Apéndices

El objeto de estos apéndices es resumir todas las nociones elementales de las teorías de conjuntos, grupos y anillos que son necesarias para el desarrollo de los capítulos anteriores. Supondremos que se conocen los números naturales con su suma, su producto y su orden. También supondremos que el lector está familiarizado con los números enteros y con los números racionales (fraccionarios) con sus sumas, productos y órdenes respectivos, si bien daremos una construcción formal de los números enteros a partir de los naturales y de los números racionales a partir de los enteros.

A Generalidades sobre Teoría de Conjuntos

A.1 En Matemáticas, *conjunto* es uno de los términos básicos no definidos, aceptándose como válida la idea intuitiva que de él se tiene. Los objetos que integran un conjunto se llaman *elementos* de ese conjunto; dados un objeto a y un conjunto C, si a es un elemento de C escribiremos simbólicamente "$a \in C$" y diremos que "a pertenece a C"; en caso contrario (esto es, si a no pertenece a C) escribiremos "$a \notin C$".

Un conjunto lo podemos determinar por *extensión* (explícitamente) citando todos y cada uno de los elementos que lo integran (por ejemplo $C = \{1, 2, 3\}$), ó por *caracterización* (implícitamente) dando una propiedad tal que los elementos del conjunto, y sólo ellos, la satisfacen (por ejemplo $C = \{n \in \mathbb{N}$ tal que n es par$\}$, donde $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ es el conjunto de los números naturales).

A.2 (Notación) Para simplificar la escritura en el "lenguaje matemático" se utilizan símbolos universalmente aceptados. A continuación describimos los más usuales.

- *Operador universal*: su símbolo es "$\forall$" y se lee "para todo".
- *Operador existencial*: su símbolo es "$\exists$" y se lee "existe".
- *Operador de existencia y unicidad*: su símbolo es "$\exists^{\cdot}$" (ó también "$\exists!$") y se lee "existe un único".
- *Operador condicional*: su símbolo es "/" (ó también ":") y se lee "tal que" ó "tales que".
- *Igualdad*: puede ocurrir que al estudiar un conjunto A identifiquemos el mismo elemento con dos nombres distintos "a" y "b"; decimos entonces que "a es igual a b" y escribimos "$a = b$"; si a y b son nombres de elementos distintos se dice que "a es distinto de b" y se escribe "$a \neq b$".

- *Implicación*: en el razonamiento lógico la implicación es fundamental, y los elementos que liga se llaman *proposiciones* (una proposición es una sentencia ó enunciado que puede ser verdadero ó falso): si $\mathcal{A}$ y $\mathcal{B}$ son dos proposiciones tales que $\mathcal{B}$ se deduce lógicamente de $\mathcal{A}$, entonces se escribe "$\mathcal{A} \Rightarrow \mathcal{B}$" y se lee "$\mathcal{A}$ implica $\mathcal{B}$" ó "si $\mathcal{A}$, entonces $\mathcal{B}$". Por ejemplo, si a, b y c son elementos de un conjunto se satisface

$$a = b\,, \quad b = c \qquad \Rightarrow \qquad a = c\,;$$

la anterior implicación expresa la "transitividad" de la igualdad (se transmite de a a c por medio de b). La implicación es también transitiva, ya que si se satisfacen simultáneamente "$\mathcal{A} \Rightarrow \mathcal{B}$" y "$\mathcal{B} \Rightarrow \mathcal{C}$", entonces también se satisface "$\mathcal{A} \Rightarrow \mathcal{C}$", es decir

$$\mathcal{A} \Rightarrow \mathcal{B}\,, \quad \mathcal{B} \Rightarrow \mathcal{C} \qquad \Rightarrow \qquad \mathcal{A} \Rightarrow \mathcal{C}\,.$$

El razonamiento se efectua transitivamente encadenando implicaciones,

$$\mathcal{A} \Rightarrow \mathcal{B} \Rightarrow \mathcal{C} \Rightarrow \ldots\,;$$

digamos, en un lenguaje poco formal, que la acción de encadenar proposiciones es la "deducción".

- *Equivalencia*: dos proposiciones $\mathcal{A}$ y $\mathcal{B}$ se dice que son equivalentes si se satisfacen simultáneamente $\mathcal{A} \Rightarrow \mathcal{B}$ y $\mathcal{B} \Rightarrow \mathcal{A}$, en cuyo caso se escribe "$\mathcal{A} \Leftrightarrow \mathcal{B}$" y se lee "$\mathcal{A}$ si y sólo si $\mathcal{B}$" ó "para que $\mathcal{A}$ sea cierto es condición necesaria y suficiente que $\mathcal{B}$ sea cierto". Nótese que cualesquiera que sean las proposiciones $\mathcal{A}$ y $\mathcal{B}$, obtenemos a partir de ellas la nueva proposición verdadera

$$(\mathcal{A} \Rightarrow \mathcal{B}) \qquad \Longleftrightarrow \qquad \mathrm{no}\,\mathcal{B} \Rightarrow \mathrm{no}\,\mathcal{A}\,,$$

donde $\mathrm{no}\,\mathcal{A}$ (respectivamente, $\mathrm{no}\,\mathcal{B}$) es la proposición que se obtiene al negar $\mathcal{A}$ (respectivamente, $\mathcal{B}$).

- *Inclusión*: gracias a la noción de pertenencia aparece el concepto de inclusión y la idea de subconjunto; dados dos conjuntos A y B, diremos que "A está incluido en B si todo elemento de A pertenece a B, en cuyo caso escribiremos "$A \subseteq B$" y se dice que A es un *subconjunto* de B; la negación de "$A \subseteq B$" es que "existe un elemento de A que no pertenece a B", en cuyo caso escribiremos "$A \not\subseteq B$". Simbólicamente sería

$$\begin{aligned} A \subseteq B \qquad &\Longleftrightarrow \qquad a \in B \ \ \forall\, a \in A\,, \\ A \not\subseteq B \qquad &\Longleftrightarrow \qquad \exists\, a \in A \ / \ a \notin B\,. \end{aligned}$$

Nótese que cualquiera que sea el conjunto A se satisface "$A \subseteq A$".

- *Igualdad entre conjuntos*: dos conjuntos A y B se dice que son iguales si satisfacen $A \subseteq B$ y $B \subseteq A$, en cuyo caso se escribe $A = B$; la negación de $A = B$ es que "en uno de los dos conjuntos existe un elemento que no está en el otro", y se denota "$A \neq B$". Simbólicamente sería

$$\begin{aligned} A = B \qquad &\Longleftrightarrow \qquad A \subseteq B \ \text{ y } \ B \subseteq A \\ &\Longleftrightarrow \qquad a \in B \ \ \forall\, a \in A \ \text{ y } \ b \in A \ \ \forall\, b \in B\,, \\ A \neq B \qquad &\Longleftrightarrow \qquad A \not\subseteq B \ \text{ ó } \ B \not\subseteq A \\ &\Longleftrightarrow \qquad \exists\, a \in A \ / \ a \notin B \ \text{ ó } \ \exists\, b \in B \ / \ b \notin A\,. \end{aligned}$$

- *Igualdad por definición*: su símbolo es "$:=$" y se lee "igual por definición"; por ejemplo, si escribimos $B := \{a, b, c\}$ queremos decir que B se define como el conjunto cuyos elementos son a, b y c.
- *Equivalencia por definición*: su símbolo es "$:\Leftrightarrow$" y se utiliza para definir "relaciones" entre "objetos"; por ejemplo, diremos por definición que dos conjuntos A y B son "disjuntos" cuando A y B no tienen ningún elemento en común, es decir,

$$A \text{ y } B \text{ son disjuntos} \quad :\Longleftrightarrow \quad A \text{ y } B \text{ no tienen elementos comunes}\,.$$

A.3 (Conjunto vacío) Se admite la existencia de un conjunto que no tiene elementos, el cual se denomina *vacío* y se denota con el símbolo "$\emptyset$". Es claro que el vacío es subconjunto de cualquier otro conjunto.

A.4 (Conjunto de las partes) Dado un conjunto A, se define el *conjunto de las partes* de A como el conjunto cuyos elementos son todos los subconjuntos de A; se denota $\mathcal{P}(\mathcal{A})$,

$$\mathcal{P}(\mathcal{A}) := \{\mathcal{B} \text{ conjunto } : \mathcal{B} \subseteq \mathcal{A}\}\,.$$

Es claro que $\emptyset, A \in \mathcal{P}(\mathcal{A})$, y que $\{a\} \in \mathcal{P}(\mathcal{A})$ para todo $a \in A$. A $\mathcal{P}(\mathcal{A})$ también se le conoce como *conjunto potencia* de A.

A.5 (Familias indexadas) Dado un conjunto I, una *familia de conjuntos indexada por* I consiste en dar un conjunto A_i para cada elemento $i \in I$; la familia se denota $\{A_i\}_{i\in I}$ y el conjunto I se dice que es el *conjunto de índices* de la familia. Por ejemplo:
(a) $\{A_1, A_2, A_3\} = \{A_i\}_{i\in I}$ donde $I = \{1, 2, 3\}$;
(b) Dado un conjunto A, si para cada $a \in A$ denotamos $A_a = \{a\}$ tenemos la familia $\{A_a\}_{a\in I}$, donde $I = A$;
(c) Cuando $I = \mathbb{N}$, una familia de conjuntos indexada por I se denomina *sucesión de conjuntos*, $\{A_i\}_{i\in\mathbb{N}} = \{A_0, A_1, \ldots, A_n, \ldots\}$.

A.6 (Operaciones con conjuntos) Sean A y B conjuntos. Se define la *intersección* de A y B, y se denota por $A \cap B$, como el conjunto formado por todos los elementos que son comunes a A y a B,

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

Se dice que A y B son dos conjuntos *disjuntos* cuando $A \cap B = \emptyset$.

Se define la *unión* de A y B, y se denota por $A \cup B$, como el conjunto formado por todos los elementos que pertenecen al menos a uno de los dos conjuntos,

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

Si B es un subconjunto de A se define el *complementario* de B en A, y se denota B^{c} (ó $A - B$), como el conjunto formado por todos los elementos de A que no están en B,

$$B^{\mathrm{c}} := \{x \in A : x \notin B\}\,.$$

Es sencillo comprobar que se satisfacen las siguientes propiedades:
(a) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (conmutativas);

(b) $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$ (asociativas);
(c) $A \cap A = A$, $A \cup A = A$ (idempotencias);
(d) $A \cap B = A \Leftrightarrow A \subseteq B \Leftrightarrow A \cup B = B$;
(e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivas);
(f) $A \cup (B \cap A) = A = A \cap (B \cup A)$;
(g) si A y B son subconjuntos de un conjunto C tenemos las leyes de De Morgan,

$$(A \cap B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B^{\mathrm{c}}\,, \qquad (A \cup B)^{\mathrm{c}} = A^{\mathrm{c}} \cap B^{\mathrm{c}}\,,$$

donde los complementarios se toman en C.

En general, dada una familia de conjuntos $\{A_i\}_{i\in I}$ se definen la intersección y la unión de los conjuntos de dicha familia como los conjuntos $\cap_{i\in I} A_i$ y $\cup_{i\in I} A_i$, respectivamente, dados por las igualdades

$$\cap_{i\in I} A_i := \{a \,:\, a \in A_i \ \ \forall\, i \in I\}\,, \qquad \cup_{i\in I} A_i := \{a \,:\, \ \exists\, i \in I \ \text{con}\ a \in A_i\}\,;$$

son igualmente fáciles de demostrar las siguientes igualdades:
(h) $(\cap_{i\in I} A_i) \cap B = \cap_{i\in I}(A_i \cap B)$, $(\cap_{i\in I} A_i) \cup B = \cap_{i\in I}(A_i \cup B)$;
(i) $(\cup_{i\in I} A_i) \cap B = \cup_{i\in I}(A_i \cap B)$, $(\cup_{i\in I} A_i) \cup B = \cup_{i\in I}(A_i \cup B)$;
(j) leyes de De Morgan: $(\cap_{i\in I} A_i)^{\mathrm{c}} = \cup_{i\in I} A_i^{\mathrm{c}}$, $(\cup_{i\in I} A_i)^{\mathrm{c}} = \cap_{i\in I} A_i^{\mathrm{c}}$ (si todos los conjuntos de la familia son subconjuntos de un conjunto C y los complementarios de toman en C).

Por ejemplo, si $\mathbb{N}_+$ son los números naturales no nulos y para cada $n \in \mathbb{N}_+$ definimos el conjunto A_n por la igualdad $A_n := \{z \in \mathbb{Q} \,:\, -1/n \le z \le 1/n\}$ donde $\mathbb{Q}$ son los números fraccionarios, entonces tenemos

$$\cup_{n\in\mathbb{N}_+} A_n = A_1\,, \qquad \cap_{n\in\mathbb{N}_+} A_n = \{0\}\,.$$

A.7 (Particiones) Sea A un conjunto y sea $\{A_i\}_{i\in I}$ una familia de subconjuntos de A (es decir, $\{A_i\}_{i\in I}$ es un subconjunto de $\mathcal{P}(\mathcal{A})$; véase A.4). Se dice que la anterior familia es una *partición* del conjunto A si satisface:

(i) $A_i \neq \emptyset$ para todo $i \in I$;
(ii) $A = \cup_{i\in I} A_i$;
(iii) si $i, j \in I$ tales que $i \neq j$ entonces $A_i \cap A_j = \emptyset$.

Veamos unos ejemplos:
(a) Dado un conjunto A, la familia $\{A_a\}_{a\in A}$ es una partición de A, donde $A_a = \{a\}$.
(b) Si $\mathbb{Q}_+$ son los números fraccionarios positivos y para cada $z \in \mathbb{Q}_+$ definimos $A_z = \{-z, z\}$, entonces la familia $\{A_z\}_{z\in\mathbb{Q}_+}$ es una partición de $\mathbb{Q} - \{0\}$.
(c) Obténganse particiones del conjunto $E = \{1, 2, 3, 4, 5\}$.

A.8 (Producto directo) Dados conjuntos A y B, se define el conjunto *producto directo* (ó *producto cartesiano*) de A y B (en ese orden), y se denota por $A \times B$, como el conjunto de todos los "pares ordenados de elementos" tales que el primero pertenece a A y el segundo pertence a B:

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

Dados elementos (a,b) y (a',b') de $A\times B$, por definición tenemos

$$(a,b)=(a',b') \qquad \Longleftrightarrow \qquad a=a' \text{ y } b=b'\,,$$

y es claro que no es cierto que siempre se satisface la igualdad $A\times B=B\times A$.

Dados conjuntos $A_1,\ldots,A_n$ se define el producto directo de $A_1,\ldots,A_n$ (en ese orden) como el conjunto de "n-uplas" de elementos $(a_1,\ldots,a_n)$ tales que $a_i\in A_i$ para todo $i\in\{1,\ldots,n\}$ (una n-upla es una colección ordenada de n elementos):

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

Como es usual usaremos la siguiente notación:

$$A\times A=A^2\,,\quad A\times A\times A=A^3\,,\quad \ldots\,,\quad A\times\overset{n}{\cdots}\times A=A^n\,.$$

Algunas propiedades sencillas de comprobar son:

(a) $A'\subseteq A\,,\,B'\subseteq B \quad\Longleftrightarrow\quad A'\times B'\subseteq A\times B\,;$

(b) $A\times(B\cup C)=(A\times B)\cup(A\times C)\,,\ (B\cup C)\times A=(B\times A)\cup(C\times A)\,;$

(c) $A\times(B\cap C)=(A\times B)\cap(A\times C)\,,\ (B\cap C)\times A=(B\times A)\cap(C\times A)\,;$

(d) $A\times B\neq\emptyset \quad\Longleftrightarrow\quad A\neq\emptyset$ y $B\neq\emptyset$.

En general, dada una familia de conjuntos $\{A_i\}_{i\in I}$ se define el producto directo de los conjuntos de dicha familia como el conjunto de las familias de elementos $(a_i)_{i\in I}$ indexadas por I tales que $a_i\in A_i$ para todo $i\in I$.

A.9 (Correspondencias) Dados conjuntos A y B, se llama *correspondencia* de A en B a todo subconjunto de $A\times B$.

Hay dos tipos importantes de correspondencias: las aplicaciones y las relaciones.

A.10 (Aplicaciones) Dados conjuntos A y B, se llama *aplicación* de A en B a toda correspondencia $G\subseteq A\times B$ que satisfaga

$$\forall\, a\in A\quad \exists^{\cdot}\, b\in B\quad /\quad (a,b)\in G\,.$$

Una aplicación G de A en B suele denotarse $f:A\to B$, $a\mapsto f(a)$, con el siguiente criterio: dado $a\in A$, el único elemento $b\in B$ que satisface $(a,b)\in G$ se denota $f(a)$ y se denomina "imagen de a por la aplicación"; de este modo suele hablarse de la aplicación f, y al conjunto G (que es la aplicación estrictamente hablando) se le llama *grafo* ó *gráfica* de la aplicación f.

Sea $f:A\to B$ una aplicación. El conjunto A se llama *dominio* (ó *conjunto de definición*) de la aplicación y B se denomina *codominio* de (ó *conjunto donde valora*) la aplicación. Se define la *imagen* de la aplicación f, y se denota $\operatorname{Im} f$, como el conjunto

$$\operatorname{Im} f:=\{f(a)\,:\,a\in A\}\,,$$

que es un subconjunto del codominio, $\operatorname{Im} f\subseteq B$. Se dice que la aplicación f es *epiyectiva* cuando $\operatorname{Im} f=B$, es decir, si se satisface

$$\forall\, b\in B\quad \exists\, a\in A\quad /\quad f(a)=b\,;$$

esto es, f es epiyectiva si todo elemento de B es imagen por f de algún elemento de A. Se dice que la aplicación f es *inyectiva* si satisface

$$a, a' \in A \quad / \quad a \neq a' \qquad \Rightarrow \qquad f(a) \neq f(a')$$

(elementos distintos de A tienen imagen distinta por f), ó equivalentemente

$$a, a' \in A \quad / \quad f(a) = f(a') \qquad \Rightarrow \qquad a = a' .$$

Cuando una aplicación es inyectiva y epiyectiva simultáneamente se dice de ella que es *biyectiva* (ó *biunívoca*).

Por ejemplo, si A es un subconjunto de un conjunto B hay una aplicación natural de A en B que se denomina *inmersión* (ó *inclusión*) de A en B:

$$\begin{array}{rcl} i : A & \to & B \\ a & \mapsto & a ; \end{array}$$

la gráfica de i es $G = \{(a, a) : a \in A\} \subseteq A \times B$. Cuando $A = B$ (lo que ocurre si y sólo si i es epiyectiva), dicha inmersión de denomina *aplicación identidad* de A.

A.11 (Imágenes directa e inversa) Sea $f : A \to B$ una aplicación. Para cada subconjunto A' de A se define la *imagen directa* de A' por f (ó simplemente "imagen" de A' por f) como el subconjunto $f(A')$ de B dado por la igualdad

$$f(A') := \{f(a) : a \in A'\} .$$

En particular se satisface $\operatorname{Im} f = f(A)$.

Para cada subconjunto B' de B se define la *imagen inversa* (ó *imagen recíproca*, ó *contraimagen*) de B' por f como el subconjunto $f^{-1}(B')$ de A dado por la igualdad

$$f^{-1}(B') := \{a \in A : f(a) \in B'\} .$$

Con las definiciones anteriores tenemos que f induce aplicaciones entre los conjuntos de las partes:

$$\begin{array}{rcl} \mathcal{P}(\mathcal{A}) & \to & \mathcal{P}(\mathcal{B}) \\ A' & \mapsto & f(A') , \end{array} \qquad\qquad \begin{array}{rcl} \mathcal{P}(\mathcal{B}) & \to & \mathcal{P}(\mathcal{A}) \\ B' & \mapsto & f^{-1}(B') ; \end{array}$$

es fácil comprobar que dichas aplicaciones conservan la inclusión: si $A', A'' \in \mathcal{P}(\mathcal{A})$ tales que $A' \subseteq A''$ entonces $f(A') \subseteq f(A'')$, y si $B', B'' \in \mathcal{P}(\mathcal{B})$ tales que $B' \subseteq B''$ entonces $f^{-1}(B') \subseteq f^{-1}(B'')$.

Tenemos las siguientes propiedades:

(a) Dada una familia $\{A_i\}_{i \in I}$ de subconjuntos de A se satisfacen
  (i) $f(\cup_{i \in I} A_i) = \cup_{i \in I} f(A_i)$;
  (ii) $f(\cap_{i \in I} A_i) \subseteq \cap_{i \in I} f(A_i)$, y se da la igualdad cuando f es inyectiva.

