$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_i b_j\right)x^k.$$

Por ejemplo, un elemento de $\mathbb{Z}[x]$ es $2x^5 + 5x^2 - 11x + 6$. Se trata de un polinomio de grado 5 con coeficiente director igual a 2.

En la práctica escribiremos $p = p(x_1, \ldots, x_n)$ para indicar que las indeterminadas $x_1, \ldots, x_n$ son las únicas (a lo sumo) que aparecen en el polinomio p con exponentes no nulos.

2.2 Evaluación de polinomios

La evaluación de polinomios es un concepto muy sencillo: si $p(x) = 2x^2 - 4x$, pretendemos que $p(3)$ sea $2 \cdot 3^2 - 4 \cdot 3 = 6$. No obstante vamos a definir las evaluaciones en un contexto más general que nos será útil después.

Definición 2.9 Sean A y B dos anillos conmutativos y unitarios, $\phi : A \longrightarrow B$ un homomorfismo, S un conjunto y $v : S \longrightarrow B$ cualquier aplicación. Para cada polinomio $p = \sum_{i=1}^{m} a_i\, x_1^{k_{i1}} \ldots x_n^{k_{in}} \in A[S]$ definimos

$$\phi p(v) = \sum_{i=1}^{m} \phi(a_i)\, v(x_1)^{k_{i1}} \ldots\ v(x_n)^{k_{in}} \in B.$$

La conmutatividad de B y la unicidad de la expresión hacen que $\phi p(v)$ esté bien definido, pues dos expresiones de p difieren sólo en el orden de las indeterminadas y en la presencia de monomios con coeficiente 0, o de indeterminadas con exponente 0, pero en cualquier caso se obtiene el mismo elemento de B.

Tenemos, por tanto, una aplicación $\Phi : A[S] \longrightarrow B$ dada por $\Phi(p) = \phi p(v)$.

En definitiva $\Phi(p)$ se calcula reemplazando los coeficientes de p por su imagen por ϕ y las indeterminadas por sus imágenes por v.

En la práctica, si $p = p(x_1, \ldots, x_n)$ escribiremos $\phi p(b_1, \ldots, b_n)$ para indicar el polinomio que resulta de evaluar cada indeterminada x_i con el elemento b_i. Notar que aunque S pueda ser infinito, $\phi p(v)$ sólo depende de la forma en que v actúa sobre las indeterminadas que aparecen en p, que son siempre un número finito.

Cuando ϕ sea simplemente la identidad en A no lo escribiremos, y pondremos simplemente $p(b_1, \ldots, b_n)$.

Teorema 2.10 *Sean A y B dos anillos conmutativos y unitarios, $\phi : A \longrightarrow B$ un homomorfismo tal que $\phi(1) = 1$, S un conjunto y $v : S \longrightarrow B$ cualquier aplicación. Entonces la evaluación $\Phi : A[S] \longrightarrow B$ es el único homomorfismo que coincide con ϕ sobre A y con v sobre S.*

Demostración: Sean $p,\ q \in A[S]$, digamos $p = \sum_{i=1}^{m} a_i\, x_1^{k_{i1}} \ldots\ x_n^{k_{in}}$ y $q = \sum_{i=1}^{m} b_i\, x_1^{k_{i1}} \ldots\ x_n^{k_{in}}$. Observar que no hay problema en suponer que los exponentes de los monomios son los mismos, pues podemos añadir monomios con coeficiente 0 hasta igualar ambas expresiones.

$$\Phi(p+q) = \Phi\left(\sum_{i=1}^{m} (a_i + b_i)\, x_1^{k_{i1}} \ldots\ x_n^{k_{in}}\right) = \sum_{i=1}^{m} \phi(a_i + b_i) v(x_1)^{k_{i1}} \ldots\ v(x_n)^{k_{in}}$$

$$= \sum_{i=1}^{m} \big(\phi(a_i) + \phi(b_i)\big) v(x_1)^{k_{i1}} \dots\ v(x_n)^{k_{in}} = \sum_{i=1}^{m} \phi(a_i) v(x_1)^{k_{i1}} \dots\ v(x_n)^{k_{in}}$$

$$+ \sum_{i=1}^{m} \phi(b_i) v(x_1)^{k_{i1}} \dots\ v(x_n)^{k_{in}} = \Phi(p) + \Phi(q).$$

Para probar que Φ conserva productos usaremos el hecho ya probado de que conserva las sumas.

$$\begin{aligned}
\Phi(pq) &= \Phi\left(\sum_{i,j=1}^{m} a_i b_j\, x_1^{k_{i1}+k_{j1}} \dots\ x_n^{k_{in}+k_{jn}} \right) \\
&= \sum_{i,j=1}^{m} \Phi(a_i b_j\, x_1^{k_{i1}+k_{j1}} \dots\ x_n^{k_{in}+k_{jn}}) \\
&= \sum_{i,j=1}^{m} \phi(a_i b_j)\, v(x_1)^{k_{i1}+k_{j1}} \dots\ v(x_n)^{k_{in}+k_{jn}} \\
&= \sum_{i,j=1}^{m} \phi(a_i)\phi(b_j)\, v(x_1)^{k_{i1}+k_{j1}} \dots\ v(x_n)^{k_{in}+k_{jn}} \\
&= \left(\sum_{i=1}^{m} \phi(a_i)\, v(x_1)^{k_{i1}} \dots v(x_n)^{k_{in}} \right) \left(\sum_{j=1}^{m} \phi(b_j)\, v(x_1)^{k_{j1}} \dots v(x_n)^{k_{jn}} \right) \\
&= \Phi(p)\Phi(q).
\end{aligned}$$

La unicidad es evidente. ∎

De este teorema se deducen varios casos particulares de interés.

Teorema 2.11 *Sean A y B anillos conmutativos y unitarios y $\phi : A \longrightarrow B$ un homomorfismo tal que $\phi(1) = 1$. Sea S un conjunto. Entonces existe un único homomorfismo $\bar{\phi} : A[S] \longrightarrow B[S]$ que coincide con ϕ en A y deja invariantes a las indeterminadas. Además es inyectivo, suprayectivo o biyectivo si ϕ lo es.*

Demostración: El homomorfismo no es sino el construido en el teorema anterior tomando como v la identidad en S. Concretamente

$$\bar{\phi}\left(\sum_{i=1}^{m} a_i\, x_1^{k_{i1}} \dots\ x_n^{k_{in}} \right) = \sum_{i=1}^{m} \phi(a_i)\, x_1^{k_{i1}} \dots\ x_n^{k_{in}}.$$

Todo lo pedido es obvio. ∎

Esto significa en particular que si A es un subanillo de B podemos considerar $A[S]$ como un subanillo de $B[S]$. Así por ejemplo, $\mathbb{Z}[S] \subset \mathbb{Q}[S]$.

Teorema 2.12 *Sea A un anillo conmutativo y unitario. Sea S un conjunto y supongamos que $S = X \cup Y$ con X e Y disjuntos. Sea B el conjunto de los polinomios de $A[S]$ tales que todos sus monomios con coeficientes no nulos tengan tan sólo indeterminadas de X con exponentes no nulos. Entonces B es un subanillo de $A[S]$ isomorfo a $A[X]$ y $A[S]$ es isomorfo a $A[X][Y]$.*

DEMOSTRACIÓN: Sea $\phi : A[X] \longrightarrow A[S]$ el homomorfismo construido en 2.10 con la identidad en A y la identidad en X. Es claro que B es la imagen de ϕ y que ϕ es un monomorfismo.

Ahora sea $\psi : A[X][Y] \longrightarrow A[S]$ el homomorfismo construido en 2.10 a partir de ϕ y de la identidad en Y. Es inmediato probar que se trata de un isomorfismo de anillos. ∎

Por ejemplo, el polinomio $3x^5y^2z^2 + 8x^2z - 6z^2 + 5$ de $\mathbb{Z}[x, y, z]$ puede ser identificado con $(3x^5y^2 - 6)z^2 + (8x^2)z + 5 \in \mathbb{Z}[x, y][z]$, donde ahora $3x^5y^2 - 6$ es el coeficiente de z^2.

