Dominios y divisibilidad

Índice

1 Monoides 2

2 Monoides factoriales 7

3 Más ejemplos 15

4 Existencia y unicidad de factorizaciones 17

5 Máximo común divisor 19

6 Dominios de ideales principales 22

7 Polinomios sobre un DFU 26

Referencias 31

Introducción

El tema central de estas notas es el problema de divisibilidad o factorización en un dominio conmutativo. En pocas palabras, el objetivo será poner en un contexto general el siguiente resultado fundamental:

Teorema 0.1 (Teorema fundamental de la aritmética)**.** *Dado un número entero positivo m, no nulo y distinto de* 1*, existe una lista no vacía de primos positivos $p_1, \ldots, p_k$ tal que*

$$m = p_1 \cdots p_k \ . \tag{1}$$

La lista es única, salvo por el orden de los factores.

Que la lista sea no vacía quiere decir que $k \geq 1$. En (1), los factores p_i pueden aparecer repetidos, es decir, con multiplicidad. Esta expresión se denomina *factorización de m como producto de primos*. A veces, usamos el término "descomposición" en lugar de "factorización" y también diremos que (1) es la descomposición de m como producto de irreducibles.

En el anillo $\mathbb{Z}$ de enteros racionales, los conceptos de "número irreducible" y de "número primo" coinciden. Esto es cierto en cualquier dominio de factorización única.[1] Pero, a diferencia, de lo que ocurre con los enteros positivos, en general hay que tener en cuenta que una descomposición de la forma $a = b\,c$ puede variar de distintas maneras, no sólo en el orden de los factores. Esto se relaciona con la presencia de unidades en un dominio arbitrario. En $\mathbb{Z}$, las únicas unidades son $\{1, -1\}$, con lo que los primos racionales son los primos positivos 2, 3, 5, 7, ... y los correspondientes negativos -2, -3, -5, -7, ... En general, en un dominio D, si p es irreducible y u es una unidad en D, entonces el producto $u\,p$ es irreducible, también. Los elementos p y $u\,p$ se dicen *asociados*. Se ve, así, que, si quisiéramos generalizar el Teorema 0.1 a un dominio arbitrario, debemos tener en cuenta que es posible obtener descomposiciones que difieren en cambiar un factor por un asociado.

1 Monoides

Definición 1.1. Un *monoide* es una terna $(M, *, e)$ conformada por un conjunto *no vacío* M, una operación binaria $* : M \times M \to M$ *asociativa* y un elemento $e \in M$ con la propiedad de que $e * x = x = x * e$ cualquiera sea $x \in M$. Llamamos *producto en* M a la operación binaria $*$ y *unidad de* M al elemento e. Si la operación $*$ es conmutativa, decimos que el monoide es *conmutativo*.

Para simplificar la notación, a veces escribiremos $x\,y$ en lugar de $x * y$. También diremos, simplemente, que M es un monoide, sin hacer explícitas la operación $*$ ni la unidad e.

Ejemplo 1.2. La terna $(\mathbb{N}_0, +, 0)$, conformada por el conjunto de números naturales con el 0, la suma usual en $\mathbb{N}_0$ y el 0 como primer elemento, es un monoide. También es un monoide la terna $(\mathbb{Z}, +, 0)$.

Ejemplo 1.3. La terna $(\mathbb{N}, \cdot, 1)$ es un monoide con el producto dado por la multiplicación usual en $\mathbb{N}$. También son monoides $(\mathbb{N}_0, \cdot, 1)$ y $(\mathbb{Z}, \cdot, 1)$.

Ejemplo 1.4. En general, si R es un anillo (con unidad), entonces $(R, +, 0)$ y $(R, \cdot, 1)$ son monoides, donde $+$ denota la suma en R y $\cdot$ denota el producto en R.

Ejemplo 1.5. Sea R un anillo, Si $R^\times$ denota el grupo de unidades (elementos con inverso multiplicativo), entonces $(R^\times, \cdot, 1)$ es un monoide. Más en general, si $M \subset R$ es un subconjnto multiplicativamente cerrado que contiene a 1, entonces $(M, \cdot, 1)$ es un monoide.[2] En particular, si D es un dominio, $(D \setminus \{0\}, \cdot, 1)$ es un monoide.

Ejemplo 1.6. Sea S un conjunto y sea $\mathcal{P}(S)$ el conjunto de partes de S. Las ternas $(\mathcal{P}(S), \cap, S)$, $(\mathcal{P}(S), \cup, \varnothing)$ y $(\mathcal{P}(S), \Delta, \varnothing)$ son monoides.

[1] **??**.

[2] Si no asumimos que $1 \in M$, se obtiene un *semigrupo*.

Definición 1.7. Sea M un monoide. Decimos que $x \in M$ es *invertible a izquierda*, si existe $x' \in M$ tal que $x'\,x = e$ y que es *invertible a derecha*, si existe x' tal que $x\,x' = M$. Decimos que $x \in M$ es *invertible*,[3] si es invertible a izquierda y a derecha.

Observación 1.8. Sea M un monoide y sea $U \subset M$ el subconjunto de elementos invertibles. Dado $x \in U$, existen, por definición, $x', x'' \in M$ tales que $x'\,x = e = x\,x''$. Como el producto en M es asociativo, podemos deducir que

$$x' \;=\; x'\,e \;=\; x'\,(x\,x'') \;=\; (x'\,x)\,x'' \;=\; e\,x'' \;=\; x'' \;.$$

Por lo tanto, si x es invertible, entonces los inversos a izquierda y a derecha coinciden. En particular, si x es invertible, hay un único elemento de M que es inverso x (tanto a derecha, como a izquierda). Por otro lado, si M es conmutativo, no hay distinción entre inversos a izquierda e inversos a derecha, con lo cual, en ese caso, sólo tiene sentido hablar de elementos invertibles y de inversos, a secas.

Definición 1.9. Un *submonoide* de un monoide $(M, *, e)$ es un subconjunto N de M que contiene a la unidad y es cerrado por la multiplicación en M. En símbolos, $N \subset M$,

(i) $e \in N$ y

(ii) $x, y \in N$ implica $x * y \in N$.

Observación 1.10. Si $N \subset M$ es un submonoide de $(M, *, e)$, entonces $(N, *, e)$ es un monoide. Si $N \subset M$ es un submonoide de $(M, *, e)$ y $\tilde{N} \subset N$ es un submonoide de $(N, *, e)$, entonces $\tilde{N} \subset M$ es un submonoide de $(M, *, e)$.

Observación 1.11. Si M es un monoide, el subconjunto $U \subset M$ de elementos invertibles es un submonoide. En particular, es un monoide con la estructura heredada de M. Más aun, es un grupo con dicha estructura. Los elementos invertibles a izquierda constituyen un submonoide de M, como también los invertibles a derecha.

Ejemplo 1.12. En el Ejemplo 1.2, $\mathbb{N}_0 \subset \mathbb{Z}$ es un submonoide de $(\mathbb{Z}, +, 0)$.

Ejemplo 1.13. En el Ejemplo 1.3, $\mathbb{N}_0 \subset \mathbb{Z}$ es un submonoide de $(\mathbb{Z}, \cdot, 1)$ y $\mathbb{N} \subset \mathbb{N}_0$ es un submonoide de $(\mathbb{N}_0, \cdot, 1)$.

Ejemplo 1.14. Dado un dominio D, el conjunto de unidades $D^\times$ es submonoide de $D \setminus \{0\}$.

Definición 1.15. Dados monoides $(M, *_M, e_M)$ y $(N, *_N, e_N)$, un *morfismo de monoides (de M en N)* es una función $f : M \to N$ que verifica:

(i) $f(e_M) = e_N$ y

(ii) $f(x *_M y) = f(x) *_N f(y)$, para todo par de elementos $x, y \in M$.

[3] También decimos que x es una *unidad en M*, en el caso del monoide multiplicativo de un anillo.

En general, omitiremos los subíndices para distinguir el producto en M del producto en N y la unidad de M de la unidad de N.

Observación 1.16. Si $f : M \to N$ es un morfismo de monoides, los subconjuntos

$$K := f^{-1}(e) = \{x \in M : f(x) = e\} \subset M \quad \text{e} \quad \mathsf{img}(f) = \{f(x) : x \in M\} \subset N$$

son submonoides. Por el ítem i de la Definición 1.15, $e \in K$ y, por el ítem ii, si $x, y \in K$, entonces $f(x\,y) = f(x)\,f(y) = e\,e = e$ y $x\,y \in K$. En definitiva, $K \subset M$ es un submonoide. Por otro lado, como $f(e) = e$, $e \in \mathsf{img}(f)$ y si $f(x), f(y) \in \mathsf{img}(f)$, entonces $f(x)\,f(y) = f(x\,y) \in \mathsf{img}(f)$, también. Así, vemos que $\mathsf{img}(f) \subset N$ es un submonoide.

Si $f : M \to N$ es morfismo de grupos, $K = f^{-1}(e)$ es, simplemente, el núcleo de f. Pero en la categoría de monoides, no existe una manera canónica de asociarle un objeto núcleo a un morfismo. El submonoide K no tiene, en general, la propiedad universal correspondiente.

Observación 1.17. Dado un morfismo $f : M \to N$ podemos definir la siguiente relación en M

$$x \sim y \Leftrightarrow f(x) = f(y)\,. \tag{2}$$

Esta relación es reflexiva, simétrica y transitiva, con lo que es de equivalencia. Al conjunto de clases $M/\sim$ podemos darle una estructura de monoide. Si $x \in M$, denotamos su clase en $M/\sim$ por $\big[x\big]$. Dados $x, y \in M$, definimos

$$\big[x\big] \bar{*} \big[y\big] := \big[x\,y\big]\,. \tag{3}$$

La clase $\big[x\,y\big]$ está bien definida, pues, si $x \sim x'$ e $y \sim y'$, entonces

$$f(x'\,y') = f(x')\,f(y') = f(x)\,f(y) = f(x\,y)\,.$$

La clase $\big[e\big]$ es un elemento neutro con respecto a $\bar{*}$:

$$\big[e\big] \bar{*} \big[x\big] = \big[e\,x\big] = \big[x\big] \quad \text{y} \quad \big[x\big] \bar{*} \big[e\big] = \big[x\,e\big] = \big[x\big]\,.$$

En definitiva, $(M/\sim, \bar{*}, \big[e\big])$ es un monoide.

La construcción de la Observación 1.17 se puede generalizar. Sea M un monoide y supongamos dada una relación de equivalencia en M con la propiedad

$$x \sim x',\, y \sim y' \Rightarrow x\,y \sim x'\,y'\,. \tag{4}$$

Entonces, si $M/\sim$ denota el conjunto de clases de equivalencia, $\bar{*}$ denota la operación binaria en $M/\sim$ definida como en (3) y $\bar{e} = \big[e\big]$, la terna $(M/\sim, \bar{*}, \bar{e})$ es un monoide. Si $f : M \to N$ es un morfismo, la relación en M definida por $f(x) = f(y) \Rightarrow x \sim y$ cumple con (4).

Definición 1.18. Dado un monoide M, una relación de equivalencia $\sim$ en M que verifica (4) se denomina *relación de congruencia.* Si $\sim$ es una relació de congruencia en M, llamamos *monoide cociente (de M por $\sim$)* al monoide $(M/\sim, \bar{*}, \bar{e})$, donde $\bar{e}$ denota la clase de e con respecto a $\sim$ y $\bar{*}$ está definida por (3).

En realidad, la construcción de la Observación 1.17 es equivalente a la Definición 1.18, es decir, todo monoide cociente se puede recuperar como el módulo cociente por una relación de la forma $f(x) = f(y) \Rightarrow x \sim y$, para algún morfismo $f : M \to N$. Notemos que, dado un monoide M y una relación de congruencia en M, la aplicación $q : M \to M/\sim$ dada por $q(x) = \big[x\big]$ –donde $\big[x\big] = \{y \in M : y \sim x\}$ denota la clase de x respecto de la relación– es un morfismo de monoides. Más aun, vale que

$$x \sim y \Leftrightarrow q(x) = q(y) \ ,$$

con lo que la relación $\sim$ en M es un caso particular del tipo de relaciones visto en la Observación 1.17.

Supongamos dados una relación de congruencia en M y un morfismo $f : M \to N$. Supongamos, además, que se cumple

$$x \sim y \Rightarrow f(x) = f(y) \ . \tag{5}$$

Dada una clase $\big[x\big]$ con respecto a $\sim$, no hay ambigüedad en el valor de $f(x)$. La aplicación $\bar{f} : M/\sim \to N$ dada por

$$\bar{f}\big(\big[x\big]\big) := f(x) \tag{6}$$

está bien definida, pues $f(x)$ no depende del representante x de la clase. Si $x, y \in M$,

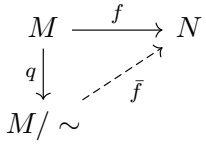
$$\bar{f}\big(\big[x\big]\,\big[y\big]\big) = \bar{f}\big(\big[x\,y\big]\big) = f(x\,y) = f(x)\,f(y) = \bar{f}\big(\big[x\big]\big)\,\bar{f}\big(\big[y\big]\big) \ .$$

Concluimos que $\bar{f}$ es un morfismo de monoides. Resumimos la discusión anterior en el resultado siguiente.

