|P - P_0| = r$ .  
 b)  $|P - P_0| \leq r$ .

c)  $|P - P_0| < r$ .  
 d)  $|P - P_0| > r$ .

5. Si  $C_1$  y  $C_2$  son círculos de centro  $P_1 = (3, 1)$  y  $P_2 = (-1, 0)$ , respectivamente y de radio 3, describáse su unión y su intersección usando el concepto de módulo. Dibújese una figura.

**Argumento.** El argumento de un vector distinto de  $O$  del plano real  $\mathbf{R}^2$  será un número real entre 0 y  $2\pi$ , más precisamente, mayor o igual que cero y menor que  $2\pi$ . Al origen no se le asigna argumento. Consideremos primero un vector  $P$  de módulo uno, es decir, un punto de la circunferencia unitaria con centro en el origen. El argumento de este vector  $P$  es, por definición, la longitud del arco entre el punto  $E_1 = (1, 0)$  y  $P$ . [Un punto  $P$  en la circunferencia determina, en realidad, dos arcos entre  $E_1$  y  $P$ . En la definición anterior consideramos el menor de los arcos si la ordenada de

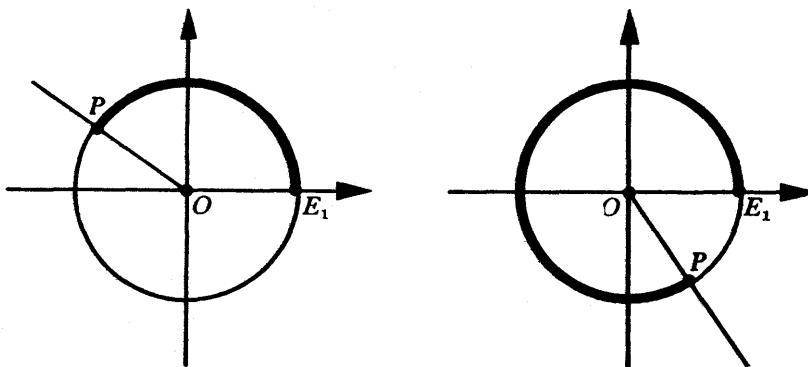


Figura 9.2

$P$  es  $\geq 0$  y mayor de ellos si la ordenada de  $P$  es  $\leq 0$  (fig. 9.2); el punto  $(1, 0)$  tiene argumento 0.]

Para un vector arbitrario  $P \neq O$  podemos definir el argumento como sigue. Sabemos que  $P$  se puede escribir de manera única en la forma  $P = rP_0$  con  $r = |P| \neq 0$  y  $P_0$  en la circunferencia de radio 1 y centro en  $O$  (fig. 9.3). Entonces simplemente definimos el argumento de  $P$  como el argumento de  $P_0$ .

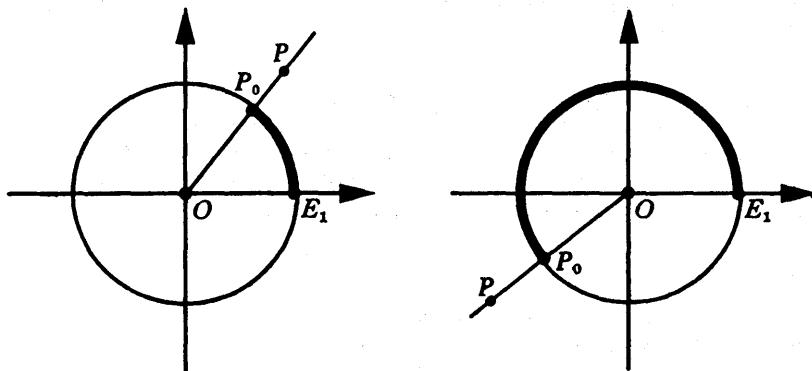


Figura 9.3

Al argumento de un vector  $P$  se le denotará con  $\arg P$ .

Así pues, todos los puntos de una semirrecta con vértice en  $O$  tienen un mismo argumento e, inversamente, el conjunto de puntos del plano cuyo argumento es igual a cierto número fijo  $s$  ( $0 \leq s < 2\pi$ ) es una semirrecta de extremo  $O$ .

#### Ejemplos:

1. a) El argumento de los vectores distintos de cero en el semieje positivo de las abscisas es 0 y el de los vectores no nulos en el semieje negativo de las abscisas es  $\pi$ .  
b) Los vectores distintos de cero del semieje positivo de las ordenadas tienen argumento  $\frac{\pi}{2}$  y los del semieje negativo  $\frac{3\pi}{2}$ .

2. Los argumentos de los vectores de los cuatro cuadrantes son como se indican en la figura 9.4 ( $O$  no tiene argumento):

#### EJERCICIOS

6. Pruébese que si el argumento de un vector  $P$  es  $s$  y  $0 \leq s \leq \pi$ , entonces el argumento de  $-P$  es  $s + \pi$ .

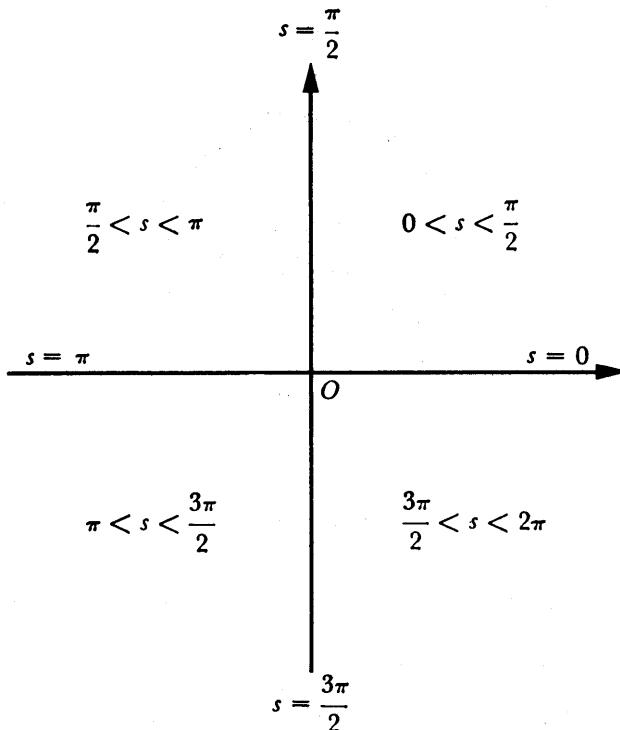


Figura 9.4

7. Pruébese que si el argumento de un vector  $P$  es  $s$  y  $\pi \leq s < 2\pi$ , entonces el argumento de  $-P$  es  $s - \pi$ .

8. Pruébese que si el argumento de un vector  $P = (a, b)$  es  $s$ , entonces el argumento de  $P = (a, -b)$  es  $2\pi - s$ .

9. Pruébese que si el argumento de un vector  $P = (a, b)$  es  $s$  y  $b \geq 0$ , entonces el argumento de  $P' = (-a, b)$  es  $\pi - s$ .

10. Pruébese que si el argumento de un vector  $P = (a, b)$  es  $s$  y  $b \leq 0$ , entonces el argumento de  $P' = (-a, b)$  es  $3\pi - s$ .

**Argumento en grados.** Es frecuente expresar también el argumento de un vector distinto de  $O$  del plano real en grados.

Tomando en cuenta que el argumento  $s$  de un vector  $P \neq O$  es la longitud del arco  $E_1 P_0$  (véase la figura 9.5), el argumento, en grados, de  $P$  será la medida  $\alpha$  del ángulo  $\angle E_1 O P$ .

Ya que  $0 \leq s < 2\pi$ , se tendrá que  $0 \leq \alpha < 360^\circ$ .

Recordemos la relación que hay entre la medida en grados de un ángulo formado por dos semirrectas con vértice en el origen y la longitud del

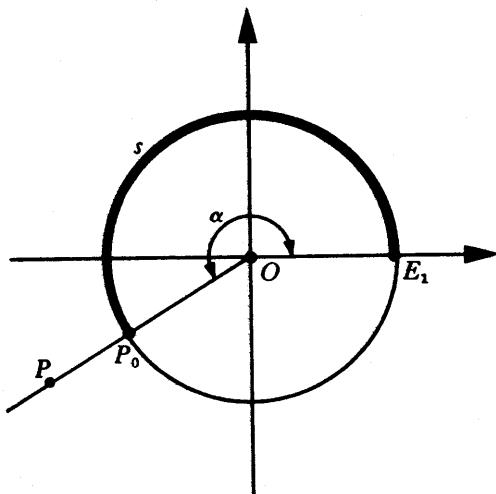


Figura 9.5

arco que éstas determinan sobre la circunferencia unitaria con centro en el origen.

La longitud de la circunferencia de radio 1 es  $2\pi$ . Por lo tanto la longitud de un arco, sobre ésta, correspondiente a un ángulo de un grado es  $\frac{2\pi}{360}$ .

Luego, si el argumento de un punto  $P$  medido en grados es  $\alpha$  y la longitud del arco correspondiente es  $s$ , la relación entre  $\alpha$  y  $s$  será

$$s = \alpha \frac{2\pi}{360},$$

o bien

$$\alpha = s \frac{360}{2\pi}.$$

#### Ejemplos:

3. Si el argumento de un vector  $P$  es  $\frac{5\pi}{4}$ , la semirrecta  $\overrightarrow{OP}$  forma un ángulo de  $225^\circ$  con la semirrecta  $\overrightarrow{OE_1}$ , es decir, el argumento de  $P$  es de  $225$  grados.

4. Si se nos indica que el argumento de un vector  $P$  es  $60^\circ$ , el arco determinado por el ángulo  $\angle E_1OP$  tendrá una longitud de  $\frac{2\pi}{6} = \frac{\pi}{3}$ , es decir, el argumento de  $P$  será  $\frac{\pi}{3}$ .

Utilizando las funciones trigonométricas es fácil expresar el argumento de un vector  $P \neq O$  del plano. Consideremos primero, como antes, el caso de que  $|P| = 1$  (fig. 9.6). Si  $s$  es el argumento de  $P$ , de las definiciones de las funciones trigonométricas sen y cos, se sigue que

$$P = (\cos s, \sin s).$$

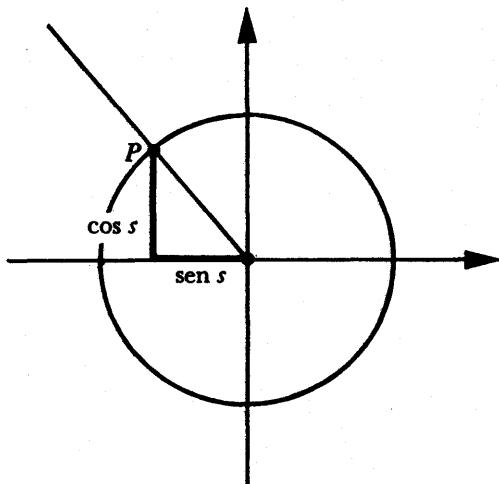


Figura 9.6

Así pues, si  $P = (a, b)$  es un punto tal que  $a^2 + b^2 = 1$ , su argumento es el número real  $s$  tal que  $0 \leq s < 2\pi$  y

$$\cos s = a, \quad \sin s = b.$$

En el caso general, si  $P = (a, b) \neq O$ , entonces

$$P = |P| P_0$$

con  $|P| = \sqrt{a^2 + b^2}$ ,  $P_0 = \left( \frac{a}{\sqrt{a^2 + b^2}}, \frac{b}{\sqrt{a^2 + b^2}} \right)$  y  $|P_0| = 1$ . El argumento

de  $P$  es igual al argumento de  $P_0$  y, por lo anterior, el argumento de  $P$  es el número real  $s$  tal que  $0 \leq s < 2\pi$  y

$$\cos s = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin s = \frac{b}{\sqrt{a^2 + b^2}}.$$

Hemos visto pues, que si  $P = (a, b)$  podemos escribir

$$P = r(\cos s, \operatorname{sen} s)$$

en donde  $r = |P| = \sqrt{a^2 + b^2}$  y  $s = \arg P$ , es decir,  $0 \leq s < 2\pi$  y  $\cos s = \frac{a}{\sqrt{a^2 + b^2}}$ ,

$\operatorname{sen} s = \frac{b}{\sqrt{a^2 + b^2}}$ . A esta forma de expresar un punto se le suele llamar la *forma polar o trigonométrica* del vector  $P$ .

Con esto hemos demostrado que si conocemos el módulo  $r$  y el argumento  $s$  de un vector, entonces el vector es

$$r(\cos s, \operatorname{sen} s).$$

Esta expresión de un punto diferente de  $(0, 0)$  es única. Es decir, si sabemos que

$$r(\cos s, \operatorname{sen} s) = r'(\cos s', \operatorname{sen} s'),$$

y que  $0 < r$ ,  $0 < r'$ ,  $0 \leq s < 2\pi$ ,  $0 \leq s' < 2\pi$  (o bien  $0 \leq s < 360$  y  $0 \leq s' < 360$  si  $s$  y  $s'$  están expresados en grados), entonces podemos asegurar que

$$r = r' \quad y \quad s = s'.$$

## EJERCICIOS

**11.** Calcúlense las coordenadas de los vectores del plano cuyo módulo sea  $r$  y cuyo argumento sea  $s$ , para los siguientes valores de  $r$  y  $s$ :

$r = 1, \quad s = 0^\circ$	$r = 2, \quad s = 30^\circ$	$r = \sqrt{2}, \quad s = 45^\circ$
$r = 2, \quad s = 60^\circ$	$r = 3, \quad s = 90^\circ$	$r = 4, \quad s = 120^\circ$
$r = 3\sqrt{2}, \quad s = 225^\circ$	$r = 2, \quad s = 270^\circ$	$r = 2, \quad s = 300^\circ$

**12.** ¿En qué cuadrantes están los vectores de argumento  $s$  para  $s = 1, s = 2, s = 3, s = 4, s = 5, s = 6$ ?

**13.** Usando las tablas trigonométricas calcúlense las coordenadas de los vectores de módulo 1 y argumento  $s$  para

$$s = 1 \quad s = 2 \quad s = 3.$$

**14.** Pruébese que el argumento de  $(3, 1)$  está entre  $0$  y  $\frac{\pi}{6}$ .

**15.** Pruébese que el argumento de  $(-3, -4)$  está entre  $\frac{7\pi}{6}$  y  $\frac{4\pi}{3}$ .

**16.** Úsense las tablas trigonométricas para calcular los argumentos de los siguientes vectores:

$$(1, 2), (2, -3), (-3, 4), (-4, -5).$$

SUGERENCIA: Exprésese  $(a, b)$  como  $\sqrt{a^2 + b^2} \left( \frac{a}{\sqrt{a^2 + b^2}}, \frac{b}{\sqrt{a^2 + b^2}} \right)$  y obténgase un ángulo  $s$  tal que

$$\cos s = \frac{a}{\sqrt{a^2 + b^2}}, \quad \operatorname{sen} s = \frac{b}{\sqrt{a^2 + b^2}}.$$

17. Exprésense los vectores del ejercicio anterior en forma polar.

## 2. LOS NÚMEROS COMPLEJOS

Consideremos ahora a los números reales  $\mathbf{R}$  como un subconjunto de  $\mathbf{R}^2$  identificando cada número real  $a$  con el punto  $(a, 0)$ . De esta manera  $\mathbf{R}$  se identificará con el eje de las abscisas. Más precisamente, establecemos una función

$$\mathbf{R} \rightarrow \mathbf{R}^2$$

asociando a cada número real  $a$  el punto  $(a, 0)$ . Esta es, evidentemente inyectiva.

Ahora bien, en párrafos anteriores hemos definido una suma entre puntos y, por otra parte, también hay una suma entre números reales. ¿Corresponde bajo esta identificación a la suma de dos números reales  $a$  y  $b$  la suma de los puntos identificados  $(a, 0)$  y  $(b, 0)$ ?

La respuesta es afirmativa:

$$\begin{aligned} a &\mapsto (a, 0) \\ b &\mapsto (b, 0) \\ a + b &\mapsto (a + b, 0) = (a, 0) + (b, 0). \end{aligned}$$

Cuando esto sucede, se dice que la operación de suma en  $\mathbf{R}^2$  se extiende a la suma de números reales.

Naturalmente se presenta la siguiente pregunta: ¿Es posible extender el producto de números reales a un producto en  $\mathbf{R}^2$ ? En este párrafo definiremos un producto en  $\mathbf{R}^2$  que extenderá el producto de números reales.

*Al plano real  $\mathbf{R}^2$  con las operaciones de suma y producto* (que definiremos) *se le llamará el campo de los números complejos* y a los puntos del plano que ahora, con estas operaciones, podrán ya sumarse y multiplicarse los llamaremos **números complejos**.

Las observaciones anteriores indican que el campo de los números complejos contiene al campo de los números reales, siendo estos últimos, los puntos del eje de las abscisas (al cual se llamará, por esto, el eje real).

La razón por la cual se emplea la palabra *campo* al hablar de los números complejos se dará al final de este capítulo (véase también el capítulo 8 en donde se habla del campo de los números reales y del campo de los números racionales).

La figura 9.7 ilustra las observaciones anteriores:

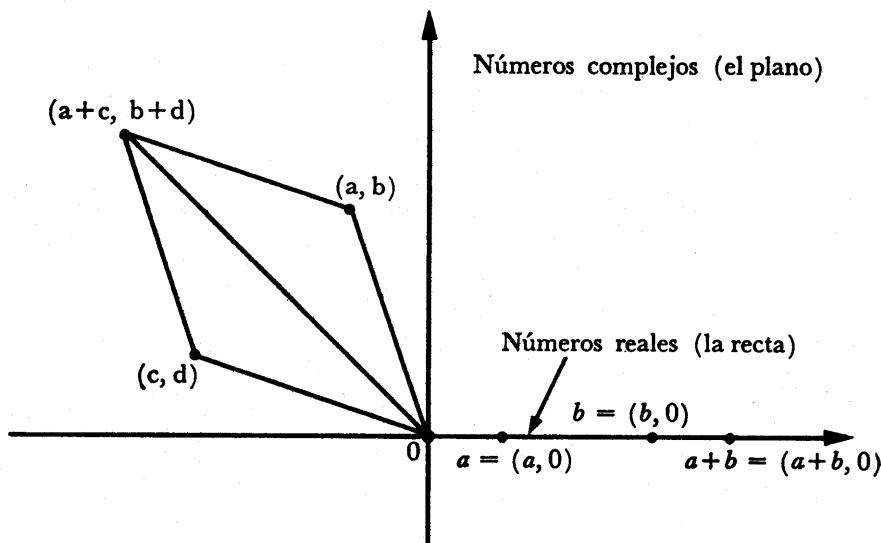


Figura 9.7

**Producto de números complejos de módulo uno.** Definiremos primero el producto de dos números complejos de módulo uno, es decir, puntos del plano que estén en la circunferencia unitaria con centro en el origen:

Sean  $z_1$  y  $z_2$  dos números complejos\* de módulo 1 y argumento  $s_1$  y  $s_2$  respectivamente:

$$z_1 = (\cos s_1, \operatorname{sen} s_1).$$

$$z_2 = (\cos s_2, \operatorname{sen} s_2).$$

El producto de  $z_1$  por  $z_2$  se define como el complejo

$$z_1 z_2 = (\cos(s_1 + s_2), \operatorname{sen}(s_1 + s_2)).$$

\* En general, hemos empleado letras mayúsculas  $O$ ,  $P$ ,  $Q$ , etc., para denotar a los puntos del plano. Cuando se piense en ellos, como números complejos, usaremos con más frecuencia, para seguir la costumbre, las letras  $z$ ,  $v$ ,  $w$ , etc.

O sea, el producto de dos complejos de módulo 1 es el complejo de módulo 1 cuyo argumento  $s$  es:

- a)  $s = s_1 + s_2$  si  $s_1 + s_2 < 2\pi$ , o bien  
 b)  $s = s_1 + s_2 - 2\pi$  si  $s_1 + s_2 \geq 2\pi$ .

La figura 9.8 ilustra esta definición:

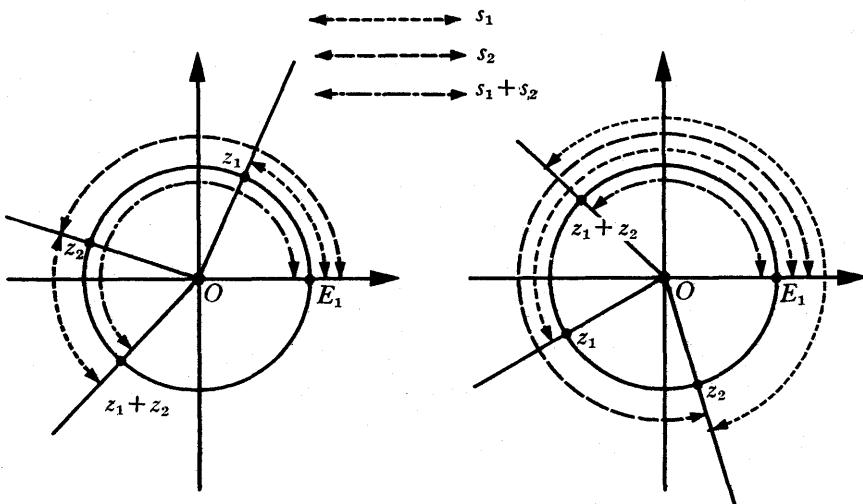


Figura 9.8

En esta situación se acostumbra decir que el argumento del producto es la suma de los argumentos de los factores salvo por un múltiplo de  $2\pi$ .

### Ejemplos:

1.  $(0, 1)(-1, 0) = (0, 1)$ .