(b) Dada una familia $\{B_i\}_{i \in I}$ de subconjuntos de B se satisfacen
  (i) $f^{-1}(\cup_{i \in I} B_i) = \cup_{i \in I} f^{-1}(B_i)$;
  (ii) $f^{-1}(\cap_{i \in I} B_i) = \cap_{i \in I} f^{-1}(B_i)$.

(c) Para cada $A' \in \mathcal{P}(\mathcal{A})$ se satisface $A' \subseteq f^{-1}(f(A'))$, y se da la igualdad si f es inyectiva.

(d) Para cada $B' \in \mathcal{P}(\mathcal{B})$ se satisface $f(f^{-1}(B')) \subseteq B'$, y se da la igualdad si f es epiyectiva.

Las demostraciones de las anteriores propiedades son sencillas y se omiten. Recuérdese que para probar la igualdad entre dos conjuntos hay que probar las dos correspondientes inclusiones.

A.12 (Composición de aplicaciones) Sean $f : A \to B$ y $g : B \to C$ aplicaciones. Como el codominio de f coincide con el dominio de g podemos definir la nueva aplicación

$$\begin{array}{rcl} A & \to & C \\ a & \mapsto & g(f(a))\,, \end{array}$$

la cual se denomina *composición* de f y g y se denota por $g \circ f$ (primero se aplica f y después se aplica g).

La composición de aplicaciones es "asociativa", es decir, si $h : C \to D$ es otra aplicación se satisface $(h \circ g) \circ f = h \circ (g \circ f)$. Gracias a la asociatividad podemos quitar los paréntesis y escribir simplemente $h \circ g \circ f$.

Se satisface el siguiente importante resultado:

Teorema A.13 *Una aplicación $f : A \to B$ es biyectiva si y sólo si existe otra aplicación $g : B \to A$ tal que $f \circ g = I_B$ y $g \circ f = I_A$, donde I_A e I_B denotan la aplicación identidad de A y la aplicación identidad de B, respectivamente.*

Además, si f es biyectiva entonces la aplicación $g : B \to A$ que satisface las igualdades $f \circ g = I_B$, $g \circ f = I_A$ es única y se denomina aplicación inversa *de f, denotándose f^{-1}.*

Demostración. Supongamos en primer lugar que $f : A \to B$ es una aplicación biyectiva. Tenemos

$$\begin{array}{lll} \text{(por ser } f \text{ inyectiva)} & a, a' \in A \;\; / \;\; f(a) = f(a') & \Rightarrow \quad a = a'\,, \\ \text{(por ser } f \text{ epiyectiva)} & \forall\, b \in B \;\; \exists\, a \in A \;\; / \;\; f(a) = b\,; & \end{array}$$

las dos anteriores líneas podemos escribirla en una sola como sigue:

$$\forall\, b \in B \;\; \exists^{\cdot}\, a \in A \;\; / \;\; f(a) = b\,, \tag{A.1}$$

de modo que tenemos la aplicación $g : B \to A$ siguiente: dado $b \in B$, si a es el único elemento de A que satisface $f(a) = b$ entonces $g(b) = a$. Es decir, si $G = \{(a, f(a)) : a \in A\} \subseteq A \times B$ es el grafo de f y consideramos la correspondencia $G' = \{(b, a) : (a, b) \in G\} \subseteq B \times A$, entonces (A.1) nos dice que G' es una aplicación; dicha aplicación es la g que hemos definido. De la construcción de g se siguen inmediatamente las igualdades $f \circ g = I_B$ y $g \circ f = I_A$.

Supongamos ahora que existe una aplicación $g : B \to A$ tal que $f \circ g = I_B$, $g \circ f = I_A$ y probemos que entonces f es biyectiva. Sean $a, a' \in A$ tales que $f(a) = f(a')$, en cuyo caso $g(f(a)) = g(f(a'))$; como $g \circ f = I_A$ obtenemos $g(f(a)) = a$, $g(f(a')) = a'$ y concluimos que $a = a'$; por lo tanto f es inyectiva. Dado $b \in B$ el elemento $a = g(b) \in A$ satisface $f(a) = f(g(b)) = b$ (porque $f \circ g = I_B$), de modo que f es epiyectiva.

Se deja como ejercicio para el lector la demostración de la última parte del enunciado del teorema (la unicidad, cuando exista, de la aplicación g). ∎

A.14 (Relaciones) Sea A un conjunto no vacío. Se llama *relación* en A a toda correspondencia de A en A, es decir, a todo subconjunto de $A \times A$.

Sea $R \subseteq A \times A$ una relación en un conjunto A. Si $a, b \in A$ tales que $(a, b) \in R$ se dice que a está *relacionado* con b por R, y se escribe aRb. Las siguientes son las cuatro propiedades que se consideran sobre una relación:

(i) Se dice que R es *reflexiva* si aRa para todo $a \in A$.

(ii) Se dice que R es *simétrica* si satisface la implicación: $aRb \quad \Rightarrow \quad bRa$.

(iii) Se dice que R es *antisimétrica* si satisface la implicación: $aRb,\ bRa \quad \Rightarrow \quad a = b$.

(iv) Se dice que R es *transitiva* si satisface la implicación: $aRb,\ bRc \quad \Rightarrow \quad aRc$.

Como ejemplo estúdiense las propiedades que satisfacen las siguientes relaciones:
(a) En el conjunto $\mathbb{Z}$ de los números enteros, $R = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} : nm > 0\}$.
(b) En el conjunto $A = B \times B$ con $B = \{1, 2, 3, 4, 5\}$, $R = \{((a, b), (c, d)) \in A \times A : a + d = b + c\}$.
(c) Relación de igualdad entre los elementos de un conjunto (es decir, sobre un conjunto cualquiera A la relación $R = \{(a, b) \in A \times A : a = b\}$).
(d) Relación de inclusión entre las partes de un conjunto.
(e) En el conjunto de las rectas de un plano, relación de perpendicularidad.
(f) En el conjunto de las rectas de un plano, relación de paralelismo.
(g) En un conjunto A de cartulinas de colores, $R = \{(a, b) \in A \times A : a$ tiene igual color que $b\}$.
(h) En el conjunto $\mathbb{N}_+$ de los números naturales no nulos, $R = \{(n, m) \in \mathbb{N} \times \mathbb{N} : n$ divide a $m\}$.
(i) En el conjunto $\mathbb{Q}$ de los números fraccionarios, $R = \{(n, m) \in \mathbb{Q} \times \mathbb{Q} : n \leq m\}$.

A.15 (Relaciones de orden) Una relación R sobre un conjunto A se dice que es una *relación de orden* si es reflexiva, antisimétrica y transitiva (ejemplos (d), (h), (i) de A.14). Una relación de orden R sobre A suele denotarse por el símbolo "$\leq$" ("menor ó igual"), es decir, si $a, b \in A$ tal que aRb entonces se escribe $a \leq b$ y se dice que "a es menor ó igual que b". Un *conjunto ordenado* es un par $(A, \leq)$ formado por un conjunto A y una relación de orden "$\leq$" sobre A.

Sea $(A, \leq)$ un conjunto ordenado. Dos elementos $a, b \in A$ se dice que son *comparables* si $a \leq b$ ó $b \leq a$; si todo par de elementos de A son comparables se dice que $(A, \leq)$ es un *conjunto totalmente ordenado* (ó que $\leq$ es un *orden total* sobre A). Si a, b son elementos de A que satisfacen $a \leq b$ y $a \neq b$, entonces se escribe "$a < b$" y se dice que "a es menor que b". También se escribe a veces "$b \geq a$" ("b es mayor ó igual que a") en lugar de "$a \leq b$", y "$b > a$" ("b es mayor que a") en lugar de "$a < b$"

Sea E un subconjunto de A. Un elemento $a \in A$ se dice que es *cota superior* de E si todo elemento de E es menor ó igual que a: $e \leq a$ para todo $e \in E$. No necesariamente existen cotas superiores de E; si existen se dice que E está *acotado superiormente*. Si E está acotado superiormente y existe la más pequeña de las cotas superiores de E (que de existir es única por la propiedad antisimétrica), entonces dicho elemento recibe el nombre de *supremo* de E y se denota $\sup E$. Es decir, si $\sup E$ existe es el único elemento de A caracterizado por satisfacer las dos siguientes propiedades

- $\sup E$ es cota superior de E: $e \leq \sup E$ para todo $e \in E$;
- toda cota superior de E es mayor ó igual que $\sup E$: $a \in A$, $e \leq a$ para todo $e \in E \ \Rightarrow \sup E \leq a$.

Un conjunto puede estar acotado superiormente y no tener supremo. Si $\sup E$ existe y pertenece a E entonces dicho supremo se denomina *máximo* de E y se denota $\max E$.

Se llama elemento *maximal* de E a todo elemento $\bar{e} \in E$ para el que se satisfaga que en E no existen elementos mayores que $\bar{e}$; es decir, $\bar{e}$ es un elemento maximal de E si $\bar{e} \in E$ y para todo $e \in E$ se satisface: $e \leq \bar{e}$ ó e y $\bar{e}$ no son comparables.

De modo análogo se definen: *cota inferior*, *conjunto acotado inferiormente*, *ínfimo* ($\inf$), *mínimo* ($\min$), *elemento minimal*. Un subconjunto de A se dice que es *acotado* si está acotado superior e inferiormente. Si A (como subconjunto de sí mismo) tiene ínfimo entonces éste será automáticamente el mínimo de A y se dice que es el *primer elemento* del conjunto ordenado. Del mismo modo, se define el *último elemento* del conjunto ordenado A como el máximo de A (cuando exista).

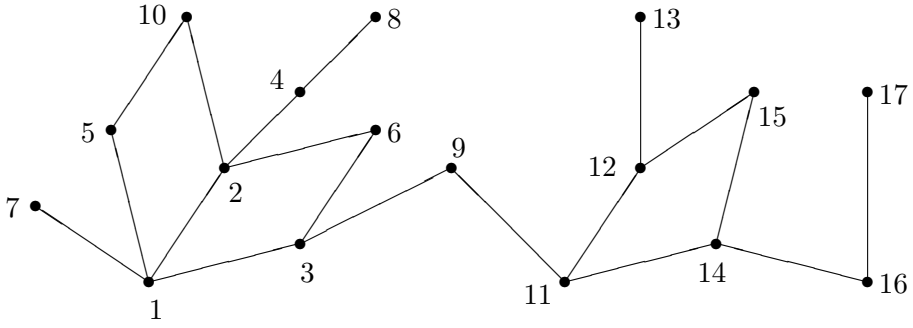

Figura 1.

Ejemplos A.16 (a) Sea C un conjunto y consideremos en $A = \mathcal{P}(\mathcal{C})$ la relación de orden que define la inclusión, es decir, dados C_1 y C_2 subconjuntos de C diremos que C_1 está relacionado con C_2 cuando $C_1 \subseteq C_2$ (ejemplo A.14 (d)).

Sea E un subconjunto de A, es decir, sea E una familia de subconjuntos de C: $E = \{C_i\}_{i \in I}$ con C_i subconjunto de C para todo $i \in I$. Una cota superior para E será todo subconjunto de C que contenga a todos los subconjuntos de la familia E, por ejemplo el propio C (C es el último elemento de A); una cota inferior para E será todo subconjunto de C que esté contenido en todos los subconjuntos de E, por ejemplo $\emptyset$ ($\emptyset$ es el primer elemento de A); en este caso siempre existen $\inf E$ y $\sup E$,

$$\inf E = \cap_{i \in I} C_i \,, \qquad \sup E = \cup_{i \in I} C_i \,.$$

(b) Sea $A = \{1, 2, \ldots, 17\}$ con el orden determinado por el "diagrama de árbol" de la figura 1 del siguiente modo: dados $a, b \in A$, $a \leq b$ si y sólo si $a = b$ ó a y b están unidos por segmentos que forman un camino que es ascendente al ir desde a hasta b. En este caso A no tiene ni primer ni último elemento.

Sea $E = \{9, 12, 13, 14\}$. El subconjunto E de A no está acotado superiormente pero sí está acotado inferiormente; además su única cota inferior es 11 y por lo tanto $\inf E = 11$; E no tiene mínimo porque $11 \notin E$. Los elementos maximales de E son 9, 13 y 14, y los elementos minimales de E son 9, 12 y 14.

Estúdiense los siguientes subconjuntos de A: $B = \{3, 9, 11, 12, 13, 14, 15, 16, 17\}$, $C = \{1, 2, 3, 4, 6, 8, 9, 11\}$, $D = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

(c) Sea $A = \mathbb{Q}$ con el orden usual de números fraccionarios (que es un orden total) y consideremos el conjunto $E = \{q \in \mathbb{Q} : 2 \leq q < 3\}$; E está acotado inferiormente e $\inf E = 2$;

además como $2 \in E$ existe el mínimo de E, $\min E = 2$; E también está acotado superiormente y $\sup E = 3$, pero no existe el máximo de E porque $3 \notin E$.

(d) Es conocido que el conjunto $\mathbb{N}$ de los números naturales dotado de su orden usual es un conjunto totalmente ordenado, y que todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo.

A.17 (Morfismos de conjuntos ordenados) Sean $(X, \leq)$, $(Y, \leq)$ conjuntos ordenados. Aunque denotamos de igual modo el orden de X y el orden de Y no debe de haber motivo de confusión, pues el contexto aclara a cual de ellos representa el símbolo $\leq$: si escribimos $x_1 \leq x_2$ con $x_1, x_2 \in X$ es claro que entonces $\leq$ denota el orden de X, y si escribimos $y_1 \leq y_2$ con $y_1, y_2 \in Y$ entonces $\leq$ denota el orden de Y.

Una aplicación $f : X \to Y$ se dice que es un *morfismo de conjuntos ordenados* si conserva el orden, es decir, si satisface la implicación

$$x_1, x_2 \in X\,, \quad x_1 \leq x_2 \qquad \Rightarrow \qquad f(x_1) \leq f(x_2)\,.$$

Sea $f : X \to Y$ un morfismo de conjuntos ordenados. Se dice que f es un *isomorfismo de conjuntos ordenados* si existe un morfismo de conjuntos ordenados $g : Y \to X$ tal que $f \circ g = I_Y$ y $g \circ f = I_X$, donde I_X e I_Y denotan la aplicación identidad de X y la aplicación identidad de Y, respectivamente. Es fácil comprobar que si f es un isomorfismo de conjuntos ordenados, entonces el morfismo de conjuntos ordenados $g : Y \to X$ que satisface $f \circ g = I_Y$ y $g \circ f = I_X$ es único, por lo que se denomina *morfismo inverso* de f y se denota f^{-1}.

Si f es un isomorfismo de conjuntos ordenados entonces f es una aplicación biyectiva y su isomorfismo inverso f^{-1} es la aplicación inversa de f (véase A.13). Es decir, un morfismo de conjuntos ordenados es un isomorfismo si es biyectivo y su aplicación inversa es morfismo de conjuntos ordenados. Puede ocurrir que el morfismo de conjuntos ordenados f sea una aplicación biyectiva y que su aplicación inversa no sea morfismo de conjuntos ordenados, en cuyo caso f no es un isomorfismo. Por ejemplo, sean $X = \{a, b\}$, $Y = \{c, d\}$ con los órdenes dados por los diagramas de árbol de la figura 2, y sea $f : X \to Y$ definida como $f(a) = c$ y $f(b) = d$; es claro que f es un morfismo de conjuntos ordenados biyectivo que no es isomorfismo,

Figura 2.

pues su aplicación inversa no es morfismo de conjuntos ordenados.

Ejemplo A.18 Sea $g : A \to B$ una aplicación entre conjuntos y consideremos $X = \mathcal{P}(\mathcal{A})$, $Y = \mathcal{P}(\mathcal{B})$ dotados con el orden definido por la inclusión. La aplicación imagen directa por g, que está definida en X y valora en Y, es un morfismo de conjuntos ordenados (véase A.11); la aplicación imagen inversa por g también es un morfismo de conjuntos ordenados. Además, si g es biyectiva entonces su imagen directa y su imagen inversa son isomorfismos de conjuntos ordenados, inverso uno del otro.

A.19 (Retículos) Se denomina *retículo* a todo conjunto ordenado en el que todo subconjunto finito no vacío tiene supremo e ínfimo.

Ejemplos: es claro que todo conjunto totalmente ordenado es un retículo; si A es un conjunto y $\mathcal{P}(\mathcal{A})$ es considerado con su orden natural (el dado por la inclusión), entonces $\mathcal{P}(\mathcal{A})$ es un retículo (véase (a) de A.16).

Sean $(X, \leq)$ e $(Y, \leq)$ retículos. Una aplicación $f : X \to Y$ se dice que es un *morfismo de retículos* si transforma supremos en supremos e ínfimos en ínfimos, es decir, si dados $x_1, \ldots, x_n \in X$ se satisface

$$f\Big(\sup\{x_1, \ldots, x_n\}\Big) = \sup\Big\{f(x_1), \ldots, f(x_n)\Big\}\,.$$

Es inmediato demostrar que todo morfismo de retículos es en particular un morfismo de conjuntos ordenados; el recíproco no es cierto (pónganse ejemplos).

Sea $f : X \to Y$ un morfismo de retículos. Se dice que f es un *isomorfismo de retículos* si existe un morfismo de retículos $g : Y \to X$ tal que $f \circ g = I_Y$ y $g \circ f = I_X$. Es fácil comprobar que si f es un isomorfismo de retículos entonces el morfismo de retículos $g : Y \to X$ que satisface $f \circ g = I_Y$ y $g \circ f = I_X$ es único, por lo que se denomina *morfismo inverso* de f y se denota f^{-1}; claramente, como aplicación f^{-1} es la aplicación inversa de f.

Dada una aplicación $f : X \to Y$ entre retículos tenemos:

(i) Si f es un isomorfismo de conjuntos ordenados entonces f es un isomorfismo de retículos. (Pruébese como ejercicio.)

(ii) Si f es un morfismo de retículos que es biyectivo entonces su aplicación inversa es también un morfismo de retículos y por lo tanto f es un isomorfismo de retículos (compárese en A.17 con lo que ocurre para los morfismos de conjuntos ordenados). Para demostrarlo bastará ver que la aplicación inversa f^{-1} es un morfismo de conjuntos ordenados, pues entonces f sería un isomorfismo de conjuntos ordenados y concluiríamos aplicando el apartado (i) anterior. Sean $y_1, y_2 \in Y$ tales que $y_1 \leq y_2$ y probemos que entonces $f^{-1}(y_1) \leq f^{-1}(y_2)$: si denotamos $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$ tenemos

$$f\Big(\sup\{x_1, x_2\}\Big) = \sup\Big\{f(x_1), f(x_2)\Big\} = \sup\{y_1, y_2\} = y_2\,,$$

y por lo tanto

$$\sup\{x_1, x_2\} = f^{-1}(y_2) = x_2 \qquad \Rightarrow \qquad x_1 \leq x_2\,.$$

Ejemplo A.20 Sea $g : A \to B$ una aplicación entre conjuntos y consideremos $X = \mathcal{P}(\mathcal{A})$, $Y = \mathcal{P}(\mathcal{B})$ dotados con sus ordenes naturales, con los que son retículos. De lo dicho en A.11 (b) se sigue que la imagen inversa por g es un morfismo de retículos de Y en X. La imagen directa por g no siempre es morfismo de retículos (aunque sí es morfismo de conjuntos ordenados); cuando g es inyectiva la imagen directa por g sí es morfismo de retículos (véase A.11 (a)). Además, si g es biyectiva entonces su imagen directa y su imagen inversa son isomorfismos de retículos, inverso uno del otro.

A.21 (Lema de Zorn) Sea $(X, \leq)$ un conjunto ordenado. Dado un subconjunto C de X, el orden de X restringido a C define de modo natural un orden sobre C: dados $c, c' \in C$, diremos que $c \leq c'$ en C cuando $c \leq c'$ en X. Se dice que C es una *cadena* de X si $(C, \leq)$ es un conjunto totalmente ordenado.

En Teoría de Conjuntos se acepta como válido el siguiente resultado conocido como "Lema de Zorn": *Sea* $(X, \leq)$ *un conjunto ordenado. Si toda cadena de* X *está acotada superiormente, entonces en* X *existen elementos maximales.*

A.22 (Relaciones de equivalencia) Una relación en un conjunto se dice que es de *equivalencia* si es reflexiva, simétrica y transitiva. Dichas relaciones suelen denotarse por el símbolo "$\sim$", es decir, si R es una relación de equivalencia en un conjunto A y $a, b \in A$ tales que aRb, entonces escribimos $a \sim b$.