Proposición 1.19. *Sea M un monoide y $\sim$ una relación de congruncia en M. Dado un morfismo $f : M \to N$ que verifica* (5)*, existe un único morfismo $\bar{f} : M/\sim \to N$ tal que*

$$f = \bar{f} \circ q \ . \tag{7}$$

En términos de diagramas, el morfismo $\bar{f}$ es único tal que el siguiente diagrama conmuta:



Ejemplo 1.20. Sea $M = \mathbb{Z}_{\neq 0}$ el monoide compuesto por los enteros no nulos[4] con el producto usual y sea $U \subset M$ el submonoide $U = \{1, -1\}$. Decimos que dos enteros no nulos n y m son *asociados*, si $m = n$ o $m = -n$. Para simplificar, m y n son asociados, si existe $u \in U$ tal que $n = u\,m$.[5] La relación entre enteros de ser asociados es de equivalencia y, más aun, de congruencia: si $m = u\,m'$ y $n = v\,n'$, con $u, v \in U$ entonces

$$m\,n \;=\; (u\,m')\,(v\,n') \;=\; (u\,v)\,(m'\,n') \;.$$

Como $u\,v \in U$, concluimos que $m\,n \sim m'\,n'$. El cociente $M/\sim$ es isomorfo a $\mathbb{N}$.

Generalizando un poco el Ejemplo 1.20, dado un monoide conmutativo M y un submonoide $U \subset M$ que es, además, un grupo, definimos una relación en M por

$$x \sim y \Leftrightarrow x \in U\,y = \left\{u\,y \,:\, u \in U\right\} \;. \tag{8}$$

Esta relación es reflexiva pues $1 \in U$, es transitiva porque U es cerrado por la multiplicación en M y, como todo elemento de U posee inverso, es simétrica. La conmutatividad del producto en M garantiza que esta relación sea de congruencia.

Ejemplo 1.21. Dado $m \in \mathbb{Z}_{\neq 0}$, definimos su *longitud* como la cantidad de factores irreducibles en su descompsición, si m es positivo, o en la descomposición de $-m$, si es negativo, de acuerdo con el Teorema 0.1. Denotamos la longitud de m por $\mathsf{l}(m)$. Por ejemplo, si $m = p$ es un primo, $\mathsf{l}(p) = 1$, si $m \in \{1, -1\}$, entonces $\mathsf{l}(m) = 0$ y, si $m = a\,b$ con a y b enteros no nulos, entonces

$$\mathsf{l}(m) \;=\; \mathsf{l}(a) \,+\, \mathsf{l}(b) \;. \tag{9}$$

En particular, la aplicación $\mathsf{l} : \mathbb{Z}_{\neq 0} \to \mathbb{N}_0$ es un morfismo de monoides. La ecuación (9) muestra que este morfismo toma los mismos valores en enteros asociados, con lo que se factoriza por $\mathbb{N}$. Pero existen enteros no asociados con la misma longitud: $\mathsf{l}(2) = \mathsf{l}(3) = 1$ –más en general, si p y q son primos distintos no asociados, $\mathsf{l}(p) = \mathsf{l}(q) = 1$.

El Ejemplo 1.21 muestra que no toda relación de congruencia en un monoide M –incluso en el caso conmutativo– es de la forma (8).

Observación 1.22. Sea $f : M \to N$ un morfismo de monoides y supongamos que f es una función inyectiva. Veamos que f es un monomorfismo (en el sentido categórico). Si $h, k : \tilde{N} \to M$ son morfismos tales que $f \circ h = f \circ k$, entonces, dado $\tilde{x} \in \tilde{N}$,

$$f(h(\tilde{x})) \;=\; f(k(\tilde{x})) \;\Rightarrow\; h(\tilde{x}) \;=\; k(\tilde{x}) \;.$$

Como $\tilde{x}$ era arbitrario, $h = k$ y f es monomorfismo. Recíprocamente, supongamos que f es monomorfismo y sean $x, y \in M$ tales que $f(x) = f(y)$. Sea $\tilde{N} = \mathbb{N}_0$ y sean $h, k : \mathbb{N}_0 \to M$ los morfismos

$$h(n) \;:=\; x^n \quad \text{y} \quad k(n) \;:=\; y^n$$

[4] No hay razón para quitar el 0 a los fines de obtener una relación de congruencia. Como nos interesará entender el monoide multiplicativo de los elementos no nulos de un dominio, incluimos este ejemplo.

[5] Podríamos decir también que m y n son asociados, si $|m| = |n|$.

(con la convención de que $x^0 := e$ e $y^0 := e$). Entonces

$$f \circ k(n) \;=\; f(x)^n \;=\; f(y)^n \;=\; f \circ h(n)\ .$$

Como f es monomorfismo, $k = h$ y, en particular,

$$x \;=\; h(1) \;=\; k(1) \;=\; y$$

No es cierto, sin embargo, que todo epimorfismo entre monoides sea sobreyectivo. Por ejemplo, el morfismo $f : \mathbb{N}_0 \to \mathbb{Z}$ determinado por $f(1) = 1$ (inclusión) es epi, pero no sobre. Si $h, k : \mathbb{Z} \to M$ son dos morfismos tales que $h\,f = k\,f$, entonces $h(b) = k(b)$, para todo $b \geq 0$. En particular,

$$h(b) + h(-b) \;=\; h(b-b) \;=\; h(0) \;=\; 0 \;=\; k(0) \;=\; k(b-b) \;=\; k(b) + k(-b)\ .$$

Por unicidad del inverso en monoides, $h(-b) = k(-b)$, también.[6]

2 Monoides factoriales

Definición 2.1. Sea M un monoide. Un elemento $x \in M$ se dice *cancelable a izquierda*, si, para todo par $y, z \in M$

$$x\,y \;=\; x\,z \;\Rightarrow\; y \;=\; z\ . \tag{10}$$

Análogamente, x es *cancelable a derecha*, si, para todo par $y, z \in M$, $y\,x = z\,x$ implica $y = z$. Decimos que x es *cancelable*, si es cancelable a izquierda y a derecha.

Definición 2.2. Un *monoide cancelativo* es un monoide en el cual todo elemento es cancelable.[7]

Observación 2.3. Todo elemento invertible a izquierda es cancelable a izquierda y todo invertible a derecha es cancelable a derecha. En particular, todo grupo es un monoide cancelativo.

Ejemplo 2.4. El monoide $\mathbb{Z} \setminus \{0\}$ con el producto usual es un monoide cancelativo: si $a\,b = a\,c$, entonces $a\,(b-c) = 0$ y, como $\mathbb{Z}$ no posee divisores de 0, debe cumplirse $b = c$. En general, si D es un dominio íntegro, el monoide $D \setminus \{0\}$ es un monoide cancelativo.

De ahora en adelante M denotará un monoide conmutativo cancelativo y $U \subset M$ el submonoide (grupo) de elementos invertibles. Abreviaremos el producto en M yuxtaponiendo los argumentos y denotaremos 1 al elemento neutro.

Definición 2.5. Dados $a, b \in M$, decimos que b *es un divisor de* a, si existe $c \in M$ tal que $a = b\,c$. Decimos también que b es un *factor* de a, que b divide a a o que a es un múltiplo de b. Ser divisor o múltiplo define una relación en M, escribimos $b|a$ para indicar que b divide a a. Nos referimos a esta relación como la *relación de divisibilidad* en M.

[6] En la categoría de anillos, la inclusión $\mathbb{Z} \hookrightarrow \mathbb{Q}$ es un ejemplo de epimorfismo que no es sobreyectivo. El argumento es similar al del ejemplo anterior.

[7] Comparar con la definición de grupo: un grupo es un monoide en el cual todo elemento es invertible.

Observación 2.6. La relación de divisibilidad en M es una realción reflexiva y transitiva, pero no necesariamente simétrica. Por ejemplo, en $\mathbb{Z} \setminus \{0\}$, $2|(-2)$, $(-2)|2$, pero $2 \neq -2$. Sin embargo, en $\mathbb{N}$, la relación de divisibilidad sí es simétrica. La razón de que esto sea así es que, en $\mathbb{N}$, el único elemento invertible es 1.

Observación 2.7. Un elemento $u \in M$ es invertible, si y sólo si $u|1$. Además, los elementos invertibles son factores *triviales* en el sentido de que son factores de cualquier elemento del monoide.

Definición 2.8. Dos elementos $a, b \in M$ se dicen *asociados*, si $a|b$ y $b|a$. Equivalentemente, a y b son asociados, si existe un elemento invertible $u \in U$ tal que $a = u\,b$.[8] Usaremos la notación $a \sim b$ para indicar que a y b son asociados.

Ejemplo 2.9. Dado $k \in \mathbb{Z}$, los enteros k y $-k$ son asociados en $\mathbb{Z}$. Los enteros -1 y 1 son las únicas unidades en $\mathbb{Z}$: si $a, b \in \mathbb{Z}$ y $a \neq 0$,[9]

$$a\,b = 1 \quad \Rightarrow \quad |a| \leq 1 \quad \Rightarrow \quad |a| = 1 \quad \Rightarrow \quad a \in \{-1, 1\}\ .$$

En particular, los únicos asociados de $k \in \mathbb{Z}$ son k y $-k$.

Ejemplo 2.10. El *anillo de enteros de Gauss*, es el conjunto

$$\mathbb{Z}[i] := \left\{a + b\,i\ :\ a,\, b \in \mathbb{Z}\right\}\ ,$$

donde $i \in \mathbb{C}$ es una raíz cuadrada de -1, con las operaciones usuales heredadas de $\mathbb{C}$. Observamos que

- dados $a, b, c, d \in \mathbb{Z}$, $a + b\,i = c + d\,i$, si y sólo si $a = c$ y $b = d$ y que
- $(a + b\,i)\,(c + d\,i) = (a\,c - b\,d) + (a\,d + b\,c)\,i$.

Este anillo es un dominio de integridad, pues $\mathbb{C}$ es un cuerpo. Además de -1 y 1, $\mathbb{Z}[i]$ posee otras unidades. Por ejemplo, i y $-i$ son unidades, pues $i\,(-i) = -(-1) = 1$. Más aun, éstas son todas las unidades.[10] De las propiedades enunciadas arriba, vemos que

$$(a + b\,i)\,(c + d\,i) = 1 \quad \Leftrightarrow \quad a\,c - b\,d = 1 \quad \text{y} \quad a\,d = -b\,c\ .$$

De la primera igualdad, deducimos que a y b deben ser coprimos en $\mathbb{Z}$. Pasando a la segunda, $a|b\,c$ implica $a|c$. Pero c y d también deben ser coprimos y $c|a\,d$ implica $c|a$. Es decir, a y c son asociados en $\mathbb{Z}$. De acuerdo con el Ejemplo 2.9, $a = c$ o $a = -c$. Análogamente, $b = d$ o $b = -d$. Separando en casos, alguna de las siguientes igualdades debe ser cierta:

$$\begin{aligned} a^2 - b^2 = 1 \quad &, \quad a^2 + b^2 = 1\ , \\ -a^2 - b^2 = 1 \quad &\text{o} \quad -a^2 + b^2 = 1\ . \end{aligned}$$

[8] Si $a = u\,b$ con u invertible, entonces $b|a$ –por definición– y $b = u^{-1}\,a$, con lo que $a|b$. Recíprocamente, si $a|b$ y $b|a$, entonces existen $u, v \in M$ tales que $a = u\,b$ y $b = v\,a$. Así, $a = (u\,v)\,a$ y, como M es cancelativo, $u\,v = 1$, lo que significa que u y v son unidades.

[9] Necesitamos usar propiedades de los números reales.

