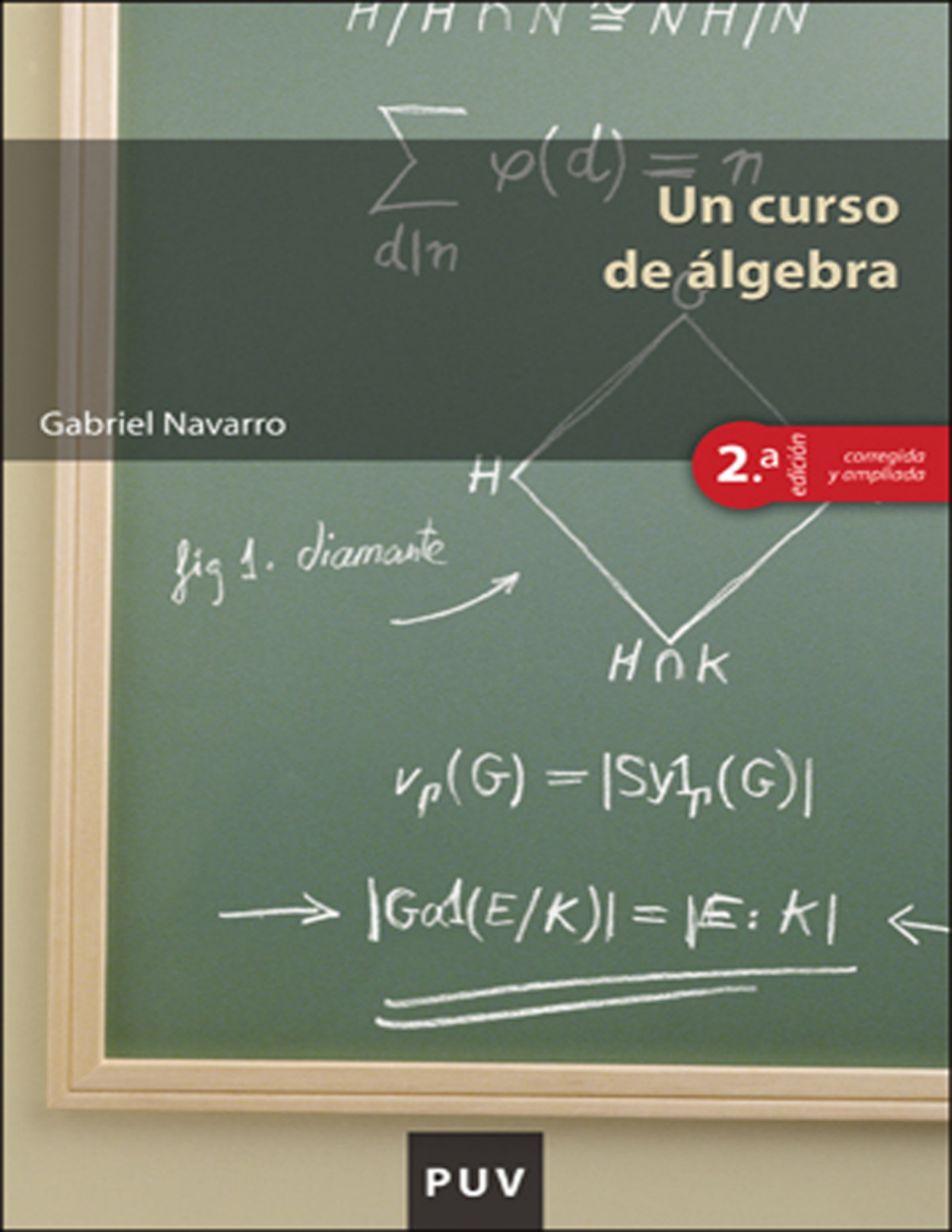
Un curso de álgebra

Gabriel Navarro

2.ª edición corregida y ampliada



PUV

UN CURSO DE ÁLGEBRA

Gabriel Navarro

UN CURSO DE ÁLGEBRA

UNIVERSITAT DE VALÈNCIA

Colección: Educació. Materials

1.ª edición: abril 2002
2.ª edición, corregida y aumentada: mayo 2016

Coordinación editorial: Maite Simón
Maquetación: el autor
Corrección: Communico-Letras y Píxeles S.L.
Cubierta: Celso Hernández de la Figuera