Si observamos el ejemplo (g) de A.14 podemos darnos cuenta de que la relación definida en el conjunto de cartulinas las clasifica por colores. En general, una relación de equivalencia "particiona" el conjunto sobre el que está definida en el sentido que precisaremos a continuación (véase A.7).

Sea $\sim$ una relación de equivalencia sobre un conjunto A. Para cada $a \in A$ se define la *clase de equivalencia* de a como el siguiente subconjunto $\pi(a)$ de A:

$$\pi(a) := \{b \in A \,:\, a \sim b\}\,.$$

Es claro que toda clase de equivalencia es un conjunto no vacío, pues dado $a \in A$ se tiene $a \in \pi(a)$; también es clara la igualdad $A = \cup_{a\in A}\pi(a)$; tenemos además que dados $a, b \in A$ se satisfacen

$$a \sim b \iff \pi(a) = \pi(b)\,, \qquad a \not\sim b \iff \pi(a) \cap \pi(b) = \emptyset\,,$$

donde $a \not\sim b$ significa que a no está relacionado con b. Por lo tanto mediante la relación $\sim$ todos los elementos de A quedan clasificados en partes disjuntas cuya unión es A.

El recíproco también es cierto: una partición del conjunto A define una relación de equivalencia sobre A cuyas clases de equivalencia son los subconjuntos de la partición. En efecto, una partición $\{A_i\}_{i\in I}$ de A define la siguiente relación: dados $a, b \in A$,

$$a \sim b \quad :\Longleftrightarrow \quad \exists\, i \in I \,:\, a, b \in A_i\,;$$

es decir, dos elementos están relacionados cuando pertenecen a un mismo subconjunto de los de la partición; dicha relación es de equivalencia, y para cada $a \in A$ la clase de equivalencia de a es el único subconjunto de la partición que contiene a a.

Sea A un conjunto dotado de una relación de equivalencia $\sim$. El conjunto cuyos elementos son todas las clases de equivalencia de dicha relación se denota $A/\!\sim$ y se denomina *conjunto cociente* de A por la relación $\sim$, $A/\!\sim := \{\pi(a) \,:\, a \in A\}$. Tenemos la aplicación natural $\pi : A \to A/\!\sim$, $a \mapsto \pi(a)$, que manda cada elemento de A a su clase de equivalencia; esta aplicación es siempre epiyectiva y se denomina *aplicación de paso al cociente*. Dado $a \in A$, si $b \in \pi(a)$ se dice que "b es un representante de la clase $\pi(a)$"; es obvio que a representa a $\pi(a)$.

A.23 (Números enteros) Veamos la construcción de los números enteros a partir de los números naturales. Suponemos conocido el conjunto de los números naturales $\mathbb{N} = \{0, 1, 2, \dots\}$ con su suma, su producto y su orden; recordemos que dados $a, b \in \mathbb{N}$, $b - a$ tiene sentido en $\mathbb{N}$ (es decir, existe $c \in \mathbb{N}$ tal que $b = c + a$) sólo cuando $b \geq a$.

En el conjunto $\mathbb{N} \times \mathbb{N}$ definimos la siguiente relación: dados $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$,

$$(a, b) \sim (c, d) \qquad :\Longleftrightarrow \qquad a + d = b + c\,.$$

Es inmediato comprobar que la anterior es una relación de equivalencia. Se define el conjunto $\mathbb{Z}$ de los *números enteros* como el conjunto cociente de $\mathbb{N}\times\mathbb{N}$ por la relación $\sim$ definida, $\mathbb{Z} := (\mathbb{N}\times\mathbb{N})/\!\sim$. Tenemos la aplicación $\pi : \mathbb{N}\times\mathbb{N} \to \mathbb{Z}$ de paso al cociente.

En $\mathbb{Z}$ definimos la suma "$+$", el producto "$\cdot$" y el orden "$\leq$" siguientes:

$$\begin{aligned} \pi(a,b) + \pi(c,d) &:= \pi(a+c, b+d)\,, \\ \pi(a,b)\cdot\pi(c,d) &:= \pi(ac+bd, bc+ad)\,, \\ \pi(a,b) \leq \pi(c,d) \quad &:\Longleftrightarrow \quad a+d \leq b+c\,. \end{aligned}$$

Es fácil comprobar que las anteriores definiciones no dependen de los representantes elegidos en las clases de equivalencia. Veámoslo por ejemplo para la suma: si $\pi(a,b) = \pi(a',b')$ y $\pi(c,d) = \pi(c',d')$ entonces $a+b' = b+a'$ y $c+d' = d+c'$, de modo que $a+c+b'+d' = b+d+a'+c'$ y por lo tanto $\pi(a+c, b+d) = \pi(a'+c', b'+d')$.

De las definiciones anteriores y de las propiedades de los números naturales se deducen fácilmente las siguientes propiedades de los números enteros

(i) la suma y el producto son operaciones conmutativas y asociativas;

(ii) el producto distribuye a la suma: $z_1\cdot(z_2+z_3) = z_1\cdot z_2 + z_1\cdot z_3$ $(z_1, z_2, z_3 \in \mathbb{Z})$;

(iii) en $\mathbb{Z}$ hay "elemento nulo": dado $a\in\mathbb{N}$, $\pi(a,a) = \pi(0,0)$ es el único elemento de $\mathbb{Z}$ que satisface $\pi(a,a) + z = z$ para todo $z\in\mathbb{Z}$;

(iv) en $\mathbb{Z}$ hay "opuestos": dado un número entero $\pi(a,b)$, $\pi(b,a)$ es el único elemento de $\mathbb{Z}$ que satisface $\pi(a,b) + \pi(b,a) = \pi(0,0)$ ($=$elemento nulo);

(v) en $\mathbb{Z}$ hay "elemento unitario": dado $a\in\mathbb{N}$, $\pi(a+1,a) = \pi(1,0)$ es el único elemento de $\mathbb{Z}$ que satisface $\pi(a+1,a)\cdot z = z$ para todo $z\in\mathbb{Z}$;

(vi) en $\mathbb{Z}$ no hay "divisores de cero": si $z_1, z_2 \in \mathbb{Z}$ tales que $z_1\cdot z_2 = \pi(0,0)$, entonces uno de los enteros z_1, z_2 es igual a $\pi(0,0)$;

(vii) "$\leq$" es una relación de orden total sobre $\mathbb{Z}$.

Cada número natural n define el número entero $\pi(n,0)$, de modo que tenemos la aplicación natural $\mathbb{N}\to\mathbb{Z}$, $n\mapsto\pi(n,0)$, que es inyectiva y permite considerar a $\mathbb{N}$ como un subconjunto de $\mathbb{Z}$; la suma, el producto y la ordenación de números enteros coincide en $\mathbb{N}$ con la suma, el producto y la ordenación de números naturales.

Sea $\pi(a,b)$ un número entero. Si $a\geq b$ y $n = a-b\in\mathbb{N}$, entonces $\pi(a,b) = \pi(n,0)$ es el número natural n. Si $a<b$ entonces $b-a = n$ es un número natural que es el opuesto de $\pi(a,b)$, $\pi(b-a,0) + \pi(a,b) = \pi(0,0)$; cuando $a<b$ el número entero $\pi(a,b)$ lo denotaremos $-n$, donde $n = b-a\in\mathbb{N}$.

De lo dicho en el párrafo anterior, y teniendo en cuenta que si la suma de dos números naturales es nula entonces ambos sumandos son nulos, se sigue: "*El conjunto de los números enteros es la unión disjunta de* $\mathbb{N}$ *con el conjunto de los opuestos de los números naturales no nulos.*" Esto es,

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

El anterior resultado permite definir el *valor absoluto* de $z\in\mathbb{Z}$ como el número entero $|z|$ dado por la igualdad $|z| := \max\{z, -z\}$, que es siempre un número natural porque $z\geq 0$ si y sólo si $z\in\mathbb{N}$; de otro modo, $|z| = z$ si $z\geq 0$ y $|z| = -z$ si $z<0$. Un número entero z se dice que es *positivo* cuando $z>0$, y se dice que es *negativo* si $z<0$.

En adelante, dados $z_1, z_2\in\mathbb{Z}$ escribiremos z_1z_2 en lugar de $z_1\cdot z_2$.

Teorema A.24 (División entera) *Sea d un número entero no nulo. Para cada número entero z existe una única pareja de números enteros c, r (llamados respectivamente* cociente *y* resto *de la* división *de z por d) tal que*

$$z = cd + r\,, \qquad 0 \leq r < |d|\,.$$

Demostración. Veamos la existencia de la pareja r, c. El conjunto de números naturales

$$N = \{n \in \mathbb{N} \,:\, n = z + sd \text{ para algún } s \in \mathbb{Z}\}$$

no es vacío ($z+(zzd)d \in N$) y por tanto tiene primer elemento (véase A.16 (d)); sea $r = \min N$. Por definición $r \geq 0$ y existe $s \in \mathbb{Z}$ tal que $r = z + sd$, luego $z = (-s)d + r$. Si $r \geq |d|$ entonces $r - |d| = z + (s \pm 1)d$ está en N y es estrictamente menor que r, en contra de la elección de r. Luego $r < |d|$.

Probemos ahora la unicidad del cociente y del resto. Si c', r' son otros números enteros tales que $z = c'd + r'$ y $0 \leq r' < |d|$, podemos suponer que $r \leq r'$, en cuyo caso $r' - r = (c - c')d$ es un múltiplo no negativo de $|d|$ menor que $|d|$, y se sigue que $r' - r = 0$ y $cd = c'd$. Como d es no nulo concluimos que $r = r'$ y $c = c'$. ∎

A.25 (Factorización canónica de aplicaciones) Sea $f : A \to B$ una aplicación entre conjuntos; f define de modo natural en A la siguiente relación: dados $a, b \in A$,

$$a \sim b \qquad :\Longleftrightarrow \qquad f(a) = f(b)\,.$$

Es inmediato comprobar que la anterior es una relación de equivalencia. Se satisface el siguiente resultado conocido como "teorema de factorización canónica de aplicaciones" : *Existe una única aplicación biyectiva $\bar{f} : A/\!\sim \to \operatorname{Im} f$ que hace que el cuadrado de aplicaciones*

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ A/\!\sim & \xrightarrow{\ \bar{f}\ } & \operatorname{Im} f \end{array}$$

sea conmutativo, es decir, $f = i \circ \bar{f} \circ \pi$ (π denota la aplicación de paso de A al cociente $A/\!\sim$, que es epiyectiva, e i es la inclusión de $\operatorname{Im} f$ en B, que es inyectiva). La demostración de este teorema es sencilla y se deja como ejercicio para el lector.

A.26 (Axiomas de inducción) *Sea $A \subseteq \mathbb{N}$ y sea $n_0 \in \mathbb{N}$. Si se satisfacen*

(i) $n_0 \in A$,

(ii) $A \subseteq \{n \in \mathbb{N} \,:\, n \geq n_0\} = \{n_0, n_0 + 1, n_0 + 2, \dots\}$,

(iii) $n \in A \quad \Rightarrow \quad n + 1 \in A$,

entonces $A = \{n \in \mathbb{N} \,:\, n \geq n_0\}$.

La anterior afirmación se conoce como "axioma de inducción transfinita", y se usa como técnica de demostración del siguiente modo: Sea P una "función proposicional" sobre los elementos de $\mathbb{N}$, es decir, para cada $n \in \mathbb{N}$ tenemos una proposición $\mathrm{P}(n)$ que puede ser verdadera ó falsa; si por ejemplo queremos probar que $\mathrm{P}(n)$ es cierto para todos los números

naturales del conjunto $\{n \in \mathbb{N} : n \geq 7\}$ (aquí $n_0 = 7$ y $A = \{n \in \mathbb{N} : n \geq 7 \text{ y } \mathrm{P}(n) \text{ es cierto}\}$), probamos en primer lugar que $\mathrm{P}(7)$ es cierto y a continuación demostramos que si n es un natural tal que $n \geq 7$ y $\mathrm{P}(n)$ es cierto entonces $\mathrm{P}(n+1)$ también es cierto; el axioma de inducción nos dice entonces que $A = \{n \in \mathbb{N} : n \geq 7\}$, es decir, que $\mathrm{P}(n)$ es cierto para todo $n \geq 7$.

Tenemos también el conocido como "axioma de inducción completa": *Sea* $A \subseteq \mathbb{N}$ *y sean* $n_1, n_2 \in \mathbb{N}$ *tales que* $n_1 < n_2$. *Si se satisfacen*

(i) $n_1 \in A$,

(ii) $A \subseteq [n_1, n_2] = \{n \in \mathbb{N} : n_1 \leq n \leq n_2\}$,

(iii) $n \in A,\ n < n_2 \quad \Rightarrow \quad n+1 \in A$,

entonces $A = [n_1, n_2]$.

Como aplicación sencilla del axioma de inducción demuéstrese que para todo número natural $n \neq 0$ se satisfacen las siguientes igualdades:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}\,, \qquad \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}\,,$$

$$6(1 + 7 + 7^2 + \cdots + 7^n) + 1 = 7^{n+1}\,, \qquad 1 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}\,.$$

Ejercicio A.27 Sean N un conjunto con n elementos y M un conjunto con m elementos tales que $m \leq n$. Pruébese que el conjunto $\{$aplicaciones inyectivas de M en $N\}$ tiene $n\cdot(n-1)\cdot(n-2)\cdot\cdots\cdot(n-[m-1])$ elementos. Como consecuencia obténgase que si A es un conjunto con n elementos entonces el número de "permutaciones" de A es $n! := n\cdot(n-1)\cdot(n-2)\cdot\cdots\cdot 2\cdot 1$ (el símbolo $n!$ se lee "n factorial"). (Se denomina *permutación* de un conjunto A a toda aplicación biyectiva de A en A.)

B Generalidades sobre Teoría de Grupos

B.1 (Grupos) Se llama *grupo* a todo par $(G, *)$ formado por un conjunto G y por una aplicación

$$\begin{array}{ccc} G\times G & \xrightarrow{*} & G \\ (a,b) & \mapsto & a*b\,, \end{array}$$

denominada *operación* del grupo, que satisface las siguientes propiedades:

(i) (asociativa) $a*(b*c) = (a*b)*b$ cualesquiera que sean $a, b, c \in G$; la asociatividad de la operación permite quitar los paréntesis en la expresión $a*(b*c)$ para escribir simplemente $a*b*c$:

(ii) (existencia de elemento neutro) existe $e \in G$ tal que $a*e = e*a = a$ cualquiera que sea $a \in G$; dicho elemento es único, ya que si hubiera dos con la anterior propiedad, e y e', tendríamos

$$e = e*e' = e'\,;$$

el elemento e se conoce como *neutro* de la operación;

(iii) (existencia de simétricos) para todo $a \in G$ existe $b \in G$ tal que $a * b = b * a = e$; dado $a \in G$, el elemento $b \in G$ que satisface la anterior propiedad es único, ya que si hubiera dos, b y b', tendríamos

$$b = e * b = (b' * a) * b = b' * (a * b) = b' * e = b' ;$$

el elemento b anterior se denomina *simétrico* de a; es claro que si b es el simétrico de a entonces a es el simétrico de b.

Se dice que el grupo $(G, *)$ es *conmutativo* (ó *abeliano*) si su operación es conmutativa, esto es, si $a * b = b * a$ cualesquiera que sean $a, b \in G$.

Ejemplos B.2 (a) Hay un grupo que tiene un único elemento (el elemento neutro); se denomina grupo *trivial*, y es claro que es abeliano.

(b) Dado un conjunto A, si $P(A)$ es el conjunto de todas las biyecciones de A en A y "$\cdot$" es la operación "composición de aplicaciones" sobre $P(A)$, entonces $(P(A), \cdot)$ es un grupo: la composición de aplicaciones es asociativa, el elemento neutro es la aplicación identidad de A, y dada $f \in P(A)$ su simetrico es la aplicación f^{-1}. Dicho grupo se denomina *grupo de las permutaciones del conjunto* A. Cuando $A = \{1, 2, \ldots, n\}$ $(n \in \mathbb{N})$ el grupo $P(A)$ se denota S_n y se denomina *grupo simétrico de orden* n; según A.27, el número de elementos de S_n es $n!$.

(c) Los números enteros con su suma, $(\mathbb{Z}, +)$, tienen estructura de grupo abeliano (véase A.23); el elemento neutro es 0, y dado $n \in \mathbb{Z}$ su simétrico es el entero $-n$. Es fácil ver que $(\mathbb{Z}, \cdot)$ no es un grupo.

Proposición B.3 *Para todo grupo* $(G, *)$ *se satisfacen*

(i) *(propiedad de simplificación) si* $a, b, c \in G$ *son tales que* $a * c = b * c$ *entonces* $a = b$*;*

(ii) *dados* $a, b \in G$*, si* $\bar{a}$ *es el simétrico de* a *y* $\bar{b}$ *es el simétrico de* b *entonces el simétrico de* $a * b$ *es* $\bar{b} * \bar{a}$*.*

Demostración. Para probar (i) basta operar por la derecha en los dos miembros de la igualdad por el simétrico de c. En cuanto a (ii) tenemos

$$(a * b) * (\bar{b} * \bar{a}) = a * b * \bar{b} * \bar{a} = a * \bar{a} = e\,, \qquad (\bar{b} * \bar{a}) * (a * b) = \bar{b} * \bar{a} * \bar{a} * b = \bar{b} * b = e\,,$$

y basta tener en cuenta la unicidad del elemento simétrico para concluir. ∎

B.4 (Notaciones) La operación de un grupo suele denotarse por el símbolo "$\cdot$" ó por el símbolo "$+$"; en el primer caso la notación se denomina *multiplicativa* y en el segundo caso *aditiva*.

En $(G, \cdot)$ su elemento neutro se denomina elemento *unitario* (ó simplemente *uno*) y se denota "1"; dado $a \in G$ su simétrico se denomina *inverso* de a y se denota a^{-1}. Dados $a \in G$ y $n \in \mathbb{Z}$ se denomina "a elevado a n" al elemento $a^n \in G$ dado por la igualdad

$$a^n := \begin{cases} a \cdot \overset{n}{\ldots} \cdot a & \text{si } n > 0\,, \\ 1 & \text{si } n = 0\,, \\ a^{-1} \cdot \overset{|n|}{\ldots} \cdot a^{-1} & \text{si } n < 0\,. \end{cases}$$

Cualesquiera que sean $a \in G$ y $n, m \in \mathbb{Z}$ se satisface $a^{n+m} = a^n \cdot a^m$; NO es siempre cierto que dados $a, b \in G$ y $n \in \mathbb{Z}$ se satisfaga la igualdad $(a \cdot b)^n = a^n \cdot b^n$.

Análogamente, en $(G, +)$ su elemento neutro se denomina elemento *nulo* (ó simplemente *cero*) y se denota "0"; dado $a \in G$ su simétrico se denomina *opuesto* de a y se denota $-a$. Dados $a \in G$ y $n \in \mathbb{Z}$ se denomina "producto de n por a" al elemento $na \in G$ dado por la igualdad

$$na := \begin{cases} a + \overset{n}{\ldots} + a & \text{si } n > 0\,, \\ 0 & \text{si } n = 0\,, \\ (-a) + \overset{|n|}{\ldots} + (-a) & \text{si } n < 0\,. \end{cases}$$

Cualesquiera que sean $a \in G$ y $n, m \in \mathbb{Z}$ se satisface $(n + m)a = na + ma$; NO es siempre cierto que dados $a, b \in G$ y $n \in \mathbb{Z}$ se satisfaga la igualdad $n(a + b) = na + nb$. Dados $a, b \in G$, para simplificar escribiremos $a - b$ en lugar de $a + (-b)$.

Cuando se estudia la Teoría de Grupos generalmente se utiliza la notación multiplicativa; nosotros por el contrario usaremos para esta breve introducción la notación aditiva, a no ser que estudiemos un grupo concreto cuya notación sea multiplicativa (como por ejemplo el grupo de las permutaciones de un conjunto). Para simplificar, en lugar de decir "Sea $(G, +)$ un grupo ..." diremos simplemente "Sea G un grupo ...", entendiendo que sobre G hay una operación que denotaremos "$+$".

Ejercicio B.5 Dado un grupo G, pruébese que son equivalentes las siguientes afirmaciones:

(a) G es abeliano;

(b) cualesquiera que sean $a, b \in G$ y $n \in \mathbb{Z}$ se satisface $n(a + b) = na + nb$;

(c) cualesquiera que sean $a, b \in G$ se satisface $-(a + b) = -a - b$.

[Indicación: Pruébense las implicaciones (a)⇒(b), (b)⇒(c) y (c)⇒(a) (nótese que la segunda implicación es trivial). Para probar la primera implicación se pueden seguir los siguientes pasos: en primer lugar probarla para $n > 0$ usando el axioma de iducción, en segundo lugar probarla para $n < 0$ teniendo en cuenta la igualdad $-n(a + b) = n(-a - b)$, y por último probarla para $n = 0$.]