[10]

Como $a, b \in \mathbb{R}$, la tercera no se puede ocurrir. Como $a, b \in \mathbb{Z}$, la segunda se cumple sólo si uno de a y b es 0 y el otro es ± 1. La primera es una diferencias de cuadrados: $a^2 - b^2 = (a+b)(a-b)$. Si este producto fuese igual a 1, valdría que $a+b = 1$ o $a+b = -1$. En el primer caso, $a-b = 1$, con lo que $b = 0$, y, en el segundo, $a-b = -1$ y $b = 0$, también. La cuarta es similar a la primera. En ese caso, deduciríamos que debe ser $a = 0$. En definitiva, las únicas unidades son de la forma $a + b\,i$ con $a = \pm 1$ y $b = 0$ o con $a = 0$ y $b = \pm 1$. Si ahora $x \in \mathbb{Z}[i]$, el conjunto de asociados de x está dado por

$$\{x,\, -x,\, i\,x,\, (-i)\,x\}\ .$$

El argumento es *ad hoc* en el caso de los enteros de Gauss. En general, el argumento es el siguiente. Si $x = a + b\,i \in \mathbb{Z}[i]$, llamamos *conjugado de* x al entero $\bar{x} = a - b\,i$. Se puede comprobar, usando las propiedades de $\mathbb{Z}[i]$ mencionadas, que $x\,\bar{x} \in \mathbb{Z}$ y que, si x es una unidad en $\mathbb{Z}[i]$ con inverso y, entonces $\bar{x}$ es una unidad, también, y su inverso es $\bar{y}$. Pero entonces, en tal caso, como $x\,y = 1$ y $\bar{x}\,\bar{y} = 1$, vale que $(x\,\bar{x})\,(y\,\bar{y}) = 1$ y el producto $x\,\bar{x}$ –la *norma* de x– es una unidad en $\mathbb{Z}$. Si $x = a + b\,i$, entonces $x\,\bar{x} = a^2 + b^2$. En particular, todas las unidades de $\mathbb{Z}[i]$ tienen norma positiva. De esto se deduce que, o bien $a = 0$ y $b = \pm 1$, o bien $a = \pm 1$ y $b = 0$. Recíprocamente, si la norma de x es 1 (o -1), entonces x es una unidad.

Corolario 2.11. *Conjugar es un morfismo de monoides en* $\mathbb{Z}[i] \setminus \{0\}$*, es decir, si* $x\,y = z$*, entonces* $\bar{z} = \bar{x}\,\bar{y}$*. La aplicación dada por tomar norma,* $x \mapsto x\,\bar{x}$*, también es morfismo de monoides. En particular,* $x \in \mathbb{Z}[i]$ *es una unidad, si y sólo si* $x\,\bar{x} \in \mathbb{Z}$ *es una unidad*

Ejemplo 2.12. Sea $\sqrt{-5} \in \mathbb{C}$ una raíz cuadrada de -5. El conjunto

$$\mathbb{Z}[\sqrt{-5}] := \left\{a + b\sqrt{-5} \,:\, a,\, b \in \mathbb{Z}\right\}$$

es un subanillo de $\mathbb{C}$ y, en particular, un dominio íntegro. Dado $x = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, su *conjugado* es el elemento $\bar{x} = a - b\sqrt{-5}$ del anillo. La *norma* de x es, en este caso,

$$x\,\bar{x} \;=\; a^2 \,+\, 5\,b^2\ .$$

En particular, si x es una unidad, su norma es ± 1, de lo que se deduce que $b = 0$ y $a = \pm 1$. Esto quiere decir que, en el anillo $\mathbb{Z}[\sqrt{-5}]$, las únicas unidades son -1 y 1. En definitiva, los únicos asociados de $x \in \mathbb{Z}[\sqrt{-5}]$ son $-x$ y x.

Como vimos en el Ejemplo 1.20, ser asociados es una relación de congruencia en M.

Definición 2.13. Dado $a \in M$, si $b \in M$ es tal que $b|a$, pero $a \nmid b$, decimos que b es un *factor propio* de a. Se dice que a es *irreducible (en M)*, si

(i) a no es una unidad y

(ii) los únicos factores propios de a son las unidades.

Observación 2.14. Las unidades no poseen factores propios y son factores de todos los elementos de M. Si $a \in M$ no es una unidad, entonces las unidades son factores propios de a. Si a es irreducible, sus asociados también lo son.

Ejemplo 2.15. Los primos racionales son irreducibles en $\mathbb{Z}$. Un entero $p \in \mathbb{Z}$ se dice *primo*, si $p|ab$ con $a, b \in \mathbb{Z}$ implica $p|a$ o $p|b$. Si $p = h\,k$ es primo, entonces $p|h\,k$. Por definición, o $p|h$ o $p|k$. Sin pérdida de generalidad, podemos suponer que $p|h$ y que $h = p\,l$ con $l \in \mathbb{Z}$. Pero entonces, como $\mathbb{Z}$ es dominio íntegro y $p = (p\,l)\,k$, $1 = l\,k$. Esto significa que l y k son unidades en $\mathbb{Z}$.

El argumento del Ejemplo 2.15 es válido en cualquier monoide cancelativo.

Ejemplo 2.16. Sea $\mathbb{Z}[i]$ el anillo definido en el Ejemplo 2.10. El entero racional $2 \in \mathbb{Z}$, si bien es irreducible en $\mathbb{Z}$, se factoriza en $\mathbb{Z}[i]$ de manera no trivial:

$$2 \;=\; (1+i)\,(1-i) \;=\; (-i)\,(1+i)^2 \;. \tag{11}$$

Por lo visto en el Ejemplo 2.10, $1+i$ y $1-i$ no son unidades en $\mathbb{Z}[i]$. El factor $1+i$ es irreducible. Si $x\,y = 1+i$, entonces, multiplicando por los conjugados, $(x\,\bar{x})\,(y\,\bar{y}) = (1+i)\,(1-i) = 2$. Dado que 2 es irreducible en $\mathbb{Z}$, deducimos que

- $x\,\bar{x} \in \{-1, 1\}$ e $y\,\bar{y} \in \{-2, 2\}$, o
- $x\,\bar{x} \in \{-2, 2\}$ e $y\,\bar{y} \in \{-1, 1\}$.

En el primer caso, x es una unidad, y, en el segundo, y lo es. En definitiva $1+i$ es irreducible. Como $1-i$ es asociado de $1+i$ (multiplicando por la unidad $(-i)$), deducimos que $1-i$ es irreducible, también.

Observación 2.17. Del Corolario 2.11, se deduce que, si $x \in \mathbb{Z}[i]$ no es irreducible, entonces su norma $x\,\bar{x} \in \mathbb{Z}$ tampoco es irreducible. Equivalentemente, si $x\,\bar{x}$ es irreducible en $\mathbb{Z}$, entonces x es irreducible en $\mathbb{Z}[i]$.

Ejemplo 2.18. Sea $\mathbb{Z}[\sqrt{-5}]$ el anillo del Ejemplo 2.12. Veamos que los elementos de norma 9 son irreducibles. Sea $x \in \mathbb{Z}[\sqrt{-5}]$ tal que $x\,\bar{x} = 9$. Supongamos que existe una factorización $x = r\,s$, con r y s no unidades en el anillo. Aplicando norma, por el Corolario 2.11, $r\,\bar{r} = \pm 3$. Esto quiere decir que existe una solución de

$$a^2 \,+\, 5\,b^2 \;=\; \pm 3 \;, \tag{12}$$

con $a, b \in \mathbb{Z}$. El lado izquierdo es no negativo y, si b no es cero, entonces el resultado es al menos 5 y, así, $b = 0$. Pero no existe a entero tal que $a^2 = 3$, con lo que no hay solución de (12) en $\mathbb{Z}$. En conclusión, no existen elementos de norma ± 3 en este anillo y los elementos de norma 9 deben ser irreducibles. Así, por ejemplo, ± 3 son irreducibles en $\mathbb{Z}$ y siguen siendo irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Pero no son los únicos irreducibles de norma 9. En $\mathbb{Z}[\sqrt{-5}]$,

$$9 \;=\; 3 \cdot 3 \;=\; (2+\sqrt{-5})\,(2-\sqrt{-5}) \;. \tag{13}$$

$x\,\bar{x}$	x
2	$\varnothing$
3	$\varnothing$
4	± 2
5	$\pm\sqrt{-5}$
6	$\pm(1+\sqrt{-5}), \pm(1-\sqrt{-5})$
7	$\varnothing$
8	$\varnothing$
9	$\pm 3, \pm(2+\sqrt{-5}), \pm(2-\sqrt{-5})$
10	$\varnothing$
11	$\varnothing$
12	$\varnothing$
13	$\varnothing$
14	$\pm(3+\sqrt{-5}), \pm(3-\sqrt{-5})$

Tabla 1: Elementos de $\mathbb{Z}[\sqrt{-5}]$ de norma dada.

De estas igualdades, se deduce que $2 \pm \sqrt{-5}$ son irreducibles de norma 9. Notamos que 3 no es asociado de $2+\sqrt{-5}$ ni de $2-\sqrt{-5}$.[11] La Tabla 1 contiene todos los elementos de $\mathbb{Z}[\sqrt{-5}]$ con un valor específico de la norma. Podemos ver que, en particular, los elementos de norma 4, 5, 6, 9 o 14 son irreducibles.

Definición 2.19. Dado $a \in M$, una *factorización de a como producto de irreducibles* es una expresión de la forma

$$a \;=\; p_1 \cdots p_s \;, \tag{14}$$

donde cada p_i es un elemento irreducible en M.

No es cierto, dado un monoide cancelativo y conmutativo, que todo elemento admita una factorización como producto de irreducibles. Pero, cuando exista, nos importará saber bajo qué condiciones y en qué sentido es (14) una factorización "única". Hay dos maneras "triviales" en las que podemos alterar los factores $p_1, \ldots, p_s$ para obtener otras factorizaciones posibles.

Ejemplo 2.20. En $\mathbb{Z}$, $6 = 2 \cdot 3$, pero también $6 = (-2)\cdot(-3) = 3 \cdot 2 = (-3)\cdot(-2)$. El Teorema 0.1 garantiza que éstas son todas las posibles factorizaciones de 6 como producto de irreducibles en $\mathbb{Z}$.

Ejemplo 2.21. Podemos utilizar la observación del Ejemplo 2.20 para obtener condiciones sobre las posibles factorizaciones de 6 en $\mathbb{Z}[i]$. Si $6 = p_1 \cdots p_s$, aplicando la norma, se obtiene la siguiente factorización en $\mathbb{Z}$:

$$36 \;=\; (p_1\,\bar{p}_1) \cdots (p_s\,\bar{p}_s) \;.$$

[11] Ni tampoco es $2+\sqrt{-5}$ asociado de $2-\sqrt{-5}$.

Si definimos $a_i = p_i\,\bar{p}_i$, entonces $a_i \geq 2$ y $a_i|36$ para todo i. Como $36 = 2 \cdot 2 \cdot 3 \cdot 3$, por el Teorema 0.1, $s \leq 4$ y, además,

$$a_i \,=\, 2^{u_i}\,3^{v_i} \quad , \quad 0 \,\leq\, u_i,\, v_i \,\leq\, 2 \quad , \quad u_i + v_i \,\geq\, 1 \quad \text{para todo } i \quad \text{y}$$
$$\sum_i u_i \,=\, \sum_i v_i \,=\, 2\ .$$

Ahora bien, según lo visto en el Ejemplo 2.16, $2 = (1+i)\,(1-i)$ en $\mathbb{Z}[i]$. Se puede comprobar, usando un argumento similar al del Ejemplo 2.18, que 3 es irreducible en este anillo. La identidad (11) proporciona las siguientes factorizaciones de 6 en $\mathbb{Z}[i]$:

$$6 \,=\, (1+i)\,(1-i)\,3 \,=\, (1+i)^2\,(-3\,i)\ .$$

Más aun, no hay elementos de norma 3, 6 o 12, con lo cual cada a_i en la factorización de 36 debe pertenecer al conjunto de divisores $\{1,\, 2,\, 4,\, 9,\, 18,\, 36\}$. Así, módulo cambiar un factor por un asociado o reordenarlos, la factorización anterior de 6 es la única posible.

En general, si (14) es una factorización de a como producto de irreducibles y si $u_1, \ldots, u_s$ son unidades tales que $u_1 \cdots u_s = 1$, entonces, cambiando cada p_i por su asociado $p'_i = u_i\,p_i$, se encuentra una factorización posiblemente distinta

$$a \,=\, p'_1 \cdots p'_s\ .$$

Lo mismo ocurre, si reordenamos los factores: si j es una permutación de $\{1, \ldots, s\}$, entonces

$$a \,=\, p_{j(1)} \cdots p_{j(s)}$$

también es una factorización de a como producto de irreducibles, posiblemente distinta.

Definición 2.22. Sea M un monoide cancelativo y conmutativo. Dado $a \in M$, diremos que una factorización $a = p_1 \cdots p_s$ como producto de irreducibles *es esencialmente única*, si, dada cualquier factorización como producto de irreducibles $a = p'_1 \cdots p'_t$ se cumple que

(i) $t = s$,

(ii) existe una permutación j de $\{1, \ldots, s\}$ tal que $p'_i \sim p_{j(i)}$ para todo i.

En palabras, un elemento de M se factoriza de manera esencialmente única como producto de irreducibles, si toda factorización como producto de irreducibles posee la misma cantidad de factores irreducibles y si la misma se puede obtener a partir de cualquier otra reordenando los factores y tomando asociados.

Definición 2.23. Un monoide conmutativo y cancelativo se dice *factorial* (o *monoide de factorización única*), si todo elemento distinto de una unidad posee una factorización esencialmente única como producto de irreducibles. Un *dominio de factorización única* (D.F.U.) es un dominio D cuyo monoide multiplicativo $D \setminus \{0\}$ es factorial.