[Tanto  $(0, 1)$  como  $(-1, 0)$  tienen módulo 1.] Tenemos que

$$\arg(0, 1) = \frac{\pi}{2}$$

$$\arg(-1, 0) = \pi.$$

Como  $\frac{\pi}{2} + \pi = \frac{3\pi}{2} < 2\pi$ ,  $(0, 1)(-1, 0)$  tiene por argumento  $\frac{3\pi}{2}$ , y siendo 1 su módulo, tenemos que (fig. 9.9),

$$(0, 1)(-1, 0) = (0, -1).$$

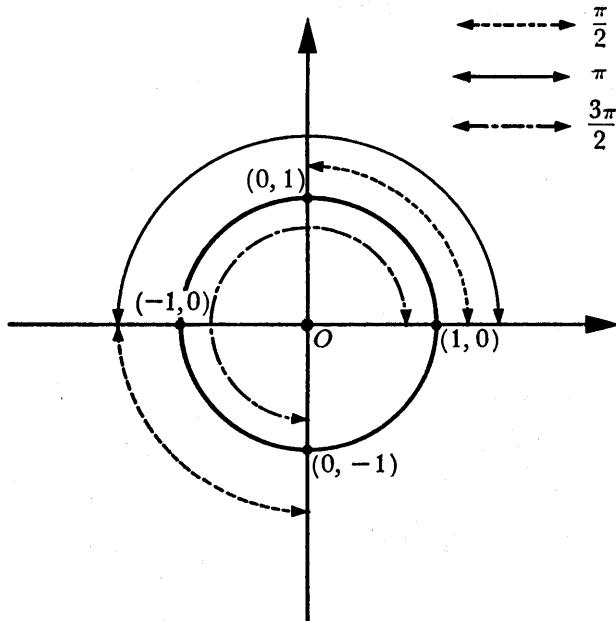


Figura 9.9

$$2. (-1, 0)(0, -1) = (0, 1).$$

Podemos aplicar la definición ya que ambos factores tienen módulo 1. Tenemos que

$$\arg(-1, 0) = \pi, \quad \arg(0, -1) = \frac{3\pi}{2}.$$

Como  $\pi + \frac{3\pi}{2} = \frac{5\pi}{2} > 2\pi$ , el argumento del producto es, por definición,  $\pi + \frac{3\pi}{2} - 2\pi = \frac{\pi}{2}$ . Por consiguiente, el producto es el complejo de módulo 1 y argumento  $\frac{\pi}{2}$ , es decir, es  $(0, 1)$  (fig. 9.10).

$$3. \left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)\left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right) = (1, 0).$$

El módulo de ambos factores es 1 y podemos aplicar la definición de producto. Tenemos que

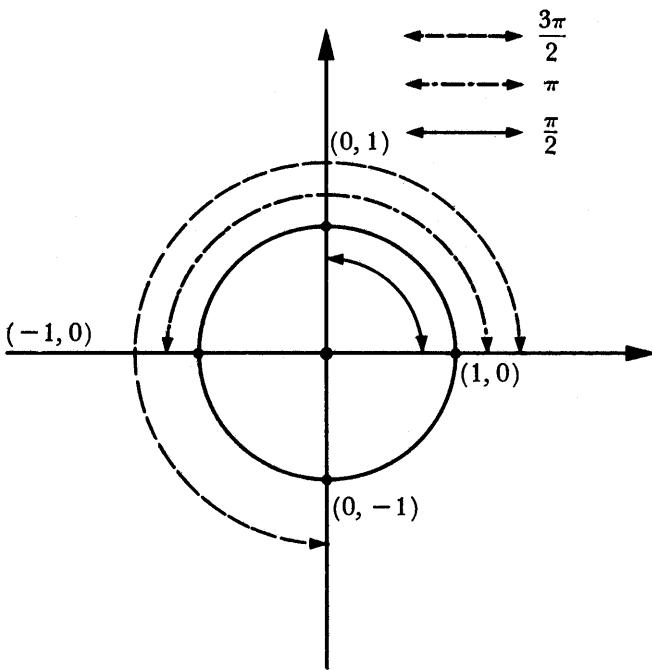


Figura 9.10

$$\arg\left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right) = \frac{3\pi}{4}, \quad \arg\left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right) = \frac{5\pi}{4}.$$

Como  $\frac{3\pi}{4} + \frac{5\pi}{4} = 2\pi$ , el argumento del producto es  $\frac{3\pi}{4} + \frac{5\pi}{4} - 2\pi = 0$  y el producto es  $(1, 0)$ .

$$4. \quad (1, 0)(a, b) = (a, b).$$

Para poder aplicar la definición debemos suponer que  $a^2 + b^2 = 1$  [aunque esta fórmula valdrá, como veremos más adelante, para un complejo  $(a, b)$  arbitrario]. Ya que el argumento de  $(1, 0)$  es 0, el argumento de  $(1, 0)(a, b)$  es igual al argumento de  $(a, b)$  y siendo el módulo del producto también 1, se tiene el resultado.

### EJERCICIOS

1. Calcúlese  $\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)\left(\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right)$ .

2. Demuéstrese que  $(\cos 35^\circ, \operatorname{sen} 35^\circ) (\cos 55^\circ, \operatorname{sen} 55^\circ) = (0, 1)$ .
3. Calcúlese  $(0, -1)(0, -1)$ .
4. Si  $z = (0, 1)$  calcúlese  $z^2$ .
5. Calcúlese  $(\cos 180^\circ, \operatorname{sen} 180^\circ) (\operatorname{sen} 270^\circ, \cos 270^\circ)$ .
6. Calcúlese  $(\cos 1, \operatorname{sen} 1) (\cos 2, \operatorname{sen} 2)$ .
7. Calcúlese  $(\cos 4, \operatorname{sen} 4) (\cos 3, \operatorname{sen} 3)$ .

**Producto. Caso general.** Sean ahora  $w$  y  $w'$  dos números complejos arbitrarios. Podemos escribir

$$\begin{aligned} w &= rz & \text{con } r = |w| \text{ y } |z| = 1 \\ w' &= r'z' & \text{con } r' = |w'| \text{ y } |z'| = 1 \end{aligned}$$

Hemos ya definido el producto  $zz'$ , pues ambos son complejos de módulo uno. Definimos ahora el producto de  $w$  por  $w'$  como

$$ww' = (rr') zz'.$$

Explícitamente, si

$$\begin{aligned} w &= r(\cos s, \operatorname{sen} s) \\ w' &= r'(\cos s', \operatorname{sen} s') \end{aligned}$$

se define

$$ww' = rr'(\cos(s + s'), \operatorname{sen}(s + s')).$$

En otras palabras, *el módulo del producto de dos números complejos es igual al producto de sus módulos y el argumento del producto es igual a la suma de los argumentos.* (Por supuesto, esto último salvo por un múltiplo de  $2\pi$ .)

### Ejemplo

5. Calculemos  $(4, 4)(-1, -1)$ .

El módulo de  $(4, 4)$  es  $4\sqrt{2}$  y el de  $(-1, -1)$  es  $\sqrt{2}$ . Por lo tanto, el módulo del producto es  $4\sqrt{2}\sqrt{2} = 8$ .

El argumento de  $(4, 4)$  es  $\frac{\pi}{4}$  y el de  $(-1, -1)$  es  $\frac{5\pi}{4}$ . Por lo tanto, el argumento del producto es  $\frac{\pi}{4} + \frac{5\pi}{4} = \frac{3\pi}{2}$

Luego, el producto es  $8(0, -1) = (0, -8)$ .

## EJERCICIOS

8. Calcúlese el producto de los siguientes números complejos:

- a)  $(4, 4\sqrt{3}) (2\sqrt{3}, 2)$
- b)  $2(\cos 25^\circ, \operatorname{sen} 25^\circ) 3(\cos 30^\circ, \operatorname{sen} 30^\circ)$
- c)  $2(\cos 365^\circ, \operatorname{sen} 365^\circ) \sqrt{2} (\cos 360^\circ, \operatorname{sen} 360^\circ).$

## 3. PROPIEDADES DE LAS OPERACIONES

**El número complejo  $i$ .** Al número complejo  $(0, 1)$  lo denotaremos con la letra  $i$ :

$$i = (0, 1).$$

$i$  es un punto del eje de las ordenadas y todo punto de este eje es de la forma  $bi$ . En efecto,

$$(0, b) = b(0, 1) = bi.$$

Como se recuerda, todo número complejo, es decir, todo punto  $z$  de  $\mathbf{R}^2$  se puede escribir como

$$z = (a, b) = (a, 0) + (0, b)$$

con  $(a, 0)$  en el eje de las abscisas y  $(0, b)$  en el eje de las ordenadas.

Ya que hemos identificado al eje de las abscisas con los números reales, a los puntos de la forma  $(a, 0)$  los denotaremos simplemente con  $a$ :

$$(a, 0) = a.$$

Así pues, todo número complejo  $z = (a, b)$  es la suma

$$z = a + bi$$

de los números complejos  $a = (a, 0)$  y  $bi = (0, b)$ .

Es claro que si

$$(a, b) = \boxed{a + bi = a' + b'i} = (a', b')$$

entonces

$$\boxed{a = a' \quad y \quad b = b'}$$

De aquí en adelante usaremos con más frecuencia la expresión  $a + bi$  para el número complejo  $(a, b)$ .

Si  $z = a + bi$ , (con  $a, b \in \mathbb{R}$ ) se dice que  $a$  es la *parte real* y que  $bi$  es la *parte imaginaria* de  $z$ ;  $b$  se llama el *coeficiente de la parte imaginaria* de  $z$ . Los complejos de la forma  $bi$  se llaman *números imaginarios* y, como lo hemos indicado anteriormente, los números complejos  $a + 0i = (a, 0) = a$  serán los números reales. Insistimos en que, de esta manera, los *números reales son números complejos*, a saber, aquellos cuya parte imaginaria es cero. Así pues,  $\mathbb{R} \subset \mathbb{C}$ . Al eje de las abscisas se le llama el *eje real* y al de las ordenadas, el *eje imaginario*.

El número imaginario  $i$  tiene la siguiente propiedad:

$$i^2 = -1.$$

En efecto  $|i| = 1$  y su argumento es  $\frac{\pi}{2}$ . Por lo tanto  $i^2$  tiene módulo 1 y argumento  $\pi$ , es decir  $i^2 = (-1, 0) = -1$ .

**Suma y producto de números complejos expresados en la forma  $a + bi$ .** Es conveniente obtener fórmulas que expresen la parte real y la parte imaginaria de la suma y el producto de dos números complejos en términos de las partes reales e imaginarias de sus sumandos o factores.

Para la suma éstas se obtienen inmediatamente, pues la misma definición de suma:

$$(a, b) + (c, d) = (a + c, b + d)$$

implica que

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Examinaremos ahora las fórmulas para el producto. En los párrafos anteriores hemos definido el producto de dos números complejos, utilizando sus módulos y argumentos, mediante las fórmulas siguientes:

Si

$$(a, b) = a + bi = r(\cos s, \operatorname{sen} s)$$

$$(c, d) = c + di = r'(\cos s', \operatorname{sen} s')$$

entonces

$$(a + bi)(c + di) = rr'(\cos(s + s'), \operatorname{sen}(s + s')).$$

Probaremos ahora que:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

De las igualdades anteriores sabemos que

$$\begin{array}{ll} a = r \cos s & c = r' \cos s' \\ b = r \operatorname{sen} s & d = r' \operatorname{sen} s'. \end{array}$$

Además, conocemos las fórmulas:

$$\begin{aligned} \cos(s + s') &= \cos s \cos s' - \operatorname{sen} s \operatorname{sen} s'. \\ \operatorname{sen}(s + s') &= \operatorname{sen} s \cos s' + \cos s \operatorname{sen} s'. \end{aligned}$$

Por lo tanto,

$$\begin{aligned} (a+bi)(c+di) &= rr'(\cos s \cos s' - \operatorname{sen} s \operatorname{sen} s', \operatorname{sen} s \cos s' + \cos s \operatorname{sen} s') \\ &= ((r \cos s)(r' \cos s') - (r \operatorname{sen} s)(r' \operatorname{sen} s'), (r \operatorname{sen} s)(r' \cos s') \\ &\quad + (r \cos s)(r' \operatorname{sen} s')) \\ &= (ac - bd, ad + bc) = (ac - bd) + (ad + bc)i, \end{aligned}$$

que es lo que se quería probar.\*

Como caso especial de esta fórmula obtenemos de nuevo la relación  $i^2 = -1$ . En efecto,

$$i^2 = (0+1i)(0+1i) = (0-1) + (0+0)i = -1.$$

## EJERCICIOS

1. Efectúense las siguientes operaciones:

- a)  $(3-2i) + (6-4i)$ ;
- b)  $(-3) + (-2+i)$ ;
- c)  $2i - (-3+2i)$ ;
- d)  $(2+3i)(1+2i)$ .
- e)  $(-2-i)(3+i)$ ;
- f)  $(-i)(1+i)$ ;
- g)  $(-i)(i)$ .

2. Si  $u = 2-3i$ ,  $v = 1+2i$ ,  $w = 1-i$  compruebe que

- a)  $(uv)w = u(vw)$ ;
- b)  $uv = vu$ ;
- c)  $u(v+w) = uv+uw$ .

3. Si  $z = (a-b) - (a+b)i$  y  $w = (a+b) + (a-b)i$  con  $a, b \in \mathbb{R}$ , calcúlense  $zw$  y  $wz$ .

\* El lector observador notará que al identificar  $c$  con  $(c, 0)$  el producto  $c(a, b)$  puede interpretarse de dos maneras distintas. Una, como el producto de un escalar por un punto, y otra, como el producto de los números complejos  $(c, 0)$  y  $(a, b)$ . Sin embargo no hay ambigüedad, ya que ambos productos coinciden:

$$\begin{aligned} c(a, b) &= (ca, cb) \\ (c, 0)(a, b) &= (ca-0b, cb-0a) = (ca, cb). \end{aligned}$$

**Algunas propiedades de las operaciones.** El producto de números complejos es asociativo, conmutativo y distribuye a la suma, es decir, si  $u, v, w$  son números complejos, entonces

$$\begin{array}{ll} (uv)w = u(vw) & \text{(asociatividad)} \\ uv = vu & \text{(conmutatividad)} \\ u(v+w) = uv + uw & \text{(distributividad).} \end{array}$$

Las demostraciones de estas propiedades son directas, es decir, utilizando las fórmulas para la suma y el producto se calculan las dos expresiones que se quiere probar que son iguales y se comprueba que en efecto lo son.

Como ejemplo, demostraremos a continuación que el producto distribuye a la suma:

$$\begin{aligned} u(v+w) &= (a+bi)((c+di)+(e+fi)) = (a+bi)((c+e)+(d+f)i) = \\ &= (a(c+e)-b(d+f)) + (a(d+f)+b(c+e))i = \\ &= (ac+ae-bd-bf) + (ad+af+bc+be)i. \end{aligned}$$

$$\begin{aligned} uv + uw &= (a+bi)(c+di) + (a+bi)(e+fi) = \\ &= ((ac-bd)+(ad+bc)i) + ((ae-bf)+(af+be)i) = \\ &= (ac-bd+ae-bf) + (ad+bc+af+be)i, \end{aligned}$$

de donde,  $u(v+w) = uv + uw$ .

Utilizando las propiedades anteriores es posible multiplicar números complejos recordando únicamente que  $i^2 = -1$ . En efecto:

$$\begin{aligned} &(a+bi)(c+di) = && \text{(propiedad distributiva)} \\ &= (a+bi)c + (a+bi)di \\ &= ac + bci + adi + bdi^2 && \text{(propiedad asociativa, conmutativa,} \\ &&& \text{distributiva)} \\ &= (ac - bd) + (ad + bc)i && \text{(propiedad conmutativa, distributiva,} \\ &&& i^2 = -1). \end{aligned}$$

## EJERCICIOS

4. Utilizando las propiedades de las operaciones entre números complejos calcúlense:

- |                          |   |
|--------------------------|---|
| a) $(-3-i)(2+i) - i^2$ ; | f) $(-i)^2$ ;   |
| b) $(2-2i) - (1-i)^2$ ;  | g) $(-i)^4$ ;   |
| c) $(2+i)^2$ ;           | h) $i^5$ ;  |
| d) $(1-i)^3$ ;           | i) $\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right)^3$ ;     |
| e) $i^3$ ;               | $\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^4$ . |

5. Pruébense las propiedades asociativa y conmutativa del producto.

**Conjugación.** El *conjugado* de un número complejo  $z = a + bi$  ( $a, b \in \mathbf{R}$ ) se define como el número complejo  $a - bi$  y se denota con  $\bar{z}$ , es decir,  $\bar{z} = a - bi$ .

Por ejemplo, si  $z = 2 - 3i$ ,  $\bar{z} = 2 + 3i$ ; si  $z = i$ ,  $\bar{z} = -i$ ; si  $z = 5$ ,  $\bar{z} = 5$ . En general si  $z$  es un número real,  $z = \bar{z}$ . Recíprocamente, si  $z = \bar{z}$ , entonces  $a + bi = a - bi$  ( $a, b \in \mathbf{R}$ ), de donde  $2bi = 0$  y por lo tanto  $b = 0$ , es decir, el complejo  $z$  es real.

Si  $z = a + bi$  ( $a, b \in \mathbf{R}$ ),

$$z + \bar{z} = a + bi + a - bi = 2a$$

$$z - \bar{z} = a + bi - (a - bi) = 2bi;$$

es decir,

$$\text{la parte real de } z = \frac{1}{2}(z + \bar{z})$$

$$\text{la parte imaginaria de } z = \frac{1}{2}(z - \bar{z}).$$

La transformación del plano real  $\mathbf{R}^2$  en sí mismo que asocia a cada número complejo su conjugado:

$$\mathbf{R}^2 \rightarrow \mathbf{R}^2, \quad z \rightarrow \bar{z}$$

es la reflexión del plano alrededor del eje real (fig. 9.11):

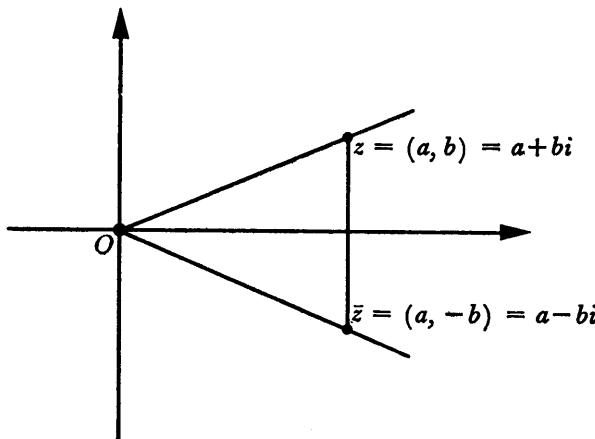


Figura 9.11

Esta transformación conserva, desde luego, la distancia al origen, o sea,  $|z| = |\bar{z}|$ .

Además, evidentemente,  $\bar{\bar{z}} = z$ .

Aquí se ve también claramente el resultado ya antes demostrado, de que un número complejo es real (es decir, está en el eje real) si y solo si  $z = \bar{z}$ . Demostrarímos ahora algunas propiedades de la conjugación.

a) Si  $u$  y  $v$  son números complejos, entonces

$$\overline{u+v} = \bar{u} + \bar{v}$$

$$\overline{uv} = \bar{u}\bar{v},$$

es decir, el conjugado de la suma de dos números complejos es igual a la suma de sus conjugados y el conjugado del producto de dos números complejos es igual al producto de sus conjugados.

Las demostraciones son directas. Verificaremos, como ejemplo, la segunda propiedad:

$$\text{Si } u = a+bi, v = c+di \quad (a, b, c, d \in \mathbf{R})$$

$$uv = (ac-bd) + (ad+bc)i$$

$$\bar{u}\bar{v} = (ac-bd) - (ad+bc)i$$

$$\bar{u}\bar{v} = (a-bi)(c-di) = (ac-bd) - (ad+bc)i.$$

b) Otra propiedad que se usará más adelante es la siguiente:

$$z\bar{z} = |z|^2,$$

es decir, el producto de un número complejo por su conjugado es igual al cuadrado de su módulo.

En efecto, si  $z = a + bi \quad (a, b \in \mathbf{R})$ ,

$$z\bar{z} = (a+bi)(a-bi) = a^2 + b^2.$$

### EJERCICIOS

6. Calcúlese  $\overline{2-3i}$ ,  $\bar{i}$ ,  $\bar{3}$ ,  $\bar{i^2}$ .

7. Si  $u = 1-2i$ ,  $v = -2+3i$ ,  $w = -1+4i$  calcúlese

$$u\bar{v} - \bar{u}v + \bar{w}, \quad (\overline{u+v})w - (u-\bar{v}), \quad (\overline{u+v})(\bar{u}-\bar{v}).$$

8. Si  $u = i$ ,  $v = 2$ , ¿cuál es el conjugado de  $z = u - vi$ ?

9. Si  $z = 3-4i$ , encuéntrese un complejo  $z'$  tal que  $zz' = 25$  (obsérvese que en este caso  $|z|^2 = 25$ ).

10. ¿Para qué parejas  $u$ ,  $v$  de números complejos es cierto que

a)  $\overline{uv} - \bar{u}\bar{v} = 0$ ;

b)  $\bar{u} + (\overline{u+v}) - \bar{u} - \bar{v} = u$ ?

**Inverso multiplicativo.** Probaremos ahora que todo número complejo distinto de cero tiene inverso multiplicativo, es decir, si  $z \neq 0$ , existe un número complejo, denotado con  $z^{-1}$  y llamado el inverso multiplicativo de  $z$ , tal que  $zz^{-1} = 1$ .

Sea  $z = a + bi \neq 0$  ( $a, b \in \mathbb{R}$ ). Planteemos la ecuación

$$(a+bi)(x+yi) = 1.$$

Obtenemos

$$(ax - by) + (ay + bx)i = 1,$$

de donde

$$\begin{cases} ax - by = 1 \\ bx + ay = 0. \end{cases}$$

Ya que el determinante del sistema es  $a^2 + b^2 \neq 0$ , existe una solución (y solo una), que es

$$x = \frac{a}{a^2 + b^2}, \quad y = \frac{-b}{a^2 + b^2}.$$

Es decir, si  $z = a + bi \neq 0$  ( $a, b \in \mathbb{R}$ ),

$$z^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i.$$

Utilizando los conceptos de módulo y de conjugado de un número complejo distinto de cero puede calcularse su inverso en la forma siguiente:

El producto de un número complejo por su conjugado es igual al cuadrado de su módulo. Si  $z \neq 0$  y  $|z| = r$

$$\bar{z}z = r^2 \neq 0,$$

de donde,

$$\left(\frac{1}{r^2}\bar{z}\right)z = 1,$$

es decir,

$$z^{-1} = \frac{1}{r^2}\bar{z}$$

que es lo mismo que se obtuvo anteriormente.

**Cociente.** El cociente de dos números complejos  $u, v$  con  $v \neq 0$  denotado con  $\frac{u}{v}$  se define como

$$\frac{u}{v} = uv^{-1}.$$

En particular, se tiene

$$\frac{1}{v} = v^{-1}.$$

De lo anterior se sigue que

$$\frac{u}{v} = \frac{1}{|v|^2} u\bar{v}.$$

Para calcular el cociente de dos números complejos puede también procederse como sigue:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i,$$

(desde luego,  $c+di \neq 0$ ).