ISBN: 978-84-9134-029-4

Para Isabel, *Javier*, *Gabo y Nacho*

Índice general

Introducción

Este libro ofrece un primer curso de álgebra no lineal. En él, elegimos el objetivo de probar el gran teorema de Galois sobre la resolubilidad de ecuaciones polinómicas por radicales. Al mismo tiempo que aprendemos a «hacer» álgebra con el alumno, este tiene la sensación de que estamos resolviendo un problema natural con raíces históricas.

En la primera parte del libro introducimos los grupos.

Aunque tratamos de no apartarnos de nuestro objetivo, algunas veces no podemos resistir probar algunos teoremas que no son estrictamente necesarios para llegar a este. Por ejemplo, en el capítulo 5 damos una nueva demostración del teorema fundamental de los grupos abelianos finitos. Tampoco la teoría de Sylow sería esencial, aunque difícilmente un especialista en teoría de grupos finitos podrá dejar de presentarla.

La segunda parte del libro empieza en el capítulo 6 con los resultados más básicos sobre anillos y polinomios que nos permiten desarrollar la teoría de Galois. Seguramente, un especialista en teoría de anillos preferirá aumentar los contenidos de esta sección a costa de la parte de grupos.

En el capítulo 7, estudiamos las extensiones de cuerpos (donde por vez primera necesitaremos resultados elementales de álgebra lineal). Finalmente, en el capítulo 8, estamos ya preparados para estudiar la teoría de Galois. Por simplicidad, sus teoremas principales los probaremos sobre cuerpos de característica cero. (Una vez entendido este caso, el alumno interesado no tendrá dificultad en entender la teoría de Galois sobre cuerpos de cualquier característica).

Dependiendo del tiempo que quedara de curso, se podrían introducir algunos de los tópicos que no incluimos como construcciones con regla y compás o extensiones ciclotómicas.

A lo largo de los distintos capítulos, proponemos diversos ejercicios que solemos utilizar en las demostraciones. La resolución de estos siempre es

rutinaria y permite al alumno practicar las definiciones y entender mejor los teoremas. Al final de cada capítulo, proponemos una serie de problemas (algunas de cuyas soluciones las encontrará el lector al final del libro).

En la bibliografía, damos la referencia de algunos de los textos con los que el alumno podrá continuar estudiando álgebra.

Finalmente, este libro no hubiera sido el mismo sin la colaboración de una profesora extraordinaria de álgebra: María Jesús Iranzo. También quiero dar las gracias a Alexander Moretó y a Francisco Pérez Monasor.

Valencia, febrero de 2002

Nota a la segunda edición

Han pasado catorce años desde que apareció la primera edición de este libro y el álgebra que aquí se explica no ha cambiado en este tiempo. Pero el autor sí, y quizá también el tipo de alumnos que llega a las facultades de matemáticas. Pienso por ejemplo en mi hijo Nacho, actualmente uno de esos estudiantes. Al *recomendarle* mi libro, estaba convencido de que iba a apreciar, entre otras cosas, la brevedad de alguna de mis demostraciones, pero no ha sido exactamente así (aunque tampoco, creo, al contrario).

De la experiencia de explicar el contenido de este libro a mis alumnos he aprendido mucho: cuándo y cómo explicar mejor un argumento, dónde introducir exactamente determinada definición, qué conceptos es necesario que se repasen de clase en clase, etc. Desafortunadamente, el estilo del aula no se puede trasladar literalmente a un libro. Aunque algo sí.

Aparte de corregir algún error, de mejorar demostraciones, añadir nuevos teoremas, reordenar ciertas secciones, o de escribir más ejemplos y problemas, he creído conveniente escribir dos capítulos nuevos. En el primero introduzco informalmente números, conjuntos y aplicaciones, tal y como lo hago en clase. Esta introducción no pretende ser exhaustiva. También, antes de empezar la teoría de Galois, he escrito un capítulo sobre espacios vectoriales, solo con los resultados básicos que luego necesitaré. (Por tanto, la numeración de los capítulos es distinta respecto de la pasada edición). Dependiendo de los objetivos específicos que se tengan en el curso o del nivel de los estudiantes, tanto estos nuevos capítulos como otros pueden ser omitidos.