Si lo queremos en $\mathbb{Z}[z][x, y]$ será: $3z^2(x^5y^2) + (8z)x^2 + (-6z^2 + 5)$, donde ahora $-6z^2 + 5$ es el término independiente.

Por otra parte si $S \subset T$ podemos considerar $A[S] \subset A[T]$.

2.3 Propiedades algebraicas

Las principales propiedades algebraicas de los anillos de polinomios se deducen a partir de consideraciones sobre los grados. Es obvio que el grado de la suma de dos polinomios f y g de $A[x]$ es menor o igual que el máximo de los grados de f y g. Será igual a dicho máximo si sus grados son distintos, pero si coinciden se pueden cancelar los coeficientes directores y el grado de la suma disminuye:

$$(3x^5 - 2x^2 + 5x + 2) + (-3x^5 + x^3 - x^2 + 1) = x^3 - 3x^2 + 5x + 3.$$

El grado del producto es a lo sumo la suma de los grados. Normalmente se da la igualdad. Las únicas excepciones se dan si uno de los factores es nulo, o si alguno de los coeficientes directores es un divisor de cero.

Teorema 2.13 *Sea A un anillo unitario y p, q dos polinomios no nulos de $A[x]$ tales que al menos el coeficiente director de uno de ellos no sea un divisor de cero. Entonces $pq \neq 0$, $\operatorname{grad}(pq) = \operatorname{grad}(p) + \operatorname{grad}(q)$ y el coeficiente director del producto es el producto de los coeficientes directores.*

DEMOSTRACIÓN: Sean $p = \sum_{i=0}^{m} a_i x^i$, $q = \sum_{i=0}^{n} b_i x^i$, con $a_m \neq 0 \neq b_n$. Entonces $pq = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$ y el coeficiente de x^{m+n} es exactamente $a_m b_n \neq 0$, puesto que uno de ellos no es divisor de cero. Por lo tanto $a_m b_n$ es el coeficiente director de pq y el grado es $m + n$. ∎

Teorema 2.14 *Sea A un dominio íntegro y S un conjunto cualquiera. Entonces $A[S]$ es un dominio íntegro.*

DEMOSTRACIÓN: El teorema anterior nos da que si A es un dominio íntegro entonces $A[x]$ también lo es. Aplicándolo un número finito de veces obtenemos que si A es un dominio íntegro y S es finito, entonces $A[S]$ también lo es. Si S es arbitrario y f, g son dos polinomios no nulos de $A[S]$, entonces los monomios

con coeficientes no nulos de f y g contienen un número finito de indeterminadas con exponente no nulo, luego f y g están en un subanillo $A[X]$ con X finito, luego $A[X]$ es un dominio íntegro, luego $fg \neq 0$. Por tanto $A[S]$ es un dominio íntegro. ∎

Teorema 2.15 *Sea A un dominio íntegro y S un conjunto. Entonces las unidades de $A[S]$ son las mismas que las de A.*

DEMOSTRACIÓN: Veámoslo primero para $A[x]$. Si $p \in A[x]$ es una unidad, entonces existe otro polinomio no nulo q tal que $pq = 1$. Por 2.13 tenemos que $\operatorname{grad} p + \operatorname{grad} q = \operatorname{grad} 1 = 0$, luego ha de ser $\operatorname{grad} p = \operatorname{grad} q = 0$, es decir, p y q están en A, luego p es una unidad en A.

De aquí se sigue el resultado para $A[S]$ con S finito y, por el mismo argumento que en el teorema anterior, vale para todo S. ∎

En particular vemos que $A[S]$ no es un cuerpo aunque A lo sea. Como sí es un dominio íntegro, podemos definir su cuerpo de fracciones.

Definición 2.16 Sea A un dominio íntegro y S un conjunto. Llamaremos cuerpo de las *fracciones algebraicas* o *funciones racionales* sobre A con indeterminadas en S al cuerpo de cocientes de $A[S]$. Lo representaremos por $A(S)$.

Así, por ejemplo, un elemento de $\mathbb{Z}(x, y)$ es $\frac{x^4 - x^3 y}{x^3 - 4xy^2 + 4}$.

Ejercicio: Probar que $\mathbb{Z}(S) = \mathbb{Q}(S)$.

Quizá éste es un buen momento para empezar a entender la utilidad del lenguaje algebraico que empezamos a introducir en el capítulo anterior: el hecho de que $\mathbb{Z}[x]$ sea un anillo (y más concretamente un dominio íntegro) nos permite tratar formalmente a sus elementos con las mismas reglas básicas que a los números enteros. El hecho de que conozcamos la construcción general del cuerpo de cocientes de un dominio íntegro justifica que hablemos de fracciones de polinomios exactamente igual que de fracciones de enteros, y estos ejemplos son sólo una mínima parte de los que nos vamos a encontrar.

Debemos ocuparnos ahora de la posibilidad de dividir polinomios. Esta es una característica importantísima de los anillos con una indeterminada.

Teorema 2.17 *Sea A un anillo unitario, D y d dos polinomios no nulos de $A[x]$ tales que el coeficiente director de d sea una unidad en A. Entonces existen unos únicos polinomios c y r en $A[x]$ tales que $D = dc + r$ con el grado de r menor estrictamente que el grado de d (también podemos exigir que $D = cd + r$, pero si A no es conmutativo los polinomios que cumplan esto no tienen por qué ser los mismos).*

DEMOSTRACIÓN: Si $\operatorname{grad} D < \operatorname{grad} d$ basta tomar $c = 0$ y $r = D$. Supongamos que $\operatorname{grad} d \leq \operatorname{grad} D$.

Sea $D = \sum_{i=0}^{n} a_i x^i$, $d = \sum_{i=0}^{m} b_i x^i$, con $a_n \neq 0 \neq b_m$ y $m \leq n$. Además estamos suponiendo que b_m es una unidad de A. Veamos el teorema por inducción sobre n.

Si $n = 0$, entonces también $m = 0$, es decir, $D = a_0$, $d = b_0$, luego basta tomar $c = (b_0)^{-1}a_0$ y $r = 0$. Supongámoslo cierto para polinomios de grado menor que n.

Consideremos $db_m^{-1}a_nx^{n-m} = \sum_{i=0}^{m} b_ib_m^{-1}a_nx^{i+n-m}$. El monomio de mayor grado es $b_m(b_m)^{-1}a_nx^{m+n-m} = a_nx^n$, luego se trata de un polinomio de grado n con coeficiente director a_n.

Consecuentemente el polinomio $D - d(b_m)^{-1}a_nx^{n-m}$ tiene grado menor que n, luego por hipótesis de inducción existen polinomios c' y r de manera que $D - db_m^{-1}a_nx^{n-m} = dc' + r$ con $\operatorname{grad} r < \operatorname{grad} d$.

Sea $c = b_m^{-1}a_nx^{n-m} + c'$. Así $D = dc + r$ como se pedía.

Veamos ahora la unicidad. Supongamos que $D = dc+r = dc'+r'$. Entonces $d(c-c') = r'-r$. Si $c-c' \neq 0$, como el coeficiente director de d es una unidad, por el teorema 2.13. resulta que $\operatorname{grad}(r'-r) = \operatorname{grad}(d(c-c')) = \operatorname{grad} d+\operatorname{grad}(c-c')$, pero $\operatorname{grad}(r'-r) < \operatorname{grad} d \leq \operatorname{grad} d + \operatorname{grad}(c-c')$, contradicción.

Concluimos entonces que $c = c'$, luego también $r = r'$. ∎

El lector que sepa dividir números naturales puede adaptar su método para dividir también polinomios. No hay ninguna diferencia esencial.