## EJERCICIOS

**11.** Calcúlense los cocientes indicados:

$$a) \frac{1}{1-i};$$

$$e) \frac{1}{\cos \frac{\pi}{4} + i \operatorname{sen} \frac{\pi}{4}};$$

$$b) \frac{1}{i};$$

$$f) \frac{i^4 - 1}{i-1};$$

$$c) \frac{1+i}{3-4i};$$

$$g) \frac{i^2 + i^4 + i^6}{i^3 + i^5 + i^7};$$

$$d) \frac{1+i}{i};$$

$$h) \frac{-2+i}{3+4i}.$$

## 4. RAÍZ CUADRADA

Al estudiar el campo  $\mathbf{R}$  de los números reales se vio que cada número real positivo  $a$  tiene exactamente dos raíces cuadradas, una positiva, denotada por  $\sqrt{a}$ , y una negativa,  $-\sqrt{a}$ . Se vio también que los números reales negativos no tienen, en  $\mathbf{R}$ , ninguna raíz cuadrada; en otras palabras, que si  $a$  es un número real negativo no existe ningún número real  $x$  tal que  $x^2 = a$ .

Ahora demostraremos que en los números complejos la ecuación  $x^2 = z$ , (en donde  $z$  es un número complejo arbitrario  $\neq 0$ ), tiene exactamente dos soluciones; o sea que todo número complejo distinto de cero tiene exactamente dos raíces cuadradas. En particular, los números reales negativos tendrán también dos raíces cuadradas que serán números complejos.

Por ejemplo si  $z = -1$ , sabemos ya que  $i$  es una raíz cuadrada de  $z$ , pues  $i^2 = -1$ . Pero  $-i$  también es una raíz cuadrada de  $z$ , pues  $(-i)^2 = -1$ . Se verá después que  $i$ ,  $-i$  son las únicas raíces cuadradas de  $-1$ . Más aún, es cierto (como se probará más adelante) que si  $z$  es un número complejo distinto de cero, la ecuación

$$x^n = z$$

tiene exactamente  $n$  soluciones, es decir, todo número complejo, distinto de cero, tiene  $n$  raíces  $n$ -ésimas, distintas entre sí.

Trataremos, como ejemplo, de encontrar las raíces cuadradas de  $5 - 12i$ , es decir, de encontrar números complejos  $x + yi$  ( $x, y \in \mathbf{R}$ ) tales que

$$(x + yi)^2 = 5 - 12i,$$

tenemos que

$$(x^2 - y^2) + 2xyi = 5 - 12i,$$

de donde

$$\begin{cases} x^2 - y^2 = 5 \\ 2xy = -12. \end{cases}$$

Elevando al cuadrado ambas ecuaciones, obtenemos

$$\begin{cases} x^4 - 2x^2y^2 + y^4 = 25 \\ 4x^2y^2 = 144 \end{cases}$$

y sumando las ecuaciones obtenidas resulta

$$x^4 + 2x^2y^2 + y^4 = 169,$$

de donde

$$x^2 + y^2 = 13$$

(descartamos la posibilidad  $x^2 + y^2 = -13$ , pues  $x, y \in \mathbf{R}$ ). Sumando esta ecuación con  $x^2 - y^2 = 5$  obtenemos

$$2x^2 = 18$$

y, restándolas,

$$2y^2 = 8,$$

de donde,  $x^2 = 9$ ,  $y^2 = 4$  y por lo tanto  $x = \pm 3$ ,  $y = \pm 2$ . Como  $2xy = -12 < 0$ ,  $x, y$  no pueden ser ambos positivos ni ambos negativos. Entonces, las posibles

soluciones serán  $x = 3, y = -2$  y  $x = -3, y = 2$ . Obtenemos de esta manera, los dos números complejos

$$u_1 = 3 - 2i, \quad u_2 = -3 + 2i.$$

Una comprobación directa demuestra que  $u_1^2 = 5 - 12i$  y  $u_2^2 = 5 - 12i$  también. Es decir,  $5 - 12i$  tiene exactamente dos raíces cuadradas.

Este método puede aplicarse para encontrar las raíces cuadradas de cualquier número complejo. Supongamos que

$$(x + yi)^2 = a + bi, \quad (x, y, a, b \in \mathbf{R}).$$

Como antes, tenemos que

$$x^2 - y^2 = a$$

$$2xy = b,$$

$$x^4 - 2x^2y^2 + y^4 = a^2$$

$$4x^2y^2 = b^2$$

$$x^4 + 2x^2y^2 + y^4 = a^2 + b^2$$

$$x^2 + y^2 = \sqrt{a^2 + b^2} = r \in \mathbf{R}$$

$$2x^2 = r + a \geq 0$$

$$x = \pm \sqrt{\frac{r+a}{2}}$$

$$2y^2 = r - a \geq 0$$

$$y = \pm \sqrt{\frac{r-a}{2}}$$

Un análisis análogo al del ejemplo demuestra que esto conduce a dos soluciones. Es decir, si  $a + bi \neq 0$ ,  $a + bi$  tiene exactamente dos raíces cuadradas.

Es interesante un caso particular: ¿Cómo son las raíces de los números reales negativos?

Sea  $z = -a$ , un número real negativo (es decir,  $a > 0$ ). Las ecuaciones antes planteadas adquieren la forma

$$\begin{cases} x^2 - y^2 = -a \\ 2xy = 0. \end{cases}$$

La segunda ecuación implica que  $x = 0$  o bien  $y = 0$ . Pero si  $y$  fuera igual a cero, la primera ecuación quedaría  $x^2 = -a$ , la cual no tiene ninguna solución real  $x$ . Por lo tanto la única posibilidad de encontrar soluciones es

cuando  $x = 0$ . Entonces nos queda  $-y^2 = -a$ , es decir,  $y^2 = a$ , o sea,  $y = \sqrt{a} \in \mathbb{R}$ , o bien  $y = -\sqrt{a} \in \mathbb{R}$ , pues  $a$  es un real positivo. Entonces las raíces  $x + yi$  de  $-a$  serán:

$$\sqrt{a}i, \quad -\sqrt{a}i.$$

A veces se usa la notación  $\sqrt{-a}$  para indicar la primera de esas raíces; es decir, se escribe  $\sqrt{-a} = \sqrt{a}i$  ( $a \in \mathbb{R}$ ,  $a > 0$ ). Así pues se acostumbra escribir  $\sqrt{-1} = i$ .

**Interpretación geométrica.** Recordando la definición geométrica del producto de números complejos podemos describir fácilmente las raíces cuadradas de un número complejo.

Sea  $z$  un número complejo de módulo  $r > 0$  y argumento  $s$ , y  $w$  un número complejo cuyo cuadrado es igual a  $z$ , es decir,

$$w^2 = z.$$

Sea  $r' = |w|$  y  $s' = \arg w$ . Entonces

$$r = |w|^2 = r'^2$$

$$s = \arg(w^2) = \begin{cases} 2s' & (\text{si } 2s' < 2\pi) \\ 2s' - 2\pi & (\text{si } 2s' \geq 2\pi). \end{cases}$$

Entonces

$$r' = \sqrt{r} \quad (\text{pues } r \text{ y } r' \text{ son reales positivos});$$

y

$$s' = \frac{s}{2}, \text{ o bien}$$

$$s' = \frac{s}{2} + \pi.$$

Por consiguiente existen dos números complejos

$$w_1 = \sqrt{r} \left( \cos \frac{s}{2}, \operatorname{sen} \frac{s}{2} \right)$$

$$w_2 = \sqrt{r} \left( \cos \left( \frac{s}{2} + \pi \right), \operatorname{sen} \left( \frac{s}{2} + \pi \right) \right)$$

cuyo cuadrado es

$$z = r (\cos s, \operatorname{sen} s).$$

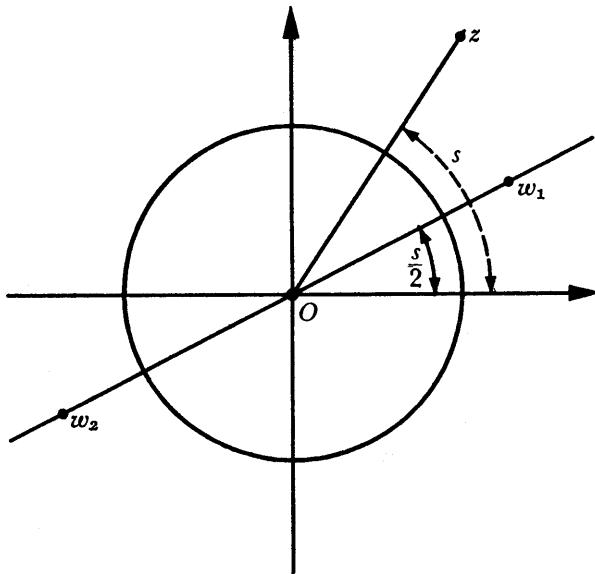


Figura 9.12

## EJERCICIOS

1. Calcúlense las raíces cuadradas de los siguientes números complejos

$$2i, \quad -2i, \quad 13 - 12i, \quad 24 - 10i,$$

$$4 \left( \cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right) \quad 8 \left( \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2} \right).$$

2. Demuéstrese que

$$1, \quad w_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad w_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

son raíces cúbicas de 1, es decir, que  $1^3 = w_1^3 = w_2^3 = 1$ .

3. Compruébese que 1,  $i$ ,  $-1$ ,  $-i$  son raíces cuartas de 1.

**Ecuaciones de segundo grado.** Desde los primeros cursos de álgebra se enseña a resolver las ecuaciones de segundo grado con coeficientes reales, es decir, las de la forma

$$ax^2 + bx + c = 0 \quad (a, b, c \in \mathbf{R}, \quad a \neq 0)$$

y se demuestra que

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{d}}{2a} \quad (d = b^2 - 4ac).$$

Pero cuando el discriminante de la ecuación es menor que cero, es decir, cuando  $d < 0$ , nos encontrábamos con que la ecuación no tenía solución en  $\mathbf{R}$ , pues los reales negativos no tienen raíz cuadrada real.

Sin embargo ahora, trabajando ya con números complejos, cuando el discriminante es negativo, digamos  $d = -d' < 0$ , vemos que las soluciones de la ecuación son los números complejos

$$x = \frac{-b \pm \sqrt{d'} i}{2a} = -\frac{b}{2a} \pm \frac{\sqrt{d'}}{2a} i.$$

### EJERCICIOS

4. Encuéntrense las soluciones de las ecuaciones

$$x^2 + x + 1 = 0$$

$$x^2 + 5 = 0$$

$$x^2 + 1 = 0$$

$$x^2 - 2x + 2 = 0$$

## 5. RAÍCES $n$ -ÉSIMAS DE NÚMEROS COMPLEJOS

En el párrafo anterior analizamos las raíces cuadradas de los números complejos. Vimos que cada número complejo distinto de cero tiene dos raíces cuadradas. Veremos ahora que *cada número complejo distinto de cero tiene  $n$  raíces  $n$ -ésimas*.

Recordemos primero que para multiplicar dos números complejos expresados en forma polar, se multiplican los módulos y se suman los argumentos restando  $2\pi$  a esta suma, cuando resulte  $\geq 2\pi$  (para obtener como argumento un número  $\geq 0$  y  $< 2\pi$ ).

Si hay más de dos factores, de todas maneras se multiplican los módulos y se suman los argumentos, pero puede ser necesario restar  $2\pi$  varias veces a esta suma (para, como antes, obtener un argumento  $\geq 0$  y  $< 2\pi$ ). Esto es:

- a) El módulo de un producto es el producto de los módulos.
- b) El argumento de un producto es la suma de los argumentos salvo por un múltiplo entero de  $2\pi$ .

Sea

$$z = r(\cos s + i \operatorname{sen} s)$$

un complejo distinto de cero. Con las observaciones anteriores en mente obtendremos todos los complejos  $w$  que tienen la propiedad

$$w^n = z,$$

es decir, que son raíces  $n$ -ésimas de  $z$  (siendo  $n$  un entero positivo).

Para que el complejo

$$w = \rho(\cos \sigma + i \sin \sigma)$$

satisfaga la condición  $w^n = z$ , es necesario y suficiente que

- a)  $\rho^n = r$
- b)  $n\sigma = s$  salvo por un múltiplo de  $2\pi$ .

Los siguientes números complejos son raíces  $n$ -ésimas de  $z$ :

$$w_0 = \sqrt[n]{r} \left( \cos \frac{s}{n} + i \sin \frac{s}{n} \right)$$

$$w_1 = \sqrt[n]{r} \left( \cos \left( \frac{s}{n} + \frac{2\pi}{n} \right) + i \sin \left( \frac{s}{n} + \frac{2\pi}{n} \right) \right)$$

$$w_2 = \sqrt[n]{r} \left( \cos \left( \frac{s}{n} + \frac{2\pi}{n} \cdot 2 \right) + i \sin \left( \frac{s}{n} + \frac{2\pi}{n} \cdot 2 \right) \right)$$

$$w_3 = \sqrt[n]{r} \left( \cos \left( \frac{s}{n} + \frac{2\pi}{n} \cdot 3 \right) + i \sin \left( \frac{s}{n} + \frac{2\pi}{n} \cdot 3 \right) \right)$$

.....

$$w_{n-1} = \sqrt[n]{r} \left( \cos \left( \frac{s}{n} + \frac{2\pi}{n} (n-1) \right) + i \sin \left( \frac{s}{n} + \frac{2\pi}{n} (n-1) \right) \right).$$

En efecto, sea  $w_k$  ( $k = 0, 1, \dots, n-1$ ) cualquiera de ellos:

$$w_k = \sqrt[n]{r} \left( \cos \left( \frac{s}{n} + \frac{2\pi}{n} k \right) + i \sin \left( \frac{s}{n} + \frac{2\pi}{n} k \right) \right).$$

Se satisface la condición (a):

$$(\sqrt[n]{r})^n = r$$

y la condición (b):

$$n \left( \frac{s}{n} + \frac{2\pi}{n} k \right) = s + 2\pi k = s + (\text{un múltiplo de } 2\pi).$$

Observemos que dos cualesquiera de las  $w_k$  son diferentes, puesto que sus argumentos son diferentes.

Comprobaremos ahora que los  $n$  complejos  $w_0, w_1, \dots, w_{n-1}$  son *todas* las raíces  $n$ -ésimas de  $z$ . Si  $w$  es una raíz  $n$ -ésima de  $z$ , sea

$$w = \rho(\cos \sigma + i \sin \sigma).$$

Por (a),  $\rho^n = z$ , esto es,  $\rho = \sqrt[n]{z}$ . Por (b),

$n\sigma = s + 2\pi k$  (para alguna  $k \in \mathbb{Z}$ ),  
tenemos que

$$0 \leq \sigma < 2\pi, 0 \leq s < 2\pi,$$

de donde,

$$0 \leq n\sigma < 2\pi n, -2\pi < -s \leq n\sigma - s < 2\pi n - s,$$

por lo que

$$\begin{aligned} -2\pi &< 2\pi k < 2\pi n - s \\ -1 &< k < n - \frac{s}{2\pi} < n \\ 0 &\leq k \leq n - 1, \end{aligned}$$

lo que implica que  $w = w_k$  que teníamos en nuestra lista.

En resumen, hemos demostrado que

Todo número complejo  $z \neq 0$

$$z = r(\cos s + i \sin s)$$

tiene exactamente  $n$  raíces  $n$ -ésimas, que son

$$w_k = \sqrt[n]{r} \left( \cos \left( \frac{s}{n} + \frac{2\pi}{n} k \right) + i \sin \left( \frac{s}{n} + \frac{2\pi}{n} k \right) \right)$$

para  $k = 0, 1, \dots, n - 1$ .

## EJERCICIOS

1. Calcúlense las raíces cúbicas de 1 y de  $-1$ , las raíces cuartas de 1 y  $-1$  y las raíces sextas de 1 y  $-1$ . Exprésense las soluciones en la forma  $a + bi$  y represéntelas gráficamente.

2. Después de observar las gráficas en el ejercicio anterior demuéstrese que las raíces  $n$ -ésimas de 1 son los vértices de un polígono regular inscrito en una circunferencia de radio 1 y centro en  $O$ , con uno de los vértices igual a 1.

## 6. EL CAMPO DE LOS NÚMEROS COMPLEJOS

En este último párrafo queremos simplemente destacar las propiedades básicas de los números complejos.

Los números complejos son los elementos de un conjunto:

el conjunto de los puntos del plano real  $\mathbf{R}^2$

en el cual se han definido dos operaciones, suma y producto:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Estas operaciones tienen las siguientes propiedades básicas: Si  $u, v, w$  son números complejos, entonces

- a)  $(u + v) + w = u + (v + w)$ .
- b) Existe un número complejo, el 0, tal que  $u + 0 = u$ .
- c) Dado  $u$ , existe un número complejo,  $-u$ , tal que  
 $u + (-u) = 0$ .
- d)  $u + v = v + u$ .
- e)  $(uv)w = u(vw)$ .
- f) Existe un número complejo, el 1, tal que  $u \cdot 1 = u$ .
- g) Dado  $u \neq 0$ , existe un número complejo  $u^{-1}$ , tal que  $uu^{-1} = 1$ .
- h)  $uv = vu$ .
- i)  $u(v + w) = uv + uw$ .

Como se comentó al discutir los números reales, cuando se tiene un conjunto con dos operaciones que satisfacen las propiedades anteriores se dice que esta estructura es un *campo*. Por esta razón al hablar de los números complejos nos referimos a ellos como *el campo de los números complejos*. La notación usual para este campo es **C**.

Además, el campo **C** de los números complejos contiene al campo **R** de los números reales y las operaciones de **C** se extienden a las operaciones de **R**. Se dice, en esta situación, que **R** es un *subcampo* de **C**. Cuando se discutió el campo de los números reales se observó que el campo **Q** de los números racionales, es un subcampo de **R**. Así pues se tienen tres campos

$$\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

Ya que **R** y **C** son campos, sus operaciones tienen en común las propiedades características de los campos. Sin embargo, hemos visto propiedades en **C** que no son válidas en **R**. Por ejemplo en **R** no todo número real

tiene una raíz cuadrada real (solamente los no negativos) y más aún, hay polinomios, con coeficientes reales que no tienen raíces reales (por ejemplo, las ecuaciones de segundo grado con discriminante negativo; en particular, el polinomio  $x^2 + 1$ ). En cambio, hemos demostrado que todo número complejo tiene raíces cuadradas. Además, aun cuando este resultado no se demuestre aquí, vale el llamado teorema fundamental del álgebra, el cual asegura que *todo polinomio con coeficientes en  $\mathbf{C}$  tiene raíces complejas*.

Finalmente queremos observar que algunas de las propiedades que juegan un importante papel en  $\mathbf{R}$ , desaparecen al extender este campo a  $\mathbf{C}$ . Nos referimos aquí al orden. Puede demostrarse que en  $\mathbf{C}$  no es posible definir una relación de orden que tenga las propiedades usuales con respecto a las operaciones de  $\mathbf{C}$ .



# 10

CAPÍTULO

## Polinomios y teoría de ecuaciones

### 1. POLINOMIOS

Llamamos *polinomios* a las expresiones

$$a_0 + a_1x + \cdots + a_nx^n,$$

donde  $a_0, a_1, \dots, a_n$  son números complejos. A estos números se les llama *coeficientes* del polinomio. Al símbolo  $x$  se le llama *indeterminada*.  $a_0, a_1x, \dots, a_n x^n$  son los *términos* del polinomio. Los coeficientes  $a_i$  pueden ser todos reales, en cuyo caso decimos que se trata de un polinomio con coeficientes reales, o pueden ser todos racionales (o enteros), y diremos entonces que el polinomio tiene coeficientes racionales (o enteros). Pueden también considerarse polinomios cuyos coeficientes pertenecen a alguna estructura algebraica distinta de los complejos. Sin embargo en este capítulo, polinomio será sinónimo de polinomio con coeficientes complejos.

Haremos varias observaciones:

- a) Cuando  $a_i = 0$  se conviene en que se puede omitir el término  $a_i x^i$  al escribir el polinomio, siempre que no se omitan todos los términos. Así, los polinomios

$$\begin{aligned} & 2 + 3x + 0x^2 + 5x^3, \\ & 0 + 2x + 0x^2, \\ & 0 + 0x, \end{aligned}$$

pueden escribirse, respectivamente, como

$$\begin{aligned} & 2 + 3x + 5x^3, \\ & 2x, \\ & 0. \end{aligned}$$

b) Se conviene en escribir  $x^i$  en lugar de  $1x^i$ , y  $-ax^i$  en lugar de  $(-a)x^i$  o de  $+(-a)x^i$ . Así, el polinomio

$$(-1)x + 0x^2 + 1x^3 + (-2)x^4$$

se escribe

$$-x + x^3 - 2x^4.$$

c) El término  $a_0$  también puede escribirse como  $a_0x^0$ . Nos referimos al término  $a_i x^i$  como al *término de grado i*. Al término de grado cero le llamamos *término independiente*. Al polinomio 0 le llamamos *polinomio nulo*.

d) No es necesario escribir los términos de un polinomio siempre en el mismo orden. Tampoco es necesario denotar siempre con  $a_i$  el coeficiente del término de grado  $i$ . Por ejemplo, el polinomio  $a + bx + cx^2$  puede escribirse también  $bx + cx^2 + a$ ,  $a + cx^2 + bx$ , etcétera, pero la forma más usual, aparte de la que estamos utilizando, es  $cx^2 + bx + a$ , es decir, en orden decreciente de los grados.

e) Otra manera de denotar los polinomios consiste en escribir la sucesión de sus coeficientes en orden creciente, sin omitir ninguno, conviniendo en que todos los términos que no aparecen tienen coeficiente cero. Con esta convención los polinomios  $-x^2 + 2x^5$ , 0,  $x^2 + ax + b$ , 5, se representan así:

$$\begin{aligned} & (0, 0, -1, 0, 0, 2, 0, 0, \dots), \\ & (0, 0, 0, \dots), \\ & (b, a, 1, 0, 0, \dots), \\ & (5, 0, 0, \dots). \end{aligned}$$

La siguiente noción es muy importante:

**DEFINICIÓN:** El grado de un polinomio no nulo es el mayor de los grados de los términos que tienen coeficiente diferente de cero.

Según esto los grados de los polinomios

$$\begin{aligned} & 2 - 3x^2, \\ & x + 0x^4, \\ & -1 + ix + (1+i)x^2 + 0x^3, \\ & x^3 + bx^2 + cx + d, \\ & \sqrt[3]{2}, \end{aligned}$$

son, respectivamente, 2, 1, 2, 3 y 0.

Puede definirse el grado del polinomio 0 como  $-\infty$ . Más adelante se aclarará qué sentido tiene esto.