Ejemplo 2.24. El anillo $\mathbb{Z}$ de enteros racionales es un D.F.U., por el Teorema 0.1. El anillo $\mathbb{Z}[i]$ de enteros de Gauss también es un D.F.U.[12] La identidad (13) muestra que el anillo $\mathbb{Z}[\sqrt{-5}]$ no es un D.F.U. Usando la Tabla 1, podemos obtener otros contraejemplos de la unicidad de la factorización.

A continuación, deducimos dos propiedades que todo monoide factorial posee y probamos que son, también, condiciones suficientes.

Definición 2.25. Sea M un monoide factorial. Dado $a \in M$, definimos la *longitud* de a como la cantidad de factores irreducibles en cualquier factorización de a como producto de irreducibles. Denotamos la longitud de a por $\mathsf{l}(a)$.

Si M es factorial, la longitud de $a \in M$ está bien definida: por un lado, como a admite al menos una factorización como producto de irreducibles, podemos hablar de la longitud de la factorización, pero, por otro lado, como toda tal factorización posee la misma cantidad de factores irreducibles, no hay ambigüedad, si la longitud de a se define como la longitud de cualquiera de ellas. La longitud caracteriza a las unidades y a los irreducibles.

Proposición 2.26. *Sea M un monoide factorial y sea $a \in M$. Entonces*

1. *a es una unidad, si y sólo si $\mathsf{l}(a) = 0$;*
2. *a es irreducible, si y sólo si $\mathsf{l}(a) = 1$;*
3. *si $a = b\,c$, entonces $\mathsf{l}(a) = \mathsf{l}(b) + \mathsf{l}(c)$;*
4. *si b es un factor propio de a, entonces $\mathsf{l}(a) > \mathsf{l}(b)$.*

Demostración. Si $a = b\,c$ y $\mathsf{l}(a) = r$, $\mathsf{l}(b) = s$ y $\mathsf{l}(c) = t$, entonces existen factorizaciones $a = p_1 \cdots p_r$, $b = p'_1 \cdots p'_s$ y $c = p'_{s+1} \cdots p'_{s+t}$ como productos de irreducibles para a, b y c, respectivamente. La igualdad

$$p_1 \cdots p_r \;=\; (p'_1 \cdots p'_s)\,(p'_{s+1} \cdots p'_{s+t})$$

y la unicidad de la longitud implican que $r = s + t$. □

Observación 2.27. Sea M es un monoide factorial y sea $a = b\,c \in M$. Dadas factorizaciones $a = p_1 \cdots p_r$ y $b = p'_1 \cdots p'_s$ como productos de irreducibles, $s \leq r$ y existe una función inyectiva $j : \{1, \ldots, s\} \to \{1, \ldots, r\}$ tal que

$$p'_i \sim p_{j(i)} \ .$$

Es decir, la lista de los posibles divisores de a se obtiene a partir de considerar los productos parciales de los factores irreducibles que aparecen en cualquier factorización de a como producto de irreducibles y asociados de estos productos.

[12] C.f. **??**

Teorema 2.28. *Sea M un monoide factorial y sean $a, b \in M$ tales que $b|a$. Si b es un factor propio de a, entonces $\mathsf{l}(a) > \mathsf{l}(b)$. En particular, en un monoide factorial no existen sucesiones infinitamente largas $\{a_i\}_{i\geq 0} \subset M$ tales que a_{i+1} sea un divisor propio de a_i para todo $i \geq 0$.*

Definición 2.29. Sea M un monoide (conmutativo). Decimos que M *satisface la condición de cadenas de divisores*,[13] si, dada una sucesión $\{a_i\}_{i\geq 0} \subset M$ tal que $a_{i+1}|a_i$ para todo $i \geq 0$, entonces existe $k \geq 0$ tal que $a_i \sim a_k$ para todo $i \geq k$.

Dicho de otra manera, M satisface la condición de cadenas de divisores, si toda sucesión $\{a_i\}_{i\geq 0}$ en M tal que $a_{i+1}|a_i$ es eventualmente esencialmente constante.

La segunda condición necesaria tiene que ver con la noción de primalidad.

Definición 2.30. En un monoide M, un elemento $p \in M$ se dice *primo*, si

(i) p no es una unidad y

(ii) si $p|a\,b$, entonces $p|a$ o $p|b$.

Observación 2.31. Si $p \in M$ es un elemento primo en un monoide *cancelativo*, entonces p es irreducible. Si $p = k\,h$ es una factorización en M, por el ítem ii de la Defínción 2.30, $p|k$ o $p|h$. Sin pérdida de generalidad, podemos asumir que $p|k$ y que $k = p\,b$, para cierto $b \in M$. Así, $p = (p\,b)\,h$. Dado que M es cancelativo, $b\,h = 1$ y h es una unidad.

Teorema 2.32. *En un monoide factorial, todo elemento irreducible es primo.*

Demostración. Sea M un monoide factorial y sea $p \in M$ un elemento irreducible. Dados $a, b \in M$, existen factorizaciones $a = p_1 \cdots p_s$ y $b = p_{s+1} \cdots p_{s+t}$ como productos de irreducibles. En particular,

$$a\,b = p_1 \cdots p_s \cdot p_{s+1} \cdots p_{s+t}$$

es una factorización de $a\,b$ como producto de irreducibles. Si $p|a\,b$, entonces, por lo mencionado en la Observación 2.27, debe existir $i \in \{1, \ldots, s+t\}$ tal que $p \sim p_i$. Si $i \leq s$, entonces $p|a$ y si $i > s$, entonces $p|b$. □

Definición 2.33. Sea M un monoide (conmutativo). Decimos que M *satisface la condición de primalidad*, si todo elemento irreducible es primo.

El Teorema 2.28 y el Teorema 2.32 implican que todo monoide factorial satisface la condición de cadenas de divisores y la condición de primalidad.

[13] Cadenas *ascendentes* de divisores. Comparar con la condición de cadenas ascendentes que caracterizan a los módulos/anillos noetherianos.

3 Más ejemplos

Ejemplo 3.1. Ya mencionamos en el Ejemplo 2.24 que $\mathbb{Z}[\sqrt{-5}]$ no es un D.F.U. Esto era consecuencia de que teníamos dos factorizaciones esencialmente distintas para 9: $3 \not\sim 2 \pm \sqrt{-5}$), pero

$$9 \;=\; 3 \cdot 3 \;=\; (2+\sqrt{-5})\,(2-\sqrt{-5})\;.$$

Supongamos que $x, y \in \mathbb{Z}[\sqrt{-5}]$ son tales que $x|y$. Entonces la norma de x divide a la norma de y. Si, además, asumimos que $x\,\bar{x} = y\,\bar{y}$, entonces $x \sim y$. Dado que 3 y $2+\sqrt{-5}$ y $2-\sqrt{-5}$ son de norma 9 y que no son asociados, deducimos que 3 no es primo en este anillo, pues:

- $3|(2+\sqrt{-5})\,(2-\sqrt{-5})$, pero
- $3 \nmid 2 \pm \sqrt{-5}$.

Análogamente, $2 \pm \sqrt{-5}$ no son primos, tampoco.

Es decir, $\mathbb{Z}[\sqrt{-5}]$ no satisface la condición de primalidad. Veamos que, sin embargo, sí satisface la condición de cadenas de divisores. El argumento es similar al que usamos arriba para mostrar que 3 no es primo. Por esta razón y porque es válido más en general, lo dejamos expresado en el siguiente lema. Si $x \in \mathbb{Z}[\sqrt{-5}]$, usamos la notación $\mathsf{Nm}(x)$ para referirnos a la norma de x.

Lema 3.2. *Sean $x, y \in \mathbb{Z}[\sqrt{-5}]$ tales que $x|y$. Entonces $\mathsf{Nm}(x)|\mathsf{Nm}(y)$. Si, además, $\mathsf{Nm}(x) \sim \mathsf{Nm}(y)$, entonces $x \sim y$. Equivalentemente, si x es un divisor propio de y, entonces $\mathsf{Nm}(x)$ es un divisor propio de $\mathsf{Nm}(y)$.*

Ejemplo 3.3. El anillo $\mathbb{Z}[\sqrt{-5}]$ satisface la condición de cadenas de divisores. Si $\{x_i\}_{i\geq 0}$ es una sucesión de divisores, es decir, elementos del anillo tales que $x_{i+1}|x_i$, entonces, aplicando la norma, obtenemos una sucesión de divisores $\{\mathsf{Nm}(x_i)\}_{i\geq 0}$ en $\mathbb{Z}$. Pero el anillo de enteros racionales es un D.F.U. y, por lo tanto, satisface la condición de cadenas de divisores. En particular, existe $k \geq 0$ tal que $\mathsf{Nm}(x_i) \sim \mathsf{Nm}(x_k)$ para todo $i \geq k$. Por el Lema 3.2, esto implica que $x_i \sim x_k$ para $i \geq k$. En definitiva, $\mathbb{Z}[\sqrt{-5}]$ satisface la condición de cadenas de divisores.

Como veremos en la sección 4, todo dominio íntegro noetheriano satisface la condición de cadenas de divisores. El anillo $\mathbb{Z}[\sqrt{-5}]$, como todo anillo de enteros, es noetheriano y, en particular, satisface la condición de cadenas de divisores. El argumento del Ejemplo 3.3 sigue siendo válido en un anillo de enteros algebraicos, o siempre que haya un morfismo "norma" con imagen en un D.F.U.

Ejemplo 3.4. Sea $\mathbb{Z}[\sqrt{10}]$ el subanillo de $\mathbb{R}$ de elementos de la forma $a+b\sqrt{10}$, con $a, b \in \mathbb{Z}$. Este anillo satisface la condición de cadenas de divisores. Definimos el conjugado de $x = a + b\sqrt{10}$ como $\bar{x} = a - b\sqrt{10}$ y su norma como $\mathsf{Nm}(x) = a^2 - 10\,b^2$. La norma es un morfismo de monoides

$$\mathsf{Nm} \;:\; \mathbb{Z}[\sqrt{10}] \smallsetminus \{0\} \;\to\; \mathbb{Z} \smallsetminus \{0\}\;,$$

por lo tanto, $x|y$ implica $\mathsf{Nm}(x)|\mathsf{Nm}(y)$. En particular, las unidades de $\mathbb{Z}[\sqrt{10}]$ tienen norma -1 o 1. Recíprocamente, si $\mathsf{Nm}(x) = \pm 1$, entonces x es una unidad con inverso $\pm\bar{x}$. En definitiva, el Lema 3.2 es cierto con $\mathbb{Z}[\sqrt{10}]$ en lugar de $\mathbb{Z}[\sqrt{-5}]$ y $\mathbb{Z}[\sqrt{10}] \setminus \{0\}$ satisface la condición de cadenas de divisores. Pero el anillo no es un D.F.U. Veamos primero que 2, 5 y $\sqrt{10}$ son irreducibles.

La norma de 2 es 4, con lo cual, el problema de determinar si 2 es o no irreducible se reduce a determinar si existen elementos de norma ± 2. Si existiesen $a, b \in \mathbb{Z}$ tales que

$$a^2 \, - \, 10\, b^2 \, = \, \pm 2 \ ,$$

entonces $a^2 \equiv \pm 2 \ (\mathsf{mod}\, 5)$. Pero esta congruencia no tiene solución, pues, los posibles restos cuadráticos módulo 5 son 0, 1 y 4. Análogamente, no existen elementos de norma ± 5, pues, si

$$a^2 \, - \, 10\, b^2 \, = \, \pm 5 \ ,$$

entonces, $5|a$, $5 \nmid b$ y $\mp 5 \equiv 10\, b^2 \, (\mathsf{mod}\, 25)$. En particular, b debe ser solución de

$$\mp 1 \, \equiv \, 2\, b^2 \quad (\mathsf{mod}\, 5) \ ,$$

que es imposible. Esto demuestra que 2 y 5 son irreducibles en $\mathbb{Z}[\sqrt{10}]$. En cuanto a $\sqrt{10}$, ninguno de los divisores propios de $\mathsf{Nm}(\sqrt{10}) = -10$ pertenece a la imagen del morfismo Nm, con lo que $\sqrt{10}$ es irreducible.

Ahora bien, en $\mathbb{Z}[\sqrt{10}]$ valen las igualdades

$$10 \, = \, 2 \cdot 5 \, = \, (\sqrt{10})^2 \ .$$

Pero $2 \not\sim \sqrt{10}$ (ni tampoco es 5 asociado de $\sqrt{10}$). En definitiva, 10 admite dos factorizaciones esencialmente distintas.

