Tema 6

Dominios de Factorización Única

Recordemos que un elemento p en un Dominio de Integridad A es *irreducible* si no es cero ni unidad y sus únicos divisores son los triviales, esto es, las unidades y sus asociados, esto es, si no se pueden factorizar como $p = ab$ donde ni a ni b son unidades.

Definición 6.0.1. *Un Dominio de Factorización Única (DFU) es un dominio de integridad A en el cual todo elemento no nulo ni unidad $a \in A$ se puede expresar como un producto*

$$a = p_1 \cdots p_s$$

donde cada p_i es irreducible, y tal factorización es "esencialmente única", en el sentido si $a = q_1 \cdots q_t$ es otra, con cada q_j irreducible, entonces $s = t$ y hay una permutación $\sigma : \{1, \ldots, s\} \cong \{1, \ldots, s\}$ tal que cada p_i y $q_{\sigma(i)}$ son asociados.

Ejemplo. Las factorizaciones de -6 en $\mathbb{Z}$, $(-2) \cdot 3 = (-3) \cdot 2 = 3 \cdot (-2)$ son esencialmente la misma.

Si dos elementos del anillo son asociados, tienen los mismos divisores y, por tanto, uno es irreducible si y solo si lo es el otro. En un DFU, A, siempre podemos seleccionar un "*conjunto P, representativo de todos los irreducibles*", en el sentido que: (1) Todo elemento de P es irreducible, (2) Todo irreducible es asociado con uno de P, y (3) dos elementos distintos de P no son asociados. Por ejemplo, si $A = \mathbb{Z}$, podemos tomar como P el conjunto de los irreducibles positivos, y si $A = K[x]$ con K un cuerpo, podemos tomar como P el conjunto de los irreducibles mónicos (de coeficiente líder 1). En tal caso, cada elemento $a \in A$, $a \neq 0$, admite una factorización esencialmente única de la forma

$$a = up_1^{e_1} \cdots p_r^{e_r} = u \prod_{i=1}^{r} p_i^{e_i}, \tag{6.1}$$

donde u es una unidad, $r \geq 0$ ($a = u$ si $r = 0$), cada $p_i \in P$, cada exponente $e_i \geq 1$ es un entero positivo, y $p_i \neq p_j$ si $i \neq j$. En efecto, si a no es una unidad y $a = q_1 \cdots q_s$ es cualquier factorización en irreducibles de a, tendremos cada $q_j = u_j p_j$, con $p_j \in P$, para cierta unidad u_j. Entonces, tomando $u = u_1 \cdots u_t$, tendremos $a = up_1 \cdots p_t$, con $p_j \in P$, y u una unidad. Finalmente, reordenando loos factores irreducibles y agrupando todos los que se repitan, obtenemos una tal expresión de a.

Para cada elemento del DFU $a \in A$, $a \neq 0$, cuya factorización sea la dada en (6.1), y cada irreducible $p \in P$, denotaremos por

$$e(p, a)$$

al exponente con que p aparece en la factorización de de a, acordando que $e(p, a) = 0$ si p no aparece en la factorización. Esto es, para cada $i = 1, \ldots, r$, $ep_i, a) = e_i$, y para cualquier $p \notin \{p_1, \ldots, p_r\}$, ponemos $e(p, a) = 0$. Puesto que en tal caso es $p^{e(p,a)} = 1$, podemos usar la expresión

$$a = u \prod_{p \in P} p^{e(p,a)},$$

donde en realidad solo intervienen un número finito de factores distintos de uno, para indicar la factorización en irreducibles del elemento. Esta es útil para observar que en todo DFU hay mcd y mcm de cualesquiera dos elementos

Lema 6.0.2. *(i) Para cualesquiera elementos no nulos $a, b \in A$, y $p \in P$, se verifica que*

$$e(p, ab) = e(p, a) + e(p, c).$$

(ii) Para cualesquiera elementos no nulos $a, c \in A$, se verifica que

$$a|c \Leftrightarrow e(p, a) \leq e(p, c), \quad \forall p \in P.$$

Demostración. Si $a|c$ será $c = ab$ para un cierto b, pero entonces

$$e(p, c) = e(p, a) + e(p, b) \geq e(p, a).$$

Recíprocamente, si $a = u \prod_{p \in P} p^{e(p,c)}$, $c = v \prod_{p \in P} p^{e(p,c)}$, y $e(p, a) \leq e(p, c)$, para todo $p \in P$, definiendo $b = u^{-1} v \prod_{p \in P} p^{e(p,c)-e(p,a)}$, claramente $ab = c$ y $a|c$. ■

Proposición 6.0.3. *En un DFU existen mcd y mcm de cualesquiera elementos. Para $a, b \neq 0$, se tiene que*

$$mcd(a, b) = \prod_{p \in P} p^{min\{e(p,a), e(p,b)\}}, \qquad mcm(a, b) = \prod_{p \in P} p^{max\{e(p,a), e(p,b)\}}.$$

Demostración. Para cualquier $c \neq 0$, se tiene que $c|a$ y $c|b$ si y solo si, para todo $p \in P$, $e(p, c) \leq e(p, a)$ y $e(p, c) \leq e(p, a)$; esto es, si y solo si $e(p, c) \leq min\{e(p, b), e(p, b)$. Entonces $c|a$ y $c|b$ si y solo si $c| \prod_{p \in P} p^{min\{e(p,a), e(p,b)\}}$. ■

6.1 Caracterización de DFU

Definición 6.1.1. *Sea A un DI. Un elemento $p \in A$, no nulo ni unidad, se dice que es "primo" si verifica la siguiente propiedad*

$$p|ab \Rightarrow p|a \vee p|b.$$

En otras palabras, si p no divide a dos elementos, entonces tampoco divide a su producto.

Proposición 6.1.2.
(i) En cualquier DI, todo primo es irreducible.
(ii) En un DFU, un elemento es primo si y solo si es irreducible.

Demostración.

(*i*) Sea p es primo. Veamos que sus unicos divisores son los triviales. Supongamos que a es un divisor de p, y que no es asociado. Entonces p no divide a a. Como existirá un b tal que $p = ab$, y p es primo, será $p|a$ o $p|b$. Necesariamente entonces $p|b$. Pero $b|p$ y p y b serán asociados. Digamos que $p = ub$, con u una unidad. Entonces, $ub = ab$, implica que $a = u$, y a es unidad.

(*ii*) Sea p un irreducible en un DFU, que podemos suponer en P, y supongamos que $p|ab$. Entonces $1 = e(p,p) \leq e(p,ab) = e(p,a) + e(p,b)$. Necesariamente entonces $e(p,a) \geq 1$ o $e(p,b) \geq 1$. Luego $p|a$ o $p|b$. ■

Teorema 6.1.3. *Sea A un DI. Son equivalentes,*

(1) *A es un DFU.*

(2) $\begin{cases} \bullet \text{ todo elemento no nulo ni unidad es producto de irreducibles.} \\ \bullet \text{ existe mcd de todo par de elementos.} \end{cases}$

(3) $\begin{cases} \bullet \text{ todo elemento no nulo ni unidad es producto de irreducibles.} \\ \bullet \text{ todo irreducible es primo.} \end{cases}$

Demostración. La implicación (1) $\Rightarrow$ (2) es clara. Para ver que (2) $\Rightarrow$ (3), sea p un irreducible y supongamos que no divide ni a a ni a b. Entonces $(p,a) = 1 = (p,b)$. Entonces $b = b1 = b(p,a) = (pb, ab)$ y

$$1 = (p,b) = (p,(pb,ab)) = ((p,pb),ab) = (p(1,b),ab) = (p,ab),$$

de donde concluimos que p no divide a ab. Así que p es primo.