## EJERCICIOS

1. ¿Cuáles son los términos independientes y de grado 2 de los polinomios  $1 + x + x^2$ ,  $1$ ,  $-x + 2x^3$  y  $0x^3$ ?
2. ¿Podemos decir cuál es el grado de un polinomio de la forma

$$ax^3 + bx^2 + cx + d?$$

## 2. LOS POLINOMIOS COMO FUNCIONES

Al polinomio  $a_0 + a_1x + \cdots + a_nx^n$  le corresponde la función que a cada complejo  $\alpha$  le asocia el complejo

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

que se obtiene al poner  $\alpha$  en lugar de la indeterminada  $x$  y darle a los signos + el sentido usual de suma. Si a esa función la denotamos por  $f$  tenemos

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Se acostumbra denotar el polinomio al que le corresponde la función  $f$  con  $f(x)$ .

### Ejemplos

1. Sea  $f(x) = 1 + x + x^2$ . Entonces

$$\begin{aligned} f(0) &= 1 + 0 + 0^2 = 1, \\ f(-1) &= 1 + (-1) + (-1)^2 = 1, \\ f(\sqrt{2}) &= 1 + \sqrt{2} + (\sqrt{2})^2 = 3 + \sqrt{2}. \end{aligned}$$

2. Sea  $f(x) = -3$ . Entonces  $f(\alpha) = -3$  para todo  $\alpha \in \mathbb{C}$ .

OBSERVACIÓN: En el párrafo anterior hemos convenido en que se puede escribir el término independiente  $a_0$  de un polinomio en la forma  $a_0x^0$ . Si escribimos

$$f(x) = a_0x^0 + a_1x + \cdots + a_nx^n$$

es necesario, al calcular  $f(\alpha)$ , convenir en que  $\alpha^0 = 1$  para todo  $\alpha \in \mathbb{C}$  (incluso para  $\alpha = 0$ ). Por ejemplo, si  $f(x) = x^0 = 1$ , tenemos que  $f(0) = 0^0 = 1$ .

## EJERCICIOS

1. Sea  $f(x) = x^3 - 1$ ; sea  $w = \frac{1}{2} + (\sqrt{\frac{3}{2}})i$ . Calcúlese  $f(w)$ ,  $f(w^2)$  y  $f(w^3)$ .
2. Sea  $f(x) = 1 + x + x^2$ . Obténgase el polinomio  $g(x)$  que tiene la propiedad  $g(\alpha) = f(\alpha - 1)$  para todo  $\alpha \in \mathbb{C}$ .
3. Sean  $f(x) = 1 + 2x + 3x^2$ ,  $g(x) = 2 - x$ . Encuéntrese el polinomio  $h(x)$  para el cual  $h(\alpha) = f(g(\alpha))$  para todo  $\alpha \in \mathbb{C}$ .
4. ¿Existe algún polinomio no nulo  $f(x) = a + bx$  tal que  $f(0) = f(1) = 0$ ?
5. ¿Existe algún polinomio no nulo  $f(x) = a + bx + cx^2$  tal que  $f(0) = f(1) = f(-1) = 0$ ?
6. Sean  $f_1(x) = a_1x^2 + b_1x + c_1$ ,  $f_2(x) = a_2x^2 + b_2x + c_2$ , y supóngase que  $f_1(\alpha) = f_2(\alpha)$  para todo  $\alpha \in \mathbb{C}$ . Demuéstrese que  $f_1(x) = f_2(x)$ , es decir, que  $a_1 = a_2$ ,  $b_1 = b_2$  y  $c_1 = c_2$ .

## 3. SUMA Y PRODUCTO DE POLINOMIOS

Pensaremos en el polinomio

$$a_0 + a_1x + \cdots + a_nx^n$$

como si tuviera una infinidad de términos, conviniendo en que a partir del grado  $n + 1$  todos los coeficientes son cero. Por ejemplo:

$$2 - 5x^2 = 2 - 5x^2 + 0x^3 + 0x^4 + 0x^5 + \cdots$$

$a_0 + a_1x + \cdots + a_nx^n = a_0 + a_1x + \cdots$ , donde  $a_i = 0$  para  $i > n$ . Con esta convención resulta muy fácil definir la suma y el producto:

*Definición de la suma:*

$$(a_0 + a_1x + a_2x^2 + \cdots) + (b_0 + b_1x + b_2x^2 + \cdots) = \\ = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots.$$

*Definición del producto:*

$$(a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots) = \\ = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$$

El coeficiente de  $x^n$  en la suma es  $a_n + b_n$ , y en el producto es

$$\sum_{i+j=n} a_i b_j.$$

Es importante observar que la suma y el producto pueden obtenerse manejando la indeterminada  $x$  como si fuera un número y aplicando las reglas

usuales de las operaciones con números complejos, que son la comutatividad y asociatividad de sumas y productos, y la distributividad. Por ejemplo, para calcular el producto tendremos que multiplicar cada término del primer factor por cada uno de los del segundo, obteniendo productos

$$a_i b_j x^{i+j}.$$

Podemos entonces observar que para un exponente fijo  $n$  aparece un término de grado  $n$  cada vez que  $i + j = n$ , y así vemos que el coeficiente de  $x^n$ , es la suma de todos los productos  $a_i b_j$  para los cuales  $i + j = n$ , tal como aparece en la fórmula que define al producto. Una discusión parecida puede hacerse con respecto a la suma.

Las observaciones que acabamos de hacer pueden expresarse como sigue:

**PROPOSICIÓN:** Sean  $g(x) = f_1(x) + f_2(x)$  y  $h(x) = f_1(x)f_2(x)$ . Para todo  $\alpha \in \mathbf{C}$  se cumple

$$\begin{aligned} g(\alpha) &= f_1(\alpha) + f_2(\alpha), \\ h(\alpha) &= f_1(\alpha)f_2(\alpha). \end{aligned}$$

**PROPOSICIÓN 1.** El grado de la suma de dos polinomios no nulos es menor o igual que el máximo de los grados de los sumandos.

**PROPOSICIÓN 2.** El grado del producto de dos polinomios no nulos es la suma de los grados de los factores.

La hipótesis de que los polinomios sean no nulos puede eliminarse en las dos proposiciones anteriores. Esto se hará en los ejercicios 8 y 9.

*Demostración de la proposición 1.* Sean  $f(x) = a_0 + a_1x + \dots$ ,  $g(x) = b_0 + b_1x + \dots$ , de grados  $m$  y  $n$ , respectivamente, y supongamos, para fijar ideas, que  $m \geq n$ . Debemos demostrar que el grado de  $f(x) + g(x)$  es  $\leq m$ . Esto equivale a mostrar que el coeficiente de  $x^i$  en la suma es igual a cero siempre que  $i > m$ . Ese coeficiente es  $a_i + b_i$  y es cero si  $i > m$  ya que  $a_i = 0$  por ser  $i > m$  y  $b_i = 0$  por ser  $i > m \geq n$ .

*Demostración de la proposición 2.* Consideraremos los mismos polinomios. El coeficiente de  $x^{m+n}$  en el producto es

$$a_0 b_{m+n} + a_1 b_{m+n-1} + \dots + a_{m+n} b_0.$$

En esta suma aparece  $a_m b_n$ , que es diferente de cero, puesto que  $a_m \neq 0$  y  $b_n \neq 0$ . Todos los demás sumandos  $a_i b_j$  son cero puesto que  $i + j = m + n$  e  $i \neq m$ , lo que implica  $i > m$  o que  $j > n$ . En el primer caso se tiene  $a_i = 0$  y en el segundo  $b_j = 0$ . Por tanto el coeficiente de  $x^{m+n}$  es  $a_m b_n \neq 0$ . Para

terminar la demostración debemos ver que el coeficiente de  $x^s$  en el producto es 0 si  $s > m + n$ . Pero ese coeficiente es la suma de los  $a_i b_j$ , tales que  $i + j = s > m + n$ , lo que implica que  $i > m$  o  $j > n$ , y en ambos casos  $a_i b_j = 0$ .

## EJERCICIOS

**1.** Calcúlese:

- a)  $(x+1)(x-1)$
- b)  $(a_0x^2 + a_1x + a_2)(b_0x^3 + b_1x^2 + b_2x + b_3)$
- c)  $[(ax^3 + bx^2 + cx + d)^2 + (ex + f)^3](gx^2 + hx + j)$ .

**2.** Demuéstrese que el polinomio  $x^2 - 2$  no puede expresarse como producto de dos polinomios con coeficientes racionales de grado 1.

**3.** Exprésese  $x^2 - 2$  como producto de dos polinomios de grado 1.

**4.** Sea  $f(x) = x^3 + 3x^2 + 3x + 1$ . Encuéntrense todos los  $\alpha \in \mathbb{C}$  tales que  $f(\alpha) = 0$ .

**5.** Utilizando las fórmulas que definen la suma y el producto y los resultados de este párrafo demuééstrense que las afirmaciones siguientes para polinomios  $f(x)$ ,  $g(x)$  y  $h(x)$  cualesquiera:

- a)  $f(x) + g(x) = g(x) + f(x)$
- b)  $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$
- c)  $0 + f(x) = f(x)$ .
- d) Existe un polinomio que sumado con  $f(x)$  da el polinomio 0 [este polinomio se denota  $-f(x)$ ]:
- e)  $f(x)g(x) = g(x)f(x)$
- f)  $f(x)(g(x)h(x)) = (f(x)g(x))h(x)$
- g)  $1f(x) = f(x)$
- h) Si  $f(x) \neq 0$  y  $g(x) \neq 0$ , entonces  $f(x)g(x) \neq 0$
- i) Si  $f(x) \neq 0$  y  $f(x)g(x) = f(x)h(x)$ , entonces  $g(x) = h(x)$
- j)  $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$ .

**6.** Supóngase que  $f(x)$ ,  $g(x)$ ,  $h(x)$  tienen coeficientes enteros, que  $f(x) = g(x)h(x)$  y que  $g(0) = -3$ . ¿Es posible que  $f(0) = 1234567$ ? ¿Por qué?

**7.** Encuéntrese el polinomio  $f(x)$  de grado 2 para el que se cumple  $f(0) = 1$ ,  $f(2) = 1$ ,  $f(-3) = 0$ .

**8.** Admitamos que  $-\infty + n = -\infty$  para todos los enteros  $n$  y que  $-\infty + (-\infty) = -\infty$ . Definimos el grado del polinomio nulo como  $-\infty$ . Demuéstrese que la proposición 2 del párrafo 3 es válida para polinomios cualesquiera.

**9.** Admitamos que  $-\infty > n$  para todo entero  $n$ . Demuéstrese que la proposición 1 del párrafo 3 es válida para polinomios cualesquiera.

**10.** Sea  $f(x)$  de grado 9 y supóngase que

$$f(x) = f_1(x)f_2(x)f_3(x)f_4(x),$$

donde  $f_i(x)$  es de grado  $> 0$  para  $i = 1, 2, 3, 4$ . Demuéstrese que dos de los  $f_i(x)$  tienen el mismo grado.

**11.** Decimos que una función  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  es polinomial si existe un polinomio  $f(x)$  tal que  $\varphi(n) = f(n)$  para todo  $n \in \mathbb{N}$ . Demuéstrese que la función

$$\varphi(n) = \sum_{j=1}^n (2n-1)$$

es polinomial.

**12.** Demuéstrese que

$$\varphi(n) = \sum_{j=1}^n j^2$$

es una función polinomial.

#### 4. DIVISIÓN CON RESIDUO

**PROPOSICIÓN:** Sea  $f(x)$  cualquier polinomio y sea  $g(x)$  un polinomio no nulo. Existen dos únicos polinomios,  $q(x)$  y  $r(x)$ , que satisfacen las condiciones siguientes:

- a)  $f(x) = g(x)q(x) + r(x)$ ;
- b) grado de  $r(x) <$  grado de  $g(x)$ .

Los polinomios  $q(x)$  y  $r(x)$  son el *cociente* y el *resto* de la *división de  $f(x)$  entre  $g(x)$* , respectivamente. Los polinomios  $f(x)$  y  $g(x)$  son el *dividendo* y el *divisor*, respectivamente.

Es muy fácil comprobar que solo puede haber una pareja de polinomios que satisfacen a) y b). En efecto, supóngase que

$$\begin{aligned} f(x) &= g(x)q(x) + r(x) \\ &= g(x)q_1(x) + r_1(x), \end{aligned}$$

con los grados de  $r(x)$  y de  $r_1(x)$  menores que el grado  $n$  de  $f(x)$ . Entonces

$$g(x)(q(x) - q_1(x)) = r_1(x) - r(x),$$

de donde, según las proposiciones 1 y 2 del párrafo 3 y los ejercicios 8 y 9 del párrafo 3,

$$n + \text{grado de } (q(x) - q_1(x)) = \text{grado de } (r_1(x) - r(x)) < n,$$

lo que solo es posible si  $q(x) - q_1(x) = 0$ , en cuyo caso  $r_1(x) = r(x)$  y  $q_1(x) = q(x)$ .

La existencia de  $q(x)$  y  $r(x)$  quedará demostrada al describir la manera de obtenerlos. El procedimiento consiste en ir obteniendo una sucesión de parejas de polinomios  $q_i(x)$  y  $r_i(x)$  tales que

$$f(x) = g(x) q_i(x) + r_i(x)$$

de manera que los grados de los  $r_i(x)$  decrezcan con lo que necesariamente llegaremos a que

$$\text{grado de } r_s(x) < n,$$

y en ese momento habremos encontrado  $q(x)$  y  $r(x)$  que serán precisamente  $q_s(x)$  y  $r_s(x)$ . La manera de ir obteniendo esas parejas de polinomios es como sigue:

a) Si el grado de  $f(x)$  es menor que el de  $g(x)$  se toman  $q_1(x) = 0$  y  $r_1(x) = f(x)$ , con lo que termina el proceso.

b) Si el grado  $m$  de  $f(x)$  es mayor que el grado  $n$  de  $g(x)$ , sean

$$\begin{aligned} f(x) &= a_0 x^m + a_1 x^{m-1} + \dots + a_m, \\ g(x) &= b_0 x^n + b_1 x^{n-1} + \dots + b_n, \end{aligned}$$

y describiremos primero cómo se obtienen  $q_1(x)$  y  $r_1(x)$  y, en seguida, cómo se obtienen  $q_{i+1}(x)$  y  $r_{i+1}(x)$  a partir de  $q_i(x)$  y  $r_i(x)$ :

i) Se toman  $q_1(x) = a_0 b_0^{-1} x^{m-n}$  y  $r_1(x) = f(x) - g(x) q_1(x)$ .

ii) Suponiendo ya obtenidos  $q_i(x)$  y  $r_i(x)$  sea

$$r_i(x) = a_{i,0} x^{m_i} + a_{i,1} x^{m_i-1} + \dots + a_{i,m_i}, \quad a_{i,0} \neq 0,$$

y supongamos que  $m_i \geq n$ , porque en caso contrario ya ha terminado el proceso. Tomemos  $q_{i+1}(x) = q_i(x) + a_{i,0} b_0^{-1} x^{m_i-n}$  y

$$\begin{aligned} r_{i+1}(x) &= r_i(x) - g(x) a_{i,0} b_0^{-1} x^{m_i-n} \\ &= (a_{i,0} x^{m_i} + \dots) - (b_0 x^n + \dots) a_{i,0} b_0^{-1} x^{m_i-n}, \end{aligned}$$

que es un polinomio de grado menor que el grado  $m_i$  de  $r_i(x)$ . Además, es claro que  $f(x) = g(x) q_{i+1}(x) + r_{i+1}(x)$ , ya que

$$\begin{aligned} r_{i+1}(x) &= f(x) - g(x) q_i(x) - g(x) a_{i,0} b_0^{-1} x^{m_i-n} \\ &= f(x) - g(x) q_{i+1}(x). \end{aligned}$$

Así queda descrito el procedimiento para dividir con residuo. Este algoritmo se suele practicar siguiendo un esquema muy conocido que recordaremos con un ejemplo:

$$\begin{array}{r}
 x^4 + 5x^3 - 2x^2 + x - 1 \\
 \underline{- x^4 + \frac{1}{2}x^3 - \frac{3}{2}x^2} \\
 \hline
 \frac{11}{2}x^3 - \frac{7}{2}x^2 + x - 1 \\
 \underline{- \frac{11}{2}x^3 + \frac{11}{4}x^2 - \frac{33}{4}x} \\
 \hline
 -\frac{3}{4}x^2 - \frac{29}{4}x - 1 \\
 +\frac{3}{4}x^2 - \frac{3}{8}x + \frac{9}{8} \\
 \hline
 -\frac{61}{8}x + \frac{1}{8}
 \end{array}$$

En el ejemplo anterior se dividió  $x^4 + 5x^3 - 2x^2 + x - 1$  entre  $2x^2 - x + 3$  obteniendo el cociente  $\frac{1}{2}x^2 + \frac{11}{4}x - \frac{3}{8}$  y el resto  $-\frac{61}{8}x + \frac{1}{8}$ .

El primer sumando  $\frac{1}{2}x^2$  del cociente se forma de manera que al multiplicarlo por el divisor y restárselo al dividendo se obtenga el primer resto parcial,  $\frac{11}{2}x^3 - \frac{7}{2}x^2 + x - 1$ , de grado menor que el del dividendo, es decir, de manera que se elimine el término de grado máximo. El segundo término del cociente,  $\frac{11}{4}x$ , se calcula de manera que al multiplicarlo por el divisor y restarle el resultado al primer resto parcial se elimine el término de grado máximo de este último y dar un segundo resto parcial,  $-\frac{3}{4}x^2 - \frac{29}{4}x - 1$ , que es de grado menor que el del primero, etc., hasta obtener un resto de grado menor que el del divisor.

**PROPOSICIÓN:** Con la misma notación de la proposición anterior se puede afirmar lo siguiente:

Si  $f(x)$  y  $g(x)$  tienen coeficientes reales (racionales),  $q(x)$  y  $r(x)$  también tienen coeficientes reales (racionales).

*Demostración.* Basta observar que todos los coeficientes que aparecen al calcular  $q(x)$  y  $r(x)$  se obtienen por sumas, restas, multiplicaciones y divisiones a partir de los coeficientes de  $f(x)$  y  $g(x)$  que son reales (racionales) por hipótesis.

## EJERCICIOS

**1.** Divídase  $x^2 + 2x + 1$  entre  $x + 1$ . Divídase  $x + 1$  entre  $x^2$ . Divídase  $x^3 + 2x^2 + 3x + 4$  entre  $x^2 + 2x + 3$ .

**2.** Se dice que  $f(x)$  es divisible entre  $g(x)$ , o que  $g(x)$  divide a  $f(x)$ , o que  $f(x)$  es múltiplo de  $g(x)$  si existe algún polinomio  $h(x)$  tal que  $f(x) = g(x)h(x)$ . En ese caso escribimos  $g(x)|f(x)$ . Demuéstrese que  $g(x)|f(x)$  si y solo si el resto de la división de  $f(x)$  entre  $g(x)$  es 0.

**3.** Diremos que un polinomio  $f(x)$  tiene inverso multiplicativo si existe algún  $g(x)$  tal que  $f(x)g(x) = 1$ . Demuéstrese que las siguientes afirmaciones son equivalentes:

- a)  $f(x)$  tiene inverso multiplicativo;
- b)  $f(x) | 1$ ;
- c)  $f(x)$  es de grado cero.

**4.** Demuéstrese que  $x - a | x - b \iff a = b$ .

**5.** Decimos que  $f(x)$  y  $g(x)$  son asociados si  $f(x) | g(x)$  y  $g(x) | f(x)$ . Demuéstrese que  $f(x)$  y  $g(x)$  son asociados si y solo si  $f(x) = cg(x)$  para algún complejo  $c \neq 0$ .

## 5. RAÍCES DE POLINOMIOS. TEOREMA DEL RESIDUO. TODO POLINOMIO DE GRADO POSITIVO TIENE RAÍCES

Se dice que  $a$  es *raíz* de  $f(x)$  si  $f(a) = 0$ . A las raíces de  $f(x)$  también se les llama *ceros* de  $f(x)$ . Las raíces de  $f(x)$  son las *soluciones de la ecuación*  $f(x) = 0$ , entendiendo por ecuación una igualdad que solo es verdadera si en lugar de  $x$  se ponen ciertos números a los cuales llamamos soluciones de la ecuación.

La proposición siguiente es un caso particular de la primera proposición del párrafo 4.

**PROPOSICIÓN:** Sea  $f(x)$  un polinomio y sea  $a \in \mathbb{C}$ . Existen un polinomio  $q(x)$  (cociente) y  $r \in \mathbb{C}$  (resto), tales que

$$f(x) = (x - a) q(x) + r.$$

Además,  $q(x)$  y  $r$  son únicos.

[Según dicha proposición, el residuo  $r(x)$  es de grado  $< 1$ . Es, por tanto, un elemento de  $\mathbb{C}$ , o constante.]

**Teorema del residuo.** El residuo de la división de  $f(x)$  entre  $x - a$  es igual a  $f(a)$ .

La demostración no puede ser más simple: tenemos que

$$f(x) = (x - a) q(x) + r,$$

de donde

$$f(a) = (a - a) q(a) + r = r.$$

**COROLARIO 1:**  $a$  es raíz de  $f(x) \iff x - a \mid f(x)$ .

**COROLARIO 2:**  $x - a \mid f(x) - f(a)$ .

**COROLARIO 3:**  $x - a \mid f(x) g(x) \iff x - a \mid f(x) \text{ o } x - a \mid g(x)$ .

El corolario 1 es inmediato (equivale a decir que  $x - a \mid f(x)$  si y solo si  $r = 0$ ). El corolario 2 se obtiene de la igualdad  $f(x) = (x - a) q(x) + r$  pasando  $r$  al primer miembro. El corolario 3 se obtiene así:  $x - a \mid f(x) g(x) \implies a$  es raíz de  $f(x) g(x) \implies f(a) g(a) = 0 \implies f(a) = 0 \text{ o } g(a) = 0 \implies a$  es raíz de  $f(x)$  o de  $g(x) \implies x - a \mid f(x)$  o  $x - a \mid g(x)$ .

El siguiente resultado, que afirma que  $f(x) = 0$  tiene solución siempre que  $f(x)$  sea de grado positivo, es conocido a veces como el “Teorema fundamental del álgebra”.

**TEOREMA:** Todo polinomio de grado  $> 0$  tiene (al menos) una raíz (en **C**).

La demostración no se incluye aquí.

## EJERCICIOS

1. ¿Cuáles son las raíces del polinomio  $x^4 - 1$ ?
2. Exprésese  $x^3 - 1$  como producto de polinomios de grado 1.
3. Resuélvase la ecuación  $x^8 - 1 = 0$ .
4. ¿Cuáles son los polinomios que no tienen ninguna raíz?
5. Dése un polinomio que tenga una infinitud de raíces.
6. Supóngase que  $f(x) \mid g(x)$ . Demuéstrese que toda raíz de  $f(x)$  es raíz de  $g(x)$ .
7. Sea  $f(x)$  un polinomio con coeficientes reales. Demuéstrese que  $x - a \mid f(x) \iff x - \bar{a} \mid f(x)$ .
8. Supóngase que todos los coeficientes de

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

son enteros. Supóngase que  $\frac{a}{b}$  es una raíz de  $f(x)$ , donde  $a$  y  $b$  son enteros

y  $(a, b) = 1$ . Demuéstrese que  $a \mid a_0$  y  $b \mid b_0$ .