Ejemplo 3.5. Sea $\mathbb{Z}[X]$ el anillo de polinomios en una variable con coeficientes enteros. Puesto que $\mathbb{Z}$ es un dominio, las unidades en $\mathbb{Z}[X]$ son exactamente las unidades en $\mathbb{Z}$, es decir, -1 y 1. Esto significa que $f \sim g$, si y sólo si $f = \pm g$. Dado $f \in \mathbb{Z}[X]$, denotamos el grado de f por $\mathsf{gr}(f)$. El grado de un polinomio tiene la siguiente propiedad:

$$\mathsf{gr}(f\, g) \, = \, \mathsf{gr}(f) \, + \, \mathsf{gr}(g) \ . \tag{15}$$

En particular, si $f|g$, vale que $\mathsf{gr}(f) \leq \mathsf{gr}(g)$. Más aun, si f es un divisor propio de g, entonces la desigualdad es estricta. Concluimos, así, que no pueden existir cadenas no acotadas de divisores.

Observación 3.6. La propiedad del grado expresada en (15) es cierta para todo anillo de polinomios con coeficientes en un dominio íntegro. En particular, dado un dominio D, las unidades en $D[X]$ son exactamente las unidades en D y el monoide $D[X] \setminus \{0\}$ satisface la condición de cadenas de divisores.

Ejemplo 3.7. Sea D el anillo que se obtiene agregando a $\mathbb{Z}[X]$ "las raíces de X". Es decir, existe un elemento que denotamos $X^{1/2}$ tal que $(X^{1/2})^2 = X$ y, en general existe $X^{1/N} \in D$ tal que $(X^{1/N})^N = X$. Entonces D es un dominio íntegro que no satisface la condición de cadenas de divisores, ya que incluye, por ejemplo, la sucesión de divisores propios $\{X^{1/2^i}\}_{i\geq 0}$.

Para evitar problemas de definición, podemos considerar el subanillo $\mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \dots]$ de $\mathbb{C}$ (o de $\mathbb{R}$). En particular, por ser subanillo de un cuerpo, debe ser dominio, y se puede comprobar que $\{\sqrt[2^i]{2}\}_{i\geq 0}$ es una sucesión de divisores propios.

4 Existencia y unicidad de factorizaciones

Como mencionamos en la sección 2, no es cierto que en un monoide cancelativo todo elemento admita una factorización como producto de irreducibles. Dados un anillo A y un elemento $a_0 \in A$, si no fuese irreducible, entonces existirían $a_1, b_1 \in A$ tales que $a_0 = a_1\, b_1$. Si a_1, por ejemplo, tampoco fuese irreducible, $a_1 = a_2\, b_2$, para ciertos $a_2, b_2 \in A$. Supongamos que existe una sucesión $\{a_i\}_{i\geq 0}$ de elementos no nulos de A tales que, para $i \geq 0$, existe una factorización $a_{i+1} = a_i\, b_i$, para ciertos $b_i \in A$. Una sucesión así da lugar a una cadena de ideales (principales) en A:

$$\langle a_0\rangle \subset \langle a_1\rangle \subset \cdots \subset A\ . \tag{16}$$

Un anillo A se dice *noetheriano (a izquierda)*, si satisface la *condición de cadenas ascendentes* de ideales (a izquierda), es decir, dada una sucesión de ideales

$$I_0 \subset I_1 \subset \cdots \subset A$$

existe $k \geq 0$ tal que $I_i = I_k$ para todo $i \geq k$. Si A es noetheriano, la cadena (16) debe estabilizarse a partir de cierto punto, es decir, $\langle a_i\rangle = \langle a_k\rangle$, para todo $i \geq k$, digamos. Si $A = D$ es un dominio íntegro noetheriano, entonces $a_i \sim a_k$, para $i \geq k$.

Corolario 4.1. *Sea D un dominio íntegro y sea $M = D \setminus \{0\}$ el monoide multiplicativo de elementos no nulos. La condición de cadenas de divisores en el monoide M equivale a la condición de cadenas ascendentes* de ideales principales *en D. En particular, si D es un dominio íntegro noetheriano, entonces el monoide M satisface la condición de cadenas de divisores.*

Observación 4.2. En un monoide conmutativo y cancelativo que satisface la condición de cadenas de divisores, todo elemento que no es una unidad, admite al menos una factorización como producto de irreducibles. Para demostrar esta afirmación, será suficiente probar que todo elemento distinto de una unidad posee, al menos, un factor irreducible. Sea M es un monoide conmutativo y cancelativo. Si existe $a \in M$ distinto de una unidad que no admite factores irreducibles, es posible definir una sucesión $\{a_i\}_{i\geq 0}$ de elementos de M que verifica $a_{i+1}|a_i$ propiamente. En primer lugar, $a_0 = a$ no es irreducible, con lo cual existen factores propios a_1 y b_1 de a (no asociados a a, ni unidades) y, como a no admite factores irreducibles, a_1 no es irredcible. Dada una lista $a_1, \dots, a_i$ tal que cada

elemento es un divisor propio del elemento anterior, como a_i es factor de a, no puede ser irreducible y existe una factorización $a_i = a_{i+1}\, b_{i+1}$, con a_{i+1} y b_{i+1} factores propios de a_i. En definitiva, existe una cadena de divisores propios en M.

En particular, en un dominio íntegro noetheriano, todo elemento no nulo admite *alguna* factorización como producto de irreducibles. Aun así, la existencia de factorizaciones no es una propiedad exclusiva de los dominios noetherianos.

Ejemplo 4.3. El anillo $A = k[X_1, X_2, \dots]$ de polinomios en infinitas indeterminadas con coeficientes en un cuerpo k no es noetheriano, pero todo elemento admite una factorización como producto de irreducibles. Más aun, dicha factorización es única, ya que, si $f \in A$, entonces f pertenece a alguno de los subanillos $k[X_1, \dots, X_n]$ y cada uno de éstos es un dominio de factorización única.[14]

Teorema 4.4. *Sea M un monoide conmutativo y cancelativo. Si M satisface la condición de cadenas de divisores y la condición de primalidad, entonces M es factorial.*

Demostración. Tenemos que probar que todo elemento $a \in M$ posee una factorización como producto de irreducibles y que dos factorizaciones son esencialmente iguales, es decir, difieren solamente en cambiar factores irreducibles por asociados e intercambiar el orden de los factores. Por la Observación 4.2, como M satisface la condición de cadenas de divisores, dado $a \in M$ sabemos que existe al menos una factorización $a = p_1 \cdots p_r$ en donde los p_i son irreducibles. Sea $a = p'_1 \cdots p'_s$ alguna otra factorización. Si $r = 1$, entonces, por la condición de primalidad, p_1 es primo y divide a un producto de irreducibles $p'_1 \cdots p'_s$. Como p_1 es primo, divide a p'_i para algún i. Sin pérdida de generalidad, podemos asumir que $i = 1$, es decir, $p_1 | p'_1$. Ahora, la igualdad $p_1 = p'_1 \cdots p'_s$ implica que p'_1 también divide a p_1. Ahora, como p'_1 es irreducible y p_1 no es unidad, $p_1 \sim p'_1$. Si, además, $s \geq 2$, cancelando,

$$1 \;=\; u\, p'_2 \cdots p'_s \;,$$

para cierta unidad u. Pero esto contradice la irreducibilidad de los p'_i (por definición, no son unidades). Entonces $r = s = 1$ y $p_1 \sim p'_1$, lo que significa que las factorizaciones son esencialmente la misma.

Supongamos que $r \geq 2$ (por simetría $s \geq 2$, también). De nuevo, $p_1 | p'_1 \cdots p'_s$ implica que p_1 divide a alguno de los p'_i. Permutando los factores, podemos asumir que $p_1 | p'_1$. Como p'_1 es irreducible, $p_1 \sim p'_1$. Cancelando, obetenemos la igualdad

$$p_2 \cdots p_r \;=\; u\, p'_2 \cdots p'_s \;,$$

para cierta unidad u. Inductivamente, $r = s$ y existe una permutación $i \mapsto j(i)$ tal que $p'_i \sim p_{j(i)}$. □

Observación 4.5. Sea M un monoide conmutativo y cancelativo y sean $a, a', b, b' \in M$ tales que $a \sim a'$ y $b \sim b'$. Por definición, existen unidades $u, v \in M$ que verifican que

[14] C.f. la Definición 2.23.

$a = u\,a'$ y $b = v\,b'$. Tomando el producto, se ve que $a\,b = (u\,v)\,a'\,b'$. Pero $u\,v \in M$ es una unidad. En definitiva, $a\,b \sim a'\,b'$. Esto prueba que la relación entre elementos de M de ser asociados es una relación de congruencia. El cociente $M/\sim$ de un monoide conmutativo y cancelativo M es un monoide conmutativo y cancelativo, también. Los elementos de $M/\sim$ son las clases $\big[a\big] = \{b \in M \,:\, b \sim a\}$ de elementos de M módulo asociados en M. Por la Observación 2.14, las unidades de M pertenecen a una misma clases. Esta clase es $\big[1\big]$, sólo contiene unidades y, además, es el elemento neutro para el producto en $M/\sim$ dado por $\big[a\big]\,\big[b\big] = \big[a\,b\big]$. Una igualdad de la forma

$$\big[a\big] \;=\; \big[b\big]\,\big[c\big]$$

equivale a $a \sim b\,c$. Por lo tanto,

- la única unidad en $M/\sim$ es $\big[1\big]$,
- los irreducibles en $M/\sim$ son las clases $\big[p\big]$, donde $p \in M$ es irreducible y
- si $\big[a\big]$ y $\big[b\big]$ son asociados *en* $M/\sim$, entonces $\big[a\big] = \big[b\big]$.

La existencia de factorizaciones en un monoide se puede interpretar en términos de generadores. En un monoide conmutativo y cancelativo, todo elemento distinto de una unidad admite una factorización como producto de irreducibles, si y sólo si el conjunto de elementos irreducibles genera el monoide. En tal caso, podría haber cierta ambigüedad en la factorización de un elemento, es decir, la misma podría no ser única (ni esencialmente única). Un primer paso hacia la eliminación de esta ambigüedad es pasar al monoide cociente. Los elementos de un monoide conmutativo y cancelativo M admiten factorizaciones como productos de irreducibles, si y sólo si los elementos (clases) de $M/\sim$ admiten factorizaciones como productos de (clases de) irreducibles. Además, por la Observación 4.5, las factorizaciones en M son esencialmente únicas, si y sólo si las factorizaciones en $M/\sim$ son únicas, salvo por el orden de los factores.

Teorema 4.6. *Un monoide conmutativo y cancelativo M es factorial, si y sólo si el monoide cociente $M/\sim$ es el monoide abeliano libre en $\big\{\big[p\big] \,:\, p \in M \text{ irreducible}\big\}$. En tal caso, si $I \subset M$ es un conjunto de representantes de las clases de irreducibles módulo asociados y $U \subset M$ es el subgrupo de unidades,*

$$M \;=\; U \times \langle I\rangle \;\;,$$

donde $\langle I\rangle = \big\{p_1^{r_1}\cdots p_s^{r_s} \,:\, s \geq 1,\, p_i \in I,\, r_i \geq 1\big\}$ es el submonoide generado por I.

5 Máximo común divisor

Definición 5.1. Sea M un monoide conmutativo y sean $a, b \in M$. Un *máximo común divisor* (M.C.D.) de a y b es un elemento $d \in M$ que verifica:

1. $d|a$ y $d|b$ y

2. si $c|a$ y $c|b$, entonces $c|d$.

Denotamos por $\big(a : b\big)$ un M.C.D. de a y b.

Observación 5.2. Si existe un M.C.D. para $a, b \in M$, entonces es único, salvo asociados. Por esta razón, si d es un M.C.D. para a y b, escribimos $\big(a : b\big) \sim d$. Además, si $a \sim a'$, entonces existe un M.C.D. para a y b, si y sólo si existe uno para a' y b, pues $d|a$, si y sólo si $d|a'$. En tal caso, $\big(a : b\big) \sim \big(a' : b\big)$.

Hay dos casos en los que está garantizada la existencia de un M.C.D.

Proposición 5.3. *Sea M un monoide conmutativo y cancelativo. Entonces, para todo $b \in M$,*

1. *si $u \in M$ es una unidad, existe un M.C.D. para u y b y $\big(u : b\big) \sim 1$;*
2. *si $p \in M$ es irreducible, existe un M.C.D. para p y b y*

$$\big(p : b\big) \sim \begin{cases} p & si\ p \mid b\ , \\ 1 & si\ p \nmid b\ . \end{cases}$$

Demostración. Sean $u, p, b \in M$, u unidad, p irreducible y b arbitrario. Entonces $1|u$ y $1|b$. Si $c|u$ y $c|b$, en particular, $c|u$. Como $u \sim 1$, debe cumplirse que $c|1$, con lo cual 1 es un M.C.D. para u y b. En cuanto al irreducible, si $p|b$, entonces $p|p$ y $p|b$. Si $c|p$ y $c|b$, en particular $c|p$ y p es un M.C.D. para p y b. Si, en cambio, $p \nmid b$, entonces consideramos el divisor común 1: $1|p$ y $1|b$. Si $c|p$ y $c|b$, en particular, $c|p$. Por definición, $c \sim 1$ o $c \sim p$. Si fuese $c \sim p$, deducimos que $p|b$, contradiciendo $p \nmid b$. Así, debe ser que $c \sim 1$ y, en particular, $c|1$. En definitiva, en este caso también existe un M.C.D. □

Definición 5.4. Dado un monoide conmutativo y cancelativo M, dos elementos $a, b \in M$ se dicen *coprimos*, si existe un M.C.D. para a y b y $\big(a : b\big) \sim 1$.