Es importante que para poder dividir polinomios el divisor debe tener coeficiente director unitario. En particular podemos dividir siempre entre polinomios mónicos. Cuando A es un cuerpo todos los coeficientes son unidades, luego se pueden dividir polinomios cualesquiera. Como en este caso el grado del producto es la suma de los grados, tenemos todas las condiciones exigidas en la definición de dominio euclídeo, es decir:

Teorema 2.18 *Si K es un cuerpo, entonces el anillo de polinomios $K[x]$ es un dominio euclídeo.*

Sin embargo esto es falso si K no es un cuerpo. Por ejemplo $\mathbb{Z}[x]$ no es un dominio euclídeo. Tampoco es cierto en anillos de polinomios con más de una indeterminada, por ejemplo $\mathbb{Q}[x, y]$ no es un dominio euclídeo. Estos hechos los probaremos en el capítulo siguiente. Es interesante notar que en estos momentos no tenemos idea de cómo puede probarse la no existencia de una norma euclídea. Si bien la teoría que estamos desarrollando ha surgido para resolver una serie de problemas anteriores a ella misma, estamos ante un ejemplo (a un nivel muy simple) de cómo cada teoría plantea de forma natural nuevos problemas a la vez que resuelve otros, problemas que nunca se hubieran podido formular fuera del contexto creado por ella.

Capítulo III

Ideales

En los capítulos anteriores hemos introducido los que van a ser por ahora nuestros objetos de estudio principales: los números enteros y racionales y sus anillos de polinomios. Ahora vamos a introducir un concepto que ha resultado ser fundamental en el estudio de éstos y otros anillos relacionados. Se trata del concepto de ideal. Por razones que luego podremos entrever, el concepto de ideal surgió con cierto retraso en el estudio de los números. Nosotros lo introducimos desde un principio porque, dada su importancia, conviene familiarizarse con él cuanto antes. Sin embargo, para evitar un grado de abstracción que todavía no podemos justificar, aquí nos limitaremos a ver las mínimas ideas que nos puedan ser útiles de momento.

3.1 Ideales en un dominio

Definición 3.1 Un ideal en un dominio[1] A es un conjunto $I \subset A$ que cumpla las propiedades siguientes:

1. $0 \in I$,
2. si a, $b \in I$, entonces $a + b \in I$,
3. si $a \in A$ y $b \in I$ entonces $ab \in I$.

Todo anillo tiene al menos dos ideales, a saber, $\{0\}$ y el propio A. Se les llama ideales *impropios.* El ideal $\{0\}$ es el ideal *trivial* y se representa simplemente por 0.

Una observación trivial es que si un ideal I de dominio A contiene una unidad u, entonces $I = A$. En efecto, por definición de ideal se cumple que $1 = u^{-1}u \in I$ y si $a \in A$, entonces $a = a1 \in I$, es decir, todo elemento de A está en I.

[1]La definición es válida para anillos (unitarios) arbitrarios sin más que añadir que también $ba \in I$ en la propiedad 3.

Por lo tanto los únicos ideales de un cuerpo son los impropios, pues si un ideal de un cuerpo posee un elemento no nulo, será una unidad, y el ideal será el cuerpo completo.

Definición 3.2 Es inmediato que la intersección de una familia de ideales de un anillo A sigue siendo un ideal de A. Por lo tanto si $X \subset A$, existe un mínimo ideal de A que contiene a X, a saber, la intersección de todos los ideales de A que contienen a X (existe al menos uno, el propio A). Lo llamaremos *ideal generado* por X y lo representaremos por (X). También se dice que el conjunto X es un *generador* del ideal (X).

Así, para todo subconjunto X de A tenemos que (X) es un ideal de A, $X \subset (X)$ y si I es un ideal de A tal que $X \subset I$, entonces $(X) \subset I$. Otro hecho obvio es que si $X \subset Y \subset A$, entonces $X \subset (Y)$, luego $(X) \subset (Y)$.

Cuando el conjunto X es finito, $X = \{x_1, \ldots, x_n\}$, el ideal generado por X se representa por $(x_1, \ldots, x_n)$. Entonces se dice que el ideal está *finitamente generado.*

El teorema siguiente nos da la forma de los elementos de un ideal a partir de sus generadores.

Teorema 3.3 *Sea A un dominio y $X \subset A$. Entonces*

$$(X) = \{a_1x_1 + \cdots + a_nx_n \mid n \in \mathbb{N}, a_i \in A, x_i \in X\}$$

En particular si $x \in A$, entonces $(x) = \{ax \mid a \in A\}$.

Demostración: Se comprueba sin dificultad que el conjunto de la derecha es un ideal de A y claramente contiene a X, luego

$$(X) \subset \{a_1x_1 + \cdots + a_nx_n \mid n \in \mathbb{N}, a_i \in A, x_i \in X\}.$$

Por otra parte (X) ha de contener a los elementos de la forma ax, con x en X, y por ser un subanillo a las sumas de estos elementos, luego se da la igualdad.

Si X tiene un sólo elemento x, las sumas $\sum_{i=1}^n a_ix = (\sum_{i=1}^n a_i)\, x$ están en $\{ax \mid a \in A\}$, luego $(X) \subset \{ax \mid a \in A\}$. La otra inclusión es obvia. ∎

Entre los ideales de un anillo se puede definir una suma y un producto como sigue:

Definición 3.4 Sea A un anillo y sean $S_1, \ldots, S_n$ subconjuntos de A. Llamaremos

$$\begin{aligned} S_1 + \cdots + S_n &= \{s_1 + \cdots + s_n \mid s_i \in S_i \text{ para } \ i = 1, \ldots, n\} \\ S_1 \cdots S_n &= \Big\{\sum_{i=1}^m s_{i1} \cdots s_{in} \mid m \in \mathbb{N} \text{ y } s_{ij} \in S_j \text{ para } j = 1, \ldots, n\Big\} \end{aligned}$$

Es pura rutina comprobar que la suma y el producto de ideales de A vuelve a ser un ideal de A. Además son operaciones asociativas, conmutativas y distributivas, es decir, $P(Q + R) = PQ + PR$. De la definición de ideal se sigue que $PQ \subset P \cap Q$.

3.2 Dominios de ideales principales

Definición 3.5 Un ideal de un dominio A es *principal* si está generado por un solo elemento, es decir, si es de la forma $(a) = aA = \{ab \mid b \in A\}$.

Un *dominio de ideales principales* (DIP) es un dominio íntegro en el que todo ideal es principal.

Teorema 3.6 *Todo dominio euclídeo es un dominio de ideales principales.*

Demostración: Sea A un dominio euclídeo y sea $\phi : A \setminus \{0\} \longrightarrow \mathbb{N}$ su norma euclídea. Sea $I \neq 0$ un ideal de A (si $I = 0$ ya es principal).

Sea $a \in I$ tal que $\phi(a)$ sea el mínimo del conjunto $\{\phi(b) \mid b \in I, b \neq 0\}$.

Si $b \in I$, entonces $b = ac + r$, para $r = 0$ o bien $\phi(r) < \phi(a)$. Como $a \in I$, por la definición de ideal $ac \in I$, y como I es un subanillo, también $b - ac \in I$, es decir, $r \in I$. Como $\phi(a)$ es mínimo, no puede ser $\phi(r) < \phi(a)$, luego $r = 0$, es decir, $b = ac \in Aa$.

Hemos probado que $I \subset Aa$. Como $a \in I$, la otra inclusión es consecuencia de la definición de ideal. Por tanto $I = aA$ es un ideal principal. ∎

En particular tenemos que $\mathbb{Z}$ es un DIP, es decir, los únicos ideales de $\mathbb{Z}$ son los de la forma $n\mathbb{Z}$, para $n \in Z$. También son DIP los anillos $K[x]$, donde K es un cuerpo.

Como los cuerpos no tienen más ideales que los impropios, y éstos son principales, $(0 = (0), A = (1))$, resulta que los cuerpos son trivialmente DIPs. (Alternativamente, sabemos que los cuerpos son dominios euclídeos.)