9. Compruébese que el polinomio  $2x^7 - 3x^5 + 2x^4 - x^3 + 7x - 2$  no tiene ninguna raíz racional.

10. Supóngase que  $f(x) \neq 0$ , que  $f(a) = f(b) = f(c) = 0$  y que  $a \neq b$ ,  $a \neq c$ ,  $b \neq c$ . Demuéstrese que  $f(x)$  es de grado  $\geq 3$ .

**11.** Demuéstrese que toda raíz racional del polinomio  $x^n + a_1x^{n-1} + \dots + a_n$  es entera, si los  $a_i$  son enteros.

**12.** Encuéntrese una raíz real de  $x^3 + x - 3$  con aproximación de la segunda cifra decimal.

**13.** Demuéstrese si  $x-a \mid f(x)$  y  $x-a \nmid g(x)$ , entonces

$$x-a \nmid f(x) + g(x).$$

## 6. ECUACIONES DE SEGUNDO GRADO

Como ejemplo de utilización del teorema del residuo describiremos en este párrafo la manera de encontrar las raíces de los polinomios de grado 2.

Sea  $f(x) = ax^2 + bx + c$  cualquier polinomio de segundo grado.

Podemos factorizarlo como sigue:

$$\begin{aligned} f(x) &= a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) \\ &= a\left(x^2 + 2\frac{b}{2a}x + \left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right) \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right]. \end{aligned}$$

Sea

$$\alpha = \frac{\sqrt{b^2 - 4ac}}{2a}.$$

Es decir,  $\alpha$  es uno cualquiera de los dos complejos que tiene la propiedad

$$\alpha^2 = \frac{b^2 - 4ac}{4a^2}.$$

Entonces

$$\begin{aligned} f(x) &= a\left[\left(x + \frac{b}{2a}\right)^2 - \alpha^2\right] \\ &= a\left(x + \frac{b}{2a} + \alpha\right)\left(x + \frac{b}{2a} - \alpha\right) \\ &= a\left[x - \left(-\frac{b}{2a} - \alpha\right)\right]\left[x - \left(-\frac{b}{2a} + \alpha\right)\right]. \end{aligned}$$

Esta es la factorización de  $f(x)$  que buscábamos.

Vemos que:

$$x - \left( -\frac{b}{2a} - \alpha \right) \mid f(x),$$

$$x - \left( -\frac{b}{2a} + \alpha \right) \mid f(x),$$

lo que implica, por el corolario 1 del teorema del residuo, que

$$-\frac{b}{2a} - \alpha \text{ es raíz de } f(x),$$

$$-\frac{b}{2a} + \alpha \text{ es raíz de } f(x).$$

Sustituyendo  $\alpha$  por su expresión con radicales llegamos al siguiente resultado familiar:

Las raíces del polinomio  $ax^2 + bx + c$  de grado 2 son:

$$\frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{y} \quad \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Una última observación. Acabamos de admitir tácitamente que las únicas raíces de nuestro polinomio son las que se acaban de obtener. Esto se justifica así:

Sea  $\beta$  cualquier raíz de  $ax^2 + bx + c$ . Entonces

$$x - \beta \mid a \left[ x - \left( -\frac{b}{2a} + \alpha \right) \right] \left[ x - \left( -\frac{b}{2a} - \alpha \right) \right].$$

Por el corolario 3 del teorema del residuo  $x - \beta$  debe dividir a uno de los polinomios que están entre corchetes (puesto que  $x - \beta \nmid a$ ). Por lo tanto se tiene que cumplir una de las igualdades:

$$\beta = -\frac{b}{2a} - \alpha,$$

$$\beta = -\frac{b}{2a} + \alpha,$$

como se quería demostrar.

## EJERCICIOS

1. Dése una ecuación de grado 2 que no tenga dos soluciones diferentes.
2. Dése un polinomio de grado 2 con coeficientes reales que no tenga ninguna raíz real.
3. El *discriminante* del polinomio  $f(x) = ax^2 + bx + c$  es  $\Delta = b^2 - 4ac$ . Demuéstrelo lo siguiente, suponiendo que  $a$ ,  $b$  y  $c$  son reales, y  $a \neq 0$ :
  - a) Si  $\Delta > 0$ ,  $f(x)$  tiene dos raíces reales diferentes.
  - b) Si  $\Delta = 0$ ,  $f(x)$  tiene una sola raíz, que es real.
  - c) Si  $\Delta < 0$ ,  $f(x)$  tiene dos raíces no reales, conjugadas una de la otra.

## 7. DIVISIÓN SINTÉTICA. EXPRESIÓN DE UN POLINOMIO EN LA FORMA $\sum a_i(x-a)^i$

Reflexionemos sobre la división de un polinomio entre un binomio  $x-a$ . Dividamos, por ejemplo,  $2x^4 - 5x^3 + 2x^2 - x + 9$  entre  $x-3$ :

$$\begin{array}{r}
 2x^4 - 5x^3 + 2x^2 - x + 9 \\
 - 2x^4 + 6x^3 \\
 \hline
 x^3 + 2x^2 - x + 9 \\
 - x^3 + 3x^2 \\
 \hline
 5x^2 - x + 9 \\
 - 5x^2 + 15x \\
 \hline
 14x + 9 \\
 - 14x + 42 \\
 \hline
 51
 \end{array}
 \quad
 \begin{array}{c|l}
 & x-3 \\
 \hline
 & 2x^3 + x^2 + 5x + 14
 \end{array}$$

Si no escribimos los símbolos  $x^i$  y solo escribimos los coeficientes, y si omitimos también lo superfluo, la división queda como sigue:

$$\begin{array}{r}
 2 \quad -5 \quad 2 \quad -1 \quad 9 \\
 \underline{-} \quad 6 \\
 \hline
 1 \\
 \underline{\quad 3 \quad} \\
 5 \\
 \underline{\quad 15 \quad} \\
 14 \\
 \underline{\quad 42 \quad} \\
 51
 \end{array}
 \quad
 \begin{array}{c|l}
 & 3 \\
 \hline
 & 2+1+5+14
 \end{array}$$

Observemos:

Primero, que los coeficientes del cociente son el primer número del primer renglón y los números que aparecen inmediatamente abajo de las rayas horizontales, con excepción del último de ellos, que es el resto. Segundo, que el número que aparece en el renglón siguiente al de cada uno de los coeficientes del cociente es igual a ese coeficiente multiplicado por  $a$ , que en nuestro caso es 3. Finalmente, que cada uno de los números que aparecen inmediatamente abajo de las líneas horizontales es la suma de los otros dos números que aparecen en su misma columna (en renglones anteriores).

Para ahorrar espacio podemos escribir la misma división en la forma:

$$\begin{array}{r} 2 & -5 & 2 & -1 & 9 \\ & 6 & 3 & 15 & 42 \\ \hline 2 & 1 & 5 & 14 & | 51 \end{array} \quad | \underline{3}$$

Los números que aparecen en el último renglón (antes de la raya vertical), son los coeficientes del cociente; el que aparece al final es el resto. Según las observaciones anteriores la regla para formar el segundo y tercer renglones a partir del primero es la siguiente: se pone el primer coeficiente (2) abajo de la raya, se multiplica por  $a$  (por 3) y se pone el resultado (6) arriba de la raya, debajo del segundo coeficiente ( $-5$ ), y se suma con este escribiendo el resultado (1) abajo de la raya; se multiplica este resultado por  $a$  y se escribe el producto (3) arriba de la raya, debajo del tercer coeficiente, etc.

Otro ejemplo:

$$\begin{array}{r} -1 & 2 & -2 & 0 & 3 & 5 \\ & 2 & -8 & 20 & -40 & 74 \\ \hline -1 & 4 & -10 & 20 & -37 & | 79 \end{array} \quad | \underline{-2}$$

Así que

$$-x^5 + 2x^4 - 2x^3 + 3x + 5 = (x+2)(-x^4 + 4x^3 - 10x^2 - 20x - 37) + 79.$$

A este procedimiento abreviado se le llama *división sintética*.

Consideremos un polinomio  $f(x)$  de grado  $n$  y un complejo  $a$  y hagamos la siguiente serie de divisiones:

$$\begin{aligned} f(x) &= (x-a)f_1(x) + b_0 \\ f_1(x) &= (x-a)f_2(x) + b_1 \\ &\dots \\ f_{n-1}(x) &= (x-a)f_n(x) + b_{n-1}. \end{aligned}$$

Como  $f_i(x)$  es de grado  $n-i$  es claro que  $f_n(x) \in \mathbf{C}$ . Sea

$$f_n(x) = b_n \in \mathbf{C}.$$

Tenemos entonces, usando sucesivamente estas igualdades,

$$\begin{aligned} f(x) &= b_0 + f_1(x)(x-a) \\ &= b_0 + b_1(x-a) + f_2(x)(x-a)^2 \\ &= b_0 + b_1(x-a) + b_2(x-a)^2 + f_3(x)(x-a)^3 \\ &\quad \dots \\ &= b_0 + b_1(x-a) + \dots + b_n(x-a)^n. \end{aligned}$$

Así hemos expresado el polinomio  $f(x)$  en la forma

$$f(x) = \sum_{i=0}^n b_i(x-a)^i,$$

en donde  $b_0$  es el resto de la división de  $f(x)$  entre  $x-a$ ;  $b_1$  el resto de la división del cociente de esa primera división entre  $x-a$ ;  $b_2$  el resto de la división del nuevo cociente entre  $x-a$ , etc.

Estos  $b_i$  se pueden ir obteniendo rápidamente usando la división sintética.

Supongamos, por ejemplo, que queremos expresar  $2x^4+3x^3-x^2+x-2$  en la forma  $\sum a_i(x-2)^i$ :

$$\begin{array}{r} 2 & 3 & -1 & 1 & -2 \\ & 4 & 14 & 26 & 54 \\ \hline 2 & 7 & 13 & 27 & 52 \\ & 4 & 22 & 70 & \\ \hline 2 & 11 & 35 & | & 97 \\ & 4 & 30 & & \\ \hline 2 & 15 & 65 & & \\ & 4 & & & \\ \hline 2 & | & 19 & & \end{array} \quad | 2$$

Hemos obtenido:

$$2x^4+3x^3-x^2+x-2 = 2(x-2)^4+19(x-2)^3+65(x-2)^2+97(x-2)+52.$$

### EJERCICIOS

- Exprésese  $x^2 + 3x + 1$  en la forma  $\sum a_i(x+1)^i$ .

2. Desde el punto de vista del cálculo diferencial un polinomio es una función que tiene derivadas de todos los órdenes. Si  $f(x) = \sum a_i (x-a)^i$ , demuéstrese que

$$a_i = \frac{f^{(i)}(a)}{i!}.$$

3. Exprésese  $x^4 - 3x^3 + 4x^2 - 5x + 2$  en la forma  $\sum a_i (x-1)^i$ .

## 8. CÁLCULO DE UNA RAÍZ AISLADA EN UN INTERVALO EN CUYOS EXTREMOS EL POLINOMIO TIENE SIGNOS CONTRARIOS

En este párrafo se utilizará la siguiente proposición del cálculo diferencial:

Si  $\phi:[a, b] \rightarrow \mathbf{R}$  es continua,  $Im\phi \supset [\phi(a), \phi(b)]$ .

Todo polinomio es una función continua. Por lo tanto, si  $f(a)$  y  $f(b)$  son de signos contrarios,  $f(x)$  tiene una raíz en  $[a, b]$ . Supondremos esto y además supondremos que  $f(x)$  tiene una sola raíz en el intervalo  $[a, b]$ .

El método teóricamente más simple de obtener la raíz  $\alpha$  de  $f(x)$  con tanta aproximación como se quiera consiste en ir obteniendo intervalos más y más pequeños en cuyos extremos el polinomio tenga signos diferentes. Es claro que  $\alpha$  está en cada uno de esos intervalos. Si  $[a', b']$  es uno de esos intervalos es claro que  $|\alpha - a'| < b' - a'$ . Si  $[a', b']$  es muy pequeño tendremos  $\alpha$  con una aproximación muy grande: si, por ejemplo,  $b' - a' = 0.001$  tendremos que  $|\alpha - a'| < 0.001$  y podremos escribir  $\alpha = a'$  con aproximación de milésimos.

Es claro que esto puede hacerse de muchas maneras. Podemos, por ejemplo, tomar el punto medio  $c = \frac{1}{2}(a+b)$  del intervalo y calcular  $f(c)$ . El signo de  $f(c)$  es contrario al de  $f(a)$  o al de  $f(b)$ , [excepto si  $f(c) = 0$ , en cuyo caso  $\alpha = c$  y nuestra labor ha terminado]. Supongamos que  $f(a) \times f(c) < 0$ . Entonces  $\alpha \in [a, c]$  y podemos repetir el proceso con  $[a, c]$  y con los nuevos intervalos que se vayan obteniendo. A la  $n$ -ésima etapa habremos encontrado un intervalo  $[a', b']$  de longitud  $2^{-n}(b-a)$  que contiene a  $\alpha$ . Entonces tendremos que

$$\alpha = a' \text{ con aproximación } \frac{b-a}{2^n}.$$

Si, por ejemplo,  $a = 3$  y  $b = 7$  y queremos encontrar  $\alpha$  con aproximación de milésimas, el número  $n$  de etapas debe satisfacer la condición

$$\frac{7-3}{2^n} \leq 0.001,$$

es decir,

$$2^n \geq 4000$$

$$n \geq \frac{\log 4000}{\log 2}$$

Este tipo de procedimiento es muy laborioso. Describiremos otro método que tiene un fundamento teórico más complejo pero que es mucho más eficiente.

**El método de Horner.** Lo describiremos en el caso en que  $\alpha$  está aislada en un intervalo  $[A, A+1]$  [en cuyos extremos  $f(x)$  tiene signos contrarios], siendo  $A$  un entero no negativo. En ese caso la raíz  $\alpha$  se expresa como un decimal

$$\alpha = A \cdot a_1 a_2 a_3 \dots$$

y nuestro problema es encontrar tantas de las cifras  $a_i$  como queramos. En el método de Horner se construyen polinomios  $f_0(x), f_1(x), f_2(x), \dots$ , que tienen la propiedad

$$f_0(c-A) = f(c) \text{ y } f_i(c-A \cdot a_1 \dots a_i) = f(c) \text{ para todo } c \in \mathbb{C}. \quad (1)$$

Una vez conocido  $f_i(x)$  puede obtenerse  $a_{i+1}$ , y una vez obtenida  $a_{i+1}$  podemos obtener  $f_{i+1}(x)$ . El método queda perfectamente descrito una vez que se describan a) Cómo obtener  $f_0(x)$ ; b) cómo obtener  $a_{i+1}$  conocido  $f_i(x)$ ; c) cómo obtener  $f_{i+1}(x)$  conocidos  $f_i(x)$  y  $a_{i+1}$ . Esto es lo que haremos a continuación.

1º Expresamos  $f(x)$  en la forma

$$f(x) = \sum_j a_{0,j} (x-A)^j;$$

por el método descrito en el párrafo 7; definimos

$$f_0(x) = \sum_j a_{0,j} x^j.$$

Es claro que se cumple (1):

$$f_0(c-A) = \sum_j a_{0,j} (c-A)^j = f(c).$$

2º Conocido  $f_i(x)$ , que cumple (1), calculemos  $f_i(10^{-i-1})$ ,  $f_i(10^{-i-1} \times 2)$ ,  $f_i(10^{-i-1} \times 3)$ , etc., que son los restos de la división de  $f_i(x)$  entre  $x - 10^{-i-1}$ ,

$x - 10^{-i-1} \times 2$ ,  $x - 10^{-i-1} \times 3$ , etc., hasta obtener el primer natural  $k$  para el cual  $f_i(10^{-i-1}k)$  es de signo contrario al de  $f(A)$ . Es claro que  $f_i(10^{-i-1}(k-1))$  tiene el mismo signo que  $f(A)$  o es cero. Observando que, por (1),

$$\begin{aligned} f(A \cdot a_1 \dots a_i + 10^{-i-1}(k-1)) &= f_i(10^{-i-1}(k-1)), \\ f(A \cdot a_1 \dots a_i + 10^{-i-1}k) &= f_i(10^{-i-1}k), \end{aligned}$$

es claro entonces que

$$\alpha \in [A \cdot a_1 \dots a_i + 10^{-i-1}(k-1), A \cdot a_1 \dots a_i + 10^{-i-1}k].$$

Como, obviamente,

$$\alpha \in [A \cdot a_1 \dots a_{i+1}, A \cdot a_1 \dots a_{i+1} + 10^{-i-1}],$$

concluimos que

$$a_{i+1} = k - 1.$$

[Si  $f_i(10^{-i-1}(k-1)) = f_i(10^{-i-1}a_{i+1}) = 0$ , entonces  $f(A \cdot a_1 \dots a_{i+1}) = 0$  y el proceso termina puesto que  $\alpha = A \cdot a_1 \dots a_{i+1}$ .]

3º Expresemos  $f_i(x)$  como

$$f_i(x) = \sum_j a_{i+1,j} (x - 10^{-i-1}a_{i+1})^j,$$

por el procedimiento del párrafo 7 y definamos

$$f_{i+1}(x) = \sum_j a_{i+1,j} x^j.$$

Es claro que se cumple (1):

$$\begin{aligned} f_{i+1}(c - A \cdot a_1 \dots a_{i+1}) &= f_{i+1}(c - A \cdot a_1 \dots a_i - 10^{-i-1}a_{i+1}) \\ &= f_i(c - A \cdot a_1 \dots a_i) = f(c). \end{aligned}$$

Así termina la descripción del método. Si  $\alpha$  está aislada en  $[-A - 1, -A]$ , donde  $A$  es un entero no negativo, es claro que  $\alpha = -A \cdot a_1 a_2 \dots$  y la descripción de los pasos 1º, 2º y 3º es válida también en este caso, si tenemos cuidado de anteponerle el signo  $-$  a  $A$ ,  $A \cdot a_1 \dots a_i$ ,  $A \cdot a_1 \dots a_{i+1}$  y  $10^{-i-1}$  y en todas sus apariciones, y en cambiar el orden en que están escritos los extremos de los intervalos que aparecen en el paso 2º.

**Ejemplo**

Sea  $f(x) = x^3 + x - 3$ . Vemos que  $f(1) = -1 < 0$ ,  $f(2) = 6 > 0$ . La función es creciente en el intervalo  $[1, 2]$  (su derivada es positiva) y por lo tanto hay una sola raíz,

$$\alpha = 1. a_1 a_2 \dots$$

en ese intervalo.

Calculamos  $f_0(x)$

$$\begin{array}{r} 1 \ 0 \ 1 \ -3 \ | \ 1 \\ \underline{-} \quad 1 \ 1 \ 2 \\ 1 \ 1 \ 2 \ | \ -1 \\ \underline{-} \quad 1 \ 2 \\ 1 \ 2 \ | \ 4 \\ \underline{-} \quad 1 \\ 1 \ 3 \end{array}$$

$$f_0(x) = x^3 + 3x^2 + 4x - 1.$$

Calculamos  $a_1$

$$\left. \begin{array}{r} 1 \ 3 \ 4 \ -1 \ | \ 0.1 \\ 0.1 \ 0.31 \ 0.431 \\ \hline 1 \ 3.1 \ 4.31 \ -0.569 < 0 \\ 1 \ 3 \ 4 \ -1 \ | \ 0.2 \\ 0.2 \ 0.64 \ 0.928 \\ \hline 1 \ 3.2 \ 4.64 \ -0.072 < 0 \\ 1 \ 3 \ 4 \ -1 \ | \ 0.3 \\ 0.3 \ 0.99 \ 1.497 \\ \hline 1 \ 3.3 \ 4.99 \ 0.497 > 0 \end{array} \right\} a_1 = 2$$

Calculamos  $f_1(x)$

$$\begin{array}{r} 1 \ 3 \ 4 \ -1 \ | \ 0.2 \\ 0.2 \ 0.64 \ 0.928 \\ \hline 0.2 \ 0.68 \ | \ -0.072 \\ 1 \ 3.2 \ 4.64 \\ \hline 1 \ 3.4 \ | \ 5.32 \\ 0.2 \\ \hline 1 \ 3.6 \end{array}$$

$$f_1(x) = x^3 + 3.6x^2 + 5.32x - 0.072.$$

Calculamos  $a_2$

1	3.6	5.32	-0.072	0.01
	0.01	0.0361	0.053561	
1	3.61	5.3561	-0.018439 < 0	0.02
	1	3.6	5.32	0.02
	0.02	0.0724	0.107848	
1	3.62	5.3924	0.035848 > 0	

Si solamente queremos aproximar hasta la segunda cifra decimal tenemos  $\alpha = 1.21$ . Si queremos más aproximación continuamos el procedimiento.

Hemos descrito como obtener las raíces reales una vez que se han aislado convenientemente. En muchos casos es suficiente un poco de ingenio para lograr esto, como se ha visto en el ejemplo anterior, pero no siempre es este el caso. En un párrafo posterior se demuestra el teorema de Sturm, que proporciona un medio seguro de aislar las raíces reales de un polinomio con coeficientes racionales. En cuanto a las raíces complejas, véase el párrafo 16.

## EJERCICIOS

- Calcúlese  $\sqrt[n]{2}$  para  $n = 1, 2, 3, 4$ , approximando hasta la tercera cifra decimal (aplique el método de Horner a  $x^n - 2$  para  $n = 1, 2, 3, 4$ ).
- Encuéntrense las raíces del polinomio  $x^3 - 2x^2 + 2$  con aproximación de centésimas. (Para aislar las raíces conviene dibujar la gráfica de la función con sus máximos y mínimos.)