Teorema 5.5. *En un monoide factorial, todo par de elementos posee un M.C.D.*

Observación 5.6. Sea M un monoide factorial y sea $a \in M$. Por el Teorema 4.6, existen una unidad u, irreducibles $p_1, \ldots, p_s$ y enteros positivos $e_1, \ldots, e_s \geq 1$ tales que $a = u\, p_1^{e_1} \cdots p_s^{e_s}$. Los divisores de a en M son exactamente los elementos de la forma:

$$c \;=\; w\, p_1^{h_1} \cdots p_s^{h_s}\ , \tag{17}$$

para cierta unidad w y enteros $h_1, \ldots, h_s$ que cumplen $0 \leq h_i \leq e_i$.

Demostración. Sea M un monoide factorial y sean $a, b \in M$. Si a es una unidad o si b es una unidad, entonces $\big(a : b\big) = 1$ es un M.C.D. de a y de b. Supongamos que ni a, ni b son unidades. Por el Teorema 4.6, existen unidades u, v, irreducibles no asociados $p_1, \ldots, p_s$ y enteros no negativos $e_1, \ldots, e_s, f_1, \ldots, f_s \geq 0$ tales

$$a \;=\; u\, p_1^{e_1} \cdots p_s^{e_s} \quad \text{y} \quad b \;=\; v\, p_1^{f_1} \cdots p_s^{f_s}\ .$$

Por la Observación 5.6, si $c|a$ y $c|b$, entonces $c = w\, p_1^{h_1} \cdots p_s^{h_s}$, para cierta unidad w y enteros $h_1, \ldots, h_i$ que cumplen $0 \leq h_i \leq \min\{e_i, f_i\}$. En particular, nuevamente por la Observación 5.6, si $g_i = \min\{e_i, f_i\}$, entonces

$$d = p_1^{g_1} \cdots p_s^{g_s}$$

es un M.C.D. de a y de b. □

Observación 5.7. En un monoide factorial M, dos elementos a y b son coprimos, si y sólo si a es una unidad, b es una unidad o no poseen factores irreducibles en común.

Definición 5.8. Un monoide conmutativo y cancelativo *satisface la condición del máximo común divisor* (la condición del M.C.D.), si todo par de elementos admite un M.C.D.

Proposición 5.9. *Todo monoide conmutativo y cancelativo que satisface la condición del M.C.D. satisface la condición de primalidad.*

Antes de demostrar la Proposición 5.9, probamos algunas propiedades del M.C.D.

Lema 5.10. *Sea M un monoide conmutativo, cancelativo y que satisface la condición del M.C.D. Entonces,*

1. *dados $a_1, \ldots, a_r \in M$ existe $d \in M$ que verifica que $d|a_i$ para todo i y que, si $c|a_i$ para todo i, entonces $c|d$;*
2. *dados $a, b, c \in M$, $\big((a : b) : c\big) \sim \big(a : (b : c)\big)$;*
3. *dados $a, b, c \in M$, $\big(c\,a : c\,b\big) \sim c\,\big(a : b\big)$;*
4. *dados $a, b, c \in M$, si $\big(a : b\big) \sim 1$, entonces $\big(a : b\,c\big) \sim \big(a : c\big)$.*

Demostración. Sea $d_0 = a_1$ y, en general, $d_i = \big(d_{i-1} : a_i\big)$. Entonces $d = d_r|d_{r-1}| \cdots |d_2|d_1$. En particular, como $d_i|a_i$, vale que $d|a_i$ para todo i. Además, si $c|a_i$ para todo i, entonces $c|d_i$ para todo i y, por lo tanto, $c|d_r = d$.

Si $a, b, c \in M$, entonces $d = \big((a : b) : c\big)$ y $d' = \big(a : (b : c)\big)$ verifican que $d|\big(a : b\big)|a, b$ y $d|c$, $d'|a$ y $d'|\big(b : c\big)|b, c$. Entonces $d|\big(b : c\big)$ y, por lo tanto, $d|d'$. Análogamente, $d'|\big(a : b\big)$ y, por lo tanto, $d'|d$.

Sean, ahora, $d = \big(a : b\big)$ y $e = \big(c\,a : c\,b\big)$. Entonces, $c\,d|c\,a$ y $c\,d|c\,b$, con lo cual, $c\,d|e$. Esto quiere decir que existe $x \in M$ tal que $e = (c\,d)\,x$. Como $e|c\,a$, se deduce que $d\,x|a$, porque M es cancelativo. Análogamente, $d\,x|b$ y, en consecuencia, $d\,x|\big(a : b\big) = d$. En definitiva, $d\,x \sim d$ y x era una unidad de M. Es decir, $e \sim c\,d$.

Si $\big(a : b\big) \sim 1$, entonces $\big(a\,c : b\,c\big) \sim c\,\big(a : b\big) \sim c$. Por otro lado, en general, $\big(a : a\,c\big) \sim a\,\big(1 : c\big) \sim a$. Así, por la Observación 5.2,

$$\big(a : b\,c\big) \sim \big(\big(a : a\,c\big) : b\,c\big) \sim \big(a : \big(a\,c : b\,c\big)\big) \sim \big(a : \big(a : b\big)\,c\big) \sim \big(a : c\big)\ .$$

□

Si $d \in M$ satisface las condiciones del ítem 1, decimos que d es un M.C.D. para $a_1, \ldots, a_r$ y escribimos $d \sim (a_1 : \cdots : a_r)$. El ítem 2 muestra que no importa el orden en que se toman los divisores sucesivos.

Demostración de 5.9. Sea M un monoide conmutativo, cancelativo que satisface la condición del M.C.D. Si $p \in M$ es un irreducible y $a, b \in M$ son tales que $p \nmid a$ y $p \nmid b$, entonces, por la Proposición 5.3, $(p : a) \sim 1$ y $(p : b) \sim 1$. Por el ítem 4 del Lema 5.10, vale que $(p : a\,b) \sim 1$, también. Pero, nuevamente por la Proposición 5.3, $p \nmid a\,b$. En definitiva, p es primo. □

Teorema 5.11. *Sea M un monoide conmutativo y cancelativo. Las siguientes propiedades son equivalentes:*

1. *M es factorial;*
2. *M satisface la condición de cadenas de divisores y la condición de primalidad;*
3. *M satisface la condición de cadenas de divisores y la condición del M.C.D.*

Demostración. El Teorema 2.28 y el Teorema 2.32 muestran que 1 implica 2. El Teorema 4.4 muestra que 2 implica 1. La Proposición 5.9 muestra que 3 implica 2 y el Teorema 5.5, junto con el Teorema 2.28, muestra que 1 implica 3. □

6 Dominios de ideales principales

El objetivo principal de esta sección es demostrar el siguiente resultado.

Teorema 6.1. *Todo D.I.P. es un D.F.U.*

Si D es un dominio íntegro, el monoide $M := D \setminus \{0\}$ es conmutativo y cancelativo. El dominio D es un D.F.U., precisamente cuando M es factorial. Empezamos demostrando que, si D es un D.I.P., entonces M satisface la condición de cadenas e divisores. Por el Corolario 4.1, será suficiente demostrar que D es noetheriano.

Proposición 6.2. *Todo D.I.P. es un anillo noetheriano.*

Demostración. Sea D un D.I.P. Todo ideal en D es de la forma $\langle a \rangle$ para cierto $a \in D$. Entonces, dada una familia $\{I_j\}_{j \geq 1}$ de ideales de D tales que $I_j \subset I_{j+1}$ para todo $j \geq 1$, definimos $I := \bigcup_{j \geq 1} I_j$. Esta unión es un ideal y, por lo tanto, existe $a \in D$ tal que $I = \langle a \rangle$. Ahora, como $a \in \bigcup_{j \geq 1} I_j$, existe j tal que $a \in I_j$. En ese caso, $I_j = I$ y, en consecuencia, $I_{j+k} = I_j$ para todo $k \geq 0$. □

Corolario 6.3. *Si D es un D.I.P., el monoide $D \setminus \{0\}$ satisface la condición de cadenas de divisores.*

Proposición 6.4. *Si D es un D.I.P., el monoide $D \setminus \{0\}$ satisface la condición del M.C.D.*

Demostración. Sean $a, b \in M := D \setminus \{0\}$ y sea $I = \langle a, b \rangle$ el ideal generado por a y por b. Como D es un D.I.P., existe $d \in D$ tal que $\langle d \rangle = I$. Necesariamente, como $I \neq 0$, $d \in M$, Afirmamos que d es un M.C.D. para a y b. Si logramos demostrar esta afirmación, como a y b eran elementos arbitrarios de M, habremos demostrado que todo par de elementos no nulos admite un M.C.D. y que

$$\langle a, b \rangle \; = \; \big\langle \big(a : b\big) \big\rangle \; . \tag{18}$$

Ahora, como $a, b \in \langle d \rangle$, $d \in M$ es un divisor común. Si $c \in M$ es un divisor común de a y de b, entonces

$$\langle d \rangle \; = \; \langle a, b \rangle \; \subset \; \langle c \rangle \; ,$$

es decir, $c|d$. □

A continuación, damos una demostración independiente de la Proposición 6.4 de que en un D.I.P. se verifica la condición de primalidad.

Proposición 6.5. *Si D es un D.I.P., el monoide $D \setminus \{0\}$ satisface la condición de primalidad.*

Demostración. Si $p \in M := D \setminus \{0\}$ es un irreducible, entonces el ideal $I = \langle p \rangle$ es maximal en D, pues, si $J \lhd D$ es un ideal tal que $I \subset J$ y $J = \langle x \rangle$, entonces $x|p$ y $x \sim p$ o $x \sim 1$. En el primer caso, $J = I$ y, en el segundo, $J = D$. Pero todo ideal maximal es primo.[15] Por lo tanto, si $a, b \in M$ son tales que $a\,b \in \langle p \rangle$, se cumple que, o bien $a \in \langle p \rangle$, o bien $b \in \langle p \rangle$. Es decir, o bien $p|a$, o bien $p|b$. □

Demostración de 6.1. Sea D un D.I.P. y sea $M := D \setminus \{0\}$. Por el Corolario 6.3, el monoide M satisface la condición de cadenas de divisores. Por la Proposición 6.4, M satisface la condición del M.C.D. –equivalentemente, por la Proposición 6.5, M satisface la condición de primalidad. En todo caso, M es factorial, por el Teorema 5.11. □

Observación 6.6. Sean D y E dominios íntegros que satisfacen la condición del M.C.D. y supongamos que $D \subset E$ es un subanillo. Dados $a, b \in D$, tenemos, *a priori*, dos definiciones de M.C.D. para a y b. Sea $d = \big(a : b\big)_D$ un M.C.D. para a y b vistos como elementos de D y sea $e = \big(a : b\big)_E$ un M.C.D. vistos como elementos de E. En general, como $d \in E$ y d divide a a y a b en D, los divide en E y, por definición $d|e$. Si asumimos que D es un D.I.P., entonces, por (18), existen $x, y \in D$ tales que

$$d \; = \; x\,a \; + \; y\,b \; .$$

En particular, en tal caso, $e|d$, también.

Como caso particular de la Observación 6.6 tenemos el resultado siguiente.

[15] Sea I un ideal maximal en un anillo conmutativo R. Si $a \notin I$, por maximalidad, $1 = x\,a + y$, para ciertos $x \in R$ e $y \in I$. Si, además, $a\,b \in I$, entonces $b = x\,(a\,b) + b\,y \in I$.

Proposición 6.7. *Sea D un D.I.P. y sea E un D.F.U. tales que D es subanillo de E. Dados $a, b \in D$, se cumple que*

$$\big(a : b\big)_E \sim \big(a : b\big)_D$$

(asociados en E).

Para probar que un dominio particular es un D.I.P. es útil saber qué estructura adicional posee el anillo. Una clase importante de dominios que son dominios de ideales principales es la clase de dominios euclideos.

Definición 6.8. Un dominio D es un *dominio euclideo* (D.E.), si existe una función $\delta : D \to \mathbb{Z}_{\geq 0}$ que verifica que, dados $a, b \in D \setminus \{0\}$, existen $q, r \in D$ tales que

$$a = q\,b + r \quad \text{y} \quad \delta(r) < \delta(b) \ .$$

La función δ se suele denominar *función euclidea*.

Teorema 6.9. *Todo D.E. es un D.I.P.*

Ejemplo 6.10. El anillo de enteros racionales $\mathbb{Z}$ es un D.E. con la función $\delta(a) := |a|$.