El hecho de que los anillos más importantes sean DIPs es la explicación de que el concepto de ideal tardara en surgir en teoría de números. Cualquier afirmación sobre ideales en un DIP puede reformularse como una afirmación sobre los elementos del anillo, pues cada ideal está determinado por su generador. No obstante hay anillos que no son DIP, y al estudiarlos conviene saber cuántas cosas son ciertas para ideales en general aunque no sean principales. De hecho, en ciertos casos de interés, resultados que en DIPs pueden formularse con elementos y con ideales, son falsos en otros anillos en términos de elementos, pero siguen siendo ciertos en términos de ideales.

Vamos a ver unos ejemplos de dominios íntegros que no son DIPs.

Teorema 3.7 *Sea A un dominio íntegro. Entonces $A[x]$ es DIP si y sólo si A es un cuerpo.*

Demostración: Si A es un cuerpo sabemos que $A[x]$ es un dominio euclídeo, luego es un DIP. Recíprocamente, si $A[x]$ es DIP, sea $a \in A$ un elemento no nulo y veamos que es una unidad en A. Para ello consideramos el ideal (x, a) de $A[x]$. Como ha de ser un ideal principal existe un polinomio $p \in A[x]$ tal que $(x, a) = (p)$, luego $a = pq$ para cierto $q \in A[x]$, pero entonces $\operatorname{grad} p + \operatorname{grad} q = \operatorname{grad} a = 0$, luego $\operatorname{grad} p = 0$ y por tanto $p \in A$. Por otra parte también $x = pr$, para cierto $r \in A[x]$, pero entonces el coeficiente director de x, que es 1,

es el producto de p por el coeficiente director de r, luego p es una unidad y $(p) = A[x]$.

Entonces $1 \in (p) = (x, a)$, luego $1 = ux + va$, para ciertos polinomios $u, v \in A[x]$. Sin embargo el término independiente de ux es 0 y el de va es ba, donde b es el término independiente de v. Resulta, pues, que $1 = ba$, con lo que a es una unidad en A. ∎

Esto nos da muchos ejemplos de dominios íntegros que no son DIP (ni por tanto euclídeos). A saber, $\mathbb{Z}[x]$ y más en general $A[S]$ cuando el cardinal de S es mayor que 1 (pues $A[S] = A\big[S \setminus \{x\}\big][x]$ y $A[S \setminus \{x\}]$ no es un cuerpo).

Ejercicio: Probar que $(x, 2)$ no es un ideal principal de $\mathbb{Z}[x]$, y que (x, y) no es un ideal principal de $\mathbb{Q}[x, y]$.

3.3 Anillos noetherianos

Para acabar el capítulo vamos a definir una clase de anillos más general que la de los DIPs y que jugará un papel relevante en el próximo capítulo.

Definición 3.8 Un dominio íntegro A es un anillo *noetheriano* si todo ideal de A es finitamente generado.

Evidentemente, todo DIP es un anillo noetheriano.

Teorema 3.9 *Sea A un dominio íntegro. Son equivalentes:*

1. *A es un anillo noetheriano.*
2. *Para toda cadena ascendente de ideales de A*

$$I_0 \subset I_1 \subset I_2 \subset I_3 \subset \ \ldots$$

existe un número natural n tal que $I_n = I_m$ para todo $m \geq n$.

3. *Toda familia de ideales de A tiene un maximal para la inclusión.*

Demostración: Si $I_0 \subset I_1 \subset I_2 \subset I_3 \subset \ \ldots$ es una cadena ascendente de ideales de A, es fácil ver que la unión $\bigcup_{i=0}^{\infty} I_i$ es también un ideal de A. Si A es noetheriano ha de tener un generador finito X. Cada elemento de X está en uno de los ideales I_i, y como X es finito y los ideales forman una cadena, existirá un natural n tal que $X \subset I_n$, pero entonces $\bigcup_{i=0}^{\infty} I_i = (X) \subset I_n$, lo que implica que $I_i = I_n$ para todo $i \geq n$. Por tanto 1) implica 2).

Si una familia de ideales de A no tuviera maximal, sería posible extraer una cadena ascendente de ideales que contradijera 2), luego 2) implica 3).

Si A tuviera un ideal I que no admitiera un generador finito, entonces, dado cualquier elemento a_0 de I, se cumple que $(a_0) \neq I$, luego existe un elemento $a_1 \in I \setminus (a_0)$, luego $(a_0) \subset (a_0, a_1) \neq I$, y de esta forma podemos conseguir una cadena de ideales

$$(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \ldots$$

sin que ninguno de ellos sea maximal. Por lo tanto 3) implica 1). ∎

Capítulo IV

Divisibilidad en dominios íntegros

El concepto de divisibilidad es uno de los más importantes en el estudio de los números. A partir de él se plantean los más interesantes y variados problemas cuyo estudio ha ocupado a los matemáticos durante milenios. Aquí desarrollaremos la teoría básica al respecto. En capítulos posteriores profundizaremos más en ella.

4.1 Conceptos básicos

Definición 4.1 Sea A un dominio íntegro y a, b dos elementos de A. Diremos que a *divide* a b, o que a es un *divisor* de b, o que b es un *múltiplo* de a (y lo representaremos $a \mid b$) si existe un elemento c de A tal que $b = ac$.

Por ejemplo en $\mathbb{Z}$ es fácil ver que 3 divide a 15, pero no a 16.

Es obvio que si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

Si u es una unidad, cualquier elemento a de A se expresa como $a = u(u^{-1}a)$, luego las unidades dividen a todo elemento de A. Por otra parte si u es una unidad y $a \mid u$, entonces existe un b en A tal que $u = ab$, luego $1 = abu^{-1}$, es decir, a es una unidad. En otras palabras, los divisores de las unidades son las unidades.

Por el contrario 0 no divide a nadie salvo a sí mismo.

Diremos que dos elementos a y b de A son *asociados* si $a \mid b$ y $b \mid a$. Por ejemplo en $\mathbb{Z}$ se cumple que 3 y -3 son asociados. Ser asociado es una relación de equivalencia. Si dos elementos son asociados tienen los mismos múltiplos y divisores.

La asociación está estrechamente relacionada con la existencia de unidades. En efecto, si a y b son asociados no nulos, entonces $a = ub$ y $b = va$, para ciertos u y v del anillo A. Por lo tanto $a = uva$, de donde $uv = 1$, o sea, u y v son unidades. Así pues, si dos elementos son asociados, uno se obtiene del otro

multiplicándolo por una unidad. El recíproco es cierto, como es fácil observar. Además, cuando un mismo elemento no nulo se multiplica por unidades distintas obtenemos elementos distintos, luego un elemento no nulo de A tiene tantos asociados como unidades hay en A. Como $\mathbb{Z}$ tiene dos unidades, los asociados en $\mathbb{Z}$ forman parejas, salvo el cero, que es su único asociado.

Tenemos, pues, que todo elemento de A tiene por divisores a las unidades de A y a sus propios asociados (entre los que está él mismo). A estos divisores los llamaremos *divisores impropios* de a. Cualquier otro divisor es un *divisor propio.* Por ejemplo, los divisores impropios de 4 en $\mathbb{Z}$ son 1, -1, 4 y -4. Sus divisores propios son 2 y -2.

Estas consideraciones nos llevan al concepto de elemento irreducible: Un elemento a de un dominio íntegro A es *irreducible* en A si es no nulo, no es una unidad y no admite ninguna descomposición $a = bc$ con b y c elementos de A, salvo que uno de ellos sea una unidad (y, por lo tanto, el otro es un asociado de a).

Equivalentemente, un elemento (no nulo ni unidad) es irreducible si sus únicos divisores son los impropios. También es obvio que un elemento es irreducible si y sólo si lo es cualquiera de sus asociados.