## 9. FACTORIZACIÓN DE UN POLINOMIO. RAÍCES MÚLTIPLES

**Teorema de factorización.** *Sea  $f(x)$  un polinomio de grado  $n > 0$  con coeficientes complejos. Existen  $n$  números complejos,  $\alpha_1, \dots, \alpha_n$ , no necesariamente diferentes dos a dos, y un complejo  $c$  tales que*

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n).$$

*Además, esta factorización es única. Es decir, si*

$$f(x) = c'(x - \alpha'_1) \cdots (x - \alpha'_n),$$

*entonces  $c' = c$  y existe una permutación  $\varphi$  de  $\{1, \dots, n\}$ , de manera que  $\alpha'_i = \alpha_{\varphi(i)}$  para todo  $i$ .*

*Demostración.*

1. Demostraremos primero la existencia de la factorización total, por inducción sobre el grado  $n$ . Si  $n = 1$  se tiene

$$f(x) = a_0 + a_1 x = a_1(x - (-a_1^{-1}a_0)).$$

Supóngase que todo polinomio de grado  $n$  se puede factorizar como se afirma en el teorema y considérese un polinomio  $f(x)$  de grado  $n + 1$ . Por el teorema final del párrafo 5,  $f(x)$  tiene una raíz  $\alpha$ , y

$$f(x) = (x - \alpha) q(x),$$

por el corolario 1 del teorema del residuo. Por la hipótesis de inducción

$$q(x) = c(x - \alpha_1) \cdots (x - \alpha_n),$$

de donde, tomando  $\alpha_{n+1} = \alpha$ ,

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_{n+1}),$$

como se quería demostrar.

2. La unicidad también se demostrará por inducción. Sea  $n = 1$  y supóngase que

$$\begin{aligned} f(x) &= c(x - \alpha_1) = cx - c\alpha_1 \\ &= c'(x - \alpha'_1) = c'x - c'\alpha'_1. \end{aligned}$$

Entonces  $c' = c$ ,  $c\alpha_1 = c'\alpha'_1$  y, en consecuencia,  $\alpha'_1 = \alpha_1$ . Supóngase ahora que la unicidad es verdadera para polinomios de grado  $n$  y sea  $f(x)$  de grado  $n + 1$  tal que

$$\begin{aligned} f(x) &= c(x - \alpha_1) \cdots (x - \alpha_{n+1}) \\ &= c'(x - \alpha'_1) \cdots (x - \alpha'_{n+1}). \end{aligned}$$

Entonces  $x - \alpha'_{n+1} \mid c(x - \alpha_1) \cdots (x - \alpha_{n+1})$ , de donde  $x - \alpha'_{n+1} \mid x - \alpha_i$  para algún  $i$ , por el corolario 3 del teorema del residuo, de donde  $\alpha'_{n+1} = \alpha_i$ . Sea  $\psi$  cualquier permutación de  $\{1, \dots, n + 1\}$  que aplique  $n + 1$  en  $i$ . Observemos que  $\alpha'_{n+1} = \alpha_{\psi(n+1)}$  y que

$$c(x - \alpha_{\psi(1)}) \cdots (x - \alpha_{\psi(n+1)}) = c'(x - \alpha'_1) \cdots (x - \alpha'_{n+1})$$

Por lo tanto

$$c(x - \alpha_{\psi(1)}) \cdots (x - \alpha_{\psi(n+1)}) = c'(x - \alpha'_1) \cdots (x - \alpha'_{n+1})$$

y cancelando el último factor [(véase ejercicio 5) i) del párrafo 3],

$$c(x - \alpha_{\psi(1)}) \cdots (x - \alpha_{\psi(n)}) = c'(x - \alpha'_1) \cdots (x - \alpha'_n).$$

Introducimos la notación  $\alpha_{\psi(i)} = \alpha_i^*$ . Por la hipótesis de inducción  $c' = c$  y existe una permutación  $\chi$  de  $\{1, \dots, n\}$  tal que

$$\alpha'_i = \alpha_{\chi(i)}^* = \alpha_{\varphi(\chi(i))} \text{ para } i = 1, \dots, n.$$

Definiendo  $\chi(n+1) = n+1$  podemos considerar  $X$  como una permutación de  $\{1, \dots, n+1\}$ . Sea  $\varphi = \Psi \cdot X$ . Tenemos que

$$\alpha'_i = \alpha_{\varphi(i)} \text{ para } i = 1, \dots, n+1,$$

lo que termina la demostración.

**OBSERVACIÓN:** Sea  $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ ,  $c \neq 0$ ,  $n > 0$ . Entonces  $\alpha$  es raíz de  $f(x)$  si y solo si  $\alpha = \alpha_i$  para algún  $i$ .

En efecto,

$$f(\alpha) = 0 \iff c(\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0 \iff \alpha - \alpha_i = 0 \text{ para algún } i.$$

Se acaba de observar que a cada raíz  $\alpha$  de  $f(x)$  le corresponde un factor  $x - \alpha$  en la factorización de  $f(x)$ . Pero este factor puede aparecer más de una vez. Esto da lugar a la noción de *multiplicidad* de una raíz:

**DEFINICIÓN:** Sea  $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$  un polinomio de grado  $n > 0$ . Sea  $\alpha \in \mathbb{C}$ . Se dice que  $\alpha$  es raíz de multiplicidad  $m$  de  $f(x)$  si hay precisamente  $m$  índices  $i$  para los cuales  $\alpha_i = \alpha$ .

Se puede también definir la multiplicidad como sigue:

**DEFINICIÓN:**  $\alpha$  es raíz de multiplicidad  $m$  del polinomio  $f(x)$  de grado positivo si  $(x - \alpha)^m \mid f(x)$  pero  $(x - \alpha)^{m+1} \nmid f(x)$ .

Es indispensable comprobar que las dos definiciones son equivalentes, lo que se deja al cuidado del lector.

## EJERCICIOS

1. Sean  $\alpha_1, \dots, \alpha_r$ , todas las raíces diferentes de  $f(x)$ . Sea  $m_i$  la multiplicidad de la raíz  $\alpha_i$ . Demuéstrese que

$$m_1 + \cdots + m_r = \text{grado de } f(x).$$

**2.** Encuéntrese un polinomio de grado 5 del cual son raíces 0, 1, 2, 3 y 4.

**3.** Supóngase que  $\alpha$  es raíz de multiplicidad  $m_1$  de  $f_1(x)$  y raíz de multiplicidad  $m_2$  de  $f_2(x)$ . Demuéstrese que  $\alpha$  es raíz de multiplicidad  $\geq \min(m_1, m_2)$  de  $f_1(x)g_1(x) + f_2(x)g_2(x)$ , cualesquiera que sean  $g_1(x)$  y  $g_2(x)$ . Si  $m_1 > m_2$ , demuéstrese que  $\alpha$  es raíz de multiplicidad  $m_2$  de  $f_1(x) + f_2(x)$ .

**4.** Usando la primera definición de multiplicidad demuéstrese la equivalencia de las afirmaciones siguientes:

- a)  $\alpha$  es raíz de multiplicidad 0 de  $f(x)$ ;
- b)  $\alpha$  no es raíz de  $f(x)$ .

**5.** Sea  $f(x) = g(x)h(x)$ . Supóngase que  $\alpha$  es raíz de  $g(x)$  y de  $h(x)$ , con multiplicidades  $m_1$  y  $m_2$ , respectivamente. Demuéstrese que  $\alpha$  es raíz de multiplicidad  $m_1 + m_2$  de  $f(x)$ .

**6.** Determínese la multiplicidad de 1 como raíz de cada uno de los polinomios siguientes:

$$\begin{aligned}x^4 - 2x^3 + 2x^2 - 2x + 1, \\x^4 - x^3, \\x^5 - 3x^4 + 5x^3 - 4x^2 + 3x - 1.\end{aligned}$$

**7.** Supóngase que  $f(\alpha) = g(\alpha)$  para todo  $\alpha \in \mathbb{C}$ . Demuéstrese que  $f(x) = g(x)$ .

## 10. DERIVADAS Y MULTIPLICIDAD

**Derivadas.** Sea  $f(x) = a_0 + a_1x + \dots + a_nx^n$ ;  $a_i \in \mathbb{C}$

Definimos la *derivada*  $f'(x)$  de  $f(x)$  como sigue:

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \dots + na_nx^{n-1}.$$

Para  $n \geq 1$  definimos la  $n+1$ -ésima derivada,  $f^{(n)}(x)$ , como la derivada de la  $n$ -ésima derivada. Con esto queda definida  $f^{(n)}(x)$  para todo  $n \in \mathbb{N}$ .

**PROPOSICIÓN:** *Sea  $f(x) = g(x)h(x)$ . Entonces*

$$f'(x) = g(x)h'(x) + g'(x)h(x).$$

*Demostración.* Si  $g(x)$  y  $h(x)$  tienen coeficientes reales la proposición es un caso particular de un teorema del cálculo diferencial. Pero hay una demostración simple que no utiliza el cálculo y que además es válida para coeficientes complejos. Esta es la que daremos. Usaremos la notación

$$g(x) = a_0 + a_1x + \dots = \sum_{i=0}^{\infty} a_i x^i$$

$$h(x) = b_0 + b_1x + \dots = \sum_{i=0}^{\infty} b_i x^i.$$

Entonces

$$\begin{aligned}
 f(x) &= \sum_{k=0}^{\infty} \sum_{i+j=k} a_i b_j x^k \\
 f'(x) &= \sum_{k=0}^{\infty} (k+1) \sum_{i+j=k+1} a_i b_j x^k \\
 g'(x) &= \sum_{k=0}^{\infty} (k+1) a_{k+1} x^k \\
 &= \sum_{k=0}^{\infty} a'_k x^k, \text{ donde } a'_k = (k+1) a_{k+1}, \\
 h'(x) &= \sum_{k=0}^{\infty} b'_k x^k, \text{ donde } b'_k = (k+1) b_{k+1}, \\
 g(x) h'(x) &= \sum_{k=0}^{\infty} \sum_{i+j=k} a_i b'_{j+1} x^k \\
 &= \sum_{k=0}^{\infty} \sum_{i+j=k} (j+1) a_i b_{j+1} x^k \\
 &= \sum_{k=0}^{\infty} \sum_{i+j=k+1} j a_i b_j x^k \\
 g'(x) h(x) &= \sum_{k=0}^{\infty} \sum_{i+j=k+1} i a_i b_j x^k \\
 g(x) h'(x) + g'(x) h(x) &= \sum_{k=0}^{\infty} \sum_{i+j=k+1} (k+1) a_i b_j x^k = f'(x)
 \end{aligned}$$

**PROPOSICIÓN:** Si  $f(x) = g(x)^m$ , entonces

$$f'(x) = m g(x)^{m-1} g'(x).$$

La demostración se puede hacer fácilmente por inducción.

**TEOREMA:** Sea  $f(x)$  de grado  $n > 0$  y sea  $m$  un entero positivo.  $\alpha$  es raíz de multiplicidad  $m$  de  $f(x)$  si y solo si se cumplen las condiciones siguientes:

- a)  $f(\alpha) = f'(\alpha) = \dots = f^{(m-1)}(\alpha) = 0$
- b)  $f^{(m)}(\alpha) \neq 0$ .

[Convenimos en que  $f^{(0)}(x) = f(x)$ . En el caso  $m = 1$  la condición a) se reduce a  $f(\alpha) = 0$ .]

*Demostración* (por inducción) :

1. Afirmación directa. Para  $m = 1$ ,  $f(x) = (x - \alpha)g(x)$  y  $x - \alpha \nmid g(x)$ . Entonces  $f'(x) = (x - \alpha)g'(x) + g(x)$  y  $f'(\alpha) = g(\alpha) \neq 0$ . Supondremos ahora que la afirmación es verdadera para  $m$  y la demostrarímos para  $m + 1$ . Tenemos que  $f(x) = (x - \alpha)^{m+1}g(x)$  y  $x - \alpha \nmid g(x)$ . Entonces

$$\begin{aligned} f'(x) &= (x - \alpha)^{m+1}g'(x) + (m+1)(x - \alpha)^m g(x) \\ &= (x - \alpha)^m((x - \alpha)g'(x) + (m+1)g(x)), \end{aligned}$$

y es claro que  $x - \alpha$  no divide al segundo factor. Por lo tanto  $\alpha$  es raíz de multiplicidad  $m$  de  $f'(x)$ . Por la hipótesis de inducción aplicada a  $f'(x)$  tenemos

$$f'(\alpha) = f''(\alpha) = \dots = f^{(m)}(\alpha) = 0, f^{(m+1)}(\alpha) \neq 0.$$

Como además  $f(\alpha) = 0$  hemos comprobado que se cumplen  $a)$  y  $b)$ .

2. Afirmación recíproca. Para  $m = 1$  las condiciones  $a)$  y  $b)$  nos dicen que  $f(\alpha) = 0$ , de donde  $f(x) = (x - \alpha)g(x)$ , y que  $f'(\alpha) \neq 0$ , y esto último implica que  $(x - \alpha)^2 \nmid f(x)$ , porque en caso contrario se tendría

$$\begin{aligned} f(x) &= (x - \alpha)^2 g_1(x) \\ f'(x) &= 2(x - \alpha)g_1(x) + (x - \alpha)^2 g'_1(x) \\ f'(\alpha) &= 0 \text{ (contradicción).} \end{aligned}$$

Supongamos ahora que la afirmación es verdadera para  $m$  y la demostrarímos que  $m + 1$ . Partimos de que

$$f(\alpha) = f'(\alpha) = \dots = f^{(m)}(\alpha) = 0, f^{(m+1)}(\alpha) \neq 0.$$

Por la hipótesis de inducción aplicada a  $f'(x)$  concluimos que  $\alpha$  es raíz de multiplicidad  $m$  de  $f'(x)$ , así que

$$f'(x) = (x - \alpha)^m g(x) \quad y \quad x - \alpha \nmid g(x).$$

Como  $f(\alpha) = 0$  tenemos, para algún  $s \geq 1$ ,

$$f(x) = (x - \alpha)^s g_1(x) \quad y \quad x - \alpha \nmid g_1(x).$$

Entonces

$$f'(x) = (x - \alpha)^{s-1} [(x - \alpha)g_1(x) + sg'_1(x)]$$

y es claro que  $x - \alpha$  no divide al segundo factor. Comparando esta expresión de  $f'(x)$  con la anterior vemos que  $s = m + 1$  y

$$f(x) = (x - \alpha)^{m+1} g_1(x) \quad y \quad x - \alpha \nmid g_1(x),$$

lo que termina la demostración.

## EJERCICIOS

1. El polinomio  $x^4 - 3x^3 - 6x^2 + 28x - 24$  tiene una raíz triple. Expréselo como producto de polinomios de grado 1.
2. El polinomio  $x^5 - 5\sqrt{2}x^4 + 8x^3 + 8\sqrt{2}x^2 - 20x + 4\sqrt{2}$  tiene una raíz cuádruple. ¿Cuál es?
3. Sea  $f(x) = x^4 + (2+4i)x^3 + (-5+6i)x^2 + (-6-2i)x - 2i$ . Se sabe que  $f'(i+\frac{1}{2}) = 0$  y que  $f(x)$  tiene raíces múltiples. Factorícese  $f(x)$  en polinomios de grado 1.
4. Demuéstrese que las únicas raíces de  $x^5 - ix^4 + 2x^3 - 2ix^2 + x - i$  son  $i$  y  $-i$ .
5. Demuéstrese que  $x^5 - 5x^4 + 1$  no tiene ninguna raíz de multiplicidad 4.

## 11. COEFICIENTES Y RAÍCES

PROPOSICIÓN: Sea

$$x^n + a_1x^{n-1} + \dots + a_n = (x - \alpha_1) \dots (x - \alpha_n).$$

Entonces

$$a_i = \sum_{1 \leq r_1 < \dots < r_i \leq n} \prod_{j=1}^i (-\alpha_{r_j})$$

para  $i = 1, 2, \dots, n$ .

Conviene aclarar la notación en la fórmula anterior. El significado del símbolo

$$\sum_{1 \leq r_1 < \dots < r_i \leq n}$$

es que para cada sistema de  $i$  números enteros  $r_1, \dots, r_i$  que satisfacen las condiciones  $1 \leq r_1 < \dots < r_i \leq n$  debe considerarse el sumando

$$\prod_{j=1}^i (-\alpha_{r_j}) = (-\alpha_{r_1})(-\alpha_{r_2}) \dots (-\alpha_{r_i})$$

correspondiente a esos  $r_1, \dots, r_i$ .

Por ejemplo, si  $i = 2$  y  $n = 3$  tenemos las siguientes maneras de elegir  $r_1$  y  $r_2$ :

$$\begin{aligned} r_1 &= 1 & r_2 &= 2, \\ r_1 &= 1 & r_2 &= 3, \\ r_1 &= 2 & r_2 &= 3. \end{aligned}$$

Por lo tanto

$$\begin{aligned} \sum_{1 \leq r_1 < r_2 \leq 3} \prod_{j=1}^2 (-\alpha_{r_j}) &= \sum_{1 \leq r_1 < r_2 \leq 3} (-\alpha_{r_1})(-\alpha_{r_2}) \\ &= (-\alpha_1)(-\alpha_2) + (-\alpha_1)(-\alpha_3) + (-\alpha_2)(-\alpha_3) \\ &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3. \end{aligned}$$

Una vez aclarado el simbolismo se sugiere al lector que compruebe la proposición para  $n = 1, 2, 3, \dots$ , con lo que se convencerá que es verdadera y podrá dar una demostración general, que aquí omitiremos.

## EJERCICIOS

**1.** Demuéstrese la proposición anterior para  $n = 2$  a partir de las fórmulas obtenidas en el párrafo 6 para las raíces de una ecuación de segundo grado.

**2.** Sea  $(\alpha_1, \alpha_2, \dots)$  una sucesión cualquiera de números complejos. Sean

$$a_{n,i} = \sum_{1 \leq r_1 < \dots < r_i \leq n} \prod_{j=1}^i (-\alpha r_j)$$

para todos los naturales  $i, n$ , tales que  $i \leq n$ . Definimos también

$$s_{n,i} = \sum_{j=1}^n \alpha_j^i, \quad i \leq n.$$

Demuéstrese,

$$\alpha_{n,1} + s_{n,1} = 0 \text{ para todo } n \geq 1$$

$$2\alpha_{n,2} + \alpha_{n,1}s_{n,1} + s_{n,2} = 0 \text{ para todo } n \geq 2$$

$$3\alpha_{n,3} + \alpha_{n,2}s_{n,1} + \alpha_{n,1}s_{n,2} + s_{n,3} = 0 \text{ para } n \geq 3.$$

**3.** Con la notación del ejercicio anterior:

- a) Exprésense  $\alpha_{2,1}$  y  $\alpha_{2,2}$  en términos de  $s_{2,1}$  y  $s_{2,2}$ , y recíprocamente.
- b) Exprésense  $\alpha_{3,1}$ ,  $\alpha_{3,2}$  y  $\alpha_{3,3}$  en términos de  $s_{3,1}$ ,  $s_{3,2}$  y  $s_{3,3}$ , y recíprocamente.

**4.** Sean  $\alpha_1$  y  $\alpha_2$  las raíces de  $x^2 + bx + c$ . Demuéstrese que  $(\alpha_2 - \alpha_1)^2 = 4c - b^2$ .

## 12. POLINOMIOS CON COEFICIENTES REALES

Decimos que un polinomio es *mónico* si el coeficiente del término de grado máximo es 1.

Hemos visto en párrafos anteriores cómo un polinomio de grado positivo puede expresarse como una constante por un producto de polinomios monícos de primer grado.

En este párrafo veremos cómo todo polinomio con coeficientes reales puede expresarse como un número real por un producto de polinomios de dos tipos:

- a) polinomios monícos de grado 1 con coeficientes reales;
- b) polinomios monícos de grado 2 con coeficientes reales que no tienen raíces reales.

Por ejemplo, el polinomio  $x^3 - 1$  puede expresarse como

$$x^3 - 1 = (x - 1)(x - w)(x - w^2),$$

donde

$$w = \frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

pero también puede expresarse como

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

En esta última factorización los factores tienen coeficientes reales, lo que no sucede en la primera.

Necesitamos algunos preliminares.

Si  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ , escribiremos

$$\bar{f}(x) = \bar{a}_0x^n + \bar{a}_1x^{n-1} + \dots + \bar{a}_n.$$

Es claro que  $\bar{f}(x) = f(x)$  si y solo si  $f(x)$  tiene coeficientes reales.

Es fácil comprobar lo siguiente:

Si  $f(x) = g(x)h(x)$ , entonces  $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ ;

$$g(x) | f(x) \iff \bar{g}(x) | \bar{f}(x);$$

Si  $f(x)$  tiene coeficientes reales, entonces

$$g(x) | f(x) \iff \bar{g}(x) | \bar{f}(x).$$

Aplicaremos esta última observación al caso en que  $g(x) = (x - \alpha)^m$ . Tendremos el resultado siguiente:

**LEMA:** Sea  $f(x)$  un polinomio con coeficientes reales. Entonces

$$(x - \alpha)^m | f(x) \iff (x - \bar{\alpha})^m | \bar{f}(x).$$

Como consecuencia:

**PROPOSICIÓN:** Si  $\alpha$  es raíz de un polinomio con coeficientes reales,  $\bar{\alpha}$  es raíz del mismo polinomio con la misma multiplicidad.

Por tanto, si  $f(x)$  tiene coeficientes reales y

$$f(x) = c(x - \alpha_1)^{m_1} \dots (x - \alpha_r)^{m_r}, \quad \alpha_i \neq \alpha_j \text{ para } i \neq j,$$

cada vez que aparezca un factor  $(x - \alpha_i)^{m_i}$  en el que  $\alpha_i \notin \mathbb{R}$  aparecerá también el factor  $(x - \bar{\alpha}_i)^{m_i}$ .

Supongamos que  $\alpha_1, \dots, \alpha_s \in \mathbf{R}$ ,  $\alpha_{s+1}, \dots, \alpha_r \notin \mathbf{R}$ . Entonces los  $r-s$  complejos  $\alpha_{s+1}, \dots, \alpha_r$  aparecen por parejas de conjugados, es decir que  $r-s$  es par, pongamos  $r-s = 2t$ , y podemos suponer que

$$\alpha_{r+i+t} = \bar{\alpha}_{r+i} \text{ para } i = 1, \dots, t;$$

podemos escribir

$$\begin{aligned} f(x) &= c \prod_{i=1}^s (x - \alpha_i)^{m_i} \prod_{i=1}^t (x - \alpha_{s+i})^{m_{s+i}} \prod_{i=1}^t (x - \bar{\alpha}_{s+i})^{m_{s+i}} \\ &= c \prod_{i=1}^s g_i(x)^{m_i} \prod_{i=1}^t f_i(x)^{m_{s+i}}, \end{aligned}$$

donde

$$\begin{aligned} g_i(x) &= x - \alpha_i \\ f_i(x) &= (x - \alpha_{s+i})(x - \bar{\alpha}_{s+i}) \\ &= x^2 - (\alpha_{s+i} + \bar{\alpha}_{s+i})x + \alpha_{s+i}\bar{\alpha}_{s+i}. \end{aligned}$$

Los polinomios  $g_i(x)$  y  $f_i(x)$  tienen coeficientes reales. Es claro también que  $c \in \mathbf{R}$ , puesto que es el cociente de dos polinomios con coeficientes reales. Así queda demostrado el resultado enunciado al principio, que volvemos a expresar a continuación:

**TEOREMA:** Todo polinomio  $f(x)$  de grado positivo con coeficientes reales puede expresarse como producto de algún real y ciertos polinomios de primero o segundo grados, con coeficientes reales, con la particularidad de que estos últimos (los de segundo grado) no pueden, a su vez, expresarse como productos de polinomios de primer grado con coeficientes reales.