Ejemplo 6.11. El anillo de polinomios con coeficientes en un cuerpo es un D.E. con función euclidea $\delta(f) := 2^{\mathsf{gr}(f)}$. En este caso, es más conveniente considerar el grado y polinomio nulo como caso a parte.

Ejemplo 6.12. En $\mathbb{Z}[i]$, la función $\delta(a) = \mathsf{Nm}(a)$ es una función euclidea. Notamos que $\delta(a) \in \mathbb{Z}_{\geq 0}$ para todo $a \in \mathbb{Z}[i]$ y que $\delta(a) = 0$, si y sólo si $a = 0$. Sean $a = m + n\,i$ y $b = x + y\,i$, con $m, n, x, y \in \mathbb{Z}$. Si $b \neq 0$, podemos tomar el cociente a/b:

$$a\,b^{-1} = \frac{a\,\bar{b}}{\mathsf{Nm}(b)} = \frac{(m + n\,i)\,(x + y\,i)}{x^2 + y^2} = \frac{m\,x - n\,y}{x^2 + y^2} + \frac{n\,x + m\,y}{x^2 + y^2}\,i \ .$$

Si bien los coeficientes de $a\,b^{-1}$ son, en principio, racionales, existen $q \in \mathbb{Z}[i]$ y $u, v \in \mathbb{Q}$ tales que $|u|, |v| \leq 1/2$ y

$$a\,b^{-1} = q + (u + v\,i) \ .$$

Pero $\mathsf{Nm}(u + v\,i) = u^2 + v^2 \leq 1/2$, con lo cual,

$$a = q\,b + r \ ,$$

donde $r = (u + v\,i)\,b \in \mathbb{Z}[i]$ y $\delta(r) \leq (1/2)\delta(b)$.

Ejemplo 6.13. En el anillo $\mathbb{Z}[\sqrt{2}]$, definimos $\delta(x + y\,\sqrt{2}) = |x^2 - 2\,y^2|$. Veamos que δ es una función euclidea. Notamos que $\delta(a) = |\mathsf{Nm}(a)|$, donde

$$\mathsf{Nm}(x + y\,\sqrt{2}) = (x + y\,\sqrt{2})\,(x - y\,\sqrt{2}) = x^2 - 2\,y^2 \ .$$

Al igual que en el Ejemplo 6.12, Nm es una función multiplicativa, $\mathsf{Nm}(a) \in \mathbb{Z}$, si $a \in \mathbb{Z}[\sqrt{2}]$ y $\mathsf{Nm}(a) = 0$, si y sólo si $a = 0$. Sean $a, b \in \mathbb{Z}[\sqrt{2}]$ y $b \neq 0$. Entonces, existe $q \in \mathbb{Z}[\sqrt{2}]$ tal que $a\,b^{-1} - q = u + v\,\sqrt{2}$, con $u, v \in \mathbb{Q}$ y $|u|, |v| \leq 1/2$. Dado que

$$\delta(u + v\,\sqrt{2}) \;=\; |u^2 - 2\,v^2| \;\leq\; \frac{1}{4} \;+\; \frac{1}{2}\;,$$

deducimos que $a = q\,b + r$, donde $r = (u + v\,\sqrt{2})\,b$ y $\delta(r) \leq (3/4)\,\delta(b)$.

Ejemplo 6.14. El anillo $\mathbb{Z}[\sqrt{-3}]$ no es D.E. Si quisiéramos repetir el argumento de los ejemplos anteriores, llegaríamos a que $a = q\,b + r$, con $\delta(r) \leq \delta(b)$, donde $\delta(a) = \mathsf{Nm}(a) = x^2 + 3\,y^2$ es la función norma en el anillo. Para ver que no es D.E., probamos que no es un D.F.U. Por ejemplo,

$$(1 + \sqrt{-3})\,(1 - \sqrt{-3}) \;=\; 4 \;=\; 2^2$$

y, tanto 2 como $1 \pm \sqrt{-3}$ son irreducibles no asociados. Que no son asociados, se debe a que las únicas unidades en el anillo son $\{\mathsf{Nm} = \pm 1\} = \{\pm 1\}$.[16] Para ver que son irreducibles, bastará con demostrar que no hay elementos de norma ± 2 en $\mathbb{Z}[\sqrt{-3}]$. Pero $x^2 + 3\,y^2 = \pm 2$, con $x, y \in \mathbb{Z}$ implica $y = 0$ y $x^2 = 2$, que no tiene solución.

Ejemplo 6.15. El anillo $\mathbb{Z}[\sqrt{-5}]$ no es un D.F.U., por el Ejemplo 2.24. En particular, no es D.I.P., ni tampoco es D.E. El argumento con la norma no funciona: quedaría $\delta(r) \leq (5/4)\,\delta(b)$.

Ejemplo 6.16. El anillo $\mathbb{Z}[w]$, donde $w = \frac{1+\sqrt{-3}}{2}$, es un D.E. Nuevamente, tomamos la función $\delta(a) = |\mathsf{Nm}(a)|$. Para demostra que este anillo es euclideo, notamos que

$$\mathbb{Z}[w] \;=\; \mathbb{Z} \,\oplus\, \mathbb{Z}\,w \;=\; \tfrac{1}{2}\,\mathbb{Z} \,\oplus\, \tfrac{1}{2}\,\mathbb{Z}\,\sqrt{-3}\;.$$

Es decir, $a \in \mathbb{Z}[w]$, si $a = x + y\,\sqrt{-3}$, donde x e y son enteros o la mitad de un entero. En este anillo, la norma está dada por

$$\mathsf{Nm}(x + y\,\sqrt{-3}) \;=\; x^2 + 3\,y^2\;.$$

Si $a, b \in \mathbb{Z}[w]$ y $b \neq 0$, entonces $a\,b^{-1} \in \mathbb{Q}(w)$. Por lo tanto, existen $q \in \mathbb{Z}[w]$ y $u, v \in \mathbb{Q}$ tales que $a\,b^{-1} = q + (u + v\,\sqrt{-3})$, pero, ahora, $|u|, |v| \leq 1/4$. Entonces, $a = q\,b + r$, donde $r = (u + v\,\sqrt{-3})\,b$ y

$$\delta(r) \;=\; \delta(u + v\,\sqrt{-3})\,\delta(b) \;\leq\; \left(\tfrac{1}{8} + \tfrac{3}{8}\right)\delta(b) \;=\; \tfrac{1}{2}\,\delta(b)\;.$$

Observación 6.17. Un *dominio de Dedekind* –como los anillos de enteros en un cuerpo de números, como en los Ejemplos 6.10, 6.12, 6.13, 6.14, 6.15 y 6.16– es D.I.P., si y sólo si es D.F.U.

[16] C.f. el Ejemplo 2.18.

Ejemplo 6.18. El anillo de polinomios $k[X]$ con coeficientes en un cuerpo es un D.I.P., pues es D.E. Pero el anillo $k[X,Y]$ de polinomios en dos indeterminadas, si bien es D.F.U., no es D.I.P.: el ideal $\langle X, Y\rangle$ no puede ser principal. En el Ejemplo 4.3, mostramos un dominio que no es noetheriano, pero que es D.F.U.

En algún sentido, el anillo $k[X,Y]$ es un ejemplo "genérico" de un D.F.U. que no es D.I.P. De manera similar, podemos obtener un ejemplo genérico de un dominio que no es D.F.U. considerando $k[X,Y,Z,W]/\langle X\,Y - Z\,W\rangle$. Si k es un cuerpo que posee una raíz $i = \sqrt{-1}$, entonces en $k[X,Y,Z]/\left\langle X^2 + Y^2 + Z^2 - 1\right\rangle$ se verifica que

$$(X + Y\,i)\,(X - Y\,i) \;=\; X^2 \,+\, Y^2 \;=\; 1 \,-\, Z^2 \;=\; (1 - Z)\,(1 + Z)\;.$$

7 Polinomios sobre un DFU

En esta sección introducimos el *contenido* de un polinomio con coeficientes en un D.F.U. y demostramos el Lema de Gauss (Lema 7.11), con el objetivo de probar que el anillo de polinomios $D[X]$ es D.F.U., si D lo es. Un corolario importante de este resultado es que todo polinomio irreducible en $D[X]$ es irreducible sobre el cuerpo de fracciones.

Dado un anillo A y un polinomio $f \in A[X]$, diremos que f satisface una propiedad "*sobre* A" o "*en* $A[X]$", si f posee la propiedad en tanto elemento del anillo de polinomios $A[X]$.

Definición 7.1. Dado un dominio íntegro D, existe un cuerpo, $\mathsf{Quot}(D)$, y un morfismo inyectivo de anillos $\mathsf{inc}_D : D \hookrightarrow \mathsf{Quot}(D)$ tal que, para todo anillo B y todo morfismo de anillos $\varphi : D \to B$ tal que $\varphi(D \smallsetminus \{0\}) \subset B^\times$, existe un único morfismo de anillos $\overline{\varphi} : \mathsf{Quot}(D) \to B$ tal que

$$\overline{\varphi} \circ \mathsf{inc}_D \;=\; \varphi\;.$$

El cuerpo $\mathsf{Quot}(D)$ se denomina *cuerpo cociente* o *cuerpo de fracciones* de D; es único salvo único isomorfismo.

Observación 7.2. Si D es un dominio íntegro, entonces $f \in D[X]$ es una unidad, si y sólo si f es constante e invertible en D. Es decir, $D[X]^\times = D^\times$. Además, si $p \in D$ es irreducible, sigue siendo irreducible en $D[X]$.

En lo que resta de esta sección asumimos que D es un dominio íntegro tal que $D \smallsetminus \{0\}$ satisface la condición del M.C.D. Diremos que D *posee M.C.D.*

Observación 7.3. Dado $\gamma \in \mathsf{Quot}(D)$, existen, por definición, $a, b \in D$ tales que $\gamma = a/b$. Asumiendo que D posee M.C.D., podemos elegir a y b coprimos: si $d = \big(a : b\big)$, entonces $a = d\,\tilde{a}$ y $b = d\,\tilde{b}$ y $\gamma = \tilde{a}/\tilde{b}$, pero $\big(\tilde{a} : \tilde{b}\big) \sim 1$, pues, si c es un divisor común de $\tilde{a}$ y de $\tilde{b}$, $d\,c$ es un divisor común de a y de b y, por definición, $d\,c$ divide a d, lo que implica que $c \sim 1$.

Definición 7.4. Dado un polinomio no nulo $f \in D[X]$, definimos el *contenido de* f como el M.C.D. de sus coeficientes: si $f = a_0 + a_1\,X + \cdots + a_n\,X^n \neq 0$, $a_i \in D$, entonces el contenido de f es

$$\mathsf{cont}(f) \;:=\; \big(a_0 \,:\, a_1 \,:\, \cdots \,:\, a_n\big)\;.$$

El contenido está definido salvo asociados en D.

Definición 7.5. Un polinomio $f \in D[X]$ es un *polinomio primitivo*, si $\mathsf{cont}(f) \sim 1$.

Proposición 7.6. *Sea D un dominio que posee M.C.D. Entonces:*

1. *todo polinomio no nulo $f \in D[X]$ se puede expresar como $f = c\,g$, donde $c \in D$ y $g \in D[X]$ es primitivo;*
2. *si $a \in D$ y $f \in D[X]$, entonces $\mathsf{cont}(a\,f) \sim a\,\mathsf{cont}(f)$;*
3. *una expresión para $f \in D[X]$ como en 1 es única módulo asociados: si $f = d\,h$ con $d \in D$ y $h \in D[X]$ primitivo, entonces $d \sim c$ en D y $h \sim g$ en $D[X]$.*

Demostración. Para ver 1, basta con notar que, si $g = \tilde{a}_0 + \tilde{a}_1\,X + \cdots + \tilde{a}_n\,X^n$ y $\tilde{a}_i = a_i/\mathsf{cont}(f)$, entonces $f = \mathsf{cont}(f)\,g$. El ítem 2 se deduce del Lema 5.10:

$$\begin{aligned}\mathsf{cont}(a\,f) \;&=\; \big(a\,a_0 \,:\, a\,a_1 \,\cdots\, a\,a_n\big) \;\sim\; \big(a\,a_0 \,:\, \big(a\,a_1 \,:\, \cdots \,:\, a\,a_n\big)\big)\\ &\sim\; \big(a\,a_0 \,:\, a\,\big(a_1 \,:\, \cdots\, a_n\big)\big) \;\sim\; a\,\big(a_0 \,:\, a_1 \,:\, \cdots \,:\, a_n\big)\;.\end{aligned}$$

Finalmente, si $c\,g = d\,h$ con $c, d \in D$ y $g, h \in D[X]$, entonces, tomando contenido,

$$c\,\mathsf{cont}(g) \;\sim\; \mathsf{cont}(c\,g) \;=\; \mathsf{cont}(d\,h) \;\sim\; d\,\mathsf{cont}(h)\;.$$

Si g y h son primitivos, entonces c y d son asocicados. En tal caso, existe $u \in D^\times$ tal que $c = u\,d$. De la igualdad $c\,g = d\,h$, se deduce que $u^{-1}\,g = h$. Pero u^{-1} es unidad en D y, por lo tanto, unidad en $D[X]$. □

Lema 7.7. *Dado $f \in \mathsf{Quot}(D)[X]$ no nulo, existen $\gamma \in \mathsf{Quot}(D)$ y $g \in D[X]$ primitivo tales que*

$$f \;=\; \gamma\,g\;. \tag{19}$$

Si $f = \delta\,h$ con $\delta \in \mathsf{Quot}(D)$ y $h \in D[X]$ primitivo, entonces existe una unidad $u \in D^\times$ tal que $\gamma = u\,\delta$. En particular, $g \sim h$ en $D[X]$.