B.6 (Subgrupos) Sea G un grupo y sea G' un subconjunto de G. Se dide que G' es un *subgrupo* de G si satisface:

(i) G' es cerrado frente a la operación de G, es decir, si $a, b \in G'$ entonces $a + b \in G'$;

(ii) G' contiene al elemento neutro de G, es decir, $0 \in G'$;

(iii) G' contiene al opuesto de cada elemento suyo, es decir, si $a \in G'$ entonces $-a \in G'$.

Si G' es un subgrupo de G podemos restringir la operación de G a G' y se satisface que $(G', +)$ es también un grupo.

Proposición B.7 *Sea G un grupo. Dado un subconjunto no vacío G' de G se satisface: G' es un subgrupo si y sólo si $a - b \in G'$ para cualesquiera $a, b \in G'$.*

Demostración. Es claro que si G' es un subgrupo de G entonces $a - b \in G'$ cualesquiera que sean $a, b \in G'$.

Supongamos que para todo $a, b \in G'$ se tiene $a - b \in G'$, y probemos que entonces G' es un subgrupo. Como $G' \neq \emptyset$ existe $c \in G'$, de modo que $0 = c - c \in G'$. Ahora, dado $a \in G'$ se tiene $-a = 0 - a \in G'$, y dados $a, b \in G'$ se satisface $a + b = a - (-b) \in G'$. ∎

Ejemplos B.8 (a) Todo grupo es un subgrupo de él mismo; dicho subgrupo se denomina *total* ó *impropio*; un subgrupo de un grupo se dice que es *propio* si es distinto del total.

(b) Todo grupo tiene un subgrupo denominado *trivial*: el que tiene como único elemento el cero.

(c) Consideremos el grupo $(\mathbb{Z}, +)$. Dado $a \in \mathbb{Z}$ sea (a) el conjunto de los "múltiplos enteros" de a,

$$(a) := \{na \,:\, n \in \mathbb{Z}\} = \{\dots, -2a, -a, 0, a, 2a, \dots\}\,;$$

se comprueba fácilmente que (a) es un subgrupo de $\mathbb{Z}$. Veamos que todo subgrupo de $\mathbb{Z}$ es así. Sea H un subgrupo de $\mathbb{Z}$ y supongamos que $H \neq 0$ (si $H = 0$ entonces $H = (0)$); sea a el entero positivo más pequeño de H. Es claro que al ser $a \in H$ se satisface $(a) \subseteq H$. Veamos la otra inclusión: dado $b \in H$, existen $c, r \in \mathbb{Z}$ tales que $b = ac + r$ con $0 \leq r < a$ (véase A.24); si fuera $0 < r < a$ tendríamos que $r = b - ac \in H$ es un entero positivo de H más pequeño que a, lo que contradice la elección de a; por lo tanto debe ser $r = 0$ y concluimos que $b = ac \in (a)$.

(d) Dados subgrupos H_1 y H_2 de un grupo G, la intersección $H_1 \cap H_2$ es un subgrupo de G (compruébese). Además, dicho subgrupo intersección es el mayor (con el orden dado por la inclusión) de todos los subgrupos de G que están contenidos en H_1 y H_2.

(e) Si H_1 y H_2 son subgrupos de un grupo G no siempre es cierto que la unión $H_1 \cup H_2$ sea un subgrupo de G; concretamene se satisface (compruébese)

$$H_1 \cup H_2 \text{ es subgrupo} \qquad \Longleftrightarrow \qquad H_1 \subseteq H_2 \;\text{ ó }\; H_2 \subseteq H_1\,.$$

(f) Sean H_1 y H_2 subgrupos de un grupo G. Se define la *suma* de H_1 y H_2 como el conjunto $H_1 + H_2$ dado por la igualdad

$$H_1 + H_2 = \{h_1 + h_2 \,:\, h_1 \in H_1,\, h_2 \in H_2\}\,;$$

es decir, $H_1 + H_2$ es el conjunto de los elementos de G que se pueden poner como suma de un elemento de H_1 y un elemento de H_2 (en ese orden). NO siempre es cierta la igualdad $H_1 + H_2 = H_2 + H_1$; concretamente se satisface (compruébese)

$$H_1 + H_2 \text{ es subgrupo} \qquad \Longleftrightarrow \qquad H_1 + H_2 = H_2 + H_1\,.$$

Es fácil demostrar que $H_i \subseteq H_1 + H_2$ $(i = 1, 2)$, y que cuando $H_1 + H_2$ es subgrupo es el menor (con el orden dado por la inclusión) de todos los subgrupos de G que contienen a H_1 y H_2.

Si el grupo G es abeliano entonces siempre se satisface $H_1 + H_2 = H_2 + H_1$, de modo que $H_1 + H_2$ siempre es subgrupo.

(g) De lo dicho en los apartados (a), (b), (d) y (f) se obtiene lo siguiente: Sea G un grupo abeliano y sea $S(G)$ el conjunto de todos los subgrupos de G; si consideramos el conjunto $S(G)$ dotado del orden definido por la inclusión entonces $S(G)$ es un retículo con primer y último elemento (véanse A.15, A.16 (a) y A.19).

B.9 (Morfismos de grupos) Sean G y G' grupos. Una aplicación $f : G \to G'$ se dice que es un *morfismo de grupos* (ó un *homomorfismo de grupos*) si es compatible con las operaciones de los grupos, es decir, si satisface

$$f(a+b) = f(a) + f(b) \qquad \forall\, a, b \in G\,.$$

Si un morfismo de grupos es inyectivo se denomina *monomorfismo*, si es epiyectivo se llama *epimorfismo* y si es biyectivo se denomina *isomorfismo*. A los morfismos de grupos del grupo G en sí mismo se les llama *endomorfismos* de G, y a los isomorfismos de grupos de G en sí mismo se les llama *automorfismos* de G. El conjunto de todos los endomorfismos de G se denota $\mathrm{End}(G)$, y el conjunto de todos los automorfismos de G se denota $\mathrm{Aut}(G)$.

Sea $f : G \to G'$ un morfismo de grupos. Se define el *núcleo* de f como el subconjunto $\mathrm{Ker}\, f$ de G dado por la igualdad

$$\mathrm{Ker}\, f := \{a \in G \,:\, f(a) = 0\}\,.$$

Considerando f como aplicación tenemos también su imagen, $\mathrm{Im}\, f$, que es un subconjunto de G' (véase en A.10 la definición de $\mathrm{Im}\, f$).

Proposición B.10 *Para todo morfismo de grupos $f : G \to G'$ se satisfacen:*

(i) $f(0) = 0$;
(ii) $f(-a) = -f(a)$;
(iii) $\mathrm{Ker}\, f$ *es un subgrupo de* G ;
(iv) $\mathrm{Im}\, f$ *es un subgrupo de* G' ;
(v) f *es inyectiva* $\iff$ $\mathrm{Ker}\, f = 0$.

Demostración. (i) Si tomamos un elemento cualquiera $a \in G$ tenemos

$$0 + f(a) = f(a) = f(0 + a) = f(0) + f(a)\,,$$

y basta aplicar la propiedad de simplificación para concluir que $f(0) = 0$ (véase B.3).

(ii) Dado $a \in G$ tenemos

$$f(a) - f(a) = 0 = f(0) = f(a - a) = f(a) + f(-a)\,,$$

y de nuevo basta aplicar la propiedad de simplificación para obtener que $f(-a) = -f(a)$.

Los apartados (iii) y (iv) se dejan como ejercicio.

(v) Supongamos que f es inyectiva; según (i) tenemos que $0 \in \mathrm{Ker}\, f$ porque $f(0) = 0$, de modo que la imagen por f de todo elemento de G distinto de 0 es distinta de $f(0) = 0$, es decir, $\mathrm{Ker}\, f = 0$. Recíprocamente, supongamos que $\mathrm{Ker}\, f = 0$ y probemos que entonces f es inyectiva: si $a, b \in G$ son tales que $f(a) = f(b)$ tenemos

$$f(a) = f(b) \;\Rightarrow\; f(a) - f(b) = 0 \;\Rightarrow\; f(a-b) = 0 \;\Rightarrow\; a - b \in \mathrm{Ker}\, f \;\Rightarrow\; a - b = 0\,,$$

es decir, $a = b$. ∎

Lema B.11 *La composición de morfismos de grupos es otro morfismo de grupos.*

Demostración. Inmediata; basta tener en cuenta las definiciones. ∎

Lema B.12 *Si un morfismo de grupos es un isomorfismo (es decir, es biyectivo), entonces su aplicación inversa también es morfismo de grupos (y por lo tanto también es un isomorfismo).*

Demostración. Sea $f : G \to G'$ un isomorfismo de grupos y sea $f^{-1} : G' \to G$ su aplicación inversa. Dado $a' \in G'$, recordemos que $f^{-1}(a')$ es, por definición, el único elemento de G cuya imagen por f es igual a a'; entonces, para ver que dados $a', b' \in G'$ se satisface la igualdad $f^{-1}(a' + b') = f^{-1}(a') + f^{-1}(b')$ bastará probar que la imagen por f de $f^{-1}(a') + f^{-1}(b')$ es igual a $a' + b'$, lo cual es una sencilla comprobación. ∎

Ejemplos B.13 (a) Si G' es un subgrupo de un grupo G entonces G' es un grupo y la inclusión $G' \hookrightarrow G$ es un monomorfismo de grupos cuya imagen es G'.

(b) Fijado un número entero a definimos $f : \mathbb{Z} \to \mathbb{Z}$ como $f(n) = an$ para todo $n \in \mathbb{Z}$; f también es un monomorfismo de grupos cuya imagen es (a) (véase B.8 (c)).

Proposición B.14 *Para todo morfismo de grupos $f : G \to G'$ se satisfacen:*

(i) *la imagen directa por f de todo subgrupo H de G, $f(H) = \{f(a) : a \in H\}$, es un subgrupo de G';*

(ii) *la imagen inversa por f de todo subgrupo H' de G', $f^{-1}(H') = \{a \in G : f(a) \in H'\}$, es un subgrupo de G.*

Demostración. Ejercicio. ∎

B.15 (Producto directo de grupos) Sean G_1 y G_2 grupos. El conjunto producto directo $G_1 \times G_2$ está dotado de las aplicaciones

$$\begin{array}{rcl} p_1 : G_1 \times G_2 & \to & G_1 \\ (a_1, a_2) & \mapsto & a_1 \ , \end{array} \qquad \begin{array}{rcl} p_2 : G_1 \times G_2 & \to & G_1 \\ (a_1, a_2) & \mapsto & a_2 \ , \end{array}$$

las cuales se denominan *proyecciones* sobre los conjuntos factores. Nos planteamos el problema de dotar a $G_1 \times G_2$ de estructura de grupo de modo que p_1 y p_2 sean morfismos de grupos.

Dados $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ definimos la suma $(a_1, a_2) + (b_1, b_2)$ por la igualdad

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2) \, ;$$

se comprueba fácilmente que la anterior suma es una operación que dota al conjunto producto $G_1 \times G_2$ de estructura de grupo para la cual las proyecciones son morfismos de grupos. Veamos que es la única. Supongamos que "$*$" es otra operación sobre $G_1 \times G_2$ tal que $(G_1 \times G_2, *)$ es un grupo y las proyecciones son morfismos de grupo, y sean $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ tales que $(a_1, a_2) * (b_1, b_2) = (c_1, c_2)$; utilizando que p_1 es un morfismo de grupos obtenemos

$$c_1 = p_1(c_1, c_2) = p_1((a_1, a_2) * (b_1, b_2)) = p_1(a_1, a_2) + p_1(b_1, b_2) = a_1 + b_1 \, ,$$

y del mismo modo se obtiene la igualdad $c_2 = a_2 + b_2$; por lo tanto $(a_1, a_2) * (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$.

Análogamente, dados grupos $G_1, \ldots, G_n$ hay una única operación sobre el conjunto producto $G_1 \times \cdots \times G_n$ que lo dota de estructura de grupo para la cual las proyecciones

$$\begin{array}{rcll} p_i : G_1 \times \cdots \times G_n & \to & G_i & \\ (a_1, \ldots, a_n) & \mapsto & a_i & \end{array} \qquad (i = 1, \ldots, n)$$

son morfismos de grupos; dicha operación es la suma sobre el producto definida "componente a componente", esto es, dados $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \cdots \times G_n$ su suma es

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)\,.$$

Al grupo $G_1 \times \cdots \times G_n$ (con la anterior suma) se le llama *grupo producto directo* de los grupos $G_1, \ldots, G_n$ (en ese orden).

Ejercicio B.16 Dados grupos $G_1, \ldots, G_n$, pruébese que el grupo $G_1 \times \cdots \times G_n$ es abeliano si y sólo si todos los grupos $G_1, \ldots, G_n$ son abelianos.

B.17 (Subgrupos normales, grupo cociente) Sea H un subgrupo de un grupo G; H induce en G la relación de equivalencia "$\sim_H$" siguiente: dados $a, b \in G$,

$$a \sim_H b \qquad :\Longleftrightarrow \qquad a - b \in H\,,$$

es decir, a está relacionado con b si y sólo si existe $h \in H$ tal que $a = h + b$. A la relación "$\sim_H$" se le llama *relación de equivalencia módulo* H, y el conjunto cociente $G/\!\sim_H$ se denota G/H (véase A.22). La clase de equivalencia de un elemento $a \in G$ es

$$\begin{aligned} \pi(a) &= \{b \in G \,:\, b \sim_H a\} = \{b \in G \,:\, b = h + a \text{ para algún } h \in H\} \\ &= \{h + a \,:\, h \in H\} = H + a\,. \end{aligned}$$

Nos planteamos el problema de dotar a G/H de una suma con la que sea un grupo para el cual la aplicación de paso al cociente $\pi : G \to G/H$ sea un morfismo de grupos (y por tanto un epimorfismo, ya que π es una aplicación epiyectiva). Si dicho problema tiene solución debe ser única, pues dados $\pi(a), \pi(b) \in G/H$ su suma debe satisfacer

$$\pi(a) + \pi(b) = \pi(a + b)\,,$$

es decir, "la suma de dos clases de equivalencia debe ser igual a la clase de la suma de representantes de dichas clases". Ahora bien, para que la anterior suma tenga sentido no debe depender de los representantes, esto es, dados $a, b, c, d \in G$ tales que $\pi(a) = \pi(c)$ y $\pi(b) = \pi(d)$ debe satisfacerse que $\pi(a + b) = \pi(c + d)$; veamos si lo anterior es cierto:

$$\left.\begin{array}{rcl} a \sim_H c & \Rightarrow & \exists\, h \in H \;/\; a = h + c \\ b \sim_H d & \Rightarrow & \exists\, h' \in H \;/\; b = h' + d \end{array}\right\} \;\Rightarrow\; a + b = h + c + h' + d\,,$$

y de la última igualdad no siempre se sigue que $a + b = h'' + c + d$ para algún $h'' \in H$ (si el grupo G fuera abeliano sí sería $a + b = h'' + c + d$ con $h'' = h + h'$), por lo tanto no necesariamente se satisface $\pi(a + b) = \pi(c + d)$.

Veremos que el problema planteado tiene solución si y sólo si el subgrupo H es "normal" (véase B.22 más adelante): se dice que un subgrupo H de un grupo G es *normal* si satisface

$$a + H = H + a \qquad \text{para todo } a \in G\,.$$

¡OJO!, la igualdad $a + H = H + a$ no significa que dado $h \in H$ se satisfaga $a + h = h + a$; es una igualdad entre subconjuntos de G y por lo tanto significa que se satisfacen las inclusiones $a + H \subseteq H + a$ (para todo $h \in H$ existe $h' \in H$ tal que $a + h = h' + a$) y $H + a \subseteq a + H$ (para todo $h \in H$ existe $h' \in H$ tal que $h + a = a + h'$).

Lema B.18 *Sea H un subgrupo de un grupo G. Son equivalentes:*

(i) *H es normal;*

(ii) *para cualesquiera $a \in G$, $h \in H$ se satisface $a + h - a \in H$.*

Demostración. Ejercicio. ∎

Teorema B.19 *Sea H un subgrupo normal de un grupo G. Sobre el conjunto cociente G/H existe una única estructura de grupo para la que la aplicación de paso al cociente es un morfismo de grupos; el núcleo de dicho morfismo es el subgrupo H, $\operatorname{Ker}\pi = H$. El grupo G/H se denomina* grupo cociente de G módulo H.

Demostración. Veamos que la suma descrita sobre G/H en B.17 no depende de los representantes:

$$\left.\begin{array}{rcl} \pi(a) = \pi(c) & \Rightarrow & \exists\, h \in H \;/\; a = h + c \\ \pi(b) = \pi(d) & \Rightarrow & \exists\, h' \in H \;/\; b = h' + d \end{array}\right\} \;\Rightarrow\; a + b = h + c + h' + d\,;$$

como H es normal existe $h'' \in H$ tal que $c + h' = h'' + c$ y por lo tanto $a + b = h + h'' + c + d$ con $h + h'' \in H$, es decir, $\pi(a + b) = \pi(c + d)$, que es lo que queríamos probar.

Así pues, por ser H normal es posible definir sobre G/H la suma

$$\begin{array}{rcl} G/H \times G/H & \xrightarrow{+} & G/H \\ (\pi(a), \pi(b)) & \mapsto & \pi(a + b)\,, \end{array}$$

y es fácil demostrar que esta suma dota a G/H de estructura de grupo: es asociativa, su elemento neutro es $\pi(0)$ (la clase de equivalencia del cero de G), y dado $a \in G$ el opuesto de la clase $\pi(a) \in G/H$ es $\pi(-a)$. Además, el núcleo de π está formado por los elementos de G que están en la clase de 0, esto es,

$$\operatorname{Ker}\pi = \{a \in G \,:\, a \sim_H 0\} = \{a \in G \,:\, a - 0 = a \in H\} = H\,.$$

La unicidad de la estructura de grupo sobre G/H ya se discutió en B.17. ∎

Lema B.20 *Si G es un grupo abeliano, todo subgrupo H de G es normal y el grupo cociente G/H es también abeliano.*

Demostración. Ejercicio. ∎

Lema B.21 *Sea $f : G \to G'$ un morfismo de grupos. Para todo subgrupo normal H' de G' se satisface que $f^{-1}(H')$ es un subgrupo normal de G. En particular el núcleo de f,* $\operatorname{Ker} f = f^{-1}(0)$*, es un subgrupo normal de G.*

Demostración. Sea H' un subgrupo normal de G'. Según B.14 tenemos que $f^{-1}(H')$ es un subgrupo de G. Dados $a \in G$ y $h \in f^{-1}(H')$, para probar que $f^{-1}(H')$ es normal tenemos que ver que $a + h - a \in f^{-1}(H')$ (véase B.18): como $f(a) \in G'$, $f(h) \in H'$ y H' es normal se satisface $f(a) + f(h) - f(a) \in H'$; pero $f(a) + f(h) - f(a) = f(a + h - a)$ y por lo tanto $a + h - a \in f^{-1}(H')$. ∎

B.22 Sea H un subgrupo de un grupo G. Hemos visto que si H es normal entonces se puede dotar al conjunto G/H de estructura de grupo de modo que la aplicación $\pi : G \to G/H$ de paso al cociente es morfismo de grupos. El recíproco también en cierto: si sobre G/H existe una estructura de grupo para la que π es morfismo de grupos entonces H es normal; en efecto, basta tener en cuenta que H sería el núcleo de π (véase B.21).

Teorema B.23 (Factorización canónica de morfismos de grupos) *Sea $f : G \to G'$ un morfismo de grupos. Existe un único isomorfismo de grupos $\bar{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$ que hace que el cuadrado de morfismos de grupos*

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\operatorname{Ker} f & \xrightarrow{\ \bar{f}\ } & \operatorname{Im} f \end{array}$$

sea conmutativo, es decir, $f = i \circ \bar{f} \circ \pi$ (π es el morfismo de paso al cociente de G a $G/\operatorname{Ker} f$, que es un epimorfismo, e i es la inclusión de $\operatorname{Im} f$ *en G', que es un monomorfismo).*

Demostración. Veamos cómo es en G la relación de equivalencia que el subgrupo $\operatorname{Ker} f$ define: dados $a, b \in G$,

$$a \sim_{\operatorname{Ker} f} b \quad \Longleftrightarrow \quad a - b \in \operatorname{Ker} f \quad \Longleftrightarrow \quad f(a - b) = 0 \quad \Longleftrightarrow \quad f(a) = f(b)\,;$$

es decir, $\sim_{\operatorname{Ker} f}$ es precisamente la relación que la aplicación f define en G (véase A.25). Aplicando la factorización canónica de aplicaciones obtenemos que existe una biyección $\varphi : G/\operatorname{Ker} f \to \operatorname{Im} f$ tal que $f = i \circ \varphi \circ \pi$. Para terminar hay que comprobar que φ es un morfismo de grupos, lo que se deja como ejercicio. ∎

Ejemplos B.24 (a) Sea 0 el subgrupo trivial de un grupo G. Como 0 es un subgrupo normal de G tenemos el grupo cociente $G/0$. Es fácil ver que la relación que el subgrupo 0 define en G es la relación de igualdad entre elementos de G, así que $G = G/0$. De otro modo, el morfismo de paso el cociente $G \to G/0$ es un isomorfismo de grupos.