Después de estos catorce años, no estoy seguro de ser mejor matemático; pero creo que he mejorado como profesor, y he procurado que esto quede reflejado en lo que he escrito.

Es posible que no haya una tercera edición del libro, por lo que he intentado que esta sea la definitiva. Quiero dar las gracias a Noelia Rizo,

Lucía Sanus, Joan Tent y Carolina Vallejo por toda la ayuda prestada.

Valencia, abril de 2016

1. Conjuntos, aplicaciones, números

1

En este libro, un **conjunto** A es una colección de objetos a los que llamamos **elementos** de A. Dado un objeto x y un conjunto A, decimos que x **pertenece** a A si x es un elemento de A. En este caso escribimos $x \in A$. En caso contrario, decimos que x **no pertenece** a A, y escribimos $x \notin A$.

Denotamos los conjuntos con letras mayúsculas, y los definimos especificando o describiendo con exactitud los elementos que pertenecen a ellos. Por ejemplo, $A = \{1, 2, 3, 4\}$ es el conjunto cuyos elementos son 1, 2, 3 y 4. Así, escribimos $3 \in A$ y $5 \notin A$. El conjunto $B = \{1, \{1, 2\}, \{1, 2, 3\}\}$ tiene tres elementos: 1, el conjunto $\{1, 2\}$, y el conjunto $\{1, 2, 3\}$. Por tanto, escribimos $\{1, 2, 3\} \in B$. El **conjunto vacío** $\varnothing$ es el conjunto que no tiene elementos. Un conjunto A es **finito** si tiene un número finito de elementos. En este caso escribimos $|A|$ para denotar el número de elementos del conjunto A. Por ejemplo, $|\{1, 2, 3, 4\}| = 4$, $|\{1, \{1, 2\}, \{1, 2, 3\}\}| = 3$ y $|\varnothing| = 0$.

No siempre es posible o conveniente listar todos y cada uno de los elementos de un conjunto: nos basta con que describamos con precisión los que pertenecen a él. Por ejemplo, el conjunto

$$C = \{x \in \mathbb{N} \mid x = 2n + 1 \text{ para algún } n \in \mathbb{N}\}$$

es el conjunto de los números naturales impares. En este libro, los **números naturales** son los elementos del conjunto $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. Algunos autores no consideran 0 como número natural, pero esta es una polémica inútil. La línea vertical "|" en la definición del conjunto C se lee "tal que"; así, decimos que C es el conjunto de los números naturales x tales que pueden escribirse de la forma $x = 2n + 1$ para algún $n \in \mathbb{N}$. Algunos autores

utilizan ":" en lugar de la línea vertical. Los lectores deben ser conscientes de que diferentes autores pueden utilizar notaciones distintas y de que esto no es necesariamente negativo. Volviendo a C, podríamos haber escrito

$$C = \{2n + 1 \mid n \in \mathbb{N}\}$$

que es una notación más ágil.

Considaremos ahora el conjunto $D = \{n \in \mathbb{N} \mid 0 < n > 5\}$ y lo comparamos con el conjunto $A = \{1, 2, 3, 4\}$ definido en el segundo párrafo. Desde luego, observamos que D y A son *iguales*, pero necesitamos formular esto de forma precisa. Si A y B son conjuntos, decimos que A **está contenido** en B si para todo $a \in A$ se tiene que $a \in B$. En este caso, escribimos $A \subseteq B$, y decimos que A es un **subconjunto** de B. En caso contrario, decimos que A **no está contenido** en B, y lo escribimos $A \nsubseteq B$. Los conjuntos A y B son **iguales** si $A \subseteq B$ y $B \subseteq A$, y lo escribimos $A = B$. En caso contrario, escribimos $A \neq B$. Observamos que $\varnothing \subseteq A$ para todo conjunto A.