Por ejemplo, es fácil ver que los únicos divisores de 5 en $\mathbb{Z}$ son 1, -1, 5 y -5, lo que implica que 5 es irreducible en $\mathbb{Z}$. En cambio 15 no es irreducible, pues factoriza como $15 = 3 \cdot 5$.

Si un número entero (no nulo ni unidad) no es irreducible, entonces factoriza como producto de dos enteros estrictamente menores en módulo. Si éstos no son irreducibles factorizarán a su vez en factores menores, y este proceso tiene que acabar antes o después, por lo que todo número entero se puede expresar como producto de irreducibles. Más aún, puede probarse que esta descomposición es esencialmente única. Para formular esto con precisión y en términos aplicables a otros casos (como por ejemplo a polinomios), conviene introducir el concepto siguiente:

Un dominio íntegro A es un *dominio de factorización única* (DFU) si todo elemento a de A no nulo y que no sea una unidad se descompone como producto de elementos irreducibles $a = c_1 \cdots c_n$ y la descomposición es única salvo ordenación o cambio por asociados (es decir, si $a = c_1 \cdots c_n = d_1 \cdots d_m$ son dos descomposiciones de a en elementos irreducibles, entonces $m = n$ y, ordenando los factores adecuadamente, cada c_i es asociado a d_i).

No es difícil probar por métodos elementales que $\mathbb{Z}$ es un DFU. Por ejemplo la factorización única de 140 es $140 = 2 \cdot 2 \cdot 5 \cdot 7 = (-5) \cdot 2 \cdot 7 \cdot (-2) = \cdots$ Sin embargo vamos a probar más en general que todo DIP es un DFU. Esto lo veremos en la sección siguiente. Acabaremos ésta con algunas consideraciones adicionales sobre DFUs que nos ayudarán a familiarizarnos con ellos.

Si A es un DFU y a es un elemento no nulo ni unitario, para cada elemento irreducible p de A llamaremos *exponente* de p en a al número de veces que p o sus asociados aparecen en cualquier descomposición de a en factores irreducibles

(puede ser igual a 0). Lo denotaremos por $e_p(a)$. En una descomposición de a aparecerán $e_p(a)$ factores asociados a p, es decir, factores de la forma up donde u es una unidad. Si multiplicamos todas las unidades que así aparecen, resulta que a admite una descomposición en la forma $a = u \cdot p_1^{n_1} \cdots p_n^{n_m}$, donde los p_i son irreducibles distintos, $n_i = e_{p_i}(a)$ y u es una unidad. La presencia de u es necesaria, pues por ejemplo la única forma de factorizar en $\mathbb{Z}$ el -25 de este modo es $-25 = (-1)5^2$. Lo importante es que cada p aparece siempre con exponente $e_p(a)$ en virtud de la unicidad de la factorización.

Además el exponente de un irreducible en un elemento a es por definición el mismo que el de sus asociados, y el exponente de un irreducible en un elemento a es el mismo que en los asociados de a (pues una factorización de un asociado de a se obtiene multiplicando una factorización de a por una unidad, sin cambiar los irreducibles).

La factorización en irreducibles de un producto puede obtenerse como el producto de las factorizaciones de los factores, de donde se sigue la relación $e_p(ab) = e_p(a) + e_p(b)$.

Podemos definir $e_p(a) = 0$ para todo irreducible p cuando a es una unidad y así la relación anterior es válida también si a o b es una unidad.

Notar también que un irreducible p divide a un elemento a si y sólo si $e_p(a) \neq 0$. En efecto, si $e_p(a) \neq 0$ eso significa que p aparece en una factorización de a, luego $p \mid a$. Por otra parte si $p \mid a$, entonces $a = pb$ para cierto elemento b, luego $e_p(a) = e_p(p) + e_p(b) = 1 + e_p(b) \neq 0$.

Si $a \mid b$, ha de cumplirse que $e_p(a) \leq e_p(b)$ para todo irreducible p de A. La condición es también suficiente, pues si se cumple esto, entonces b se obtiene como producto de a por el producto de todos los irreducibles p que dividen a b elevados al exponente $e_p(b) - e_p(a)$ (y una unidad adecuada). Dos elementos a y b son asociados si y sólo si $e_p(a) = e_p(b)$ para todo irreducible p de A.

Como consecuencia de estos hechos tenemos que en un DFU, si p es irreducible y $p \mid ab$, entonces $p \mid a$ o $p \mid b$. En efecto, estamos suponiendo que $0 \neq e_p(a) + e_p(b)$, luego una de los dos exponentes ha de ser no nulo.

Este hecho resulta ser muy importante en la teoría de la divisibilidad, hasta el punto de que conviene introducir un nuevo concepto para comprenderlo adecuadamente:

Si A es un dominio íntegro, un elemento p de A es *primo* si es no nulo, no es una unidad y cuando $p \mid ab$ entonces $p \mid a$ o $p \mid b$ para todos los elementos a y b de A.

Ya hemos probado la mitad del siguiente teorema fundamental:

Teorema 4.2 *Sea A un dominio íntegro*

1. *Todo primo de A es irreducible.*
2. *Si A es DFU, entonces un elemento de A es primo si y sólo si es irreducible*

Demostración: Efectivamente, si p es primo y se descompone como $p = ab$, entonces $p \mid a$ o $p \mid b$, pero como $a \mid p$ y $b \mid p$, lo que tenemos es que p es asociado

con a o con b, lo que implica que el otro es una unidad. La segunda afirmación ya está probada. ∎

4.2 Ideales y divisibilidad

Aunque todavía no estamos en condiciones de comprender enteramente por qué, lo cierto es que los ideales proporcionan el lenguaje idóneo para expresar los hechos más relevantes de la divisibilidad en un anillo. En primer lugar hemos de notar que si a es un elemento de un dominio íntegro A, entonces el ideal $(a) = Aa$ es precisamente el conjunto de todos los múltiplos de a. Es claro que $a \mid b$ equivale a $(b) \subset (a)$, de donde se sigue que a y b son asociados si y sólo si $(a) = (b)$, es decir, si y sólo si generan el mismo ideal.

Hemos de pensar que dos elementos asociados son una misma cosa a efectos de divisibilidad (ambos tienen los mismos múltiplos y divisores). Ahora vemos que a cada familia de elementos asociados de un dominio íntegro le corresponde un único ideal principal. En particular el 0 se corresponde con el ideal $0 = (0)$ y las unidades de A se corresponden todas ellas con el ideal $A = (1)$.

El lector que quiera comprender adecuadamente la teoría de la divisibilidad debe esforzarse por llegar a entender que los ideales principales representan mejor que los elementos mismos del anillo los posibles divisores de un elemento dado. Quizá en esta dirección le ayude conocer un débil esbozo informal del modo en que el concepto de ideal era concebido cuando apareció en la teoría:

Consideremos las dos afirmaciones siguientes relativas a $\mathbb{Z}$. Por una parte $2 \mid 6$ y por otra $-2 \mid 6$. A efectos de divisibilidad ambas son equivalentes, puesto que 2 y -2 son asociados. Podemos resumirlas en una sola si consideramos que es el ideal $(2) = (-2)$ el que divide a 6, y escribimos en consecuencia $(2) \mid 6$. Podemos pensar que los divisores de los elementos de un dominio íntegro no son otros elementos del anillo, sino sus ideales. Así, podemos definir $(a) \mid b$ como $a \mid b$, lo cual no depende del generador elegido para el ideal, pues dos cualesquiera son asociados. Notar que esto equivale a que $b \in (a)$, luego si I es un ideal principal tenemos (por definición) que $I \mid b \Leftrightarrow b \in I$. Lo que hace de esto una idea brillante es que en realidad no tenemos por qué exigir a I que sea principal, con lo que cualquier ideal I puede dividir a un elemento en este sentido. En un DIP cada 'divisor ideal' se corresponde con una familia de 'divisores reales' asociados (sus generadores), pero hay anillos no DIP en los que se puede hablar coherentemente de divisores ideales en este sentido sin que estén asociados a divisores reales, es decir, sin que sean principales. Tales 'divisores ideales' resultan esenciales para formular una teoría de divisibilidad razonable (y útil) en dichos anillos. De hecho, los ideales en el sentido moderno fueron introducidos por Dedekind a finales del siglo XIX para formalizar esta idea de divisor ideal que no se corresponde con ningún divisor real.