(b) Sea $a \in \mathbb{Z}$. Tenemos en $\mathbb{Z}$ el subgrupo (a) de los múltiplos enteros de a; además sabemos que todos los subgrupos de $\mathbb{Z}$ son de esa forma (véase el ejemplo (c) de B.8). Como $\mathbb{Z}$ es abeliano todo subgrupo suyo es normal y por tanto tenemos el grupo cociente $\mathbb{Z}/(a)$, el cual se denota $\mathbb{Z}_a$ y se denomina *grupo de las clases de resto módulo a*. Veamos cómo es este

grupo. Supongamos $a > 0$ (si $a < 0$ entonces $(a) = (-a)$, y si $a = 0$ tenemos $(a) = 0$ y por tanto $\mathbb{Z}_a = \mathbb{Z}$). Dados $m, n \in \mathbb{Z}$,

$$m \sim_{(a)} n \qquad \Longleftrightarrow \qquad m - n \in (a) \qquad \Longleftrightarrow \qquad m - n \text{ es múltiplo de } a\,.$$

La relación $\sim_{(a)}$ se denomina *relación de congruencia módulo* a; cuando $m, n \in \mathbb{Z}$ son tales que $m \sim_{(a)} n$ se escribe "$m \equiv n \bmod a$" y se dice que m *es congruente con* n *módulo* a. Si para cada $m \in \mathbb{Z}$ denotamos por $\overline{m}$ la clase de equivalencia de m en $\mathbb{Z}_a$, veamos que se satisface la igualdad

$$\mathbb{Z}_a = \{\overline{0}, \overline{1}, \ldots, \overline{a-1}\}\,,$$

siendo además $\overline{m} \neq \overline{n}$ si $m, n \in \{0, 1, \ldots, a-1\}$. En efecto, dado $m \in \mathbb{Z}$ existen $c, r \in \mathbb{Z}$ tales que $m = ca + r$ y $0 \leq r < a$, de modo que $\overline{m} = \overline{r}$ porque $m - r = ca \in (a)$; es decir, la clase de m es igual a la clase del resto que se obtiene al hacer la división entera de m por a; como los únicos restos posibles son $\{0, 1, \ldots, a-1\}$ concluimos. La suma de $\mathbb{Z}_a$ es la siguiente: dados $\overline{m}, \overline{n} \in \mathbb{Z}_a$,

$$\overline{m} + \overline{n} = \overline{r}$$

donde r es el resto de la división entera de $m + n$ por a.

B.25 (Grupo simétrico) Dado un entero positivo n sea S_n el grupo simétrico de orden n (véase el ejemplo (b) de B.2). Dada una permutación $\sigma \in S_n$ suele escribirse

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix};$$

por ejemplo, si $\sigma \in S_3$ es tal que $\sigma(1) = 3$, $\sigma(2) = 1$ y $\sigma(3) = 2$, entonces escribiremos

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

En el grupo S_n se utiliza notación multiplicativa (véase B.4), por lo que su operación (la "composición" de permutaciones) se denomina "producto". Dicho producto es claro; por ejemplo en S_3 tenemos

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Si $n \geq 2$ podemos definir la aplicación

$$\begin{array}{ccc} S_{n-1} & \to & S_n \\ \sigma & \mapsto & \overline{\sigma}\ , \end{array}$$

donde dada $\sigma \in S_{n-1}$, $\overline{\sigma}$ es la permutación de S_n definida del siguiente modo: $\overline{\sigma}(i) = \sigma(i)$ si $i < n$ y $\overline{\sigma}(n) = n$. Es inmediato comprobar que esta aplicación es un monomorfismo de grupos mediante el cual se identifica S_{n-1} con el subgrupo de S_n formado por las permutaciones de $\{1, \ldots, n\}$ que dejan fijo a n.

Una permutación $\tau \in S_n$ $(n \geq 2)$ se dice que es una *trasposición* si intercambia dos números de $\{1, \ldots, n\}$ y a los demás los deja fijos, es decir, si existen $i, j \in \{1, \ldots, n\}$, $i \neq j$, tales que

$\tau(i) = j$, $\tau(j) = i$ y $\tau(m) = m$ para todo $m \in \{1, \ldots, n\} - \{i, j\}$. Es claro que toda trasposición τ es su propia inversa, esto es $\tau \cdot \tau = 1_n$ (con 1_n denotaremos la permutación identidad de S_n). En S_3 hay $3! = 6$ permutaciones, que son

$$1_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

de ellas τ_1, τ_2, τ_3 son trasposiciones y para el resto se satisfacen

$$\begin{aligned} 1_3 &= \tau_1 \cdot \tau_1 = \tau_2 \cdot \tau_2 = \tau_3 \cdot \tau_3 \,, \\ s_1 &= \tau_3 \cdot \tau_2 = \tau_1 \cdot \tau_3 = \tau_2 \cdot \tau_1 \,, \\ s_2 = s_1^{-1} &= \tau_2 \cdot \tau_3 = \tau_3 \cdot \tau_1 = \tau_1 \cdot \tau_2 \,. \end{aligned}$$

Probaremos en el siguiente teorema que lo que ocurre en S_3 es un hecho general: toda permutación puede ponerse (no de modo único) como producto de trasposiciones.

Teorema B.26 *Sea $n \geq 2$. Toda permutación de S_n es producto de trasposiciones de S_n.*

Demostración. La haremos por inducción en n, siendo trivial para $n = 2$.

Sea $n > 2$ y probemos el teorema para S_n supuesto que es cierto para S_{n-1}. Consideremos una permutación $\sigma \in S_n$. Si $\sigma(n) = n$ entonces $\sigma = \overline{\rho}$ para alguna permutación ρ de S_{n-1}, y aplicando la hipótesis de inducción obtenemos que existen trasposiciones $\tau_1, \ldots, \tau_s$ de S_{n-1} tales que $\rho = \tau_1 \cdot \cdots \cdot \tau_s$, en cuyo caso $\overline{\tau}_1, \ldots, \overline{\tau}_s$ son trasposiciones de S_n tales que $\sigma = \overline{\tau}_1 \cdot \cdots \cdot \overline{\tau}_s$. Si $\sigma(n) \neq n$, sea $m \in \{1, \ldots, n-1\}$ tal que $\sigma(n) = m$ y consideremos la trasposición τ de S_n que intercambia n y m; entonces la permutación $\tau \cdot \sigma$ deja invariante a n y aplicando al caso anterior obtenemos que existen trasposiciones $\tau_1, \ldots, \tau_r$ de S_n tales que $\tau \cdot \sigma = \tau_1 \cdot \cdots \cdot \tau_r$, de modo que $\sigma = \tau \cdot \tau_1 \cdot \cdots \cdot \tau_r$. ∎

B.27 (Signo de una permutación) Sea $n \geq 2$ y sea $\sigma \in S_n$. Dados $i, j \in \{1, \ldots, n\}$, se dice que el par (i, j) *presenta inversión* para la permutación σ si $i < j$ y $\sigma(i) > \sigma(j)$. Por ejemplo, los pares que presentan inversión para la permutación $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix} \in S_5$ son $(1,2)$, $(1,4)$, $(1,5)$, $(2,4)$, $(2,5)$, $(3,4)$ y $(3,5)$.

Consideremos los números enteros Δ y Δ_σ dados por las igualdades

$$\Delta = \prod_{i<j} (j - i) \,, \qquad \Delta_\sigma = \prod_{i<j} (\sigma(j) - \sigma(i))$$

(donde dado un conjunto finito C de números enteros, $\prod_{z \in C} z$ denota el producto de todos ellos); se satisface que Δ y Δ_σ se diferencian a lo sumo en el signo; concretamente tenemos $\Delta_\sigma = (-1)^h \Delta$ donde h es el numero de pares que presentan inversión para σ. El entero $(-1)^h$ se llama *signo* de la permutación σ y se denota $\mathrm{sig}(\sigma)$. Se dice que una permutación es *par* si su signo es igual a 1, y que es *impar* si su signo es igual a -1.

Si consideramos el grupo $\{1,-1\}$ (dotado del producto usual) se satisface que la aplicación

$$\begin{array}{rcl} \mathrm{sig} : S_n & \to & \{1,-1\} \\ \sigma & \mapsto & \mathrm{sig}(\sigma) \end{array}$$

es un morfismo de grupos, es decir, $\mathrm{sig}(\sigma\cdot\rho)=\mathrm{sig}(\sigma)\,\mathrm{sig}(\rho)$. Las trasposiciones presentan una única inversión y por lo tanto son impares; como consecuencia se sigue que $\mathrm{sig}(\sigma)$ es igual a -1 elevado al número de trasposiciones en las que σ se puede poner como producto, es decir, si σ es par entonces puede ponerse como producto de un número par de trasposiciones, y si σ es impar entonces puede ponerse como producto de un número impar de trasposiciones.

Otra consecuencia de que $\mathrm{sig} : S_n \to \{1,-1\}$ sea un morfismo de grupos es que $A_n = \{\sigma \in S_n \,:\, \sigma \text{ es par}\}$ es un subgrupo de S_n (según B.21, $A_n = \mathrm{Ker}(\mathrm{sig})$ es un subgrupo normal de S_n); A_n se denomina *grupo alternado de orden n*.

C Generalidades sobre Teoría de Anillos

C.1 (Anillos) Se llama *anillo* a toda terna $(A,+,\cdot)$ formada por un conjunto A y por dos aplicaciones

$$\begin{array}{rcl} G\times G & \stackrel{+}{\longrightarrow} & G \\ (a,b) & \mapsto & a+b\,, \end{array} \qquad\qquad \begin{array}{rcl} G\times G & \stackrel{\cdot}{\longrightarrow} & G \\ (a,b) & \mapsto & a\cdot b\,, \end{array}$$

llamadas respectivamente *suma* y *producto* del anillo, que cumplen las siguientes propiedades:

(i) $(A,+)$ es un grupo abeliano (véase B.1);

(ii) el producto es asociativo: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ cualesquiera que sean $a,b,c\in A$;

(iii) existe un elemento en A, llamado *unidad* y denotado por 1, tal que $a\cdot 1 = 1\cdot a = a$ para todo $a\in A$; dicha unidad es única;

(iv) el producto es distributivo respecto de la suma: cualesquiera que sean $a,b,c\in A$ se satisfacen $a\cdot(b+c) = a\cdot b + a\cdot c$, $(a+b)\cdot c = a\cdot c + b\cdot c$.

Se dice que un anillo es *conmutativo* si su producto es conmutativo.

Sea $(A,+,\cdot)$ un anillo. De acuerdo con la propiedad distributiva, para cada $a\in A$ la aplicacación $A\to A$, $b\mapsto a\cdot b$, es un morfismo de grupos respecto de la suma, así que en todo anillo A se satisfacen las siguientes reglas de cálculo (véase B.10):

$$a\cdot 0 = 0\,, \qquad a\cdot(-b) = -(a\cdot b) = (-a)\cdot b\,, \qquad (-a)\cdot(-b) = a\cdot b\,.$$

Un elemento $a\in A$ se dice que es *invertible* si existe $b\in A$ tal que $a\cdot b = b\cdot a = 1$, en cuyo caso tal elemento b es único y se denota a^{-1}. Los elementos invertibles del anillo A forman un grupo respecto del producto, grupo que se denota A^* y se denomina *grupo multiplicativo* del anillo A. Diremos que el anillo A es un *cuerpo* si $A\neq 0$ y todo elemento nulo de A es invertible, esto es, $A^* = A - \{0\}$. Un elemento de A se dice que es *propio* si es no nulo y no invertible.

Notas **C.2** (a) A veces en la definición de anillo no se pide la existencia de unidad; en ese caso, cuando un anillo tiene unidad se dice de él que es un *anillo unitario*.

(b) En adelante, en lugar de decir "Sea $(A,+,\cdot\,)$ un anillo ..." diremos simplemente "Sea A un anillo ...", entendiendo que A está dotado de su suma y de su producto.

(c) Dados elementos a,b de un anillo A, escribiremos a veces "ab" en lugar de "$a\cdot b$". Además, cuando a es invertible y A es conmutativo los elementos $a^{-1}b$ y ba^{-1} son iguales y suelen denotarse $\dfrac{b}{a}$ ó b/a.

Ejemplos C.3 (a) Los números enteros con su suma y su producto, $(\mathbb{Z},+,\cdot\,)$, tienen estructura de anillo conmutativo (véase A.23); $\mathbb{Z}$ no es cuerpo porque $\mathbb{Z}^*=\{-1,1\}$.

(b) Dado $a\in\mathbb{Z}$, $a\neq 0$, el grupo cociente $\mathbb{Z}_a$ puede ser dotado de estructura de anillo conmutativo mediante el producto siguiente (véase B.24 (b)): dados $\overline{m},\overline{n}\in\mathbb{Z}_a$,

$$\overline{m}\cdot\overline{n}:=\overline{r}$$

donde r es el resto de la división entera de mn por a.

(c) **(Cuerpo de los números racionales)** Veamos la construcción de los números fraccionarios a partir del anillo $\mathbb{Z}$ de los números enteros. Sea $S=\mathbb{Z}-\{0\}$ el conjunto de los enteros no nulos y consideremos sobre el conjunto $\mathbb{Z}\times S$ la siguiente relación: dados $(z,s),(z',s')\in\mathbb{Z}\times S$,

$$(z,s)\sim(z',s') \qquad :\Longleftrightarrow \qquad zs'=z's\,;$$

es fácil ver que la anterior es una relación de equivalencia. Se define el conjunto $\mathbb{Q}$ de los *números racionales* como el conjunto cociente $\mathbb{Z}\times S/\!\sim$; el número racional que define un par $(z,s)\in\mathbb{Z}\times S$ se denota $\dfrac{z}{s}$ (ó también z/s) y se dice que es el *cociente* de los números enteros z y s; con esta notación tenemos

$$\mathbb{Q}=\left\{\frac{z}{s}\,:\,z,s\in\mathbb{Z}\,,\ s\neq 0\right\}.$$

Dados $z/s,z'/s'\in\mathbb{Q}$ definimos la suma $(z/s)+(z'/s')$ y el producto $(z/s)\cdot(z'/s')$ por las igualdades

$$\frac{z}{s}+\frac{z'}{s'}:=\frac{zs'+z's}{ss'}\,,\qquad\qquad \frac{z}{s}\cdot\frac{z'}{s'}:=\frac{zz'}{ss'}\,,$$

y diremos que z/s es *positivo* cuando los enteros z y s sean ambos positivos ó negativos; diremos que $z/s\leq z'/s'$ cuando $z/s=z'/s'$ ó cuando $(z'/s')-(z/s)=(z's-zs')/ss'$ sea positivo. Una comprobación estandar prueba que las anteriores definiciones no dependen de los representantes elegidos en cada clase de equivalencia.

De las propiedades de los números enteros se deducen sin dificultad las propiedades de la suma, el producto y la ordenación de los números racionales (véase A.23), satisfaciéndose que $(\mathbb{Q},\leq)$ está totalmente ordenado y que $(\mathbb{Q},+,\cdot\,)$ es un cuerpo conmutativo (el cero de $\mathbb{Q}$ es $0/1=0/s$ con s entero no nulo cualquiera, el opuesto de un número racional z/s es $(-z)/s$, el uno de $\mathbb{Q}$ es $1/1=s/s$ con s entero no nulo cualquiera, y dado z/s con $z\neq 0$ su inverso es s/z).

Cada número entero z define el número racional $z/1$, de modo que tenemos la aplicación natural $\mathbb{Z}\to\mathbb{Q}$, $z\mapsto z/1$, que es inyectiva y permite considerar a $\mathbb{Z}$ como un subconjunto de $\mathbb{Q}$; la suma, el producto y la ordenación de números racionales coincide en $\mathbb{Z}$ con la suma, el producto y la ordenación de números enteros.

(d) **(Cuerpo de los números reales)** Sea $(q_n)_{n\in\mathbb{N}}$ una sucesión de números racionales. Se dice que $(q_n)_{n\in\mathbb{N}}$ es una *sucesión de Cuachy* si para cada racional positivo ε existe un natural ν tal que $|q_n - q_m| < \varepsilon$ siempre que $n, m \geq \nu$. Se dice que la sucesión $(q_n)_{n\in\mathbb{N}}$ *converge* a cero si para cada racional positivo ε existe un natural ν tal que $|q_n| < \varepsilon$ siempre que $n \geq \nu$. Sea $\mathcal{C}$ el conjunto de todas las sucesiones de Cuachy de números racionales.

En el curso de Análisis Matemático se construye el conjunto $\mathbb{R}$ de los *números reales* como el conjunto cociente de $\mathcal{C}$ por la relación de equivalencia

$$(a_n) \sim (b_n) \qquad :\Longleftrightarrow \qquad (a_n - b_n) \text{ converge a cero}\,.$$

Se definen la suma y el producto de números reales y una ordenación total de $\mathbb{R}$, y se prueba que $(\mathbb{R}, +, \cdot\,)$ es un cuerpo conmutativo. Cada número racional q define el número real "clase de equivalencia de la sucesión $(q, q, \dots)$", que se denota también q, obteniéndose así una aplicación inyectiva natural $\mathbb{Q} \to \mathbb{R}$ que permite identificar $\mathbb{Q}$ con un subconjunto de $\mathbb{R}$; la suma, el producto y la ordenación de números reales coincide en $\mathbb{Q}$ con la suma, el producto y la ordenación de números racionales.

También se prueba en el curso de Análisis la siguiente importante propiedad: dado un número real no negativo c (esto es, $c \geq 0$), para cada entero positivo n existe un único número real no negativo cuya potencia n-ésima es c, número real que denotaremos $\sqrt[n]{c}$ (cuando $n = 2$ se escribe simplemente $\sqrt{c}\,$).

(e) **(Cuerpo de los números complejos)** Se define el conjunto $\mathbb{C}$ de los *números complejos* como el conjunto de pares ordenados de números reales,

$$\mathbb{C} = \{a + b\,\mathrm{i} \,:\, a, b \in \mathbb{R}\}\,.$$

Dados $a + b\,\mathrm{i}, c + d\,\mathrm{i} \in \mathbb{C}$ definimos la suma $(a + b\,\mathrm{i}) + (c + d\,\mathrm{i})$ y el producto $(a + b\,\mathrm{i}) \cdot (c + d\,\mathrm{i})$ por las igualdades

$$(a + b\,\mathrm{i}) + (c + d\,\mathrm{i}) := (a + c) + (b + d)\,\mathrm{i}\,, \qquad (a + b\,\mathrm{i}) \cdot (c + d\,\mathrm{i}) := (ac - bd) + (ad + bc)\,\mathrm{i}\,.$$

De las anteriores definiciones y de las propiedades de los números reales se deducen sin dificultad las propiedades de la suma y el producto de los números complejos, satisfaciéndose que $(\mathbb{C}, +, \cdot\,)$ es un cuerpo conmutativo. Cada número real x define el número complejo $x + 0\,\mathrm{i}$, que se denota también x, obteniéndose así una aplicación inyectiva natural $\mathbb{R} \to \mathbb{C}$ que permite identificar $\mathbb{R}$ con un subconjunto de $\mathbb{C}$; la suma y el producto de números complejos coincide en $\mathbb{R}$ con la suma y el producto de números reales.

Sea $z = a + b\,\mathrm{i}$ un número complejo. Diremos que los números reales a y b son, respectivamente, la *parte real* y la *parte imaginaria* de z, que $\overline{z} := a - b\,\mathrm{i}$ es el número complejo *conjugado* de z, y que el número real no negativo $|z| := \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}$ es el *módulo* de z; son inmediatas la equivalencia "$|z| = 0 \;\Leftrightarrow\; z = 0$", las igualdades $\overline{\overline{z}} = z$ y $|\overline{z}| = |z|$, y que si $z \neq 0$ entonces $z^{-1} = \overline{z}/|z|^2$.