En este punto, debemos sincerarnos con el lector para advertirle que esta aproximación náıf a la teoría de conjuntos tiene algunas consecuencias no deseadas, como la famosa *paradoja de Russell*. Es evidente que el conjunto de los números naturales no es un número natural, por lo que la expresión $\mathbb{N} \notin \mathbb{N}$, aunque chocante, es cierta. Uno podría construir el *conjunto* $X = \{A \mid A \text{ es conjunto y } A \notin A\}$, y preguntarse si el propio $X \in X$ o si $X \notin X$. Por ejemplo, $\mathbb{N} \in X$ pues $\mathbb{N} \notin \mathbb{N}$. Sin embargo, si $X \in X$, esto significaría por definición que $X \notin X$, y al contrario. Hemos llegado a una contradicción, pues no puede pasar algo y lo opuesto al mismo tiempo. En definitiva, parece claro que tenemos un problema con nuestra definición de conjunto.

La teoría de conjuntos puede ser desarrollada de una forma axiomática que evita este tipo de contradicciones, pero este libro no es el lugar adecuado para hacerlo. La lógica es la disciplina que se ocupa de este y de otros temas.

Por otra parte, no debemos preocuparnos en exceso, al menos en lo que aqúı se refiere. Es un hecho que la mayor parte de los matemáticos puede

desarrollar una carrera exitosa utilizando nuestra definición de conjuntos sin contratiempo alguno en su vida (matemática). Digamos de una forma informal que mientras tratemos con conjuntos *pequeños* (el *conjunto* de todos los conjuntos definitivamente no es un conjunto *pequeño*), no nos vamos a encontrar con grandes problemas.

Dados dos conjuntos A y B, podemos construir nuevos conjuntos. Por ejemplo, la **unión** de A y B es el conjunto

$$A \cup B = \{x \mid x \in A \text{ ó } x \in B\}.$$

La **intersección** es el conjunto

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

La **diferencia** de A y B es

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

El **producto cartesiano** de A y B es el conjunto de pares

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

donde entendemos que $(a, b) = (a', b')$ si y solo si $a = a'$ y $b = b'$.

Si $A = \{1, 2, 3\}$ y $B = \{3, 4\}$, entonces $A \cup B = \{1, 2, 3, 4\}$, $A \cap B = \{3\}$, $A - B = \{1, 2\}$ y $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$.

Desde luego, podemos unir o intersectar una colección arbitraria de conjuntos. Si I es un conjunto, y para cada $i \in I$ tenemos definido un conjunto A_i, que depende de i, entonces definimos

$$\bigcup_{i \in I} A_i = \{x \mid \text{existe } i \in I \text{ tal que } x \in A_i\} \quad \text{y}$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ para todo } i \in I\}$$

Por ejemplo, si para $n \in \mathbb{N}$, definimos $A_n = \{m \in \mathbb{N} \mid m \geq n\}$, entonces tenemos que

$$\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N} \quad \text{y} \quad \bigcap_{n\in\mathbb{N}} A_n = \emptyset\,.$$

Si $A_1, \ldots, A_n$ son conjuntos, definimos

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}\,.$$

Si el lector está leyendo este primer capítulo, cabe la posibilidad de que no esté demasiado habituado a *probar* teoremas, habilidad que solo se adquiere con práctica, y leyendo muchas demostraciones. Probamos nuestro primer teorema.

Teorema 1.1 (Leyes de Morgan) *Supongamos que X, I y A_i para $i \in I$ son conjuntos. Entonces*

(a)

$$X - \Big(\bigcup_{i\in I} A_i\Big) = \bigcap_{i\in I}(X - A_i)\,.$$

(b)

$$X - \Big(\bigcap_{i\in I} A_i\Big) = \bigcup_{i\in I}(X - A_i)\,.$$

Demostración. Probamos (a), por ejemplo. Queremos probar que dos conjuntos son iguales. Por tanto, debemos probar que $X - (\bigcup_{i\in I} A_i)$ está contenido en $\bigcap_{i\in I}(X - A_i)$, y la inclusión contraria. Sea $x \in X - (\bigcup_{i\in I} A_i)$. Esto significa que $x \in X$ y que $x \notin \bigcup_{i\in I} A_i$. Por la definición de unión de una colección de conjuntos, tenemos que $x \notin A_i$ para todo $i \in I$. Así, $x \in X - A_i$ para todo $i \in I$, y por la definición de intersección de una colección de conjuntos, concluimos que $x \in \bigcap_{i\in I}(X - A_i)$. Recíprocamente, si $x \in \bigcap_{i\in I}$