Más en general, podemos extender la relación de divisibilidad de modo que los ideales puedan dividirse entre sí. Podemos pensar que un ideal I divide a un ideal J si $J \subset I$ (comparar con $a \mid b \Leftrightarrow (b) \subset (a)$). De momento no entraremos

en la teoría de divisores ideales. Nos limitaremos a desarrollar la teoría de divisibilidad en dominios íntegros mostrando su conexión con los ideales del anillo. El lector debe tener presente que esta conexión se volverá esencial en capítulos posteriores, por lo que debe acostumbrarse a pensar e interpretar las cosas en términos de ideales en la medida de lo posible.

Como primer ejemplo del paso a términos de ideales, veamos el equivalente del concepto de elemento primo:

Definición 4.3 Un ideal P de un anillo A es *primo* si $P \neq A$ y para todo par de ideales I, J de A tales que $IJ \subset P$, se cumple que $I \subset P$ o $J \subset P$.

Si tenemos *in mente* la equivalencia $I \mid J \Leftrightarrow J \subset I$ vemos que la definición de ideal primo es paralela a la de elemento primo. La condición $P \neq A$ se corresponde con la exigencia de que los primos no sean unidades. Hay, no obstante, una discrepancia debida principalmente a motivos históricos, y es que, mientras hemos exigido que el elemento 0 no sea considerado primo, sí admitimos que el ideal 0 sea considerado primo. He aquí una caracterización práctica del concepto de ideal primo.

Teorema 4.4 *Si A es un dominio íntegro, un ideal P de A es primo si y sólo si $P \neq A$ y para todo par de elementos a, b de A, si $ab \in P$ entonces $a \in P$ o $b \in P$.*

Demostración: Si P es primo y $ab \in P$, entonces $(a)(b) \subset (ab) \subset P$, de donde resulta que $(a) \subset P$ o $(b) \subset P$, o sea, $a \in P$ o $b \in P$.

Recíprocamente, si $IJ \subset P$, pero I no está contenido en P, entonces existe un $a \in I \setminus P$. Ahora, si $b \in J$ tenemos que $ab \in IJ \subset P$, luego $a \in P$ o $b \in P$, y ha de ser $b \in P$, es decir, $J \subset P$. ∎

Ahora es inmediato que en un dominio íntegro A se cumple que un elemento no nulo a es primo si y sólo si el ideal (a) es un ideal primo. No obstante recordamos que el ideal trivial (0) es primo, aunque el elemento 0 no lo es por definición. Si un elemento es irreducible cuando no tiene divisores propios, el concepto análogo para ideales es el siguiente:

Definición 4.5 Un ideal M de un anillo A es un ideal *maximal* si $M \neq A$ y si I es un ideal de A tal que $M \subset I \subset A$, entonces $M = I$ o $I = A$.

Como en el caso de ideales primos, estamos admitiendo la posibilidad de que el ideal 0 sea maximal (si bien no tiene por qué serlo necesariamente).

La existencia de ideales maximales en cualquier anillo conmutativo y unitario A está garantizada por el lema de Zorn. Más aún, todo ideal distinto de A está contenido en un ideal maximal (la familia de ideales distintos de A que contienen a un ideal está ordenada por la inclusión, y todo subconjunto totalmente ordenado tiene una cota superior, pues la unión de una cadena de ideales es claramente un ideal, además es un ideal distinto de A porque no puede contener a la identidad). No vamos a necesitar esto de momento.

Al contrario de lo que ocurre con el concepto de 'primo', no es cierto que un elemento a de un dominio íntegro A sea irreducible si y sólo si el ideal (a) es maximal. La situación es un poco más delicada. Concretamente a es irreducible si y sólo si (a) es maximal entre los ideales principales, es decir, si $(a) \neq A$ y cuando $(a) \subset (b) \subset A$, entonces $(a) = (b)$ o $(b) = A$.

En efecto, si a es irreducible y $(a) \subset (b) \subset A$, entonces $b \mid a$, luego o bien b es una unidad (y entonces $(b) = A$) o bien b es asociado de a (con lo que $(b) = (a)$). El recíproco es igual. Por lo tanto tenemos:

Teorema 4.6 *Sea A un dominio íntegro y $a \neq 0$ un elemento de A.*

1. *a es primo si y sólo si (a) es primo.*
2. *a es irreducible si y sólo si (a) es maximal entre los ideales principales de A.*
3. *Si A es DIP, entonces a es irreducible si y sólo si (a) es maximal.*

La tercera afirmación es inmediata, pues en un DIP los ideales maximales coinciden con los ideales maximales entre los ideales principales.

Hemos visto que todo elemento primo de un anillo es irreducible. Entre ideales podemos demostrar justo la implicación contraria:

Teorema 4.7 *En un dominio, todo ideal maximal es primo.*

Demostración: Si M es un ideal maximal en A y $ab \in M$, pero $a, b \notin M$, tendríamos que $M \subsetneq M + (a) \subset A$, luego la maximalidad de M implica que $M + (a) = A$. Por lo tanto $1 = m + xa$ para cierto $m \in M$ y cierto $x \in A$. Así pues $b = mb + xab \in M$, con lo que tenemos una contradicción. ∎

Ahora estamos en condiciones de probar dos hechos clave.

Teorema 4.8 *En un DIP los ideales maximales coinciden con los ideales primos y los elementos irreducibles coinciden con los elementos primos.*

Demostración: Si A es un DIP y (a) es un ideal primo no trivial, supongamos que (b) es un ideal tal que $(a) \subset (b) \subset A$. Entonces $a = bc$ para cierto $c \in A$. Como (a) es primo se ha de cumplir o bien $b \in (a)$ (en cuyo caso $(a) = (b)$) o bien $c \in (a)$, en cuyo caso $c = da$ para cierto $d \in A$, y así $a = bc = bda$, luego (dado que $a \neq 0$), $bd = 1$, o sea, b es una unidad y por lo tanto $(b) = A$.

La segunda afirmación se sigue de la primera y de 4.6 ∎

Con esto podemos probar el resultado principal de esta sección. Diremos que un dominio íntegro A tiene la *propiedad de factorización* si todo elemento de A no nulo ni unidad se descompone en producto de irreducibles.

Teorema 4.9 *Todo anillo noetheriano A tiene la propiedad de factorización. Si además todo elemento irreducible de A es primo, entonces A es DFU. En particular todo DIP es DFU.*

DEMOSTRACIÓN: Sea A un anillo noetheriano. Llamemos S al conjunto de los elementos de A no nulos ni unidades pero que no admitan una descomposición en irreducibles. Hemos de probar que S es vacío.

Si existe un elemento a en S, entonces a no es unidad, luego $(a) \neq A$. Si a fuera irreducible entonces él mismo sería una descomposición en irreducibles, luego no lo es. Podemos factorizar $a = bc$ donde ni b ni c es una unidad (ni 0). Si ninguno estuviera en S entonces se descompondrían en producto de irreducibles, y a también. Por tanto al menos uno de los dos está en S. Digamos que $b \in S$. Como $b \mid a$ se cumple que $(a) \subset (b)$. La inclusión es estricta, pues si $(a) = (b)$ entonces a y b serían asociados, es decir, $a = bu$ para cierta unidad u, pero entonces $bu = bc$, luego $c = u$ sería una unidad, cuando no lo es.