Veamos ahora que (3) $\Rightarrow$ (1), o sea la unicidad de las factorizaciones: Supongamos $p_1 \cdots p_r = q_1 \cdots q_s$, con los p_i y los q_j irreducibles, es decir primos en este caso. Hacemos inducción sobre $r \geq 1$. Si $r = 1$, tenemos que $p_1 = q_1 \cdots q_s$. Como p_1 es irreducible y los q_j no son unidades, ha de ser $m = 1$ y $q_1 = p_1$. Supongamos ahora $r > 1$ y damos por válido la unicidad de las factorizaciones en irreducibles donde una de ellas tiene menos de r factores irreducibles. Como $p_r|q_1 \cdots q_s$, y p_r es primo, ha de existir un j con $p_r|1q_j$. Pero p_r no tiene divisores propios, luego p_r y q_j han de ser asociados. Renumerando si es necesario, podemos suponer que $q_s = up_r$ para una cierta unidad u. Nos queda entonces

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-2}(uq_{s-1}).$$

Entonces, por hipótesis de inducción $s = r$ y, salvo renumeración, cada p_i es asociado con el correspondiente q_i. □.

6.2 Todo DE es un DFU

Ya sabemos que en todo DE hay mcd de cualquier par de elementos. Bastará probar que en un DE, digamos A, todo elemento no nulo ni unidad factoriza en producto de irreducibles. Para ello, primero observamos: *Si a es un divisor propio de b, entonces $\rho(a) < \rho(b)$.* Si fuese $\rho(a) \geq \rho(b)$, entonces $\rho(a - bq) < \rho(b) \leq \rho(a)$ para algún $q \in A$; pero $b = ac$ para algún $c \in A$ y, sustituyendo, tenemos que $\rho(a - acq) < \rho(a)$. Pero $\rho(a - acq) = \rho(a(1 - cq)) \geq \rho(a)$, lo que es una contradicción.

Veamos todo elemento no nulo ni unidad factoriza en producto de irreducibles. Supongamos, por el contrario que eso es falso, esto es, que hay elementos, que son cero ni unidad, que no factorizan en producto de irreducibles, y hagamos la siguiente observación:

Si a es un tal elemento, hay un divisor propio a' de a que tampoco admite una tal factorización.

En efecto, ese a no sería un irreducible y tendría una factorización como $a = bc$, con b y c divisores propios de a. Si ambos se pudieran factorizar como producto de irreducibles, $b = p_1 \cdots p_r$ y $b = q_1 \cdots q_s$, es claro que el propio a se factorizaría $a = p_1 \cdots p_r q_1 \cdots q_s$. Luego al menos uno de ellos no tiene una tal factorización. Sea a' ese elemento. Formemos la sucesión de elementos $a_1, a_2, \ldots, a_n, \ldots$, por la regla $a_1 = a$, y $a_{n+1} = a'_n$. Por construcción cada $a_{n+1} | a_n$ y es un divisor propio. Entonces $\rho(a_n) > rho(a_{n+1})$ y la cadena de naturales $\rho(a) = \rho(a_1) > \rho(a_2) > \cdots > \rho(a_n) > \cdots$, es infinita! □

Como corolario inmediato, tenemos que

Teorema 6.2.1 (Teorema fundamental de la Aritmética)**.**
El anillo de los enteros $\mathbb{Z}$ es un Dominio de Factorización Única.

Pero también los anillos de polinomios $K[x]$, con K un cuerpo, son DFU. También el anillo de los enteros de Gauss $\mathbb{Z}[i]$, o $\mathbb{Z}[\sqrt{2}]$, etc, son DFU.

El siguiente teorema es históricamente muy relevante

Teorema 6.2.2 (Euclides)**.** *En $\mathbb{Z}$ hay infinitos primos positivos.*

Demostración. Supongamos, por el contrario, que solo hubiera un número finito de ellos, digamos $p_1, \ldots, p_r$. En número $m = 1 + p_1 \cdots p_r$ no es cero ni unidad, tendrá una factorización en producto de primos. Habrá entonces un p_i de los anteriores que divida a m. Pero entonces, ese p_i dividirá a $m - p_1 \cdots p_r = 1$, lo que es imposible. ■

6.3 Irreducibles y primos en $\mathbb{Z}[\sqrt{n}]$

Lema 6.3.1. *Si α es un divisor propio de β en $\mathbb{Z}[\sqrt{n}]$, entonces $N(\alpha)$ es un divisor propio de $\mathbb{N}(\beta)$ en $\mathbb{Z}$.*

Demostración. Será $N(\alpha) \neq \pm 1$, y existe un α' con $N(\alpha') \neq \pm 1$ tal que $\beta = \alpha\alpha'$ con $N(\alpha') \neq \pm 1$. Pero entonces la igualdad $N(\beta) = N(\alpha)N(\alpha')$ nos dice que $N(\alpha)$ es un divisor propio de $\mathbb{N}(\beta)$ en $\mathbb{Z}$. ■

Proposición 6.3.2. *Sea $\alpha \in \mathbb{Z}[\sqrt{n}]$.*
(1) *Si $N(\alpha) = \pm p$, con p primo de $\mathbb{Z}$, entonces α es irreducible.*
(2) *Si α es primo en $\mathbb{Z}[\sqrt{n}]$, entonces $N(\alpha) \in \{\pm p, \pm p^2\}$, con $p \geq 2$ un primo de $\mathbb{Z}$. Además, si $N(\alpha) = \pm p^2$, entonces α y p son asociados en $\mathbb{Z}[\sqrt{n}]$.*

Demostración.
(1) Por el Lema 6.3.1 anterior, si α tuviera divisores propios, $N(\alpha) = \pm p$ los tendría. Luego α es irreducible.

(2) Supongamos α es primo. Observemos primero que hay un p primo de $\mathbb{Z}$ tal que $p = \alpha\beta$ para algún $\beta \in \mathbb{Z}[\sqrt{n}]$: En efecto, si $N(\alpha) = p_1 \cdot p_r$ con p_i primos de $\mathbb{Z}$, como $\mathbb{N}(\alpha) = \alpha\overline{\alpha}$, tenemos que $\alpha | p_1 \cdots p_r$, y como α es primo, será α / p_i para algún i, así que $p_i = \alpha\beta$ para algún β.

De la igualdad $p = \alpha\beta$, deducimos que $p^2 = N(\alpha)N(\beta)$. Entonces, $N(\alpha) | N(p) = p^2$ en $\mathbb{Z}$. Luego $N(\alpha) \in \{\pm p, \pm p^2\}$ (no puede ser ± 1 pues α no es unidad). Además, si $N(\alpha) = \pm p^2$, tendremos que $p^2 = N(\alpha)N(\beta) = \pm p^2 N(\beta)$, de donde $N(\beta) = \pm 1$, y β es unidad. Como $p = \alpha\beta$, p y α son asociados. ■

Nota. Si $N(\alpha) = p^2$, con p un primo de $\mathbb{Z}$, no tiene por qué ser α irreducible (ni primo, entonces). Por ejemplo, en $\mathbb{Z}[i]$, $N(2) = 2^2$, pero no es irreducible: $2 = (1+i)(1-i)$.