## EJERCICIOS

1. Exprésense los polinomios  $x^4 - 1$  y  $x^6 - 1$  como productos de polinomios con coeficientes reales de grados uno y dos.
2. Compruébese que  $\frac{1}{2}(-1 + \sqrt{5} + \sqrt[5]{10 + 2\sqrt{5}}i)$  es una raíz quinta de 1 y exprése  $x^4 + x^3 + x^2 + x + 1$  como producto de dos polinomios de segundo grado con coeficientes reales.

## 13. EL ALGORITMO DE EUCLIDES CON POLINOMIOS

Para polinomios existe la noción de máximo común divisor lo mismo que para enteros. La teoría es análoga en los dos casos. En este párrafo se enunciarán los resultados sin demostración. El lector podrá demostrarlos guiándose, si es necesario, por las demostraciones de los resultados análogos para enteros.

**PROPOSICIÓN 1:** Sean  $f_1(x)$  y  $f_2(x)$  dos polinomios cualesquiera. Si  $g(x) \mid f_1(x)$  y  $g(x) \mid f_2(x)$ , entonces

$$g(x) \mid f_1(x)h_1(x) + f_2(x)h_2(x),$$

cualesquiera que sean  $h_1(x)$  y  $h_2(x)$ .

**PROPOSICIÓN 2:** Sean  $f_1(x)$  y  $f_2(x)$  dos polinomios no ambos nulos y sea

$$d(x) = f_1(x)g_1(x) + f_2(x)g_2(x)$$

una combinación lineal de ellos no nula de grado mínimo. Entonces  $d(x)$  divide a cualquier combinación lineal de  $f_1(x)$  y  $f_2(x)$ .

**COROLARIO:**  $d(x)$  divide a  $f_1(x)$  y a  $f_2(x)$ .

**DEFINICIÓN:** Sean  $f_1(x)$  y  $f_2(x)$  dos polinomios no ambos nulos. Llamamos **máximo común divisor** de  $f_1(x)$  y  $f_2(x)$  a cualquier combinación lineal de ellos no nula de grado mínimo.

**PROPOSICIÓN 3:** Dos máximos comunes divisores de  $f_1(x)$  y  $f_2(x)$  son asociados [recordemos que  $g(x)$  y  $h(x)$  son asociados si  $g(x) \mid h(x)$  y  $h(x) \mid g(x)$ ].

**PROPOSICIÓN 4:** Si  $d(x)$  es máximo común divisor de  $f_1(x)$  y  $f_2(x)$ , y si  $g(x)$  es cualquier otro divisor común de esos dos polinomios, entonces  $g(x) \mid d(x)$ .

**PROPOSICIÓN 5:** Si  $d(x)$  es un divisor común de  $f_1(x)$  y  $f_2(x)$  que es divisible entre cualquier otro divisor común de  $f_1(x)$  y  $f_2(x)$ , entonces  $d(x)$  es un máximo común divisor de  $f_1(x)$  y  $f_2(x)$ .

**NOTA 1.** El máximo común divisor de 0 y 0 es 0, por definición.

**NOTA 2.** Un máximo común divisor de 0 y  $f(x)$  es  $f(x)$ , según puede deducirse fácilmente de la definición.

**NOTA 3.** Hay un solo máximo común divisor mónico de dos polinomios que no sean ambos nulos. Podemos reservar el símbolo  $(f_1(x), f_2(x))$  para denominarlo y referirnos a él como “el máximo común divisor de  $f_1(x)$  y  $f_2(x)$ ”.

**NOTA 4.** El máximo común divisor de polinomios no nulos puede obtenerse por el algoritmo de Euclides lo mismo que en los enteros. Al tomar cada resto como un nuevo divisor podemos sustituirlo por cualquier polinomio asociado.

**NOTA 5.** La proposición siguiente (que el lector puede demostrar), es un ejemplo de la utilidad de la teoría del máximo común divisor para polinomios.

**PROPOSICIÓN 6:**  $f(x)$  tiene una raíz de multiplicidad  $> 1$  si y solo si  $(f(x), f'(x)) \neq 1$ .

### EJERCICIOS

1. Sean  $f(x)$  y  $g(x)$  dos polinomios no nulos. Supóngase que  $\{\alpha_1, \dots, \alpha_t\}$  es el conjunto de las raíces comunes de  $f(x)$  y  $g(x)$  y denótense por  $m_i$  y  $n_i$  las multiplicidades de  $\alpha_i$  como raíces de  $f(x)$  y  $g(x)$ , respectivamente. Demuéstrese que

$$(f(x), g(x)) = \prod_{i=1}^t (x - \alpha_i)^{\min(m_i, n_i)}.$$

2. Sea  $f_1(x)$  el cociente de las  $f(x)$  (no nulo) entre  $(f(x), f'(x))$ . Demuéstrese que  $f_1(x)$  tiene las mismas raíces que  $f(x)$ , pero todas ellas con multiplicidad 1.

3. Calcúlese el máximo común divisor de  $f(x) = x^7 + x^3 + 1$  y su derivada y compruébese que  $f(x)$  no tiene raíces de multiplicidad  $> 1$ .

4. Factorícese totalmente el polinomio

$$x^3 + (-6 - 3i)x^2 + (9 + 12i)x + (-2 - 11i).$$

### 14. AISLAMIENTO DE LAS RAÍCES REALES DE UN POLINOMIO CON COEFICIENTES REALES (TEOREMA DE STURM)

Sea  $f(x)$  un polinomio con coeficientes reales de grado positivo sin raíces múltiples (es decir, sin raíces de multiplicidad  $> 1$ ). El máximo común divisor de  $f(x)$  y  $f'(x)$  es 1. Poniendo

$$\begin{aligned} r_0(x) &= f(x) \\ r_1(x) &= f'(x) \end{aligned}$$

y denotando con  $r_2(x), r_3(x), \dots$ , los restos que se van obteniendo al aplicar el algoritmo de Euclides a  $f(x)$  y  $f'(x)$  tendremos

$$\begin{aligned} r_0(x) &= r_1(x) q_1(x) + r_2(x) \\ r_1(x) &= r_2(x) q_2(x) + r_3(x) \end{aligned}$$

$$r_{n-2}(x) = r_{n-1}(x) q_{n-1}(x) + r_n(x),$$

donde  $r_n(x)$  es una constante  $\neq 0$ .

Sean

$$\begin{aligned} f_0(x) &= r_0(x), f_1(x) = r_1(x), f_2(x) = -r_2(x), f_3(x) = -r_3(x), \\ f_4(x) &= r_4(x), f_5(x) = r_5(x), f_6(x) = -x_6(x), f_7(x) = -r_7(x), \\ &\text{etcétera.} \end{aligned}$$

Observamos que  $r_i(x) | r_{i-1}(x) - r_i(x)$  para  $i = 1, \dots, n - 1$ , de donde deducimos que

$$f_i(x) | f_{i-1}(x) + f_i(x) \text{ para } 1 \leq i \leq n - 1. \quad (1)$$

Si  $c$  es un real que no es raíz de ninguno  $f_i(x)$  consideremos el número de cambios de signo que aparecen en la sucesión  $f_0(c), \dots, f_n(c)$ , es decir, el número de índices  $i$  comprendidos entre 0 y  $n - 1$  para los cuales  $f_i(c)$  y  $f_{i+1}(c)$  tienen signos contrarios. Este número de variaciones de signo en  $c$  lo denotamos con  $V(c)$ .

**Teorema de Sturm.** Sea  $f(x)$  un polinomio con coeficientes reales de grado positivo y sean  $f_0(x), \dots, f_n(x)$  los polinomios (con coeficientes reales) que se acaban de definir. Sean  $a$  y  $b$  dos reales que no son raíces de ninguno de los  $f_i(x)$  y supóngase que  $a < b$ . El número de raíces de  $f(x)$  en el intervalo  $[a, b]$  es igual a  $V(a) - V(b)$ .

*Demostración.* Si no hay ninguna raíz de ninguno de los  $f_i(x)$  en  $[a, b]$  cada  $f_i(x)$  tiene el mismo signo a lo largo de todo el intervalo y es evidente que  $V(a) = V(b)$ , lo que comprueba el teorema. Eliminado este caso sean  $\rho_1, \dots, \rho_r$  todos los puntos de  $[a, b]$  que son raíces de algún  $f_i(x)$ , en orden creciente. Tomemos  $a_0 = a, a_1, \dots, a_{r-1}, a_r = b$  de manera que  $a_0 < \rho_1 < a_1 < \rho_2 < a_2 < \dots < a_{r-1} < \rho_r < a_r$ . Observamos que

$$V(a) - V(b) = \sum_{i=1}^r (V(a_{i-1}) - V(a_i)).$$

Debido a esto será suficiente demostrar que, para cada  $i$ ,

$$V(a_{i-1}) - V(a_i) = \begin{cases} 0 & \text{si } f(\rho_i) \neq 0 \\ 1 & \text{si } f(\rho_i) = 0 \end{cases}$$

Para simplificar la notación observaremos que demostrar esto último es lo mismo que demostrar el teorema con la hipótesis adicional de que solo hay un número  $\rho$  en  $[a, b]$  que es raíz de algún  $f_i(x)$ . Así, pues, supondremos esto y demostraremos que

$$V(a) - V(b) = \begin{cases} 0 & \text{si } f(\rho) \neq 0 \\ 1 & \text{si } f(\rho) = 0 \end{cases}$$

a) Si  $f(\rho) \neq 0$ . Entonces  $\rho$  es raíz de uno o más de los  $f_j(x)$  para  $1 \leq j \leq n - 1$ . Supongamos que  $\rho$  es raíz de  $f_{j_1}(x), \dots, f_{j_t}(x)$ . No hay dos de estos índices  $j_i$  que sean consecutivos, porque en caso contrario habría dos restos consecutivos en el algoritmo de Euclides con una raíz común, lo que permitiría deducir que  $f(x)$  y  $f'(x)$  tienen una raíz común. Al contar  $V(a)$  y  $V(b)$  podemos ignorar los cambios de signo entre  $f_j(x)$  y  $f_{j+1}(x)$  siempre que  $j$  y  $j + 1$  no pertenezcan a  $\{j_1, \dots, j_t\}$ , ya que cada una de esas dos funciones tiene el mismo signo a lo largo de  $[a, b]$  y un cambio de signo en  $a$  siempre va acompañado de un cambio en  $b$ , y viceversa, por lo que la diferencia  $V(a) - V(b)$  no está afectada por dichos cambios. Habremos demostrado que  $V(a) - V(b) = 0$  si comprobamos que el número de cambios de signo en cada una de las series

$$\begin{aligned} &f_{j_{t-1}}(a), f_{j_t}(a), f_{j_{t+1}}(a), \\ &f_{j_{t-1}}(b), f_{j_t}(b), f_{j_{t+1}}(b), \end{aligned}$$

es 1, para cualquier  $i$ . De (1) concluimos que  $f_{j_{t-1}}(\rho) + f_{j_{t+1}}(\rho) = 0$ , lo que implica que las funciones  $f_{j_{t-1}}(x)$  y  $f_{j_{t+1}}(x)$ , que no cambian de signo a lo largo de  $[a, b]$ , tienen signos contrarios. Tanto si  $f_{j_t}(a) > 0$  y  $f_{j_t}(b) < 0$  como si  $f_{j_t}(a) < 0$  y  $f_{j_t}(b) > 0$  hay un solo cambio de signo en cada una de las dos series.

b) Si  $f(\rho) = 0$ . Es claro que  $f'(x)$  tiene signo constante a lo largo de  $[a, b]$ , puesto que  $f'(\rho) \neq 0$ . Con un razonamiento análogo al de a) puede comprobarse que el número de cambios de signo que se presentan en la serie

$$f_1(a), \dots, f_n(a)$$

es el mismo que el de los de la serie

$$f_1(b), \dots, f_n(b).$$

Observando ahora que  $f(a)$  y  $f(b)$  tienen signos contrarios habremos demostrado el teorema una vez que comprobemos que  $f(b)$  y  $f'(b)$  tienen el mismo signo [porque entonces  $f(a)$  y  $f'(a)$  tendrán signos contrarios]. Para comprobarlo expresamos  $f(x)$  como

$$f(x) = a_0 + a_1(x - \rho) + a_2(x - \rho)^2 + \dots,$$

donde  $a_0 = f(\rho) = 0$  y  $a_1 = f'(\rho)$ , de donde

$$\text{signo de } a_1 = \text{signo de } f'(\rho) = \text{signo de } f'(b).$$

Nos falta ver que signo de  $f(b) = \text{signo de } a_1$ . Tómese  $\sigma \in (\rho, b)$  de manera que

$$|a_1(\sigma - \rho)| > |a_2(\sigma - \rho)^2 + a_3(\sigma - \rho)^3 + \dots|.$$

Entonces

$$\text{signo de } f(\sigma) = \text{signo de } a_1(\sigma - \rho) = \text{signo de } a_1.$$

Pero como no hay ninguna raíz de  $f(x)$  en  $[\sigma, b]$  tenemos

$$\text{signo de } f(b) = \text{signo de } f(\sigma) = \text{signo de } a_1.$$

**Un ejemplo de aplicación del teorema de Sturm.** Consideremos el polinomio  $f(x) = x^4 - x - 3$ . Aplicamos el algoritmo de Euclides a  $f(x)$  y su derivada:

$$\begin{array}{r}
 \begin{array}{c|ccc}
 x^4 & - & x & -3 \\
 -x^4 & + & \frac{1}{4}x & \\
 \hline
 & - & \frac{3}{4}x & -3
 \end{array} & | \begin{array}{c} 4x^3 - 1 \\ \hline \frac{1}{4}x \end{array} \\
 \hline
 \begin{array}{c|cc}
 4x^3 & & -1 \\
 -4x^3 & -16x^2 & \\
 \hline
 & -16x^2 & -1
 \end{array} & | \begin{array}{c} x+4 \\ \hline 4x^2 - 16x + 64 \end{array} \\
 \hline
 \begin{array}{c|cc}
 & & -1 \\
 & +16x^2 & +64x \\
 \hline
 & 64x & -1
 \end{array} & \\
 \begin{array}{c|cc}
 & -64x & -256 \\
 \hline
 & -257 &
 \end{array} & 
 \end{array}$$

[Si no llegáramos a que  $(f(x), f'(x)) = 1$  deberíamos dividir  $f(x)$  entre el máximo común divisor para poder aplicar el teorema de Sturm al cociente.]

Tenemos

$$\begin{aligned}
 f_0(x) &= x^4 - x - 3 \\
 f_1(x) &= 4x^3 - 1 \\
 f_2(x) &= \frac{3}{4}x + 3 \\
 f_3(x) &= 257
 \end{aligned}$$

Hacemos una tabla en la que en cada columna aparecen los signos de los valores de los  $f_i(x)$  para el valor de  $x$  que encabeza la columna. Bajo cada columna escribimos el número de cambios de signo:

	-2	2	0	-1	1
$f_0(x)$	+	+	-	-	-
$f_1(x)$	-	+	-	-	+
$f_2(x)$	+	+	+	+	+
$f_3(x)$	+	+	+	+	+
	2	0	1	1	1

Las dos primeras columnas nos muestran que hay dos raíces en  $[-2, 2]$ . Las otras columnas refinan el resultado y nos permiten concluir que hay una raíz en  $[-2, -1]$  y una raíz en  $[1, 2]$ . Estas se pueden calcular con los métodos del párrafo 8. Nos convencemos de que no hay raíces fuera de  $[-2, 2]$  gracias a la desigualdad

$$|x^4| > |x + 3| \quad \text{para } |x| > 2.$$

En general, para el polinomio  $x^n + a_1x^{n-1} + \dots + a_n$  podemos afirmar que, si  $|x| > \max(1, |a_1| + \dots + |a_n|) = A$ ,

$$|x^n| > |a_1x^{n-1} + \dots + a_n|,$$

y por lo tanto no hay raíces fuera de  $[-A, A]$ .

En algunos ejemplos en los que las raíces son muy cercanas puede ser necesario introducir muchos puntos intermedios antes de lograr aislar las raíces. Sin embargo, si nos piden que, por ejemplo, calculemos las raíces con aproximación de milésimas, una vez que tengamos varias raíces en un mismo intervalo de longitud  $< 0.001$  no necesitamos aislarlas, puesto que podemos tomar cualquier punto del intervalo como valor aproximado de todas esas raíces.

Un problema más grave puede presentarse, en cambio, si los coeficientes solo son conocidos aproximadamente (lo que siempre sucede si no son racionales), porque en ese caso la aproximación puede no ser suficiente para decidir si el valor de alguno de los  $f_i(x)$  en algún punto es positivo, negativo o cero.

### EJERCICIO

Aíslense y calcúlense todas las raíces reales de algunos polinomios.

## 15. FRACCIONES RACIONALES. DESCOMPOSICIÓN EN FRACCIONES PARCIALES

**Fracciones racionales.** Consideremos las expresiones:

$$\frac{f(x)}{g(x)}$$

formadas con los polinomios  $f(x)$  (*numerador*) y  $g(x) \neq 0$  (*denominador*). Introducimos una relación  $\sim$  en el conjunto de tales expresiones:

$$\frac{f_1(x)}{f_2(x)} \sim \frac{f_1(x)}{g_2(x)} \quad \text{si} \quad f_1(x)g_2(x) = f_2(x)g_1(x).$$

**LEMA:**  $\sim$ es una relación de equivalencia.

*Demostración* (ejercicio): La relación determina una partición del conjunto. Denotaremos la clase de un elemento con el mismo símbolo con que denotamos al elemento. Podremos entonces escribir  $=$  en lugar de  $\sim$ .

Las clases de esta partición son las *fracciones racionales*. Hay dos operaciones:

$$\begin{aligned}\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} &= \frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)} \\ \frac{f_1(x)}{g_1(x)} - \frac{f_2(x)}{g_2(x)} &= \frac{f_1(x)g_2(x) - f_2(x)g_1(x)}{g_1(x)g_2(x)}.\end{aligned}$$

Este procedimiento para pasar de los polinomios a las fracciones racionales es el mismo que se sigue frecuentemente para pasar de los enteros a los racionales.

En el cálculo integral es conveniente poder expresar las fracciones racionales como suma de otras de cierto tipo, cuyas integrales se conocen. En este párrafo se describirá cómo se logra esto.

**LEMA 1:** Si  $g(x) = h(x)k(x)$  y  $(h(x), k(x)) = 1$ , entonces para cada  $f(x)$  existen polinomios  $s(x)$  y  $t(x)$  tales que

$$\frac{f(x)}{g(x)} = \frac{s(x)}{h(x)} + \frac{t(x)}{k(x)}.$$

Si  $f(x)$ ,  $h(x)$  y  $k(x)$  tienen coeficientes reales,  $s(x)$  y  $t(x)$  también tienen coeficientes reales.

*Demostración.* Sean  $h_1(x)$  y  $k_1(x)$  tales que

$$1 = h(x)h_1(x) + k(x)k_1(x).$$

Entonces

$$\begin{aligned}\frac{f(x)}{g(x)} &= \frac{f(x)[h(x)h_1(x) + k(x)k_1(x)]}{g(x)} \\ &= \frac{f(x)h_1(x)}{k(x)} + \frac{f(x)k_1(x)}{h(x)},\end{aligned}$$

lo que demuestra el lema, para  $s(x) = f(x)k_1(x)$  y  $t(x) = f(x)h_1(x)$ . Cuando  $h(x)$  y  $k(x)$  tienen coeficientes reales lo mismo sucede con  $h_1(x)$  y  $k_1(x)$ , porque todos los polinomios que aparecen al aplicar el algoritmo de Euclides a dos polinomios con coeficientes reales tienen coeficientes reales. Si además  $f(x)$  tiene coeficientes reales es claro que  $s(x)$  y  $t(x)$  tienen coeficientes reales.

LEMÁ 2. Dados  $h(x)$  de grado positivo,  $f(x)$  y un entero positivo  $t$ , existen  $s_0(x), s_1(x), \dots, s_t(x)$ , con el grado de  $s_i(x)$  menor que el grado de  $h(x)$  para  $i = 1, \dots, t$ , tales que

$$\frac{f(x)}{h(x)^t} = s_0(x) + \frac{s_1(x)}{h(x)} + \dots + \frac{s_t(x)}{h(x)^t}.$$

Si  $f(x)$  y  $h(x)$  tienen coeficientes reales los polinomios  $s_i(x)$  también tienen coeficientes reales.

*Demostración.* Sea  $n = \text{grado de } h(x)$ .

$$\begin{aligned} f(x) &= h(x)q_1(x) + r_1(x), \text{ grado de } r_1(x) < n, \\ q_1(x) &= h(x)q_2(x) + r_2(x), \text{ grado de } r_2(x) < n, \\ q_2(x) &= h(x)q_3(x) + r_3(x), \text{ grado de } r_3(x) < n, \\ &\text{etcétera.} \end{aligned}$$

Como grado de  $q_{i+1}(x) < \text{grado de } q_i(x)$  se tendrá que grado de  $q_m(x) < n$  para algún  $m$ . La última igualdad será

$$q_{m-1}(x) = h(x)q_m(x) + r_m(x), \text{ grado de } r_m(x) < n.$$

Sustituyendo cada expresión de  $q_i(x)$  en la anterior, empezando con la última, se tiene

$$\begin{aligned} q_{m-1}(x) &= h(x)q_m(x) + r_m(x) \\ q_{m-2}(x) &= h(x)^2q_m(x) + h(x)r_m(x) + r_{m-1}(x) \\ q_{m-3}(x) &= h(x)^3q_m(x) + h(x)^2r_m(x) + h(x)r_{m-1}(x) + r_{m-2}(x) \\ &\dots \\ q_1(x) &= h(x)^{m-1}q_m(x) + h(x)^{m-2}r_m(x) + \dots + r_2(x) \\ f(x) &= h(x)^mq_m(x) + h(x)^{m-1}r_m(x) + \dots + h(x)r_2(x) + r_1(x), \end{aligned}$$

de donde

$$\frac{f(x)}{h(x)^t} = \frac{r_1(x)}{h(x)^t} + \frac{r_2(x)}{h(x)^{t-1}} + \dots + \frac{r_t(x)}{h(x)} + s_0(x)$$

y el lema queda demostrado tomando  $s_i(x) = r_{t-i+1}(x)$ .