En definitiva hemos probado que para cada $a \in S$ existe un $b \in S$ tal que $(a) \subsetneq (b)$. Repitiendo este proceso obtendríamos una sucesión creciente de ideales $(a_o) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$ en contradicción con el teorema 3.9. Por lo tanto S ha de ser vacío y así todo elemento no nulo ni unitario de A admite una descomposición en irreducibles.

Supongamos que los irreducibles coinciden con los primos y que tenemos dos descomposiciones en irreducibles de un mismo elemento $a = c_1 \cdots c_n = d_1 \cdots d_m$. Podemos suponer que $m \leq n$.

Como d_m es primo, ha de dividir a uno de los factores de $c_1 \cdots c_n$ y como éstos son irreducibles, de hecho ha de ser asociado a uno de ellos. Pongamos que d_m es asociado a c_n. Entonces $c_n = u_m d_m$ para cierta unidad u_m.

Simplificando d_m obtenemos que $c_1 \cdots c_{n-1} u_m = d_1 \cdots d_{m-1}$. Repitiendo el proceso con d_{m-1} (y teniendo en cuenta que un irreducible no puede dividir a una unidad), llegamos tras m pasos a que $c_1 \cdots c_{n-m}\, u_1 \cdots u_m = 1$, lo que obliga a que $n = m$, pues ningún irreducible puede dividir a 1. Además hemos obtenido que cada c_i es asociado a d_i, luego la descomposición es única. ∎

Con esto tenemos probada la factorización única de $\mathbb{Z}$ y de los anillos $K[x]$ donde K es un cuerpo. Para el caso de $\mathbb{Z}$ es posible dar argumentos directos más elementales basados en el buen orden de $\mathbb{N}$. Por ejemplo, para encontrar un factor irreducible de un número entero basta tomar el menor natural que lo divide. Lo mismo ocurre con $K[x]$ considerando el grado de los polinomios.

4.3 Divisibilidad en $\mathbb{Z}$

En $\mathbb{Z}$ podemos afinar la unicidad de la descomposición en factores primos exigiendo que éstos sean positivos, es decir, números naturales. Así, la descomposición en primos del número 60 es $60 = 2 \cdot 2 \cdot 3 \cdot 5$, y no consideraremos otras como $2 \cdot 2 \cdot (-3) \cdot (-5)$. Si no se indica lo contrario, cuando hablemos de primos en $\mathbb{Z}$ nos referiremos a naturales primos.

El problema más elemental que surge a raíz de todo esto es encontrar un método para obtener las factorizaciones en primos de números cualesquiera. En particular sería conveniente hallar un método para reconocer los números primos. El método más simple para hallar todos los primos hasta un número dado es la llamada *criba de Eratóstenes,* que consiste en escribir una lista con

los primeros n naturales, tachar el 1, que no es primo por definición, después tachar todos los múltiplos de 2 (salvo el propio 2), dejar el menor número que queda (el 3) y tachar sus múltiplos, dejar el menor número que queda (el 5) y tachar sus múltiplos, etc. Los números que sobrevivan serán los primos menores que n. He aquí la lista de los primos menores que 100, que hacen un total de 25.

$$2,\quad 3,\quad 5,\quad 7,\quad 11,\quad 13,\quad 17,\quad 19,\quad 23,\quad 29,\quad 31,\quad 37,\quad 41,$$

$$43,\quad 47,\quad 53,\quad 59,\quad 61,\quad 67,\quad 71,\quad 73,\quad 79,\quad 83,\quad 89,\quad 97.$$

Para descomponer un número en factores primos podemos ir probando a dividirlo por los primos menores que él hasta hallar uno que lo divida e ir repitiendo la operación con los cocientes que vayamos obteniendo. Notar que si queremos factorizar un número n y m cumple que $n \leq m^2$, entonces, si n no es primo, el menor primo que divide a n ha de ser menor que m. Por ejemplo, el menor primo que divida a un número menor que 100 ha de ser menor que 10, es decir, si un número menor que 100 no es divisible entre 2, 3, 5 o 7, entonces es primo.

En cualquier caso, siempre es posible distinguir los números primos de los compuestos y hallar la factorización de cualquier número en un número finito de pasos. Más adelante encontraremos técnicas para abordar este problema con más elegancia.

Una cuestión importante es si el número de primos es finito o infinito. La respuesta es que es infinito. Para probarlo observemos que en general un primo p no puede dividir al mismo tiempo a un número n y a $n+1$, pues entonces dividiría a su diferencia, que es 1. De hecho, en $\mathbb{Z}$, si p divide a n, el próximo número al que divide es $n+p$. Sabiendo esto demostramos:

Teorema 4.10 *(Euclides): En $\mathbb{Z}$ hay infinitos números primos.*

DEMOSTRACIÓN: Dado un número n consideremos $n!$ Se cumple que todo número menor o igual que n divide a $n!$, luego ningún número menor o igual que n divide a $n!+1$. En consecuencia un divisor primo de $n!+1$ ha de ser mayor que n. Por lo tanto por encima de cada número n hay siempre un número primo. Esto implica que hay infinitos primos. ∎

Definición 4.11 Sea A un dominio íntegro y X un subconjunto de A. Diremos que un elemento d de A es un *máximo común divisor* (mcd) de los elementos de X si d divide a los elementos de X y cualquier elemento de A que cumpla lo mismo es un divisor de d.

Diremos que un elemento m de A es un *mínimo común múltiplo* (mcm) de los elementos de X si es múltiplo de todos los elementos de X y todo elemento de A que cumpla lo mismo es un múltiplo de m.

Es obvio que m es un mcd o un mcm de X si y sólo si lo es cualquiera de sus asociados, es decir, estos conceptos son únicos salvo unidades. Por supuesto

el mcd o el mcm de un conjunto dado no tiene por qué existir. No obstante, cualquier subconjunto finito de un DFU tiene mcd y mcm. El lector puede entretenerse probando que las siguientes "recetas" nos dan un mcd y un mcm de cualquier subconjunto finito X de un DFU.

Un mcd de X está formado por el producto de los primos que dividen a todos los elementos de X elevados al mínimo exponente con el que aparecen en alguno de los elementos de X.

Un mcm de X está formado por el producto de todos los primos que dividen a algún elemento de X elevados al mayor exponente con el que aparecen en los elementos de X.

Por ejemplo, dados los números $2^2 \cdot 3 \cdot 7^5$, $2 \cdot 5 \cdot 7$, $3^4 \cdot 5^2 \cdot 7$, el mcd es 7 y el mcm es $2^2 \cdot 3^4 \cdot 5^2 \cdot 7^5$.

Escribiremos $\text{mcd}(a_1, \ldots, a_n)$ y $\text{mcm}(a_1, \ldots, a_n)$ para representar el mcd y el mcm de los elementos $a_1, \ldots, a_n$. A veces el mcd lo representaremos simplemente por $(a_1, \ldots, a_n)$.

En $\mathbb{Z}$ el mcd es único si lo exigimos positivo. Si no se indica lo contrario siempre lo supondremos así.

Hay que prestar un poco de atención al cero: por definición todo elemento de un anillo divide a 0, de donde se sigue fácilmente que el mcd de un conjunto de elementos que contenga a 0 es el mismo que el del conjunto que resulte de eliminarlo. Por otra parte si un conjunto de elementos contiene una unidad, su mcd es 1.

Los elementos de un conjunto son *primos entre sí* si su mcd es 1, es decir, si no tienen divisores primos comunes. No hay que confundir esto con que sean primos entre sí dos a dos, que es más fuerte. Si dividimos los elementos de un conjunto por su mcd obtenemos un conjunto de elementos primos entre sí, pues si d es el mcd y p es un primo que dividiera al conjunto resultante, entonces dp dividiría al conjunto original, luego $dp \mid d$ y p sería una unidad.