EJEMPLOS.

1. *Factorizar $11 + 7i$ en producto de irreducibles (= primos) en el anillo $\mathbb{Z}[i]$.*

Como $\mathbb{Z}[i]$ es un DE, es un DFU y tal factorización existe. Observemos que su norma es $N(11+7i) = 11^2+7^2 = 170 = 2\cdot 5\cdot 17$. Claramente $11+7i$ no es irreducible, pues su norma no es un primo, ni el cuadrado de un primo de $\mathbb{Z}$. Si α es un divisor primo de $11+7i$, su norma será un divisor propio de 170 y será un primo o el cuadrado de un primo de $\mathbb{Z}$. Pero ningún primo al cuadrado de $\mathbb{Z}$ divide a 170, luego la norma de ese divisor primo habrá de ser 2, 5 o 17. Veamos que tiene un divisor primo de norma 2: Enteros de Gauss de norma 2, son los $\alpha = a+bi$ tal que $a^2+b^2 = 2$, o sea $a = \pm 1 \wedge b \pm 1$. Esto es, $\alpha = 1+i$ y sus asociados $(-1+i, -1-i, 1-i)$. Como

$$\frac{11+7i}{1+i} = \frac{(11+7i)(1-i)}{2} = \frac{11-11i+7i+7}{2} = \frac{18-4i}{2} = 9-2i \in \mathbb{Z}[i],$$

obtenemos que $1+i|11+7i$ y, de hecho, $11+7i = (1+i)(9-2i)$, donde $1+i$ es irreducible al ser de norma 2.

Nos centramos ahora en $9-2i$.

Como $N(9-2i) = 81+4 = 85 = 5\cdot 17$, este no es irreducible. Busquemos divisores de norma 5:

Si $N(a+bi) = 5$, será porque $a^2+b^2 = 5 \Leftrightarrow (a = \pm 2 \wedge b = \pm 1) \vee (a = \pm 1 \wedge b = \pm 2)$. Esto es, $2+i$ y sus asociados $(-2-2i, -1+2i, 1-2i)$ y $1+2i$ y sus asociados $(-1-2i, -2+i, 2-i)$. Veamos si $2+i/9-2i$:

$$\frac{9-2i}{2+i} = \frac{(9-2i)(2-i)}{5} = \frac{18-9i-4i-2}{5} = \frac{16-13i}{5} \notin \mathbb{Z}[i].$$

Veamos si $1+2i|9-2i$:

$$\frac{9-2i}{1+2i} = \frac{(9-2i)(1-2i)}{5} = \frac{9-18i-2i-4}{5} = \frac{5-20i}{5} = 1-4i \in \mathbb{Z}[i].$$

así que $1+2i|9-2i$ y, $9-2i = (1+2i)(1-4i)$, donde $1+2i$ es primo al ser de norma 5. Pero $(1-4i$ también, al ser de norma $1+16 = 17$ primo de $\mathbb{Z}$.

Conclusión, la factorización pedida es $11+7i = (1+i)(1+2i)(1-4i)$. □

2. *Calcular $(2i, 11+7i)$ y $[2i, 11+7i]$ en $\mathbb{Z}[i]$.*

Como $2i$ es asociado con 2, podemos sustituir $2i$ por 2 en la cuestión. Buscamos la factorización en primos de $2i$ en $\mathbb{Z}[i]$: Como $N(2i) = 4 = 2^2$, Bien $2i$ es irreducible o tiene un factor irreducible de norma 2. Antes hemos visto que los enteros de Gauss de norma 2 son $1+i$ y sus asociados. Luego 2 es irreducible, o es divisible por $1+i$:

$$\frac{2i}{1+i} = \frac{2i(1-i)}{2} = \frac{2i+2}{2} = 1+i \in \mathbb{Z}[i].$$

así que $2 = (1+i)^2$ es la factorización del 2 en irreducibles en $\mathbb{Z}[i]$. Entonces,

$$(2i, 11+7i) = ((1+i)^2, (1+i)(1+2i)(1-4i)) = 1+i.$$

$[2i, 11+7i] = [(1+i)^2, (1+i)(1+2i)(1-4i)] = (1+i)^2(1+2i)(1-4i) = 2i(9-2i) = 4+18i.$ □

3. *Factorizar* 180 *en producto de irreducibles (= primos) en el anillo* $\mathbb{Z}[\sqrt{-2}]$.

En $\mathbb{Z}$ tenemos que $180 = 2 \cdot 90 = 2^2 \cdot 45 = 2^2 \cdot 3^3 \cdot 5$. Busquemos las factorizaciones en $\mathbb{Z}[\sqrt{-2}]$ de 2, 3 y 5.

Para factorizar 2, como $N(2) = 4$, bien 2 es irreducible o es divisible por un irreducible de norma 2: $N(a + b\sqrt{2-}) = a^2 + 2b^2 = 2 \Leftrightarrow b = \pm 1 \wedge a = 0$. El único irreducible de norma 2 es $\sqrt{-2}$, y su asociado $-\sqrt{-2}$:

$$\frac{2}{\sqrt{-2}} = \frac{2 \cdot (-\sqrt{-2})}{2} = -\sqrt{-2},$$

Luego $2 = \sqrt{-2}(-\sqrt{-2}) = -(\sqrt{-2})^2$ es la factorización de 2 en producto de irreducibles.

Para factorizar 3, como $N(3) = 9$, bien 3 es irreducible o es divisible por un irreducible de norma 3: $N(a + b\sqrt{2-}) = a^2 + 2b^2 = 3 \Leftrightarrow b = \pm 1 \wedge a = \pm 1$. Los únicos irreducibles de norma 3 son $1 + \sqrt{-2}$, $1 - \sqrt{-2}$, y sus asociados $-1 - \sqrt{-2}$ y $-1 + \sqrt{-2}$:

$$\frac{3}{1 + \sqrt{-2}} = \frac{3 \cdot (1 - \sqrt{-2})}{3} = 1 - \sqrt{-2},$$

Luego $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ es la factorización de 3 en producto de irreducibles.

Para factorizar 5, como $N(5) = 5^2$, bien 5 es irreducible o es divisible por un irreducible de norma 5: Pero en $\mathbb{Z}[\sqrt{-2}]$ no existen elementos de norma 5, pues $N(a+b\sqrt{2-}) = a^2+2b^2 = 5$ y vemos que no existen tales a y b. Luego 5 es irreducible en $\mathbb{Z}[\sqrt{-2}]$.

Conclusión: La factorización buscada es

$$180 = (-5)(\sqrt{-2})^2(1 + \sqrt{-2})^3(1 - \sqrt{-2})^3,$$

salvo orden y asociados. □

4. *En* $\mathbb{Z}[\sqrt{-5}]$ *hay irreducibles que no son primos.*

Ya vimos que en este anillo no hay mcd de cualesquiera par de elementos. Por tanto no es un DFU. Veamos ahora que hay irreducibles que no son primos y como hay factorizaciones en irreducibles que no son equivalentes. Consideremos $1 + \sqrt{-5}$, su norma es $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6 = 2 \cdot 3$. Si $1 + \sqrt{-5}$ no fuese irreducible, tendría divisores de norma 2 o 3. Pero no hay elementos en este anillo de tales normas (la ecuaciónes $a^2 + 5b^2 = 2$ y $a^2+5b^2 = 3$, no tienen soluciones en $\mathbb{Z}$). Luego $1+\sqrt{-5}$ es irreducible y, por la misma razón, $1 - \sqrt{-5}$ también lo es, así como lo son 2 y 3 (cuyas normas son 4 y 9, respectivamente).