A partir de estos lemas demostraríremos los teoremas que nos permiten descomponer una fracción racional en *fracciones parciales*.

TEOREMA 1. Sea  $g(x) = (x - \alpha_1)^{r_1} \cdots (x - \alpha_s)^{r_s}$ , donde  $\alpha_i \neq \alpha_j$  para  $i \neq j$ .

La función racional  $f(x)/g(x)$  puede expresarse como

$$\frac{f(x)}{g(x)} = s(x) + \sum_{i=1}^s \sum_{j=1}^{r_i} \frac{a_{ij}}{(x-\alpha_i)^j}$$

donde  $s(x)$  es un polinomio y los  $a_{ij}$  son números complejos.

*Demostración.* Por el lema 1

$$\frac{f(x)}{g(x)} = \sum_{i=1}^s \frac{f_i(x)}{(x-\alpha_i)^{r_i}}$$

Por el lema 2

$$\frac{f_i(x)}{(x-\alpha_i)^{r_i}} = s_i(x) + \sum_{j=1}^{r_i} \frac{s_{ij}(x)}{(x-\alpha_i)^j}$$

donde el grado de  $s_{ij}(x) = 0$ .

Tomando  $s(x) = \sum_{i=1}^s s_i(x)$  y  $a_{ij} = s_{ij}(x)$  queda demostrado el teorema.

Al aplicar este teorema pueden introducirse coeficientes complejos, aunque  $f(x)$  y  $g(x)$  tengan coeficientes reales. Si se quiere evitar esto puede utilizarse la descomposición de  $g(x)$  en polinomios de primero y segundo grados con coeficientes reales, por medio del teorema siguiente.

**TEOREMA 2:** Sea

$$g(x) = (x-\alpha_1)^{r_1} \dots (x-\alpha_h)^{r_h} (x^2 + a_1x + b_1)^{s_1} \dots (x^2 + a_kx + b_k)^{s_k}$$

donde los  $\alpha_i$ ,  $a_i$  y  $b_i$  son reales,  $\alpha_i \neq \alpha_j$  para  $i \neq j$  y  $x^2 + a_ix + b_i \neq x^2 + a_jx + b_j$  para  $i \neq j$ . Si  $f(x)$  es un polinomio con coeficientes reales la fracción  $f(x)/g(x)$  puede expresarse como

$$\frac{f(x)}{g(x)} = s(x) + \sum_{i=1}^h \sum_{j=1}^{r_i} \frac{a_{ij}}{(x-\alpha_i)^j} + \sum_{i=1}^k \sum_{j=1}^{s_i} \frac{A_{ij}x + B_{ij}}{(x^2 + a_ix + b_i)^j}$$

donde  $s(x)$  tiene coeficientes reales y los  $a_{ij}$ ,  $A_{ij}$  y  $B_{ij}$  son reales.

El teorema es, como el anterior, una consecuencia simple de los lemas, según el lector puede comprobar fácilmente.

Para calcular los coeficientes de los numeradores de las fracciones parciales en que se descompone una fracción racional según los teoremas anteriores, no es indispensable seguir los pasos de las demostraciones de los lemas, sino que se pueden obtener resolviendo un sistema de ecuaciones lineales, según veremos en un ejemplo.

Consideremos la fracción

$$R(x) = \frac{2x^7 + 5x^6 + x^5 - x^4 - 7x^3 + x^2 + x + 7}{x^6 - 2x^3 + 1}.$$

En primer lugar expresaremos  $R(x)$  como la suma de un polinomio y una fracción racional cuyo numerador tiene grado menor que el del denominador. Para ello basta dividir:

$$\begin{array}{r} 2x^7 + 5x^6 + x^5 - x^4 - 7x^3 + x^2 + x + 7 \\ - 2x^7 \quad \quad \quad + 4x^4 \quad \quad \quad - 2x \\ \hline 5x^6 + x^5 + 3x^4 - 7x^3 + x^2 - x + 7 \\ - 5x^6 \quad \quad \quad + 10x^3 \quad \quad \quad - 5 \\ \hline x^5 + 3x^4 + 3x^3 + x^2 - x + 2 \end{array} \quad \left| \begin{array}{c} x^6 - 2x^3 + 1 \\ 2x + 5 \end{array} \right.$$

Tenemos pues,

$$R(x) = 2x + 5 + \frac{x^5 + 3x^4 + 3x^3 + x^2 - x + 2}{x^6 - 2x^3 + 1}.$$

Denotamos con  $R_1(x)$  la fracción que aparece en la suma anterior. La descompondremos en fracciones parciales según el teorema 2. En primer lugar debemos descomponer el denominador. Para ello necesitaríamos obtener todas las raíces (reales o no) del polinomio, para lo cual no hemos dado ningún procedimiento, si bien tales procedimientos, aunque complicados, existen. Sin embargo supondremos conocida la descomposición

$$x^6 - 2x^3 + 1 = (x-1)^2(x^2+x+1)^2.$$

De hecho, esta descomposición podríamos obtenerla poniendo  $x^3 = X$  y resolviendo la ecuación  $X^2 - 2X + 1 = 0$ , con lo que obtendríamos

$$x^6 - 2x^3 + 1 = X^2 - 2X + 1 = (X-1)^2 = (x^3-1)^2 = [(x-1)(x^2+x+1)]^2.$$

Debemos, pues, descomponer  $R_1(x)$  en la forma

$$R_1(x) = \frac{a_1}{x-1} + \frac{a_2}{(x-1)^2} + \frac{a_3x + a_4}{x^2+x+1} + \frac{a_5x + a_6}{(x^2+x+1)^2}.$$

Nuestras incógnitas son  $a_1, \dots, a_6$ . Expresemos las fracciones con denominador común:

$$\begin{aligned} R_1(x) &= \frac{a_1(x-1)(x^2+x+1)^2}{(x-1)^2(x^2+x+1)^2} + \frac{a_2(x^2+x+1)^2}{(x-1)^2(x^2+x+1)^2} + \\ &+ \frac{(a_3x+a_4)(x-1)^2(x^2+x+1)}{(x-1)^2(x^2+x+1)^2} + \frac{(a_5x+a_6)(x-1)^2}{(x-1)^2(x^2+x+1)^2}. \end{aligned}$$

Haciendo operaciones y agrupando términos semejantes,

$$R_1(x) = \frac{A_1x^5 + A_2x^4 + A_3x^3 + A_4x^2 + A_5x + A_6}{x^6 - 2x^3 + 1}$$

donde

$$\begin{aligned} A_1 &= a_1 + a_3, \quad A_2 = a_1 + a_2 - a_3 + a_4, \quad A_3 = a_1 + 2a_2 - a_4 + a_5, \\ A_4 &= -a_1 + 3a_2 - a_3 - 2a_5 + a_6, \quad A_5 = -a_1 + 2a_2 + a_3 - a_4 + a_5 - 2a_6, \\ A_6 &= -a_1 + a_2 + a_4 + a_6. \end{aligned}$$

Comparando con la expresión

$$R_1(x) = \frac{x^5 + 3x^4 + 3x^3 + x^2 - x + 2}{x^6 - 2x^3 + 1}$$

vemos que debe cumplirse

$$A_1x^5 + A_2x^4 + A_3x^3 + A_4x^2 + A_5x + A_6 = x^5 + 3x^4 + 3x^3 + x^2 - x + 2.$$

Esto es, deben cumplirse las condiciones:

$$\begin{aligned} a_1 + a_3 &= 1 \\ a_1 + a_2 - a_3 + a_4 &= 3 \\ a_1 + 2a_2 - a_4 + a_5 &= 3 \\ -a_1 + 3a_2 - a_3 - 2a_5 + a_6 &= 1 \\ -a_1 + 2a_2 + a_3 - a_4 + a_5 - 2a_6 &= -1 \\ -a_1 + a_2 + a_4 + a_6 &= 2. \end{aligned}$$

Si nos tomamos la molestia de resolver este sistema encontramos que

$$a_1 = a_2 = a_4 = a_5 = a_6 = 1, \quad a_3 = 0,$$

de donde

$$R_1(x) = \frac{1}{x-1} + \frac{1}{(x-1)^2} + \frac{1}{x^2+x+1} + \frac{x-1}{(x^2+x+1)^2}$$

y

$$R(x) = 2x + 5 + \frac{1}{x-1} + \frac{1}{(x-1)^2} + \frac{1}{x^2+x+1} + \frac{x-1}{(x^2+x+1)^2}.$$

### EJERCICIO

Descompónganse algunas fracciones racionales en fracciones parciales, usando los teoremas 1 y 2.

## 16. ECUACIONES DE TERCERO Y CUARTO GRADOS CON COEFICIENTES REALES

No nos es posible exponer aquí con detalle un método para obtener todas las raíces complejas de un polinomio. Nos limitaremos a dar métodos para resolver ecuaciones de tercero y cuarto grados con coeficientes reales.

**Ecuaciones de tercer grado con coeficientes reales.** Sea

$$f(x) = x^3 + bx^2 + cx + d; \quad b, c, d \in \mathbf{R}.$$

Es claro que

$$|x| > \max(1, |b| + |c| + |d|) = M \implies |x^3| > |bx^2 + cx + d|.$$

Por lo tanto

$$\begin{aligned} x > M &\implies x^3 + bx^2 + cx + d > 0 \\ x < -M &\implies x^3 + bx^2 + cx + d < 0. \end{aligned}$$

En consecuencia todas las raíces reales de  $f(x)$  están en  $[-M, M]$ . Podemos calcularlas usando el teorema de Sturm y el método de Horner.

El número de raíces reales es 1 o 3. Si hay tres raíces reales (si la suma de las multiplicidades de las raíces reales es 3) tendremos ya todas las raíces de  $f(x)$ . Si hay una sola raíz real  $\alpha$  dividiremos  $f(x)$  entre  $x - \alpha$  obteniendo un cociente de grado 2 cuyas raíces, fácilmente obtenibles, son las otras dos raíces de  $f(x)$ .

**Ecuaciones de cuarto grado con coeficientes reales (método de Ferrari).** Sea

$$f(x) = x^4 + bx^3 + cx^2 + dx + e; \quad b, c, d, e \in \mathbf{R}.$$

Sea  $\eta$  una raíz real de  $y^3 - cy^2 + (bd - 4e)y - b^2e + 4ce - d^2$ , es decir, sea  $\eta \in \mathbf{R}$  tal que

$$\eta^3 - c\eta^2 + (bd - 4e)\eta - b^2e + 4ce - d^2 = 0.$$

Podemos encontrar  $\eta$  con tanta aproximación como queramos con los métodos ya descritos.

Tenemos entonces

$$\begin{aligned} x^4 + bx^3 &= -cx^2 - dx - e \\ x^2 + bx^3 + \frac{1}{4}b^2x^2 &= -cx^2 - dx - e + \frac{1}{4}b^2x^2 \\ (x^2 + \frac{1}{2}bx)^2 &= (\frac{1}{4}b^2 - c)x^2 - dx - e \\ (x^2 + \frac{1}{2}bx)^2 + (x^2 + \frac{1}{2}bx)\eta + \frac{1}{4}\eta^2 &= \\ &= (\frac{1}{4}b^2 - c)x^2 - dx - e + (x^2 + \frac{1}{2}bx)\eta + \frac{1}{4}\eta^2 \\ (x^2 + \frac{1}{2}bx + \frac{1}{2}\eta)^2 &= (\frac{1}{4}b^2 - c + \eta)x^2 + (-d + \frac{1}{2}b\eta)x + (-e + \frac{1}{4}\eta^2). \quad (1) \end{aligned}$$

Existe la siguiente relación entre los coeficientes del segundo miembro de esta ecuación (1):

$$\begin{aligned} (-d + \frac{1}{2}b\eta)^2 - 4(\frac{1}{4}b^2 - c + \eta)(-e + \frac{1}{4}\eta^2) &= \\ &= d^2 - db\eta + \frac{1}{4}b^2\eta^2 + b^2e - \frac{1}{4}b^2\eta^2 - 4ce + c\eta^2 + 4\eta e - \eta^3 \\ &= -[\eta^3 - c\eta^2 + (bd - 4e)\eta - b^2e + 4ce - d^2] \\ &= 0. \end{aligned}$$

Así que

$$(-d + \frac{1}{2}b\eta)^2 = 4(\frac{1}{4}b^2 - c + \eta)(-e + \frac{1}{4}\eta^2) \quad (2)$$

Escojamos dos complejos,  $A, B$ , tales que

$$A^2 = \frac{1}{4}b^2 - c + \eta \quad (3)$$

$$B^2 = -e + \frac{1}{4}\eta^2 \quad (4)$$

$$2AB = -d + \frac{1}{2}b\eta \quad (5)$$

Para ello escojamos primero  $A_1$  y  $B_1$  tales que

$$A_1^2 = \frac{1}{4}b^2 - c + \eta$$

$$B_1^2 = -e + \frac{1}{4}\eta^2.$$

Por la igualdad (2) se cumple

$$4(A_1B_1)^2 = (-d + \frac{1}{2}b\eta),$$

de donde

$$4(A_1B_1)^2 = (-d + \frac{1}{2}b\eta)^2,$$

Si  $2A_1B_1 = -d + \frac{1}{2}b\eta$  tomamos  $A = A_1$ ,  $B = B_1$ .

Si  $2A_1B_1 = -(-d + \frac{1}{2}b\eta)$  tomamos  $A = -A_1$ ,  $B = B_1$ .

Es claro que en los dos casos,  $A$  y  $B$  satisfacen (3), (4) y (5).

El segundo miembro de (1) es entonces igual a  $(Ax+B)^2$ , y la ecuación (1) se puede escribir

$$(x^2 + \frac{1}{2}bx + \frac{1}{4}\eta^2)^2 = (Ax+B)^2.$$

Esta ecuación, equivalente a la ecuación original, se satisface si y solo si se satisface una de las ecuaciones

$$x^2 + \frac{1}{2}bx + \frac{1}{4}\eta^2 = Ax + B,$$

$$x^2 + \frac{1}{2}bx + \frac{1}{4}\eta^2 = -Ax - B.$$

Por lo tanto las raíces de  $x^4 + bx^3 + cx^2 + dx + e$  son las soluciones de las ecuaciones

$$\begin{aligned}x^2 + (\frac{1}{2}b - A)x + (\frac{1}{2}\eta - B) &= 0 \\x^2 + (\frac{1}{2}b + A)x + (\frac{1}{2}\eta + B) &= 0.\end{aligned}$$

[Cualquier solución de cualquiera de las ecuaciones es raíz de  $f(x)$ .]

### Ejemplo.

Sea  $f(x) = x^4 + 4x^3 + x + 1$ . Nuestra ecuación auxiliar es

$$\eta^3 - 17 = 0.$$

Tomamos  $\eta = \sqrt[3]{17}$ . Deben cumplirse  $A^2 = 4 + \sqrt[3]{17}$ ,  $B^2 = -1 + \frac{1}{4}\sqrt[3]{17^2}$ ,  $2AB = -1 + 2\sqrt[3]{17}$ , que se satisfacen si

$$\begin{aligned}A &= \sqrt{4 + \sqrt[3]{17}} \\B &= \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}.\end{aligned}$$

Obtenemos entonces las ecuaciones

$$\begin{aligned}x^2 + (2 - \sqrt{4 + \sqrt[3]{17}})x + (\frac{1}{2}\sqrt[3]{17} - \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}) &= 0 \\x^2 + (2 + \sqrt{4 + \sqrt[3]{17}})x + (\frac{1}{2}\sqrt[3]{17} + \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}) &= 0\end{aligned}$$

cuyas soluciones son las raíces de  $f(x)$ .

### EJERCICIOS

Resuélvanse las siguientes ecuaciones:

- a)  $x^3 + 3x^2 - 2x - 5 = 0$
- b)  $x^3 - 7x - 7 = 0$
- c)  $x^4 + 2x^3 - 12x^2 - 10x + 3 = 0$
- d)  $x^4 - 8x^3 + 9x^2 - 8x - 10 = 0$
- e)  $x^4 - 3x^2 + 6x - 2 = 0$ .

# Índice analítico

- algoritmo
  - de Euclides, 306
  - de la división, 184
- anillos, 164
- aproximación, 242
- argumento, 247
  - en grados, 249
- base, 89
  - existencia de, 92
- binomio, teorema del, 31
- buen orden, principio de, 177
- cardinalidad, 27
- codominio, 21, 49
- columnas, 97
- combinación(es), 45, 61
  - lineal, 84
- complemento, 17
- conjunto, 13
  - vacio, 14
- cota, 219
  - inferior, 219
  - superior, 219
- Cramer, fórmulas de, 145
- De Morgan, leyes de, 17
- dependencia lineal, 87
- derivadas, 300
- determinante, 113, 116
  - cálculo, 131
  - desarrollo, 128
  - propiedades básicas, 117
- diferencia, 17
- dimensión, 94
  - de un subespacio vectorial, 94
- división, 179, 180
  - algoritmo de la, 184
  - sintética, 290
- dominio, 21, 49
  - entero, 170
- ecuaciones lineales, 137
  - sistemas de, 137
- elemento, 13
  - menor del, 127
- escalares, 74, 80
- espacio vectorial, 73, 80
- estructuras numéricas, 36
- Euclides, algoritmo de, 306
- factor de, 180
- fórmulas de Cramer, 145
- fracciones racionales, 312
- frontera, 219
  - inferior, 219
  - superior, 219
- función(es), 21, 47
  - biyectivas, 24, 54
  - composición de, 22
  - inyectivas, 24, 54
  - suprayectivas, 24, 54
- Horner, método de, 294
- inducción, 29
- intersección, 16
- leyes de De Morgan, 17
- linealmente
  - dependiente, 87
  - independiente, 88
- Matriz(es), 97
  - aumentada, 138
  - cuadradas, 98
  - del sistema, 137
  - equivalente, 102
  - rango de, 101
  - transpuesta de, 100
- máximo común divisor, 187
- método de Horner, 294
- mínimo común múltiplo, 191
- módulo de un vector, 245
- multiplicidad, 300
- múltiplo, 180
- números
  - complejos, 37, 253
  - enteros, 37
    - el anillo de los, 163
  - naturales, 36

- números
  - racionales, 37
  - reales, 37
- operaciones elementales, 102
- orden, 171
- ordenaciones, 42, 59
  - con repetición, 39, 57
- pareja ordenada, 18, 48
- particiones, 33
- Pascal, triángulo de, 63
- permutaciones, 43, 61, 108
  - impares, 108
  - inversas, 111
  - pares, 108
- principio
  - de buen orden, 177
  - de inducción, 174
- producto cartesiano, 18, 49
- raíces
  - de polinomios, 286
  - múltiples, 297
  - $n$ -ésimas, 271
- relación, 20
  - de equivalencia, 33
- renglones, 97
- sistema(s)
  - de ecuaciones lineales, 137
  - homogéneo, 138, 148
  - resolución de, 154
  - solución del, 138
- Sturm, teorema de, 308
- subconjunto, 15
  - función característica del, 63
- subespacio vectorial, 82, 86
  - dimensión de un, 94
  - generado, 86
- submatriz, 99
- teorema
  - del binomio, 31
  - del residuo, 286
  - de Sturm, 308
- transposiciones, 110
- triángulo de Pascal, 63
- unión, 16
- valor absoluto, 241
- vector(es), 74, 80
  - combinación lineal de los, 84
  - módulo de un, 245

# Índice de símbolos

- N** conjunto de números naturales, 14, 36  
**Z** anillo de los números enteros, 14, 37  
**Q** campo de los números racionales, 37  
**R** campo de los números reales, 37  
**C** campo de los números complejos, 37  
 $\in$  pertenece a, 14  
 $\notin$  no pertenece a, 14  
 $\subset$  contenido en, 15  
 $\not\subset$  no contenido en, 15  
 $\emptyset$  conjunto vacío, 14  
 $A - B$  diferencia de conjuntos, 17  
 $A^c$  complemento del conjunto  $A$ , 17  
 $\cup$  unión, 16  
 $\cap$  intersección, 16  
 $(a, b)$  pareja ordenada, 18  
 $A \times B$  producto cartesiano, 19  
 $f : A \rightarrow B$  función de  $A$  en  $B$ , 21, 49  
 $A \xrightarrow{f} B$  función de  $A$  en  $B$ , 21  
 $f \circ g$  composición de funciones, 22  
 $\text{OR}_{\text{n}}^m$  ordenaciones con repetición, 41, 58  
 $O_{\text{n}}^m$  ordenaciones, 42, 60  
 $P_{\text{n}}$  permutaciones, 44, 61  
 $n!$  factorial de  $n$ , 44, 61  
 $C_{\text{n}}^m$  combinaciones, 46, 61  
 $\mathbf{R}^n$  espacio vectorial real, 74, 80  
 $\sim$  equivalente a, 102

*La publicación de esta obra la realizó  
Editorial Trillas, S. A. de C. V.*

*División Administrativa, Av. Río Churubusco 385,  
Col. Pedro María Anaya, C.P. 03340, México, D. F.  
Tel. 6884233, FAX 6041364*

*División Comercial, Calz. de la Viga 1132, C. P. 09439  
México, D. F. Tel. 6330995, FAX 6330870*

*Se terminó de imprimir y encuadrinar el 4 de enero de 1995,  
en los talleres de Rotodiseño y Color, S. A. de C. V.  
Se tiraron 1 000 ejemplares, más sobrantes de reposición.*

**BM2 75**

conjuntos y funciones, operaciones y propiedades básicas, con el fin de que el alumno que llega a la facultad, repase estos temas con los que sin duda debe estar familiarizado.

Posteriormente se estudia la combinatoria, espacios vectoriales, matrices y determinantes, sistemas de ecuaciones lineales, el anillo de los números enteros, polinomios, el campo de los números reales, etc.

## OTRO TÍTULO DE LA SERIE

### **Elementos de análisis numérico** **Peter Henrici**

El autor de esta obra intenta destacar principios unificadores y establecer conexiones entre las ramas varias de análisis matemático. Logra un equilibrio entre el contenido teórico y el práctico marcando, por primera vez en un texto de esta naturaleza, la distinción entre teoremas y algoritmos, presentando además, un considerable número de algoritmos modernos y sus respectivos teoremas.

Se presenta también, como innovación en los textos de análisis numérico, un intento de tratar la teoría de ecuaciones de diferencias con el mismo rigor y generalidad que el que usualmente se encuentra en la teoría de las ecuaciones diferenciales.

Se incluye un capítulo sobre polinomios y números complejos. La obra reúne unos 300 problemas de dificultad del cálculo y analítica bastante variados. Además, al final de algunos de los capítulos se han enunciado varios problemas de investigación.

En el último capítulo se hace un análisis de la propagación del error, que es suficientemente general para cubrir muchos algoritmos de interés práctico.