$(X - A_i)$, tenemos que $x \in X$ y $x \notin A_i$ para todo i. Entonces $x \in X$ y $x \notin \bigcup_{i \in I} A_i$, y por tanto $x \in X - (\bigcup_{i \in I} A_i)$. ∎

2

Los conjuntos se relacionan mediante *aplicaciones*. Si A y B son conjuntos, una **aplicación** o **función de** A **en** B, que escribimos

$$f : A \to B ,$$

es una correspondencia (regla o criterio) que asigna a cada elemento $a \in A$ un único elemento $f(a)$ de B. A $f(a)$ se le llama la **imagen** de a mediante f. El conjunto A se llama el **dominio** o **conjunto inicial** de f. El conjunto B se llama el **codominio** o **conjunto final** de f. El **conjunto imagen**

$$f(A) = \{f(a) \mid a \in A\}$$

es el subconjunto de B formado por todas las imágenes mediante f de los elementos de A.

Podemos imaginar una función como una *máquina* cuyos *inputs* son los elementos de A. *Damos* $a \in A$ a la máquina y esta produce un *output* perfectamente determinado que es $f(a) \in B$. Para el lector riguroso que no esté satisfecho ni con la definición ni con la idea de la *máquina*, podemos definir una función $f : A \to B$ como un subconjunto $X \subseteq A \times B$ tal que $X \cap (\{a\} \times B)$ tiene exactamente un elemento para todo $a \in A$; pero esto es innecesariamente complicado. Si pensamos un momento sobre esta última definición, observamos que X es el *grafo* de la función f.

El lector está seguramente acostumbrado a tratar con funciones entre números reales como las aplicaciones $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2 + 1$, o $g : \mathbb{R} \to \mathbb{R}$ dada por $g(x) = \text{sen}(x)$. O incluso con funciones $h : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definidas por $h(a, b) = \sqrt{a^2 + b^2}$. (En estos ejemplos tendríamos que $f(\mathbb{R}) = \{a \in \mathbb{R} \mid a \geq 1\}$, $g(\mathbb{R}) = [-1, 1]$ y $h(\mathbb{R} \times \mathbb{R}) = \{a \in \mathbb{R} \mid a \geq 0\}$). Pero quizá el lector está menos acostumbrado a tratar con funciones sobre otros conjuntos, especialmente finitos. Por ejemplo, si $A = \{1, 2\}$ y $B = \{2, 3\}$

hay exactamente cuatro aplicaciones de A en B. Recordemos que todo elemento de A debe tener una y solo una imagen en B, por lo que las posibilidades están claras: $f(1) = 2$, $f(2) = 2$, $g(1) = 3$, $g(2) = 3$, $h(1) = 2$, $h(2) = 3$, y $l(1) = 3$, $l(2) = 2$ son todas las posibles funciones $A \to B$. Tendríamos que $f(A) = \{2\}$, $g(A) = \{3\}$, $h(A) = B$ y $l(A) = B$.

Ejercicio 1.1 *Sean A y B conjuntos. Sea B^A el conjunto de las aplicaciones de A en B. Si A tiene n elementos y B tiene m elementos, probar que B^A tiene m^n elementos.*

Dos funciones $f : A \to B$, $g : C \to D$ son **iguales** si $A = C$, $B = D$ y $f(a) = g(a)$ para todo $a \in A$. Por ejemplo, las funciones $f : \mathbb{Z} \to \mathbb{Z}$ y $g : \mathbb{Z} \to \mathbb{N}$ dadas por $f(z) = g(z) = z^2$ no son iguales porque sus conjuntos finales son distintos.