Para terminar diremos que dados números complejos z_1, z_2 se satisfacen

$$\overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2\,, \qquad \overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2\,,$$

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|\,, \qquad |z_1 + z_2| \leq |z_1| + |z_2|\,.$$

(f) Sean X un conjunto no vacío y A un anillo. El conjunto $\mathcal{F}(X,A)$ de todas las aplicaciones de X en A puede ser dotado de estructura de anillo mediante la suma y el producto definidos como sigue: si $f,g\in\mathcal{F}(X,A)$, $f+g$ es la aplicación de X en A dada por la igualdad $(f+g)(x):=f(x)+g(x)$ $(x\in X)$, y $f\cdot g$ es la aplicación de X en A dada por la igualdad $(f\cdot g)(x):=f(x)g(x)$ $(x\in X)$. Si A es conmutativo entonces $\mathcal{F}(X,A)$ también es conmutativo.

(g) Sea G un grupo abeliano. El conjunto $\mathrm{End}_{\mathrm{gr}}(G)$ de todos los morfismos de grupos de G en G (esto es, de los endomorfismos del grupo G) puede ser dotado de estructura de anillo mediante la suma y el producto definidos como sigue: si $f,g\in\mathrm{End}_{\mathrm{gr}}(G)$, $f\cdot g:=f\circ g$ y $f+g$ es el endomorfismo de G dado por la igualdad $(f+g)(a):=f(a)+g(a)$ $(a\in G)$. Si $\mathrm{Aut}_{\mathrm{gr}}(G)$ denota el conjunto de todos los automorfismos del grupo G entonces $(\mathrm{End}_{\mathrm{gr}}(G))^*=\mathrm{Aut}_{\mathrm{gr}}(G)$.

(h) **(Anillos de polinomios)** Sea A un anillo. Se llaman *polinomios en una variable con coeficientes en* A a las aplicaciones $P:\mathbb{N}\to A$ que son casi nulas, esto es, para las que existe $n_0\in\mathbb{N}$ tal que $P(n)=0$ si $n>n_0$.

Sea P un polinomio. Los elementos del conjunto $\{P(n)\}_{n\in\mathbb{N}}\subseteq A$ se denominan *coeficientes* del polinomio P. Se llama polinomio *cero* (ó *nulo*) al que tiene todos sus coeficientes iguales a cero, y si P es un polinomio no nulo se llama *grado* de P al mayor número natural $n\in\mathbb{N}$ tal que $P(n)\neq 0$, y se denota $\mathrm{gr}\,P$. Convenimos en que el grado del polinomio nulo es igual a -1.

Se comprueba fácilmente que la suma y el producto de polinomios definidos por las igualdades

$$(P+Q)(n):=P(n)+Q(n)\qquad\qquad (P\cdot Q)(n):=\sum_{i+j=n}P(i)Q(j)$$

($n\in\mathbb{N}$, P,Q polinomios) dotan al conjunto de los polinomios con coeficientes en A de estructura de anillo, que es conmutativo si lo es A.

Veamos ahora cómo se representan los polinomios con coeficientes en A. Cada elemento $a\in A$ define un polinomio llamado *polinomio constante* a, y es aquel cuyos coeficientes son todos nulos excepto el 0-ésimo que vale a, esto es,

$$a(n)=\begin{cases}a & \text{si } n=0\,,\\ 0 & \text{si } n\neq 0\,.\end{cases}$$

Sea x el polinomio definido como

$$x(n)=\begin{cases}1 & \text{si } n=1\,,\\ 0 & \text{si } n\neq 1\,.\end{cases}$$

Se observa entonces que $x^m=x\cdot\overset{m}{\ldots}\cdot x$ $(m>0)$ es el polinomio dado por

$$x^m(n)=\begin{cases}1 & \text{si } n=m\,,\\ 0 & \text{si } n\neq m\,,\end{cases}$$

y si $P:\mathbb{N}\to A$ es un polinomio de grado n y $a_m=P(m)$ $(m\leq n)$ son sus coeficientes (no nulos), entonces se satisface la igualdad

$$P=a_0+a_1\cdot x+\cdots+a_n\cdot x^n\,,$$

que es la representación usual (y la que utilizaremos en adelante) de los polinomios en una variable con coeficientes en A.

El anillo de los polinomios en una variable con coeficientes en A se denota $A[x]$, y sus elementos se denotan "$P(x)$". Dados $P(x), Q(x) \in A[x]$ es fácil probar que se satisfacen

$$\operatorname{gr} P(x) = 0 \iff P(x) \text{ es un polinomio constante no nulo}\,,$$
$$\operatorname{gr}(P(x)+Q(x)) \le \max\{\operatorname{gr} P(x), \operatorname{gr} Q(x)\}\,, \qquad \operatorname{gr}(P(x)Q(x)) \le \operatorname{gr} P(x) + \operatorname{gr} Q(x)\,.$$

Además, si $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $Q(x) = b_0 + b_1 x + \cdots + b_m x^m$, entonces

$$P(x) + Q(x) = \sum_{i\ge 0} (a_i + b_i) x^i\,, \qquad P(x)Q(x) = \sum_{i\ge 0} \Big(\sum_{l+h=i} a_l b_h \Big) x^i\,.$$

De modo recurrente se definen los anillos de polinomios en varias variables con coeficientes en A; así, el anillo de polinomios en dos variables con coeficientes en A se denota $A[x,y]$ y se define como el anillo $A[x][y]$ de los polinomios en una variable con coeficientes en $A[x]$. En general, $A[x_1,\ldots,x_n] := A[x_1,\ldots,x_{n-1}][x_n]$.

(i) Dados anillo A y B, el producto cartesiano $A \times B$ se puede dotar de estructura de anillo mediante la suma y el producto definidos como sigue: dados $(a,b),(a',b') \in A \times B$,

$$(a,b) + (a',b') := (a+a', b+b')\,, \qquad (a,b)\cdot(a',b') := (aa', bb')\,.$$

El anillo $A \times B$ es conmutativo si y sólo si los anillos A y B son conmutativos. Puesto que la unidad de $A \times B$ es $(1,1)$ se satisface la igualdad $(A \times B)^* = A^* \times B^*$.

C.4 (Subanillos) Sea A un anillo y sea B un subconjunto de A. Se dice que B es un *subanillo* de A si satisface:

(i) B es subgrupo del grupo aditivo $(A,+)$ (véase B.6);
(ii) B es cerrado frente al producto de A;
(iii) B contiene al 1 de A.

Si B es un subanillo de A podemos restringir las operaciones de A a B y se satisface que $(B,+,\cdot)$ es también un anillo.

Ejemplos C.5 (a) Los números enteros $\mathbb{Z}$ son un subanillo de los números racionales $\mathbb{Q}$, $\mathbb{Q}$ es un subanillo de $\mathbb{R}$, y $\mathbb{R}$ es un subanillo de $\mathbb{C}$ (véanse los ejemplos (c), (d) y (e) de C.3).

(b) Sea A un anillo y consideremos el anillo $A[x]$ (véase el ejemplo (h) de C.3). Tenemos la aplicación natural $A \to A[x]$, $a \mapsto a$, donde $a \in A[x]$ es el polinomio constante a. Esta aplicación es inyectiva y por tanto nos permite ver A como un subconjunto de $A[x]$; mediante esta identificación se satisface que A es un subanillo de $A[x]$.

(c) Si A es un anillo, A con su suma es un grupo abeliano y tenemos el anillo $\operatorname{End}_{\mathrm{gr}}(A)$ (véase C.3 (g)). Si denotamos por $\operatorname{End}_{\mathrm{an}}(A)$ el conjunto de todos los endomorfismos del anillo A (véase C.6), entonces se satisface que $\operatorname{End}_{\mathrm{an}}(A)$ es un subanillo de $\operatorname{End}_{\mathrm{gr}}(A)$.

C.6 (Morfismos de anillos) Sean A y B anillos. Una aplicación $f : A \to B$ se dice que es un *morfismo de anillos* si es compatible con las operaciones de los anillos y transforma la unidad de A en la unidad de B, es decir, si satisface $f(1) = 1$ y $f(a+b) = f(a) + f(b)$, $f(a\cdot b) = f(a)\cdot f(b)$ cualesquiera que sean $a, b \in A$.

La terminología que se utiliza para los morfismos de anillos es la misma que para los morfismos de grupos (véase B.9); así tenemos monomorfismos, epimorfismos e isomorfismos de anillos, y endomorfismos y automorfismos de un anillo. Un morfismo de anillos es en particular un morfismo de grupos aditivos y por lo tanto satisface las propiedades de B.10, a las que hay que añadir: si $f : A \to B$ es un morfismo de anillos y $a \in A^*$, entonces $f(a) \in B^*$ y $f(a^{-1}) = (f(a))^{-1}$. Es inmediato comprobar que la composición de morfismos de anillos es un morfismo de anillos. Por último, se satisface que si un morfismo de anillos es un isomorfismo (es decir, es biyectivo), entonces su aplicación inversa también es morfismo de anillos (y por lo tanto también es un isomorfismo). (Véase B.12 y su demostración.)

Ejemplos C.7 (a) Si B es un subanillo de un anillo A, entonces B es un anillo y la inclusión $B \hookrightarrow A$ es un monomorfismo de anillos cuya imagen es B.

(b) Sea $A[x]$ el anillo de polinomios en una variable con coeficientes en un anillo A. Cada polinomio $P(x) = a_0 + a_1 x + \cdot + a_n x^n \in A[x]$ define la aplicación $A \to A$ que a cada elemento $a \in A$ le asigna $P(a) = a_0 + a_1 a + \cdot + a_n a^n \in A$; en particular, fijado $a_0 \in A$ tenemos la aplicación "tomar valor en a_0" que está definida como

$$\begin{array}{rcl} A[x] & \to & A \\ P(x) & \mapsto & P(a_0)\,; \end{array}$$

se satisface que la anterior aplicación es un epimorfismo de anillos.

(c) **(Característica de un anillo)** Para cada anillo A existe un morfismo natural de anillos $\mathrm{ch} : \mathbb{Z} \to A$ definido del siguiente modo: dado $z \in \mathbb{Z}$,

$$\mathrm{ch}(z) := z \cdot 1 = \begin{cases} 1 + \overset{z}{\ldots} + 1 & \text{si } z > 0\,, \\ 0 & \text{si } z = 0\,, \\ (-1) + \overset{|z|}{\ldots} + (-1) & \text{si } z < 0\,. \end{cases}$$

El núcleo de dicho morfismo, $\mathrm{ch}^{-1}(0)$, es un subgrupo del grupo aditivo $(\mathbb{Z}, +)$ y por lo tanto existe un único $p \in \mathbb{Z}$, $p \geq 0$, tal que $\mathrm{ch}^{-1}(0) = (p)$ (véase B.8 (c)); este entero no negativo p se denomina *característica* del anillo A y se denota $\mathrm{ch}\, A$.

Que la característica de un anillo A sea cero significa que para todo $z \in \mathbb{Z}$ se tiene $z \cdot 1 \neq 0$. Si la característica de un anillo A es $p > 0$ entonces para todo $a \in A$ se satisface $a + \overset{p}{\ldots} + a = p \cdot a = 0$; además p es el menor entero positivo que tiene la anterior propiedad (pues el menor entero positivo de (p) es p).

Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica 0; dado un entero positivo p, el anillo $\mathbb{Z}_p$ tiene caracterísrica p (véase C.3 (b)); para cada anillo A se satisface $\mathrm{ch}\, A[x] = \mathrm{ch}\, A$.

(d) Dados anillos A y B consideremos el anillo producto $A \times B$ (véase C.3 (i)). La estructura de anillo de $A \times B$ es la única que se puede definir sobre el conjunto producto cartesiano $A \times B$ de modo que las proyecciones sobre los anillos factores son morfismos de anillos (véase B.15).

C.8 (Ideales, anillo cociente) Sea A un anillo y sea B un subgrupo del grupo aditivo $(A, +)$. En A tenemos la relación de equivalencia que define B: dados $a, a' \in A$, $a \sim a'$ cuando existe $b \in B$ tal que $a = a' + b$. Como $(A, +)$ es conmutativo, B es un subgrupo normal y por lo tanto podemos dotar el conjunto cociente A/B de estructura de grupo abeliano

de manera que el morfismo de paso al cociente $\pi : A \to A/B$ es un morfismo de grupos (véase B.17). La suma de A/B es la dada por la igualdad $\pi(a) + \pi(a') = \pi(a + a')$.

El problema que nos planteamos ahora es definir un producto en A/B de manera que A/B quede dotado de estructura de anillo y que el morfismo de grupos aditivos $\pi : A \to A/B$ sea también un morfismo de anillos. Como ocurría en el problema del grupo cociente, si este problema tiene solución entonces es única, pues debe satisfacerse $\pi(a) \cdot \pi(a') = \pi(a \cdot a')$ cualesquiera que sean $a, a' \in A$, lo que determina el producto de A/B. Ahora bien, para que tal producto esté bien definido es necesario que no dependa de los representantes elegidos en las clases de equivalencia, es decir, que si $\pi(a) = \pi(\bar{a})$ y $\pi(a') = \pi(\bar{a}')$ entonces $\pi(a \cdot a') = \pi(\bar{a} \cdot \bar{a}')$. Veamos si esto es cierto: supueto que $\pi(a) = \pi(\bar{a})$ y $\pi(a') = \pi(\bar{a}')$, existen $b, \bar{b} \in B$ tales que $a = a' + b$ y $\bar{a} = \bar{a}' + \bar{b}$ y por tanto

$$a \cdot \bar{a} = (a' + b) \cdot (\bar{a}' + \bar{b}) = a' \cdot \bar{a}' + a' \cdot \bar{b} + b \cdot \bar{a}' + b \cdot \bar{b}\,;$$

de la anterior igualdad no se deduce, en general, que existe $c \in B$ tal que $a \cdot \bar{a} = a' \cdot \bar{a}' + c$ (con lo que sería $\pi(a \cdot \bar{a}) = \pi(a' \cdot \bar{a}')$). Por lo tanto el problema de dotar a A/B de estructura de anillo de modo que $\pi : A \to A/B$ sea un morfismo de anillo no siempre tiene solución. Los subgrupos para los que sí existe solución se denominan "ideales".

Llamaremos *ideal* del anillo A a todo subgrupo aditivo I de A que satisfaga: $a \cdot b \in I$, $b \cdot a \in I$ cualesquiera que sean $a \in A$, $b \in I$. Por ejemplo, 0 y A son ideales de A.

De la discusión anterior se sigue que si I es un ideal de A entonces sobre el conjunto cociente A/I existe una única estructura de anillo para la cual $\pi : A \to A/I$ es morfismo de anillos (el uno de A/I es $\pi(1)$). El anillo A/I se denomina *anillo cociente* de A por el ideal I. Si A es conmutativo entonces también lo es A/I.

Proposición C.9 *Sea $f : A \to A'$ un morfismo de anillos.*

(i) *Si I' es un ideal de A' entonces $f^{-1}(I')$ es un ideal de A; en particular el núcleo de f, $\operatorname{Ker} f = f^{-1}(0)$, es un ideal de A.*

(ii) *Si B es un subanillo de A entonces $f(B)$ es un subanillo de A'; en particular la imagen de f, $\operatorname{Im} f = f(A)$, es un subanillo de A'.*

(iii) *Si I es un ideal de A y el morfismo f es epiyectivo, entonces $f(I)$ es un ideal de A'.*

Demostración. Son sencillas y se dejan como ejercicio. ∎

Teorema C.10 (Factorización canónica de morfismos de anillos) *Sea $f : A \to A'$ un morfismo de anillos. Existe un único isomorfismo de anillos $\bar{f} : A/\operatorname{Ker} f \to \operatorname{Im} f$ que hace conmutativo el siguiente cuadrado de morfismos de anillos*

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & A' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ A/\operatorname{Ker} f & \xrightarrow{\ \bar{f}\ } & \operatorname{Im} f\,. \end{array}$$

Demostración. Ejercicio (véase B.23 y su demostración). ∎

Ejemplos C.11 (a) Sea A un anillo y sea I un ideal de A. Se dice que I es *propio* si es distinto de A. Es fácil comprobar que se satisface: $I = A \Leftrightarrow A/I = 0$. También es fácil demostrar que si algún elemento de I es invertible entonces $I = A$. Como consecuencia de la última afirmación se obtienen: (i) A es un cuerpo si y sólo si el conjunto {ideales de A} tiene exactamente dos elementos, 0 y A (véase C.1); (ii) todo morfismo de anillos entre cuerpos es inyectivo (véase C.9 (i)).

(b) Sea A un anillo conmutativo. Para cada elemento $a \in A$ tenemos el conjunto $(a) := \{ab : b \in A\}$, que es un ideal de A denominado *ideal generado* por a. Es claro que se satisface $(a) = A$ si y sólo si a es invertible; de otro modo, si $a \neq 0$ entonces: a es un elemento propio de A (esto es, a no es invertible) si y sólo si (a) es un ideal propio de A.

Por ejemplo, para cada $a \in \mathbb{Z}$ el subgrupo (a) es el ideal generado por a (nótese que el producto del anillo cociente $\mathbb{Z}/(a) = \mathbb{Z}_a$ es justamente el producto definido en C.3 (b)). Además todo ideal de $\mathbb{Z}$ es de la forma (a) con $a \in \mathbb{Z}$, ya que si I es un ideal de $\mathbb{Z}$ entonces I es un subgrupo aditivo de $\mathbb{Z}$ (véase B.8 (c)).

(c) Sea $\alpha \in \mathbb{R}$ y consideremos la aplicación $\mathbb{R}[x] \to \mathbb{R}$, $P(x) \mapsto P(\alpha)$, que es un epimorfismo de anillos (véase C.7 (b)). Probemos que su núcleo es el ideal $(x - \alpha)$: sea $Q(x) \in \mathbb{R}[x]$ tal que $Q(\alpha) = 0$, y sean $C(x) \in \mathbb{R}[x]$ y $R \in \mathbb{R}$ tales que $Q(x) = C(x)(x - \alpha) + R$ (véase D.3 más adelante); entonces $0 = Q(\alpha) = R$ y concluimos que $Q(x) = C(x)(x - \alpha) \in (x - \alpha)$. Aplicando el teorema de factorización canónica C.10 obtenemos un isomorfismo de anillos $\mathbb{R}[x]/(x - \alpha) \xrightarrow{\sim} \mathbb{R}$.

(d) Consideremos la aplicación $\mathbb{R}[x] \to \mathbb{C}$, $P(x) \mapsto P(\mathrm{i})$, que es un epimorfismo de anillos. Veamos que su núcleo es el ideal $(x^2 + 1)$: sea $Q(x)$ un polinomio tal que $Q(\mathrm{i}) = 0$ y sean $C(x) \in \mathbb{R}[x]$ y $c, d \in \mathbb{R}$ tales que $Q(x) = C(x)(x^2 + 1) + (cx + d)$; entonces $0 = Q(\mathrm{i}) = C(\mathrm{i})(-1+1) + (c\,\mathrm{i} + d) = c\,\mathrm{i} + d$ y por tanto $c = d = 0$, es decir, $Q(x) = C(x)(x^2+1) \in (x^2+1)$.

Aplicando el teorema C.10 obtenemos un isomorfismo de anillos $\mathbb{R}[x]/(x^2 + 1) \xrightarrow{\sim} \mathbb{C}$. Como consecuencia, puede tomarse $\mathbb{R}[x]/(x^2 + 1)$ como definición alternativa del anillo $\mathbb{C}$ de los números complejos. Cuando se hace así, el número complejo i, que ha de ser un elemento del cociente $\mathbb{R}[x]/(x^2 + 1)$, es la imagen $\pi(x)$ de x por el morfismo de paso al cociente $\pi : \mathbb{R} \to \mathbb{R}[x]/(x^2 + 1)$, que verifica $\pi(x)^2 = \pi(x^2) = -1$ (pues $\pi(x^2) + 1 = \pi(x^2 + 1) = 0$).

(e) Consideremos la aplicación $\mathbb{R}[x, y] \to \mathbb{R}[x]$, $P(x, y) \mapsto P(x, 0) \in \mathbb{R}[x]$ (véase C.3 (h)), que es un epimorfismo de anillos. Veamos que su núcleo es el ideal (y) generado por el polinomio y: sea $P(x, y)$ un polinomio del núcleo y escribámoslo como un polinomio en y con coeficientes en $\mathbb{R}[x]$, $P(x, y) = R_0(x) + R_1(x) \cdot y + \cdot + R_n(x) \cdot y^n$ $(R_i(x) \in \mathbb{R}[x],\ i = 0, \ldots, n)$; entonces $0 = P(x, 0) = R_0(x)$ y por lo tanto $P(x, y) = (R_1(x) + R_2(x) \cdot y + \cdot + R_n(x) \cdot y^{n-1}) \cdot y \in (y)$. Aplicando el teorema C.10 obtenemos un isomorfismo de anillos $\mathbb{R}[x, y]/(y) \xrightarrow{\sim} \mathbb{R}[x]$.