Ahora, 2 no es primo, pues $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ y, sin embargo, 2 no divide a $(1 + \sqrt{-5})$ ni a $(1 - \sqrt{-5})$. Si dividiese a alguno de ellos, tomando normas, 4 dividiría a 6, lo que no ocurre. Por la mismas razones 3, $1 + \sqrt{-5}$ y $1 + \sqrt{-5}$ son todos irreducibles pero no primos.

Finalmente, destaquemos que las dos factorizaciones del 6 en producto de irreducibles

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

son esencialmente diferentes, pues los irreducibles que intervienen no son asociados. □

6.4 Factorización única en anillos de polinomios

Conocemos que, si K es un cuerpo, entonces $K[x]$ es un DE y, por tanto, un DFU. Pero hay anillos de polinomios interesantes, por ejemplo $\mathbb{Z}[x]$, que son DFU aun no siendo Dominios Euclídeos.

Vamos, con generalidad, a estudiar el carácter DFU de un anillo $A[x]$ donde el anillo de coeficientes A es un DFU. En lo que sigue, denotaremos por $K = \mathbb{Q}(A)$ al cuerpo de fracciones de A, y tendremos muy en cuenta que $A[x] \subseteq K[x]$ es un subanillo.

Para demostrar que $A[x]$ es un DFU, utilizaremos que $K[x]$ lo es, y necesitaremos relacionar los irreducibles de estos anillos. Una primera observación al respecto concierne a los irreducibles de grado cero de $A[x]$. Notemos que en $K[x]$ no hay irreducibles de grado cero (pues todos son unidades).

Lema 6.4.1. *Un elemento $a \in A$ es irreducible en $A[x]$ si y solo si lo es en A.*

Demostración. Si a es irreducible en A y $a = fg$ en $A[x]$, necesariamente f y g serían de grado cero. Esto es $f = b \in A$ y $g = c \in A$. Entonces $a = bc$ en A y b o c son unidades de A, o sea f o g unidades de $A[x]$. Luego a es irreducible en $A[x]$. Reciprocamente, si a es irreducible en $A[x]$, y $a = bc$ en A, esa misma factorización es válida en $A[x]$ y por tanto b o c es una unidad de $A[x]$, o sea de A. ■

Para polinomios de grado ≥ 1, el siguiente concepto es muy útil.

Definición 6.4.2. *Se define el "contenido" de un polinomio $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, $n \geq 1$, como el mcd de sus coeficientes, esto es*

$$c(f) = (a_0, \ldots, a_n).$$

Decimos que f es "primitivo" si $c(f) = 1$.

Lema 6.4.3.

(i) Para cualquier $a \in A$ y $f \in A[x]$, de grado ≥ 1, se verifica que $c(af) = a\,c(f)$.

(ii) Todo polinomio $g \in A[x]$, de grado ≥ 1, se expresa de forma única como $g = af$, donde $a = c(g) \in A$ y $f \in A[x]$ es primitivo.

(iii) Todo polinomio no nulo $\phi \in K[x]$, de grado ≥ 1, se expresa de forma única como $\phi = \frac{a}{b}f$, donde $\frac{a}{b} \in K$ y $f \in A[x]$ es primitivo.

Demostración.

(i) $(aa_0, \ldots, aa_n) = a(a_0, \ldots, a_n)$.

(ii) Supongamos que $f = a_0 + a_1x + \cdots + a_nx^n$ y sea $a = c(f)$. Pongamos $a_i = c\,a_i'$ y $g = a_0' + a_1'x + \cdots + a_n'x^n$. Tenemos $f = ag$ y, como $a = c(ag) = a\,c(g)$, necesariamente $c(g) = 1$ (pues $a \neq 0$). Para la unicidad, si $ag = bh$, con g, h ambos primitivos, tomando contenidos tendríamos $a\,c(g) = b\,c(h)$, o sea que $a = b$, de donde también $g = h$.

(iii) Supongamos que $\phi = \sum_{i\geq 0}^{n} \frac{a_i}{b_i}x^i$. Si $b = \prod_{i\geq 0} b_i$, entonces $b\phi = \sum_{i\geq 0}^{n} \frac{ba_i}{b_i}x^i$. Claramente $\frac{ba_i}{b_i} = c_i \in A$, así que $b\phi \in A[x]$. Pongamos $b\phi = af$, con f primitivo. Entonces $\phi = \frac{a}{b}f$ en las condiciones anunciadas. Para la unicidad, supongamos que $\phi = \frac{a'}{b'}f'$, con $f' \in A[x]$ primitivo. Entonces de la igualdad $ab'f = a'bf'$, resulta que $ab' = a'b$, o sea que $\frac{a}{b} = \frac{a'}{b'}$. Claramente entonces también $f = f'$. ■

Teorema 6.4.4 (Lema de Gauss)**.** *El producto de dos polinomios primitivos es primitivo.*

Demostración. Sean $f = \sum_{i\geq 0} a_i x^i$ y $g = \sum_{j\geq 0} a_j x^j$, ambos primitivos. Pongamos $fg = \sum_{k\geq 0} c_k x^k$, donde cada $c_k = \sum_{i+j=k} a_i b_j$, y supongamos que fg no es primitivo. Como A es un DFU, existirá algún irreducible $p \in A$ tal que $p|c(fg)$, esto es, tal que $p|c_k$ para todo k. Como f y g son primitivos, ese irreducible p no puede dividir a todos los a_i ni a todos los b_j. Sear a_r el primer coeficiente de f que no es divisible por p y b_s el primero de g que no es divisible por p. Como p es primo, entonces p no divide a $a_r b_s$. Pero $p|c_{r+s}$ y tenemos que

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = \sum_{i<r} a_i b_{r+s-i} + a_r b_s + \sum_{i>r} a_i b_{r+s-i}.$$

Para todo $i < r$ tenemos que $p|a_i$ y para todo $i > r$ tenemos que $p|b_{r+s-i}$ (pues $r + s - i < r + s - r = s$). Entonces p divide a todos los sumandos del primer y del segundo sumatorio. Desde hay, se concluye que $p|c_{r+s}$, lo que es una contradicción. ■

Corolario 6.4.5. *Para todos $f, g \in A[x]$, , de grado ≥ 1, se verifica que $c(fg) = c(f)\, c(g)$.*

Demostración. Como $fg = c(f)c(g)f'g'$, será $c(fg) = c(f)c(g)c(f'g') = c(f)c(g)$. ■

Teorema 6.4.6. *Sea $\phi \in K[x]$ un polinomio, de grado ≥ 1. Supongamos $\phi = \frac{a}{b} f$, donde $f \in A[x]$ es primitivo. Son equivalentes*

1. *ϕ es irreducible en $K[x]$.*
2. *f es irreducible en $K[x]$.*
3. *f es irreducible en $A[x]$.*

Demostración.

Puesto que ϕ y f son asociados en $K[x]$, uno será irreducible si y solo si lo es el otro, así que (1) $\Leftrightarrow$ (2).