Para todo conjunto A, tenemos definida la función **identidad** $1_A : A \to A$ con $1_A(a) = a$ para todo $a \in A$.

Con frecuencia, lo primero que nos preguntamos sobre una aplicación f es si es *inyectiva* o *suprayectiva*; estos dos adjetivos se asocian de forma natural a las funciones. Una aplicación $f : A \to B$ es **inyectiva** si $f(a_1) = f(a_2)$ solo si $a1 = a_2$, para $a_1, a_2 \in A$. En otras palabras, f es inyectiva si elementos distintos de A tienen imágenes distintas en B. Si queremos comprobar que una función f es inyectiva, escribimos la igualdad $f(a_1) = f(a_2)$ y tratamos de averiguar si a_1 es necesariamente igual a a_2 o no. Informalmente, si f es una aplicación inyectiva, pensamos que B contiene un subconjunto ($f(A)$) que *tiene las mismas propiedades* que A.

Ejercicio 1.2 *Si A tiene n elementos, B tiene m elementos, y $f : A \to B$ es injectiva, probar que $n \leq m$.*

Una aplicación $f : A \to B$ es **suprayectiva** si $f(A) = B$. En otras palabras, si para todo $b \in B$ existe $a \in A$ tal que $f(a) = b$. Si queremos comprobar si una función f es suprayectiva, elegimos un elemento $b \in B$ arbitrario y lo intentamos expresar como $f(a)$ para algún a de A.

Ejercicio 1.3 *Si A tiene n elementos, B tiene m elementos, y $f : A \to B$ es suprayectiva, probar que $n \geq m$.*

Teorema 1.2 *Supongamos que A y B tienen n elementos, y sea $f : A \to B$. Entonces f es inyectiva si y solo si f es suprayectiva.*

Demostración. Esta es la primera vez en este libro que probamos un teorema *si y solo si*, por lo que hacemos una pausa para explicar lo que significa. Cuando tengamos que probar que un enunciado P es verdadero si y solo si un enunciado Q es verdadero, tenemos que probar que P implica Q (esto es, suponiendo P demostramos Q) y que Q implica P (suponiendo Q demostramos P).

Escribamos $A = \{a_1, \ldots, a_n\}$. Así, $f(A) = \{f(a_1), \ldots, f(a_n)\} \subseteq B$.

Supongamos que f es inyectiva. Entonces $f(A)$ tiene n elementos, pues $f(a_i) \neq f(a_j)$ si $i \neq j$. Como B tiene n elementos, necesariamente $f(A) = B$, y por tanto f es suprayectiva. Recíprocamente, si f es suprayectiva entonces $f(A) = B$ tiene n elementos, y por tanto no puede ocurrir que $f(a_i) = f(a_j)$ para distintos i y j. ∎

Finalmente, una aplicación $f : A \to B$ es **biyectiva** si f es inyectiva y suprayectiva. Las aplicaciones biyectivas (o **biyecciones**) son las *mejores* aplicaciones que podemos encontrar entre dos conjuntos.

Ejemplo 1.1 La función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n + 1$ es inyectiva, pues si $f(n) = f(m)$, entonces $2n + 1 = 2m + 1$, y concluimos que $n = m$. Sin embargo, f no es suprayectiva, pues no podemos hallar ningún $n \in \mathbb{N}$ tal que $f(n) = 2$. La función $g : \{1, 2, 3\} \to \{a, b\}$ dada por $g(1) = a$, $g(2) = b$ y $g(3) = a$ no es inyectiva, pues $g(1) = g(3)$. Sin embargo, g es suprayectiva.

Sean ahora $f : \mathbb{R} \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = \text{sen}(x)$ y $g(x) = x^2$. Observamos primero que g no es inyectiva pues $g(-1) = g(1)$. Sin embargo, si definimos $h : \mathbb{R}^+ \to \mathbb{R}$ con $h(x) = x^2$, donde $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$, entonces h es ahora inyectiva (pero no suprayectiva pues -1 no está en la imagen de h). Finalmente, si definimos $t : \mathbb{R}^+ \to \mathbb{R}^+$ con $t(x) = x^2$, entonces t es biyectiva. Algo semejante ocurre con $f(x) = \text{sen}(x)$. La función $s : [-\pi/2, \pi/2] \to [-1, 1]$ dada por $s(x) = \text{sen}(x)$ puede comprobarse que es una biyección.