En un DIP el máximo común divisor de un conjunto finito de números cumple una propiedad muy importante:

Teorema 4.12 *(Relación de Bezout): Sea A un DIP y $a_1, \ldots, a_n$ elementos de A. Sea d un* mcd *de $a_1, \ldots, a_n$. Entonces $(d) = (a_1) + \cdots + (a_n)$, luego existen ciertos elementos $r_1, \ldots, r_n$ en A de manera que $d = r_1 a_1 + \cdots + r_n a_n$.*

DEMOSTRACIÓN: Sea $(d) = (a_1) + \cdots + (a_n)$ (por definición). Vamos a ver que d es un mcd de $a_1, \ldots, a_n$.

Como cada a_i está en (d), ciertamente $d \mid a_i$. Si s divide a todos los a_i, entonces $(a_i) \subset (s)$, luego $(d) = (a_1) + \cdots + (a_n) \subset (s)$, luego $s \mid d$.

Observemos que si d' es cualquier otro mcd de los elementos dados, entonces $(d') = (d)$, luego la relación de Bezout es válida para cualquiera de ellos. ∎

Este resultado se aplica especialmente a pares de elementos primos entre sí: si m y n son primos entre sí, existen r y s tales que $rm + sn = 1$.

4.4 Divisibilidad en anillos de polinomios

El estudio de la divisibilidad no es tan sencillo si pasamos a los anillos de polinomios $A[x]$. Tomemos unos cuantos polinomios y multipliquémoslos:

$$(x^2+3x-5)(x-1)(2x^3+3) = 2x^6+4x^5-16x^4+13x^3+6x^2-24x+15.$$

¿Cómo encontrar los factores a partir del producto? De hecho ni siquiera sabemos si los factores que hemos tomado son irreducibles o no (es costumbre hablar de números primos pero de polinomios irreducibles, aunque en principio son términos equivalentes). El problema es que, a diferencia del caso numérico, hay infinitos posibles divisores para un polinomio dado. No hay ningún criterio general para determinar si un polinomio dado es o no irreducible, aunque algo se puede decir sobre el tema. De todos modos, antes de entrar en ello tenemos planteado otro problema más importante. Sabemos que $A[x]$ es un DFU cuando A es un cuerpo, pero en otro caso $A[x]$ no es DIP. ¿Sigue siendo $A[x]$ un DFU a pesar de ello? ¿Es $\mathbb{Z}[x]$ DFU?, ¿Es $\mathbb{Q}[x,y]$ DFU? Vamos a probar que sí, para lo cual necesitamos un trabajo previo.

Si D es un DFU y K es su cuerpo de cocientes, vamos a probar que $D[x]$ es un DFU apoyándonos en que $K[x]$ lo es. La situación típica con la que tenemos que encontrarnos es la siguiente: El polinomio $6x^2-24$ factoriza en $\mathbb{Z}[x]$ como

$$6x^2-24 = 6(x^2-4) = 2\cdot 3\cdot (x-2)\cdot (x+2).$$

Vemos que tiene 4 divisores primos. Sin embargo, en $\mathbb{Q}[x]$ sólo tiene dos, pues los primeros factores pasan a ser unidades. Conviene dar la definición siguiente:

Definición 4.13 Sea D un DFU y sea $c : D[x] \longrightarrow D$ una aplicación que asigne a cada polinomio $f \in D[x]$ un mcd de sus coeficientes no nulos (y $c(0) = 0$). A $c(f)$ se le llama *contenido* del polinomio f.

Usaremos la notación $a \approx b$ para indicar que a y b son asociados. Es claro que si f es un polinomio no nulo y a es un mcd de sus coeficientes no nulos, entonces $a \approx c(f)$.

Diremos que un polinomio f es *primitivo* si $c(f)$ es una unidad, o sea, si sus coeficientes son primos entre sí. En particular, todo polinomio mónico es primitivo.

Por ejemplo, el contenido del polinomio $6x^2-24 \in \mathbb{Z}[x]$ es 6 (en $\mathbb{Z}[x]$ podemos elegir los contenidos naturales), mientras que el polinomio x^2-4 es primitivo. En general es inmediato que si $f \in D[x]$ y $f \neq 0$, entonces $f(x) = c(f)g(x)$ donde $g(x) \in D[x]$ es un polinomio primitivo. Así, para probar que todo polinomio $f(x) \in D[x]$ se descompone en irreducibles basta probar que podemos factorizar por una parte polinomios constantes y por otra polinomios primitivos.

La factorización de las constantes es obvia, puesto que estamos suponiendo que D es un DFU. Notemos que todo $a \in D$ es irreducible en D si y sólo si lo

es en $D[x]$. (Una descomposición de a en factores no unitarios de $D[x]$ tendría que constar de polinomios de grado 0, luego serían factores no unitarios de D, y el recíproco es obvio.)

Para probar que todo polinomio primitivo $p(x) \in D[x]$ se descompone en irreducibles observamos que los polinomios primitivos no son divisibles entre constantes no unitarias, ya que una constante que divida a $p(x)$ divide también a su contenido.

Así, si $p(x)$ (no unitario) no pudiera descomponerse en irreducibles en $D[x]$, en particular no sería irreducible, luego se descompondría en dos factores, digamos $p(x) = p_1(x)q_1(x)$, donde ninguno de los dos es una unidad, luego ambos tienen grado menor que el grado de $p(x)$. Al menos uno de los dos no podría descomponerse en irreducibles (digamos que $p_1(x)$), luego $p_1(x)$ no es irreducible y factoriza como $p_1(x) = p_2(x)q_2(x)$, donde ambos factores son no constantes, pues dividen a $p(x)$, luego el grado de $p_2(x)$ es menor que el de $p_1(x)$. De este modo obtenemos una sucesión de polinomios $p(x), p_1(x), p_2(x), \ldots$ cuyos grados son estrictamente decrecientes, lo cual es absurdo.

Con esto tenemos demostrado que todo polinomio de $D[x]$ no nulo ni unitario se descompone en producto de irreducibles. La parte delicada es demostrar la unicidad de la descomposición. La idea es usar la factorización única en D para probar la unicidad de los factores irreducibles constantes y la unicidad en $D[x]$ para probar la unicidad de los factores irreducibles no constantes. Necesitamos dos resultados sobre $c(f)$.

Teorema 4.14 *Sea D un DFU.*

1. *Si $a \in D$ y $f \in D[x]$, entonces $c(af) \approx a \cdot c(f)$.*
2. *Si f, $g \in D[x]$, entonces $c(fg) \approx c(f)c(g)$.*

Demostración: 1) Es inmediato que $a \cdot c(f)$ es un mcd de los coeficientes de af.

2) Sea $f = c(f)f_1$ y $g = c(g)g_1$ con f_1 y g_1 primitivos. Entonces $c(fg) = c\,(c(f)f_1 \cdot c(g)g_1) \approx c(f)c(g)c(f_1g_1)$, luego basta probar que $c(f_1g_1)$ es una unidad.

Sean $f_1 = \sum_{i=0}^{n} a_i x^i$, $g_1 = \sum_{i=0}^{m} b_i x^i$, con $a_n \neq 0 \neq b_m$.

Entonces $f_1 \cdot g_1 = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k$. Si $c(f_1g_1)$ no fuera una unidad en D, existiría un irreducible p tal que $p \mid c(f_1g_1)$.

Entonces $p \mid \sum_{i+j=k} a_i b_j$ para cada k entre 0 y $n+m$.

Como $c(f_1)$ es una unidad, p no divide a $c(f_1)$, luego existe un mínimo índice s tal que $p \mid a_i$ para $i < s$ y $p \nmid a_s$ (en particular $a_s \neq 0$).

Igualmente existe un mínimo índice t tal que $p \mid b_j$ para $j < t$ y $p \nmid b_t$ ($b_t \neq 0$).

Ahora, tomando $k = s + t$, resulta que p divide a $\sum_{i+j=k} a_i b_j$ y también divide a todos los sumandos salvo quizá a $a_s b_t$, de donde divide a la diferencia, o sea, a $a_s b_t$. Como p es primo divide a uno de los factores, lo que nos da una contradicción. ∎