(2) $\Rightarrow$ (3): Supongamos que f no es irreducible en $A[x]$. Será $f = f_1 f_2$, con $f_1, f_2 \in A[x]$ no unidades de A. Notemos que ni f_1 ni f_2 son de grado cero (pues si, por ejemplo, $f_1 = a_1 \in A$, entonces $1 = c(f) = a_1 c(f_2)$ y $f_1 = a_1 \in U(A)$). Así que $gr(f_1), gr(f_2) \geq 1$. Pero entonces ni f_1 ni f_2 son unidades en $K[x]$ y la propia igualdad $f = f_1 f_2$ nos dice que f no es irreducible en $K[x]$.

(3) $\Rightarrow$ (2) Supongamos que f no es irreducible en $K[x]$. Será $f = \phi_1\phi_2$, con $\phi_1, \phi_2 \in K[x]$, ambos de grado ≥ 1. Pongamos $\phi_i = \frac{a_i}{b_i} f_i$, $i = 1, 2$, con $f_i \in A[x]$ primitivo. Entonces, la igualdad $f = \frac{a_1 a_2}{b_1 b_2} f_1 f_2$, donde f y $f_1 f_2$ son primitivos, nos lleva a que $\frac{a_1 a_2}{b_1 b_2} = 1$ y $f = f_1 f_2$, donde tanto f_1 como f_2 son de grado ≥ 1. Esto niega que f es irreducible en $A[x]$. ■

Corolario 6.4.7. *Un polinomio $f \in A[x]$ con $gr(f) \geq 1$ es irreducible si y solo si es primitivo e irreducible en $K[x]$.*

Demostración. Si f es irreducible en $A[x]$, necesariamente es primitivo, pues en otro caso $f = c(f)f'$ es una factorización de f donde ninguno de los factores es una unidad. Entonces f es irreducible en $K[x]$ por el teorema 6.4.6 anterior. El recíproco también lo da el teorema 6.4.6 anterior. ■

Teorema 6.4.8 (Teorema de Gauss)**.** *Si A es un DFU, entonces $A[x]$ es un DFU.*

Demostración. Sea $f \in A[x]$, no nulo ni unidad. Probamos primero que f puede factorizarse en producto de irreducibles de $A[x]$. Si f es de grado cero, $f = a$, como A es un DFU, será $a = p_1 \cdots p_r$ con p_i irreducibles de A, y por tanto también irreducibles de $A[x]$. Si f es de

grado ≥ 1, pongamos $f = ag$, con $a = c(f) \in A$ y $g \in A[x]$ primitivo. Si $a \neq 1$, factorizamos $a = p_1 \cdots p_r$ en A, con p_i irreducibles de A, y por tanto también de $A[x]$. Factorizamos ahora g en $k[x]$: $g = \phi_1 \cdots \phi_s$, con los ϕ_j irreducibles de $K[x]$ (en particular todos de grado ≥ 1). Expresamos estos en la forma $\phi_j = \frac{a_j}{b_j} f_j$, con los $f_j \in A[x]$ primitivos. Estos son entonces irreducibles an $A[x]$. Ademas, la igualdad

$$g = \frac{a_1 \cdots a_s}{b_1 \cdots b_s} f_1 \cdots f_s$$

implica que $\frac{a_1 \cdots a_s}{b_1 \cdots b_s} = 1$ y que $g = f_1 \cdots f_s$. Luego

$$f = p_1 \cdots p_r f_1 \cdots f_s$$

es una factorización de f en producto de irreducibles de $A[x]$.

Veamos ahora que en $A[x]$ todo irreducible es primo. Si p es un irreducible de grado cero de $A[x]$, o sea un irreducible de A, y $p|fg$, para $f, g \in A[x]$, será $ph = fg$ para un cierto $h \in A[x]$. Pero entonces $p\,c(h) = c(f)\,c(g)$ en A, y como p es primo en A, será $p|c(f)$ o $p|c(g)$. Entonces $p|f$ o $p|g$, respectivamente.

Supongamos ahora que $f \in A[x]$ es un irreducible de grado ≥ 1, por tanto primitivo y primo en $K[x]$, tal que $f|gh$ en $A[x]$. Puesto que entonces $f|gh$ también en $K[x]$, será $f|h$ o $f|h$ en $K[x]$. Supongamos es $f\phi = g$ para un cierto $\phi \in K[x]$. Pongamos $\phi = \frac{a}{b} f'$ con $f' \in A[x]$ primitivo. Entonces $\frac{a}{b} ff' = g$, de donde $aff' = bg$ y $a = bc(g)$ (pues f y f' son primitivos). Pero entonces $\frac{a}{b} = c(g)$ y $f(c(g)f') = g$, luego $f|g$ en $A[x]$. ■

6.4.1 Criterios básicos de irreducibilidad de polinomios

Nos ocuparemos aquí de mostrar algunos criterios básicos para el reconocimiento de polinomios irreducibles, con interés fundamentalmente en polinomios con coeficientes enteros y racionales. Los casos, también muy interesantes, de polinomios reales y complejos no podemos discutirlos aquí (necesitan conocimientos más elevados), pero si podremos enunciar lo que resulta en estos casos.

Comenzamos con unas observaciones generales sobre polinomios en $K[x]$, con K un cuerpo.

• *En $K[x]$ todo polinomio es asociado con uno "*mónico*"*, esto es, con coeficiente lider 1: En efecto, si $\phi = \alpha_0 + \alpha_1 x + \cdots \alpha_n x^n$ con $\alpha_n \neq 0$, entonces ϕ es asociado con $\psi = \alpha_n^{-1}\phi$, cuyo coeficiente lider es 1. Además, dos polinomios mónicos son asociados si y solo si son iguales. Por tanto, para conocer los irreducibles de $K[x]$ (salvo asociados) basta conocer los irreducibles mónicos.

• *En $K[x]$ no hay irreducibles de grado* 0, pues todos estos son unidades.

Para polinomios de grado 1, tenemos que

Proposición 6.4.9. *Todo polinomio de grado* 1 *en $K[x]$ es irreducible.*

Demostración. Si $\phi \in K[x]$ es de grado 1 y $\phi = \phi_1\phi_2$, tendríamos $1 = gr(\phi_1) + gr(\phi_2)$, lo que obliga a que uno de ellos tenga grado 0, o sea se trata de una unidad de $K[x]$. ■

Así, los irreducibles mónicos de grado 1 en $K[x]$ son todos los polinomios $x + \alpha$, con $\alpha \in K$. Así, por ejemplo, cuando el cuerpo de coeficientes es un $\mathbb{Z}_p$, los irreducibles mónicos de grado 1 son x, $x + 1$, ..., $x + p - 1$. Para polinomios con coeficientes complejos, más adelante se os probara lo siguiente:

Teorema 6.4.10 (Teorema fundamental del Álgebra (Gauss)). *En $\mathbb{C}[x]$ los únicos polinomios irreducibles son los de grado 1.*

El siguiente "*Criterio de la raíz*" es muy útil para saber si uno de los irreducibles mónicos de grado 1 aparece o no en la factorización de un polinomio de $K[x]$.