(f) Sean I, J ideales de un anillo conmutativo A. La intersección $I \cap J$, la suma $I + J = \{a + b : a \in I,\ b \in J\}$ y el producto $I \cdot J := \{a_1 \cdot b_1 + \cdots + a_n \cdot b_n : a_i \in I,\ b_i \in J\}$ son ideales de A. La unión de ideales no es, en general, un ideal. Es claro que $I \cdot J \subseteq I \cap J$.

El conjunto de los ideales de A dotado con el orden definido por la inclusión es un retículo con primer elemento (el ideal 0) y último elemento (el ideal A); dados ideales I, J tenemos $\inf\{I, J\} = I \cap J$ y $\sup\{I, J\} = I + J$.

Teorema C.12 *Sea I un ideal de un anillo A. El morfismo de anillos de paso al cociente $\pi : A \to A/I$ induce una correspondencia biyectiva entre los ideales de A/I y los ideales de A que contienen a I. Dicha correspondencia es un isomorfismo de conjuntos ordenados (véase*

A.17).

Demostración. Por una parte tenemos la aplicación "tomar imagen directa por π" restringida al conjunto de los ideales de A que contienen a I (véase C.9 (iii)),

$$\begin{array}{ccc} \left[\begin{array}{c}\text{ideales de } A\\ \text{que contienen a } I\end{array}\right] & \longrightarrow & \left[\begin{array}{c}\text{ideales de } A/I\end{array}\right] \\ J & \longmapsto & \pi(J)\ . \end{array}$$

Por otra parte, si $\bar{J}$ es un ideal de A/I entonces $\pi^{-1}(\bar{J})$ es un ideal de A que contiene a I, ya que $\pi(I) = 0 \in \bar{J}$ (véase C.9 (i)); por lo tanto la aplicación "tomar imagen inversa por π" valora en el conjunto de los ideales de A que contienen a I y tenemos la aplicación

$$\begin{array}{ccc} \left[\begin{array}{c}\text{ideales de } A/I\end{array}\right] & \longrightarrow & \left[\begin{array}{c}\text{ideales de } A\\ \text{que contienen a } I\end{array}\right] \\ \bar{J} & \longmapsto & \pi^{-1}(\bar{J})\ . \end{array}$$

Ya sabemos que estas dos aplicaciones conservan el orden (véase A.18), y es fácil demostrar que son biyectivas porque son una la inversa de la otra. ∎

D Divisibilidad

En esta sección todos los anillos que se consideren serán conmutativos.

D.1 (Anillos íntegros) Sea A un anillo. Dados $a, b \in A$, se dice que a *divide* a b (ó que b es *múltiplo* de a) si existe $c \in A$ tal que $b = ac$, es decir, si $b \in (a)$. Un elemento $a \in A$ se dice que es un *divisor de cero* si $a \neq 0$ y existe $b \in A$, $b \neq 0$, tal que $ab = 0$.

Se llama *anillo íntegro* (ó *dominio de integridad*) a todo anillo $A \neq 0$ que carezca de divisores de cero, esto es, en el que se satisfaga: $a, b \in A,\ ab = 0 \Rightarrow a = 0$ ó $b = 0$.

Ejemplos D.2 (a) Todo cuerpo es un anillo íntegro (compruébese); por lo tanto $\mathbb{R}$, $\mathbb{Q}$ y $\mathbb{C}$ son anillos íntegros. El anillo $\mathbb{Z}$ también es íntegro.

(b) El anillo $\mathbb{Z}_4$ no es íntegro: si $\pi : \mathbb{Z} \to \mathbb{Z}_4$ es el morfismo de paso al cociente, entonces $\pi(2) \neq 0$ (porque $2 \notin (4)$) y $\pi(2)\pi(2) = \pi(2 \cdot 2) = \pi(4) = 0$ (porque $4 \in (4)$).

(c) Sea A un anillo íntegro. El anillo de polinomios $A[x]$ es también íntegro. Es una consecuencia inmediata de la siguiente propiedad fácil de demostrar: si $P(x), Q(x) \in A[x]$ son polinomios no nulos entonces $\operatorname{gr}(P(x)Q(x)) = \operatorname{gr} P(x) + \operatorname{gr} Q(x)$ (véase C.3 (h)).

Otra consecuencia de la anterior igualdad es que "los elementos invertibles de $A[x]$ son los polinomios constantes definidos por elementos invertibles de A"; es decir, considerando A como un subanillo de $A[x]$ se satisface $A[x]^* = A^*$.

(d) De (a) y (c) se sigue que para todo cuerpo k el anillo $k[x]$ es íntegro.

Teorema D.3 (División de polinomios) *Sea k un cuerpo y sea $P(x) \in k[x]$, $P(x) \neq 0$. Para cada polinomio $Q(x) \in k[x]$ existe una única pareja de polinomios $C(x), R(x) \in k[x]$ (llamados respectivamente* cociente *y* resto *de la* división *de $Q(x)$ por $P(x)$) tal que*

$$Q(x) = C(x)P(x) + R(x)\,, \qquad -1 \leq \operatorname{gr} R(x) < \operatorname{gr} P(x)\,.$$

Demostración. Veamos primero la existencia. Si $-1 \leq \operatorname{gr} Q(x) < \operatorname{gr} P(x)$ entonces $C(x) = 0$ y $R(x) = Q(x)$, así que podemos suponer que $\operatorname{gr} Q(x) \geq \operatorname{gr} P(x)$, en cuyo caso procedemos por inducción en $d = \operatorname{gr} Q(x)$.

Si $d = 0$ debe ser $\operatorname{gr} P(x) = 0$ y por lo tanto existe $\alpha \in k$, $\alpha \neq 0$, tal que $P(x) = \alpha$; como k es un cuerpo, α es invertible y podemos tomar $C(x) = \alpha^{-1}Q(x)$ y $R(x) = 0$.

Sea $d \geq 1$ y supongamos que el enunciado es cierto para los polinomios de grado menor que d. Si $n = \operatorname{gr} P(x) \leq \operatorname{gr} Q(x) = d$ entonces

$$P(x) = a_0 + a_1x + \cdots + a_nx^n\,, \qquad Q(x) = b_0 + b_1x + \cdots + b_dx^d$$

con a_n y b_d no nulos; como el polinomio $\bar{Q}(x) = Q(x) - b_da_n^{-1}x^{d-n}P(x)$ tiene grado menor que d, aplicando la hipótesis de inducción obtenemos que existen $\bar{C}(x), R(x) \in k[x]$ tales que

$$\bar{Q}(x) = \bar{C}(x)P(x) + R(x)\,, \qquad -1 \leq \operatorname{gr} R(x) < \operatorname{gr} P(x)\,;$$

luego $Q(x) = (b_da_n^{-1}x^{d-n} + \bar{C}(x))P(x) + R(x)$ y terminamos.

Veamos la unicidad. Supongamos que existen otros polinomios $\bar{C}(x), \bar{R}(x) \in k[x]$ tales que $Q(x) = \bar{C}(x)P(x) + \bar{R}(x)$ y $-1 \leq \operatorname{gr} \bar{R}(x) < \operatorname{gr} P(x)$, en cuyo caso $P(x)(\bar{C}(x) - C(x)) = R(x) - \bar{R}(x)$. Entonces $R(x) - \bar{R}(x)$ es un multiplo de $P(x)$ que tiene grado menor que $\operatorname{gr} P(x)$, de modo que debe ser $R(x) - \bar{R}(x) = 0$ (véase D.2 (c)). Como consecuencia $P(x)(\bar{C}(x) - C(x)) = 0$, y como $k[x]$ es íntegro concluimos que $\bar{C}(x) - C(x) = 0$. ∎

D.4 (Ideales primos, ideales maximales) Sea I un ideal de un anillo A. Se dice que I es *primo* cuando es propio y satisface la siguiente propiedad: si $a, b \in A$ son tales que $ab \in I$, entonces $a \in I$ ó $b \in I$. Se dice que I es *maximal* cuando es propio y no está contenido en más ideales que él mismo y el total.

Teorema D.5 *Sea I un ideal propio de un anillo A. La condición necesaria y suficiente para que I sea primo es que A/I sea un anillo íntegro.*

Demostración. Nótese que $A/I \neq 0$ porque $I \neq A$. Sea $\pi : A \to A/I$ el morfismo de paso al cociente. La condición para que I sea primo es que si $ab \in I$ entonces $a \in I$ ó $b \in I$; como $I = \operatorname{Ker} \pi$ lo anterior equivale a decir que si $0 = \pi(ab) = \pi(a)\pi(b)$ entonces $\pi(a) = 0$ ó $\pi(b) = 0$, que es exactamente la condición para que A/I sea íntegro (véase D.1). ∎

Teorema D.6 *La condición necesaria y suficiente para que un ideal I de un anillo A sea maximal es que el anillo A/I sea un cuerpo. Como consecuencia, todo ideal maximal es primo.*

Demostración. La condición para que I sea maximal es que el conjunto {ideales de A que contienen a I} tenga exactamente dos elementos. Asímismo, la condición para que A/I sea un cuerpo es que el conjunto {ideales de A/I} tenga exactamente dos elementos (véase C.11 (a)). Pero ambas condiciones son equivalentes en virtud de C.12. La consecuencia se sigue de D.5, ya que todo cuerpo es un anillo íntegro. ∎

Ejemplos D.7 (a) Los ideales $(x - \alpha)$ y $(x^2 + 1)$ de $\mathbb{R}[x]$ de los ejemplos (c) y (d) de C.11 son maximales, pues se vió que $\mathbb{R}[x]/(x - \alpha)$ es isomorfo al cuerpo $\mathbb{R}$ y que $\mathbb{R}[x]/(x^2 + 1)$ es isomorfo al cuerpo $\mathbb{C}$ (y por tanto $\mathbb{R}[x]/(x - \alpha)$ y $\mathbb{R}[x]/(x^2 + 1)$ también son cuerpos).

(b) El ideal (y) del anillo de polinomios $\mathbb{R}[x,y]$ es primo pero no es maximal, ya que $\mathbb{R}[x,y]/(y)$ es isomorfo a $\mathbb{R}[x]$, que es un anillo íntegro pero no es cuerpo (véase C.11 (e)).

(c) Sea $A \neq 0$ un anillo. El que A sea íntegro es equivalente a que el ideal 0 sea primo, y el que A sea cuerpo es equivalente a que el ideal 0 sea maximal.

D.8 (Elementos primos, elementos irreducibles) Sea A un anillo. Un elemento $a \in A$ se dice que es *primo* si el ideal (a) es primo, es decir, si cada vez que a divide a un producto divide a alguno de sus factores (véanse D.1 y D.4). Un elemento $a \in A$ se dice que es *irreducible* si es propio y cada vez que descompone en un producto, $a = bc$, uno de los factores b ó c es invertible.

D.9 (Dominios de ideales principales) Sea A un anillo. Un ideal I de A se dice que es *principal* si existe $a \in A$ tal que $I = (a)$. Un anillo se dice que es un *dominio de ideales principales* si es íntegro y en él todo ideal es principal.

Sea A un dominio de ideales principales. El generador de un ideal de A no es único: dados $a, b \in A$, $(a) = (b)$ si y sólo si a y b se diferencian en un factor invertible (existe $u \in A$ invertible tal que $a = ub$). Como consecuencia, el conjunto de los ideales de A está en correspondencia, salvo factores invertibles, con los elementos de A: dado $a \in A$ tenemos el ideal (a), y todo ideal I de A tiene un único (salvo factores invertibles) generador.

Ejemplos D.10 (a) El anillo $\mathbb{Z}$ es un dominio de ideales principales (véase C.11 (b)), y es claro que dados $m, n \in \mathbb{Z}$ se satisface $(m) = (n)$ si y sólo si $m = \pm n$ (los únicos elementos invertibles de $\mathbb{Z}$ son ± 1). Como consecuencia se sigue que existe una correspondencia biunívoca entre $\mathbb{N}$ y el conjunto {ideales de $\mathbb{Z}$}.

(b) El segundo ejemplo importante de dominio de ideales principales es el anillo $k[x]$ de los polinomios en una variable con coeficientes en un cuerpo k. Sea I un ideal de $k[x]$. Si $I = 0$ no hay nada que decir, así que supongamos que $I \neq 0$. Consideremos el conjunto $N = \{n \in \mathbb{N} : n = \operatorname{gr} Q(x) \text{ para algún } Q(x) \in I, Q(x) \neq 0\}$; N es no vacío (por ser $I \neq 0$) y por lo tanto podemos considerar $m = \min N$ y un polinomio $P_0(x) \in I$ tal que $m = \operatorname{gr} P_0(x)$. Veamos que $I = (P_0(x))$. Dado $Q(x) \in I$, existen $C(x), R(x) \in k[x]$ tales que $Q(x) = C(x)P_0(x) + R(x)$ y $R(x) = 0$ ó $0 \leq \operatorname{gr} R(x) < m$; si fuera $R(x) \neq 0$ entonces $\operatorname{gr} R(x) \in N$, lo que contradice la elección de m; por lo tanto debe ser $R(x) = 0$ y concluimos que $Q(x) = C(x)P_0(x) \in (P_0(x))$.

Dado un polinomio no nulo $P(x) \in k[x]$ de grado n, será $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ con $a_n \neq 0$, y decimos que a_n es el *coeficiente principal* de $P(x)$. Los polinomios no nulos de $k[x]$ cuyo coeficiente principal es igual a 1 se denominan *unitarios*. Como los elementos invertibles de $k[x]$ son los polinomios constantes no nulos, es claro que todo polinomio no nulo se diferencia de un polinomio unitario en un factor invertible, $P(x) = a_n^{-1} Q(x)$ donde $Q(x) = a_n^{-1} a_0 + \cdots + a_n^{-1} a_{n-1} x^{n-1} + x^n$; por lo tanto existe una correspondencia biunívoca entre los conjuntos {ideales de $k[x]$} y {polinomios unitarios de $k[x]$} $\cup$ {0}.

Teorema D.11 *Sea A un dominio de ideales principales. Dado un elemento no nulo $a \in A$, son equivalentes:*

(i) *a es primo;*

(ii) *a es irreducible;*

(iii) *(a) es maximal.*

Como consecuencia, el único ideal primo de A que no es maximal es 0.

Demostración. (i) $\Rightarrow$ (ii) Supongamos que a es primo y sean $b, c \in A$ tales que $a = bc$, en cuyo caso $b \in (a)$ ó $c \in (a)$. Si, por ejemplo, es $b \in (a)$, entonces existe $d \in A$ tal que $b = ad$ y por tanto $a = bc = adc$, esto es, $a(1 - dc) = 0$, de modo que debe ser $1 - dc = 0$ (pues $a \neq 0$ y A es íntegro) y por lo tanto que c es invertible.

(ii) $\Rightarrow$ (iii) Supongamos que a es irreducible y sea $b \in A$ tal que $(a) \subseteq (b)$. Entonces $a = bc$ para algún $c \in A$, luego, ó bien b es invertible y por lo tanto $(b) = A$, ó bien c es invertible y es $(a) = (b)$.

(iii) $\Rightarrow$ (i) Se ha probado en D.6. ∎

Observación **D.12** El teorema D.11 deja de ser cierto en anillos que no son dominio de ideales principales (aunque sean íntegros), como prueba el ejemplo C.11 (e), que resulta ser una demostración indirecta de que $\mathbb{R}[x, y]$ no es un dominio de ideales principales.

D.13 (Números primos) Consideremos el anillo $\mathbb{Z}$ de los números enteros. Clásicamente, un entero p se dice que es primo si $p \neq \pm 1$ y sus únicos divisores son ± 1 y $\pm p$, es decir, cuando es irreducible. Según D.11, dicha definición clásica coincide con la dada en D.8 (salvo para el 0, que clásicamente no es un número primo). Por lo tanto, la noción de ideal primo de un anillo arbitrario generaliza la idea de número primo.

Una consecuencia de D.6 y D.11 es que si p es un número primo (no nulo) entonces el anillo cociente $\mathbb{Z}_p = \mathbb{Z}/(p)$ es un cuerpo, el cual se denota a veces por $\mathbb{F}_p$.

D.14 (Máximo común divisor, mínimo común múltiplo) Sea A un dominio de ideales principales, de modo que dados $a, b \in A$ los ideales $(a) + (b)$ y $(a) \cap (b)$ son principales. Se define el *máximo común divisor* de a y b, y se denota $\mathrm{m.\,c.\,d.}(a, b)$, como cualquier generador del ideal $(a) + (b)$, y se define el *mínimo común múltiplo* de a y b, y se denota $\mathrm{m.\,c.\,m.}(a, b)$, como cualquier generador del ideal $(a) \cap (b)$. Según dijimos en D.9 dos generadores de un mismo ideal de A se diferencian en un factor invertible, por lo que $\mathrm{m.\,c.\,d.}(a, b)$ y $\mathrm{m.\,c.\,m.}(a, b)$ están determinados salvo productos por invertibles.

Diremos que los elementos a y b son *primos entre sí* cuando $\mathrm{m.\,c.\,d.}(a, b) = 1$, es decir, cuando $(a) + (b) = A$.

Lema D.15 (Identidad de Bézout) *Sean a, b elementos de un dominio de ideales principales A. Si $d = \mathrm{m.\,c.\,d.}(a, b)$, entonces existen $d_1, d_2 \in A$ tales que $d = d_1 a + d_2 b$. Como consecuencia, la condición necesaria y suficiente para que a y b sean primos entre sí es que existan $d_1, d_2 \in A$ tales que $1 = d_1 a + d_2 b$.*

Demostración. Si $d = \mathrm{m.\,c.\,d.}(a, b)$, entonces se sigue inmediatamente de la definición de d la existencia de $d_1, d_2 \in A$ satisfaciendo $d = d_1 a + d_2 b$. En particular, si a y b son primos entre sí entonces existen $d_1, d_2 \in A$ tales que $1 = d_1 a + d_2 b$. Recíprocamente, si existen $d_1, d_2 \in A$ tales que $1 = d_1 a + d_2 b$ entonces $1 \in (a) + (b)$ y por lo tanto $A = (1) \subseteq (a) + (b) \subseteq A$, es decir, $(a) + (b) = A$. ∎

Corolario D.16 (Lema de Euclídes) *Sean a, b, c elementos de un dominio de ideales principales A. Si a divide al producto bc y es primo con b, entonces a divide a c.*

Demostración. Sea $\pi : A \to A/(a)$ el morfismo de paso al cociente de A por el ideal (a). Por una parte, existe $d \in A$ tal que $bc = da$ y por tanto $0 = \pi(bc) = \pi(b)\pi(c)$. Por otra parte, existen $d_1, d_2 \in A$ tales que $1 = d_1 a + d_2 b$ y obtenemos $\pi(1) = \pi(d_2)\pi(b)$, es decir, $\pi(b)$ es un elemento invertible de $A/(a)$. De todo se sigue que $\pi(c) = 0$, esto es, $c \in (a)$. ∎

D.17 (Anillos euclídeos) Un anillo A se dice que es un *anillo euclídeo* si es íntegro y está dotado de una aplicación $\delta : A - \{0\} \longrightarrow \mathbb{N}$ que satisface:

(i) $\delta(a) \leq \delta(ab)$ para todo par de elementos no nulos $a, b \in A$;

(ii) si $a \in A$ no es nulo, para cada $b \in A$ existen $c, r \in A$ tales que

$$b = ac + r\,, \qquad r = 0 \ \text{ó} \ \delta(r) < \delta(a)\,.$$

El anillo $\mathbb{Z}$ de los números enteros es euclídeo: para cada número entero n definimos $\delta(n) := |n|$ y aplicamos la división entera (véase A.24). El anillo $k[x]$ de los polinomios con coeficientes en un cuerpo k es euclídeo: para cada polinomio no nulo $P(x) \in k[x]$ definimos $\delta(P(x)) := \operatorname{gr} P(x)$ y aplicamos la división de polinomios (véase D.3).

Si A es un anillo euclídeo entonces A es un dominio de ideales principales. En efecto, sea I un ideal de A y supongamos que $I \neq 0$ (si $I = 0$ entonces $I = (0)$). Entre todos los elementos no nulos de I existirá alguno a tal que $\delta(a)$ sea mínimo, y se satisface $I = (a)$ (véase en B.8 (c) la demostración de que $\mathbb{Z}$ es dominio de ideales principales, ó en D.10 (b) la demostración de que $k[x]$ es dominio de ideales principales).