¿Por qué es tan importante tener aplicaciones biyectivas? Esencialmente por dos razones. La primera es que una función biyectiva posee una función *inversa*. En el ejemplo anterior, la *inversa* de *s* es la función arcsen : $[-1, 1] \to [-\pi/2, \pi/2]$, mientras que la *inversa* de *t* es la función *ráız cuadrada*. La segunda razón es que si existe una función biyectiva entre *A* y *B* cualquier propiedad que satisfaga *A* desde el punto de vista de la teoría de conjuntos la va a satisfacer *B*, y recíprocamente. Es decir, que desde la perspectiva de conjuntos, *A* y *B* son *equivalentes*. Esto nos permitirá después, por ejemplo, comparar conjuntos y sus tamaños.

Si $f : A \to B$ y $g : B \to C$, podemos crear una nueva función

$$g \circ f : A \to C$$

definida por

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

que se llama la **composición** de *g* y *f*.

Por ejemplo, si $f : \mathbb{R} \to \mathbb{R}$ es la función $f(x) = x^2 + 1$ y $g(x) = \text{sen}(x)$, entonces $(g \circ f)(x) = \text{sen}(x^2 + 1)$ y $(f \circ g)(x) = \text{sen}(x)^2 + 1$.

La primera parte del siguiente ejercicio nos dice que la composición de aplicaciones es *asociativa*.

Ejercicio 1.4 (*i) Si $f : A \to B$, $g : B \to C$ y $h : C \to D$ son aplicaciones, probar que*

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

(ii) Si $f : A \to B$ es un aplicación, probar que $f \circ 1_A = f$ y $1_B \circ f = f$.

Lema 1.3 *Sean $f : A \to B$ y $g : B \to C$ aplicaciones.*

(a) Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

(b) Si f y g son suprayectivas, entonces $g \circ f$ es suprayectiva.

(c) Si $g \circ f$ es inyectiva, entonces f es inyectiva.

(d) Si $g \circ f$ es suprayectiva, entonces g es suprayectiva.

Demostración. (a) Si $g(f(a_1)) = g(f(a_2))$, deducimos que $f(a_1) = f(a_2)$ por ser g inyectiva. Por ser f inyectiva, tenemos que $a_1 = a_2$.

(b) Si $c \in C$, entonces existe $b \in B$ tal que $g(b) = c$, por ser g suprayectiva. Por ser f suprayectiva, existe $a \in A$ tal que $f(a) = b$. Entonces $g(f(a)) = c$.

(c) Si $f(a_1) = f(a_2)$, entonces $g(f(a_1)) = g(f(a_2))$. Como $g \circ f$ es inyectiva, deducimos que $a_1 = a_2$.

(d) Si $c \in C$, por hipótesis existe $a \in A$ tal que $g(f(a)) = c$. Si $b = f(a)$, deducimos que $g(b) = c$ ∎

Decimos que una función f: $A \to B$ es **invertible** si existe g: $B \to A$ tal que $f \circ g = 1_B$ y $g \circ f = 1_A$. Observamos que la función g, si existe, es única. Efectivamente, si h: $B \to A$ también satisface $h \circ f = 1_A$, entonces

$$h = h \circ 1_B = h \circ (f \circ g) = (h \circ f) \circ g = 1_A \circ g = g.$$

La función g se llama la **función inversa** de f y se escribe $g = f^{-1}$. Observamos que en este caso f^{-1} es también invertible y que $(f^{-1})^{-1} = f$.