Proposición 6.4.11 (Ruffini). *Dado $\phi \in K[x]$ y $\alpha \in K$, se verifica que $(x-\alpha)|\phi \Leftrightarrow \phi(\alpha) = 0$.*

Demostración. $\phi = (x-\alpha)\psi$ en $K[x]$, entonces $\phi(\alpha) = (\alpha-\alpha)\psi(\alpha) = 0\psi(\alpha) = 0$. Recíprocamente, Si $\phi(\alpha) = 0$, al dividir ϕ entre $x-\alpha$, será $\phi = (x-\alpha)\psi(x) + \beta$, para un cierto $\beta \in K$. Pero entonces $0 = \phi(\alpha) = 0\psi(\alpha) + \beta = \beta$ y $\phi = (x-\alpha)\psi(x)$. Por tanto $(x-\alpha)|\phi$. ■

Corolario 6.4.12. *Si $\phi \in K[x]$ tiene grado 2 o 3, entonces ϕ es irreducible si y solo si no tiene raíces K.*

Demostración. Si ϕ tiene una raíz α, entonces $x-\alpha/\phi$ y ϕ no es irreducible. Recíprocamente, si ϕ no es irreducible, sería $\phi = \phi_1\phi_2$ donde ninguno de estos es de grado cero. Pero entonces uno es de grado uno y, asociado a uno de la forma $x-\alpha$. Luego $x-\alpha|\phi$ y $\phi(\alpha) = 0$. ■

Para polinomios con coeficientes reales, utilizando lo anterior, más adelante, se os probará lo siguiente.

Teorema 6.4.13. *En $\mathbb{R}[x]$ los únicos polinomios irreducibles son los de grado 1 y los de grado 2 de la forma ax^2+bx+c tales que $b^2-4ac<0$. Por tanto, los mónicos irreducibles de $\mathbb{R}[x]$ son los $x+a$, y x^2+bx+c con $a,b,c \in \mathbb{R}$ y $b^2-4c<0$.*

Con el anterior criterio de Ruffini, por ejemplo, podemos incluso listar todos los irreducibles mónicos de grado 2 en los primeros $\mathbb{Z}_p[x]$:

- En $\mathbb{Z}_2[x]$: x^2+x+1.

- En $\mathbb{Z}_3[x]$: x^2+1, x^2+x+2, x^2+2x+2.

- En $\mathbb{Z}_5[x]$: x^2+2, x^2+3, x^2+x+1, x^2+x+2, x^2+2x+3, x^2+2x+4, x^2+3x+3, x^2+3x+4, x^2+4x+1, x^2+4x+2.

Y de grado 3:

- En $\mathbb{Z}_2[x]$: x^3+x+1, x^3+x^2+1.

- En $\mathbb{Z}_3[x]$: x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+2x^2+1, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+x+1, x^3+2x^2+2x+2.

Con esa información, ya podemos factorizar completamente polinomios en $\mathbb{Z}_2[x]$ y en $\mathbb{Z}_3[x]$ de hasta grado 7, y en $\mathbb{Z}_5[x]$ de hasta grado 5.

EJEMPLOS. 1. *Factorizar $f = x^4+x^3+x^2+x+1$ en $\mathbb{Z}_2[x]$.*

Vemos que ni 0 ni 1 son raíces, por tanto f no tiene factores irreducibles de grado 1. Pero entonces tampoco los tiene de grado 3. Si tuviese un factor irreducible de grado 2, este sería x^2+x+1. Pero al hacer la división, resulta que $f = (x^2+x+1)x^2 + (x+1)$ y x^2+x+1 no divide a f. Luego f es irreducible.

2. *Factorizar $f = x^5+x^4+1$ en $\mathbb{Z}_2[x]$.*

Vemos que ni 0 ni 1 son raíces, por tanto f no tiene factores irreducibles de grado 1, y entonces tampoco los tiene de grado 4. Si tuviese un factor irreducible de grado 2, este sería x^2+1, x^2+x+2 o x^2+2x+2. Dividiendo,

resulta que $f = (x^2+x+2)(x^3+x)+x+1$, $f = (x^2+1)(x^3+x^2+2x)+x+1$, y $f = (x^2+2x+2)(x^3+2x^2)+2$. Luego f es irreducible.

3. *Factorizar* $f = x^5+x^4+x^2+1$ *en* $\mathbb{Z}_3[x]$.

Vemos que $f(0) = 1$, $f(1) = 1$ y $f(2) = f(-1) = -1+1+1+1 = 2$, por tanto f no tiene factores irreducibles de grado 1, y entonces tampoco los tiene de grado 4. Si tuviese un factor irreducible de grado 2, estos podrían ser x^2+1, x^2+x-1 o x^2-x-1, ninguno de los tres lo divide y por tanto el polinomio es irreducible.

Nos ocupamos en lo que sigue del caso específico de polinomios con coeficientes enteros y racionales, esto es, de polinomios en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$, que estudiamos simultáneamente. Recordar que

• *Los irreducibles de grado 0 en* $\mathbb{Z}[x]$ *son los propios irreducibles de* $\mathbb{Z}$, esto es, salvo signo, $2, 3, 5, 7, \ldots$, mientras que en $\mathbb{Q}[x]$ no los hay.

• *Si un polinomio* $f \in \mathbb{Z}[x]$ *de grado* ≥ 1 *es irreducible en* $\mathbb{Z}[x]$*, entonces es primitivo.*

• *Si* f *es primitivo, entonces* f *es irreducible en* $\mathbb{Z}[x]$ *si y solo si lo es en* $\mathbb{Q}[x]$.

• *Todo polinomio de grado* ≥ 1*,* $\phi \in Q[x]$*, se escribe de forma única como* $\phi = \frac{a}{b}f$*, con* $\frac{a}{b} \in \mathbb{Q}$ *y* $f \in \mathbb{Z}[x]$ *primitivo.* Entonces ϕ y f son asociados en $\mathbb{Q}[x]$, por tanto que ϕ es irreducible en $\mathbb{Q}[x]$ si y solo si f lo es en $\mathbb{Z}[x]$. Esto nos permite estudiar la irreducibilidad de polinomios en $\mathbb{Q}[x]$ estudiando la de los polinomios en $\mathbb{Z}[x]$ que son primitivos.

Sabemos que todo polinomio de grado 1 es irreducible en $\mathbb{Q}[x]$, por tanto un polinomio $a+bx \in \mathbb{Z}[x]$, con $b \neq 0$, será irreducible en $\mathbb{Z}[x]$ si y solo si es primitivo, o sea que

• *Un polinomio* $a+bx \in \mathbb{Z}[x]$*, con* $b \neq 0$*, es irreducible en* $\mathbb{Z}[x]$ *si y solo si* $(a, b) = 1$.

Sabemos también que un polinomio en $\mathbb{Q}[x]$ de grado 2 o de grado 3 es irreducible si y solo si no tiene raíces en $\mathbb{Q}$, por tanto

• *Un polinomio de grado* 2 *o* 3 *en* $\mathbb{Z}[x]$ *es irreducible si y solo si es primitivo y no tiene raíces en* $\mathbb{Q}$.

El siguiente hecho es relevante para saber como factorizar un polinomio en $\mathbb{Z}[x]$ que tiene una raíz en $\mathbb{Q}$, y por tanto que no es irreducible.

• *Supongamos* $f \in \mathbb{Z}[x]$ *con* $f(\frac{a}{b}) = 0$*, donde* $(a, b) = 1$*. Entonces* $(bx-a)/f$ *en* $\mathbb{Z}[x]$, y el polinomio $g \in \mathbb{Z}[x]$ tal que $f = (bx-a)g$ se calcula simplemente como el cociente de dividir f entre $bx-a$ en $\mathbb{Q}[x]$.