Demostración. Los coeficientes de f pertenecen al cuerpo de fracciones de D. Si $b\,f \in D[X]$, tomando contenido, $a = \mathsf{cont}(b\,f) \in D$ y

$$b\,f \;=\; a\,g\;,$$

para algún polinomio primitivo $g \in D[X]$. Así, $f = \gamma\,g$, con $\gamma = a/b$, de lo que se deduce la existencia de una "factorización" de la forma (19). Sean, ahora, $\gamma, \delta \in \mathsf{Quot}(D)$ y $g, h \in D[X]$ polinomios primitivos tales que

$$\gamma\,g \;=\; \delta\,h\;.$$

Si $\gamma = a/b$ y $\delta = c/d$, deducimos que

$$a\,d \;\sim\; \mathsf{cont}((a\,d)\,g) \;=\; \mathsf{cont}((b\,c)\,h) \;\sim\; b\,c\;.$$

Si suponemos, además, que $\big(a : b\big) \sim 1$ y $\big(c : d\big) \sim 1$, entonces

$$\big(a : c\big) \;\sim\; \big(a : b\,c\big) \;\sim\; \big(a : a\,d\big) \;\sim\; a\;.$$

Análogamente, $\big(a : c\big) \sim c$, de lo que se deduce que $a \sim c$. De la misma manera, se deduce que $b \sim d$. Así,

$$\frac{a}{b} \;=\; \frac{v\,c}{w\,d} \;=\; u\,\frac{c}{d}\;,$$

donde $u = w^{-1}\,v$. □

Definición 7.8. Se define el *contenido* de $f \in \mathsf{Quot}(D)[X]$, como cualquier constante $\gamma = \mathsf{cont}(f) \in \mathsf{Quot}(D)$ que verifique que existe $g \in D[X]$ primitivo tal que $f = \gamma\,g$. El contenido está bien definido salvo unidades en D.

Esta definición coincide con la Definición 7.4 para $f \in D[X]$. Como las unidades en $\mathsf{Quot}(D)[X]$ son las constantes no nulas, deducimos el siguiente resultado.

Corolario 7.9. *Sean $f, g \in D[X]$ polinomios primitivos. Si $f \sim g$ sobre $\mathsf{Quot}(D)$, entonces $f \sim g$ en $D[X]$.*

Observación 7.10. Sea $f \in D[X]$ un polinomio primitivo. Si f es constante, entonces $f = \mathsf{cont}(f) \sim 1$ y $f \in D^\times$. Si f no es constante, entonces admite una factorización como producto de irreducibles (necesariamente primitivos). Si f es irreducible, no hay nada que probar. En otro caso, existen $g, h \in D[X]$ no unidades tales que $f = g\,h$ y $\mathsf{gr}(g), \mathsf{gr}(h) \leq \mathsf{gr}(f)$. Dado que los contenidos $\mathsf{cont}(g)$ y $\mathsf{cont}(h)$ dividen a $\mathsf{cont}(f) \sim 1$, los polinomios g y h deben ser primitivos.[17] Como g y h son primitivos, no pueden ser constantes, pues, en caso contrario, serían unidades. Así, $\mathsf{gr}(g)$ y $\mathsf{gr}(h)$ son estrictamente menores que $\mathsf{gr}(f)$. Inductivamente, existen irreducibles $f_1, \ldots, f_s \in D[X]$ tales que $g = f_1 \cdots f_r$ y $h = f_{r+1} \cdots f_s$. En particular, $f = f_1 \cdots f_s$. Vale notar que, sin hipótesis adicionales,

- la factorización de un polinomio primitivo como producto de irreducibles en $D[X]$ no es necesariamente única,
- los irreducibles en $D[X]$ no son necesariamente irreducibles en $\mathsf{Quot}(D)[X]$ y
- el conjunto de polinomios primitivos no es necesariamente un monoide pero
- si $f \in D[X]$ es primitivo y admite una factorización dentro de $D[X]$, la misma debe ocurrir dentro del conjunto de polinomios primitivos.

[17] No usamos multiplicatividad del contenido –esto no es cierto en general–, sino la propiedad de sacar constantes.

Lema 7.11 (Lema de Gauss)**.** *Sobre un D.F.U., el contenido es multiplicativo: si D es D.F.U., dados $f, g \in D[X]$, $\mathsf{cont}(f\,g) = \mathsf{cont}(f)\,\mathsf{cont}(g)$. En particular, el producto de polinomios primitivos en $D[X]$ es primitivo.*

Demostración. Observamos que, si $f = \mathsf{cont}(f)\,\tilde{f}$ y $g = \mathsf{cont}(g)\,\tilde{g}$, donde $\tilde{f}$ y $\tilde{g}$ son polinomios primitivos con coeficientes en D, entonces

$$\mathsf{cont}(f\,g) \;=\; \mathsf{cont}(f)\,\mathsf{cont}(g)\,\mathsf{cont}(\tilde{f}\,\tilde{g})\ .$$

En particular, la demostración se reduce al caso en que f y g son primitivos.

Ahora bien, como D es un D.F.U., satisface la condición de cadenas de divisores. *En particular*, todo elemento no nulo que no es una unidad admite un factor irreducible.[18] Si $\mathsf{cont}(f\,g) \not\sim 1$, es decir, no es una unidad, existe algún irreducible $p \in D$ que lo divide. Como D posee M.C.D., por la Proposición 5.9, satisface la condición de primalidad. Esto implica que el factor p es primo y que el cociente $D/\langle p\rangle$ es un dominio íntegro (más aun, un cuerpo). En particular, el anillo de polinomios $\big(D/\langle p\rangle\big)[X]$ es un dominio. Pasando, entonces, al cociente,

$$f\,g \equiv 0 \quad \text{implica} \quad f \equiv 0 \quad \text{o} \quad g \equiv 0$$

en $\big(D/\langle p\rangle\big)[X]$. Pero esto significa que, o bien $p|\mathsf{cont}(f)$, o bien $p|\mathsf{cont}(g)$. □

Observación 7.12. En la demostración del Lema 7.11, sólo usamos la existencia de factores irreducibles (no de factorización en irreducibles) y la condición de primalidad, sobre un dominio. Puesto que no sé si estas condiciones son suficientes para garantizar que D es D.F.U., seguiré asumiendo la condición más fuerte.

Lema 7.13. *Sea D un D.F.U. y sea $f \in D[X]$ un polinomio no constante. Si f es irreducible en $D[X]$, entonces f es irreducible en $\mathsf{Quot}(D)[X]$.*

Demostración. Si f no fuese irreducible en $\mathsf{Quot}(D)[X]$, existirían polinomios g y h con coeficientes en $\mathsf{Quot}(D)$, ambos no constantes y tales que $f = g\,h$. Limpiando denomiadores, podemos asumir que $f = \gamma\,g\,h$, donde g y h tienen coeficientes en D y $\gamma \in \mathsf{Quot}(D)$ es una constante. Podemos asumir, también, que g y h son primitivos, incorporando el contenido de éstos a γ. Por el Lema 7.11,

$$\mathsf{cont}(f) \;\sim\; \gamma\ ,$$

es decir, $\mathsf{cont}(f) = u\,\gamma$, donde $u \in D^{\times}$. Pero esto implica que $\gamma \in D$ y que f se factoriza en $D[X]$. □

Teorema 7.14. *Si D es D.F.U., $D[X]$ es D.F.U., también.*

[18] C.f. la demostración del Teorema 4.4 ¿Es, esta condición, equivalente a la condición de cadenas de divisores? Notemos que usamos que todo elemento no unidad posee, al menos, un factor irreducible, pero no que todo elemento no unidad posee una factorización como producto de irreducibles.

Demostración. Sea $f \in D[X]$. Si f es constante, entonces f se factoriza de manera esencialmente única en D y, por la Observación 7.2, también en $D[X]$. Supongamos que f no es constante. Entonces $f = c\,g$, donde $c = \mathsf{cont}(f)$ y $g \in D[X]$ es primitivo de grado positivo. Por la Observación 7.10, existen $f_1, \ldots, f_s \in D[X]$ irreducibles no constantes tales que $g = f_1 \cdots f_s$. Como D es D.F.U., existen irreducibles $p_1, \ldots, p_k \in D$ tales que $c = p_1 \cdots p_k$. Por la Observación 7.2, los p_i son irreducibles en $D[X]$ y

$$f \;=\; p_1 \cdots p_k \, f_1 \cdots f_s$$

es una factorización de f como producto de irreducibles en $D[X]$. Notemos que $\mathsf{cont}(f) \sim p_1 \cdots p_k$ y que $\mathsf{cont}(f_1 \cdots f_s) = \mathsf{cont}(g) \sim 1$.[19]

Sean $p_1, \ldots, p_k, q_1, \ldots, q_l \in D$ irreducibles y $g_1, \ldots, g_s, h_1, \ldots, h_t \in D[X]$ de grado positivo e irreducibles, tales que

$$f \;:=\; p_1 \cdots p_k \, g_1 \cdots g_s \;=\; q_1 \cdots q_l \, h_1 \cdots h_t \;.$$

Como D es D.F.U., por el Lema 7.13, los polinomios g_i y h_j son irreducibles sobre $\mathsf{Quot}(D)$. Pero el anillo de polinomios $\mathsf{Quot}(D)[X]$ es D.I.P. y, en particular, D.F.U. En consecuencia, $s = t$ y, más aun, existe una permutación de $\{1, \cdots, s\}$, j, tal que $g_i \sim h_{j(i)}$ en $\mathsf{Quot}(D)[X]$. Por el Corolario 7.9, $g_i \sim h_{j(i)}$ en $D[X]$. Ahora, por el Lema 7.7, existe una unidad $u \in D^\times$ tal que

$$p_1 \cdots p_k \;=\; u \, q_1 \cdots q_l \;.$$

En particular, como D es D.F.U., $k = l$, también. Más aun, existe una permutación de $\{1, \cdots, k\}$, j, tal que $p_i \sim q_{j(i)}$. En definitiva, la factorización de un polinomio no constante $f \in D[X]$ es esencialmente única, también. □

Corolario 7.15. *Si D es un D.F.U. y $f \in D[X]$ es mónico, entonces todo factor mónico de f en $\mathsf{Quot}(D)[X]$ tiene coeficientes en D.*

Corolario 7.16. *Sea F un cuerpo y sea t un elemento trascendente sobre F. Si $f \in F[X]$ es un polinomio irreducible, entonces f es irreducible en $F(t)[X]$.*

Corolario 7.17. *Sea $f \in \mathbb{Z}[X]$ un polinomio mónico con coeficientes enteros. Si $x \in \mathbb{Q}$ es una raíz de f, entonces $x \in \mathbb{Z}$.*

Corolario 7.18 (criterio de irreducibilidad de Eisenstein)**.** *Sea $f = a_0 + a_1\,X + \cdots + a_n\,X^n \in \mathbb{Z}[X]$ para el cual existe un primo $p \in \mathbb{Z}$ tal que*

- *$p | a_i$, si $0 \leq i < n$,*
- *$p \nmid a_n$ y*
- *$p^2 \nmid a_0$.*

Entonces f es irreducible sobre $\mathbb{Q}$.

[19] No es aquí que usamos la hipótesis de factorización, sino antes para factorizar c. Esto es cierto, sólo porque primero separamos f como producto de su contenido y un primitivo. En general, debemos usar más insistentemente la hipótesis.

Referencias

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969). 1969.

[2] N. Jacobson. *Basic algebra I. 2nd ed*. New York: W. H. Freeman and Company. XVIII, 499 p. £ 19.95 (1985). 1985.

[3] S. MacLane and G. Birkhoff. *Algebra.* 3rd. ed. New York etc.: Chelsea Publishing Company, 1999.

[4] J. S. Milne. *Group Theory (v4.00)*. Available at www.jmilne.org/math/. 2021.

[5] I. R. Shafarevich. *Basic Algebraic Geometry 1. Varieties in Projective Space. Translated from the Russian by Miles Reid*. 3rd ed. Berlin: Springer, 2013.