D.18 (Algoritmo de Euclídes) Dados elementos no nulos a, b de un anillo euclídeo A, el "algoritmo de Euclídes" es un método que permite calcular el máximo común divisor d de a y b, así como los coeficientes d_1, d_2 que satisfacen la Identida de Bézout, $d = d_1 a + d_2 b$. Se basa en el siguiente resultado: *Sea A un dominio de ideales principales. Si $a, b, c, r \in A$ satisfacen $a = bc + r$, entonces* $\text{m. c. d.}(a, b) = \text{m. c. d.}(b, r)$. En efecto, basta tener en cuenta que $a = bc + r \in (b) + (r)$ y que $r = a - bc \in (a) + (b)$ para obtener la igualdad $(a) + (b) = (b) + (r)$.

Sean entonces a, b elementos no nulos de un anillo euclídeo A. Se efectúan las divisiones

$$\begin{aligned} a &= c_1 b + r_1 \\ b &= c_2 r_1 + r_2 \\ r_1 &= c_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= c_n r_{n-1} + r_n \\ r_{n-1} &= c_{n+1} r_n + 0 \end{aligned}$$

hasta que el resto sea nulo, lo que necesariamente ha de ocurrir, pues la sucesión de números naturales $\delta(r_1), \delta(r_2), \ldots$ es estrictamente decreciente. Según lo probado anteriormente tenemos

$$\begin{aligned} d = \text{m. c. d.}(a, b) = \text{m. c. d.}(b, r_1) = \text{m. c. d.}(r_1, r_2) = \ \ldots \ = \text{m. c. d.}(r_i, r_{i+1}) \\ = \ \ldots \ = \text{m. c. d.}(r_n, 0) = r_n\,, \end{aligned}$$

es decir, el máximo común divisor d de a y b es el último resto no nulo.

Además, cuando tengamos una descomposición $d = d_1 r_i + d_2 r_{i+1}$ de d como suma de un múltiplo de r_i y otro de r_{i+1}, la igualdad $r_{i-1} = c_{i+1} r_i + r_{i+1}$ permite descomponer d como suma de un múltiplo de r_{i-1} y otro de r_i,

$$d = d_1 r_i + d_2(r_{i-1} - c_{i+1} r_i) = d_2 r_{i-1} + (d_1 - d_2 c_{i+1}) r_i \,.$$

Al ser $d = r_n = r_{n-2} - c_n r_{n-1}$, procediendo recurrentemente de este modo obtenemos una descomposición de d como suma de un múltiplo de a y otro de b.

Teorema D.19 (Descomposición en factores irreducibles) *Todo elemento propio a de un anillo euclídeo A descompone en producto de elementos irreducibles de A (existen irreducibles $p_1, \ldots, p_r \in A$ tales que $a = p_1 \cdots p_r$). Además, dicha descomposición es única salvo el orden y factores invertibles (si $a = q_1 \cdots q_s$ es otra descomposición de a en producto de irreducibles, entonces $r = s$ y, reoordenando los factores si fuera preciso, $q_i = u_i p_i$ para ciertos invertibles $u_1, \ldots, u_r \in A$).*

Como consecuencia, para todo elemento propio $a \in A$ existen elementos irreducibles distintos $p_1, \ldots, p_t \in A$ y enteros positivos $n_1, \ldots, n_t$ tales que $a = p_1^{n_1} \cdots p_t^{n_t}$.

Demostración. Probemos primero la existencia de tal descomposición. Si a es irreducible hemos terminado, así que supongamos que a no es irreducible, en cuyo caso probemos que existe un irreducible $p_1 \in A$ que divide a a.

Sean $b, c \in A$ elementos no invertibles tales que $a = bc$ y probemos que entonces $\delta(b) < \delta(a)$ y $\delta(c) < \delta(a)$. Si, por ejemplo, fuera $\delta(b) = \delta(a)$, tendríamos que existen $d, r \in A$ tales que $b = ad + r$ con $r = 0$ ó $\delta(r) < \delta(a) = \delta(b)$; si $0 = r = b(1 - cd)$ entonces $1 = cd$, lo que no es cierto porque c no es invertible, y si $1 - cd \neq 0$ entonces r sería no nulo y tal que $\delta(r) \geq \delta(b)$, lo cual está en contradicción con $\delta(r) < \delta(b)$. Ahora, si b (ó c) es irreducible tomamos $p_1 = b$ (ó $p_1 = c$). Si b no es irreducible existen elementos no invertibles $b', c' \in A$ tales que $b = b'c'$, $\delta(b') < \delta(b)$ y $\delta(c') < \delta(b)$; de nuevo, si b' es irreducible entonces tomamos $p_1 = b'$, y si b' no es irreducible repetimos el proceso con b'. En un número finito de pasos concluimos la existencia del elemento irreducible p_1 que divide a a, ya que la sucesión $\delta(a), \delta(b), \delta(b'), \ldots$ es estrictamente decreciente.

Sean entonces $p_1, a' \in A$ tales que $a = p_1 a'$, p_1 es irreducible y a' es no invertible. Si a' es irreducible tomamos $p_2 = a'$ y terminamos; si a' no es irreducible, entonces existen $p_2, a'' \in A$ tales que $a' = p_2 a''$, p_2 es irreducible y a'' es no invertible. Si a'' es irreducible tomamos $p_3 = a''$ y terminamos; si a'' no es irreducible repetimos el proceso. En un número finito de pasos concluimos la existencia de elementos irreducible $p_1, \ldots, p_r$ tales que $a = p_1 \cdots p_r$, ya que la sucesión $\delta(a), \delta(a'), \delta(a''), \ldots$ es estrictamente decreciente.

Veamos ahora la unicidad. Sean $p_1 \cdots p_r = a = q_1 \cdots q_s$ dos descomposiciones de a en producto de irreducibles. Como p_1 divide al producto $q_1 \cdots q_s$ divide a alguno de sus factores; reordenando los factores si fuera preciso podemos suponer que p_1 divide a q_1, en cuyo caso p_1 y q_1 coninciden salvo un factor invertible. Pero entonces $p_2 \cdots p_r$ y $q_2 \cdots q_s$ también coinciden salvo un factor invertible. Reiterando el argumento, en un número finito de pasos concluimos la demostración. ∎

Corolario D.20 *Sean a, b elementos propios de un anillo euclídeo A. El máximo común divisor de a y b se obtiene multiplicando los divisores irreducibles comunes a sus descomposiciones en*

factores irreducibles, elevados al menor de los exponentes con que aparecen en cada una de ellas. El mínimo común múltiplo de a y b se obtiene multiplicando los divisores irreducibles comunes a sus descomposiciones, elevados al mayor de los exponentes con que aparecen en cada una de ellas, y los divisores irreducibles de cada uno de ellos pero no del otro, elevados a los exponentes que tienen en la correspondiente descomposición.

Nota **D.21** El teorema de descomposición D.19 (y su corolario) es válido en cualquier dominio de ideales principales, aunque la demostración de la existencia de las descomposición que hemos dado para los anillos euclídeos necesita ser modificada convenientemente.

D.22 (Descomposición en $\mathbb{Z}$) Si en el anillo euclídeo $\mathbb{Z}$ consideramos sólo los enteros positivos (véase D.10 (a)), entonces obtenemos la siguiente versión clásica de D.19: *Para todo entero positivo $m > 1$ existen números primos positivos distintos $p_1, \ldots, p_r$ y números naturales no nulos $n_1, \ldots, n_r$ tales que $m = p_1^{n_1} \cdots p_r^{n_r}$. Además, la anterior descomposición es única salvo el orden de los factores.*

D.23 (Descomposición en $k[x]$) Sea k un cuerpo. Si en el anillo euclídeo $k[x]$ consideramos sólo los polinomios irreducibles unitarios tenemos (véase D.10 (b)): *Si $P(x) \in k[x]$ es un polinomio de grado $n \geq 1$, entonces existen polinomios irreducibles distintos $P_1(x), \ldots, P_r(x)$ en $k[x]$ y números naturales no nulos $n_1, \ldots, n_r$ tales que $P(x) = P_1(x)^{n_1} \cdots P_r(x)^{n_r}$, siendo la anterior descomposición única salvo el orden de los factores.*

D.24 (Raíces de un polinomio, polinomios irreducibles) Sea k un cuerpo. Es claro que todo polinomio de grado 1 de $k[x]$ es irreducible, pues todo polinomio unitario de grado 1 lo es (lo hemos probado en el caso particular $k = \mathbb{R}$; véase D.7 (a)). Dados $\alpha \in k$ y $P(x) \in k[x]$, se dice que α es una *raíz* (ó un *cero*) del polinomio $P(x)$ si $P(\alpha) = 0$, es decir, si el polinomio irreducible $x - \alpha$ divide a $P(x)$ (véase en C.11 (c) el caso particular $k = \mathbb{R}$). De la definición se sigue inmediatamente que α es raíz de un producto de polinomios si y sólo si es raíz de alguno de los factores.

Se satisface: *Todo polinomio irreducible de $k[x]$ de grado mayor 1 carece de raíces en k.* En efecto, si $P(x) \in k[x]$ es un polinomio irreducible que admite una raíz $\alpha \in k$, entonces $P(x) = Q(x)(x - \alpha)$ para algún $Q(x) \in k[x]$; como $P(x)$ es irreducible debe satisfacerse que $Q(x)$ es invertible, es decir, $\operatorname{gr} Q(x) = 0$; concluimos que $\operatorname{gr} P(x) = 1$.

El recíproco del anterior resultado no es cierto, es decir, pueden existir polinomios en $k[x]$ que no tengan raíces en k y que sin embargo no sean irreducibles; por ejemplo, $(x^2+1)(x^2+2)$ es un polinomio no irreducible de $\mathbb{R}[x]$ que no tiene raíces en $\mathbb{R}$. Se satisface: *Si $P(x) \in k[x]$ es un polinomio de grado 2 ó 3 que no tiene raíces en k, entonces $P(x)$ es irreducible.* La demostración es sencilla y se deja como ejercicio.

Supongamos que $\alpha \in k$ es raíz de un polinomio no nulo $P(x) \in k[x]$; entonces existe un polinomio $P_1(x) \in k[x]$ tal que $P(x) = P_1(x)(x - \alpha)$; si $P_1(\alpha) \neq 0$ se dice que α es raíz *simple* de $P(x)$. Si $P_1(\alpha) = 0$ entonces existe un polinomio $P_2(x) \in k[x]$ tal que $P_1(x) = P_2(x)(x - \alpha)$ y por tanto $P(x) = P_2(x)(x-\alpha)^2$; si $P_2(\alpha) \neq 0$ se dice que α es raíz *doble* de $P(x)$. En general, existen un entero positivo m y un polinomio $Q(x) \in k[x]$ tales que $P(x) = Q(x)(x - \alpha)^m$ y $Q(\alpha) \neq 0$ (es decir, existe un entero positivo m tal que $P(x)$ es divisible por $(x - \alpha)^m$ y no es divisible por $(x - \alpha)^{m+1}$); se dice entonces que α un una raíz de $P(x)$ de *multiplicidad* m.

Teorema D.25 *Sea $P(x)$ un polinomio no nulo con coeficientes en un cuerpo k, y sean $\alpha_1, \ldots, \alpha_r \in k$ todas las raíces distintas que $P(x)$ tiene en k, de multiplicidades $m_1, \ldots, m_r$, respectivamente. Entonces existe un polinomio $Q(x) \in k[x]$ sin raíces en k tal que*

$$P(x) = (x - \alpha_1)^{m_1} \ldots (x - \alpha_r)^{m_r} Q(x)\,.$$

Como consecuencia, el número de raíces que $P(x)$ tiene en k (contando multiplicidades) no supera a $\operatorname{gr} P(x)$*: $m_1 + \cdots + m_r \leq \operatorname{gr} P(x)$.*

Demostración. Según lo dicho en D.24, existe un polinomio $P_1(x) \in k[x]$ que no tiene a α_1 por raíz y tal que $P(x) = (x - \alpha_1)^{m_1} P_1(x)$. Como $(x - \alpha_2)^{m_2}$ divide a $P(x)$ y es primo con $(x - \alpha_1)^{m_1}$ (pues $\alpha_1 \neq \alpha_2$), aplicando el Lema de Euclídes obtenemos que $(x - \alpha_2)^{m_2}$ divide a $P_1(x)$ (véase D.16). Si $P_2(x) \in k[x]$ es tal que $P_1(x) = (x - \alpha_2)^{m_2} P_2(x)$, entonces $P(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} P_2(x)$; además α_1 y α_2 no pueden ser raíz de $P_2(x)$. Reiterando el argumento, en un número finito de pasos concluimos la demostración.

La consecuencia del enunciado del teorema se sigue de la igualdad $n = \operatorname{gr} P(x) = m_1 + \cdots + m_r + \operatorname{gr} Q(x)$, ya que $\operatorname{gr} Q(x) \geq 0$. ∎

D.26 (Cuerpos algebraicamente cerrados) Sea k un cuerpo. Un polinomio no constante $P(x) \in k[x]$ no necesariamente tiene raíces en k. Por ejemplo, el polinomio $x^2 + 1 \in \mathbb{R}[x]$ no tiene raíces en $\mathbb{R}$. El cuerpo k se dice que es *algebraicamente cerrado* si todo polinomio de $k[x]$ de grado mayor ó igual a 1 tiene una raíz en k. Se comprueba fácilmente que son equivalentes las siguientes afirmaciones:

(i) k es algebraicamente cerrado;

(ii) si $P(x) \in k[x]$ tiene grado $n \geq 1$ entonces $P(x)$ tiene exactamente n raíces en k (contadas cada una con su multiplicidad);

(iii) los únicos polinomios irreducibles de $k[x]$ son los de grado 1.

El conocido como Teorema de d'Alembert afirma que *el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.* La demostración de este teorema hace uso de técnicas el Análisis y es por ello que no la hacemos.

D.27 (Cierre algebraico de un cuerpo) Sea k un cuerpo no algebraicamente cerrado y sea $P(x) \in k[x]$ un polinomio no constante que no tiene raíces en k. Si K es otro cuerpo tal que k es un subcuerpo suyo (esto es, k es un subanillo de K), entonces $k[x]$ es un subanillo de $K[x]$ y por tanto $P(x) \in K[x]$, y puede ocurrir que aunque $P(x)$ no tiene raíces en k sí las tiene en K. Por ejemplo, $\mathbb{R}$ es un subcuerpo de $\mathbb{C}$ y el polinomio $x^2 + 1 \in \mathbb{R}[x]$ no tiene raíces en $\mathbb{R}$ pero sí las tiene en $\mathbb{C}$. En D.29 probaremos que efectivamente existe un cuerpo K que contiene a k y en el que $P(x)$ sí tiene raíces.

Ahora podemos plantearnos la siguiente cuestión: ¿existen cuerpos K que contienen a k y tales que todo polinomio no constante de $k[x]$ tiene raíces en K?; y de existir, ¿hay uno que sea el "más pequeño"? Las respuestas a las anteriores preguntas son afirmativas: *Existe un cuerpo $\bar{k}$ que contiene a k en el que todo polinomio no constante de $k[x]$ tiene raíces y que satisface la siguiente propiedad: si K es otro cuerpo que contiene a k en el que todo polinomio no constante de $k[x]$ tiene raíces, entonces K contiene a $\bar{k}$. El cuerpo $\bar{k}$ es único (salvo isomorfismos de cuerpos) y se denomina* cierre algebraico *(ó* clausura algebraica*) de k.*

El anterior resultado de Teoría de Anillos (que hemos enunciado de un modo no riguroso) se sale del caracter introductorio de este capítulo y por lo tanto no lo probaremos.

Como $\mathbb{C}$ es algebraicamente cerrado todo polinomio no constante de $\mathbb{R}[x]$ tiene una raíz en $\mathbb{C}$; además todo cuerpo que contenga a $\mathbb{R}$ y a las raíces del polinomio $x^2+1 \in \mathbb{R}[x]$ debe de contener a $\mathbb{C}$. Por lo tanto el cierre algebraico de $\mathbb{R}$ es $\mathbb{C}$.

D.28 (Polinomios irreducibles de $\mathbb{R}[x]$) Ya hemos dicho en D.26 que el cuerpo $\mathbb{C}$ es algebraicamente cerrado, es decir, que los únicos polinomios irreducibles de $\mathbb{C}[x]$ son los de grado 1. En cuanto a los polinomios con coeficientes reales se satisface: *Además de los polinomios de grado* 1, *los polinomios irreducibles de* $\mathbb{R}[x]$ *son los de grado* 2 *que no tienen raíces reales.*

Para probar la anterior afirmación obsérvese que si $P(x) \in \mathbb{R}[x]$ y $z = a + b\,\mathrm{i} \in \mathbb{C}$, entonces se tiene $\overline{P(z)} = P(\overline{z})$ (véanse en C.3 (e) las propiedades de "tomar conjugado" en los números complejos); como sonsecuencia, si $z \notin \mathbb{R}$ (es decir, si $b \neq 0$) y z es raíz de $P(x)$, entonces $\bar{z} = a - b\,\mathrm{i}$ es otra raíz de $P(x)$ distinta de z, de modo que $P(x)$ es divisible en $\mathbb{C}[x]$ por el polinomio $(x-a-b\,\mathrm{i})(x-a+b\,\mathrm{i}) = x^2 - 2ax + (a^2+b^2)$, y como el anterior polinomio tiene sus coeficientes en $\mathbb{R}$ concluimos que $P(x)$ es divisible en $\mathbb{R}[x]$ por el polinomio $x^2 - 2ax + (a^2+b^2)$.

Supongamos ahora que $P(x)$ es un polinomio irreducible de $\mathbb{R}[x]$ de grado mayor que 1; entonces $P(x)$ no tiene raíces reales (véase D.24) y por lo tanto existe un número complejo $a + b\,\mathrm{i}$ con $b \neq 0$ que es raíz de $P(x)$. Según lo dicho en el anterior párrafo existe $Q(x) \in \mathbb{R}[x]$ tal que $P(x) = Q(x)(x^2 - 2ax + (a^2+b^2))$; como $P(x)$ es irreducible el polinomio $Q(x)$ debe ser invertible (esto es, de grado cero) y concluimos que el grado de $P(x)$ es 2. Para terminar habría que probar que si $P(x)$ es un polinomio de $\mathbb{R}[x]$ de grado 2 que no tiene raíces en $\mathbb{R}$ entonces $P(x)$ es irreducible, lo cual se dejo como ejercicio en D.24.

Lema D.29 (Teorema de Kronecker) *Sea $P(x)$ un polinomio no nulo con coeficientes en un cuerpo k que no tiene raíces en k. Existe un cuerpo K que contiene a k tal que $P(x)$ tiene alguna raíz en K.*

Demostración. Si $P(x)$ descompone en producto de polinomios, las raíces de $P(x)$ son las raíces de los polinomios factores. Por lo tanto, el teorema de descomposicón D.19 nos permite suponer que $P(x)$ es irreducible, en cuyo caso el anillo cociente $k[x]/(P(x)) = K$ es un cuerpo porque $(P(x))$ es un ideal maximal de $k[x]$ (véanse D.11 y D.6). Si $k \to k[x]$ es la inclusión de k en $k[x]$ y $\pi : k[x] \to K$ es el morfismo de paso al cociente, entonces la composición de los dos anteriores morfismos de anillos es un morfismo de anillos $k \to K$, que debe ser inyectivo (véase C.11 (a)) y permite consirerar a k como un subcuerpo de K. La clase de x en K, $\pi(x)$, es una raíz de $P(x)$, ya que $P(\pi(x)) = \pi(P(x)) = 0$. (Véase el ejemplo C.11 (d).) ∎

Bibliografía

[1] Abellanas, P. , *Geometría Básica*, Romo, Madrid, 1969.

[2] Castellet, M. , Llerena, I. , *Álgebra Lineal y Geometría*, Reverté, Barcelona, 1991.

[3] Espada, E. , *Problemas resueltos de Álgebra, I*, Eunibar, Barcelona, 1978.

[4] Espada, E. , *Problemas resueltos de Álgebra, II*, Eunibar, Barcelona, 1983.

[5] Gutiérrez, A. , García, F. , *Geometría*, Pirámide, madrid, 1983.

[6] Hernández, E. , *Álgebra y Geometría*, Addison-Wesley Iberoamericana, Madrid, 1994.

[7] Navarro, J.A. , *Álgebra Conmutativa Básica*, Manuales Unex n. 19, Publicaciones Univ. Extremadura, Cáceres, 1996.

[8] Ruipérez, D.H. , *Álgebra Lineal* (2^{a} edición), Ed. Univ. Salamanca, Salamanca, 1987.

[9] de la Villa, A. , *Problemas de Álgebra*, Clagsa, Madrid, 1994.