En efecto, sabemos que $(x-\frac{a}{b})/f$ en $\mathbb{Q}[x]$. Sea ϕ el cociente de dividir f entre $(x-\frac{a}{b})$. Será $f = (x-\frac{a}{b})\phi$. Pongamos $\phi = \frac{c}{d}h$, con $h \in \mathbb{Z}[x]$ primitivo. Entonces $f = (x-\frac{a}{b})\frac{c}{d}h$, de donde $bdf = c(bx-a)h$ y $bd\, c(f) = c$. Luego d/c y concluimos que $\phi \in \mathbb{Z}[x]$. $\square$

La siguiente información, sobre las posible raíces en $\mathbb{Q}$ de un polinomio con coeficientes en $\mathbb{Z}$, es también muy útil.

• *Sea* $f = a_0+a_1x+\cdots a_nx^n \in \mathbb{Z}[x]$*, con* $a_n \neq 0$*. Si* $f(\frac{a}{b}) = 0$*, donde* $(a, b) = 1$*, entonces* a/a_0 *y* b/a_n *en* $\mathbb{Z}$.

En efecto, como tendremos una igualdad en $\mathbb{Z}[x]$ de la forma

$$a_0 + a_1x + \cdots + a_nx^n = (bx-a)(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}),$$

la igualdad entre los correspondientes coeficientes de grado 0, nos dice que $a_0 = a(-b_0)$, y la de los coeficientes de grado n que $a_n = bb_{n-1}$. Por tanto a/a_0 y b/a_n. $\square$.

La observación anterior, tiene aplicaciones inmediatas interesantes. Por ejemplo:

1. *Todas las raíces en $\mathbb{Q}$ de un polinomio mónico $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ están en $\mathbb{Z}$. Por tanto, si este no tiene raíces en $\mathbb{Z}$, tampoco las tiene en $\mathbb{Q}$.*

2. *Si $n \in \mathbb{Z}$ no es un cuadrado en $\mathbb{Z}$, esto es, si $\sqrt{n} \notin \mathbb{Z}$ no es un entero, tampoco lo es en $\mathbb{Q}$, esto es $\sqrt{n} \notin \mathbb{Q}$, es un irracional.* (Ya que si $x^2 - n$ no tiene raíz en $\mathbb{Z}$ tampoco la tiene en $\mathbb{Q}$)

EJEMPLOS. 1. *Factorizar $f = 20x^4 - 10x^3 - 80x^2 + 80x - 20$ en $\mathbb{Z}[x]$.*

Claramente $c(f) = 10$. Entonces $f = 10g = 2 \cdot 5 \cdot g$, con $g = 2x^4 - x^3 - 8x^2 + 8x - 2$, que es primitivo. Sus posibles raíces en $\mathbb{Q}$ son ± 1, $\pm\frac{1}{2}$, y ± 2. Probando, vemos que $g(\frac{1}{2}) = 0$. Por tanto es seguro que $2x - 1/g$ en $\mathbb{Z}[x]$. Hacemos la divisón en $\mathbb{Q}[x]$, y obtenemos $g = (2x-1)(x^3 - 4x + 2)$. El polinomio $x^3 - 4x + 2$ es primitivo, de grado 3, y no tiene raíces en $\mathbb{Q}$ (las únicas posibles son ± 1 y ± 2, y no lo son), luego es irreducible. Así que la factorización en irreducibles de f en $\mathbb{Z}[x]$ es

$$f = 2 \cdot 5 \cdot (2x-1) \cdot (x^3 - 4x + 2).$$

La factorización en $\mathbb{Q}[x]$ sería la misma, solo que 10 es una unidad. Si tomamos como conjunto representativo de los irreducibles en $\mathbb{Q}[x]$ el conjunto P de los irreducibles monicos, la factorización sería

$$f = 20\Big(x - \frac{1}{2}\Big)(x^3 - 4x + 2).$$

2. *Factorizar $f = x^3 + \frac{1}{2}x^2 - x + 3$ en $\mathbb{Q}[x]$.* Pongamos $f = \frac{1}{2}g$ con $g = 2x^3 + x^2 - 2x + 6 \in \mathbb{Z}[x]$ primitivo. Sus posibles raíces en $\mathbb{Q}$ son ± 1, ± 2, ± 3, ± 6, $\pm\frac{1}{2}$ y $\pm\frac{3}{2}$. Probando, vemos que $g(\frac{3}{2}) = 0$, y por tanto $(2x-3)/g$ en $\mathbb{Z}[x]$. Haciendo la división en $\mathbb{Q}[x]$, obtenemos que $g = (2x-3)(x^2 - 2x + 2)$. El polinomio $x^2 + 2x + 2$ no tiene raíces en $\mathbb{Q}$, y es por tanto irreducible. Así que la factorización buscada es

$$f = \frac{1}{2}(2x-3)(x^2 - 2x + 2) = \Big(x - \frac{2}{3}\Big)(x^2 - 2x + 2).$$

• *El criterio de reducción módulo un primo.* Sea $R_p : \mathbb{Z} \to \mathbb{Z}_p$ el homomorfismo que asigna a cada entero su resto módulo un primo p de $\mathbb{Z}$. Tendremos el homomorfismo inducido $R_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, tal que $R_p(\sum_{i\geq 0} a_i x^i) = \sum_{i\geq 0} R_p(a_i)x^i$.

Proposición 6.4.14. *Sea $f \in \mathbb{Z}[x]$ tal que $R_p(f)$ y f tienen el mismo grado. Si $R_p(f)$ no tiene divisores de grado r, con $0 < r < gr(f)$, en $\mathbb{Z}_p[x]$, entonces f tampoco tiene divisores de grado r en $\mathbb{Z}[x]$. En particular, si f es primitivo y $R_p(f)$ es irreducible, entonces f es irreducible.*

DEMOSTRACIÓN. Supongamos que fuera $f = gh$ en $\mathbb{Z}[x]$, con $gr(g) = r$ y, digamos, $gr(h) = s$, de manera que $r + s = gr(f)$. Tendríamos también que $R_p(f) = R_p(g)\,R_p(h)$. Como, obviamente $gr(R_p(g)) \leq r$ y $gr(R_p(h)) \leq s$, y $gr(R_p(f)) = gr(f) = r + s = gr(R_p(g)) + gr(R_p(h))$, necesariamente $gr(R_p(g)) = r$, lo que es imposible por hipótesis. □

EJEMPLOS. 1. *El polinomio $f = x^4 + 3x^2 - 2x + 5$ es irreducible en $\mathbb{Z}[x]$ (y en $\mathbb{Q}[x]$).*

Su reducido módulo 2, $R_2(f) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ no tiene raíces y por tanto no tiene divisores de grado 1 ni de grado 3. Luego f tampoco los tiene. (Esto también se podría ver directamente viendo que ninguna de las posibles raíces de f en $\mathbb{Q}$, $\pm 1, \pm 5$ lo es). Las únicas posibilidades para f, que es primitivo, es que sea irreducible o factorize como producto de dos irreducibles de grado 2. $R_2(f)$ si tiene, sin embargo, divisores de grado 2, pues $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ es su factorización en irreducibles y no obtenemos información sobre los posibles factores irreducibles de grado dos de f. Pero podemos considerar $R_3(f) = x^4 + x + 2 \in \mathbb{Z}_3[x]$. Este resulta irreducible, pues no tiene raíces y al dividirlo por los tres irreducibles de grado 2 los restos son no nulos. Luego $R_3(f)$ es irreducible y, por tanto, f también lo es. □