Teorema 1.4 *Sea $f : A \to B$. Entonces f es invertible si y solo si f es biyectiva.*

Demostración. Supongamos que f es biyectiva. Construimos $g : B \to A$ de la siguiente manera. Dado b, sabemos que existe $a \in A$ tal que $f(a) = b$, pues f es suprayectiva. Como f es inyectiva, a es único, y por tanto b unívocamente determina a. Definimos $g(b) = a$. Es inmediato que $f \circ g = 1_B$ y $g \circ f = 1_A$. Recíprocamente, supongamos que f es invertible y sea $f^{-1} : B \to A$ su inversa. Como $f \circ f^{-1} = 1_B$ y $f^{-1} \circ f = 1_A$ son biyectivas, el teorema se sigue por el lema 1.3 partes (c) y (d). ∎

Si A es un conjunto, una **relación** en A es un subconjunto

$$R \subseteq A \times A.$$

Decimos que a **está relacionado con** b si $(a, b) \in R$. Podemos pensar que una relación es sencillamente una función $f : A \times A \to \{\text{sí, no}\}$, donde $R = \{(a, b) \in A \times A \mid f(a, b) = \text{sí}\}$.

Por ejemplo, en el conjunto $A = \{1, 2, 3\}$, definimos la relación

$$R = \{(1, 1), (1, 2), (3, 2)\}.$$

En este caso, 1 está relacionado con 1 y con 2, 2 no está relacionado con ningún elemento, y 3 está relacionado con 2. Muchas veces, en lugar de especificar R, es más sencillo describir cuándo dos elementos están relacionados. Por ejemplo, en el conjunto A de los habitantes de una ciudad, podemos decir que dos elementos de A están relacionados si viven en el mismo edificio. En este caso, observamos que cualquier $a \in A$ está relacionado consigo mismo, entre otras propiedades que analizamos a continuación. Necesitamos cierto lenguaje para hablar de relaciones.

Definición 1.5 *Sea A un conjunto y $R \subseteq A \times A$ una relación en A.*

(a) Decimos que R es **reflexiva** *si $(a, a) \in R$ para todo $a \in A$.*

(b) Decimos que R es **simétrica** *si siempre que $(a, b) \in R$, entonces $(b, a) \in R$.*

(c) Decimos que R es **antisimétrica** *si siempre que $(a, b) \in R$ y $(b, a) \in R$, entonces $a = b$.*

(d) Decimos que R es **transitiva** *si siempre que $(a, b), (b, c) \in R$, entonces $(a, c) \in R$.*

Muy pocas relaciones en un conjunto A son interesantes. De hecho, las relaciones interesantes son esencialmente de dos tipos. Una relación R es **de**

equivalencia si R es reflexiva, simétrica y transitiva. Una relación R es **una relación de orden** si R es reflexiva, antisimétrica y transitiva.

Ejemplo 1.2

(a) En el conjunto $\mathbb{R}$ de los números reales, definimos la relación $(a, b) \in R$ si y solo si $a \leq b$. Esta es una relación de orden.

(b) En el conjunto de habitantes de una ciudad, vivir en el mismo edificio establece una relación de equivalencia.

(c) En el plano $\mathbb{R}^2$, decimos que (x_1, y_1) está relacionado con (x_2, y_2) si se tiene que $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Esto define en el plano una relación de equivalencia.

(d) Si $f : A \to B$ es una aplicación, definimos $R = \{(a_1, a_2) \mid f(a_1) = f(a_2)\}$. Entonces R es una relación de equivalencia.

(e) Si A es un conjunto, definimos una relación en el conjunto $P(A)$ de todos los subconjuntos de A. Decimos que X e Y están relacionados si $X \subseteq Y$. Esto define una relación de orden en $P(A)$.

Siempre que tengamos una relación de equivalencia R sobre un conjunto A, dicho conjunto queda partido en trozos *disjuntos*. (Dos conjuntos A y B son **disjuntos** si $A \cap B = \emptyset$). Este es un hecho relevante. En el ejemplo 1.2 (b), los habitantes quedan distribuidos en edificios; en el ejemplo 1.2 (c), los elementos del plano quedan distribuidos en círculos de radio r para $r \geq 0$. En general, cada elemento $a \in A$ *vive* en su *clase de equivalencia*.

Una **partición** de un conjunto A es un conjunto P de subconjuntos no vacíos de A tales que

$$A = \bigcup_{B \in P} B$$

y $B \cap C = \emptyset$ para todos $B, C \in P$ distintos.