2. *El polinomio $f = x^4 + 3x^3 + 5x^2 + 1$ es irreducible en $\mathbb{Z}[x]$ (y en $\mathbb{Q}[x]$).*

Su reducido módulo 2, $R_2(f) = x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ tiene a 1 como raíz, y descompone como $R_2(f) = (x+1)(x^3 + x + 1)$. El polinomio $(x^3 + x + 1) \in \mathbb{Z}_2[x]$ es de grado 3 y no tiene raíces, luego es irreducible. Así que la anterior es la factorización de $R_2(f)$ en irreducibles. Claramente entonces $R_2(f)$ no tiene divisores de grado 2, luego f tampoco los tiene en $\mathbb{Z}[x]$. Las únicas posibilidades para f, que es primitivo, es que sea irreducible o factorize como producto de uno de grado uno por uno de grado 3. Pero no tiene raíces en $\mathbb{Q}$, ya que las únicas posibles son ± 1, y no lo son. Luego f es irreducible. □

3. *El polinomio* $\phi = \frac{2}{9}x^6 + \frac{2}{3}x^5 - \frac{2}{9}x^4 + \frac{2}{3}x^3 + \frac{2}{3}x^2 + \frac{2}{3}x - \frac{2}{9}$ *es irreducible en* $\mathbb{Q}[x]$.

Como $\phi = \frac{2}{9}f$, con $f = x^6 + 3x^5 - x^4 + 3x^2 + 3x - 1$, ϕ será irreducible en $\mathbb{Q}[x]$ si y solo si f lo es en $\mathbb{Z}[x]$. Ahora, $R_2(f) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ factoriza como producto de irreducibles en $\mathbb{Z}_2[x]$ como $R_2(f) = (x^3 + x + 1)(x^3 + x^2 + 1)$. Podemos concluir entonces que f no tiene divisores de grado 1, 2, 4 o 5 en $\mathbb{Z}[x]$. $R_3(f) = x^6 - x^4 - 1$ factoriza como producto de irreducibles en $\mathbb{Z}_3[x]$ como $R_3(f) = (x^2 + 1)(x^4 + x^2 - 1)$, lo que nos permite concluir que f no tiene divisores en $\mathbb{Z}[x]$ de grado 3. Luego f es irreducible, ya que no tiene divisores de grado 0 al ser primitivo.

4. *Factorizar* $f = x^5 + 8x^4 + 18^3 + 11x^2 + 7x + 3$ *en* $\mathbb{Z}[x]$. Sus posibles raíces son ± 1 y ± 3. Probando, vemos que $f(-3) = 0$. Dividiendo en $\mathbb{Q}[x]$, obtenemos que $f = (x+3)g$, con $g = x^4 + 5x^3 + 3x^2 + 2x + 1$. Las posibles raíces de g en $\mathbb{Q}$ son ± 1, y comprobamos que ninguna lo es. Luego g no tiene divisores de grado 1 ni de grado 3. Considerando $R_2(g) = x^4 + x^3 + x^2 + 1$, vemos que tiene a 1 como raíz y que factoriza en irreducibles en $\mathbb{Z}_2[x]$ como $R_2(g) = (x+1)(x^3 + x + 1)$, de donde concluimos que $R_2(g)$, y entonces g, no tiene divisores de grado 2. Luego g es irreducible y la factorización buscada es $f = (x+3)(x^4 + x^3 + x^2 + 1)$.

- *El criterio de Eisenstein*.

Proposición 6.4.15. *Sea* $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, *con* $a_n \neq 0$, *un polinomio primitivo. Entonces* f *es irreducible si existe un primo* $p \in \mathbb{Z}$ *verificando cualquiera de las siguientes condiciones:*

1. p/a_i *para todo* $i = 0, 1, \ldots, n-1$, *y* p^2 *no divide a* a_0.
2. p/a_i *para todo* $i = 1, \ldots, n$, *y* p^2 *no divide a* a_n.

DEMOSTRACIÓN. Lo demostramos en el primer supuesto. La demostración para el segundo es paralela. Supongamos $f = gh$ con $g = b_0 + b_1x + \cdots + b_rx^r$ y $h = c_0 + c_1x + \cdots + c_rx^s$, donde $b_r \neq 0 \neq c_s$ y $r, s \geq 1$. Como p/a_0 y $a_0 = b_0c_0$, p tiene que dividir a b_0 o a c_0. Pero como p^2 no divide a a_0, p no puede dividir simultáneamente a ambos. Supongamos que p/b_0, y entonces no a c_0. Como f es primitivo, y p divide a todos los coeficientes en grados menores que n, p no puede dividir a $a_n = b_rc_s$. Por tanto que p no divide ni a b_r ni a c_s. Sea i el primer natural tal que p no divide a b_i. sera $0 < i < n$, pues p/b_0 e $i \leq r < n$. Como el coeficiente a_i de f es

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c1 + b_ic_0$$

y p/a_i, concluimos que p/b_ic_0. Pero p es primo y p no divide ni a b_i ni a c_0, esto es una contradicción. □

EJEMPLOS. 1. *El polinomio* $2x^5 - 6x^3 + 9x^2 - 15$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p = 3$.)

2. *El polinomio* $3x^7 - 6x^5 + 14x^2 - 10x^2 + 2x - 18$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p = 2$.)

3. *El polinomio* $6x^4 + 9x^3 - 3x^2 + 10$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p = 3$.

4. *El polinomio* $3x^7-70x^3+140$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p=7$. Observar que no vale el primo $p=2$ para aplicar el criterio, pues $140=5\cdot 4\cdot 7$.)

• *Traslación en la indeterminada*. Sea $a\in\mathbb{Z}$ y $T_a:\mathbb{Z}[x]\to\mathbb{Z}[x]$ el homomorfismo es la identidad en los coeficientes y asigna a x el binomio $T_a(x)=x+a$. Esto es,

$$T_a\Big(\sum_{i\geq 0} a_i x^i\Big)=\sum_{i\geq 0} a_i(x+a)^i.$$

Es fácil ver que T_a es un isomorfismo, con inverso T_{-a}. Además, para cualquier $f\in\mathbb{Z}[x]$, f y $T_a(f)$ tienen el mismo grado.

Proposición 6.4.16. *Sea* $f\in\mathbb{Z}[x]$. *Si* $T_a(f)$ *es irreducible para algún* $a\in\mathbb{Z}$, *entonces* f *también lo es.*

Demostración. Si f tuviera un divisor propio, digamos g, entonces sería $f=gh$ para un cierto $h\in\mathbb{Z}[x]$, donde ni g ni h son ± 1. Entonces, tendríamos también que $T_a(f)=T_a(g)T_a(h)$, donde ni $T_a(g)$ ni $T_a(h)$ son ± 1, lo que estaría en contradicción con el supuesto de que $T_a(f)$ es irreducible. ■

EJEMPLO. *El polinomio* $f=x^4+1$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*).*

$T_1(x^4+1)=(x+1)^4+1=x^4+4x^3+6x^2+4x+2$, que es irreducible por Eisenstein para $p=2$.